Program Optimization

Peter Lammich

WS 2016/17
Overview by Lecture

- Oct 20: Slide 3
- Oct 26: Slide 36
- Oct 27: Slide 65
- Nov 3: Slide 95
- Nov 9: Slide 116
- Nov 10: Slide 128
- Nov 16: Slide 140
- Nov 17: Slide 157
- Nov 23: Slide 178
- Nov 24: Slide 202
- Nov 30: Slide 211
- Dec 1: Slide 224
- Dec 8: Slide 243
- Dec 14: Slide 259
- Dec 15: Slide 273
- Dec 21: Slide 287
- Dec 22: Slide 301
Organizational Issues

Lectures Wed 10:15-11:45 and Thu 10:15-11:45 in MI 00.13.009A
Organizational Issues

Lectures  Wed 10:15-11:45 and Thu 10:15-11:45 in MI 00.13.009A

Tutorial  Fri 8:30-10:00 (Ralf Vogler <ralf.vogler@mytum.de>)
- Homework will be corrected


Exam  Written (or Oral), Bonus for Homework!
- ≥50% of homework ⇒ 0.3/0.4 better grade on first exam attempt. Only if passed w/o bonus!
Organizational Issues

Lectures  Wed 10:15-11:45 and Thu 10:15-11:45 in MI 00.13.009A

Tutorial  Fri 8:30-10:00 (Ralf Vogler <ralf.vogler@mytum.de>)
          • Homework will be corrected

Exam    Written (or Oral), Bonus for Homework!
          • $\geq 50\%$ of homework $\Rightarrow$ 0.3/0.4 better grade

On first exam attempt. Only if passed w/o bonus!

Organizational Issues

Lectures  Wed 10:15-11:45 and Thu 10:15-11:45 in MI 00.13.009A
Tutorial  Fri 8:30-10:00 (Ralf Vogler <ralf.vogler@mytum.de>)
  • Homework will be corrected
Exam     Written (or Oral), Bonus for Homework!
  • $\geq 50\%$ of homework $\implies 0.3/0.4$ better grade
  On first exam attempt. Only if passed w/o bonus!
Organizational Issues

Lectures  Wed 10:15-11:45 and Thu 10:15-11:45 in MI 00.13.009A

Tutorial  Fri 8:30-10:00 (Ralf Vogler <ralf.vogler@mytum.de>)
  • Homework will be corrected

Exam  Written (or Oral), Bonus for Homework!
  • $\geq 50\%$ of homework $\implies 0.3/0.4$ better grade
    On first exam attempt. Only if passed w/o bonus!


How many of you are attending “Semantics” lecture?
We need tutors for Info II lecture. If you are interested, please contact Julian Kranz

julian.kranz@in.tum.de.
Proposed Content

- Avoiding redundant computations
  - E.g. Available expressions, constant propagation, code motion
- Replacing expensive with cheaper computations
  - E.g. peep hole optimization, inlining, strength reduction
- Exploiting Hardware
  - E.g. instruction selection, register allocation, scheduling
- Analysis of parallel programs
  - E.g. threads, locks, data-races
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Removing Superfluous Computations</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Interpretation</td>
</tr>
<tr>
<td>4</td>
<td>Alias Analysis</td>
</tr>
<tr>
<td>5</td>
<td>Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6</td>
<td>Interprocedural Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8</td>
<td>Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Hardware Features</td>
</tr>
<tr>
<td>10</td>
<td>Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Observation 1

Intuitive programs are often inefficient

```c
void swap (int i, int j) {
    int t;
    if (a[i] > a[j]) {
        t = a[j];
        a[j] = a[i];
        a[i] = t;
    }
}
```
Observation 1

Intuitive programs are often inefficient

```c
void swap (int i, int j) {
    int t;
    if (a[i] > a[j]) {
        t = a[j];
        a[j] = a[i];
        a[i] = t;
    }
}
```

- Inefficiencies
  - Addresses computed 3 times
  - Values loaded 2 times
Observation 1

Intuitive programs are often inefficient

```c
void swap (int i, int j) {
    int t;
    if (a[i] > a[j]) {
        t = a[j];
        a[j] = a[i];
        a[i] = t;
    }
}
```

- Inefficiencies
  - Addresses computed 3 times
  - Values loaded 2 times

- Improvements
  - Use pointers for array indexing
  - Store the values of a[i], a[j]
```c
void swap (int *p, int *q) {
    int t, ai, aj;
    ai=*p; aj=*q;
    if (ai > aj) {
        t = aj;
        *q = ai;
        *p = t; // t can also be eliminated
    }
}
```
void swap (int *p, int *q) {
    int ai, aj;
    ai=*p; aj=*q;
    if (ai > aj) {
        *q = ai;
        *p = aj;
    }
}
Caveat: Program less intuitive
Observation 2

High-level languages (even C) abstract from hardware (and efficiency) Compiler needs to transform intuitively written programs to hardware. Examples

- Filling of delay slots
- Utilization of special instructions
- Re-organization of memory accesses for better cache behavior
- Removal of (useless) overflow/range checks
Program improvements need not always be correct

- E.g. transform $f() + f()$ to $2*f()$
Observation 3

Program improvements need not always be correct

- E.g. transform $f() + f()$ to $2*f()$
- Idea: Save second evaluation of $f$
Observation 3

Program improvements need not always be correct
- E.g. transform $f(\cdot) + f(\cdot)$ to $2 \times f(\cdot)$
- Idea: Save second evaluation of $f$
- But what if $f$ has side-effects or reads input?
Insight

- Program optimizations have **preconditions**
- These must be
  - Formalized
  - Checked
- It must be **proved** that optimization is **correct**
  - I.e., preserves **semantics**
Observation 4

Optimizations techniques depend on programming language

- What inefficiencies occur
- How analyzable is the language
- How difficult it is to prove correctness
Example: Java

- (Unavoidable) inefficiencies
  - Array bound checks
  - Dynamic method invocation
  - Bombastic object organization

- Analyzability
  - No pointer arithmetic, no pointers into stack
- Dynamic class loading
  - Reflection, exceptions, threads

- Correctness proof
  - Well-defined semantics (more or less)
- Features, features, features
  - Libraries with changing behavior
Example: Java

- (Unavoidable) inefficiencies
  - Array bound checks
  - Dynamic method invocation
  - Bombastic object organization

- Analyzability
  + No pointer arithmetic, no pointers into stack
    - Dynamic class loading
    - Reflection, exceptions, threads
Example: Java

- (Unavoidable) inefficiencies
  - Array bound checks
  - Dynamic method invocation
  - Bombastic object organization

- Analyzability
  + No pointer arithmetic, no pointers into stack
  - Dynamic class loading
  - Reflection, exceptions, threads

- Correctness proof
  + Well-defined semantics (more or less)
  - Features, features, features
  - Libraries with changing behavior
In this course

- Simple imperative programming language
  
  \[
  \begin{align*}
  R &= e \\
  R &= M[e] \\
  M[e_1] &= e_2 \\
  \text{if} \ (e) \ &\ ... \ \text{else} \ ... \\
  \text{goto} \ \text{label}
  \end{align*}
  \]

  Assignment  
  Load  
  Store  
  Conditional branching  
  Unconditional branching

- Registers, assuming infinite supply
- Integer-valued expressions over constants, registers, operators
- Memory, addressed by integer $\geq 0$, assuming infinite memory
Note

- For the beginning, we omit procedures
  - Focus on *intra-procedural* optimizations
  - External procedures taken into account via statement \( f() \)
    - unknown procedure
    - may arbitrarily mess around with memory and registers
- Intermediate Language, in which (almost) everything can be translated
Example: Swap

```c
void swap (int i, int j) {
    int t;
    if (a[i] > a[j]) {
        t = a[j];
        a[j] = a[i];
        a[i] = t;
    }
}
```

1: A\_1 = A\_0 + 1*i  // R\_1 = a[i]
2: R\_1 = M[A\_1]
3: A\_2 = A\_0 + 1*j  // R\_2 = a[j]
4: R\_2 = M[A\_2]
5: if (R\_1 > R\_2) {
6:    A\_3 = A\_0 + 1*j  // t = a[j]
7:    t = M[A\_3]
8:    A\_4 = A\_0 + 1*j  // a[j] = a[i]
9:    A\_5 = A\_0 + 1*i
10:   R\_3 = M[A\_5]
11:   M[A\_4] = R\_3
12:   A\_6 = A\_0 + 1*i  // a[i] = t
13:   M[A\_6] = t
14: }
```
Example: Swap

```c
void swap (int i, int j) {
  int t;
  if (a[i] > a[j]) {
    t = a[j];
    a[j] = a[i];
    a[i] = t;
  }
}
```

Assume $A_0$ contains address of array $a$

1: $A_1 = A_0 + 1*i$  // $R_1 = a[i]$
2: $R_1 = M[A_1]$
3: $A_2 = A_0 + 1*j$  // $R_2 = a[j]$
4: $R_2 = M[A_2]$
5: if $(R_1 > R_2)$ {
6:   $A_3 = A_0 + 1*j$  // $t = a[j]$
7:   $t = M[A_3]$
8:   $A_4 = A_0 + 1*j$  // $a[j] = a[i]$
9:   $A_5 = A_0 + 1*i$
0:   $R_3 = M[A_5]$
1:   $M[A_4] = R_3$
2:   $A_6 = A_0 + 1*i$  // $a[i]=t$
3:   $M[A_6] = t$
}````
Optimizations

1. \(1 \times R \mapsto R\)

2. Re-use of sub-expressions

\[
\begin{align*}
A_1 &= A_5 = A_6, \\
A_2 &= A_3 = A_4, \\
M[A_1] &= M[A_5], \\
M[A_2] &= M[A_3], \\
R_1 &= R_3, \\
R_2 &= t
\end{align*}
\]
Now we have

1: \( A_1 = A_0 + i \)
2: \( R_1 = M[A_1] \)
3: \( A_2 = A_0 + j \)
4: \( R_2 = M[A_2] \)
5: \[ \text{if } (R_1 > R_2) \{ \]
6: \( M[A_2] = R_1 \)
7: \( M[A_1] = R_2 \)

Original was:

1: \( A_1 = A_0 + 1*i \) //\( R_1 = a[i] \)
2: \( R_1 = M[A_1] \)
3: \( A_2 = A_0 + 1*j \) //\( R_2 = a[j] \)
4: \( R_2 = M[A_2] \)
5: \[ \text{if } (R_1 > R_2) \{ \]
6: \( A_3 = A_0 + 1*j \) //\( t = a[j] \)
7: \( t = M[A_3] \)
8: \( A_4 = A_0 + 1*j \) //\( a[j] = a[i] \)
9: \( A_5 = A_0 + 1*i \)
0: \( R_3 = M[A_5] \)
1: \( M[A_4] = R_3 \)
2: \( A_6 = A_0 + 1*i \) //\( a[i]=t \)
3: \( M[A_6] = t \)
4: \]
## Gain

<table>
<thead>
<tr>
<th></th>
<th>before</th>
<th>after</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>*</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>&gt;</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>load</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>store</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$R =$</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>
Table of Contents

1 Introduction

2 Removing Superfluous Computations
   Repeated Computations
   Background 1: Rice’s theorem
   Background 2: Operational Semantics
   Available Expressions
   Background 3: Complete Lattices
   Fixed-Point Algorithms
   Monotonic Analysis Framework
   Dead Assignment Elimination
   Copy Propagation
   Summary

3 Abstract Interpretation

4 Alias Analysis

5 Avoiding Redundancy (Part II)

6 Interprocedural Analysis

7 Analysis of Parallel Programs

8 Replacing Expensive by Cheaper Operations

9 Exploiting Hardware Features

10 Optimization of Functional Programs
Idea

If same value is computed repeatedly

- Store it after first computation
- Replace further computations by look-up
Idea

If same value is computed repeatedly
  • Store it after first computation
  • Replace further computations by look-up

Method
  • Identify repeated computations
  • Memorize results
  • Replace re-computation by memorized value
Example

\[
x = 1 \\
y = M[42]
\]

A: \[ r_1 = x + y \]

\[ \ldots \]

B: \[ r_2 = x + y \]
Example

\begin{verbatim}
x = 1
y = M[42]
A: r1 = x + y
...  
B: r2 = x + y
\end{verbatim}

- Repeated computation of \(x+y\) at \(B\), if
  - \(A\) is \textbf{always} executed before \(B\)
  - \(x+y\) has the same value at \(A\) and \(B\).
Example

\begin{align*}
  x &= 1 \\
  y &= M[42] \\
  A: \quad r_1 &= x + y \\
  \quad \ldots \\
  B: \quad r_2 &= x + y
\end{align*}

- Repeated computation of \( x+y \) at \( B \), if
  - \( A \) is always executed before \( B \)
  - \( x+y \) has the same value at \( A \) and \( B \).

- We need
  - Operational semantics
  - Method to identify (at least some) repeated computations
# Table of Contents

1. Introduction

2. Removing Superfluous Computations
   - Repeated Computations
   - Background 1: Rice's theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Rice’s theorem (informal)

All non-trivial semantic properties of a Turing-complete programming language are undecidable.
Rice’s theorem (informal)

All non-trivial semantic properties of a Turing-complete programming language are undecidable.

Consequence  We cannot write the ideal program optimizer :(  

Rice’s theorem (informal)

All non-trivial semantic properties of a Turing-complete programming language are undecidable.

Consequence  We cannot write the ideal program optimizer :(  

But  Still can use approximate approaches  

- Approximation of semantic property  
- Show that transformation is still correct
Rice’s theorem (informal)

All non-trivial semantic properties of a Turing-complete programming language are undecidable.

Consequence  We cannot write the ideal program optimizer :(  
  But  Still can use approximate approaches  
    • Approximation of semantic property  
    • Show that transformation is still correct

Example: Only identify subset of repeated computations.
# Table of Contents

1. Introduction

2. **Removing Superfluous Computations**
   - Repeated Computations
   - Background 1: Rice's theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

\[
\begin{align*}
A_1 &= A_0 + 1 \times i \\
R_1 &= M[A_1] \\
A_2 &= A_0 + 1 \times j \\
R_2 &= M[A_2] \\
\text{Neg}(R_1 > R_2) &\quad \text{Pos}(R_1 > R_2) \\
A_3 &= A_0 + 1 \times j \\
\ldots
\end{align*}
\]
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

\[
\begin{align*}
A_1 &= A_0 + 1 \times i \\
R_1 &= M[A_1] \\
A_2 &= A_0 + 1 \times j \\
R_2 &= M[A_2] \\
\text{Neg}(R_1 > R_2) &\quad \text{Pos}(R_1 > R_2)
\end{align*}
\]

State:

<table>
<thead>
<tr>
<th></th>
<th>(A_0)</th>
<th>(M[0..4])</th>
<th>(i)</th>
<th>(j)</th>
<th>(A_1)</th>
<th>(A_2)</th>
<th>(R_1)</th>
<th>(R_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1,2,3,4,5</td>
<td>2</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

State:

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_0$</td>
<td>$M[0..4]$</td>
<td>i</td>
<td>j</td>
<td>$A_1$</td>
<td>$A_2$</td>
</tr>
<tr>
<td>0</td>
<td>1,2,3,4,5</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>-</td>
</tr>
</tbody>
</table>

\[ A_1 = A_0 + l \times i \]
\[ R_1 = M[A_1] \]
\[ A_2 = A_0 + l \times j \]
\[ R_2 = M[A_2] \]
\[ \text{Neg}(R_1 > R_2) \]
\[ \text{Pos}(R_1 > R_2) \]
\[ A_3 = A_0 + l \times j \]

...
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

\[ \begin{align*}
A_1 &= A_0 + 1 \times i \\
R_1 &= M[A_1] \\
A_2 &= A_0 + 1 \times j \\
R_2 &= M[A_2] \\
\text{Neg}(R_1 > R_2) &\rightarrow \text{Pos}(R_1 > R_2) \\
A_3 &= A_0 + 1 \times j
\end{align*} \]

State:

\[
\begin{array}{cccccccc}
A_0 & M[0..4] & i & j & A_1 & A_2 & R_1 & R_2 \\
0 & 1,2,3,4,5 & 2 & 4 & 2 & - & 3 & -
\end{array}
\]
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)

Represent program as control flow graph (CFG)

\[
\begin{align*}
A_1 &= A_0 + 1 \times i \\
R_1 &= M[A_1] \\
A_2 &= A_0 + 1 \times j \\
R_2 &= M[A_2] \\
\text{Neg}(R_1 > R_2) &\quad \text{Pos}(R_1 > R_2)
\end{align*}
\]

State:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A_0</td>
<td>M[0..4]</td>
<td>i</td>
<td>j</td>
<td>A_1</td>
<td>A_2</td>
<td>R_1</td>
<td>R_2</td>
</tr>
<tr>
<td>0</td>
<td>1,2,3,4,5</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

```
start
A_1 = A_0 + 1 * i

R_1 = M[A_1]

A_2 = A_0 + 1 * j

R_2 = M[A_2]

Neg(R_1 > R_2)  Pos(R_1 > R_2)

end

A_3 = A_0 + 1 * j
```

State:

<table>
<thead>
<tr>
<th></th>
<th>M[0..4]</th>
<th>i</th>
<th>j</th>
<th>A_1</th>
<th>A_2</th>
<th>R_1</th>
<th>R_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1,2,3,4,5</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
Small-step operational semantics

Intuition: Instructions modify state (registers, memory)
Represent program as control flow graph (CFG)

\[
\text{State:}
\begin{array}{cccc|c|c|ccc}
\text{A}_0 & \text{M}[0..4] & \text{i} & \text{j} & \text{A}_1 & \text{A}_2 & \text{R}_1 & \text{R}_2 \\
0 & 1,2,3,4,5 & 2 & 4 & 2 & 4 & 3 & 5 \\
\end{array}
\]
Formally (I)

Definition (Registers and Expressions)
Reg is an infinite set of register names. Expr is the set of expressions over these registers, constants and a standard set of operations.

Note: We do not formally define the set of operations here
Formally (I)

Definition (Registers and Expressions)

\( \text{Reg} \) is an infinite set of register names. \( \text{Expr} \) is the set of expressions over these registers, constants and a standard set of operations.

Note: We do not formally define the set of operations here.

Definition (Action)

\( \text{Act} = \text{Nop} \mid \text{Pos}(e) \mid \text{Neg}(e) \mid R = e \mid R = M[e] \mid M[e_1] = e_2 \)

where \( e, e_1, e_2 \in \text{Expr} \) are expressions and \( R \in \text{Reg} \) is a register.
Formally (I)

Definition (Registers and Expressions)
Reg is an infinite set of register names. Expr is the set of expressions over these registers, constants and a standard set of operations.

Note: We do not formally define the set of operations here

Definition (Action)
Act = Nop | Pos(e) | Neg(e) | \( R = e \) | \( R = M[e] \) | \( M[e_1] = e_2 \)
where \( e, e_1, e_2 \in \text{Expr} \) are expressions and \( R \in \text{Reg} \) is a register.

Definition (Control Flow Graph)
An edge-labeled graph \( G = (V, E, v_0, V_{\text{end}}) \) where \( E \subseteq V \times \text{Act} \times V, v_0 \in V, V_{\text{end}} \subseteq V \) is called control flow graph (CFG).
Formally (I)

Definition (Registers and Expressions)
Reg is an infinite set of register names. Expr is the set of expressions over these registers, constants and a standard set of operations.

Note: We do not formally define the set of operations here

Definition (Action)
Act = Nop | Pos(e) | Neg(e) | R = e | R = M[e] | M[e₁] = e₂
where e, e₁, e₂ ∈ Expr are expressions and R ∈ Reg is a register.

Definition (Control Flow Graph)
An edge-labeled graph $G = (V, E, v₀, V_{end})$ where $E ⊆ V × Act × V$, $v₀ ∈ V$, $V_{end} ⊆ V$ is called control flow graph (CFG).

Definition (State)
A state $s ∈ State$ is represented by a pair $s = (ρ, μ)$, where

$ρ : Reg → int$ is the content of registers

$μ : int → int$ is the content of memory
Formally (II)

Definition (Value of expression)

\[[e]_\rho \in \text{int}\] is the value of expression \(e\) under register content \(\rho\).
Formally (II)

Definition (Value of expression)
\([e]_\rho : \text{int}\) is the value of expression \(e\) under register content \(\rho\).

Definition (Effect of action)
The effect \(\lbrack a \rbrack\) of an action is a partial function on states:
Formally (II)

Definition (Value of expression)
$\llbracket e \rrbracket_\rho : \text{int}$ is the value of expression $e$ under register content $\rho$.

Definition (Effect of action)
The effect $\llbracket a \rrbracket$ of an action is a partial function on states:

$$\llbracket \text{Nop} \rrbracket (\rho, \mu) := (\rho, \mu)$$
Formally (II)

Definition (Value of expression)
$[[e]]_{\rho}: \text{int}$ is the value of expression $e$ under register content $\rho$.

Definition (Effect of action)
The effect $[[a]]$ of an action is a partial function on states:

- $[[\text{Nop}]](\rho, \mu) := (\rho, \mu)$
- $[[\text{Pos}(e)]](\rho, \mu) := \begin{cases} (\rho, \mu) & \text{if } [[e]]_{\rho} \neq 0 \\ \text{undefined} & \text{otherwise} \end{cases}$
Formally (II)

Definition (Value of expression)
\([e]_\rho : \text{int}\) is the value of expression \(e\) under register content \(\rho\).

Definition (Effect of action)
The effect \([a]\) of an action is a partial function on states:

- \([\text{Nop}]\)(\(\rho, \mu\)) := (\(\rho, \mu\))

- \([\text{Pos}(e)]\)(\(\rho, \mu\)) := \begin{cases} (\rho, \mu) & \text{if } [e]_\rho \neq 0 \\ \text{undefined} & \text{otherwise} \end{cases}

- \([\text{Neg}(e)]\)(\(\rho, \mu\)) := \begin{cases} (\rho, \mu) & \text{if } [e]_\rho = 0 \\ \text{undefined} & \text{otherwise} \end{cases}
Formally (II)

Definition (Value of expression)
\( \llbracket e \rrbracket_\rho : \text{int} \) is the value of expression \( e \) under register content \( \rho \).

Definition (Effect of action)
The effect \( \llbracket a \rrbracket \) of an action is a partial function on states:

\[
\begin{align*}
\llbracket \text{Nop} \rrbracket (\rho, \mu) & := (\rho, \mu) \\
\llbracket \text{Pos}(e) \rrbracket (\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } \llbracket e \rrbracket_\rho \neq 0 \\
\text{undefined} & \text{otherwise}
\end{cases} \\
\llbracket \text{Neg}(e) \rrbracket (\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } \llbracket e \rrbracket_\rho = 0 \\
\text{undefined} & \text{otherwise}
\end{cases} \\
\llbracket R = e \rrbracket (\rho, \mu) & := (\rho(R \mapsto \llbracket e \rrbracket_\rho), \mu)
\end{align*}
\]
Formally (II)

Definition (Value of expression)
\[ [e]_\rho : \text{int} \text{ is the value of expression } e \text{ under register content } \rho. \]

Definition (Effect of action)
The effect \([a]\) of an action is a partial function on states:

\[
\begin{align*}
[Nop](\rho, \mu) & := (\rho, \mu) \\
[Pos(e)](\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } [e]_\rho \neq 0 \\
\text{undefined} & \text{otherwise} 
\end{cases} \\
[Neg(e)](\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } [e]_\rho = 0 \\
\text{undefined} & \text{otherwise} 
\end{cases} \\
[R = e](\rho, \mu) & := (\rho(R \mapsto [e]_\rho), \mu) \\
[R = M[e]](\rho, \mu) & := (\rho(R \mapsto \mu([e]_\rho)), \mu)
\end{align*}
\]
Formally (II)

**Definition (Value of expression)**

\[ [e]_{\rho} : \text{int} \] is the value of expression \( e \) under register content \( \rho \).

**Definition (Effect of action)**

The effect \( [a] \) of an action is a partial function on states:

\[
\begin{align*}
[Nop]\, (\rho, \mu) & := (\rho, \mu) \\
[Pos(e)]\, (\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } [e]_{\rho} \neq 0 \\
\text{undefined} & \text{otherwise}
\end{cases} \\
[Neg(e)]\, (\rho, \mu) & := \begin{cases} 
(\rho, \mu) & \text{if } [e]_{\rho} = 0 \\
\text{undefined} & \text{otherwise}
\end{cases} \\
[R = e]\, (\rho, \mu) & := (\rho(\overset{\rightarrow}{R} \mapsto [e]_{\rho}), \mu) \\
[R = M[e]]\, (\rho, \mu) & := (\rho(\overset{\rightarrow}{R} \mapsto \mu([e]_{\rho})), \mu) \\
[M[e_1] = e_2]\, (\rho, \mu) & := (\rho, \mu([e_1]_{\rho} \mapsto [e_2]_{\rho}))
\end{align*}
\]
Formally (III)

Given a CFG $G = (V, E, v_0, V_{\text{end}})$

**Definition (Path)**

A sequence of adjacent edges $\pi = (v_1, a_1, v_2)(v_2, a_2, v_3) \ldots (v_n, a_n, v_{n+1}) \in E^*$ is called **path from** $v_1$ **to** $v_{n+1}$.

- **Notation** $v_1 \xrightarrow{\pi} v_{n+1}$
- **Convention** $\pi$ is called **path to** $v$ iff $v_0 \xrightarrow{\pi} v$
- **Special case** $v \xrightarrow{\varepsilon} v$ for any $v \in V$
Formally (III)

Given a CFG $G = (V, E, v_0, V_{end})$

Definition (Path)
A sequence of adjacent edges $\pi = (v_1, a_1, v_2)(v_2, a_2, v_3) \ldots (v_n, a_n, v_{n+1}) \in E^*$ is called path from $v_1$ to $v_{n+1}$.

Notation $v_1 \xrightarrow{\pi} v_{n+1}$

Convention $\pi$ is called path to $v$ iff $v_0 \xrightarrow{\pi} v$

Special case $v \xrightarrow{\epsilon} v$ for any $v \in V$

Definition (Effect of edge and path)
The effect of an edge $k = (u, a, v)$ is the effect of its action:

$$\llbracket (u, a, v) \rrbracket := \llbracket a \rrbracket$$

The effect of a path $\pi = k_1 \ldots k_n$ is the composition of the edge effects:

$$\llbracket k_1 \ldots k_n \rrbracket := \llbracket k_n \rrbracket \circ \ldots \circ \llbracket k_1 \rrbracket$$
Formally (IV)

Definition (Computation)
A path $\pi$ is called computation for state $s$, iff its effect is defined on $s$, i.e.,

$$s \in \text{dom}(\llbracket \pi \rrbracket)$$

Then, the state $s' = \llbracket \pi \rrbracket s$ is called result of the computation.
Summary

- **Action**: \( \text{Act} = \text{Nop} \mid \text{Pos}(e) \mid \text{Neg}(e) \mid R = e \mid R = M[e] \mid M[e_1] = e_2 \)
- **CFG**: \( G = (V, E, v_0, V_{\text{end}}) \), \( E \subseteq V \times \text{Act} \times V \)
- **State**: \( s = (\rho, \mu) \), \( \rho : \text{Reg} \rightarrow \text{int} \) (registers), \( \mu : \text{int} \rightarrow \text{int} \) (memory)
- **Value of expression under** \( \rho \): \( \lbrack e \rbrack_\rho : \text{int} \)
- **Effect of action** \( a \): \( \lbrack a \rbrack : \text{State} \rightarrow \text{State} \) (partial)
- **Path** \( \pi \): Sequence of adjacent edges
- **Effect of edge** \( k = (u, a, v) \): \( \lbrack k \rbrack = \lbrack a \rbrack \)
- **Effect of path** \( \pi = k_1 \ldots k_n \): \( \lbrack \pi \rbrack = \lbrack k_n \rbrack \circ \ldots \circ \lbrack k_1 \rbrack \)
- \( \pi \) is computation for \( s \): \( s \in \text{dom}(\lbrack \pi \rbrack) \)
- **Result of computation** \( \pi \) for \( s \): \( \lbrack \pi \rbrack s \)
<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
</tr>
<tr>
<td>2. Removing Superfluous Computations</td>
</tr>
<tr>
<td>2.1. Repeated Computations</td>
</tr>
<tr>
<td>2.2. Background 1: Rice's theorem</td>
</tr>
<tr>
<td>2.3. Background 2: Operational Semantics</td>
</tr>
<tr>
<td>2.4. Available Expressions</td>
</tr>
<tr>
<td>2.5. Background 3: Complete Lattices</td>
</tr>
<tr>
<td>2.6. Fixed-Point Algorithms</td>
</tr>
<tr>
<td>2.7. Monotonic Analysis Framework</td>
</tr>
<tr>
<td>2.8. Dead Assignment Elimination</td>
</tr>
<tr>
<td>2.9. Copy Propagation</td>
</tr>
<tr>
<td>2.10. Summary</td>
</tr>
<tr>
<td>3. Abstract Interpretation</td>
</tr>
<tr>
<td>4. Alias Analysis</td>
</tr>
<tr>
<td>5. Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6. Interprocedural Analysis</td>
</tr>
<tr>
<td>7. Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8. Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9. Exploiting Hardware Features</td>
</tr>
<tr>
<td>10. Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.
**Memorization**

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

\[ R = e \]
\[ T_e = e \]
\[ R = T_e \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

\[ R = e \]
\[ T_e = e \]
\[ R = T_e \]

\[ \text{Neg}(e) \]
\[ \text{Pos}(e) \]

\[ R = M[e] \]
\[ T_e = M[T_e] \]

\[ M[e_1] = e_2 \]
\[ T_e_1 = e_1 \]
\[ T_e_2 = e_2 \]

\[ \text{Neg}(T_e) \]
\[ \text{Pos}(T_e) \]
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

\[ R = e \]
\[ T_e = e \]
\[ T_e = T_e \]

\[ R = M[e] \]
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

\[ R = e \]
\[ T_e = e \]
\[ R = T_e \]

\[ R = M[e] \]
\[ T_e = e \]
\[ R = M[T_e] \]
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

- $R = e$
- $T_e = e$
- $R = T_e$
- $R = M[e]$
- $T_e = e$
- $R = M[T_e]$

$R = e$

$T_e = e$

Neg(e)  Pos(e)

Neg($T_e$)  Pos($T_e$)

$M[e_1] = e_2$
Memorization

First, let's memorize every expression
- **Register** $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

\[ R = e \]

\[ T_e = e \]

\[ R = T_e \]

\[ R = M[e] \]

\[ T_e = e \]

\[ R = M[T_e] \]

\[ M[e_1] = e_2 \]

\[ T_{e1} = e_1 \]

\[ T_{e2} = e_2 \]

\[ M[T_{e1}] = T_{e2} \]
Memorization

First, let’s memorize every expression

- Register $T_e$ memorizes value of expression $e$.
- Assumption: $T_e$ not used in original program.

- Transformation obviously correct
Simple intermediate language (IL)
- Registers, memory, cond/ucond branching
- Compiler: Input → Intermediate Language → Machine Code
- Suitable for analysis/optimization
Last Lecture (Oct 20)

- Simple intermediate language (IL)
  - Registers, memory, cond/ucond branching
  - Compiler: Input $\rightarrow$ Intermediate Language $\rightarrow$ Machine Code
  - Suitable for analysis/optimization

- Control flow graphs, small-step operational semantics
  - Representation for programs in IL
  - Graphs labeled with actions
    - Nop, Pos/Neg, Assign, Load, Store
  - State = Register content, memory content
  - Actions are partial transformation on states
    - undefined - Test failed
Last Lecture (Oct 20)

- Simple intermediate language (IL)
  - Registers, memory, cond/ucond branching
  - Compiler: Input $\rightarrow$ Intermediate Language $\rightarrow$ Machine Code
  - Suitable for analysis/optimization

- Control flow graphs, small-step operational semantics
  - Representation for programs in IL
  - Graphs labeled with actions
    - Nop, Pos/Neg, Assign, Load, Store
  - State = Register content, memory content
  - Actions are partial transformation on states
    - undefined - Test failed

- Memorization Transformation
  - Memorize evaluation of $e$ in register $T_e$
Available Expressions (Semantically)

Definition (Available Expressions in state)
The set of semantically available expressions in state \((\rho, \mu)\) is defined as

\[
A_{\text{exp}}(\rho, \mu) := \{ e \mid \llbracket e \rrbracket_{\rho} = \rho(T_e) \}
\]

Intuition  Register \(T_e\) contains correct value of \(e\).
Available Expressions (Semantically)

Definition (Available Expressions in state)
The set of semantically available expressions in state \((\rho, \mu)\) is defined as

\[
A_{\text{exp}}(\rho, \mu) := \{ e | \semantics{e} \rho = \rho(T_e) \}
\]

Intuition  Register \(T_e\) contains correct value of \(e\).
Border case  All expressions available in undefined state

\[
A_{\text{exp}}(\text{undefined}) := \text{Expr}
\]

(See next slide why this makes sense)
Available Expressions (Semantically)

**Definition (Available Expression at program point)**

The set $A_{exp}(u)$ of semantically available expressions at program point $u$ is the set of expressions that are available in all states that may occur when the program is at $u$.

$$A_{exp}(u) := \bigcap \{A_{exp}([\pi]s) \mid \pi, s. \ V_0 \xrightarrow{\pi} u\}$$
Available Expressions (Semantically)

Definition (Available Expression at program point)
The set $A_{exp}(u)$ of semantically available expressions at program point $u$ is the set of expressions that are available in all states that may occur when the program is at $u$.

$$A_{exp}(u) := \bigcap \{ A_{exp}([\pi]s) \mid \pi, s. \nu_0 \xrightarrow{\pi} u \}$$

Note Actual start state unknown, so all start states $s$ are considered.
Available Expressions (Semantically)

Definition (Available Expression at program point)
The set $A_{exp}(u)$ of semantically available expressions at program point $u$ is the set of expressions that are available in all states that may occur when the program is at $u$.

$$A_{exp}(u) := \bigcap\{A_{exp}(\llbracket \pi \rrbracket s) \mid \pi, s. v_0 \xrightarrow{\pi} u\}$$

Note Actual start state unknown, so all start states $s$ are considered.

Note Above definition is smoother due to $A_{exp}(\text{undefined}) := \text{Expr}$
Simple Redundancy Elimination

**Transformation** Replace edge \((u, T_e = e, v)\) by \((u, \text{Nop}, v)\) if \(e\) semantically available at \(u\).
Simple Redundancy Elimination

**Transformation** Replace edge \((u, T_e = e, v)\) by \((u, \text{Nop}, v)\) if \(e\) semantically available at \(u\).

**Correctness**
- Whenever program reaches \(u\) with state \((\rho, \mu)\), we have \(\llbracket e \rrbracket_\rho = \rho(T_e)\) (That’s exactly how semantically available is defined)
- Hence, \(\llbracket T_e = e \rrbracket(\rho, \mu) = (\rho, \mu) = \llbracket \text{Nop} \rrbracket(\rho, \mu)\)
Simple Redundancy Elimination

Transformation  Replace edge \((u, T_e = e, v)\) by \((u, \text{Nop}, v)\) if \(e\) semantically available at \(u\).

Correctness  

- Whenever program reaches \(u\) with state 
  \((\rho, \mu)\), we have \([e]_{\rho} = \rho(T_e)\) (That’s exactly how semantically available is defined)
- Hence, \([T_e = e](\rho, \mu) = (\rho, \mu) = [\text{Nop}](\rho, \mu)\)

Remaining Problem  How to compute available expressions
Simple Redundancy Elimination

**Transformation** Replace edge \((u, T_e = e, v)\) by \((u, \text{Nop}, v)\) if \(e\) semantically available at \(u\).

**Correctness**
- Whenever program reaches \(u\) with state \((\rho, \mu)\), we have \([e]_\rho = \rho(T_e)\) (That’s exactly how semantically available is defined)
- Hence, \([T_e = e]_\rho(\mu) = (\rho, \mu) = [\text{Nop}]_\rho(\mu)\)

**Remaining Problem** How to compute available expressions

**Precisely** No chance (Rice’s Theorem)
Simple Redundancy Elimination

Transformation  Replace edge \((u, T_e = e, v)\) by \((u, \text{Nop}, v)\) if \(e\) semantically available at \(u\).

Correctness  
- Whenever program reaches \(u\) with state \((\rho, \mu)\), we have \([e]_{\rho} = \rho(T_e)\) (That's exactly how semantically available is defined)
- Hence, \([T_e = e](\rho, \mu) = (\rho, \mu) = [\text{Nop}](\rho, \mu)\)

Remaining Problem  How to compute available expressions

Precisely  No chance (Rice’s Theorem)

Observation  Enough to compute subset of semantically available expressions
- Transformation still correct
Available Expressions (Syntactically)

Idea Expression e (syntactically) available after computation $\pi$
- if $e$ has been evaluated, and no register of $e$ has been assigned afterwards

\[ x + y \]

$\pi$ does not contain assignment to $x$ nor $y$
Available Expressions (Syntactically)

Idea  Expression e (syntactically) available after computation $\pi$

- if e has been evaluated, and no register of e has been assigned afterwards

$x + y$

$\pi$ does not contain assignment to x nor y

Purely syntactic criterion
Available Expressions (Syntactically)

Idea  Expression $e$ (syntactically) available after computation $\pi$

- if $e$ has been evaluated, and no register of $e$ has been assigned afterwards

$x + y$  

$\pi$ does not contain assignment to $x$ nor $y$

Purely syntactic criterion
Can be computed incrementally for every edge
Available Expressions (Computation)

Let \( A \) be a set of available expressions.

Recall: Available \( \leftarrow \) Already evaluated and no reg. assigned afterwards
Available Expressions (Computation)

Let $A$ be a set of available expressions.

Recall: Available $\iff$ Already evaluated and no reg. assigned afterwards

An action $a$ transforms this into the set $[a]^\# A$ of expressions available after $a$ has been executed

$$[\text{Nop}]^\# A := A$$
$$[\text{Pos}(e)]^\# A := A$$
$$[\text{Neg}(e)]^\# A := A$$
$$[T_e = e]^\# A := A \cup \{e\}$$
$$[R = T_e]^\# A := A \setminus \text{Expr}_R$$

$\text{Expr}_R :=$ expressions containing $R$

$$[R = M[e]]^\# A := A \setminus \text{Expr}_R$$
$$[M[e_1] = e_2]^\# A := A$$
Available Expressions (Computation)

\([a]^\#\) is called abstract effect of action \(a\)
Available Expressions (Computation)

\([a]^\#\) is called abstract effect of action \(a\)

Again, the effect of an edge is the effect of its action

\([((u, a, v))]^\# = [a]^\#\)

and the effect of a path \(\pi = k_1 \ldots k_n\) is

\([\pi]^\# := [k_n]^\# \circ \ldots \circ [k_1]^\#\)
Available Expressions (Computation)

%[a]# is called abstract effect of action a
Again, the effect of an edge is the effect of its action

%[(u, a, v)]# = [%a]#

and the effect of a path \( \pi = k_1 \ldots k_n \) is

%[\pi]# := [%k_n]# \circ \ldots \circ [%k_1]#

Definition (Available at \( v \))
The set \( A[v] \) of (syntactically) available expressions at \( v \) is

\[
A[v] := \bigcap \{ [%\pi]# \emptyset \mid \pi \cdot v_0 \xrightarrow{\pi} v \}
\]
Available Expressions (Correctness)

**Idea** Abstract effect corresponds to concrete effect

**Lemma**
\[ A \subseteq A_{exp}(s) \implies [a] \# A \subseteq A_{exp}([a]s) \]

**Proof** Check for every type of action.
Available Expressions (Correctness)

Idea Abstract effect corresponds to concrete effect

Lemma
\[ A \subseteq A_{exp}(s) \implies \llbracket a \rrbracket \# A \subseteq A_{exp}(\llbracket a \rrbracket s) \]

Proof Check for every type of action.

This generalizes to paths

\[ A \subseteq A_{exp}(s) \implies \llbracket \pi \rrbracket \# A \subseteq A_{exp}(\llbracket \pi \rrbracket s) \]
Available Expressions (Correctness)

Idea  Abstract effect corresponds to concrete effect

Lemma

\[ A \subseteq \text{Aexp}(s) \implies [a] \# A \subseteq \text{Aexp}([a]s) \]

Proof  Check for every type of action.

This generalizes to paths

\[ A \subseteq \text{Aexp}(s) \implies [\pi] \# A \subseteq \text{Aexp}([\pi]s) \]

And to program points

\[ A[u] \subseteq \text{Aexp}(u) \]

Recall:

\[ \text{Aexp}(u) = \bigcap \{ \text{Aexp}([\pi]s) \mid \pi, s. \ v_0 \xrightarrow{\pi} u \} \]

\[ A[u] = \bigcap \{ [\pi] \# \emptyset \mid \pi. \ v_0 \xrightarrow{\pi} u \} \]
Summary

1. Transform program to memorize everything
   - Introduce registers $T_e$
2. Compute $A[u]$ for every program point $u$
   - $A[u] = \bigcap \{ [\pi] \# \emptyset \mid \pi. \nu_0 \xrightarrow{\pi} u \}$
3. Replace redundant computations by $\text{Nop}$
   - $(u, T_e = e, \nu) \mapsto (u, \text{Nop}, \nu)$ if $e \in A[u]$
Summary

1. Transform program to memorize everything
   - Introduce registers $T_e$

2. Compute $A[u]$ for every program point $u$
   - $A[u] = \bigcap\{[\pi]^\#\emptyset | \pi. \nu_0 \xrightarrow{\pi} u\}$

3. Replace redundant computations by $\text{Nop}$
   - $(u, T_e = e, \nu) \mapsto (u, \text{Nop}, \nu)$ if $e \in A[u]$

**Warning** Memorization transformation for $R = e$ should only be applied if
- $R \notin \text{Reg}(e)$ (Otherwise, expression immediately unavailable)
- $e \notin \text{Reg}$ (Otherwise, only one more register introduced)
- Evaluation of $e$ is nontrivial (Otherwise, re-evaluation cheaper than memorization)
How to compute $A[u] = \bigcap\{[\pi]\#\emptyset \mid v_0 \xrightarrow{\pi} u\}$

- There may be infinitely many paths to $u$
Remaining Problem

How to compute $A[u] = \bigcap \{ [[\pi]]^{\#} \emptyset \mid v_0 \xrightarrow{\pi} u \}$

- There may be infinitely many paths to $u$

Solution: Collect restrictions to $A[u]$ into a constraint system

$$A[v_0] \subseteq \emptyset$$

$$A[v] \subseteq [a]^{\#}(A[u])$$

for edge $(u, a, v)$
Remaining Problem

How to compute $A[u] = \bigcap\{[[\pi]]_{\neq}^\emptyset \mid v_0 \xrightarrow{\pi} u\}$

- There may be infinitely many paths to $u$

Solution: Collect restrictions to $A[u]$ into a constraint system

$$A[v_0] \subseteq \emptyset$$

$$A[v] \subseteq [[a]]_{\neq}^\emptyset (A[u])$$

for edge $(u, a, v)$

Intuition

Nothing available at start node

For edge $(u, a, v)$: At $v$, at most those expressions are available that would be available if we come from $u$. 
Example

Let’s regard a slightly modified available expression analysis

- Available expressions before memorization transformation has been applied
- Yields smaller examples, but more complicated proofs :)}
Let's regard a slightly modified available expression analysis

- Available expressions before memorization transformation has been applied
- Yields smaller examples, but more complicated proofs :)

\[
\begin{align*}
\text{[Nop]} & \quad A := A \\
\text{[Pos(e)]} & \quad A := A \cup \{e\} \\
\text{[Neg(e)]} & \quad A := A \cup \{e\} \\
\text{[R = e]} & \quad A := (A \cup \{e\}) \setminus \text{Expr}_R \\
\text{[R = M[e]]} & \quad A := (A \cup \{e\}) \setminus \text{Expr}_R \\
\text{[M[e_1] = e_2]} & \quad A := A \cup \{e_1, e_2\}
\end{align*}
\]
Example

Let's regard a slightly modified available expression analysis
- Available expressions before memorization transformation has been applied
- Yields smaller examples, but more complicated proofs :)

\[
\begin{align*}
\text{[Nop]} & \# A := A \\
\text{[Pos}(e)\text{]} & \# A := A \cup \{ e \} \\
\text{[Neg}(e)\text{]} & \# A := A \cup \{ e \} \\
\text{[} R = e \text{]} & \# A := (A \cup \{ e \}) \setminus \text{Expr}_R \\
\text{[} R = M[e] \text{]} & \# A := (A \cup \{ e \}) \setminus \text{Expr}_R \\
\text{[} M[e_1] = e_2 \text{]} & \# A := A \cup \{ e_1, e_2 \}
\end{align*}
\]

Effect of transformation already included in constraint system
Example

\[ y = 1 \]
\[ \text{Neg}(x>1) \]
\[ \text{Pos}(x>1) \]

\[ y = x \times y \]
\[ x = x - 1 \]
Example

\[
\begin{align*}
A[1] & \subseteq \emptyset \\
\text{y = 1} & \quad \text{Neg}(x > 1) \\
\text{Pos}(x > 1) & \\
\text{y} = \text{x} \ast \text{y} & \\
\text{x} = \text{x} - 1 & \\
\end{align*}
\]
Example

\[ A[1] \subseteq \emptyset \]
\[ A[2] \subseteq A[1] \cup \{1\} \setminus \text{Expr}_y \]
Example

\[
\begin{align*}
A[1] \subseteq \emptyset \\
A[2] \subseteq A[1] \cup \{1\} \setminus \text{Expr}_y \\
\end{align*}
\]
$1$

$y = 1$

$\text{Neg}(x > 1)$

$2$

$\text{Pos}(x > 1)$

$3$

$\text{Pos}(x > 1)$

$4$

$\text{Nop}$

$y = x \times y$

$5$

$x = x - 1$

$6$

$\text{Neg}(x > 1)$

$A[1] \subseteq \emptyset$

$A[2] \subseteq A[1] \cup \{1\} \setminus \text{Expr}_y$


$A[4] \subseteq A[3] \cup \{x \times y\} \setminus \text{Expr}_y$
Example

\[
\begin{align*}
A[1] & \subseteq \emptyset \\
A[2] & \subseteq A[1] \cup \{1\} \setminus \text{Expr}_y \\
A[4] & \subseteq A[3] \cup \{x \ast y\} \setminus \text{Expr}_y \\
\end{align*}
\]
Example

$1$

$y = 1$

$\text{Neg}(x > 1)$

$\text{Pos}(x > 1)$

$2$

$3$

$6$

$y = x \times y$

$4$

$\text{Nop}$

$x = x - 1$

$5$

$A[1] \subseteq \emptyset$

$A[2] \subseteq A[1] \cup \{1\} \setminus \text{Expr}_y$


$A[4] \subseteq A[3] \cup \{x \times y\} \setminus \text{Expr}_y$


Example

Neg(x>1) → Pos(x>1)

y = 1
y = x*y
x = x - 1

Solution:

A[1] = \emptyset
A[2] = \{1\}
A[3] = \{1, x > 1\}
A[4] = \{1, x > 1\}
A[5] = \{1\}
A[6] = \{1, x > 1\}
Example

Also a solution:

\[ A[1] = \emptyset \]
\[ A[2] = \emptyset \]
\[ A[3] = \emptyset \]
\[ A[4] = \emptyset \]
\[ A[5] = \emptyset \]
\[ A[6] = \emptyset \]
Wanted

- **Maximally large solution**
  - Intuitively: Most precise information
Wanted

- **Maximally large** solution
  - Intuitively: Most precise information
- An **algorithm** to compute this solution
Naive Fixpoint Iteration (Sketch)

1. Initialize every $A[u] = \text{Expr}$
   - Expressions actually occurring in program!
2. Evaluate RHSs
3. Update LHSs by intersecting with values of RHSs
4. Repeat (goto 2) until values of $A[u]$ stabilize
Naive Fixpoint Iteration (Example)

- On whiteboard!
Naive Fixpoint Iteration (Correctness)

Why does the algorithm terminate?

• In each step, sets get smaller
• This can happen at most $|\text{Expr}|$ times.

Why does the algorithm compute a solution?

• If not arrived at solution yet, violated constraint will cause decrease of LHS

Why does it compute the maximal solution?

• Fixed-point theory. (Comes next)
Naive Fixpoint Iteration (Correctness)

Why does the algorithm terminate?

- In each step, sets get smaller
- This can happen at most $|\text{Expr}|$ times.
Naive Fixpoint Iteration (Correctness)

Why does the algorithm terminate?
- In each step, sets get smaller
- This can happen at most $|\text{Expr}|$ times.

Why does the algorithm compute a solution?
Naive Fixpoint Iteration (Correctness)

Why does the algorithm terminate?
- In each step, sets get smaller
- This can happen at most $|\text{Expr}|$ times.

Why does the algorithm compute a solution?
- If not arrived at solution yet, violated constraint will cause decrease of LHS
Naive Fixpoint Iteration (Correctness)

Why does the algorithm terminate?
- In each step, sets get smaller
- This can happen at most $|\text{Expr}|$ times.

Why does the algorithm compute a solution?
- If not arrived at solution yet, violated constraint will cause decrease of LHS

Why does it compute the maximal solution?
- Fixed-point theory. (Comes next)
Why does the algorithm terminate?
- In each step, sets get smaller
- This can happen at most $|\text{Expr}|$ times.

Why does the algorithm compute a solution?
- If not arrived at solution yet, violated constraint will cause decrease of LHS

Why does it compute the maximal solution?
- Fixed-point theory. (Comes next)
# Table of Contents

1. **Introduction**

2. **Removing Superfluous Computations**
   - Repeated Computations
   - Background 1: Rice’s theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. **Abstract Interpretation**

4. **Alias Analysis**

5. **Avoiding Redundancy (Part II)**

6. **Interprocedural Analysis**

7. **Analysis of Parallel Programs**

8. **Replacing Expensive by Cheaper Operations**

9. **Exploiting Hardware Features**

10. **Optimization of Functional Programs**
Partial Orders

Definition (Partial Order)
A partial order \((\mathbb{D}, \sqsubseteq)\) is a relation \(\sqsubseteq\) on \(\mathbb{D}\) that is reflexive, antisymmetric, and transitive, i.e., for all \(a, b, c \in \mathbb{D}\):

- \(a \sqsubseteq a\) (reflexive)
- \(a \sqsubseteq b \land b \sqsubseteq a \implies a = b\) (antisymmetric)
- \(a \sqsubseteq b \sqsubseteq c \implies a \sqsubseteq c\) (transitive)
Partial Orders

Definition (Partial Order)
A partial order \((\mathbb{D}, \sqsubseteq)\) is a relation \(\sqsubseteq\) on \(\mathbb{D}\) that is reflexive, antisymmetric, and transitive, i.e., for all \(a, b, c \in \mathbb{D}\):

\[
\begin{align*}
    a \sqsubseteq a & \quad \text{(reflexive)} \\
    a \sqsubseteq b \land b \sqsubseteq a & \implies a = b \quad \text{(antisymmetric)} \\
    a \sqsubseteq b \sqsubseteq c & \implies a \sqsubseteq c \quad \text{(transitive)}
\end{align*}
\]

Examples \(\leq\) on \(\mathbb{N}\), \(\subseteq\). Also \(\geq\), \(\supseteq\)
Partial Orders

Definition (Partial Order)
A partial order \((\mathbb{D}, \sqsubseteq)\) is a relation \(\sqsubseteq\) on \(\mathbb{D}\) that is reflexive, antisymmetric, and transitive, i.e., for all \(a, b, c \in \mathbb{D}\):

- \(a \sqsubseteq a\) (reflexive)
- \(a \sqsubseteq b \land b \sqsubseteq a \implies a = b\) (antisymmetric)
- \(a \sqsubseteq b \sqsubseteq c \implies a \sqsubseteq c\) (transitive)

Examples \(\leq\) on \(\mathbb{N}\), \(\subseteq\). Also \(\geq\), \(\supseteq\)

Lemma (Dual order)
We define \(a \sqsupseteq b := b \sqsubseteq a\). Let \(\sqsubseteq\) be a partial order on \(\mathbb{D}\). Then \(\sqsupseteq\) also is a partial order on \(\mathbb{D}\).
More examples

\[ D = 2^{\{a,b,c\}} \text{ with } \subseteq \]

\[
\begin{array}{c}
\{a, b, c\} \\
\{a, b\} \{a, c\} \{b, c\} \\
\{a\} \{b\} \{c\} \\
\emptyset
\end{array}
\]
More examples

\[ \mathbb{Z} \text{ with relation } = \]

\[ \cdots \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad \cdots \]
More examples

\( \mathbb{Z} \) with relation \( \leq \)

\[ \ldots \]
\[ 2 \]
\[ 1 \]
\[ 0 \]
\[ -1 \]
\[ -2 \]
\[ \ldots \]
More examples

\[ \mathbb{Z}_\bot := \mathbb{Z} \cup \{ \bot \} \text{ with relation } x \sqsubseteq y \text{ iff } x = \bot \lor x = y \]
More examples

\{a, b, c, d\} with a \sqsubseteq c, a \sqsubseteq d, b \sqsubseteq c, b \sqsubseteq d
Definition (Upper bound)

$d \in \mathbb{D}$ is called upper bound of $X \subseteq \mathbb{D}$, iff

$$\forall x \in X. \ x \sqsubseteq d$$
Upper Bound

Definition (Upper bound)

$d \in D$ is called upper bound of $X \subseteq D$, iff

$$\forall x \in X. \ x \sqsubseteq d$$

Definition (Least Upper bound)

$d \in D$ is called least upper bound of $X \subseteq D$, iff

$d$ is upper bound of $X$, and
$d \sqsubseteq y$ for every upper bound $y$ of $X$
Upper Bound

Definition (Upper bound)
\( d \in D \) is called upper bound of \( X \subseteq D \), iff
\[
\forall x \in X. \, x \subseteq d
\]

Definition (Least Upper bound)
\( d \in D \) is called least upper bound of \( X \subseteq D \), iff
\[
d \text{ is upper bound of } X, \text{ and } d \subseteq y \text{ for every upper bound } y \text{ of } X
\]

Observation
Upper bound not always exists, e.g. \( \{0, 2, 4, \ldots\} \subseteq \mathbb{Z} \)
Upper Bound

Definition (Upper bound)
\( d \in \mathbb{D} \) is called upper bound of \( X \subseteq \mathbb{D} \), iff
\[
\forall x \in X. \ x \sqsubseteq d
\]

Definition (Least Upper bound)
\( d \in \mathbb{D} \) is called least upper bound of \( X \subseteq \mathbb{D} \), iff
\[
d \text{ is upper bound of } X, \ 	ext{and} \ 
\ d \sqsubseteq y \text{ for every upper bound } y \text{ of } X
\]

Observation
Upper bound not always exists, e.g. \( \{0, 2, 4, \ldots\} \subseteq \mathbb{Z} \)
Least upper bound not always exists, e.g. \( \{a, b\} \subseteq \{a, b, c, d\} \) with \( a \sqsubseteq c, a \sqsubseteq d, b \sqsubseteq c, b \sqsubseteq d \)
Complete Lattice

Definition (Complete Lattice)
A complete lattice \((\mathcal{D}, \sqsubseteq)\) is a partial order where every subset \(X \subseteq \mathcal{D}\) has a least upper bound \(\bigcup X \in \mathcal{D}\).
Complete Lattice

Definition (Complete Lattice)

A complete lattice \((\mathbb{D}, \sqsubseteq)\) is a partial order where every subset \(X \subseteq \mathbb{D}\) has a least upper bound \(\bigcup X \in \mathbb{D}\).

Note Every complete lattice has

- A least element \(\bot := \bigcup \emptyset \in \mathbb{D}\)
- A greatest element \(\top := \bigcup \mathbb{D} \in \mathbb{D}\)
Complete Lattice

**Definition (Complete Lattice)**

A *complete lattice* $(\mathbb{D}, \sqsubseteq)$ is a partial order where every subset $X \subseteq \mathbb{D}$ has a least upper bound $\bigsqcup X \in \mathbb{D}$.

**Note** Every complete lattice has

- A least element $\bot := \bigsqcup \emptyset \in \mathbb{D}$
- A greatest element $\top := \bigsqcup \mathbb{D} \in \mathbb{D}$

Moreover $a \sqcup b := \bigsqcup \{a, b\}$ and $a \sqcap b := \bigsqcap \{a, b\}$
Examples

- \((2^{\{a,b,c\}}, \subseteq)\) is complete lattice
Examples

- $(2\{a, b, c\}, \subseteq)$ is complete lattice
- $(\mathbb{Z}, =)$ is not. Nor is $(\mathbb{Z}, \leq)$
Examples

- \((2^{\{a,b,c\}}, \subseteq)\) is complete lattice
- \((\mathbb{Z}, =)\) is not. Nor is \((\mathbb{Z}, \leq)\)
- \((\mathbb{Z}_\perp, \sqsubseteq)\) is also no complete lattice
Examples

- \((2\{a,b,c\}, \subseteq)\) is complete lattice
- \((\mathbb{Z}, =)\) is not. Nor is \((\mathbb{Z}, \leq)\)
- \((\mathbb{Z}_\perp, \sqsubseteq)\) is also no complete lattice
  - But we can define flat complete lattice
Flat complete lattice over $\mathbb{Z}$

$\mathbb{Z}^\top := \mathbb{Z} \cup \{\bot, \top\}$ with relation $x \sqsubseteq y$ iff $x = \bot \lor y = \top \lor x = y$

... −2 −1 0 1 2 ...
Flat complete lattice over $\mathbb{Z}$

$\mathbb{Z}^\bot := \mathbb{Z} \cup \{\bot, \top\}$ with relation $x \sqsubseteq y$ iff $x = \bot \lor y = \top \lor x = y$

Note This construction works for every set, not only for $\mathbb{Z}$. 
Greatest Lower Bound

**Theorem**

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigcap X$. 
Greatest Lower Bound

**Theorem**

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\cap X$.

**Proof:**
Greatest Lower Bound

Theorem

Let \( D \) be a complete lattice. Then every subset \( X \subseteq D \) has a greatest lower bound \( \bigcap X \).

Proof:

- Let \( L = \{ l \in D. \ \forall x \in X. \ l \sqsubseteq x \} \)
  - The set of all lower bounds of \( X \)
Greatest Lower Bound

Theorem

Let $D$ be a complete lattice. Then every subset $X \subseteq D$ has a greatest lower bound $\bigwedge X$.

Proof:

- Let $L = \{ l \in D. \; \forall x \in X. \; l \sqsubseteq x \}$
  - The set of all lower bounds of $X$
- Construct $\bigwedge X := \bigvee L$
  - Obvious: $\bigwedge L$ is $\sqsubseteq$ than all lower bounds
Greatest Lower Bound

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigcap X$.

Proof:

- Let $L = \{l \in \mathbb{D}. \forall x \in X. l \subseteq x\}$
  - The set of all lower bounds of $X$
- Construct $\bigcap X := \bigcup L$
  - Show: $\bigcup L$ is lower bound
Theorem

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigcap X$.

Proof:

- Let $L = \{ l \in \mathbb{D}. \ \forall x \in X. \ l \subseteq x \}$
  - The set of all lower bounds of $X$
- Construct $\bigcap X := \bigsqcup L$
  - Show: $\bigsqcup L$ is lower bound
    - Assume $x \in X$. 

Greatest Lower Bound

**Theorem**

Let $\mathcal{D}$ be a complete lattice. Then every subset $X \subseteq \mathcal{D}$ has a greatest lower bound $\bigwedge X$.

**Proof:**

- Let $L = \{l \in \mathcal{D}. \forall x \in X. l \sqsubseteq x\}$
  - The set of all lower bounds of $X$
- Construct $\bigwedge X := \bigcup L$
  - Show: $\bigcup L$ is lower bound
    - Assume $x \in X$.
    - Then $\forall l \in L. l \sqsubseteq x$ (i.e., $x$ is upper bound of $L$)
**Greatest Lower Bound**

**Theorem**

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigmeet X$.

**Proof:**

- Let $L = \{l \in \mathbb{D}. \forall x \in X. l \sqsubseteq x\}$
  - The set of all lower bounds of $X$
- Construct $\bigmeet X := \bigsqcup L$
  - Show: $\bigsqcup L$ is lower bound
    - Assume $x \in X$.
    - Then $\forall l \in L. l \sqsubseteq x$ (i.e., $x$ is upper bound of $L$)
    - Thus $\bigsqcup L \sqsubseteq x$ (b/c $\bigsqcup L$ is least upper bound)
Greatest Lower Bound

Theorem

Let $\mathbb{D}$ be a complete lattice. Then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\cap X$.

Proof:

- Let $L = \{ l \in \mathbb{D}. \forall x \in X. l \sqsubseteq x \}$
  - The set of all lower bounds of $X$
- Construct $\cap X := \bigcup L$
  - Show: $\bigcup L$ is lower bound
    - Assume $x \in X$.
    - Then $\forall l \in L. l \sqsubseteq x$ (i.e., $x$ is upper bound of $L$)
    - Thus $\bigcup L \sqsubseteq x$ (b/c $\bigcup L$ is least upper bound)
  - Obvious: $\bigcup L$ is $\sqsubseteq$ than all lower bounds
Examples

- In \((2^{\{a,b,c\}}, \subseteq)\)
  - Note, in lattices with \(\subseteq\)-ordering, we occasionally write \(\cup\), \(\cap\) instead of \(\bigcup\), \(\bigcap\)
  - \(\bigcup\{\{a, b\}, \{a, c\}\} = \{a, b, c\}\), \(\bigcap\{\{a, b\}, \{a, c\}\} = \{a\}\)
Examples

- In $(2^{\{a,b,c\}}, \subseteq)$
  - Note, in lattices with $\subseteq$-ordering, we occasionally write $\bigcup$, $\bigcap$ instead of $\bigvee$, $\bigwedge$
  - $\bigcup\{\{a, b\}, \{a, c\}\} = \{a, b, c\}$, $\bigcap\{\{a, b\}, \{a, c\}\} = \{a\}$

- In $\mathbb{Z}^+_{-\infty}$:
  - $\bigcup\{1, 2, 3, 4\} = 4$, $\bigcap\{1, 2, 3, 4\} = 1$
  - $\bigcup\{1, 2, 3, 4, \ldots\} = +\infty$, $\bigcap\{1, 2, 3, 4, \ldots\} = 1$
• Syntactic criterion for available expressions
• Constraint system to express it
  • Yet to come: Link between CS and path-based criterion
• Naive fixpoint iteration to compute maximum solution of CS
• Partial orders, complete lattices
Monotonic function

Definition
Let \((\mathbb{D}_1, \sqsubseteq_1)\) and \((\mathbb{D}_2, \sqsubseteq_2)\) be partial orders. A function \(f : \mathbb{D}_1 \rightarrow \mathbb{D}_2\) is called monotonic, iff

\[
\forall x, y \in \mathbb{D}_1. \ x \sqsubseteq_1 y \implies f(x) \sqsubseteq_2 f(y)
\]
Examples

• \( f :: \mathbb{N} \rightarrow \mathbb{Z} \) with \( f(x) := x - 10 \)
Examples

- \( f :: \mathbb{N} \rightarrow \mathbb{Z} \) with \( f(x) := x - 10 \)
- \( f :: \mathbb{N} \rightarrow \mathbb{N} \) with \( f(x) := x + 10 \)
- Functions involving negation/complement usually not monotonic.
Examples

• \( f : \mathbb{N} \rightarrow \mathbb{Z} \) with \( f(x) := x - 10 \)
• \( f : \mathbb{N} \rightarrow \mathbb{N} \) with \( f(x) := x + 10 \)
• \( f : 2\{a, b, c\} \rightarrow 2\{a, b, c\} \) with \( f(X) := (X \cup \{a, b\}) \setminus \{b, c\} \)
Examples

- $f :: \mathbb{N} \to \mathbb{Z}$ with $f(x) := x - 10$
- $f :: \mathbb{N} \to \mathbb{N}$ with $f(x) := x + 10$
- $f :: 2\{a, b, c\} \to 2\{a, b, c\}$ with $f(X) := (X \cup \{a, b\}) \setminus \{b, c\}$
  - In general, functions of this form are monotonic wrt. $\subseteq$.
Examples

• $f :: \mathbb{N} \rightarrow \mathbb{Z}$ with $f(x) := x - 10$

• $f :: \mathbb{N} \rightarrow \mathbb{N}$ with $f(x) := x + 10$

• $f :: 2^{\{a,b,c\}} \rightarrow 2^{\{a,b,c\}}$ with $f(X) := (X \cup \{a, b\}) \setminus \{b, c\}$
  • In general, functions of this form are monotonic wrt. $\subseteq$.

• $f :: \mathbb{Z} \rightarrow \mathbb{Z}$ with $f(x) := -x$ (Not monotonic)
Examples

- \( f : \mathbb{N} \rightarrow \mathbb{Z} \) with \( f(x) := x - 10 \)
- \( f : \mathbb{N} \rightarrow \mathbb{N} \) with \( f(x) := x + 10 \)
- \( f : 2^{\{a,b,c\}} \rightarrow 2^{\{a,b,c\}} \) with \( f(X) := (X \cup \{a, b\}) \setminus \{b, c\} \)
  - In general, functions of this form are monotonic w.r.t. \( \subseteq \).
- \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) with \( f(x) := -x \) (Not monotonic)
- \( f : 2^{\{a,b,c\}} \rightarrow 2^{\{a,b,c\}} \) with \( f(X) := \{x \mid x \notin X\} \) (Not monotonic)
Examples

- $f : \mathbb{N} \rightarrow \mathbb{Z}$ with $f(x) := x - 10$
- $f : \mathbb{N} \rightarrow \mathbb{N}$ with $f(x) := x + 10$
- $f : 2\{a, b, c\} \rightarrow 2\{a, b, c\}$ with $f(X) := (X \cup \{a, b\}) \setminus \{b, c\}$
  - In general, functions of this form are monotonic wrt. $\subseteq$.
- $f : \mathbb{Z} \rightarrow \mathbb{Z}$ with $f(x) := -x$ (Not monotonic)
- $f : 2\{a, b, c\} \rightarrow 2\{a, b, c\}$ with $f(X) := \{x \mid x \notin X\}$ (Not monotonic)
  - Functions involving negation/complement usually not monotonic.
Least fixed point

Definition

Let $f: \mathbb{D} \to \mathbb{D}$ be a function. A value $d \in \mathbb{D}$ with $f(d) = d$ is called fixed point of $f$.

If $\mathbb{D}$ is a partial ordering, a fixed point $d_0 \in D$ with

$$\forall d. f(d) = d \implies d_0 \sqsubseteq d$$

is called least fixed point. If such a $d_0$ exists, it is uniquely determined, and we define

$$\text{lfp}(f) := d_0$$
Examples

- \( f : \mathbb{N} \rightarrow \mathbb{N} \) with \( f(x) = x + 1 \) No fixed points
Examples

- $f :: \mathbb{N} \to \mathbb{N}$ with $f(x) = x + 1$ No fixed points
- $f :: \mathbb{N} \to \mathbb{N}$ with $f(x) = x$. Every $x \in \mathbb{N}$ is fixed point.
Examples

• $f : \mathbb{N} \rightarrow \mathbb{N}$ with $f(x) = x + 1$. No fixed points.
• $f : \mathbb{N} \rightarrow \mathbb{N}$ with $f(x) = x$. Every $x \in \mathbb{N}$ is a fixed point.
• $f : 2^{\{a,b,c\}} \rightarrow 2^{\{a,b,c\}}$ with $f(X) = X \cup \{a, b\}$. $\text{lfp}(f) = \{a, b\}$. 


Function composition

**Theorem**

If $f_1 : \mathbb{D}_1 \rightarrow \mathbb{D}_2$ and $f_2 : \mathbb{D}_2 \rightarrow \mathbb{D}_3$ are monotonic, then also $f_2 \circ f_1$ is monotonic.
Function composition

**Theorem**

If \( f_1 : D_1 \to D_2 \) and \( f_2 : D_2 \to D_3 \) are monotonic, then also \( f_2 \circ f_1 \) is monotonic.

**Proof:** \( a \sqsubseteq b \implies f_1(a) \sqsubseteq f_1(b) \implies f_2(f_1(a)) \sqsubseteq f_2(f_1(b)). \)
Function lattice

Definition
Let \((\mathbb{D}, \sqsubseteq)\) be a partial ordering. We overload \(\sqsubseteq\) to functions from \(A\) to \(\mathbb{D}\):

\[ f \sqsubseteq g \text{ iff } \forall x. \, f(x) \sqsubseteq g(x) \]

\([A \to \mathbb{D}]\) is the set of functions from \(A\) to \(\mathbb{D}\).
Function lattice

**Definition**
Let $(\mathbb{D}, \sqsubseteq)$ be a partial ordering. We overload $\sqsubseteq$ to functions from $A$ to $\mathbb{D}$:

$$f \sqsubseteq g \text{ iff } \forall x. f(x) \sqsubseteq g(x)$$

$[A \to \mathbb{D}]$ is the set of functions from $A$ to $\mathbb{D}$.

**Theorem**
If $(\mathbb{D}, \sqsubseteq)$ is a partial ordering/complete lattice, then also $([A \to \mathbb{D}], \sqsubseteq)$. In particular, we have:

$$(\bigsqcup F)(x) = \bigsqcup \{f(x) \mid f \in F\}$$
Function lattice

Definition
Let \((\mathbb{D}, \sqsubseteq)\) be a partial ordering. We overload \(\sqsubseteq\) to functions from \(A\) to \(\mathbb{D}\):

\[ f \sqsubseteq g \text{ iff } \forall x. f(x) \sqsubseteq g(x) \]

\([A \rightarrow \mathbb{D}]\) is the set of functions from \(A\) to \(\mathbb{D}\).

Theorem
If \((\mathbb{D}, \sqsubseteq)\) is a partial ordering/complete lattice, then also \(([A \rightarrow \mathbb{D}], \sqsubseteq)\).
In particular, we have:

\[ (\bigsqcup F)(x) = \bigsqcup \{f(x) \mid f \in F\} \]

Proof: On whiteboard.
Component-wise ordering on tuples

- Tuples \( \vec{x} \in \mathbb{D}^n \) can be seen as functions \( \vec{x} : \{1, \ldots, n\} \rightarrow \mathbb{D} \)
Component-wise ordering on tuples

- Tuples $\vec{x} \in \mathbb{D}^n$ can be seen as functions $\vec{x} : \{1, \ldots, n\} \to \mathbb{D}$
- Yields component-wise ordering:
  
  $\vec{x} \sqsubseteq \vec{y}$ iff $\forall i : \{1, \ldots, n\}. \ x_i \sqsubseteq y_i$
Component-wise ordering on tuples

- Tuples $\vec{x} \in \mathbb{D}^n$ can be seen as functions $\vec{x} : \{1, \ldots, n\} \to \mathbb{D}$
- Yields component-wise ordering:

  $\vec{x} \sqsubseteq \vec{y}$ iff $\forall i : \{1, \ldots, n\}. x_i \sqsubseteq y_i$

- $(\mathbb{D}^n, \sqsubseteq)$ is complete lattice if $(\mathbb{D}, \sqsubseteq)$ is complete lattice.
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form

\[ x_i \sqsupseteq f_i(x_1, \ldots, x_n) \]

where

| \( x_i \) | variables | e.g., \( A[u] \), for \( u \in V \) |
| \((\mathbb{D}, \sqsubseteq)\) | complete lattice | e.g., \( (2^{\text{Expr}}, \sqsubseteq) \) |
| \( f_i : \mathbb{D}^n \rightarrow \mathbb{D} \) | RHS | e.g., \( (A[u] \cup \{e\}) \setminus \text{Expr}_R \) |
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form

\[ x_i \sqsupseteq f_i(x_1, \ldots, x_n) \]

where

<table>
<thead>
<tr>
<th>( x_i )</th>
<th>variables</th>
<th>e.g., ( A[u] ), for ( u \in V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(( \mathbb{D}, \sqsubseteq ) )</td>
<td>complete lattice</td>
<td>e.g., ( (2^{\text{Expr}}, \sqsupseteq) )</td>
</tr>
<tr>
<td>( f_i : \mathbb{D}^n \rightarrow \mathbb{D} )</td>
<td>RHS</td>
<td>e.g., ( (A[u] \cup {e}) \setminus \text{Expr}_R )</td>
</tr>
</tbody>
</table>

- Observation: One constraint per \( x_i \) is enough.
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form

\[ x_i \sqsubseteq f_i(x_1, \ldots, x_n) \]

where

<table>
<thead>
<tr>
<th>( x_i ) (( \mathbb{D}, \sqsubseteq ))</th>
<th>Variables ( \text{complete lattice} )</th>
<th>RHS</th>
<th>e.g., ( A[u] ), for ( u \in V )</th>
<th>e.g., ( (2^{\text{Expr}}, \supseteq) )</th>
<th>e.g., ( (A[u] \cup {e}) \setminus \text{Expr}_R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_i: \mathbb{D}^n \rightarrow \mathbb{D} )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Observation: One constraint per \( x_i \) is enough.
  - Assume we have \( x_i \sqsubseteq rhs_1(x_1, \ldots, x_n), \ldots, x_i \sqsubseteq rhs_m(x_1, \ldots, x_n) \)
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form

\[ x_i \sqsupseteq f_i(x_1, \ldots, x_n) \]

where

<table>
<thead>
<tr>
<th>( x_i )</th>
<th>variables</th>
<th>e.g., ( A[u] ), for ( u \in V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (\mathbb{D}, \sqsubseteq) )</td>
<td>complete lattice</td>
<td>e.g., ( (2^{\text{Expr}}, \supseteq) )</td>
</tr>
<tr>
<td>( f_i : \mathbb{D}^n \rightarrow \mathbb{D} )</td>
<td>RHS</td>
<td>e.g., ( (A[u] \cup {e}) \setminus \text{Expr}_R )</td>
</tr>
</tbody>
</table>

- Observation: One constraint per \( x_i \) is enough.
  - Assume we have \( x_i \sqsupseteq rhs_1(x_1, \ldots, x_n), \ldots, x_i \sqsupseteq rhs_m(x_1, \ldots, x_n) \)
  - Replace by \( x_i \sqsupseteq (\bigcup\{rhs_j | 1 \leq j \leq m\})(x_1, \ldots, x_n) \)
Application

• Idea: Encode constraint system as function. Solutions as fixed points.
• Constraints have the form

\[ x_i \sqsubseteq f_i(x_1, \ldots, x_n) \]

where

<table>
<thead>
<tr>
<th>( x_i )</th>
<th>variables</th>
<th>e.g., ( A[u] ), for ( u \in V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\mathbb{D}, \sqsubseteq))</td>
<td>complete lattice</td>
<td>e.g., ((2^{\text{Expr}}, \supseteq))</td>
</tr>
<tr>
<td>( f_i : \mathbb{D}^n \to \mathbb{D} )</td>
<td>RHS</td>
<td>e.g., ((A[u] \cup {e}) \setminus \text{Expr}_R)</td>
</tr>
</tbody>
</table>

• Observation: One constraint per \( x_i \) is enough.
  • Assume we have \( x_i \sqsubseteq rhs_1(x_1, \ldots, x_n), \ldots, x_i \sqsubseteq rhs_m(x_1, \ldots, x_n) \)
  • Replace by \( x_i \sqsubseteq (\bigcup \{rhs_j \mid 1 \leq j \leq m\})(x_1, \ldots, x_n) \)
    • Does not change solutions.
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form
  \[ x_i \sqsupseteq f_i(x_1, \ldots, x_n) \]

where

| \( x_i \) | variables | e.g., \( A[u] \), for \( u \in V \) |
| \( (\mathbb{D}, \sqsubseteq) \) | complete lattice | e.g., \( (2^{\text{Expr}}, \supseteq) \) |
| \( f_i : \mathbb{D}^n \to \mathbb{D} \) | RHS | e.g., \( (A[u] \cup \{e\}) \setminus \text{Expr}_R \) |

- Observation: One constraint per \( x_i \) is enough.
  - Assume we have \( x_i \sqsupseteq \text{rhs}_1(x_1, \ldots, x_n), \ldots, x_i \sqsupseteq \text{rhs}_m(x_1, \ldots, x_n) \)
  - Replace by \( x_i \sqsupseteq (\bigcup \{\text{rhs}_j \mid 1 \leq j \leq m\})(x_1, \ldots, x_n) \)
    - Does not change solutions.

- Define \( F : \mathbb{D}^n \to \mathbb{D}^n \), with
  \[ F(x_1, \ldots, x_n) := (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \]

Then, constraints expressed by \( \vec{x} \sqsupseteq F(\vec{x}) \).
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form
  \[ x_i \sqsupseteq f_i(x_1, \ldots, x_n) \]
  where

<table>
<thead>
<tr>
<th>( x_i )</th>
<th>variables</th>
<th>e.g., ( A[u] ), for ( u \in V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (\mathbb{D}, \sqsubseteq) )</td>
<td>complete lattice</td>
<td>e.g., ( (2^{\text{Expr}}, \supseteq) )</td>
</tr>
<tr>
<td>( f_i : \mathbb{D}^n \to \mathbb{D} )</td>
<td>RHS</td>
<td>e.g., ( (A[u] \cup {e}) \setminus \text{Expr}_R )</td>
</tr>
</tbody>
</table>

- Observation: One constraint per \( x_i \) is enough.
  - Assume we have \( x_i \sqsupseteq \text{rhs}_1(x_1, \ldots, x_n), \ldots, x_i \sqsupseteq \text{rhs}_m(x_1, \ldots, x_n) \)
  - Replace by \( x_i \sqsupseteq (\bigcup \{\text{rhs}_j \mid 1 \leq j \leq m\})(x_1, \ldots, x_n) \)
    - Does not change solutions.
- Define \( F : \mathbb{D}^n \to \mathbb{D}^n \), with
  \[ F(x_1, \ldots, x_n) := (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \]
  Then, constraints expressed by \( \vec{x} \sqsupseteq F(\vec{x}) \).
  - Fixed-Points of \( F \) are solutions
Application

- Idea: Encode constraint system as function. Solutions as fixed points.
- Constraints have the form

\[ x_i \sqsubseteq f_i(x_1, \ldots, x_n) \]

where

<table>
<thead>
<tr>
<th>( x_i )</th>
<th>( (\mathbb{D}, \sqsubseteq) )</th>
<th>variables ( \mathbb{D}^n \rightarrow \mathbb{D} )</th>
<th>complete lattice</th>
<th>e.g., ( A[u], ) for ( u \in V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_i )</td>
<td>( \mathbb{D}^n \rightarrow \mathbb{D} )</td>
<td>RHS</td>
<td>e.g., ( (2^{\text{Expr}}, \supseteq) )</td>
<td>e.g., ( (A[u] \cup { e }) \setminus \text{Expr}_R )</td>
</tr>
</tbody>
</table>

- Observation: One constraint per \( x_i \) is enough.
  - Assume we have \( x_i \sqsubseteq rhs_1(x_1, \ldots, x_n), \ldots, x_i \sqsubseteq rhs_m(x_1, \ldots, x_n) \)
  - Replace by \( x_i \sqsubseteq (\bigsqcup \{ rhs_j \mid 1 \leq j \leq m \})(x_1, \ldots, x_n) \)
    - Does not change solutions.

- Define \( F : \mathbb{D}^n \rightarrow \mathbb{D}^n \), with

\[
F(x_1, \ldots, x_n) := (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))
\]

Then, constraints expressed by \( \vec{x} \sqsubseteq F(\vec{x}) \).
- Fixed-Points of \( F \) are solutions
- Least solution = least fixed point (next!)
• Moreover, $F$ is monotonic if the $f_i$ are.
• Question: Does $\text{lfp}(F)$ exist? Does fp-iteration compute it?
Knaster-Tarski fixed-point Theorem

Let \((D, \subseteq)\) be a complete lattice, and \(f : D \to D\) be a monotonic function. Then, \(f\) has a least and a greatest fixed point given by

\[
\text{lfp}(f) = \bigcap \{ x \mid f(x) \subseteq x \} \quad \text{gfp}(f) = \bigcup \{ x \mid x \subseteq f(x) \}
\]
Knaster-Tarski fixed-point Theorem

Knaster-Tarski

Let \((\mathbb{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathbb{D} \to \mathbb{D}\) be a monotonic function. Then, \(f\) has a least and a greatest fixed point given by

\[
lfp(f) = \bigcap\{x \mid f(x) \sqsubseteq x\} \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad gfp(f) = \bigcup\{x \mid x \sqsubseteq f(x)\}
\]

Proof  Let \(P = \{x \mid f(x) \sqsubseteq x\}\). (\(P\) is set of pre-fixpoints)
Knaster-Tarski fixed-point Theorem

Let \((\mathbb{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathbb{D} \rightarrow \mathbb{D}\) be a monotonic function. Then, \(f\) has a least and a greatest fixed point given by

\[
\text{lfp}(f) = \bigcap \{x \mid f(x) \sqsubseteq x\} \quad \text{gfp}(f) = \bigcup \{x \mid x \sqsubseteq f(x)\}
\]

Proof Let \(P = \{x \mid f(x) \sqsubseteq x\}\). (\(P\) is set of pre-fixpoints)

- Show (1): \(f(\bigcap P) \sqsubseteq \bigcap P\).
  - Have \(\forall x \in P. \ f(\bigcap P) \sqsubseteq f(x) \sqsubseteq x\) (lower bound, mono, def.\(P\))
  - I.e., \(f(\bigcap P)\) is lower bound of \(P\)
  - Thus \(f(\bigcap P) \sqsubseteq \bigcap P\) (greatest lower bound).
Knaster-Tarski fixed-point Theorem

Let \((\mathcal{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathcal{D} \to \mathcal{D}\) be a monotonic function. Then, \(f\) has a least and a greatest fixed point given by

\[
\text{lfp}(f) = \bigcap\{x \mid f(x) \sqsubseteq x\} \quad \text{and} \quad \text{gfp}(f) = \bigcup\{x \mid x \sqsubseteq f(x)\}
\]

Proof Let \(P = \{x \mid f(x) \sqsubseteq x\}\). \((P\) is set of pre-fixpoints)

- Show (1): \(f(\bigcap P) \sqsubseteq \bigcap P\).
  - Have \(\forall x \in P. \ f(\bigcap P) \sqsubseteq f(x) \sqsubseteq x\) (lower bound, mono, def.P)
  - I.e., \(f(\bigcap P)\) is lower bound of \(P\)
  - Thus \(f(\bigcap P) \sqsubseteq \bigcap P\) (greatest lower bound).

- Show (2): \(\bigcap P \sqsubseteq f(\bigcap P)\)
  - From (1) have \(f(f(\bigcap P)) \sqsubseteq f(\bigcap P)\) (mono)
  - Hence \(f(\bigcap P) \in P\) (def.P)
  - Thus \(\bigcap P \sqsubseteq f(\bigcap P)\) (lower bound).
Knaster-Tarski fixed-point Theorem

Let $(\mathbb{D}, \sqsubseteq)$ be a complete lattice, and $f : \mathbb{D} \to \mathbb{D}$ be a monotonic function. Then, $f$ has a least and a greatest fixed point given by

$$\text{lfp}(f) = \bigcap \{x \mid f(x) \sqsubseteq x\}$$
$$\text{gfp}(f) = \bigcup \{x \mid x \sqsubseteq f(x)\}$$

**Proof**

Let $P = \{x \mid f(x) \sqsubseteq x\}$. ($P$ is set of pre-fixpoints)

- Show (1): $f(\bigcap P) \sqsubseteq \bigcap P$.
  - Have $\forall x \in P. f(\bigcap P) \sqsubseteq f(x) \sqsubseteq x$ (lower bound, mono, def.P)
  - I.e., $f(\bigcap P)$ is lower bound of $P$
  - Thus $f(\bigcap P) \sqsubseteq \bigcap P$ (greatest lower bound).

- Show (2): $\bigcap P \sqsubseteq f(\bigcap P)$
  - From (1) have $f(f(\bigcap P)) \sqsubseteq f(\bigcap P)$ (mono)
  - Hence $f(\bigcap P) \in P$ (def.P)
  - Thus $\bigcap P \sqsubseteq f(\bigcap P)$ (lower bound).

- Show (3): Least fixed point
  - Assume $d = f(d)$ is another fixed point
  - Hence $f(d) \sqsubseteq d$ (reflexive)
  - Hence $d \in P$ (def.P)
  - Thus $\bigcap P \sqsubseteq d$ (lower bound)
Knaster-Tarski fixed-point Theorem

Let \((\mathbb{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathbb{D} \to \mathbb{D}\) be a monotonic function. Then, \(f\) has a least and a greatest fixed point given by

\[
\text{lfp}(f) = \bigcap \{x \mid f(x) \sqsubseteq x\} \quad \text{gfp}(f) = \bigcup \{x \mid x \sqsubseteq f(x)\}
\]

Proof

Let \(P = \{x \mid f(x) \sqsubseteq x\}\). \((P\) is set of pre-fixpoints\)

- Show (1): \(f(\bigcap P) \sqsubseteq \bigcap P\).
  - Have \(\forall x \in P.\ f(\bigcap P) \sqsubseteq f(x) \sqsubseteq x\) (lower bound, mono, def.P)
  - I.e., \(f(\bigcap P)\) is lower bound of \(P\)
  - Thus \(f(\bigcap P) \sqsubseteq \bigcap P\) (greatest lower bound).

- Show (2): \(\bigcap P \sqsubseteq f(\bigcap P)\).
  - From (1) have \(f(f(\bigcap P)) \sqsubseteq f(\bigcap P)\) (mono)
  - Hence \(f(\bigcap P) \in P\) (def.P)
  - Thus \(\bigcap P \subseteq f(\bigcap P)\) (lower bound).

- Show (3): Least fixed point
  - Assume \(d = f(d)\) is another fixed point
  - Hence \(f(d) \sqsubseteq d\) (reflexive)
  - Hence \(d \in P\) (def.P)
  - Thus \(\bigcap P \subseteq d\) (lower bound)

- Greatest fixed point: Dually.
Used Facts

lower bound \( x \in X \implies \bigcap X \subseteq x \)
greatest lower bound \((\forall x \in X. \ d \subseteq X) \implies d \subseteq \bigcap X\)

mono \( f \) monotonic: \( x \subseteq y \implies f(x) \subseteq f(y) \)
reflexive \( x \subseteq x \)
Knaster-Tarski Fixed-Point Theorem (Intuition)

$f(x) \sqsubseteq x$

gfp

$x = f(x)$

lfp

$x \sqsubseteq f(x)$

pre-fixpoints

post-fixpoints
Least solution = lfp

Recall: Constraints where $\vec{x} \sqsupseteq F(\vec{x})$

Knaster-Tarski: $\text{lfp}(F) = \bigcap\{\vec{x} \mid \vec{x} \sqsupseteq F(\vec{x})\}$

- I.e.: Least fixed point is lower bound of solutions
Kleene fixed-point theorem

Let \((\mathbb{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathbb{D} \rightarrow \mathbb{D}\) be a monotonic function. Then:

\[
\bigsqcup \{f^i(\bot) \mid i \in \mathbb{N}\} \sqsubseteq \text{lfp}(f)
\]

If \(f\) is distributive, we even have:

\[
\bigsqcup \{f^i(\bot) \mid i \in \mathbb{N}\} = \text{lfp}(f)
\]
Kleene fixed-point theorem

Let \((\mathbb{D}, \sqsubseteq)\) be a complete lattice, and \(f : \mathbb{D} \rightarrow \mathbb{D}\) be a monotonic function. Then:

$$\bigsqcup \{f^i(\bot) \mid i \in \mathbb{N}\} \subseteq \text{lfp}(f)$$

If \(f\) is distributive, we even have:

$$\bigsqcup \{f^i(\bot) \mid i \in \mathbb{N}\} = \text{lfp}(f)$$

Definition

Distributivity A function \(f : \mathbb{D}_1 \rightarrow \mathbb{D}_2\) over complete lattices \((\mathbb{D}_1, \sqsubseteq_1)\) and \((\mathbb{D}_2, \sqsubseteq_2)\) is called distributive, iff

$$X \neq \emptyset \implies f(\bigsqcup_1 X) = \bigsqcup_2 \{f(x) \mid x \in X\}$$

Note: Distributivity implies monotonicity.
By Knaster-Tarski theorem, $\text{lfp}(f)$ exists.
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, \( \text{lfp}(f) \) exists.
Show that for all \( i \): \( f^{i}(\bot) \subseteq \text{lfp}(f) \)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, $\text{lfp}(f)$ exists.

Show that for all $i$: $f^i(\bot) \subseteq \text{lfp}(f)$

- Induction on $i$. 

Thus, $\bigsqcup \{f^i(\bot) | i \in \mathbb{N}\} \subseteq \text{lfp}(f)$ (least upper bound)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, lfp(f) exists.

Show that for all \( i \): \( f^i(\bot) \sqsubseteq \text{lfp}(f) \)

- Induction on \( i \).
  - \( i = 0 \): \( f^0(\bot) = \bot \sqsubseteq \text{lfp}(f) \) (def. \( f^0 \), bot least)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, \( \text{lfp}(f) \) exists.

Show that for all \( i \): \( f^i(\perp) \sqsubseteq \text{lfp}(f) \)

- Induction on \( i \).
  - \( i = 0 \): \( f^0(\perp) = \perp \sqsubseteq \text{lfp}(f) \) (def. \( f^0 \), bot least)
  - \( i + 1 \): IH: \( f^i(\perp) \sqsubseteq \text{lfp}(f) \). To show: \( f^{i+1}(\perp) \sqsubseteq \text{lfp}(f) \)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, $\text{lfp}(f)$ exists.

Show that for all $i$: $f^i(\bot) \subseteq \text{lfp}(f)$

• Induction on $i$.
  • $i = 0$: $f^0(\bot) = \bot \subseteq \text{lfp}(f)$ (def.$f^0$, bot least)
  • $i + 1$: IH: $f^i(\bot) \subseteq \text{lfp}(f)$. To show: $f^{i+1}(\bot) \subseteq \text{lfp}(f)$
  • Have $f^{i+1}(\bot) = f(f^i(\bot))$ (def.$f^{i+1}$)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, lfp(f) exists.

Show that for all \( i \): \( f^i(\bot) \sqsubseteq \text{lfp}(f) \)

- Induction on \( i \).
  - \( i = 0 \): \( f^0(\bot) = \bot \sqsubseteq \text{lfp}(f) \) (def.\( f^0 \), bot least)
  - \( i + 1 \): IH: \( f^i(\bot) \sqsubseteq \text{lfp}(f) \). To show: \( f^{i+1}(\bot) \sqsubseteq \text{lfp}(f) \)
  - Have \( f^{i+1}(\bot) = f(f^i(\bot)) \) (def.\( f^{i+1} \))
  - \( \sqsubseteq f(\text{lfp}(f)) \) (IH, mono)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, $\text{lfp}(f)$ exists.

Show that for all $i$: $f^i(\bot) \sqsubseteq \text{lfp}(f)$

- Induction on $i$.
  - $i = 0$: $f^0(\bot) = \bot \sqsubseteq \text{lfp}(f)$ (def.$f^0$, bot least)
  - $i + 1$: IH: $f^i(\bot) \sqsubseteq \text{lfp}(f)$. To show: $f^{i+1}(\bot) \sqsubseteq \text{lfp}(f)$
  - Have $f^{i+1}(\bot) = f(f^i(\bot))$ (def.$f^{i+1}$)
  - $\sqsubseteq f(\text{lfp}(f))$ (IH, mono)
  - $= \text{lfp}(f)$ ($\text{lfp}(f)$ is fixed point)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, \( lfp(f) \) exists.

Show that for all \( i: f^i(\bot) \sqsubseteq lfp(f) \)

- Induction on \( i \).
  - \( i = 0: f^0(\bot) = \bot \sqsubseteq lfp(f) \) (def. \( f^0 \), bot least)
  - \( i + 1: \text{IH: } f^i(\bot) \sqsubseteq lfp(f) \). To show: \( f^{i+1}(\bot) \sqsubseteq lfp(f) \)
  - Have \( f^{i+1}(\bot) = f(f^i(\bot)) \) (def. \( f^{i+1} \))
  - \( \sqsubseteq f(lfp(f)) \) (IH, mono)
  - \( = lfp(f) \) (lfp(f) is fixed point)

I.e., \( lfp(f) \) is upper bound of \( \{f^i(\bot) \mid i \in \mathbb{N}\} \)
Kleene fixed-point theorem: Proof

By Knaster-Tarski theorem, \(\text{lfp}(f)\) exists.

Show that for all \(i\): \(f^i(\bot) \subseteq \text{lfp}(f)\)

- Induction on \(i\).
  - \(i = 0\): \(f^0(\bot) = \bot \subseteq \text{lfp}(f)\) (def. \(f^0\), bot least)
  - \(i + 1\): IH: \(f^i(\bot) \subseteq \text{lfp}(f)\). To show: \(f^{i+1}(\bot) \subseteq \text{lfp}(f)\)
  - Have \(f^{i+1}(\bot) = f(f^i(\bot))\) (def. \(f^{i+1}\))
  - \(\subseteq f(\text{lfp}(f))\) (IH, mono)
  - \(= \text{lfp}(f)\) (lfp(f) is fixed point)

I.e., \(\text{lfp}(f)\) is upper bound of \(\{f^i(\bot) \mid i \in \mathbb{N}\}\)

Thus, \(\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\} \subseteq \text{lfp}(f)\) (least upper bound) \qed
Assume $f$ is distributive.
Assume $f$ is distributive.

Hence $f(\bigsqcup\{f^i(\perp) \mid i \in \mathbb{N}\}) = \bigsqcup\{f^{i+1}(\perp) \mid i \in \mathbb{N}\}$ (def.distributive)
Kleene fixed-point theorem: Proof (ctd)

Assume $f$ is distributive.

Hence $f(\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}) = \bigsqcup\{f^{i+1}(\bot) \mid i \in \mathbb{N}\}$ (def.distributive)

$= \bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$ ($\bigsqcup(X \cup \{\bot\}) = \bigsqcup X$)
Assume $f$ is distributive.

Hence $f(\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}) = \bigsqcup\{f^{i+1}(\bot) \mid i \in \mathbb{N}\} \text{ (def. distributive)}$

$= \bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\} \text{ (def. distributive)}$

I.e., $\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$ is fixed point
Assume $f$ is distributive.

Hence $f(\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}) = \bigsqcup\{f^{i+1}(\bot) \mid i \in \mathbb{N}\}$ (def. distributive)

$= \bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$ ($\bigsqcup(X \cup \{\bot\}) = \bigsqcup X$)

I.e., $\bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$ is fixed point

Hence $\text{lfp}(f) \subseteq \bigsqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$ ($\text{lfp}$ is least fixed point)
Assume $f$ is distributive.

Hence $f(\bigsqcup\{f^i(⊥) \mid i ∈ N\}) = \bigsqcup\{f^{i+1}(⊥) \mid i ∈ N\}$ (def. distributive)

$= \bigsqcup\{f^i(⊥) \mid i ∈ N\}$ ($\bigsqcup(X \cup \{⊥\}) = \bigsqcup X$)

I.e., $\bigsqcup\{f^i(⊥) \mid i ∈ N\}$ is fixed point

Hence $\text{lfp}(f) ⊆ \bigsqcup\{f^i(⊥) \mid i ∈ N\}$ ($\text{lfp}$ is least fixed point)

With distributive implies mono, antisymmetry and first part, we get:

$$\text{lfp}(f) = \bigsqcup\{f^i(⊥) \mid i ∈ N\}$$

$\square$
Used Facts

- bot least: $\forall x. \bot \sqsubseteq x$
- fixed point: $d$ is fixed point iff $f(d) = d$
- least fixed point: $f(d) = d \implies \text{lfp}(f) \sqsubseteq d$
- least upper bound: $(\forall x \in X. x \sqsubseteq d) \implies \bigcup X \sqsubseteq d$
Summary

- Does $\text{lfp}(F)$ exist?
  - Yes (Knaster-Tarski)
Summary

- Does \( \text{lfp}(F) \) exist?
  - Yes (Knaster-Tarski)
- Does fp-iteration compute it?
  - Fp-iteration computes the \( F^i(\bot) \) for increasing \( i \)
    - By Kleene FP-Theorem, these are below \( \text{lfp}(F) \)
    - It terminates only if a fixed-point has been reached
      - This fixed point is also below \( \text{lfp}(F) \) (and thus = \( \text{lfp}(F) \))
Note

- For any monotonic function $f$, we have
  \[ f^i(\bot) \subseteq f^{i+1}(\bot) \]
- Straightforward induction on $i$
# Table of Contents

1. Introduction

2. Removing Superfluous Computations
   - Repeated Computations
   - Background 1: Rice’s theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Naive FP-iteration, again

Input  Constraint system $x_i \sqsupseteq f_i(\vec{x})$

1. $\vec{x} := (\bot, \ldots, \bot)$
2. $\vec{x} := F(\vec{x})$ (Recall $F(\vec{x}) = (f_1(\vec{x}), \ldots, f_n(\vec{x}))$)
3. If $\neg(F(\vec{x}) \sqsubseteq \vec{x})$, goto 2
4. Return “$\vec{x}$ is least solution”
Naive FP-iteration, again

Input Constraint system $x_i \sqsupseteq f_i(\vec{x})$

1. $\vec{x} := (\bot, \ldots, \bot)$
2. $\vec{x} := F(\vec{x})$ (Recall $F(\vec{x}) = (f_1(\vec{x}), \ldots, f_n(\vec{x}))$)
3. If $\neg(F(\vec{x}) \sqsubseteq \vec{x})$, goto 2
4. Return “$\vec{x}$ is least solution”

Note Originally, we had $\vec{x} := \vec{x} \sqcup F(\vec{x})$ in Step 2 and $F(\vec{x}) \not= \vec{x}$ in Step 3
- Also correct, as $F^i(\bot) \leq F^{i+1}(\bot)$, i.e., $\vec{x} \sqsubseteq F(\vec{x})$
- Saves $\sqcup$ operation.
- $\sqsubseteq$ may be more efficient than $=$.
Caveat

Naive fp-iteration may be rather inefficient

Let 
\[ S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x \]

\[ \begin{array}{l}
\text{0} \\
A[1] \quad \text{Expr} \\
A[2] \quad \text{Expr} \\
A[3] \quad \text{Expr} \\
A[4] \quad \text{Expr} \\
A[5] \quad \text{Expr} \\
\end{array} \]
Caveat

Naive fp-iteration may be rather inefficient

\[
\begin{align*}
& x := y + z \\
& M[1] := 1 \\
& M[2] := 1 \\
& M[3] := 1 \\
\end{align*}
\]

Let \( S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x \)

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A[1]</td>
<td>Expr</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Caveat

Naive fp-iteration may be rather inefficient

\[
\text{Let } S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x
\]

<table>
<thead>
<tr>
<th></th>
<th>(S)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(\emptyset)</td>
<td>1</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>1</td>
<td>Expr</td>
<td>(S)</td>
<td>({y + z})</td>
</tr>
<tr>
<td>2</td>
<td>Expr</td>
<td>Expr</td>
<td>(S)</td>
</tr>
<tr>
<td>3</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
</tr>
<tr>
<td>4</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
</tr>
<tr>
<td>5</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
</tr>
</tbody>
</table>
Caveat

Naive fp-iteration may be rather inefficient

\begin{equation}
\begin{aligned}
\text{Let } S &:= (\text{Expr} \cup \{y + z\}) - \text{Expr}_x \\
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
A[1] & \text{Expr} & \emptyset & \emptyset & \emptyset \\
A[2] & \text{Expr} & S & \{y + z\} & \{y + z\} \\
A[3] & \text{Expr} & \text{Expr} & S & \{y + z\} \\
A[4] & \text{Expr} & \text{Expr} & \text{Expr} & S \\
A[5] & \text{Expr} & \text{Expr} & \text{Expr} & \text{Expr}
\end{array}
\end{aligned}
\end{equation}
Caveat

Naive fp-iteration may be rather inefficient

Let $S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x$

<table>
<thead>
<tr>
<th></th>
<th>$S$</th>
<th></th>
<th>$\text{Expr}$</th>
<th>${y + z}$</th>
<th>${y + z}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Expr $\emptyset$</td>
<td>1</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>2</td>
<td>Expr $S$</td>
<td>3</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
</tr>
<tr>
<td>4</td>
<td>Expr $S$</td>
<td>5</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
</tr>
<tr>
<td>3</td>
<td>Expr $S$</td>
<td></td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
</tr>
</tbody>
</table>

1. $x := y + z$
Naive fp-iteration may be rather inefficient

\[
\begin{align*}
x & := y + z \\
M[1] & := 1 \\
M[2] & := 1 \\
M[3] & := 1
\end{align*}
\]

<table>
<thead>
<tr>
<th>Let ( S ) :=</th>
<th>((\text{Expr} \cup {y + z}) - \text{Expr}_x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A[1] )</td>
<td>( \text{Expr} ) ( \emptyset ) ( \emptyset ) ( \emptyset ) ( \emptyset ) ( \emptyset )</td>
</tr>
<tr>
<td>( A[2] )</td>
<td>( \text{Expr} ) ( S ) ( {y + z} ) ( {y + z} ) ( {y + z} ) ( {y + z} )</td>
</tr>
<tr>
<td>( A[3] )</td>
<td>( \text{Expr} ) ( \text{Expr} ) ( S ) ( {y + z} ) ( {y + z} ) ( {y + z} )</td>
</tr>
<tr>
<td>( A[4] )</td>
<td>( \text{Expr} ) ( \text{Expr} ) ( \text{Expr} ) ( S ) ( {y + z} ) ( {y + z} )</td>
</tr>
<tr>
<td>( A[5] )</td>
<td>( \text{Expr} ) ( \text{Expr} ) ( \text{Expr} ) ( \text{Expr} ) ( S ) ( {y + z} )</td>
</tr>
</tbody>
</table>
Idea: Instead of values from last iteration, use current values while computing RHSs.

\[
\begin{align*}
x & := y + z \\
M[1] & := 1 \\
M[2] & := 1 \\
M[3] & := 1 \\
M[4] & := 1 \\
M[5] & := 1 \\
0 & \\
A[1] & \text{Expr} \\
A[2] & \text{Expr} \\
A[3] & \text{Expr} \\
A[4] & \text{Expr} \\
A[5] & \text{Expr}
\end{align*}
\]
Round-Robin iteration

Idea: Instead of values from last iteration, use current values while computing RHSs.

1

\[ x := y + z \]

2

\[ M[1] := 1 \]

3

\[ M[2] := 1 \]

4

\[ M[3] := 1 \]

5

\[ A[1] \quad \text{Expr} \quad \emptyset \]

\[ A[2] \quad \text{Expr} \quad \{y + z\} \]

\[ A[3] \quad \text{Expr} \quad \{y + z\} \]

\[ A[4] \quad \text{Expr} \quad \{y + z\} \]

\[ A[5] \quad \text{Expr} \quad \{y + z\} \]
\( \vec{x} := (\bot, \ldots, \bot) \)

\textbf{do} {  
    finished := true  
    \textbf{for} (i=1;i<=n;++i) {  
      new := \( f_i(\vec{x}) \) \hfill // Evaluate RHS  
      \textbf{if} (x_i \neq \text{new}) { \hfill // If something changed  
        finished = false \hfill // No fp reached yet  
        x_i := x_i \sqcup \text{new} \hfill // Update variable  
      }  
    }  
  } \textbf{while} (!\text{finished})

\textbf{return} \( \vec{x} \)
Prove invariant: \( \vec{x} \sqsubseteq \text{lfp}(F) \)

- Initially, \((\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)\) holds \((\text{bot-least})\)
RR-Iteration: Correctness

Prove invariant: \( \vec{x} \sqsubseteq \text{lfp}(F) \)

- Initially, \((\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)\) holds (bot-least)
- On update:

\[ \vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x})) \]

From (1) we get \( \vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x})(\text{def.} \sqsubseteq \text{on } D^n) \)

From (IH) we get \( F(\vec{x}) \sqsubseteq \text{lfp}(F)(\text{mono, fixed-point}) \)

Hence \( \vec{x} \sqcup F(\vec{x}) \sqsubseteq \text{lfp}(F)(\text{least-upper-bound, IH}) \)

Together: \( \vec{x}' \sqsubseteq \text{lfp}(F)(\text{trans}) \)

Moreover, if algorithm terminates, we have \( \vec{x} = F(\vec{x}) \)

I.e., \( \vec{x} \) is a fixed-point.

Thus: \( \vec{x} = \text{lfp}(F) \)
RR-Iteration: Correctness

Prove invariant: \( \vec{x} \sqsubseteq \text{lfp}(F) \)

- Initially, \((\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)\) holds (bot-least)
- On update:
  - We have (1): \( \vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x})) \). We assume (IH): \( \vec{x} \sqsubseteq \text{lfp}(F) \)
Prove **invariant**: $\bar{x} \sqsubseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)$ holds (**bot-least**)
- On update:
  - We have (1): $\bar{x}' = \bar{x}(i := x_i \sqcup f_i(\bar{x}))$. We assume (**IH**): $\bar{x} \sqsubseteq \text{lfp}(F)$
  - From (1) we get $\bar{x}' \sqsubseteq \bar{x} \cup F(\bar{x})$ (**def. $\sqsubseteq$ on $\mathbb{D}^n$**)
RR-Iteration: Correctness

Prove invariant: $\vec{x} \sqsubseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)$ holds (bot-least)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \sqsubseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x})$ (def. $\sqsubseteq$ on $\mathbb{D}^n$)
  - From (IH) we get $F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (mono, fixed-point)

Moreover, if algorithm terminates, we have $\vec{x} = F(\vec{x})$.

I.e., $\vec{x}$ is a fixed-point.

Invariant: $\vec{x} \sqsubseteq \text{least fixed point}$

Thus: $\vec{x} = \text{lfp}(F)$. 

Prove **invariant**: $\vec{x} \sqsubseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)$ holds (**bot-least**)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \sqsubseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x})$ (**def. $\sqsubseteq$ on $\mathbb{D}^n$**)
  - From (IH) we get $F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (**mono, fixed-point**)
  - Hence $\vec{x} \sqcup F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (**least-upper-bound, IH**)

Moreover, if algorithm terminates, we have

\[ \vec{x} = F(\vec{x}) \]

\*I.e., $\vec{x}$ is a fixed-point.\*
Prove invariant: $\vec{x} \sqsubseteq \text{lfp}(F)$

- Initially, $(\perp, \ldots, \perp) \sqsubseteq \text{lfp}(F)$ holds (bot-least)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \sqsubseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x})$ (def.$\sqsubseteq$ on $\mathbb{D}^n$)
  - From (IH) we get $F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (mono, fixed-point)
  - Hence $\vec{x} \sqcup F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (least-upper-bound, IH)
  - Together: $\vec{x}' \sqsubseteq \text{lfp}(F)$ (trans)

Moreover, if algorithm terminates, we have $\vec{x}' = F(\vec{x})$.
I.e., $\vec{x}$ is a fixed-point.
RR-Iteration: Correctness

Prove invariant: $\vec{x} \subseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \subseteq \text{lfp}(F)$ holds (bot-least)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \subseteq \vec{x} \sqcup F(\vec{x})$ (def. $\subseteq$ on $\mathbb{D}^n$)
  - From (IH) we get $F(\vec{x}) \subseteq \text{lfp}(F)$ (mono, fixed-point)
  - Hence $\vec{x} \sqcup F(\vec{x}) \subseteq \text{lfp}(F)$ (least-upper-bound, IH)
  - Together: $\vec{x}' \subseteq \text{lfp}(F)$ (trans)

Moreover, if algorithm terminates, we have $\vec{x} = F(\vec{x})$
RR-Iteration: Correctness

Prove invariant: \( \vec{x} \sqsubseteq \text{lfp}(F) \)

- Initially, \((\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)\) holds (bot-least)
- On update:
  - We have (1): \( \vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x})) \). We assume (IH): \( \vec{x} \sqsubseteq \text{lfp}(F) \)
  - From (1) we get \( \vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x}) \) (def. \( \sqsubseteq \) on \( \mathbb{D}^n \))
  - From (IH) we get \( F(\vec{x}) \sqsubseteq \text{lfp}(F) \) (mono, fixed-point)
  - Hence \( \vec{x} \sqcup F(\vec{x}) \sqsubseteq \text{lfp}(F) \) (least-upper-bound, IH)
  - Together: \( \vec{x}' \sqsubseteq \text{lfp}(F) \) (trans)

Moreover, if algorithm terminates, we have \( \vec{x} = F(\vec{x}) \)

- I.e., \( \vec{x} \) is a fixed-point.
Prove invariant: $\vec{x} \subseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \subseteq \text{lfp}(F)$ holds (bot-least)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \subseteq \vec{x} \sqcup F(\vec{x})$ (def. $\subseteq$ on $\mathbb{D}^n$)
  - From (IH) we get $F(\vec{x}) \subseteq \text{lfp}(F)$ (mono, fixed-point)
  - Hence $\vec{x} \sqcup F(\vec{x}) \subseteq \text{lfp}(F)$ (least-upper-bound, IH)
  - Together: $\vec{x}' \subseteq \text{lfp}(F)$ (trans)

Moreover, if algorithm terminates, we have $\vec{x} = F(\vec{x})$

- l.e., $\vec{x}$ is a fixed-point.
- Invariant: $\vec{x} \subseteq$ least fixed point
RR-Iteration: Correctness

Prove invariant: $\vec{x} \sqsubseteq \text{lfp}(F)$

- Initially, $(\bot, \ldots, \bot) \sqsubseteq \text{lfp}(F)$ holds (bot-least)
- On update:
  - We have (1): $\vec{x}' = \vec{x}(i := x_i \sqcup f_i(\vec{x}))$. We assume (IH): $\vec{x} \sqsubseteq \text{lfp}(F)$
  - From (1) we get $\vec{x}' \sqsubseteq \vec{x} \sqcup F(\vec{x})$ (def.$\sqsubseteq$ on $\mathbb{D}^n$)
  - From (IH) we get $F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (mono, fixed-point)
  - Hence $\vec{x} \sqcup F(\vec{x}) \sqsubseteq \text{lfp}(F)$ (least-upper-bound, IH)
  - Together: $\vec{x}' \sqsubseteq \text{lfp}(F)$ (trans)

Moreover, if algorithm terminates, we have $\vec{x} = F(\vec{x})$

- I.e., $\vec{x}$ is a fixed-point.
- Invariant: $\vec{x} \sqsubseteq$ least fixed point
- Thus: $\vec{x} = \text{lfp}(F)$
Used Facts

\[ \text{trans } x \subseteq y \subseteq z \implies x \subseteq z \]
RR-Iteration: Improved Algorithm

We can save some operations

- Use \( \sqsubseteq \) instead of \( = \) in test
- No \( \sqcup \) on update

\( \vec{x} := (\bot, \ldots, \bot) \)

\[
\text{do } \{
\text{finished} := \text{true}
\text{for } (i=1; i<=n; ++i) \{
\text{new} := f_i(\vec{x}) \quad \text{// Evaluate RHS}
\text{if } (\neg (x_i \sqsubseteq \text{new})) \{ \quad \text{// If something changed}
\text{finished} = \text{false} \quad \text{// No fp reached yet}
\text{x_i} := \text{new} \quad \text{// Update variable}
\}
\}
\text{while } (!\text{finished})
\}
\text{return } \vec{x}
\]
RR-Iteration: Improved Algorithm: Correctness

Justification: Invariant $\vec{x} \sqsubseteq F(\vec{x})$
Justification: Invariant $\vec{x} \sqsubseteq F(\vec{x})$

- Holds initially: Obvious
Justification: Invariant $\vec{x} \subseteq F(\vec{x})$

- Holds initially: Obvious
- On update:
Justification: Invariant $\vec{x} \subseteq F(\vec{x})$

- Holds initially: Obvious
- On update:
  - We have $\vec{x}' = \vec{x}(i := f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq F(\vec{x})$
Justification: Invariant $\vec{x} \subseteq F(\vec{x})$

- Holds initially: Obvious
- On update:
  - We have $\vec{x}' = \vec{x}(i := f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq F(\vec{x})$
  - Hence $\vec{x} \subseteq \vec{x}' \subseteq F(\vec{x})$ (Def. $\subseteq$, IH)
RR-Iteration: Improved Algorithm: Correctness

Justification: Invariant $\vec{x} \subseteq F(\vec{x})$

- Holds initially: Obvious
- On update:
  - We have $\vec{x}' = \vec{x}(i := f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq F(\vec{x})$
  - Hence $\vec{x} \subseteq \vec{x}' \subseteq F(\vec{x})$ (Def.$\subseteq$, IH)
  - Hence $F(\vec{x}) \subseteq F(\vec{x}')$ (mono)
Justification: Invariant \( \vec{x} \sqsubseteq F(\vec{x}) \)

- Holds initially: Obvious
- On update:
  - We have \( \vec{x}' = \vec{x}(i := f_i(\vec{x})) \). We assume (IH): \( \vec{x} \sqsubseteq F(\vec{x}) \)
  - Hence \( \vec{x} \sqsubseteq \vec{x}' \sqsubseteq F(\vec{x}) \) (Def. \( \sqsubseteq \), IH)
  - Hence \( F(\vec{x}) \sqsubseteq F(\vec{x}') \) (mono)
  - Together \( \vec{x}' \sqsubseteq F(\vec{x}') \) (trans)
RR-Iteration: Improved Algorithm: Correctness

Justification: Invariant $\vec{x} \subseteq F(\vec{x})$

- Holds initially: Obvious
- On update:
  - We have $\vec{x}' = \vec{x}(i := f_i(\vec{x}))$. We assume (IH): $\vec{x} \subseteq F(\vec{x})$
  - Hence $\vec{x} \subseteq \vec{x}' \subseteq F(\vec{x})$ (Def.$\subseteq$, IH)
  - Hence $F(\vec{x}) \subseteq F(\vec{x}')$ (mono)
  - Together $\vec{x}' \subseteq F(\vec{x}')$ (trans)

With this invariant, we have
Justification: Invariant $\tilde{x} \sqsubseteq F(\tilde{x})$

- Holds initially: Obvious
- On update:
  - We have $\tilde{x}' = \tilde{x}(i := f_i(\tilde{x}))$. We assume (IH): $\tilde{x} \sqsubseteq F(\tilde{x})$
  - Hence $\tilde{x} \sqsubseteq \tilde{x}' \sqsubseteq F(\tilde{x})$ (Def.$\sqsubseteq$, IH)
  - Hence $F(\tilde{x}) \sqsubseteq F(\tilde{x}')$ (mono)
  - Together $\tilde{x}' \sqsubseteq F(\tilde{x}')$ (trans)

With this invariant, we have

- $x_i = f_i(\tilde{x})$ iff $x_i \sqsubseteq f_i(\tilde{x})$ (antisym)
RR-Iteration: Improved Algorithm: Correctness

Justification: Invariant \( \vec{x} \subseteq F(\vec{x}) \)

- Holds initially: Obvious
- On update:
  - We have \( \vec{x}' = \vec{x}(i := f_i(\vec{x})) \). We assume (IH): \( \vec{x} \subseteq F(\vec{x}) \)
  - Hence \( \vec{x} \subseteq \vec{x}' \subseteq F(\vec{x}) \) (Def. \( \subseteq \), IH)
  - Hence \( F(\vec{x}) \subseteq F(\vec{x}') \) (mono)
  - Together \( \vec{x}' \subseteq F(\vec{x}') \) (trans)

With this invariant, we have

- \( x_i = f_i(\vec{x}) \) iff \( x_i \sqsubseteq f_i(\vec{x}) \) (antisym)
- \( x_i \sqcup f_i(\vec{x}) = f_i(\vec{x}) \) (sup-absorb)
  - sup-absorb: \( x \sqsubseteq y \implies x \sqcup y = y \)
RR-Iteration: Termination

Definition (Chain)
A set $C \subseteq \mathbb{D}$ is called chain, iff all elements are mutually comparable:

$$\forall c_1, c_2 \in C. \ c_1 \sqsubseteq c_2 \lor c_2 \sqsubseteq c_1$$

A partial order has finite height, iff every chain is finite. Then, the height $h \in \mathbb{N}$ is the maximum cardinality of any chain.
RR-Iteration: Termination

**Definition (Chain)**

A set $C \subseteq \mathbb{D}$ is called chain, iff all elements are mutually comparable:

$$\forall c_1, c_2 \in C. \ c_1 \sqsubseteq c_2 \lor c_2 \sqsubseteq c_1$$

A partial order has **finite height**, iff every chain is finite. Then, the **height** $h \in \mathbb{N}$ is the maximum cardinality of any chain.

For a domain with finite chain height $h$, RR-iteration terminates within $O(n^2 h)$ RHS-evaluations.

- In each iteration of the outer loop, at least one variable increases, or the algorithm terminates. A variable may only increase $h - 1$ times.
Last Lecture

- Monotonic functions
  - Constraint system modeled as function
  - Least solution is least fixed point
- Knaster-Tarski fp-thm:
  - Lfp of monotonic function exists
- Kleene fp theorem:
  - Iterative characterization of lfp for distributive functions
  - Justifies naive fp-iteration
- Round-Robin iteration
  - Improves on naive iteration by using values of current round
  - Still depends on variable ordering
Problem:

The efficiency of RR depends on variable ordering
Problem:

The efficiency of RR depends on variable ordering

Let $S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x$

\[
\begin{array}{ccc}
0 & 1 \\
A[1] & \text{Expr} & \text{Expr} \\
A[2] & \text{Expr} & \text{Expr} \\
A[3] & \text{Expr} & \text{Expr} \\
A[5] & \text{Expr} & \emptyset \\
\end{array}
\]
The efficiency of RR depends on variable ordering

The diagram illustrates the variable assignments and expressions for M[1], M[2], M[3], and x := y+z.

Let $S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x$

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
</tr>
<tr>
<td>1</td>
<td>Expr</td>
<td>Expr</td>
<td>Expr</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>2</td>
<td>Expr</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>0</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>
Problem:

The efficiency of RR depends on variable ordering

\[ x := y + z \]

\[
\begin{array}{l}
M[1] := 1 \\
M[2] := 1 \\
M[3] := 1 \\
\end{array}
\]

Let \( S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x \)

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\hline
A[1] & \text{Expr} & \text{Expr} & \text{Expr} & \text{Expr} \\
A[2] & \text{Expr} & \text{Expr} & \text{Expr} & S \\
A[3] & \text{Expr} & \text{Expr} & S & \{y + z\} \\
A[4] & \text{Expr} & S & \{y + z\} & \{y + z\} \\
A[5] & \text{Expr} & \emptyset & \emptyset & \emptyset \\
\end{array}
\]
Problem:

The efficiency of RR depends on variable ordering

\[ x := y + z \]

\[
\begin{array}{c}
\text{Let } S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x \\
\hline
0 & 1 & 2 & 3 & 4 \\
\hline
A[1] & \text{Expr} & \text{Expr} & \text{Expr} & \text{Expr} & S \\
A[2] & \text{Expr} & \text{Expr} & \text{Expr} & S & \{y + z\} \\
A[3] & \text{Expr} & \text{Expr} & S & \{y + z\} & \{y + z\} \\
A[4] & \text{Expr} & S & \{y + z\} & \{y + z\} & \{y + z\} \\
A[5] & \text{Expr} & \emptyset & \emptyset & \emptyset & \emptyset \\
\end{array}
\]
Problem:

The efficiency of RR depends on variable ordering

Let $S := (\text{Expr} \cup \{y + z\}) - \text{Expr}_x$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A[3]$</td>
<td>Expr</td>
<td>Expr</td>
<td>$S$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
</tr>
<tr>
<td>$A[4]$</td>
<td>Expr</td>
<td>$S$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
<td>${y + z}$</td>
</tr>
<tr>
<td>$A[5]$</td>
<td>Expr</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
</tbody>
</table>

$x := y + z$

$M[1] := 1$

$M[2] := 1$

$M[3] := 1$
Problem:

The efficiency of RR depends on variable ordering

Rule of thumb

\( u \) before \( v \), if \( u \rightarrow^* v \)

Entry condition before loop body
Worklist algorithm

Problems of RR (remaining)

- Complete round required to detect termination
- If only one variable changes, everything is re-computed
- Depends on variable ordering.
Worklist algorithm

Problems of RR (remaining)
- Complete round required to detect termination
- If only one variable changes, everything is re-computed
- Depends on variable ordering.

Idea of worklist algorithm
- Store constraints whose RHS may have changed in a list
Worklist Algorithm: Pseudocode

\[ W = \{1...n\} \]
\[ \vec{x} = (\bot,...,\bot) \]

\textbf{while} (W \neq \varepsilon) \{ 
    \text{get an } i \in W, \ W = W - \{i\} 

    t = f_i(\vec{x}) 
    \textbf{if} (\neg (t \sqsubseteq x_i)) \{ 
        x_i = t 
        W = W \cup \{j \mid f_j \text{ depends on variable } i\} 
    \} 
\}
Worklist Algorithm: Example

- On whiteboard
Worklist Algorithm: Correctness

Invariants

1. $\vec{x} \subseteq F(\vec{x})$ and $\vec{x} \subseteq \text{lfp}F$
   - Same argument as for RR-iteration

2. $\neg(x_i \sqsubseteq f_i(\vec{x})) \implies i \in W$
   - Intuitively: Constraints that are not satisfied are on worklist
   - Initially, all $i$ in $W$
   - On update: Only RHS that depend on updated variable may change. Exactly these are added to $W$.
     If $f_i$ does not depend on variable $i$, the constraint $i$ holds for the new $\vec{x}$, so its removal from $W$ is OK.

- If loop terminates: Due to Inv. 2, we have solution. Due to Inv. 1, it is least solution.
Worklist Algorithm: Termination

Theorem

For a monotonic CS and a domain with finite height \( h \), the worklist algorithm returns the least solution and terminates within \( O(hN) \) iterations, where \( N \) is the size of the constraint system:

\[
N := \sum_{i=1}^{n} 1 + |f_i| \quad \text{where} \quad |f_i| := |\{i \mid f_i \text{ depends on variable } i\}|
\]
Theorem

For a monotonic CS and a domain with finite height \( h \), the worklist algorithm returns the least solution and terminates within \( O(hN) \) iterations, where \( N \) is the size of the constraint system:

\[
N := \sum_{i=1}^{n} 1 + |f_i| \quad \text{where} \quad |f_i| := |\{ i \mid f_i \text{ depends on variable } i \}| \]

Proof (Sketch):

• Number of iterations = Number of elements added to \( W \).
• Initially: \( n \) elements
• Constraint \( i \) added if variable its RHS depends on is changed
• Variable may not change more than \( h \) times. Constraint depends on \( |f_i| \) variables.
• Thus, no more than \( n + n \sum_{i=1}^{n} |f_i| = hN \) elements added to worklist.
Worklist Algorithm: Termination

Theorem

For a monotonic CS and a domain with finite height $h$, the worklist algorithm returns the least solution and terminates within $O(hN)$ iterations, where $N$ is the size of the constraint system:

$$N := \sum_{i=1}^{n} 1 + |f_i| \text{ where } |f_i| := |\{i \mid f_i \text{ depends on variable } i\}|$$

Proof (Sketch):

- Number of iterations = Number of elements added to $W$. 
Worklist Algorithm: Termination

Theorem

For a monotonic CS and a domain with finite height $h$, the worklist algorithm returns the least solution and terminates within $O(hN)$ iterations, where $N$ is the size of the constraint system:

$$N := \sum_{i=1}^{n} 1 + |f_i| \quad \text{where} \quad |f_i| := |\{i \mid f_i \text{ depends on variable } i\}|$$

Proof (Sketch):

- Number of iterations = Number of elements added to $W$.
- Initially: $n$ elements
Worklist Algorithm: Termination

Theorem

For a monotonic CS and a domain with finite height $h$, the worklist algorithm returns the least solution and terminates within $O(hN)$ iterations, where $N$ is the size of the constraint system:

$$N := \sum_{i=1}^{n} 1 + |f_i| \text{ where } |f_i| := \{|i| \mid f_i \text{ depends on variable } i\}|$$

Proof (Sketch):

- Number of iterations = Number of elements added to $W$.
- Initially: $n$ elements
- Constraint $i$ added if variable its RHS depends on is changed
  - Variable may not change more than $h$ times. Constraint depends on $|f_i|$ variables.
Worklist Algorithm: Termination

**Theorem**

*For a monotonic CS and a domain with finite height \( h \), the worklist algorithm returns the least solution and terminates within \( O(hN) \) iterations, where \( N \) is the size of the constraint system:*

\[
N := \sum_{i=1}^{n} 1 + |f_i| \quad \text{where} \quad |f_i| := |\{ i \mid f_i \text{ depends on variable } i \}|
\]

**Proof (Sketch):**

- Number of iterations = Number of elements added to \( W \).
- Initially: \( n \) elements
- Constraint \( i \) added if variable its RHS depends on is changed
  - Variable may not change more than \( h \) times. Constraint depends on \( |f_i| \) variables.
- Thus, no more than

\[
n + \sum_{i=1}^{n} h|f_i| = hN
\]

elements added to worklist.
Worklist Algorithm: Problems

- Dependencies of RHS need to be known.
  - No problem for our application
Worklist Algorithm: Problems

- Dependencies of RHS need to be known.
  - No problem for our application
- Which constraint to select next from worklist?
  - Requires strategy.
Worklist Algorithm: Problems

- Dependencies of RHS need to be known.
  - No problem for our application
- Which constraint to select next from worklist?
  - Requires strategy.
- Various more advanced algorithms exist
  - Determine dependencies dynamically (Generic solvers)
  - Only compute solution for subset of the variables (Local solvers)
  - Even: Local generic solvers
Summary:

- Constraint systems (over complete lattice, monotonic RHSs)
  - Encode as monotonic function \( F : \mathbb{D}^n \rightarrow \mathbb{D}^n \)
  - (Least) Solution = (least) fixed point
- Knaster-Tarski theorem: A least solution always exists
- Solve by fixpoint-iteration (naive, RR, WL)
  - Kleene-Theorem justifies naive fixpoint iteration
  - Similar ideas to justify RR, WL
Summary:

- Constraint systems (over complete lattice, monotonic RHSs)
  - Encode as monotonic function $F : \mathbb{D}^n \rightarrow \mathbb{D}^n$
  - (Least) Solution = (least) fixed point
- Knaster-Tarski theorem: A least solution always exists
- Solve by fixpoint-iteration (naive, RR, WL)
  - Kleene-Theorem justifies naive fixpoint iteration
  - Similar ideas to justify RR, WL
- Still Missing:
  - Link between least solution of constraint system, and
Available at $u$: $A[u] = \bigcap\{[\pi]\#\emptyset \mid \pi. v_0 \xrightarrow{\pi} u\}$
# Table of Contents

## 1 Introduction

## 2 Removing Superfluous Computations
- Repeated Computations
- Background 1: Rice’s theorem
- Background 2: Operational Semantics
- Available Expressions
- Background 3: Complete Lattices
- Fixed-Point Algorithms
- Monotonic Analysis Framework
- Dead Assignment Elimination
- Copy Propagation
- Summary

## 3 Abstract Interpretation

## 4 Alias Analysis

## 5 Avoiding Redundancy (Part II)

## 6 Interprocedural Analysis

## 7 Analysis of Parallel Programs

## 8 Replacing Expensive by Cheaper Operations

## 9 Exploiting Hardware Features

## 10 Optimization of Functional Programs
Monotonic Analysis Framework

Given

Flowgraph
A complete lattice $(\mathbb{D}, \sqsubseteq)$.
An initialization value $d_0 \in \mathbb{D}$
An abstract effect $\llbracket k \rrbracket^\# : \mathbb{D} \rightarrow \mathbb{D}$ for edges $k$
  • Such that $\llbracket k \rrbracket^\#$ is monotonic.
Monotonic Analysis Framework

Given
Flowgraph
A complete lattice \((\mathbb{D}, \sqsubseteq)\).
An initialization value \(d_0 \in \mathbb{D}\)
An abstract effect \([k]\# : \mathbb{D} \to \mathbb{D}\) for edges \(k\)
  * Such that \([k]\#\) is monotonic.

Wanted
\[
\text{MOP}[u] := \biguplus \{ [\pi]\#(d_0) \mid \pi \cdot v_0 \xrightarrow{\pi} u \}
\]
MOP = Merge over all paths
Monotonic Analysis Framework

Given

Flowgraph
A complete lattice \((\mathbb{D}, \sqsubseteq)\).
An initialization value \(d_0 \in \mathbb{D}\)
An abstract effect \([k]# : \mathbb{D} \rightarrow \mathbb{D}\) for edges \(k\)
  \- Such that \([k]#\) is monotonic.

Wanted

\[ MOP[u] := \bigsqcup \{ [\pi]#(d_0) \mid \pi \cdot v_0 \xrightarrow{\pi} u \} \]

\(MOP = \text{Merge over all paths}\)

Method

Compute least solution \(\text{MFP}\) of constraint system

\[
\begin{align*}
\text{MFP}[v_0] & \sqsubseteq d_0 \\
\text{init} \\
\text{MFP}[v] & \sqsubseteq [k]#(\text{MFP}[u]) \quad \text{for edges } k = (u, a, v) \\
\text{edge}
\end{align*}
\]

\(\text{MFP} = \text{Minimal fixed point}\)
In a monotonic analysis framework, we have

\[ MOP \sqsubseteq MFP \]
In a monotonic analysis framework, we have

\[ MOP \sqsubseteq MFP \]

- Intuitively: The constraint system’s least solution (MFP) is a correct approximation to the value defined over all paths reaching the program point (MOP).
In a monotonic analysis framework, we have

\[ MOP \sqsubseteq MFP \]

- Intuitively: The constraint system’s least solution (MFP) is a correct approximation to the value defined over all paths reaching the program point (MOP).
- In particular: \((\pi)[\#(d_0)] \sqsubseteq MFP[u]\) for \(v_0 \overset{\pi}{\rightarrow} u\)
To show $\text{MOP} \subseteq \text{MFP}$, i.e. (def. $\text{MOP}$, def. $\subseteq$ on $\mathbb{D}^n$)

$$\forall u. \bigcup \{ [[\pi]] # d_0 \mid \pi. v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]$$
Kam, Ullman: Proof

To show $\text{MOP} \subseteq \text{MFP}$, i.e. (def.$\text{MOP}$, def.$\subseteq$ on $\mathbb{D}^n$)

$$\forall u. \bigcup \{[\pi]^\#d_0 \mid \pi. v_0 \xrightarrow{\pi} u\} \subseteq \text{MFP}[u]$$

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

$$\forall \pi, u. v_0 \xrightarrow{\pi} u \implies [\pi]^\#d_0 \subseteq \text{MFP}[u]$$
To show \( \text{MOP} \subseteq \text{MFP} \), i.e. \((\text{def.MOP}, \text{def.} \subseteq \text{ on } \mathbb{D}^n)\)

\[
\forall u. \bigcup \{ [[\pi]]^\# d_0 \mid \pi. \ v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]
\]

It suffices to show that \( \text{MFP}[u] \) is an upper bound. \((\text{least-upper-bound})\)

\[
\forall \pi, u. \ v_0 \xrightarrow{\pi} u \implies [[\pi]]^\# d_0 \subseteq \text{MFP}[u]
\]

Induction on \( \pi \).
To show $\text{MOP} \subseteq \text{MFP}$, i.e. $(\text{def. MOP, def.} \subseteq \text{ on } \mathbb{D}^n)$

$$\forall u. \bigcup \{ [[\pi]]^\# d_0 \mid \pi, v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]$$

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

$$\forall \pi, u. v_0 \xrightarrow{\pi} u \implies [[\pi]]^\# d_0 \subseteq \text{MFP}[u]$$

**Induction on $\pi$.**

- **Base case:** $\pi = \varepsilon$. 

To show $\text{MOP} \subseteq \text{MFP}$, i.e. $(\text{def. MOP}, \text{def.} \subseteq \text{on } \mathbb{D}^n)$

\[ \forall u. \bigcup \{ [[\pi]]^\# d_0 \mid \pi. \upsilon_0 \overset{\pi}{\rightarrow} u \} \subseteq \text{MFP}[u] \]

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

\[ \forall \pi, u. \upsilon_0 \overset{\pi}{\rightarrow} u \implies [[\pi]]^\# d_0 \subseteq \text{MFP}[u] \]

Induction on $\pi$.

- Base case: $\pi = \varepsilon$.
  - We have $u = \upsilon_0$ (empty-path) and $[[\varepsilon]]^\# d_0 = d_0$ (empty-eff)
Kam, Ullman: Proof

To show \( \text{MOP} \subseteq \text{MFP} \), i.e. \((\text{def.MOP}, \text{def.} \subseteq \text{ on } \mathbb{D}^n)\)

\[
\forall u. \bigcup \{ [[\pi]] \# d_0 \mid \pi. \nu_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]
\]

It suffices to show that \( \text{MFP}[u] \) is an upper bound. (\textit{least-upper-bound})

\[
\forall \pi, u. \nu_0 \xrightarrow{\pi} u \implies [[\pi]] \# d_0 \subseteq \text{MFP}[u]
\]

\textbf{Induction on } \pi. \textbf{ }

- \textbf{Base case: } \pi = \varepsilon.
  - We have \( u = \nu_0 \) (\textit{empty-path}) and \( [[\varepsilon]] \# d_0 = d_0 \) (\textit{empty-eff})
  - As \( \text{MFP} \) is solution, the (init)-constraint yields \( d_0 \subseteq \text{MFP}[\nu_0] \).
To show $\text{MOP} \subseteq \text{MFP}$, i.e. (def. MOP, def. $\subseteq$ on $D^n$)

$$\forall u. \bigcup \{ [\pi] \# d_0 \mid \pi. v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]$$

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

$$\forall \pi, u. v_0 \xrightarrow{\pi} u \implies [\pi] \# d_0 \subseteq \text{MFP}[u]$$

Induction on $\pi$.
- **Base case:** $\pi = \varepsilon$.
  - We have $u = v_0$ (empty-path) and $[\varepsilon] \# d_0 = d_0$ (empty-eff)
  - As MFP is solution, the (init)-constraint yields $d_0 \subseteq \text{MFP}[v_0]$.
- **Step case:** $\pi = \pi'k$ for edge $k = (u, a, v)$
To show \( \text{MOP} \subseteq \text{MFP} \), i.e. (def. MOP, def. \( \subseteq \) on \( \mathbb{D}^n \))

\[
\forall u. \bigcup \{ \llbracket \pi \rrbracket \# d_0 \mid \pi. v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]
\]

It suffices to show that \( \text{MFP}[u] \) is an upper bound. (least-upper-bound)

\[
\forall \pi, u. v_0 \xrightarrow{\pi} u \implies \llbracket \pi \rrbracket \# d_0 \subseteq \text{MFP}[u]
\]

Induction on \( \pi \).

- **Base case:** \( \pi = \varepsilon \).
  - We have \( u = v_0 \) (empty-path) and \( \llbracket \varepsilon \rrbracket \# d_0 = d_0 \) (empty-eff).
  - As \( \text{MFP} \) is solution, the (init)-constraint yields \( d_0 \subseteq \text{MFP}[v_0] \).

- **Step case:** \( \pi = \pi'k \) for edge \( k = (u, a, v) \)
  - Assume \( v_0 \xrightarrow{\pi'} u \xrightarrow{a} v \) and (IH): \( \llbracket \pi' \rrbracket \# d_0 \subseteq \text{MFP}[u] \).
  - To show: \( \llbracket \pi'k \rrbracket \# d_0 \subseteq \text{MFP}[v] \)
Kam, Ullman: Proof

To show \( \text{MOP} \subseteq \text{MFP} \), i.e. (def.\( \text{MOP} \), def.\( \subseteq \) on \( \mathbb{D}^n \))

\[
\forall u. \bigcup \{ [\pi]^\# d_0 \mid \pi. v_0 \xrightarrow{\pi} u \} \subseteq \text{MFP}[u]
\]

It suffices to show that \( \text{MFP}[u] \) is an upper bound. (least-upper-bound)

\[
\forall \pi, u. v_0 \xrightarrow{\pi} u \implies [\pi]^\# d_0 \subseteq \text{MFP}[u]
\]

Induction on \( \pi \).

- **Base case:** \( \pi = \varepsilon \).
  - We have \( u = v_0 \) (empty-path) and \( [\varepsilon]^\# d_0 = d_0 \) (empty-eff).
  - As MFP is solution, the (init)-constraint yields \( d_0 \subseteq \text{MFP}[v_0] \).

- **Step case:** \( \pi = \pi'k \) for edge \( k = (u, a, v) \)
  - Assume \( v_0 \xrightarrow{\pi'} u \xrightarrow{a} v \) and (IH): \( [\pi']^\# d_0 \subseteq \text{MFP}[u] \).
    To show: \( [\pi'k]^\# d_0 \subseteq \text{MFP}[v] \)
  - Have \( [\pi'k]^\# = [k]^\# ([\pi']^\# d_0) \) (eff-comp)
Kam, Ullman: Proof

To show $\text{MOP} \sqsubseteq \text{MFP}$, i.e. $(\text{def.MOP}, \text{def.} \sqsubseteq \text{ on } \mathbb{D}^n)$

$$\forall u. \bigcup \{[[\pi]]^{\#} d_0 \mid \pi. v_0 \xrightarrow{\pi} u\} \sqsubseteq \text{MFP}[u]$$

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

$$\forall \pi, u. v_0 \xrightarrow{\pi} u \implies [[\pi]]^{\#} d_0 \sqsubseteq \text{MFP}[u]$$

Induction on $\pi$.

- Base case: $\pi = \varepsilon$.
  - We have $u = v_0$ (empty-path) and $[[\varepsilon]]^{\#} d_0 = d_0$ (empty-eff)
  - As MFP is solution, the (init)-constraint yields $d_0 \sqsubseteq \text{MFP}[v_0]$.

- Step case: $\pi = \pi' k$ for edge $k = (u, a, v)$
  - Assume $v_0 \xrightarrow{\pi'} u \xrightarrow{a} v$ and (IH): $[[\pi']]^{\#} d_0 \sqsubseteq \text{MFP}[u]$.
    - To show: $[[\pi'k]]^{\#} d_0 \sqsubseteq \text{MFP}[v]$
  - Have $[[\pi'k]]^{\#} = [[k]]^{\#} ([[\pi']]^{\#} d_0)$ (eff-comp)
  - $\sqsubseteq [[k]]^{\#} (\text{MFP}[u])$ (IH,mono)
To show $\text{MOP} \subseteq \text{MFP}$, i.e. $(\text{def.}\text{MOP}, \text{def.}\subseteq \text{on } D^n)$

$$\forall u. \bigcup \{\llbracket \pi \rrbracket \# d_0 \mid \pi \cdot v_0 \xrightarrow{\pi} u\} \subseteq \text{MFP}[u]$$

It suffices to show that $\text{MFP}[u]$ is an upper bound. (least-upper-bound)

$$\forall \pi, u. v_0 \xrightarrow{\pi} u \implies \llbracket \pi \rrbracket \# d_0 \subseteq \text{MFP}[u]$$

Induction on $\pi$.

- **Base case:** $\pi = \varepsilon$.
  - We have $u = v_0$ (empty-path) and $\llbracket \varepsilon \rrbracket \# d_0 = d_0$ (empty-eff)
  - As MFP is solution, the (init)-constraint yields $d_0 \subseteq \text{MFP}[v_0]$.

- **Step case:** $\pi = \pi'k$ for edge $k = (u, a, v)$
  - Assume $v_0 \xrightarrow{\pi'} u \xrightarrow{a} v$ and (IH): $\llbracket \pi' \rrbracket \# d_0 \subseteq \text{MFP}[u]$. To show: $\llbracket \pi'k \rrbracket \# d_0 \subseteq \text{MFP}[v]$
    - Have $\llbracket \pi'k \rrbracket \# = \llbracket k \rrbracket \# (\llbracket \pi' \rrbracket \# d_0)$ (eff-comp)
    - $\subseteq \llbracket k \rrbracket \# (\text{MFP}[u])$ (IH,mono)
    - $\subseteq \text{MFP}[v]$ (edge)-constraint, MFP is solution)
Facts

empty-path  $u \xleftarrow{\varepsilon} v \iff u = v$

empty-eff  $[\varepsilon]^\# \cdot d = d$

eff-comp  $[\pi_1 \pi_2]^\# = [\pi_2]^\# \circ [\pi_1]^\#$
Problem

- Yet another approximation :(
  - Recall: Abstract effect was already approximation
Problem

- Yet another approximation :
  - Recall: Abstract effect was already approximation
- Good news:
  - If the right-hand sides are distributive, we can compute MOP exactly
Theorem of Kildal

Kildal, 1972

In a distributive analysis framework (i.e., a monotonic analysis framework where the $[k]#$ are distributive), where all nodes are reachable, we have

$$MOP = MFP$$
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As MFP is least solution, the proposition follows.
Proof

We already know \( \text{MOP} \subseteq \text{MFP} \). To show that also \( \text{MFP} \subseteq \text{MOP} \), it suffices to show that MOP is a solution of the constraint system.

- As MFP is least solution, the proposition follows.
- Recall:

\[
\text{MOP}[u] \coloneqq \bigsqcup P[u], \text{ where } P[u] \coloneqq \{ [[\pi]]^\#(d_0) \mid \pi \cdot v_0 \overset{\pi}{\rightarrow} u \} \]
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As $\text{MFP}$ is least solution, the proposition follows.

- Recall:

$$\text{MOP}[u] := \bigsqcup P[u], \text{ where } P[u] := \{\llbracket \pi \rrbracket^\#(d_0) \mid \pi. \ v_0 \xrightarrow{\pi} u\}$$

(init) To show: $\text{MOP}[v_0] \supseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that MOP is a solution of the constraint system.

- As MFP is least solution, the proposition follows.

- Recall:

$$\text{MOP}[u] := \bigsqcup P[u], \quad \text{where } P[u] := \{[[\pi]]^\#(d_0) \mid \pi. v_0 \xrightarrow{\pi} u\}$$

(init) To show: $\text{MOP}[v_0] \supseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)

(edge) To show: $\text{MOP}[v] \supseteq [k]^\# \text{MOP}[u]$ for edge $k = (u, a, v)$
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that MOP is a solution of the constraint system.

- As MFP is least solution, the proposition follows.

Recall:

$$\text{MOP}[u] := \bigsqcup P[u], \text{ where } P[u] := \{\, \llbracket \pi \rrbracket^\#(d_0) \mid \pi. \ v_0 \xrightarrow{\pi} u \}$$

(init) To show: $\text{MOP}[v_0] \supseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)

(edge) To show: $\text{MOP}[v] \supseteq \llbracket k \rrbracket^\# \text{MOP}[u]$ for edge $k = (u, a, v)$

- Note (*): $P[u]$ not empty, as all nodes reachable
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As $\text{MFP}$ is least solution, the proposition follows.

- Recall:

\[
\text{MOP}[u] := \bigcup P[u], \text{ where } P[u] := \{ [\pi]^{\#}(d_0) \mid \pi. v_0 \xrightarrow{\pi} u \}
\]

(init) To show: $\text{MOP}[v_0] \supseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)

(edge) To show: $\text{MOP}[v] \supseteq [k]^{\#}\text{MOP}[u]$ for edge $k = (u, a, v)$

- Note (*): $P[u]$ not empty, as all nodes reachable

- $[k]^{\#}\text{MOP}[u] = \bigcup\{ [k]^{\#}(\pi)^{\#}d_0) \mid \pi. v_0 \xrightarrow{\pi} u \}$ (def.$\text{MOP}$, distrib,*
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As $\text{MFP}$ is least solution, the proposition follows.

- Recall:

  $$\text{MOP}[u] := \bigsqcup P[u], \text{ where } P[u] := \{[\pi]^\#(d_0) \mid \pi. v_0 \xrightarrow{\pi} u\}$$

(init) To show: $\text{MOP} [v_0] \supseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)

(edge) To show: $\text{MOP}[v] \supseteq [k]^\# \text{MOP}[u]$ for edge $k = (u, a, v)$

- Note (*): $P[u]$ not empty, as all nodes reachable
- $[k]^\# \text{MOP}[u] = \bigsqcup \{[k]^\#([\pi]^\#d_0) \mid \pi. v_0 \xrightarrow{\pi} u\}$ (def.MOP, distrib,*)
- $= \bigsqcup \{[\pi k]^\#d_0 \mid \pi. v_0 \xrightarrow{\pi} v\}$ (def.$[\cdot]^\#$ on paths. $k$ is edge, path-append)
Proof

We already know $\text{MOP} \subseteq \text{MFP}$. To show that also $\text{MFP} \subseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As $\text{MFP}$ is least solution, the proposition follows.

- Recall:

$$\text{MOP}[u] := \bigsqcup P[u], \text{ where } P[u] := \{[[\pi]]^\#(d_0) \mid \pi. \ v_0 \xrightarrow{\pi} u\}$$

(init) To show: $\text{MOP}[v_0] \supseteq d_0$

- Straightforward ($\text{upper-bound, empty-path, empty-eff}$)

(edge) To show: $\text{MOP}[v] \supseteq [k]^\#\text{MOP}[u]$ for edge $k = (u, a, v)$

- Note (*): $P[u]$ not empty, as all nodes reachable
- $[k]^\#\text{MOP}[u] = \bigsqcup\{[k]^\#([[\pi]]^\#d_0) \mid \pi. \ v_0 \xrightarrow{\pi} u\}$ (def.$\text{MOP}$, distrib,*)
- $= \bigsqcup\{[[\pi k]]^\#d_0 \mid \pi. \ v_0 \xrightarrow{\pi^k} v\}$ (def.$[[\cdot]]^\#$ on paths. $k$ is edge, path-append)
- $\subseteq \bigsqcup\{[[\pi]]^\#d_0 \mid \pi. \ v_0 \xrightarrow{\pi} v\}$ (sup-subset)
Proof

We already know $\text{MOP} \sqsubseteq \text{MFP}$. To show that also $\text{MFP} \sqsubseteq \text{MOP}$, it suffices to show that $\text{MOP}$ is a solution of the constraint system.

- As $\text{MFP}$ is least solution, the proposition follows.

- Recall:

$$\text{MOP}[u] := \bigsqcup P[u], \text{ where } P[u] := \{[[\pi]]^\#(d_0) \mid \pi. v_0 \xrightarrow{\pi} u\}$$

(init) To show: $\text{MOP}[v_0] \sqsupseteq d_0$

- Straightforward (upper-bound, empty-path, empty-eff)

(edge) To show: $\text{MOP}[v] \sqsupseteq [k]^\# \text{MOP}[u]$ for edge $k = (u, a, v)$

- Note (*): $P[u]$ not empty, as all nodes reachable

- $[k]^\# \text{MOP}[u] = \bigsqcup \{[[k]]^\#([\pi]^\#d_0) \mid \pi. v_0 \xrightarrow{\pi} u\}$ (def.$\text{MOP}$, distrib,*)

- $= \bigsqcup \{[[\pi k]]^\#d_0 \mid \pi. v_0 \xrightarrow{\pi k} v\}$ (def.$[[\cdot]]^\#$ on paths. $k$ is edge, path-append)

- $\sqsubseteq \bigsqcup \{[[\pi]]^\#d_0 \mid \pi. v_0 \xrightarrow{\pi} v\}$ (sup-subset)

- $= \text{MOP}[v]$ (def.$\text{MOP}$)

$\square$
Facts

path-append  \( k = (u, a, v) \in E \land v_0 \xrightarrow{\pi} u \iff v_0 \xrightarrow{\pi k} v \)

- Append edge to path

sup-subset  \( X \subseteq Y \implies \bigcup X \subseteq \bigcup Y \)
Reachability of all nodes is essential

- No paths to unreachable node $u$, i.e., $\text{MOP}[u] = \bot$
- But edges from other unreachable nodes possible

\[ \implies \text{Constraint of form } \text{MFP}[u] \supseteq \ldots \]
Note

Reachability of all nodes is essential
- No paths to unreachable node \( u \), i.e., \( \text{MOP}[u] = \perp \)
- But edges from other unreachable nodes possible
  \( \implies \) Constraint of form \( \text{MFP}[u] \supseteq \ldots \)

Eliminate unreachable nodes before creating CS
- E.g. by DFS from start node.
**Depth first search (pseudocode)**

```c
void dfs (node u) {
    if u ∉ R {
        R := R ∪ {u}
        for all v with (u, a, v) ∈ E {dfs v}
    }
}

void find_reachable () {
    R = {}
    dfs(V0)
    // R contains reachable nodes now
}
```
Summary

Input  CFG, distributive/(monotonic) analysis framework

• Framework defines domain \((\mathbb{D}, \sqsubseteq)\), initial value \(d_0 \in \mathbb{D}\) and abstract effects \([\cdot]^{\#} : E \rightarrow \mathbb{D} \rightarrow \mathbb{D}\)

• For each edge \(k\), \([k]^{\#}\) is distributive/(monotonic)

1. Eliminate unreachable nodes
2. Put up constraint system
3. Solve by worklist-algo, RR-iteration, ...

Output  (Safe approximation of) MOP - solution
Summary

Input  CFG, distributive/(monotonic) analysis framework
- Framework defines domain $(\mathbb{D}, \sqsubseteq)$, initial value $d_0 \in \mathbb{D}$ and abstract effects $\llbracket \cdot \rrbracket^\# : E \to \mathbb{D} \to \mathbb{D}$
- For each edge $k$, $\llbracket k \rrbracket^\#$ is distributive/(monotonic)

1. Eliminate unreachable nodes
2. Put up constraint system
3. Solve by worklist-algo, RR-iteration, ...

Output  (Safe approximation of) MOP - solution

Note  Abstract effects of available expressions are distributive
- As all functions of the form: $x \mapsto (a \cup x) \setminus b$
Last lecture

- Worklist algorithm: Find least solution with $O(hN)$ RHS-evaluations
  - $h$ height of domain, $N$ size of constraint system
- Monotonic analysis framework: $(D, \subseteq), d_0 \in D, \llbracket \cdot \rrbracket^\#$ (monotonic)
  - Yields $MOP[u] = \bigcup \{ \llbracket \pi \rrbracket^\# d_0 \mid \pi. v_0 \overset{\pi}{\rightarrow} u \}$
- Theorems of Kam/Ullman and Kildal
  - $MOP \subseteq MFP$,
  - Distributive framework and all nodes reachable: $MOP = MFP$
- Started with dead-assignment elimination
Summary (II) – How to develop a program optimization

- Optimization = Analysis + Transformation
Summary (II) – How to develop a program optimization

- Optimization = Analysis + Transformation
- Create semantic description of analysis result
  - Result for each program point
  - Depends on states reachable at this program point
  - In general, not computable
  - Prove transformation correct for (approximations of) this result
Summary (II) – How to develop a program optimization

• Optimization = Analysis + Transformation
• Create semantic description of analysis result
  • Result for each program point
  • Depends on states reachable at this program point
  • In general, not computable
  • Prove transformation correct for (approximations of) this result
• Create syntactic approximation of analysis result
  • Abstract effect of edges
  • Yields monotonic/distributive analysis framework
Summary (II) – How to develop a program optimization

- **Optimization = Analysis + Transformation**
- Create semantic description of analysis result
  - Result for each program point
  - Depends on states reachable at this program point
  - In general, not computable
  - Prove transformation correct for (approximations of) this result
- Create syntactic approximation of analysis result
  - Abstract effect of edges
  - Yields monotonic/distributive analysis framework
- Compute MFP.
  - Approximation of semantic result
Optimization = Analysis + Transformation

Create semantic description of analysis result
- Result for each program point
- Depends on states reachable at this program point
- In general, not computable
- Prove transformation correct for (approximations of) this result

Create syntactic approximation of analysis result
- Abstract effect of edges
- Yields monotonic/distributive analysis framework

Compute MFP.
- Approximation of semantic result

Perform transformation based on MFP
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Removing Superfluous Computations</td>
</tr>
<tr>
<td></td>
<td>Repeated Computations</td>
</tr>
<tr>
<td></td>
<td>Background 1: Rice's theorem</td>
</tr>
<tr>
<td></td>
<td>Background 2: Operational Semantics</td>
</tr>
<tr>
<td></td>
<td>Available Expressions</td>
</tr>
<tr>
<td></td>
<td>Background 3: Complete Lattices</td>
</tr>
<tr>
<td></td>
<td>Fixed-Point Algorithms</td>
</tr>
<tr>
<td></td>
<td>Monotonic Analysis Framework</td>
</tr>
<tr>
<td></td>
<td>Dead Assignment Elimination</td>
</tr>
<tr>
<td></td>
<td>Copy Propagation</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Interpretation</td>
</tr>
<tr>
<td>4</td>
<td>Alias Analysis</td>
</tr>
<tr>
<td>5</td>
<td>Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6</td>
<td>Interprocedural Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8</td>
<td>Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Hardware Features</td>
</tr>
<tr>
<td>10</td>
<td>Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Example

1: \( x = y + 2; \)
2: \( y = 4; \)
3: \( x = y + 3 \)
Example

1: x = y + 2;
2: y = 4;
3: x = y + 3

Value of $x$ computed in line 1 never used
Now: Dead-Assignment Elimination

Example

1: \( x = y + 2; \)
2: \( y = 4; \)
3: \( x = y + 3 \)

Value of \( x \) computed in line 1 never used

Equivalent program:

1: \text{nop};
2: \( y = 4; \)
3: \( x = y + 3 \)
Now: Dead-Assignment Elimination

Example

1: \( x = y + 2; \)
2: \( y = 4; \)
3: \( x = y + 3 \)

Value of \( x \) computed in line 1 never used

Equivalent program:

1: \text{nop};
2: \( y = 4; \)
3: \( x = y + 3 \)

\( x \) is called \textit{dead} at 1.
Live registers (semantically)

Register $x$ is **semantically live** at program point $u$, iff there is an execution to an end node, that depends on the value of $x$ at $u$:

$$x \in \text{Live}[u] \iff \exists \pi, v, \rho, \mu, a.
\begin{align*}
u &\xrightarrow{\pi} v \land v \in V_{\text{end}} \\
&\land (\rho, \mu) \in \llbracket u \rrbracket \\
&\land \llbracket \pi \rrbracket(\rho(x := a), \mu) \neq x \llbracket \pi \rrbracket(\rho, \mu)
\end{align*}$$

Where $\llbracket u \rrbracket := \{(\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. v_0 \xrightarrow{\pi} u \land \llbracket \pi \rrbracket(\rho_0, \mu_0) = (\rho, \mu)\}$

- Intuition: All states reachable at $u$
- Collecting semantics
Live registers (semantically)

Register $x$ is semantically live at program point $u$, iff there is an execution to an end node, that depends on the value of $x$ at $u$:

\[
x \in \text{Live}[u] \iff \exists \pi, v, \rho, \mu, a. \\
\quad u \xrightarrow{\pi} v \land v \in V_{\text{end}} \\
\quad \land (\rho, \mu) \in [u] \\
\quad \land [\pi](\rho(x := a), \mu) \neq x [\pi](\rho, \mu)
\]

Where $[u] := \{ (\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \ v_0 \xrightarrow{\pi} u \land [\pi](\rho_0, \mu_0) = (\rho, \mu) \}$

- Intuition: All states reachable at $u$
- Collecting semantics
  - $(\rho, \mu) =_X (\rho', \mu')$ iff $\mu = \mu'$ and $\forall x \in X. \ \rho(x) = \rho'(x)$
    - Equal on memory and “interesting” registers $X$
Live registers (semantically)

Register $x$ is **semantically live** at program point $u$, iff there is an execution to an end node, that depends on the value of $x$ at $u$:

$$x \in \text{Live}[u] \iff \exists \pi, \nu, \rho, \mu, a.
\begin{align*}
  u &\xrightarrow{\pi} \nu \land \nu \in V_{\text{end}} \\
  \land (\rho, \mu) &\in [u] \\
  \land [\pi](\rho(x := a), \mu) &\neq x [\pi](\rho, \mu)
\end{align*}$$

Where $[u] := \{(\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \nu_0 \xrightarrow{\pi} u \land [\pi](\rho_0, \mu_0) = (\rho, \mu)\}$

- Intuition: All states reachable at $u$
- Collecting semantics

- $(\rho, \mu) =_X (\rho', \mu')$ iff $\mu = \mu'$ and $\forall x \in X. \rho(x) = \rho'(x)$
- Equal on memory and “interesting” registers $X$

- $x$ is **semantically dead** at $u$, iff it is not live.
  - No execution depends on the value of $x$ at $u$. 
Transformation: Dead-Assignment Elimination

- Replace assignments/loads to dead registers by $\text{Nop}$
- $(u, x := *, v) \mapsto (u, \text{Nop}, v)$ if $x$ dead at $v$
- Obviously correct
  - States reachable at end nodes are preserved
- Correct approximation: Less dead variables ($=$ More live variables)
Live registers (syntactic approximation)

Register \( x \) is live at \( u \) (\( x \in L[u] \)), iff there is a path \( u \xrightarrow{\pi} v \), \( v \in V_{\text{end}} \), such that

- \( \pi \) does not contain writes to \( x \), and \( x \in X \)
- or \( \pi \) contains a read of \( x \) before the first write to \( x \)
Live registers (syntactic approximation)

Register $x$ is live at $u$ ($x \in L[u]$), iff there is a path $u \xrightarrow{\pi} v$, $v \in V_{\text{end}}$, such that

- $\pi$ does not contain writes to $x$, and $x \in X$
- or $\pi$ contains a read of $x$ before the first write to $x$

Abstract effects, propagating live variables backwards over edge

\[
\begin{align*}
[Nop] \# L &= L \\
[\text{Pos}(e)] \# L &= L \cup \text{regs}(e) \\
[\text{Neg}(e)] \# L &= L \cup \text{regs}(e) \\
[x := e] \# L &= L \setminus \{x\} \cup \text{regs}(e) \\
[x := M(e)] \# L &= L \setminus \{x\} \cup \text{regs}(e) \\
[M(e_1) := M(e_2)] \# L &= L \cup \text{regs}(e_1) \cup \text{regs}(e_2)
\end{align*}
\]

Note: distributive.
Live registers (syntactic approximation)

Register $x$ is live at $u$ ($x \in L[u]$), iff there is a path $u \xrightarrow{\pi} v$, $v \in V_{\text{end}}$, such that

- $\pi$ does not contain writes to $x$, and $x \in X$
- or $\pi$ contains a read of $x$ before the first write to $x$

Abstract effects, propagating live variables backwards over edge

\[
\begin{align*}
\text{[Nop]} \# L &= L \\
\text{[Pos}(e)\text{]} \# L &= L \cup \text{regs}(e) \\
\text{[Neg}(e)\text{]} \# L &= L \cup \text{regs}(e) \\
\text{[x := e]} \# L &= L \setminus \{x\} \cup \text{regs}(e) \\
\text{[x := M}(e)\text{]} \# L &= L \setminus \{x\} \cup \text{regs}(e) \\
\text{[M}(e_1) := M(e_2)\text{]} \# L &= L \cup \text{regs}(e_1) \cup \text{regs}(e_2)
\end{align*}
\]

Note: distributive.

Lift to path (backwards!): $[k_1 \ldots k_n] \# := [k_1] \# \circ \ldots \circ [k_n] \#$
Live registers (syntactic approximation)

Register $x$ is live at $u$ ($x \in L[u]$), iff there is a path $u \xrightarrow{\pi} v$, $v \in V_{\text{end}}$, such that

- $\pi$ does not contain writes to $x$, and $x \in X$
- or $\pi$ contains a read of $x$ before the first write to $x$

Abstract effects, propagating live variables backwards over edge

Abstract effects, propagating live variables backwards over edge

$$[[\text{Nop}]]^\# L = L$$
$$[[\text{Pos}(e)]]^\# L = L \cup \text{regs}(e)$$
$$[[\text{Neg}(e)]]^\# L = L \cup \text{regs}(e)$$
$$[[x := e]]^\# L = L \setminus \{x\} \cup \text{regs}(e)$$
$$[[x := M(e)]]^\# L = L \setminus \{x\} \cup \text{regs}(e)$$
$$[[M(e_1) := M(e_2)]]^\# L = L \cup \text{regs}(e_1) \cup \text{regs}(e_2)$$

Note: distributive.

Lift to path (backwards!): $[[k_1 \ldots k_n]]^\# := [[k_1]]^\# \circ \ldots \circ [[k_n]]^\#$

Live at $u$ (MOP): $L[u] = \bigcup \{[[\pi]]^\# X \mid \exists v \in V_{\text{end}}. u \xrightarrow{\pi} v\}$
Example

1. $x = y + 2$
2. $y = 5$
3. $x = y + 2$
4. $M[y] = x$
5. $x = 0$
6. $x = 0$
Example

\[
\begin{align*}
x &= y + 2 \\
y &= 5 \\
x &= y + 2 \\
M[y] &= x \\
x &= 0
\end{align*}
\]
Example

1. $x = y + 2$
2. $y = 5$
3. $x = y + 2$
4. $M[y] = x \{y\}$
5. $x = 0 \{x, y\}$
Example

1. $x = y + 2$
2. $y = 5$
3. $x = y + 2$
4. $\{x, y\}$
5. $M[y] = x$
6. $\{y\}$
7. $x = 0$
8. $\{x, y\}$
Example

1. \( x = y + 2 \)
2. \( y = 5 \)
3. \( \{ y \} \)
4. \( x = y + 2 \)
5. \( \{ x, y \} \)
6. \( \{ y \} \)
7. \( M[y] = x \)
8. \( x = 0 \)
9. \( \{ x, y \} \)
Example

1. $x = y + 2$  
2. $\{\}$  
3. $y = 5$  
4. $x = y + 2$  
5. $M[y] = x$  
6. $\{x, y\}$

1. $x = y + 2$  
2. $\{\}$  
3. $y = 5$  
4. $x = y + 2$  
5. $M[y] = x$  
6. $\{x, y\}$
Example

\[ \{y\} \xrightarrow{x=y+2} \{\} \xrightarrow{y=5} \{y\} \xrightarrow{x=y+2} \{x, y\} \xrightarrow{M[y]=x} \{y\} \xrightarrow{x=0} \{x, y\} \]
Example

\[ \{y\} \xrightarrow{x=y+2} \{\} \xrightarrow{y=5} \{y\} \xrightarrow{x=y+2} \{x, y\} \xrightarrow{M[y]=x} \{y\} \xrightarrow{x=0} \{x, y\} \]
Liveness: Correct approximation

Theorem

(Syntactic) liveness is a correct approximation of semantic liveness

\[ \text{Live}[u] \subseteq L[u] \]
Liveness: Correct approximation

Theorem

(Syntactic) liveness is a correct approximation of semantic liveness

\[ \text{Live}[u] \subseteq \text{L}[u] \]

- Proof: On whiteboard.
Computing $L$

Use constraint system

$$L[u] \supseteq X$$

$$L[u] \supseteq [k] \# L[v]$$

for $u \in V_{\text{end}}$

for edges $k = (u, a, v)$
Computing $L$

Use constraint system

\[
L[u] \supseteq X \quad \text{for } u \in V_{\text{end}}
\]

\[
L[u] \supseteq [[k]] \# L[v] \quad \text{for edges } k = (u, a, v)
\]

Information propagated backwards
Computing L

Use constraint system

\[ L[u] \supseteq X \quad \text{for } u \in V_{\text{end}} \]

\[ L[u] \supseteq [k]^\# L[v] \quad \text{for edges } k = (u, a, v) \]

Information propagated backwards

Domain: \((\text{Reg}, \subseteq)\)

- \text{Reg}: The finitely many registers occurring in program.
  \(\Rightarrow\) Finite height

- Moreover, the \([k]^\#\) are distributive
Computing L

Use constraint system

\[ L[u] \supseteq X \quad \text{for } u \in V_{\text{end}} \]

\[ L[u] \supseteq \llbracket k \rrbracket \# L[v] \quad \text{for edges } k = (u, a, v) \]

Information propagated backwards

Domain: \((\text{Reg}, \subseteq)\)

- Reg: The finitely many registers occurring in program.
  \[ \Rightarrow \] Finite height

- Moreover, the \(\llbracket k \rrbracket \#\) are distributive

Can compute least solution (MFP)

- Worklist algo, RR-iteration, naive fp-iteration
Backwards Analysis Framework

Given CFG, Domain: \((\mathbb{D}, \sqsubseteq)\), init. value: \(d_0 \in \mathbb{D}\), abstract effects: 

\[
\llbracket \cdot \rrbracket^\#: \mathbb{D} \rightarrow \mathbb{D}, \text{ monotonic}
\]

\[
\text{MOP}[u] := \bigsqcup \{ \llbracket \pi \rrbracket^# d_0 \mid \exists v \in V_{\text{end}}. u \xrightarrow{\pi} v \}
\]

MFP is least solution of

\[
\text{MFP}[u] \sqsupseteq d_0 \quad \text{for } u \in V_{\text{end}}
\]

\[
\text{MFP}[u] \sqsupseteq \llbracket k \rrbracket^\# \text{MFP}[v] \quad \text{for edges } k = (u, a, v)
\]
Backwards Analysis Framework

Given CFG, Domain: $(\mathcal{D}, \sqsubseteq)$, init. value: $d_0 \in \mathcal{D}$, abstract effects: $\llbracket \cdot \rrbracket^\# : \mathcal{D} \to \mathcal{D}$, monotonic

$$\text{MOP}[u] := \bigsqcup \{ \llbracket \pi \rrbracket^\# d_0 \mid \exists v \in V_{\text{end}}. \ u \xrightarrow{\pi} v \}$$

MFP is least solution of

$$\text{MFP}[u] \sqsupseteq d_0 \quad \text{for } u \in V_{\text{end}}$$

$$\text{MFP}[u] \sqsupseteq \llbracket k \rrbracket^\# \text{MFP}[v] \quad \text{for edges } k = (u, a, v)$$

• We have:

$$\text{MOP} \sqsubseteq \text{MFP}$$
Backwards Analysis Framework

Given CFG, Domain: \((\mathbb{D}, \sqsubseteq)\), init. value: \(d_0 \in \mathbb{D}\), abstract effects:
\[
[\cdot]^\#: \mathbb{D} \rightarrow \mathbb{D}, \text{ monotonic}
\]
\[
\text{MOP}[u] := \bigsqcup \{[[\pi]]^# d_0 \mid \exists v \in V_{\text{end}}. \ u \xrightarrow{\pi} v\}
\]
MFP is least solution of
\[
\text{MFP}[u] \sqsubseteq d_0 \quad \text{for } u \in V_{\text{end}}
\]
\[
\text{MFP}[u] \sqsubseteq [[k]]^# \text{MFP}[v] \quad \text{for edges } k = (u, a, v)
\]

- We have:

\[
\text{MOP} \sqsubseteq \text{MFP}
\]

- If the \([[k]]^#\) are distributive, and from every node an end node can be reached:

\[
\text{MOP} = \text{MFP}
\]
Backwards Analysis Framework

Given CFG, Domain: \((\mathbb{D}, \sqsubseteq)\), init. value: \(d_0 \in \mathbb{D}\), abstract effects:
\(\llbracket \cdot \rrbracket^\#: \mathbb{D} \rightarrow \mathbb{D}\), monotonic

\[
MOP[u] := \bigsqcup \{ \llbracket \pi \rrbracket^\# d_0 \mid \exists v \in V_{\text{end}}. \ u \xrightarrow{\pi} v \}
\]

MFP is least solution of

\[
MFP[u] \sqsupseteq d_0 \quad \text{for } u \in V_{\text{end}}
\]

\[
MFP[u] \sqsupseteq \llbracket k \rrbracket^\# \text{MFP}[v] \quad \text{for edges } k = (u, a, v)
\]

• We have:

\[
MOP \sqsubseteq MFP
\]

• If the \(\llbracket k \rrbracket^\#\) are distributive, and from every node an end node can be reached:

\[
MOP = MFP
\]

• Proofs:
Backwards Analysis Framework

Given CFG, Domain: \((\mathbb{D}, \sqsubseteq)\), init. value: \(d_0 \in \mathbb{D}\), abstract effects:
\[
\begin{bmatrix}\cdot\end{bmatrix}^\# : \mathbb{D} \to \mathbb{D}, \text{ monotonic}
\]
\[
\text{MOP}[u] := \bigsqcup \{\begin{bmatrix}\pi\end{bmatrix}^#d_0 \mid \exists v \in V_{\text{end}}. u \xrightarrow{\pi} v\}
\]
MFP is least solution of
\[
\begin{align*}
\text{MFP}[u] & \sqsubseteq d_0 \\ 
\text{MFP}[u] & \sqsubseteq \begin{bmatrix}k\end{bmatrix}^\# \text{MFP}[v]
\end{align*}
\]
\text{for } u \in V_{\text{end}} \text{ for edges } k = (u, a, v)

- We have:
\[
\text{MOP} \sqsubseteq \text{MFP}
\]
- If the \([k]^\#\) are distributive, and from every node an end node can be reached:
\[
\text{MOP} = \text{MFP}
\]
- Proofs:
  - Analogously to forward case :)
Example: Dead Assignment elimination

```c
while (x>0) {
    y = y + 1
    x = x + y
    x = 1
}
```

On whiteboard.
Last Lecture

- Monotonic forward/backward framework
- Live variables, dead assignment elimination
  - $x$ live at $u$
  - Semantically: $x \in \text{Live}[u]$: Exists execution that depends on value of $x$ at $u$
  - Syntactic approximation: $x \in L[u]$: $x$ read before it is overwritten
  - Correctness proof
    - Induction on path, case distinction over edges
Analysis: Classifications

- Forward vs. backward
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cap$
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq = \subseteq$, i.e. $\cup = \cup$
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backward** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cap$
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq = \subseteq$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $\llbracket k \rrbracket \# X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
Analysis: Classifications

- **Forward vs. backward**
  - **Forward**: Considers executions reaching a program point
  - **Backwards**: Considers executions from program point to end

- **Must vs. May**
  - **Must**: Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cap$
  - **May**: Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $[[k]]^# X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq \subset$, i.e. $\cup = \cap$
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq \subset$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $[k]^\# X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.

- **Examples:**
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: \( \subseteq = \supseteq \), i.e. \( \cup = \cap \)
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: \( \subseteq = \subsetneq \), i.e. \( \cup = \cup \)

- **Kill/Gen analysis**
  - Effects have form \( \lbrack [k] \rbrack \# X = X \cap \text{kill}_k \cup \text{gen}_k \)
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.

- **Examples:**
  - Available expressions:
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** considers executions reaching a program point
  - **Backwards** considers executions from program point to end

- **Must vs. May**
  - **Must** something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cap$
  - **May** something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq = \subseteq$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $\text{fun}_k X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.

- **Examples:**
  - Available expressions: forward, must, kill-gen
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq \supseteq = \cap$, i.e. $\cup = \cap$
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq \subseteq$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $\llbracket k \rrbracket^k X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.

- **Examples:**
  - Available expressions: forward,must,kill-gen
  - Live variables:
Analysis: Classifications

- **Forward vs. backward**
  - **Forward** Considers executions reaching a program point
  - **Backwards** Considers executions from program point to end

- **Must vs. May**
  - **Must** Something is guaranteed to hold, and thus allows optimization
    - On set domain: $\subseteq = \supseteq$, i.e. $\cup = \cap$
  - **May** Something may hold, and thus prevents (correct) optimization
    - On set domain: $\subseteq = \subseteq$, i.e. $\cup = \cup$

- **Kill/Gen analysis**
  - Effects have form $\llbracket k \rrbracket X = X \cap \text{kill}_k \cup \text{gen}_k$
  - Particular simple class. Distributive by construction.
  - Bitvector analysis: Kill/Gen on finite set domain.

- **Examples**:
  - Available expressions: forward, must, kill-gen
  - Live variables: backward, may, kill-gen
Eliminating dead assignments may lead to new dead assignments

1. \{\} 
2. \{x\} 
3. y = x 
4. \{x\} 
5. \{x, y\}
Eliminating dead assignments may lead to new dead assignments

\[
\emptyset \xrightarrow{x=1} \{x\} \xrightarrow{y=x} \emptyset \xrightarrow{x=1} \{x\} \xrightarrow{y=1} \{x, y\}
\]
Eliminating dead assignments may lead to new dead assignments

\[
\begin{aligned}
\{\} & \xrightarrow{x=1} \{\} & \xrightarrow{y=x} \{\} & \xrightarrow{x=1} \{x\} & \xrightarrow{y=1} \{x, y\}
\end{aligned}
\]
Dead Assignment Elimination: Problems

Eliminating dead assignments may lead to new dead assignments

```
{}  x=1  {}  y=x  {}  x=1  {x}  {x, y}
```

1  2  3  4  5

In a loop, a variable may keep itself alive

```
x=0  x=x+1
```

```
x=1
y=1
```
Dead Assignment Elimination: Problems

Eliminating dead assignments may lead to new dead assignments:

\[
\begin{align*}
\{ & \} \\
1 & \rightarrow 2 & x = 1 & \rightarrow 3 & y = x & \rightarrow 4 & x = 1 & \rightarrow 5 & x, y \}
\end{align*}
\]

In a loop, a variable may keep itself alive:

\[
\begin{align*}
\{ x \} & \rightarrow 1 & x = x + 1 & \rightarrow 2 & x = 0
\end{align*}
\]
Truly live registers

Idea: Consider assignment edge \((u, x = e, v)\).

- If \(x\) is not semantically live at \(v\), the registers in \(e\) need not become live at \(u\).
- There values influence a register that is dead anyway.
Example

1 -> x=1 -> 2 -> y=x -> 3 -> x=1 -> 4 -> y=1 -> 5
Example

\[ \{x, y\} \]
Example
Example
Example
Example
Example
True Liveness vs. repeated liveness

- True liveness detects more dead variables than repeated liveness

Repeated liveness:

\[
\begin{align*}
\{x\} & \rightarrow 1 \quad x = x + 1 \\
& \quad x = 0 \\
& \rightarrow 2 \quad \{x\}
\end{align*}
\]
True Liveness vs. repeated liveness

- True liveness detects more dead variables than repeated liveness

True liveness:

\[
\begin{align*}
&\{\} \quad 1 \xrightarrow{x=x+1} \quad x=0 \\
&\{x\} \quad 2
\end{align*}
\]
True Liveness vs. repeated liveness

- True liveness detects more dead variables than repeated liveness

True liveness:

\[
\begin{align*}
\{x\} & \xrightarrow{x=x+1} 1 \\
1 & \xrightarrow{x=0} 0 \\
\{x\} & \xrightarrow{\text{}} 2 \\
\end{align*}
\]
Live registers: Abstract effects

\[ \begin{align*}
\llbracket \text{Nop} \rrbracket & \# L = L \\
\llbracket \text{Pos}(e) \rrbracket & \# L = L \cup \text{regs}(e) \\
\llbracket \text{Neg}(e) \rrbracket & \# L = L \cup \text{regs}(e) \\
\llbracket x := e \rrbracket & \# L = L \setminus \{x\} \cup (\text{regs}(e)) \\
\llbracket x := M(e) \rrbracket & \# L = L \setminus \{x\} \cup (\text{regs}(e)) \\
\llbracket M(e_1) := e_2 \rrbracket & \# L = L \cup \text{regs}(e_1) \cup \text{regs}(e_2)
\end{align*} \]
Truly live registers: Abstract effects

\[
\begin{align*}
\llbracket \text{Nop} \rrbracket &\ # TL = TL \\
\llbracket \text{Pos}(e) \rrbracket &\ # TL = TL \cup \text{regs}(e) \\
\llbracket \text{Neg}(e) \rrbracket &\ # TL = TL \cup \text{regs}(e) \\
\llbracket x := e \rrbracket &\ # TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset) \\
\llbracket x := M(e) \rrbracket &\ # TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset) \\
\llbracket M(e_1) := e_2 \rrbracket &\ # TL = TL \cup \text{regs}(e_1) \cup \text{regs}(e_2)
\end{align*}
\]
Truly live registers: Abstract effects

\[
\begin{align*}
\llbracket \text{Nop} \rrbracket &\# TL = TL \\
\llbracket \text{Pos}(e) \rrbracket &\# TL = TL \cup \text{regs}(e) \\
\llbracket \text{Neg}(e) \rrbracket &\# TL = TL \cup \text{regs}(e) \\
\llbracket x := e \rrbracket &\# TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset) \\
\llbracket x := M(e) \rrbracket &\# TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset) \\
\llbracket M(e_1) := e_2 \rrbracket &\# TL = TL \cup \text{regs}(e_1) \cup \text{regs}(e_2)
\end{align*}
\]

Effects are more complicated. No kill/gen, but still distributive.
Truly live registers: Abstract effects

\[\[[\text{Nop}]\]# TL = TL\]
\[\[[\text{Pos}(e)]\]# TL = TL \cup \text{regs}(e)\]
\[\[[\text{Neg}(e)]\]# TL = TL \cup \text{regs}(e)\]
\[\[[x := e]\]# TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset)\]
\[\[[x := M(e)]\]# TL = TL \setminus \{x\} \cup (x \in TL?\text{regs}(e): \emptyset)\]
\[\[[M(e_1) := e_2]\]# TL = TL \cup \text{regs}(e_1) \cup \text{regs}(e_2)\]

Effects are more complicated. No kill/gen, but still distributive. We have MFP = MOP :)
True Liveness: Correct approximation

Theorem

*True liveness is a correct approximation of semantic liveness* $\text{Live}[u] \subseteq \text{TL}[u]$
True Liveness: Correct approximation

Theorem

True liveness is a correct approximation of semantic liveness $\text{Live}[u] \subseteq \text{TL}[u]$

- Proof: On whiteboard.
# Table of Contents

1. Introduction

2. Removing Superfluous Computations
   - Repeated Computations
   - Background 1: Rice’s theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.

- E.g., $R = T_e$ after redundancy elimination
Copy propagation

Idea: Often have assignments of form \( r_1 = r_2 \).
- E.g., \( R = T_e \) after redundancy elimination
- In many cases, we can, instead, replace \( r_1 \) by \( r_2 \) in subsequent code
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.
  - E.g., $R = T_e$ after redundancy elimination
  - In many cases, we can, instead, replace $r_1$ by $r_2$ in subsequent code
    $\implies \quad r_1$ becomes dead, and assignment can be eliminated
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.

- E.g., $R = T_e$ after redundancy elimination
- In many cases, we can, instead, replace $r_1$ by $r_2$ in subsequent code

$\implies r_1$ becomes dead, and assignment can be eliminated

$r_1 = T_e; \ M[0] = r_1 + 3$
Copy propagation

Idea: Often have assignments of form \( r_1 = r_2 \).
- E.g., \( R = T_e \) after redundancy elimination
- In many cases, we can, instead, replace \( r_1 \) by \( r_2 \) in subsequent code

\[ \implies r_1 \text{ becomes dead, and assignment can be eliminated} \]

\[ r_1 = T_e; \quad M[0] = T_e + 3 \]
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.

- E.g., $R = T_e$ after redundancy elimination
- In many cases, we can, instead, replace $r_1$ by $r_2$ in subsequent code

$\implies r_1$ becomes dead, and assignment can be eliminated

\begin{align*}
\text{Nop;} \quad M[0] &= T_e + 3
\end{align*}
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.
- E.g., $R = T_e$ after redundancy elimination
- In many cases, we can, instead, replace $r_1$ by $r_2$ in subsequent code

⇒ $r_1$ becomes dead, and assignment can be eliminated

Analysis: Maintain an acyclic graph between registers
- Edge $x \to y$ implies $\rho(x) = \rho(y)$ for every state reachable at $u$
- Assignment $x = y$ creates edge $x \to y$. 
Copy propagation

Idea: Often have assignments of form $r_1 = r_2$.
- E.g., $R = T_e$ after redundancy elimination
- In many cases, we can, instead, replace $r_1$ by $r_2$ in subsequent code

$\implies r_1$ becomes dead, and assignment can be eliminated

Analysis: Maintain an acyclic graph between registers
- Edge $x \rightarrow y$ implies $\rho(x) = \rho(y)$ for every state reachable at $u$
- Assignment $x = y$ creates edge $x \rightarrow y$.

Transformation: Replace variables in expressions according to graph
Example

On Whiteboard
Abstract Effects

\[
\begin{align*}
\text{\texttt{[Nop]}} \# C &= C \\
\text{\texttt{[Pos(e)]}} \# C &= C \\
\text{\texttt{[Neg(e)]}} \# C &= C \\
\text{\texttt{[x = y]}} \# C &= C \setminus \{x \to *, * \to x\} \cup \{x \to y\} \quad \text{for } y \in \text{Reg}, y \neq x \\
\text{\texttt{[x = e]}} \# C &= C \setminus \{x \to *, * \to x\} \quad \text{for } e \in \text{Expr} \setminus \text{Reg} \text{ or } e = x \\
\text{\texttt{[x = M[e]]}} \# C &= C \setminus \{x \to *, * \to x\} \\
\text{\texttt{[M[e_1] = e_2]}} \# C &= C
\end{align*}
\]

where \( \{x \to *, * \to x\} \) is the set of edges from/to \( x \)

Obviously, abstract effects preserve acyclicity of \( C \)

Moreover, out-degree of nodes is \( \leq 1 \)

Abstract effects are distributive
Last Lecture

- Classification of analysis
  - Forward vs. backward, must vs. may, kill/gen, bitvector
- Truly live variables
  - Better approximation of „semantically life”
  - Idea: Don’t care about values of variables that only affect dead variables anyway.
- Copy propagation
  - Replace registers by registers with equal value, to create dead assignments
- Whole procedure: Simple redundancy elimination, then CP and DAE to clean up
Analysis Framework

- Domain: \( \mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq \)  
  - I.e.: More precise means more edges (Safe approximation: less edges)  
  - Join: \( \cap \) (Must analysis)  
  - Forward analysis, initial value \( d_0 = \emptyset \)

\[ MOP[u] = \bigcap \{ [\pi] \# \emptyset \mid v_0 \xrightarrow{\pi} u \} \]
Analysis Framework

- **Domain:** $(\mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq)$
  - I.e.: More precise means more edges (Safe approximation: less edges)
  - Join: $\cap$ (Must analysis)
  - Forward analysis, initial value $d_0 = \emptyset$

$$\implies \text{MOP}[u] = \bigcap \{ [[\pi]] \neq \emptyset \mid v_0 \xrightarrow{\pi} u \}$$

- **Correctness:** $x \rightarrow y \in \text{MOP}[u] \implies \forall (\rho, \mu) \in [u]. \rho(x) = \rho(y)$
  - Justifies correctness of transformation wrt. MOP
  - Proof: Later!

- Note: Formally, domain contains all graphs.
  - Required for complete lattice property!
  - But not suited for implementation (Set of all pairs of registers)
  - Add $\bot$-element to domain.
  - Intuition: $\bot$ means unreachable.
Analysis Framework

- **Domain:** $(\mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq)$
  - I.e.: More precise means more edges (Safe approximation: less edges)
  - Join: $\cap$ (Must analysis)
  - Forward analysis, initial value $d_0 = \emptyset$

  \[
  \text{MOP}[u] = \bigcap \{[\pi]\#\emptyset \mid v_0 \xrightarrow{\pi} u\}
  \]

  - **Correctness:** $x \rightarrow y \in \text{MOP}[u] \implies \forall (\rho, \mu) \in [u]. \rho(x) = \rho(y)$
    - Justifies correctness of transformation wrt. MOP
    - Proof: Later!

  - **Note:** Formally, domain contains all graphs.
Analysis Framework

- **Domain:** $(\mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq)$
  - i.e.: More precise means more edges (Safe approximation: less edges)
  - Join: $\cap$ (Must analysis)
  - Forward analysis, initial value $d_0 = \emptyset$

\[ \implies MOP[u] = \bigcap \{ [\pi] \# \emptyset | v_0 \xrightarrow{\pi} u \} \]

- **Correctness:** $x \rightarrow y \in MOP[u] \implies \forall (\rho, \mu) \in [u]. \rho(x) = \rho(y)$
  - Justifies correctness of transformation wrt. MOP
  - Proof: Later!

- **Note:** Formally, domain contains all graphs.
  - Required for complete lattice property!
Analysis Framework

- **Domain:** \( (\mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq) \)
  - I.e.: More precise means more edges (Safe approximation: less edges)
  - Join: \( \cap \) (Must analysis)
  - Forward analysis, initial value \( d_0 = \emptyset \)

\[ \implies \text{MOP}[u] = \bigcap \{ [\pi] \not\supseteq \emptyset | v_0 \xrightarrow{\pi} u \} \]

- **Correctness:** \( x \rightarrow y \in \text{MOP}[u] \implies \forall (\rho, \mu) \in [u]. \rho(x) = \rho(y) \)
  - Justifies correctness of transformation wrt. MOP
  - Proof: Later!

- **Note:** Formally, domain contains all graphs.
  - Required for complete lattice property!
  - But not suited for implementation (Set of all pairs of registers)
Analysis Framework

- **Domain:** \((D = 2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
  - I.e.: More precise means more edges (Safe approximation: less edges)
  - Join: \(\cap\) (Must analysis)
  - Forward analysis, initial value \(d_0 = \emptyset\)

  \[ \Rightarrow \text{MOP}[u] = \bigcap \{[[\pi]] \neq \emptyset \mid v_0 \xrightarrow{\pi} u\} \]

- **Correctness:** \(x \rightarrow y \in \text{MOP}[u] \implies \forall (\rho, \mu) \in [u]. \rho(x) = \rho(y)\)
  - Justifies correctness of transformation wrt. MOP
  - Proof: Later!

- **Note:** Formally, domain contains all graphs.
  - Required for complete lattice property!
  - But not suited for implementation (Set of all pairs of registers)
  - Add \(\bot\)-element to domain. \([k] \neq \bot := \bot\).
Analysis Framework

- **Domain:** \( (\mathbb{D} = 2^{\text{Reg} \times \text{Reg}}, \supseteq) \)
  - I.e.: More precise means more edges (Safe approximation: less edges)
  - Join: \( \cap \) (Must analysis)
  - Forward analysis, initial value \( d_0 = \emptyset \)

\[ \implies \text{MOP}[u] = \bigcap \{ \llbracket \pi \rrbracket \# \emptyset \mid v_0 \xrightarrow{\pi} u \} \]

- **Correctness:** \( x \rightarrow y \in \text{MOP}[u] \implies \forall (\rho, \mu) \in \llbracket u \rrbracket. \rho(x) = \rho(y) \)
  - Justifies correctness of transformation wrt. MOP
  - Proof: Later!

- **Note:** Formally, domain contains all graphs.
  - Required for complete lattice property!
  - But not suited for implementation (Set of all pairs of registers)
  - Add \( \perp \)-element to domain. \( \llbracket k \rrbracket \# \perp := \perp. \)
  - Intuition: \( \perp \) means unreachable.
# Table of Contents

1. Introduction

2. Removing Superfluous Computations
   - Repeated Computations
   - Background 1: Rice's theorem
   - Background 2: Operational Semantics
   - Available Expressions
   - Background 3: Complete Lattices
   - Fixed-Point Algorithms
   - Monotonic Analysis Framework
   - Dead Assignment Elimination
   - Copy Propagation
   - Summary

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Procedure as a whole

1. Simple redundancy elimination
   - Replaces re-computation by memorization
   - Inserts superfluous moves

2. Copy propagation
   - Removes superfluous moves
   - Creates dead assignments

3. Dead assignment elimination
Example: $a[7] \rightarrow$

1. $r_1 = M[a+7]$  
2. $r_2 = r_1 - 1$  
3. $M[a+7] = r_2$
Example: $a[7]$ — —

Introduced memorization registers

$T_1 = a+7$

$r_1 = M[T_1]$

$T_2 = r_1 - 1$

$r_2 = T_2$

$T_1 = a+7$

$M[T_1] = r_2$
Example: $a[7] − −$

Eliminated redundant computations

- $T_1 = a + 7$
- $r_1 = M[T_1]$
- $T_2 = r_1 - 1$
- $r_2 = T_2$
- Nop
- $M[T_1] = r_2$
Example: $a[7] - -$ 

Copy propagation done 

$T_1 = a + 7$ 

$r_1 = M[T_1]$ 

$T_2 = r_1 - 1$ 

$r_2 = T_2$ 

Nop 

$M[T_1] = T_2$
Example: $a[7] \rightarrow \rightarrow$

Eliminated dead assignments

$T_1 = a + 7$

$r_1 = M[T_1]$

$T_2 = r_1 - 1$

Nop

Nop

$M[T_1] = T_2$
<table>
<thead>
<tr>
<th></th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Removing Superfluous Computations</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Interpretation</td>
</tr>
<tr>
<td>4</td>
<td>Alias Analysis</td>
</tr>
<tr>
<td>5</td>
<td>Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6</td>
<td>Interprocedural Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8</td>
<td>Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Hardware Features</td>
</tr>
<tr>
<td>10</td>
<td>Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Background: Simulation

• Given:
  
  Concrete values \( C \), abstract values \( D \), actions \( A \)
  
  Initial values \( c_0 \in C, d_0 \in D \)
  
  Concrete effects \([ [ a ] ] : C \to C\), abstract effects \([ [ a ] ] \# : D \to D\)
  
  With forward-generalization to paths:
  
  \([ [ k_1 \ldots k_n ] ] = [ [ k_n ] ] \circ \ldots \circ [ [ k_1 ] ]\) and
  
  \([ [ k_1 \ldots k_n ] ] \# = [ [ k_n ] ] \# \circ \ldots \circ [ [ k_1 ] ] \#\)
  
  Relation \( \Delta \subseteq C \times D \)
  
  Assume:
  
  Initial values in relation: \( c_0 \Delta d_0 \)
  
  Relation preserved by effects: \( c \Delta d = \Rightarrow [ [ k ] ] c \Delta [ [ k ] ] \# d\)
  
  Get: Relation preserved by paths from initial values: \([ [ \pi ] ] c_0 \Delta [ [ \pi ] ] \# d_0\)
  
  Proof: Straightforward induction on paths. On whiteboard!
Background: Simulation

- **Given:**
  - Concrete values $\mathbb{C}$, abstract values $\mathbb{D}$, actions $A$
Background: Simulation

- Given:
  - Concrete values $C$, abstract values $D$, actions $A$
  - Initial values $c_0 \in C$, $d_0 \in D$
Given:

- Concrete values $C$, abstract values $D$, actions $A$
- Initial values $c_0 \in C$, $d_0 \in D$
- Concrete effects $[a] : C \rightarrow C$, abstract effects $[a]^{\#} : D \rightarrow D$
  - With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^{\#} = [k_n]^{\#} \circ \ldots \circ [k_1]^{\#}$
Background: Simulation

• Given:
  • Concrete values $\mathbb{C}$, abstract values $\mathbb{D}$, actions $A$
  • Initial values $c_0 \in \mathbb{C}$, $d_0 \in \mathbb{D}$
  • Concrete effects $[a] : \mathbb{C} \to \mathbb{C}$, abstract effects $[a]^\# : \mathbb{D} \to \mathbb{D}$
    • With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^\# = [k_n]^\# \circ \ldots \circ [k_1]^\#$
  • Relation $\Delta \subseteq \mathbb{C} \times \mathbb{D}$
**Background: Simulation**

- **Given:**
  - Concrete values $C$, abstract values $D$, actions $A$
  - Initial values $c_0 \in C$, $d_0 \in D$
  - Concrete effects $[a] : C \rightarrow C$, abstract effects $[a]^# : D \rightarrow D$
    - With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^# = [k_n]^# \circ \ldots \circ [k_1]^#$
  - Relation $\Delta \subseteq C \times D$

- **Assume:**
Background: Simulation

- **Given:**
  - Concrete values $C$, abstract values $D$, actions $A$
  - Initial values $c_0 \in C$, $d_0 \in D$
  - Concrete effects $\llbracket a \rrbracket : C \rightarrow C$, abstract effects $\llbracket a \rrbracket^\# : D \rightarrow D$
    - With forward-generalization to paths: $\llbracket k_1 \ldots k_n \rrbracket = \llbracket k_n \rrbracket \circ \ldots \circ \llbracket k_1 \rrbracket$ and $\llbracket k_1 \ldots k_n \rrbracket^\# = \llbracket k_n \rrbracket^\# \circ \ldots \circ \llbracket k_1 \rrbracket^\#$
  - Relation $\Delta \subseteq C \times D$

- **Assume:**
  - Initial values in relation: $c_0 \Delta d_0$
Background: Simulation

- **Given:**
  - Concrete values $\mathbb{C}$, abstract values $\mathbb{D}$, actions $A$
  - Initial values $c_0 \in \mathbb{C}$, $d_0 \in \mathbb{D}$
  - Concrete effects $[a] : \mathbb{C} \rightarrow \mathbb{C}$, abstract effects $[a]^\# : \mathbb{D} \rightarrow \mathbb{D}$
    - With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^\# = [k_n]^\# \circ \ldots \circ [k_1]^\#$
  - Relation $\Delta \subseteq \mathbb{C} \times \mathbb{D}$

- **Assume:**
  - Initial values in relation: $c_0 \Delta d_0$
  - Relation preserved by effects: $c \Delta d \implies [k]c \Delta [k]^\#d$
Background: Simulation

- **Given:**
  - Concrete values $\mathbb{C}$, abstract values $\mathbb{D}$, actions $A$
  - Initial values $c_0 \in \mathbb{C}$, $d_0 \in \mathbb{D}$
  - Concrete effects $[a]: \mathbb{C} \rightarrow \mathbb{C}$, abstract effects $[a]^\#: \mathbb{D} \rightarrow \mathbb{D}$
    - With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^\# = [k_n]^\# \circ \ldots \circ [k_1]^\#
  - Relation $\Delta \subseteq \mathbb{C} \times \mathbb{D}$

- **Assume:**
  - Initial values in relation: $c_0 \Delta d_0$
  - Relation preserved by effects: $c \Delta d \implies [k]c \Delta [k]^\# d$

- **Get:** Relation preserved by paths from initial values: $[\pi]c_0 \Delta [\pi]^\# d_0$
Given:

- Concrete values $C$, abstract values $D$, actions $A$
- Initial values $c_0 \in C$, $d_0 \in D$
- Concrete effects $[a] : C \rightarrow C$, abstract effects $[a]^\# : D \rightarrow D$
  
  - With forward-generalization to paths: $[k_1 \ldots k_n] = [k_n] \circ \ldots \circ [k_1]$ and $[k_1 \ldots k_n]^\# = [k_n]^\# \circ \ldots \circ [k_1]^\#$

Assume:

- Initial values in relation: $c_0 \Delta d_0$
- Relation preserved by effects: $c \Delta d \implies [k]c \Delta [k]^\# d$

Get: Relation preserved by paths from initial values: $[\pi]c_0 \Delta [\pi]^\# d_0$

Proof: Straightforward induction on paths. On whiteboard!
Background: Description relation

- Now: $c \Delta d$ — Concrete value $c$ described by abstract value $d$
Background: Description relation

- Now: $c \triangle d$ — Concrete value $c$ described by abstract value $d$
- Moreover, assume complete lattices on $\mathbb{C}$ and $\mathbb{D}$.
  - Intuition: $x \sqsubseteq x'$ — $x$ is more precise than $x'$

147 / 471
Background: Description relation

- Now: \( c \triangle d \) — Concrete value \( c \) described by abstract value \( d \)
- Moreover, assume complete lattices on \( C \) and \( D \).
  - Intuition: \( x \sqsubseteq x' \) — \( x \) is more precise than \( x' \)
- Assume \( \triangle \) to be monotonic on abstract values:

  \[
  c \triangle d \land d \sqsubseteq d' \implies c \triangle d'
  \]

  - Intuition: Less precise abstract value still describes concrete value

- Assume for all sets of paths \( P \):

  \[
  \left( \forall \pi \in P. \left[ [\pi] \right] c_0 \triangle \left[ [\pi] \right] d_0 \right) \implies \left( \bigsqcup_{\pi \in P} \left[ [\pi] \right] c_0 \right) \triangle \left( \bigsqcup_{\pi \in P} \left[ [\pi] \right] d_0 \right)
  \]

  - Intuition: Concrete values due to paths \( P \) described by abstract values
Background: Description relation

- Now: $c \triangle d$ — Concrete value $c$ described by abstract value $d$
- Moreover, assume complete lattices on $\mathbb{C}$ and $\mathbb{D}$.
  - Intuition: $x \sqsubseteq x'$ — $x$ is more precise than $x'$
- Assume $\Delta$ to be monotonic on abstract values:
  \[
  c \triangle d \land d \sqsubseteq d' \implies c \triangle d'
  \]
  - Intuition: Less precise abstract value still describes concrete value
- Assume $\Delta$ to be distributive on concrete values:
  \[
  (\forall c \in \mathbb{C}. \ c \triangle d) \iff (\bigsqcup \mathbb{C}) \triangle d
  \]
  - Note: Implies anti-monotonicity: $c' \sqsubseteq c \land c \triangle d \implies c' \triangle d$
  - Intuition: More precise concrete values still described by abstract value

- Assumptions and implications:

We get for all sets of paths $P$:

\[
(\forall \pi \in P. \ \llbracket \pi \rrbracket c_0 \triangle \llbracket \pi \rrbracket d_0) \implies (\bigsqcup \pi \in P. \ \llbracket \pi \rrbracket c_0) \triangle (\bigsqcup \pi \in P. \ \llbracket \pi \rrbracket d_0)
\]

- Intuition: Concrete values due to paths $P$ described by abstract values
Background: Description relation

- Now: \( c \triangle d \) — Concrete value \( c \) described by abstract value \( d \)
- Moreover, assume complete lattices on \( C \) and \( D \).
  - Intuition: \( x \sqsubseteq x' \) — \( x \) is more precise than \( x' \)
- Assume \( \Delta \) to be monotonic on abstract values:

\[
c \triangle d \land d \sqsubseteq d' \implies c \triangle d'
\]

  - Intuition: Less precise abstract value still describes concrete value
- Assume \( \Delta \) to be distributive on concrete values:

\[
(\forall c \in C. \ c \triangle d) \iff (\bigsqcup C) \triangle d
\]

  - Note: Implies anti-monotonicity: \( c' \sqsubseteq c \land c \triangle d \implies c' \triangle d \)
  - Intuition: More precise concrete values still described by abstract value
- We get for all sets of paths \( P \):

\[
(\forall \pi \in P. [\pi]c_0 \triangle [\pi]\#d_0) \implies (\bigsqcup_{\pi \in P} [\pi]c_0) \triangle (\bigsqcup_{\pi \in P} [\pi]\#d_0)
\]

  - Intuition: Concrete values due to paths \( P \) described by abstract values
Application to Program Analysis

- Concrete values: Sets of states with \( \subseteq \)
  - Intuition: Less states = more precise information

\[ C := \bigcup_{(\rho,\mu) \in C \cap \text{dom}[k]} [k](\rho,\mu), \text{i.e., don't include undefined effects} \]

- Concrete initial values: All states: \( c_0 = \text{State} \)

- Abstract values: Domain of analysis, abstract effects: \( [k], d_0 \)

- Description relation: States described by abstract value
  - Usually: Define \( \Delta \) on single states, and lift to set of states: \( S \Delta A \iff \forall (\rho,\mu) \in S. (\rho,\mu) \Delta A \)
  - This guarantees distributivity in concrete states

\[ [u] \Delta MOP [u] \]

- All states reachable at \( u \) described by analysis result at \( u \).
Application to Program Analysis

- **Concrete values**: Sets of states with $\subseteq$
  - Intuition: Less states = more precise information
- **Concrete effects**: Effects of edges (generalized to sets of states)
  - $[k]C := \bigcup_{(\rho,\mu) \in C \cap \text{dom}[k]} [k](\rho, \mu)$, i.e., don’t include undefined effects
Application to Program Analysis

- Concrete values: Sets of states with $\subseteq$
  - Intuition: Less states = more precise information
- Concrete effects: Effects of edges (generalized to sets of states)
  - $\llbracket k \rrbracket C := \bigcup_{(\rho, \mu) \in C \cap \text{dom}[k]} \llbracket k \rrbracket(\rho, \mu)$, i.e., don’t include undefined effects
- Concrete initial values: All states: $c_0 = \text{State}$
Application to Program Analysis

- Concrete values: Sets of states with $\subseteq$
  - Intuition: Less states = more precise information
- Concrete effects: Effects of edges (generalized to sets of states)
  - $\llbracket k \rrbracket C := \bigcup_{(\rho, \mu) \in C \cap \text{dom}[k]} \llbracket k \rrbracket (\rho, \mu)$, i.e., don’t include undefined effects
- Concrete initial values: All states: $c_0 = \text{State}$
- Abstract values: Domain of analysis, abstract effects: $\llbracket k \rrbracket \#$, $d_0$
Application to Program Analysis

- Concrete values: Sets of states with $\subseteq$
  - Intuition: Less states = more precise information
- Concrete effects: Effects of edges (generalized to sets of states)
  - $\llbracket k \rrbracket C := \bigcup_{(\rho, \mu) \in C \cap \text{dom}[k]} \llbracket k \rrbracket(\rho, \mu)$, i.e., don’t include undefined effects
- Concrete initial values: All states: $c_0 = \text{State}$
- Abstract values: Domain of analysis, abstract effects: $\llbracket k \rrbracket\#$, $d_0$
- Description relation: States described by abstract value
  - Usually: Define $\Delta$ on single states, and lift to set of states:
    \[ S \Delta A \text{ iff } \forall (\rho, \mu) \in S. (\rho, \mu) \Delta A \]
  - This guarantees distributivity in concrete states
Application to Program Analysis

- Concrete values: Sets of states with $\subseteq$
  - Intuition: Less states = more precise information
- Concrete effects: Effects of edges (generalized to sets of states)
  - $\llbracket k \rrbracket C := \bigcup_{(\rho, \mu) \in C \cap \text{dom}[k]} \llbracket k \rrbracket(\rho, \mu)$, i.e., don’t include undefined effects
- Concrete initial values: All states: $c_0 = \text{State}$
- Abstract values: Domain of analysis, abstract effects: $\llbracket k \rrbracket \#$, $d_0$
- Description relation: States described by abstract value
  - Usually: Define $\Delta$ on single states, and lift to set of states:
    \[ S \Delta A \iff \forall (\rho, \mu) \in S. (\rho, \mu) \Delta A \]
  - This guarantees distributivity in concrete states
- We get: $\llbracket u \rrbracket \Delta \text{MOP}[u]$
  - All states reachable at $u$ described by analysis result at $u$. 
Example: Available expressions

- Recall: $\mathcal{D} = (2^{\text{Expr}}, \supseteq)$
Example: Available expressions

- Recall: $\mathbb{D} = (2^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangleq A$ iff $\forall e \in A. \llbracket e \rrbracket \rho = \rho(T_e)$
Example: Available expressions

- Recall: $\mathbb{D} = (2^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangle A$ iff $\forall e \in A. \llbracket e \rrbracket \rho = \rho(T_e)$
- Prove: $A \supseteq A' \land (\rho, \mu) \triangle A \implies (\rho, \mu) \triangle A'$
Example: Available expressions

• Recall: $\mathbb{D} = (\mathcal{2}^{\text{Expr}}, \supseteq)$

• Define: $(\rho, \mu) \triangle A$ iff $\forall e \in A. \llbracket e \rrbracket \rho = \rho(T_e)$

• Prove: $A \supseteq A' \wedge (\rho, \mu) \triangle A \implies (\rho, \mu) \triangle A'$

• Prove: $(\rho, \mu) \triangle A \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, A) \rrbracket (\rho, \mu)$
  - where $\text{tr}(T_e = e, A) = \text{if } e \in A \text{ then Nop else } T_e = e |$
  - $\text{tr}(a, A) = a$
Example: Available expressions

- Recall: $\mathbb{D} = (2^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangleq A$ iff $\forall e \in A. [e] \rho = \rho(T_e)$
- Prove: $A \supseteq A' \land (\rho, \mu) \triangleq A \implies (\rho, \mu) \triangleq A'$
- Prove: $(\rho, \mu) \triangleq A \implies [a](\rho, \mu) = [\text{tr}(a, A)](\rho, \mu)$
  - where $\text{tr}(T_e = e, A) = \begin{cases} \text{Nop} & \text{if } e \in A \\ T_e = e \end{cases}$ | $\text{tr}(a, A) = a$
- Transformation in CFG: $(u, a, v) \mapsto (u, \text{tr}(a, A[u]), v)$
Example: Available expressions

- Recall: $\mathbb{D} = (2^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangle A$ iff $\forall e \in A. [e]_\rho = \rho(T_e)$
- Prove: $A \supseteq A' \land (\rho, \mu) \triangle A \implies (\rho, \mu) \triangle A'$
- Prove: $(\rho, \mu) \triangle A \implies [a]((\rho, \mu) = [\text{tr}(a, A)]((\rho, \mu))$
  - where $\text{tr}(T_e = e, A) = \text{if } e \in A \text{ then } \text{Nop} \text{ else } T_e = e$
  - $\text{tr}(a, A) = a$
- Transformation in CFG: $(u, a, v) \mapsto (u, \text{tr}(a, A[u]), v)$
- Prove: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  - For AE, we have $d_0 = \emptyset$, which implies the above.
Example: Available expressions

- Recall: $\mathbb{D} = (2^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangle A$ iff $\forall e \in A. \llbracket e \rrbracket \rho = \rho(T_e)$
- Prove: $A \supseteq A' \land (\rho, \mu) \triangle A \implies (\rho, \mu) \triangle A'$
- Prove: $(\rho, \mu) \triangle A \implies \llbracket a \rrbracket(\rho, \mu) = \llbracket \text{tr}(a, A) \rrbracket(\rho, \mu)$
  - where $\text{tr}(T_e = e, A) = \text{if } e \in A \text{ then Nop else } T_e = e | \text{tr}(a, A) = a$
  - Transformation in CFG: $(u, a, v) \mapsto (u, \text{tr}(a, A[u]), v)$
- Prove: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  - For AE, we have $d_0 = \emptyset$, which implies the above.
- Prove: $(\rho, \mu) \in \text{dom}[k] \land (\rho, \mu) \triangle D \implies \llbracket k \rrbracket(\rho, \mu) \triangle [k]^\# D$
Example: Available expressions

- Recall: $\mathbb{D} = (\mathcal{P}^{\text{Expr}}, \supseteq)$
- Define: $(\rho, \mu) \triangle D$ iff $\forall e \in A. \llbracket e \rrbracket_\rho = \rho(T_e)$
- Prove: $A \supseteq A' \land (\rho, \mu) \triangle A \implies (\rho, \mu) \triangle A'$
- Prove: $(\rho, \mu) \triangle A \implies \llbracket a \rrbracket(\rho, \mu) = \llbracket \text{tr}(a, A) \rrbracket(\rho, \mu)$
  - where $\text{tr}(T_e = e, A) = \text{if } e \in A \text{ then } \text{Nop } \text{ else } T_e = e |$
  - $\text{tr}(a, A) = a$
  - Transformation in CFG: $(u, a, \nu) \mapsto (u, \text{tr}(a, A[u]), \nu)$
- Prove: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  - For AE, we have $d_0 = \emptyset$, which implies the above.
- Prove: $(\rho, \mu) \in \text{dom}[k] \land (\rho, \mu) \triangle D \implies \llbracket k \rrbracket(\rho, \mu) \triangle [k]D$
- Get: $\llbracket u \rrbracket \triangle \text{MOP}[u]$, thus $\llbracket u \rrbracket \triangle \text{MFP}[u]$
  - Which justifies correctness of transformation wrt. MFP
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
Example: Copy propagation

- $(\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)$
- $(\rho, \mu) \Delta C$ iff $\forall (x \rightarrow y) \in C. \; \rho(x) = \rho(y)$
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C \text{ iff } \forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \Delta C\) iff \(\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
Example: Copy propagation

• \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \sqsupseteq)\)
• \((\rho, \mu) \triangle C \text{ iff } \forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  • Monotonic for abstract values.
  • \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
  • \((\rho, \mu) \triangle C \implies [a](\rho, \mu) = [\text{tr}(a, C)](\rho, \mu)\)
    • Replace variables by equal variables
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C\) iff \(\forall (x \to y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
- \((\rho, \mu) \triangle C \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, C) \rrbracket (\rho, \mu)\)
  - Replace variables by equal variables
- \(d_0 = \emptyset\). Obviously \((\rho_0, \mu_0) \triangle \emptyset\) for all \(\rho_0, \mu_0\).
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C\) iff \(\forall (x \to y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
- \((\rho, \mu) \triangle C \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, C) \rrbracket (\rho, \mu)\)
  - Replace variables by equal variables
- \(d_0 = \emptyset\). Obviously \((\rho_0, \mu_0) \triangle \emptyset\) for all \(\rho_0, \mu_0\).
- Show \((\rho, \mu) \in \text{dom}\llbracket k \rrbracket \land (\rho, \mu) \triangle C \implies \llbracket k \rrbracket (\rho, \mu) \triangle \llbracket k \rrbracket \# C\)
Example: Copy propagation

- $\mathcal{D}, \sqsubseteq = (2^{\text{Reg} \times \text{Reg}}, \supseteq)$
- $(\rho, \mu) \triangle C$ iff $\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)$
  - Monotonic for abstract values.
  - $\text{tr}(a, C)$: Replace variables in expressions due to edges in $C$
- $(\rho, \mu) \triangle C \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, C) \rrbracket (\rho, \mu)$
  - Replace variables by equal variables
- $d_0 = \emptyset$. Obviously $(\rho_0, \mu_0) \triangle \emptyset$ for all $\rho_0, \mu_0$.
- Show $(\rho, \mu) \in \text{dom} [k] \land (\rho, \mu) \triangle C \implies \llbracket k \rrbracket (\rho, \mu) \triangle \llbracket k \rrbracket \# C$
  - Assume (IH) $\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)$
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C\) iff \(\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
- \((\rho, \mu) \triangle C \implies [a](\rho, \mu) = [\text{tr}(a, C)](\rho, \mu)\)
  - Replace variables by equal variables
- \(d_0 = \emptyset\). Obviously \((\rho_0, \mu_0) \triangle \emptyset\) for all \(\rho_0, \mu_0\).
- Show \((\rho, \mu) \in \text{dom} [k] \land (\rho, \mu) \triangle C \implies [k](\rho, \mu) \triangle [k] \# C\)
  - Assume (IH) \(\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Assume (1) \((\rho', \mu') = [k](\rho, \mu)\) and (2) \(x \rightarrow y \in [k] \# C\)
Example: Copy propagation

- \((D, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C\) iff \(\forall (x \rightarrow y) \in C. \, \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C)\): Replace variables in expressions due to edges in \(C\)
- \((\rho, \mu) \triangle C \Rightarrow \llbracket a \rrbracket(\rho, \mu) = \llbracket \text{tr}(a, C) \rrbracket(\rho, \mu)\)
  - Replace variables by equal variables
- \(d_0 = \emptyset.\) Obviously \((\rho_0, \mu_0) \triangle \emptyset\) for all \(\rho_0, \mu_0.\)
- Show \((\rho, \mu) \in \text{dom}[k] \land (\rho, \mu) \triangle C \Rightarrow [k](\rho, \mu) \triangle [k]^{\#} C\)
  - Assume (IH) \(\forall (x \rightarrow y) \in C. \, \rho(x) = \rho(y)\)
  - Assume (1) \((\rho', \mu') = [k](\rho, \mu)\) and (2) \(x \rightarrow y \in [k]^{\#} C\)
  - Show \(\rho'(x) = \rho'(y)\)
Example: Copy propagation

- \((\mathbb{D}, \sqsubseteq) = (2^{\text{Reg} \times \text{Reg}}, \supseteq)\)
- \((\rho, \mu) \triangle C\) iff \(\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Monotonic for abstract values.
  - \(\text{tr}(a, C):\) Replace variables in expressions due to edges in \(C\)
- \((\rho, \mu) \triangle C \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, C) \rrbracket (\rho, \mu)\)
  - Replace variables by equal variables
- \(d_0 = \emptyset.\) Obviously \((\rho_0, \mu_0) \triangle \emptyset\) for all \(\rho_0, \mu_0.\)
- Show \((\rho, \mu) \in \text{dom}[k] \land (\rho, \mu) \triangle C \implies \llbracket k \rrbracket (\rho, \mu) \triangle \llbracket k \rrbracket^\# C\)
  - Assume (IH) \(\forall (x \rightarrow y) \in C. \rho(x) = \rho(y)\)
  - Assume (1) \((\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)\) and (2) \(x \rightarrow y \in \llbracket k \rrbracket^\# C\)
  - Show \(\rho'(x) = \rho'(y)\)
  - By case distinction on \(k.\) On whiteboard.
Table of Contents

1 Introduction

2 Removing Superfluous Computations

3 Abstract Interpretation
   - Constant Propagation
   - Interval Analysis

4 Alias Analysis

5 Avoiding Redundancy (Part II)

6 Interprocedural Analysis

7 Analysis of Parallel Programs

8 Replacing Expensive by Cheaper Operations

9 Exploiting Hardware Features

10 Optimization of Functional Programs
Constant Propagation: Idea

- Compute constant values at compile time
- Eliminate unreachable code
Constant Propagation: Idea

- Compute constant values at compile time
- Eliminate unreachable code
Constant Propagation: Idea

- Compute constant values at compile time
- Eliminate unreachable code
Constant Propagation: Idea

- Compute constant values at compile time
- Eliminate unreachable code

- Dead-code elimination afterwards to clean up (assume y not interesting)
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^T$

```
    T
   / \  /
  -2  -1 0  1  2 ...
```

- Intuition: $T$ — don't know value of register
- $D = (\text{Reg} \to \mathbb{Z}^T) \cup \{\bot\}$
  - Add a bottom-element
  - Intuition: $\bot$ — program point not reachable

- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
- $(D, \sqsubseteq)$ is complete lattice

- Examples
  - $D[u] = \bot$: $u$ not reachable
  - $D[u] = \{x \mapsto T, y \mapsto 5\}$: $y$ is always 5 at $u$, nothing known about $x$
Approach

• Idea: Store, for each register, whether it is definitely constant at $u$
  • Assign each register a value from $\mathbb{Z}^T$
    \[
    \begin{align*}
    &\vdots & -2 & -1 & 0 & 1 & 2 & \cdots \\
    & & & T & & & & \\
    & & & & & & & \\
    \end{align*}
    \]
  • Intuition: $T$ — don’t know value of register

• $D[u] = \bot$: $u$ not reachable
• $D[u] = \{x \mapsto \top, y \mapsto 5\}$: $y$ is always 5 at $u$, nothing known about $x$
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^T$
    - Intuition: $\top$ — don’t know value of register
  - $D = (\text{Reg} \rightarrow \mathbb{Z}^T)$
Approach

- Idea: Store, for each register, whether it is definitely constant at \( u \)
  - Assign each register a value from \( \mathbb{Z}^T \)

\[
\begin{array}{c}
\top \\
\cdot \\
\cdot \\
\cdots \\
-2 \\
-1 \\
0 \\
1 \\
2 \\
\cdots \\
\end{array}
\]

- Intuition: \( \top \) — don’t know value of register
- \( \mathbb{D} = (\text{Reg} \to \mathbb{Z}^T) \cup \{ \bot \} \)
- Add a bottom-element
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^T$
  
  \[
  \begin{array}{cccccc}
    & & & & & \\
    & & & & & \\
    \Top & & & & & \\
    & & & & & \\
    \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\
  \end{array}
  \]

  - Intuition: $\Top$ — don’t know value of register

- $D = (\text{Reg} \rightarrow \mathbb{Z}^T) \cup \{\bot\}$
- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^\top$
    
    $$
    \begin{array}{cccc}
    \top & \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\
    \end{array}
    $$
  - Intuition: $\top$ — don’t know value of register
- $\mathbb{D} = (\text{Reg} \rightarrow \mathbb{Z}^\top) \cup \{\bot\}$
- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable
- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^\top$

  $\top \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad \cdots$

  - Intuition: $\top$ — don’t know value of register

- $\mathbb{D} = (\text{Reg} \to \mathbb{Z}^\top) \cup \{\bot\}$
- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable

- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
- $(\mathbb{D}, \sqsubseteq)$ is complete lattice
Approach

- **Idea:** Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^\top$
  - Intuition: $\top$ — don’t know value of register

- $\mathcal{D} = (\text{Reg} \rightarrow \mathbb{Z}^\top) \cup \{\bot\}$
- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable

- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
- $(\mathcal{D}, \sqsubseteq)$ is complete lattice

- **Examples**
Approach

- **Idea:** Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^T$

  \[
  \begin{array}{cccccc}
  & & & T & & \\
  & -2 & -1 & 0 & 1 & 2 \\
  & & & \cdots & & \cdots
  \end{array}
  \]

  - Intuition: $T$ — don’t know value of register

- $\mathcal{D} = (\text{Reg} \rightarrow \mathbb{Z}^T) \cup \{\bot\}$
- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable

- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
- $(\mathcal{D}, \sqsubseteq)$ is complete lattice

- **Examples**
  - $D[u] = \bot$: 

Approach

• Idea: Store, for each register, whether it is definitely constant at $u$
  • Assign each register a value from $\mathbb{Z}^T$

\[
\begin{array}{cccccc}
\cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\
\end{array}
\]

• Intuition: $\top$ — don’t know value of register

• $\mathcal{D} = (\text{Reg} \rightarrow \mathbb{Z}^T) \cup \{\bot\}$
  • Add a bottom-element
    • Intuition: $\bot$ — program point not reachable

• Ordering: Pointwise ordering on functions, $\bot$ being the least element.
  • $(\mathcal{D}, \sqsubseteq)$ is complete lattice

• Examples
  • $D[u] = \bot$: $u$ not reachable
Approach

- Idea: Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^\top$
    - Intuition: $\top$ — don’t know value of register
  - $D = (\text{Reg} \rightarrow \mathbb{Z}^\top) \cup \{\bot\}$
  - Add a bottom-element
    - Intuition: $\bot$ — program point not reachable
  - Ordering: Pointwise ordering on functions, $\bot$ being the least element.
    - $(D, \sqsubseteq)$ is complete lattice

- Examples
  - $D[u] = \bot$: $u$ not reachable
  - $D[u] = \{x \mapsto \top, y \mapsto 5\}$:
Approach

- **Idea:** Store, for each register, whether it is definitely constant at $u$
  - Assign each register a value from $\mathbb{Z}^\top$

  $$\begin{array}{c}
  \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \\
  {\top} & & & & & & \\
  \cdots & & & & & & \\
  \end{array}$$

  - Intuition: $\top$ — don’t know value of register

- $\mathbb{D} = (\text{Reg} \to \mathbb{Z}^\top) \cup \{\bot\}$

- Add a bottom-element
  - Intuition: $\bot$ — program point not reachable

- Ordering: Pointwise ordering on functions, $\bot$ being the least element.
  - $(\mathbb{D}, \sqsubseteq)$ is complete lattice

- **Examples**
  - $D[u] = \bot$: $u$ not reachable
  - $D[u] = \{x \mapsto \top, y \mapsto 5\}$: $y$ is always 5 at $u$, nothing known about $x$
Abstract evaluation of expressions

- For concrete operator $\Box : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, we define abstract operator $\Box^\# : \mathbb{Z}^\top \times \mathbb{Z}^\top \to \mathbb{Z}^\top$:

$$
\Box^\# \top x := \top \\
x \Box^\# \top := \top \\
x \Box^\# y := x \Box y
$$
Abstract evaluation of expressions

- For concrete operator $\Box : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, we define abstract operator $\Box^\# : \mathbb{Z}^\top \times \mathbb{Z}^\top \rightarrow \mathbb{Z}^\top$:

  $\top \Box^\# x := \top$
  $x \Box^\# \top := \top$
  $x \Box^\# y := x \Box y$

- Evaluate expression wrt. abstract values and operators:
  $\llbracket e \rrbracket^\# : \text{Reg} \rightarrow \mathbb{Z}^\top \rightarrow \mathbb{Z}^\top$

  $\llbracket c \rrbracket^\# D := c$ for constant $c$
  $\llbracket r \rrbracket^\# D := D(r)$ for register $r$
  $\llbracket e_1 \ Box e_2 \rrbracket^\# D := \llbracket e_1 \rrbracket^\# D \ Box^\# \llbracket e_2 \rrbracket^\# D$ for operator $\Box$
Abstract evaluation of expressions

- For concrete operator $\square : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, we define abstract operator $\square^# : \mathbb{Z}^\top \times \mathbb{Z}^\top \to \mathbb{Z}^\top$:

  $\top \square^# x := \top$

  $x \square^# \top := \top$

  $x \square^# y := x \square y$

- Evaluate expression wrt. abstract values and operators:

  $[[e]]^# : (\text{Reg} \to \mathbb{Z}^\top) \to \mathbb{Z}^\top$

  $[[c]]^# D := c$ for constant $c$

  $[[r]]^# D := D(r)$ for register $r$

  $[[e_1 \square e_2]]^# D := [[e_1]]^# D \square^# [[e_2]]^# D$ for operator $\square$

  Analogously for unary, ternary, etc. operators
Example

- Example: $D = \{ x \mapsto \top, y \mapsto 5 \}$
Example

- Example: $D = \{ x \mapsto \top, y \mapsto 5 \}$

\[
= 5 - 3
= 2
\]
Example

- Example: $D = \{x \mapsto \top, y \mapsto 5\}$

$$\begin{align*}
[y - 3]#D &= [y]#D - [3]#D \\
&= 5 - [3]#D \\
&= 5 - 3 \\
&= 2
\end{align*}$$

$$\begin{align*}
[x + y]#D &= [x]#D + [y]#D \\
&= \top + [5]#D \\
&= \top
\end{align*}$$
Abstract effects (forward)

\[
\llbracket k \rrbracket# \perp := \perp
\]

\[
\llbracket \text{Nop} \rrbracket# D := D
\]

\[
\llbracket \text{Pos}(e) \rrbracket# := \begin{cases} 
\perp & \text{if } \llbracket e \rrbracket# D = 0 \\
D & \text{otherwise}
\end{cases}
\]

\[
\llbracket \text{Neg}(e) \rrbracket# := \begin{cases} 
\perp & \text{if } \llbracket e \rrbracket# D = v, v \in \mathbb{Z} \setminus \{0\} \\
D & \text{otherwise}
\end{cases}
\]

\[
\llbracket r = e \rrbracket# D := D(r \mapsto \llbracket e \rrbracket# D)
\]

\[
\llbracket r = M[e] \rrbracket# D := D(r \mapsto \top)
\]

\[
\llbracket M[e_1] = e_2 \rrbracket# D := D
\]

For \( D \neq \perp \).
Abstract effects (forward)

\[
\begin{align*}
[k] \# \bot & := \bot \\
[Nop] \# D & := D \\
[\text{Pos}(e)] \# & := \begin{cases} 
\bot & \text{if } [e] \# D = 0 \\
D & \text{otherwise}
\end{cases} \\
[\text{Neg}(e)] \# & := \begin{cases} 
\bot & \text{if } [e] \# D = v, v \in \mathbb{Z} \setminus \{0\} \\
D & \text{otherwise}
\end{cases} \\
[r = e] \# D & := D(r \mapsto [e] \# D) \\
[r = M[e]] \# D & := D(r \mapsto \top) \\
[M[e_1] = e_2] \# D & := D
\end{align*}
\]

For \( D \neq \bot \).

Initial value at start: \( d_0 := \lambda x. \top \).
Abstract effects (forward)

\[ [k] \perp := \perp \]
for any edge \( k \)
\[ [\text{Nop}] D := D \]
\[ [\text{Pos}(e)] := \begin{cases} \perp & \text{if } [e] D = 0 \\ D & \text{otherwise} \end{cases} \]
\[ [\text{Neg}(e)] := \begin{cases} \perp & \text{if } [e] D = v, v \in \mathbb{Z} \setminus \{0\} \\ D & \text{otherwise} \end{cases} \]
\[ [r = e] D := D(r \mapsto [e] D) \]
\[ [r = M[e]] D := D(r \mapsto \top) \]
\[ [M[e_1] = e_2] D := D \]

For \( D \neq \perp \).

Initial value at start: \( d_0 := \lambda x. \top \).
(Reachable, all variables have unknown value)
Simulation based framework for program analysis

Abstract setting:
- Actions preserve relation $\Delta$ between concrete and abstract state.
  $\Rightarrow$ States after executing path are related
- Approximation: Complete lattice structure
  - $\Delta$ monotonic
  - Distributive $\Rightarrow$ generalization to sets of path

For program analysis:
- Concrete state: Sets of program states
  - All states reachable via path.

Constant propagation
Example

```
M[0] = 1

Pos(x-y) > 5
Neg(x-y) > 5
```

Transformations:
- Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\)
- \((u, r = e, v)\) if \([e] \# D[u] = c \in \mathbb{Z}\)
- Analogously for test, load, store

\((u, \text{Pos}(c), v)\) if \(c \in \mathbb{Z} \{0\}\)
\((u, \text{Neg}(0), v)\) if \(x = y\)
Example

$D[1] = x \mapsto \top, y \mapsto \top$

- $M[0] = 1$
- $y = 3$
- $x = y$
- $y = y + 2$
- $M[0] = 1$
- $y = 5$
- $y < 3$
- $x = y$
- $Pos(x - y) > 5$
- $Neg(x - y) > 5$
- $Neg(y < 3)$
- $Pos(y < 3)$
Example

D[1] = x \mapsto \top, y \mapsto \top
D[2] = x \mapsto \top, y \mapsto 3
Example

D[1] = x ⊸ T, y ⊸ T
D[2] = x ⊸ T, y ⊸ 3
D[3] = x ⊸ T, y ⊸ 3
Example

1. $y = 3$
2. $\text{Pos}(x-y) > 5$
3. $\text{Neg}(x-y) > 5$
4. $M[0] = 1$
5. $y = y + 2$
6. $y = 5$
7. $\text{Pos}(y < 3)$
8. $\text{Neg}(y < 3)$

$D[1] = x \mapsto T, y \mapsto T$
$D[2] = x \mapsto T, y \mapsto 3$
$D[3] = x \mapsto T, y \mapsto 3$
$D[4] = x \mapsto T, y \mapsto 3$
Example

1. \( y = 3 \)
2. \( \text{Pos}(x-y) > 5 \)
3. \( \text{Neg}(x-y) > 5 \)
4. \( y = y + 2 \)
5. \( M[0] = 1 \)
6. \( y = 5 \)
7. \( \text{Pos}(y < 3) \)
8. \( \text{Neg}(y < 3) \)

**Transformations:**

- Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\)
- \((u, r = e, v)\) map to \((u, r = c, v)\) if \([e] \# (D[u]) = c \in \mathbb{Z}\)

Analogously for test, load, store

- \((u, \text{Pos}(c), v)\) map to \(\text{Nop}\) if \(c \in \mathbb{Z}\) \(\{0\}\)
- \((u, \text{Neg}(0), v)\) map to \(\text{Nop}\)
Example

D[1] = x \mapsto T, y \mapsto T
D[2] = x \mapsto T, y \mapsto 3
D[3] = x \mapsto T, y \mapsto 3
D[4] = x \mapsto T, y \mapsto 3
D[5] = x \mapsto T, y \mapsto 3
D[6] = x \mapsto T, y \mapsto 5
Example

\[ y = 3 \]
\[ \text{Pos}(x - y) > 5 \]
\[ \text{Neg}(x - y) > 5 \]

\[ y = y + 2 \]
\[ M[0] = 1 \]
\[ y = 5 \]
\[ \text{Pos}(y < 3) \]
\[ \text{Neg}(y < 3) \]

\[ \text{D}[1] = x \mapsto T, y \mapsto T \]
\[ \text{D}[2] = x \mapsto T, y \mapsto 3 \]
\[ \text{D}[3] = x \mapsto T, y \mapsto 3 \]
\[ \text{D}[4] = x \mapsto T, y \mapsto 3 \]
\[ \text{D}[5] = x \mapsto T, y \mapsto 3 \]
\[ \text{D}[6] = x \mapsto T, y \mapsto 5 \]
\[ \text{D}[7] = \bot \]
Example

\[
\begin{align*}
D[1] &= x \mapsto T, y \mapsto T \\
D[2] &= x \mapsto T, y \mapsto 3 \\
D[3] &= x \mapsto T, y \mapsto 3 \\
D[4] &= x \mapsto T, y \mapsto 3 \\
D[5] &= x \mapsto T, y \mapsto 3 \\
D[6] &= x \mapsto T, y \mapsto 5 \\
D[7] &= \bot \\
D[8] &= x \mapsto T, y \mapsto 5
\end{align*}
\]
Example

\begin{align*}
D[1] & = x \mapsto \top, y \mapsto \top \\
D[2] & = x \mapsto \top, y \mapsto 3 \\
D[3] & = x \mapsto \top, y \mapsto 3 \\
D[4] & = x \mapsto \top, y \mapsto 3 \\
D[5] & = x \mapsto \top, y \mapsto 3 \\
D[6] & = x \mapsto \top, y \mapsto 5 \\
D[7] & = \perp \\
D[8] & = x \mapsto \top, y \mapsto 5
\end{align*}

Transformations:
Remove \((u, a, v)\) if \(D[u] = \perp\) or \(D[v] = \perp\)
Example


d\[1\] = \(x \mapsto \top, y \mapsto \top\)
d\[2\] = \(x \mapsto \top, y \mapsto 3\)
d\[3\] = \(x \mapsto \top, y \mapsto 3\)
d\[4\] = \(x \mapsto \top, y \mapsto 3\)
d\[5\] = \(x \mapsto \top, y \mapsto 3\)
d\[6\] = \(x \mapsto \top, y \mapsto 5\)
d\[7\] = \(\bot\)
d\[8\] = \(x \mapsto \top, y \mapsto 5\)

Transformations:

Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\)
\((u, r = e, v)\) \(\mapsto\) \((u, r = c, v)\) if \([e]^{\#}(D[u]) = c \in \mathbb{Z}\)
Example

\begin{align*}
D[1] &= x \mapsto \top, y \mapsto \top \\
D[2] &= x \mapsto \top, y \mapsto 3 \\
D[3] &= x \mapsto \top, y \mapsto 3 \\
D[4] &= x \mapsto \top, y \mapsto 3 \\
D[5] &= x \mapsto \top, y \mapsto 3 \\
D[6] &= x \mapsto \top, y \mapsto 5 \\
D[7] &= \bot \\
D[8] &= x \mapsto \top, y \mapsto 5
\end{align*}

Transformations:

- Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\)
- \((u, r = e, v)\) ⃗\(→\) \((u, r = c, v)\) if \(\llbracket e \rrbracket (D[u]) = c \in \mathbb{Z}\)
  Analogously for test, load, store
Example

\[
\begin{align*}
D[1] & = x \mapsto \top, y \mapsto \top \\
D[2] & = x \mapsto \top, y \mapsto 3 \\
D[3] & = x \mapsto \top, y \mapsto 3 \\
D[4] & = x \mapsto \top, y \mapsto 3 \\
D[5] & = x \mapsto \top, y \mapsto 3 \\
D[6] & = x \mapsto \top, y \mapsto 5 \\
D[7] & = \\nD[8] & = x \mapsto \top, y \mapsto 5
\end{align*}
\]

Transformations:

Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\)
\((u, r = e, v) \mapsto (u, r = c, v)\) if \([e]^{\#}(D[u]) = c \in \mathbb{Z}\)
Analogously for test, load, store
\((u, \text{Pos}(c), v) \mapsto \text{Nop} \text{ if } c \in \mathbb{Z} \setminus \{0\}\)
Example

\[
\begin{align*}
D[1] &= x \mapsto T, y \mapsto T \\
D[2] &= x \mapsto T, y \mapsto 3 \\
D[3] &= x \mapsto T, y \mapsto 3 \\
D[4] &= x \mapsto T, y \mapsto 3 \\
D[5] &= x \mapsto T, y \mapsto 3 \\
D[6] &= x \mapsto T, y \mapsto 5 \\
D[7] &= \bot \\
D[8] &= x \mapsto T, y \mapsto 5
\end{align*}
\]

Transformations:

Remove \((u, a, v)\) if \(D[u] = \bot\) or \(D[v] = \bot\) \\
\((u, r = e, v) \mapsto (u, r = c, v)\) if \([e] \# (D[u]) = c \in \mathbb{Z}\) \\
Analogously for test, load, store \\
\((u, \text{Pos}(c), v) \mapsto \text{Nop}\) if \(c \in \mathbb{Z} \setminus \{0\}\) \\
\((u, \text{Neg}(0), v) \mapsto \text{Nop}\)
Correctness (Description Relation)

- Establish description relation
  - Between values, valuations, states
Correctness (Description Relation)

- Establish description relation
  - Between values, valuations, states
- Values: for $\nu \in \mathbb{Z}$: $\nu \Delta \nu$ and $\nu \Delta \top$
  - Value described by same value, all values described by $\top$
- Note: Monotonic (Same point-wise definition as for $\sqsubseteq$)
- States: $(\rho, \mu) \Delta \rho \#$ if $\rho \Delta \rho \#$ and $\forall s. \neg(s \Delta \bot)$
  - Bottom describes no states (i.e., empty set of states)
  - Note: Monotonic. (Only new case: $s \Delta \bot \land \bot \sqsubseteq d = \Rightarrow s \Delta d$)
Correctness (Description Relation)

- Establish description relation
  - Between values, valuations, states
- Values: for $v \in \mathbb{Z}$: $v \Delta v$ and $v \Delta \top$
  - Value described by same value, all values described by $\top$
  - Note: Monotonic, i.e. $v \Delta d \land d \sqsubseteq d' \implies v \Delta d'$
    - Only cases: $d = d'$ or $d' = \top$ (flat ordering).
Correctness (Description Relation)

- Establish description relation
  - Between values, valuations, states
- Values: for $v \in \mathbb{Z}$: $v \Delta v$ and $v \Delta \top$
  - Value described by same value, all values described by $\top$
  - Note: Monotonic, i.e. $v \Delta d \land d \sqsubseteq d' \implies v \Delta d'$
    - Only cases: $d = d'$ or $d' = \top$ (flat ordering).
- Valuations: For $\rho: \text{Reg} \to \mathbb{Z}$, $\rho\#: \text{Reg} \to \mathbb{Z}^\top$: $\rho \Delta \rho\#$ iff $\forall x. \rho(x) \Delta \rho\#(x)$
  - Value of each variable must be described.
  - Note: Monotonic. (Same point-wise definition as for $\sqsubseteq$)
Correctness (Description Relation)

- Establish description relation
  - Between values, valuations, states
- Values: for $v \in \mathbb{Z}$: $v \Delta v$ and $v \Delta \top$
  - Value described by same value, all values described by $\top$
  - Note: Monotonic, i.e. $v \Delta d \land d \sqsubseteq d' \implies v \Delta d'$
    - Only cases: $d = d'$ or $d' = \top$ (flat ordering).
- Valuations: For $\rho : \text{Reg} \to \mathbb{Z}, \rho^\# : \text{Reg} \to \mathbb{Z}^\top$: $\rho \Delta \rho^\#$ iff $\forall x. \rho(x) \Delta \rho^\#(x)$
  - Value of each variable must be described.
  - Note: Monotonic. (Same point-wise definition as for $\sqsubseteq$)
- States: $(\rho, \mu) \Delta \rho^\#$ if $\rho \Delta \rho^\#$ and $\forall s. \neg(s \Delta \bot)$
  - Bottom describes no states (i.e., empty set of states)
  - Note: Monotonic. (Only new case: $s \Delta \bot \land \bot \sqsubseteq d \implies s \Delta d$)
Correctness (Abstract values)

- Show: For every constant \( c \) and operator \( \square \), we have

\[
c \triangle c^# \\
\nu_1 \triangle d_1 \land \nu_2 \triangle d_2 \implies (\nu_1 \boxdot \nu_2) \triangle (d_1 \boxdot d_2)
\]
Correctness (Abstract values)

• Show: For every constant $c$ and operator $\square$, we have

$$c \Delta c^\#$$

$$v_1 \Delta d_1 \land v_2 \Delta d_2 \implies (v_1 \square v_2) \Delta (d_1 \square^\# d_2)$$

• We get (by induction on expression)

$$\rho \Delta \rho^\# \implies \llbracket e \rrbracket \rho \Delta \llbracket e \rrbracket^\# \rho^\#$$
Correctness (Abstract values)

- Show: For every constant $c$ and operator $\Box$, we have
  \[ c \triangle c^\# \]
  \[ v_1 \triangle d_1 \land v_2 \triangle d_2 \implies (v_1 \Box v_2) \triangle (d_1 \Box^\# d_2) \]

- We get (by induction on expression)
  \[ \rho \triangle \rho^\# \implies [e] \rho \triangle [e]^\# \rho^\# \]

- Moreover, show $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  - Here: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle \lambda x. \top$
Correctness (Abstract values)

- Show: For every constant $c$ and operator $\Box$, we have
  \[
c \triangle c^\# 
  \]
  \[
v_1 \triangle d_1 \land v_2 \triangle d_2 \implies (v_1 \Box v_2) \triangle (d_1 \Box^\# d_2)
  \]

- We get (by induction on expression)
  \[
  \rho \triangle \rho^\# \implies [e] \rho \triangle [e]^\# \rho^#
  \]

- Moreover, show $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  
  - Here: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle \lambda x. \top$
  
  \[
  \iff \rho_0 \triangle \lambda x. \top
  \]

Holds by definition.
Correctness (Abstract values)

• Show: For every constant $c$ and operator $\Box$, we have

$$c \triangle c^\#$$

$$v_1 \triangle d_1 \land v_2 \triangle d_2 \implies (v_1 \Box v_2) \triangle (d_1 \Box^\# d_2)$$

• We get (by induction on expression)

$$\rho \triangle \rho^\# \implies \llbracket e \rrbracket \rho \triangle \llbracket e \rrbracket^\# \rho^\#$$

• Moreover, show $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle d_0$
  • Here: $\forall \rho_0, \mu_0. (\rho_0, \mu_0) \triangle \lambda x. \top$
    $$\iff \rho_0 \triangle \lambda x. \top$$
    $$\iff \forall x. \rho_0(x) \triangle \top. \text{Holds by definition.}$$
Correctness (Of Transformations)

- Assume $(\rho, \mu) \Delta \rho^\#$. Show $[a](\rho, \mu) = \mathsf{tr}(a, \rho^\#)(\rho, \mu)$

- Remove edge if $\rho^\# = \bot$. Trivial.

- Replace $r = e$ by $r = [e] \rho^\#$ if $[e] \rho^\# \neq \top$.

- From $\rho \Delta \rho^\# \Rightarrow [e] \rho \Delta [e] \rho^\# \Rightarrow [e] \rho = [e] \rho^#$.

- Analogously for expressions in load, store, Neg, Pos.

- Replace tests on constants by Nop: Obviously correct.

- Does not depend on analysis result.
Correctness (Of Transformations)

- Assume $(\rho, \mu) \triangleright \rho^\#$. Show $[a](\rho, \mu) = [\text{tr}(a, \rho^\#)](\rho, \mu)$
  - Remove edge if $\rho^\# = \bot$. Trivial.

- Analogously for expressions in load, store, Neg, Pos.

- Replace tests on constants by Nop: Obviously correct.
  - Does not depend on analysis result.
Correctness (Of Transformations)

• Assume \((\rho, \mu) \Delta \rho^\#\). Show \([a](\rho, \mu) = [\text{tr}(a, \rho^\#)](\rho, \mu)\)
  - Remove edge if \(\rho^\# = \bot\). Trivial.
  - Replace \(r = e\) by \(r = [e]^\# \rho^\#\) if \([e]^\# \rho^\# \neq \top\)
    - From \(\rho \Delta \rho^\# \implies [e]\rho \Delta [e]^\# \rho^\# \implies [e]\rho = [e]^\# \rho^\#\)

• Analogously for expressions in load, store, Neg, Pos.
• Replace tests on constants by \(\text{Nop}\): Obviously correct.
• Does not depend on analysis result.
Correctness (Of Transformations)

- Assume $(\rho, \mu) \Delta \rho^\#$. Show $[[a](\rho, \mu)] = [[\text{tr}(a, \rho^\#)]](\rho, \mu)$
  - Remove edge if $\rho^\# = \perp$. Trivial.
  - Replace $r = e$ by $r = [[e]^\# \rho^\#]$ if $[[e]^\# \rho^\#] \neq \top$
    - From $\rho \Delta \rho^\# \implies [[e] \rho \Delta [[e]^\# \rho^\#] \implies [[e] \rho = [[e]^\# \rho^\#$
    - Analogously for expressions in load, store, Neg, Pos.
Correctness (Of Transformations)

• Assume \((\rho, \mu) \Delta \rho^\#\). Show \([a](\rho, \mu) = [\text{tr}(a, \rho^\#)](\rho, \mu)\)
  - Remove edge if \(\rho^\# = \bot\). Trivial.
  - Replace \(r = e\) by \(r = \lceil e \rceil^\#_\rho^\#\) if \(\lceil e \rceil^\#_\rho^\# \neq T\)
    • From \(\rho \Delta \rho^\# \Rightarrow \lceil e \rceil_\rho \Delta \lceil e \rceil^\#_\rho^\# \Rightarrow \lceil e \rceil_\rho = \lceil e \rceil^\#_\rho^\#\)
    • Analogously for expressions in load, store, Neg, Pos.
  - Replace tests on constants by \(\text{Nop}\): Obviously correct.
    • Does not depend on analysis result.
Correctness (Steps)

• Assume $(\rho', \mu') = [k](\rho, \mu)$ and $(\rho, \mu) \Delta C$. Show $(\rho', \mu') \Delta [k] \# C.$
Correctness (Steps)

• Assume \((\rho', \mu') = [k](\rho, \mu)\) and \((\rho, \mu) \Delta C\). Show \((\rho', \mu') \Delta [k]^\# C\).
  • By case distinction on \(k\). Assume \(\rho^\# := C \neq \bot\).
    • Note: We have \(\rho \Delta \rho^\#\)
Correctness (Steps)

- Assume $(\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)$ and $(\rho, \mu) \triangle C$. Show $(\rho', \mu') \triangle \llbracket k \rrbracket^\# C$.
  - By case distinction on $k$. Assume $\rho^\# := C \neq \bot$.
    - Note: We have $\rho \triangle \rho^\#$
  - Case $k = (u, x = e, v)$: To show $\rho(x := \llbracket e \rrbracket \rho) \triangle \rho^\#(x := \llbracket e \rrbracket^\# \rho^\#)$
Correctness (Steps)

- Assume \((\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)\) and \((\rho, \mu) \triangle C\). Show \((\rho', \mu') \triangle \llbracket k \rrbracket^\#C\).
  - By case distinction on \(k\). Assume \(\rho^\# := C \neq \bot\).
    - Note: We have \(\rho \triangle \rho^\#\)
  - Case \(k = (u, x = e, v)\): To show \(\rho(x := e[\rho]) \triangle \rho^\#(x := e[\rho^\#])\)
    \[\iff\] \(e[\rho] \triangle e[\rho^\#] \triangle \rho^\#.\) Already proved.
Correctness (Steps)

- Assume \((\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)\) and \((\rho, \mu) \triangleq C\). Show \((\rho', \mu') \triangleq \llbracket k \rrbracket \# C\).
  - By case distinction on \(k\). Assume \(\rho\# := C \neq \bot\).
    - Note: We have \(\rho \triangleq \rho\#\)
  - Case \(k = (u, x = e, v)\): To show \(\rho(x := \llbracket e \rrbracket \rho) \triangleq \rho\#(x := \llbracket e \rrbracket \# \rho\#)\)
    \[\iff \llbracket e \rrbracket \rho \triangleq \llbracket e \rrbracket \# \rho\#. \text{Already proved.}\]
  - Case \(k = (u, \text{Pos}(e), v)\) and \(\llbracket e \rrbracket \# \rho\# = 0\):
Correctness (Steps)

- Assume \((\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)\) and \((\rho, \mu) \not\Delta C\). Show \((\rho', \mu') \not\Delta \llbracket k \rrbracket^\# C\).
  - By case distinction on \(k\). Assume \(\rho^\# := C \neq \bot\).
    - Note: We have \(\rho \not\Delta \rho^\#\)
  - Case \(k = (u, x = e, v)\): To show \(\rho(x := \llbracket e \rrbracket \rho) \not\Delta \rho^\#(x := \llbracket e \rrbracket^\# \rho^\#)\)
    \(\iff\) \(\llbracket e \rrbracket \rho \not\Delta \llbracket e \rrbracket^\# \rho^\#.\) Already proved.
  - Case \(k = (u, \text{Pos}(e), v)\) and \(\llbracket e \rrbracket^\# \rho^# = 0\):
    - From \(\llbracket e \rrbracket \rho \not\Delta \llbracket e \rrbracket^\# \rho^#\), we have \(\llbracket e \rrbracket \rho = 0\)
Correctness (Steps)

• Assume \((\rho', \mu') = \llbracket k \rrbracket(\rho, \mu)\) and \((\rho, \mu) \Delta C\). Show \((\rho', \mu') \Delta \llbracket k \rrbracket^\# C\).
  • By case distinction on \(k\). Assume \(\rho^\# := C \neq \bot\).
    • Note: We have \(\rho \Delta \rho^\#\)
  • Case \(k = (u, x = e, v)\): To show \(\rho(x := \llbracket e \rrbracket \rho) \Delta \rho^\#(x := \llbracket e^\# \rrbracket \rho^\#)\)
    \(\leftarrow \llbracket e \rrbracket \rho \Delta \llbracket e^\# \rrbracket \rho^\#.\) Already proved.
  • Case \(k = (u, \text{Pos}(e), v)\) and \(\llbracket e^\# \rrbracket \rho^\# = 0\):
    • From \(\llbracket e \rrbracket \rho \Delta \llbracket e^\# \rrbracket \rho^\#,\) we have \(\llbracket e \rrbracket \rho = 0\)
    • Hence, \(\llbracket \text{Pos}(e) \rrbracket(\rho, \mu) = \text{undefined}.\) Contradiction to assumption.
Correctness (Steps)

• Assume \((\rho', \mu') = [k](\rho, \mu)\) and \((\rho, \mu) \triangle C\). Show \((\rho', \mu') \triangle [k]^\# C\).
  • By case distinction on \(k\). Assume \(\rho^\# := C \neq \perp\).
    • Note: We have \(\rho \triangle \rho^\#\)
  • Case \(k = (u, x = e, v)\): To show \(\rho(x := [e]\rho) \triangle \rho^\#(x := [e]^\# \rho^\#)\)
      \(\iff [e]\rho \triangle [e]^\# \rho^\#.\) Already proved.
  • Case \(k = (u, \text{Pos}(e), v)\) and \([e]^\# \rho^\# = 0\):
    • From \([e]\rho \triangle [e]^\# \rho^\#,\) we have \([e]\rho = 0\)
    • Hence, \([\text{Pos}(e)](\rho, \mu) = \text{undefined.}\) Contradiction to assumption.
• Other cases: Analogously.
Correctness (Steps)

- Assume \((\rho', \mu') = \llbracket k \rrbracket (\rho, \mu)\) and \((\rho, \mu) \Delta C\). Show \((\rho', \mu') \Delta \llbracket k \rrbracket^# C\).
  - By case distinction on \(k\). Assume \(\rho^# := C \neq \bot\).
    - Note: We have \(\rho \Delta \rho^#\)
  - Case \(k = (u, x = e, v)\): To show \(\rho(x := \llbracket e \rrbracket \rho) \Delta \rho^# (x := \llbracket e \rrbracket^# \rho^#)\)
    \(\iff \llbracket e \rrbracket \rho \Delta \llbracket e \rrbracket^# \rho^#. \) Already proved.
  - Case \(k = (u, \text{Pos}(e), v)\) and \(\llbracket e \rrbracket^# \rho^# = 0\):
    - From \(\llbracket e \rrbracket \rho \Delta \llbracket e \rrbracket^# \rho^#\), we have \(\llbracket e \rrbracket \rho = 0\)
    - Hence, \(\llbracket \text{Pos}(e) \rrbracket(\rho, \mu) = \text{undefined}. \) Contradiction to assumption.
  - Other cases: Analogously.

- Our general theory gives us: \(\llbracket u \rrbracket \Delta \text{MFP}[u]\)
  - Thus, transformation wrt. MFP is correct.
Constant propagation: Caveat

- Abstract effects are monotonic
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**

\[
\rho_1 = \{ x \mapsto 3, \ y \mapsto 2 \} \\
\rho_2 = \{ x \mapsto 2, \ y \mapsto 3 \}
\]

- Have:
  \[
  \rho_1 \sqcup \rho_2 = \{ x \mapsto \top, \ y \mapsto \top \}
  \]
  - I.e.:
    \[
    [ [ x = x + y ] ] (\rho_1 \sqcup \rho_2) = \{ x \mapsto \top, \ y \mapsto \top \}
    \]
  - However:
    \[
    [ [ x = x + y ] ] \rho_1 = \{ x \mapsto 5, \ y \mapsto 2 \}
    \]
    and
    \[
    [ [ x = x + y ] ] \rho_2 = \{ x \mapsto 5, \ y \mapsto 3 \}
    \]
    - I.e.:
      \[
      [ [ x = x + y ] ] (\rho_1 \sqcup [ [ x = x + y ] ] \rho_2) = \{ x \mapsto 5, \ y \mapsto \top \}
      \]

Thus, \textit{MFP} only approximation of \textit{MOP} in general.
Constant propagation: Caveat

- Abstract effects are monotonic
- Unfortunately: Not distributive
  - Consider $\rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \}$ and $\rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \}$
Constant propagation: Caveat

- Abstract effects are monotonic
- Unfortunately: Not distributive
  - Consider \( \rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \} \) and \( \rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \} \)
  - Have: \( \rho_1^\# \sqcup \rho_2^\# = \)

Thus, MFP only approximation of MOP in general.
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider $\rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \}$ and $\rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \}$
  - Have: $\rho_1^\# \sqcup \rho_2^\# = \{ x \mapsto \top, y \mapsto \top \}$
• Abstract effects are **monotonic**
• Unfortunately: **Not distributive**
  • Consider $\rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \}$ and $\rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \}$
  • Have: $\rho_1^\# \sqcup \rho_2^\# = \{ x \mapsto \top, y \mapsto \top \}$
  • I.e.: $\llbracket x = x + y \rrbracket^\# (\rho_1^\# \sqcup \rho_2^\#) =$

Constant propagation: Caveat
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider \( \rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \} \) and \( \rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \} \)
  - Have: \( \rho_1^\# \sqcup \rho_2^\# = \{ x \mapsto \top, y \mapsto \top \} \)
  - I.e.: \( [x = x + y]^\# (\rho_1^\# \sqcup \rho_2^\#) = \{ x \mapsto \top, y \mapsto \top \} \)
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider $\rho_1^\# = \{x \mapsto 3, y \mapsto 2\}$ and $\rho_2^\# = \{x \mapsto 2, y \mapsto 3\}$
  - Have: $\rho_1^\# \sqcup \rho_2^\# = \{x \mapsto \top, y \mapsto \top\}$
  - I.e.: $[x = x + y]^\#(\rho_1^\# \sqcup \rho_2^\#) = \{x \mapsto \top, y \mapsto \top\}$
  - However: $[x = x + y]^\#(\rho_1^\#) =$ and $[x = x + y]^\#(\rho_2^\#) =$
Constant propagation: Caveat

- Abstract effects are monotonic
- Unfortunately: Not distributive
  - Consider \( \rho_1^* = \{ x \mapsto 3, y \mapsto 2 \} \) and \( \rho_2^* = \{ x \mapsto 2, y \mapsto 3 \} \)
  - Have: \( \rho_1^* \sqcup \rho_2^* = \{ x \mapsto \top, y \mapsto \top \} \)
  - I.e.: \( \left[ x = x + y \right]^* (\rho_1^* \sqcup \rho_2^*) = \{ x \mapsto \top, y \mapsto \top \} \)
  - However: \( \left[ x = x + y \right]^* (\rho_1^*) = \{ x \mapsto 5, y \mapsto 2 \} \) and \( \left[ x = x + y \right]^* (\rho_2^*) = \)
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider \( \rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \} \) and \( \rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \} \)
  - Have: \( \rho_1^\# \sqcup \rho_2^\# = \{ x \mapsto \top, y \mapsto \top \} \)
  - I.e.: \( [x = x + y]^\#(\rho_1^\# \sqcup \rho_2^\#) = \{ x \mapsto \top, y \mapsto \top \} \)
  - However:
    - \( [x = x + y]^\#(\rho_1^\#) = \{ x \mapsto 5, y \mapsto 2 \} \) and \( [x = x + y]^\#(\rho_2^\#) = \{ x \mapsto 5, y \mapsto 3 \} \)
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider $\rho_1^# = \{ x \mapsto 3, y \mapsto 2 \}$ and $\rho_2^# = \{ x \mapsto 2, y \mapsto 3 \}$
  - Have: $\rho_1^# \sqcup \rho_2^# = \{ x \mapsto \top, y \mapsto \top \}$
  - I.e.: $\llbracket x = x + y \rrbracket^{\#} (\rho_1^# \sqcup \rho_2^#) = \{ x \mapsto \top, y \mapsto \top \}$
  - However: $\llbracket x = x + y \rrbracket^{\#} (\rho_1^#) = \{ x \mapsto 5, y \mapsto 2 \}$ and $\llbracket x = x + y \rrbracket^{\#} (\rho_2^#) = \{ x \mapsto 5, y \mapsto 3 \}$
  - I.e.: $\llbracket x = x + y \rrbracket^{\#} (\rho_1^#) \sqcup \llbracket x = x + y \rrbracket^{\#} (\rho_2^#) =$
Constant propagation: Caveat

- Abstract effects are **monotonic**
- Unfortunately: **Not distributive**
  - Consider $\rho_1^\# = \{ x \mapsto 3, y \mapsto 2 \}$ and $\rho_2^\# = \{ x \mapsto 2, y \mapsto 3 \}$
  - Have: $\rho_1^\# \sqcup \rho_2^\# = \{ x \mapsto \top, y \mapsto \top \}$
  - I.e.: $\llbracket x = x + y \rrbracket^\#(\rho_1^\# \sqcup \rho_2^\#) = \{ x \mapsto \top, y \mapsto \top \}$
  - However: $\llbracket x = x + y \rrbracket^\#(\rho_1^\#) = \{ x \mapsto 5, y \mapsto 2 \}$ and $\llbracket x = x + y \rrbracket^\#(\rho_2^\#) = \{ x \mapsto 5, y \mapsto 3 \}$
  - I.e.: $\llbracket x = x + y \rrbracket^\#(\rho_1^\#) \sqcup \llbracket x = x + y \rrbracket^\#(\rho_2^\#) = \{ x \mapsto 5, y \mapsto \top \}$

Thus, $MFP$ only an approximation of $MOP$ in general.
• Abstract effects are monotonic
• Unfortunately: Not distributive
  • Consider $\rho_1^# = \{x \mapsto 3, y \mapsto 2\}$ and $\rho_2^# = \{x \mapsto 2, y \mapsto 3\}$
  • Have: $\rho_1^# \sqcup \rho_2^# = \{x \mapsto \top, y \mapsto \top\}$
  • I.e.: $\llbracket x = x + y \rrbracket^#(\rho_1^# \sqcup \rho_2^#) = \{x \mapsto \top, y \mapsto \top\}$
  • However: $\llbracket x = x + y \rrbracket^#(\rho_1^#) = \{x \mapsto 5, y \mapsto 2\}$ and
    $\llbracket x = x + y \rrbracket^#(\rho_2^#) = \{x \mapsto 5, y \mapsto 3\}$
  • I.e.: $\llbracket x = x + y \rrbracket^#(\rho_1^#) \sqcup \llbracket x = x + y \rrbracket^#(\rho_2^#) = \{x \mapsto 5, y \mapsto \top\}$
• Thus, MFP only approximation of MOP in general.
Undecidability of MOP

- MFP only approximation of MOP

Theorem
For constant propagation, it is undecidable whether $MOP(u(x)) = \top$.

Proof: By undecidability of Hilbert's 10th problem
Undecidability of MOP

- MFP only approximation of MOP
- And there is nothing we can do about :(

**Theorem**

*For constant propagation, it is undecidable whether $MOP[u](x) = \top$.***
Undecidability of MOP

- MFP only approximation of MOP
- And there is nothing we can do about :(

**Theorem**

*For constant propagation, it is undecidable whether $\text{MOP}[u](x) = \top$.*

- Proof: By undecidability of Hilbert’s 10th problem
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation

\[ p(x_1, \ldots, x_n) = 0 \]
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation
  \[ p(x_1, \ldots, x_n) = 0 \]
- Where \( p \) is a polynomial with integer coefficients.
  - E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
Hilbert’s 10th problem (1900)

• Find an integer solution of a Diophantine equation
  \[ p(x_1, \ldots, x_n) = 0 \]

• Where \( p \) is a polynomial with integer coefficients.
  • E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
  • Solution:
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation

\[ p(x_1, \ldots, x_n) = 0 \]

- Where \( p \) is a polynomial with integer coefficients.
  - E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
  - Solution: \((-1,1)\)
Hilbert’s 10th problem (1900)

• Find an integer solution of a Diophantine equation

\[ p(x_1, \ldots, x_n) = 0 \]

• Where \( p \) is a polynomial with integer coefficients.
  • E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
  • Solution: (-1,1)

• Hard problem. E.g. \( x^n + y^n = z^n \) for \( n > 2 \).
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation
  \[ p(x_1, \ldots, x_n) = 0 \]
  - Where \( p \) is a polynomial with integer coefficients.
    - E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
    - Solution: \((-1,1)\)
  - Hard problem. E.g. \( x^n + y^n = z^n \) for \( n > 2 \). (Fermat’s last Theorem)
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation

\[ p(x_1, \ldots, x_n) = 0 \]

- Where \( p \) is a polynomial with integer coefficients.
  - E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
  - Solution: (-1,1)

- Hard problem. E.g. \( x^n + y^n = z^n \) for \( n > 2 \). (Fermat’s last Theorem)
  - Wiles, Taylor: No solutions.
Hilbert’s 10th problem (1900)

- Find an integer solution of a Diophantine equation
  \[ p(x_1, \ldots, x_n) = 0 \]

- Where \( p \) is a polynomial with integer coefficients.
  - E.g. \( p(x_1, x_2) = x_1^2 + 2x_1 - x_2^2 + 2 \)
  - Solution: \((-1,1)\)

- Hard problem. E.g. \( x^n + y^n = z^n \) for \( n > 2 \). (Fermat’s last Theorem)
  - Wiles, Taylor: No solutions.

**Theorem (Matiyasevich, 1970)**

*(Based on work of David, Putnam, Robinson)*

*It is undecidable whether a Diophantine equation has an integer solution.*
Regard the following program

\[ x_1 = x_2 = \ldots = x_n = 0 \]

while (*) { \( x_1 = x_1 + 1 \) }

\[ \ldots \]

while (*) { \( x_n = x_n + 1 \) }

r=0

if (\( p(x_1, \ldots, x_n) = 0 \)) then r=1

u: Nop

- For any valuation of the variables, there is a path through the program
Regard the following program

\[ x_1 = x_2 = \ldots x_n = 0 \]
while (*) { \( x_1 = x_1 + 1 \) }
...
while (*) { \( x_n = x_n + 1 \) }

r=0
if (p(x_1, \ldots, x_n) == 0) then r=1

u: Nop

- For any valuation of the variables, there is a path through the program
- For every path, constant propagation computes the values of the \( x_i \)
Regard the following program

\[ x_1 = x_2 = \ldots x_n = 0 \]
while (\(*\)) { \( x_1 = x_1 + 1 \) }
\[ \ldots \]
while (\(*\)) { \( x_n = x_n + 1 \) }
\[ r = 0 \]
if (\( p(x_1, \ldots, x_n) == 0 \)) then \( r = 1 \)
u: Nop

- For any valuation of the variables, there is a path through the program
- For every path, constant propagation computes the values of the \( x_i \)
- And gets a precise value for \( p(x_1, \ldots, x_n) \)
Regard the following program

\[ x_1 = x_2 = \ldots x_n = 0 \]

while (*) { \( x_1 = x_1 + 1 \) }

... 

while (*) { \( x_n = x_n + 1 \) }

\( r = 0 \)

if (\( p(x_1, \ldots, x_n) == 0 \)) then \( r = 1 \)

\( u: \text{Nop} \)

- For any valuation of the variables, there is a path through the program
- For every path, constant propagation computes the values of the \( x_i \)
- And gets a precise value for \( p(x_1, \ldots, x_n) \)
- \( r \) is only found to be non-constant, if \( p(x_1, \ldots, x_n) = 0 \)
Regard the following program

\[
x_1 = x_2 = \ldots x_n = 0\\
\text{while } (* \text{) } \{ x_1 = x_1 + 1 \} \\
\ldots \\
\text{while } (*) \{ x_n = x_n + 1 \} \\
r = 0 \\
\text{if } (p(x_1, \ldots, x_n) == 0) \text{ then } r = 1 \\
u: \text{Nop}
\]

- For any valuation of the variables, there is a path through the program
- For every path, constant propagation computes the values of the \( x_i \)
- And gets a precise value for \( p(x_1, \ldots, x_n) \)
- \( r \) is only found to be non-constant, if \( p(x_1, \ldots, x_n) = 0 \)
- Thus, \( \text{MOP}[u](r) = \top \) if, and only if \( p(x_1, \ldots, x_n) = 0 \) has a solution
Extensions

- Also simplify subexpressions:
  - For \( \{ x \mapsto \top, y \mapsto 3 \} \), replace \( x + 2 \times y \) by \( x + 6 \).
Extensions

- Also simplify subexpressions:
  - For \( \{x \mapsto \top, y \mapsto 3\} \), replace \( x + 2 \times y \) by \( x + 6 \).
- Apply further arithmetic simplifications
  - E.g. \( x \times 0 \rightarrow 0 \), \( x \times 1 \rightarrow x \), ...
Extensions

- Also simplify subexpressions:
  - For \( \{ x \mapsto \top, y \mapsto 3 \} \), replace \( x + 2 * y \) by \( x + 6 \).
- Apply further arithmetic simplifications
  - E.g. \( x * 0 \to 0, x * 1 \to x \), \ldots
- Exploit equalities in conditions
  - \textbf{if} (x==4) M[0]=x+1 \textbf{else} M[0]=x \to
Extensions

- Also simplify subexpressions:
  - For \( \{ x \mapsto \top, y \mapsto 3 \} \), replace \( x + 2 \times y \) by \( x + 6 \).
- Apply further arithmetic simplifications
  - E.g. \( x \times 0 \rightarrow 0, x \times 1 \rightarrow x \) ...
- Exploit equalities in conditions
  - \( \text{if} \ (x==4) \ M[0]=x+1 \ \text{else} \ M[0]=x \ \rightarrow \)
    \( \text{if} \ (x==4) \ M[0]=5 \ \text{else} \ M[0]=x \)
Extensions

- Also simplify subexpressions:
  - For \( \{ x \mapsto \top, y \mapsto 3 \} \), replace \( x + 2 \times y \) by \( x + 6 \).
- Apply further arithmetic simplifications
  - E.g. \( x \times 0 \rightarrow 0, x \times 1 \rightarrow x, \ldots \)
- Exploit equalities in conditions
  - \( \text{if } (x==4) M[0]=x+1 \text{ else } M[0]=x \rightarrow \)
    \( \text{if } (x==4) M[0]=5 \text{ else } M[0]=x \)
  - Use

\[
\llbracket \text{Pos}(x == e) \rrbracket^\# = \begin{cases} 
D & \text{if } \llbracket x == e \rrbracket^\# D = 1 \\
\perp & \text{if } \llbracket x == e \rrbracket^\# D = 0 \\
D_1 & \text{otherwise}
\end{cases}
\]

where \( D_1 := D(x := D(x) \sqcap \llbracket e \rrbracket^\# D) \)
Extensions

- Also simplify subexpressions:
  - For \( \{ x \mapsto \top, y \mapsto 3 \} \), replace \( x + 2 \times y \) by \( x + 6 \).
- Apply further arithmetic simplifications
  - E.g. \( x \times 0 \rightarrow 0 \), \( x \times 1 \rightarrow x \), ...
- Exploit equalities in conditions
  - if \((x==4)\) \( M[0]=x+1 \) else \( M[0]=x \) \( \rightarrow \)
    if \((x==4)\) \( M[0]=5 \) else \( M[0]=x \)
  - Use

\[
\llbracket \text{Pos}(x == e) \rrbracket^\# = \begin{cases} 
D & \text{if } \llbracket x == e \rrbracket^\# D = 1 \\
\bot & \text{if } \llbracket x == e \rrbracket^\# D = 0 \\
D_1 & \text{otherwise}
\end{cases}
\]

where \( D_1 := D(x := D(x) \cap \llbracket e \rrbracket^\# D) \)

- Analogously for \( \text{Neg}(x \neq e) \)
Table of Contents

1 Introduction

2 Removing Superfluous Computations

3 Abstract Interpretation
   - Constant Propagation
   - Interval Analysis

4 Alias Analysis

5 Avoiding Redundancy (Part II)

6 Interprocedural Analysis

7 Analysis of Parallel Programs

8 Replacing Expensive by Cheaper Operations

9 Exploiting Hardware Features

10 Optimization of Functional Programs
Interval Analysis

- Constant propagation finds constants
- But sometimes, we can restrict the value of a variable to an interval, e.g., [0..42].
Example

```c
int a[42];
for (i=0; i<42; ++i) {
    if (0<=i && i<42)
        a[i] = i*2;
    else
        fail();
```

- Array access with bounds check
**Example**

```c
int a[42];
for (i=0;i<42;++i) {
    if (0<=i && i<42)
        a[i] = i*2;
    else
        fail();
}

- Array access with bounds check
- From the for-loop, we know \( i \in [0..41] \)
```c
int a[42];
for (i=0;i<42;++i) {
  if (0<=i && i<42)
    a[i] = i*2;
  else
    fail();
```

- Array access with bounds check
- From the for-loop, we know $i \in [0..41]$
- Thus, bounds check not necessary
Intervals

Interval $\mathbb{I} := \{[l, u] \mid l \in \mathbb{Z}^{-\infty} \land u \in \mathbb{Z}^{+\infty} \land l \leq u\}$
Intervals

Interval $\mathbb{I} := \{[l, u] | l \in \mathbb{Z}^{-\infty} \land u \in \mathbb{Z}^{+\infty} \land l \leq u\}$

Ordering $\subseteq$, i.e. $[l_1, u_1] \subseteq [l_2, u_2]$ iff $l_1 \geq l_2 \land u_1 \leq u_2$

- Smaller interval contained in larger one
- Hence:

$$[l_1, u_1] \sqcup [l_2, u_2] = [\min(l_1, l_2), \max(u_1, u_2)]$$

$\top = [-\infty, +\infty]$
Intervals

**Interval** \( \mathbb{I} := \{[l, u] \mid l \in \mathbb{Z}^{-\infty} \land u \in \mathbb{Z}^{+\infty} \land l \leq u\} \)

**Ordering** \( \subseteq \), i.e. \([l_1, u_1] \subseteq [l_2, u_2]\) iff \( l_1 \geq l_2 \land u_1 \leq u_2 \)

- Smaller interval contained in larger one
- Hence:

\[
[l_1, u_1] \sqcup [l_2, u_2] = [\min(l_1, l_2), \max(u_1, u_2)]
\]

\( T = [-\infty, +\infty] \)

Problems
Intervals

Interval \( \mathbb{I} := \{ [l, u] \mid l \in \mathbb{Z}^{-\infty} \land u \in \mathbb{Z}^{+\infty} \land l \leq u \} \)

Ordering \( \subseteq \), i.e. \( [l_1, u_1] \subseteq [l_2, u_2] \) iff \( l_1 \geq l_2 \land u_1 \leq u_2 \)

- Smaller interval contained in larger one
- Hence:

\[
[l_1, u_1] \cup [l_2, u_2] = [\min(l_1, l_2), \max(u_1, u_2)]
\]

\( \top = [-\infty, +\infty] \)

Problems

- Not a complete lattice. (Will add \( \bot \) - element later)
Intervals

Interval \( \mathbb{I} := \{[l, u] \mid l \in \mathbb{Z}^{-\infty} \land u \in \mathbb{Z}^{+\infty} \land l \leq u\} \)

Ordering \( \subseteq \), i.e. \([l_1, u_1] \subseteq [l_2, u_2]\) iff \(l_1 \geq l_2 \land u_1 \leq u_2\)
  
  - Smaller interval contained in larger one
  - Hence:

\[
[l_1, u_1] \cup [l_2, u_2] = [\min(l_1, l_2), \max(u_1, u_2)]
\]

\(\top = [\infty, +\infty]\)

Problems
  
  - Not a complete lattice. (Will add \(\bot\) - element later)
  - Infinite ascending chains: \([0, 0] \sqsubset [0, 1] \sqsubset [0, 2] \sqsubset \ldots\)
Building the Domain

• Analogously to CP:
  • $\mathbb{D} := (\text{Reg} \rightarrow \mathbb{I}) \cup \{\bot\}$
  • Intuition: Map variables to intervals their value must be contained in.
  • $\bot$ — unreachable

\[I \triangleq \mathbb{D}\]
Building the Domain

- Analogously to CP:
  - $\mathbb{D} := (\text{Reg} \to \mathbb{I}) \cup \{\perp\}$
  - Intuition: Map variables to intervals their value **must** be contained in.
  - $\perp$ — unreachable
- Description relation:
Building the Domain

• Analogously to CP:
  • \( \mathbb{D} := (\text{Reg} \rightarrow \mathbb{I}) \cup \{ \perp \} \)
  • Intuition: Map variables to intervals their value \textit{must} be contained in.
  • \( \perp \) — unreachable

• Description relation:
  • On values: \( z \Delta [l, u] \text{ iff } l \leq z \leq u \)
Building the Domain

- Analogously to CP:
  - \( \mathbb{D} := (\text{Reg} \rightarrow \mathbb{I}) \cup \{\perp\} \)
  - Intuition: Map variables to intervals their value must be contained in.
  - \( \perp \) — unreachable

- Description relation:
  - On values: \( z \Delta [l, u] \text{ iff } l \leq z \leq u \)
  - On register valuations: \( \rho \Delta \rho^\# \text{ iff } \forall x. \rho(x) \Delta \rho^\#(x) \)
Building the Domain

- Analogously to CP:
  - \( \mathbb{D} := (\text{Reg} \to \mathbb{I}) \cup \{\bot\} \)
  - Intuition: Map variables to intervals their value must be contained in.
  - \( \bot \) — unreachable

- Description relation:
  - On values: \( z \Delta [l, u] \) iff \( l \leq z \leq u \)
  - On register valuations: \( \rho \Delta \rho^\# \) iff \( \forall x. \rho(x) \Delta \rho^\#(x) \)
  - On configurations: \( (\rho, \mu) \Delta l \) iff \( \rho \Delta l \) and \( l \neq \bot \)

Obviously monotonic. (Larger interval admits more values)
Building the Domain

- Analogously to CP:
  - \( \mathbb{D} := (\text{Reg} \rightarrow \mathbb{I}) \cup \{ \perp \} \)
  - Intuition: Map variables to intervals their value must be contained in.
  - \( \perp \) — unreachable

- Description relation:
  - On values: \( z \Delta [l, u] \text{ iff } l \leq z \leq u \)
  - On register valuations: \( \rho \Delta \rho^\# \text{ iff } \forall x.\rho(x) \Delta \rho^\#(x) \)
  - On configurations: \( (\rho, \mu) \Delta I \text{ iff } \rho \Delta I \text{ and } I \neq \perp \)
  - Obviously monotonic. (Larger interval admits more values)
Abstract operators

Constants  \( c^\# := [c, c] \)
Abstract operators

Constants \( c^\# := [c, c] \)

Addition \([l_1, u_1] +^\# [l_2, u_2] := [l_1 + l_2, u_1 + u_2] \)

- Where \(-\infty + _:= _ + -\infty := -\infty, \infty + _:= _ + \infty := \infty \)
Abstract operators

Constants  \( c^# := [c, c] \)

Addition  \([l_1, u_1] +^# [l_2, u_2] := [l_1 + l_2, u_1 + u_2] \)
  
  • Where  \(-\infty + -\infty := -\infty, \infty + -\infty := -\infty, \infty + -\infty := -\infty, \infty + \infty := \infty \)

Negation  \(-^#[l, u] := [-u, -l] \)
Abstract operators

Constants  \( c^\#: = [c, c] \)

Addition  \([l_1, u_1] +^\# [l_2, u_2] := [l_1 + l_2, u_1 + u_2] \)

• Where  \(-\infty + _:= _ + -\infty := -\infty, \infty + _:= _ + \infty := \infty \)

Negation  \(-^\#[l, u] := [-u, -l] \)

Multiplication  \([l_1, u_1] \ast^\# [l_2, u_2] := [\min\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}, \max\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}] \)
Abstract operators

Constants
\[ c^\# := [c, c] \]

Addition
\[ [l_1, u_1] +^\# [l_2, u_2] := [l_1 + l_2, u_1 + u_2] \]
- Where \(-\infty + _- := _- + -\infty := -\infty, \infty + _- := _- + \infty := \infty\)

Negation
\[ -^\# [l, u] := [-u, -l] \]

Multiplication
\[ [l_1, u_1] *^\# [l_2, u_2] := \]
\[ [\min\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}, \max\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}] \]

Division
\[ [l_1, u_1] /^\# [l_2, u_2] := \]
\[ [\min\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}, \max\{l_1 l_2, l_1 u_2, u_1 l_2, u_1 u_2\}] \]
- If \(0 \notin [l_2, u_2]\), otherwise \([l_1, u_1] /^\# [l_2, u_2] := \top\)
Examples

• $5^# =$

• $[3, \infty) + [\frac{1}{2}, 2] = [2, \infty)$

• $[\frac{1}{2}, 3] * [\frac{5}{2}, \frac{1}{2}] = [\frac{5}{2}, 5]$ (round towards zero)

• $[1, 4] / [\frac{2}{5}, 5] = \top$
Examples

- \(5^\# = [5, 5]\)
Examples

- $5# = [5, 5]$
- $[3, \infty] + # [-1, 2] =$

$\left[ \begin{array}{c}
3 \\
5
\end{array} \right]$
Examples

- $5^# = [5, 5]$
- $[3, \infty] +^# [-1, 2] = [2, \infty]$
Examples

- $5# = [5, 5]$
- $[3, \infty] + # [-1, 2] = [2, \infty]$
- $[-1, 3] * # [-5, -1] =$
Examples

- \(5\# = [5, 5]\)
- \([3, \infty] + \# [-1, 2] = [2, \infty]\)
- \([-1, 3] \ast \# [-5, -1] = [-15, 5]\)
Examples

• $5# = [5, 5]$
• $[3, \infty] + # [-1, 2] = [2, \infty]$
• $[-1, 3] \ast # [-5, -1] = [-15, 5]$
• $-# [1, 5] =$
Examples

- $5^\# = [5, 5]$
- $[3, \infty] +^\# [-1, 2] = [2, \infty]$
- $[-1, 3] \ast^\# [-5, -1] = [-15, 5]$
- $-^\# [1, 5] = [-5, -1]$
Examples

- \(5\# = [5, 5]\)
- \([3, \infty] + \# [-1, 2] = [2, \infty]\)
- \([-1, 3] \times \# [-5, -1] = [-15, 5]\)
- \(-\# [1, 5] = [-5, -1]\)
- \([3, 5]/\# [2, 5] = \) (round towards zero)
Examples

- $5^# = [5, 5]$
- $[3, \infty] +^# [-1, 2] = [2, \infty]$
- $[-1, 3] \times^# [-5, -1] = [-15, 5]$
- $-^# [1, 5] = [-5, -1]$
- $[3, 5] /^# [2, 5] = [0, 2]$ (round towards zero)
Examples

- $5^# = [5, 5]$
- $[3, \infty] +^# [-1, 2] = [2, \infty]$
- $[-1, 3] \times^# [-5, -1] = [-15, 5]$
- $-^# [1, 5] = [-5, -1]$
- $[3, 5] /^# [2, 5] = [0, 2]$ (round towards zero)
- $[1, 4] /^# [-1, 1] = \top$
Examples

• $5\# = [5, 5]$
• $[3, \infty] + \# [−1, 2] = [2, \infty]$
• $[−1, 3] \ast \# [−5, −1] = [−15, 5]$
• $−\# [1, 5] = [−5, −1]$
• $[3, 5] / \# [2, 5] = [0, 2]$ (round towards zero)
• $[1, 4] / \# [−1, 1] = \top$
Abstract operators

Equality

\[[l_1, u_1] \equiv\# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]
Abstract operators

Equality

\[[l_1, u_1] == ['#'] [l_2, u_2] := \begin{cases} 
[1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\
[0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\
[0, 1] & \text{otherwise}
\end{cases}\]

Less-or-equal

\[[l_1, u_1] \leq ['#'] [l_2, u_2] := \begin{cases} 
[1, 1] & \text{if } u_1 \leq l_2 \\
[0, 0] & \text{if } l_1 > u_2 \\
[0, 1] & \text{otherwise}
\end{cases}\]
Abstract operators

Equality

\[ [l_1, u_1] == # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Less-or-equal

\[ [l_1, u_1] \leq # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Examples

- \([1, 2] == # [4, 5] = [0, 0]\)
Abstract operators

Equality

\[[l_1, u_1] \equiv [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Less-or-equal

\[[l_1, u_1] \leq [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Examples

- \([1, 2] \equiv [4, 5] = [0, 0]\)
Abstract operators

Equality

\[[l_1, u_1] ==[# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Less-or-equal

\[[l_1, u_1] \leq[# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Examples

- \[[1, 2] ==[# [4, 5] = [0, 0]\]
- \[[1, 2] ==[# [-1, 1] =\]
Abstract operators

Equality

\[[l_1, u_1] == # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Less-or-equal

\[[l_1, u_1] \leq # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Examples

- \([1, 2] == # [4, 5] = [0, 0]\)
- \([1, 2] == # [-1, 1] = [0, 1]\)
Abstract operators

Equality

\[ [l_1, u_1] == \# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Less-or-equal

\[ [l_1, u_1] \leq \# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Examples

- \([1, 2] == \# [4, 5] = [0, 0]\)
- \([1, 2] == \# [-1, 1] = [0, 1]\)
- \([1, 2] \leq \# [4, 5] = \]
Abstract operators

Equality

\[ [l_1, u_1] =\# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Less-or-equal

\[ [l_1, u_1] \leq\# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Examples

- \([1, 2] =\# [4, 5] = [0, 0]\)
- \([1, 2] =\# [-1, 1] = [0, 1]\)
- \([1, 2] \leq\# [4, 5] = [1, 1]\)
Abstract operators

Equality

\[[l_1, u_1] ==\# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Less-or-equal

\[[l_1, u_1] \leq\# [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases}\]

Examples

- \([1, 2] ==\# [4, 5] = [0, 0]\)
- \([1, 2] ==\# [-1, 1] = [0, 1]\)
- \([1, 2] \leq\# [4, 5] = [1, 1]\)
- \([1, 2] \leq\# [-1, 1] =\)
Abstract operators

Equality

\[ [l_1, u_1] == # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \text{ or } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Less-or-equal

\[ [l_1, u_1] \leq # [l_2, u_2] := \begin{cases} [1, 1] & \text{if } u_1 \leq l_2 \\ [0, 0] & \text{if } l_1 > u_2 \\ [0, 1] & \text{otherwise} \end{cases} \]

Examples

- \([1, 2] == # [4, 5] = [0, 0]\)
- \([1, 2] == # [-1, 1] = [0, 1]\)
- \([1, 2] \leq # [4, 5] = [1, 1]\)
- \([1, 2] \leq # [-1, 1] = [0, 1]\)
Proof obligations

\[ c \triangle c^\# \]

\[ \nu_1 \triangle d_1 \land \nu_2 \triangle d_2 \implies \nu_1 \Box \nu_2 \triangle d_1 \Box^\# d_2 \]

Analogously for unary, ternary, etc. operators
Proof obligations

c \Delta \ c^#

\nu_1 \Delta d_1 \land \nu_2 \Delta d_2 \implies \nu_1 \Box \nu_2 \Delta d_1 \Box^# d_2

Analogously for unary, ternary, etc. operators

Then, we get \rho \Delta \rho^# \implies \llbracket e \rrbracket \rho \Delta \llbracket e \rrbracket ^# \rho^#

- As for constant propagation
Effects of edges

For \( \rho^# \neq \bot \)

\[
\begin{align*}
\text{[.]#} \bot &= \bot \\
\text{[Nop]}# \rho# &= \rho# \\
\text{[x = e]}# \rho# &= \rho#(x \rightarrow \text{[e]}# \rho#) \\
\text{[x = M[e]}# \rho# &= \rho#(x \rightarrow \top) \\
\text{[M[e]}# \rho# &= \rho# \\
\text{[Pos(e)]#} \rho# &= \begin{cases} 
\bot & \text{if } \text{[e]}# \rho# = [0, 0] \\
\rho# & \text{otherwise}
\end{cases} \\
\text{[Neg(e)]#} \rho# &= \begin{cases} 
\rho# & \text{if } \text{[e]}# \rho# \sqsubseteq [0, 0] \\
\bot & \text{otherwise}
\end{cases}
\end{align*}
\]
Last lecture

- Constant propagation
  - Idea: Abstract description of values, lift to valuations, states
- Monotonic, but not distributive
  - MOP solution undecidable (Reduction to Hilbert’s 10th problem)
- Interval analysis
  - Associate variables with intervals of possible values
Better exploitation of conditions

\[
\begin{align*}
\llbracket \text{Pos}(e) \rrbracket &\# \rho^# = \\
&\begin{cases}
\bot & \text{if } \llbracket e \rrbracket \# \rho^# = [0, 0] \\
\rho^#(x \mapsto \rho^#(x) \cap [\llbracket e_1 \rrbracket \# \rho^#]) & \text{if } e = x = e_1 \\
\rho^#(x \mapsto \rho^#(x) \cap [-\infty, u]) & \text{if } e = x \leq e_1 \text{ and } \llbracket e_1 \rrbracket \# \rho^# = [\_, u] \\
\rho^#(x \mapsto \rho^#(x) \cap [l, \infty]) & \text{if } e = x \geq e_1 \text{ and } \llbracket e_1 \rrbracket \# \rho^# = [l, \_] \\
\ldots & \\
\rho^# & \text{otherwise}
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\llbracket \text{Neg}(e) \rrbracket &\# \rho^# = \\
&\begin{cases}
\bot & \text{if } \llbracket e \rrbracket \# \rho^# \not\subseteq [0, 0] \\
\rho^#(x \mapsto \rho^#(x) \cap [\llbracket e_1 \rrbracket \# \rho^#]) & \text{if } e = x \neq e_1 \\
\rho^#(x \mapsto \rho^#(x) \cap [-\infty, u]) & \text{if } e = x > e_1 \text{ and } \llbracket e_1 \rrbracket \# \rho^# = [\_, u] \\
\rho^#(x \mapsto \rho^#(x) \cap [l, \infty]) & \text{if } e = x < e_1 \text{ and } \llbracket e_1 \rrbracket \# \rho^# = [l, \_] \\
\ldots & \\
\rho^# & \text{otherwise}
\end{cases}
\end{align*}
\]

- where \([l_1, u_1] \cap [l_2, u_2] = [\max(l_1, l_2), \min(u_1, u_2)]\)
  - only exists if intervals overlap
  - this is guaranteed by conditions
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
- Replace subexpressions $e$ with $[e]^{\# \rho^\#} = [v, v]$ by $v$ (constant propagation)
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
- Replace subexpressions $e$ with $\llbracket e \rrbracket_{\#} \rho_{\#} = [v, v]$ by $v$ (constant propagation)
- Replace $\text{Pos}(e)$ by $\text{Nop}$ if $[0, 0] \nsubseteq \llbracket e \rrbracket_{\#} \rho_{\#}$ (0 cannot occur)
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
- Replace subexpressions $e$ with $\llbracket e \rrbracket^\rho = [v, v]$ by $v$ (constant propagation)
- Replace $\text{Pos}(e)$ by $\text{Nop}$ if $[0, 0] \not\subseteq \llbracket e \rrbracket^\rho$ (0 cannot occur)
- Replace $\text{Neg}(e)$ by $\text{Nop}$ if $\llbracket e \rrbracket^\rho = [0, 0]$ (Only 0 can occur)
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
- Replace subexpressions $e$ with $\llbracket e \rrbracket^{\#} \rho^\# = [v, v]$ by $v$ (constant propagation)
- Replace $\text{Pos}(e)$ by $\text{Nop}$ if $[0, 0] \not\subseteq \llbracket e \rrbracket^{\#} \rho^\#$ (0 cannot occur)
- Replace $\text{Neg}(e)$ by $\text{Nop}$ if $\llbracket e \rrbracket^{\#} \rho^\# = [0, 0]$ (Only 0 can occur)
- Yields function $\text{tr}(k, \rho^\#)$
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \perp$ (unreachable)
- Replace subexpressions $e$ with $\llbracket e \rrbracket \rho_\# = [v, v]$ by $v$ (constant propagation)
- Replace $\text{Pos}(e)$ by $\text{Nop}$ if $[0, 0] \not\subseteq \llbracket e \rrbracket \rho_\#$ (0 cannot occur)
- Replace $\text{Neg}(e)$ by $\text{Nop}$ if $\llbracket e \rrbracket \rho_# = [0, 0]$ (Only 0 can occur)
- Yields function $\text{tr}(k, \rho_\#)$
- Transformation: $(u, k, v) \mapsto (u, \text{tr}(k, \text{MFP}[u]), v)$
Transformations

- Erase nodes $u$ with $\text{MOP}[u] = \bot$ (unreachable)
- Replace subexpressions $e$ with $\llbracket e \rrbracket^\# \rho^\# = [v, v]$ by $v$ (constant propagation)
- Replace $\text{Pos}(e)$ by $\text{Nop}$ if $[0, 0] \not\subseteq \llbracket e \rrbracket^\# \rho^\#$ ($0$ cannot occur)
- Replace $\text{Neg}(e)$ by $\text{Nop}$ if $\llbracket e \rrbracket^\# \rho^\# = [0, 0]$ (Only $0$ can occur)
- Yields function $\text{tr}(k, \rho^\#)$
- Transformation: $(u, k, v) \mapsto (u, \text{tr}(k, \text{MFP}[u]), v)$
- Proof obligation:
  - $(\rho, \mu) \Delta \rho^\# \implies \llbracket k \rrbracket(\rho, \mu) = \llbracket \text{tr}(k, \rho^\#) \rrbracket(\rho, \mu)$
Example

$\bot$

$i=0$

Neg($i<42$)

Pos($i<42$)

Neg($0<=i<42$)

Pos($0<=i<42$)

$M[a+i]=i*2$

$i=i+1$

$\bot$

About 40 iterations later ...
Example

\{i \mapsto T\}

\[ \text{Neg}(i<42) \]

\[ \text{Neg}(0\leq i<42) \]

\[ \text{M}[a+i]=i*2 \]

\[ i=i+1 \]
Example

\[
\{ i \mapsto \top \}
\]

\[
i = 0
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
i = i + 1
\]

Neg \(i < 42\)

\[
\text{Pos} \ (i < 42)
\]

\[
\text{Neg} \ (0 \leq i < 42)
\]

\[
\text{Pos} \ (0 \leq i < 42)
\]

\[
M[a+i] = i \times 2
\]

\[
\bot
\]
Example

\begin{align*}
&\{i \mapsto T\} \\
&i=0 \\
&\{i \mapsto [0, 0]\} \quad i=i+1 \\
&\neg (i<42) \\
&\neg (0\leq i<42) \\
&M[a+i]=i*2 \\
&\{i \mapsto [0, 0]\} \\
&\neg (0\leq i<42) \\
&\neg (i<42) \\
&\bot \\
&\bot \\
&\bot \\
\end{align*}

About 40 iterations later ...
Example

\[
\{ i \mapsto T \} \quad \text{i=0} \quad \{ i \mapsto [0, 0] \} \quad \{ i \mapsto [0, 0] \} \\
\]

Neg(i<42) Pos(i<42) M[a+i]=i*2

Neg(0<=i<42) Pos(0<=i<42)
Example

\[
\{ i \mapsto T \} \\
\{ i \mapsto [0, 0] \}
\]

\[
\text{Neg}(i<42) \quad \text{Pos}(i<42)
\]

\[
\text{Neg}(0\leq i<42) \quad \text{Pos}(0\leq i<42)
\]

\[
M[a+i]=i\times2
\]

About 40 iterations later ...

181 / 471
Example

\{i \mapsto T\}

\{i \mapsto [0, 1]\}

\{i \mapsto [0, 0]\}

\{i \mapsto [0, 0]\}

Neg(i<42)

Pos(i<42)

\{i \mapsto [0, 0]\}

Neg(0\leq i<42)

Pos(0\leq i<42)

\{i \mapsto [0, 0]\}

M[a+i]=i*2

\{i \mapsto [0, 0]\}

About 40 iterations later...
Example

\[
\begin{align*}
\{ i \mapsto 0 \} & \quad \text{Neg(0<i<42)} \\
\{ i \mapsto [0, 1] \} & \quad \text{Pos(0<i<42)} \\
\{ i \mapsto [0, 1] \} & \quad \text{i=i+1} \\
\{ i \mapsto [0, 42] \} & \quad \text{M[a+i]=i*2} \\
\{ i \mapsto [0, 0] \} & \\
\{ i \mapsto [0, 0] \} & \\
\{ i \mapsto T \} & \\
\end{align*}
\]

About 40 iterations later ...
Example

\[
\begin{align*}
\{i \mapsto T\} \\
\{i \mapsto [0,1]\} \\
\{i \mapsto [0,1]\} \\
\{i \mapsto [0,1]\} \\
\{i \mapsto [0,1]\} \\
\{i \mapsto [0,0]\} \\
\end{align*}
\]

\[
\begin{align*}
&\text{Neg}(i<42) \\
&\text{Neg}(0\leq i<42) \\
&\text{M}[a+i] = i\times 2
\end{align*}
\]
Example

\{i \mapsto T\}

i = 0

\{i \mapsto [0, 1]\}

i = i + 1

Neg(i < 42)

Pos(i < 42)

Neg(0 <= i < 42)

Pos(0 <= i < 42)

M[a+i] = i*2

\{i \mapsto [0, 1]\}

\{i \mapsto [0, 1]\}

\{i \mapsto [0, 1]\}

About 40 iterations later...
Example

About 40 iterations later ...
Example

About 40 iterations later ...
Problem

- Interval analysis takes many iterations
- May not terminate at all for (i=0; x>0; x--) i=i+1
Widening

- Idea: Accelerate the iteration
Widening

- Idea: Accelerate the iteration — at the price of imprecision
Widening

- Idea: Accelerate the iteration — at the price of imprecision
- Here: Disallow updates of interval bounds in $\mathbb{Z}$.
  - A maximal chain: $[3, 8] \sqsubseteq [\neg \infty, 8] \sqsubseteq [\neg \infty, \infty]$
Widening (Formally)

- Given: Constraint system (1) \( x_i \sqsupseteq f_i(\vec{x}) \)
  - \( f_i \) not necessarily monotonic
- Regard the system (2) \( x_i = x_i \sqcup f_i(\vec{x}) \)
- Obviously: \( \vec{x} \) solution of (1) iff \( \vec{x} \) solution of (2)
  - Note: \( x \sqsubseteq y \iff x \sqcup y = y \)
- (2) induces a function \( G : \mathbb{D}^n \rightarrow \mathbb{D}^n \)
  \[
  G(\vec{x}) = \vec{x} \sqcup (f_1(\vec{x}), \ldots, f_n(\vec{x}))
  \]
- \( G \) is not necessarily monotonic, but increasing:
  \[
  \forall \vec{x}. \quad \vec{x} \sqsubseteq G(\vec{x})
  \]
Widening (Formally)

- $G$ is increasing $\rightarrow \perp \subseteq G(\perp) \subseteq G^2(\perp) \subseteq \ldots$
  - i.e., $\langle G^i(\perp) \rangle_{i \in \mathbb{N}}$ is ascending chain
- If it stabilizes, i.e., $\vec{x} = G^k(\perp) = G^{k+1}(\perp)$, then $\vec{x}$ is solution of (1)
- If $\mathcal{D}$ has infinite ascending chains, still no termination guaranteed
- Replace $\cup$ by widening operator $\sqcup$
  - Get (3) $x_i = x_i \sqcup f_i(\vec{x})$
- Widening: Any operation $\mathcal{D} \times \mathcal{D} \rightarrow \mathcal{D}$
  1. with $x \sqcup y \subseteq x \sqcup y$
  2. and for every sequence $a_0, a_1, \ldots$, the chain $b_0 = a_0, b_{i+1} = b_i \sqcup a_{i+1}$ eventually stabilizes
- Using FP-iteration (naive, RR, worklist) on (3) will
  - compute a solution of (1)
  - terminate
To show

- Solutions of (3) are solutions of (1)
  - $x_i = x_i \sqcup f_i(\vec{x})$
To show

- Solutions of (3) are solutions of (1)
  - \( x_i = x_i \sqcup f_i(\vec{x}) \supseteq x_i \sqcup f_i(\vec{x}) \)
To show

- Solutions of (3) are solutions of (1)
  - $x_i = x_i \sqcup f_i(\vec{x}) \sqsubseteq x_i \sqcup f_i(\vec{x}) \sqsubseteq f_i(\vec{x})$

  □
To show

- Solutions of (3) are solutions of (1)
  - \( x_i = x_i \sqcup f_i(\vec{x}) \supseteq x_i \sqcup f_i(\vec{x}) \supseteq f_i(\vec{x}) \)

- FP-iteration computes a solution of (3).
  - Valuation increases until it stabilizes (latest at \( \vec{x} = (\top, \ldots, \top) \))
To show

- Solutions of (3) are solutions of (1)
  - $x_i = x_i \sqcup f_i(\vec{x}) \sqsubseteq x_i \sqcup f_i(\vec{x}) \sqsubseteq f_i(\vec{x})$
- FP-iteration computes a solution of (3).
  - Valuation increases until it stabilizes (latest at $\vec{x} = (\top, \ldots, \top)$)
- FP-iteration terminates
  - FP-iteration step: Replace (some) $x_i$ by $x_i \sqcup f_i(\vec{x})$
  - This only happens finitely many times (Widening operator, Criterion 2)
For interval analysis

- Widening defined as $[l_1, u_1] \sqcup [l_2, u_2] := [l, u]$ with

  $$l := \begin{cases} 
  l_1 & \text{if } l_1 \leq l_2 \\
  -\infty & \text{otherwise}
  \end{cases}$$

  $$u := \begin{cases} 
  u_1 & \text{if } u_1 \geq u_2 \\
  +\infty & \text{otherwise}
  \end{cases}$$
For interval analysis

• Widening defined as \([l_1, u_1] \sqcup [l_2, u_2] := [l, u]\) with

\[
l := \begin{cases} 
  l_1 & \text{if } l_1 \leq l_2 \\
  -\infty & \text{otherwise}
\end{cases}
\]

\[
u := \begin{cases} 
  u_1 & \text{if } u_1 \geq u_2 \\
  +\infty & \text{otherwise}
\end{cases}
\]

• Lift to valuations: \((\rho_1^\# \sqcup \rho_2^\#)(x) := \rho_1^\#(x) \sqcup \rho_2^\#(x)\)

\[\sqcup\] is widening operator

1 \[\sqcup\] is not commutative.

Lower and upper bound updated at most once.

Note:
For interval analysis

• Widening defined as \([l_1, u_1] \uplus [l_2, u_2] := [l, u]\) with

\[
\begin{align*}
  l &:= \begin{cases} l_1 & \text{if } l_1 \leq l_2 \\ -\infty & \text{otherwise} \end{cases} \\
u &:= \begin{cases} u_1 & \text{if } u_1 \geq u_2 \\ +\infty & \text{otherwise} \end{cases}
\end{align*}
\]

• Lift to valuations: \((\rho_1^\# \uplus \rho_2^\#)(x) := \rho_1^\#(x) \uplus \rho_2^\#(x)\)

• and to \(\mathbb{D} = (\text{Reg} \to \mathbb{I}) \cup \{\bot\}: \bot \uplus x = x \uplus \bot = x\)
For interval analysis

- Widening defined as $[l_1, u_1] \sqcup [l_2, u_2] := [l, u]$ with

  $$
l := \begin{cases} 
  l_1 & \text{if } l_1 \leq l_2 \\
  -\infty & \text{otherwise}
  \end{cases}
$$

  $$
u := \begin{cases} 
  u_1 & \text{if } u_1 \geq u_2 \\
  +\infty & \text{otherwise}
  \end{cases}
$$

- Lift to valuations: $(\rho_1^\# \sqcup \rho_2^\#)(x) := \rho_1^\#(x) \sqcup \rho_2^\#(x)$
- and to $\mathbb{D} = (\text{Reg} \rightarrow \mathbb{I}) \cup \{\bot\}$: $\bot \sqcup x = x \sqcup \bot = x$
- $\sqcup$ is widening operator
  1. $x \sqcup y \subseteq x \sqcup y$. Obvious
  2. Lower and upper bound updated at most once.
For interval analysis

- Widening defined as $[l_1, u_1] \sqcup [l_2, u_2] := [l, u]$ with

$$l := \begin{cases} l_1 & \text{if } l_1 \leq l_2 \\ -\infty & \text{otherwise} \end{cases}$$

$$u := \begin{cases} u_1 & \text{if } u_1 \geq u_2 \\ +\infty & \text{otherwise} \end{cases}$$

- Lift to valuations: $(\rho_1^\# \sqcup \rho_2^\#)(x) := \rho_1^\#(x) \sqcup \rho_2^\#(x)$
- and to $\mathbb{D} = (\text{Reg} \to \mathbb{I}) \cup \{\bot\}: \bot \sqcup x = x \sqcup \bot = x$
- $\sqcup$ is widening operator
  1. $x \sqcup y \subseteq x \sqcup y$. Obvious
  2. Lower and upper bound updated at most once.
- Note: $\sqcup$ is not commutative.
Examples

- $[-2, 2] \sqcup [1, 2] = $

- $[1, 2] \sqcup [-2, 2] = $

- $[1, 2] \sqcup [1, 3] = $
Examples

• \([-2, 2] \sqcup [1, 2] = [-2, 2]\)
Examples

- \([-2, 2] \sqcup [1, 2] = [-2, 2]\)
- \([1, 2] \sqcup [-2, 2] =\)
Examples

- \([-2, 2] \uplus [1, 2] = [-2, 2]\)
- \([1, 2] \uplus [-2, 2] = [-\infty, 2]\)

Widening returns larger values more quickly
Examples

- $[-2, 2] \sqcup [1, 2] = [-2, 2]$
- $[1, 2] \sqcup [-2, 2] = [-\infty, 2]$
- $[1, 2] \sqcup [1, 3] =$
Examples

- $[-2, 2] \sqcup [1, 2] = [-2, 2]$
- $[1, 2] \sqcup [-2, 2] = [-\infty, 2]$
- $[1, 2] \sqcup [1, 3] = [1, +\infty]$
Examples

• \([-2, 2] \sqcup [1, 2] = [-2, 2]\)
• \([1, 2] \sqcup [-2, 2] = [-\infty, 2]\)
• \([1, 2] \sqcup [1, 3] = [1, +\infty]\)
• Widening returns larger values more quickly
Widening (Intermediate Result)

- Define **suitable** widening
Widening (Intermediate Result)

- Define suitable widening
- Solve constraint system (3)
Widening (Intermediate Result)

- Define **suitable** widening
- Solve constraint system (3)
- Guaranteed to terminate and return over-approximation of MOP
Widening (Intermediate Result)

- Define suitable widening
- Solve constraint system (3)
- Guaranteed to terminate and return over-approximation of MOP
- But: Construction of good widening is black magic
Widening (Intermediate Result)

- Define **suitable** widening
- Solve constraint system (3)
- Guaranteed to terminate and return over-approximation of MOP
- But: Construction of good widening is **black magic**
  - Even may choose $\sqcup$ *dynamically* during iteration, such that
    - Values do not get too complicated
    - Iteration is guaranteed to terminate
Example (Revisited)

\[\neg(i < 42)\]
\[\neg(0 \leq i < 42)\]
\[M[a+i]=i \times 2\]
Example (Revisited)

\( \{i \mapsto [-\infty, +\infty]\} \)

\( i = 0 \)

\( \perp \)

\( i = i + 1 \)

Neg \( (i < 42) \)

Pos \( (i < 42) \)

Neg \( (0 \leq i < 42) \)

Pos \( (0 \leq i < 42) \)

M \[ a + i \] = i \times 2

\( \perp \)

Not exactly what we expected :(
Example (Revisited)

\[
\{ i \mapsto [-\infty, +\infty] \} 
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[ i = 0 \]

\[ i = i + 1 \]

\[
\bot
\]

\[ \neg (i < 42) \]

\[ \neg (0 \leq i < 42) \]

\[ M[a+i] = i \times 2 \]

\[ \bot \]

\[ \bot \]
Example (Revisited)

\[
\{ i \mapsto [-\infty, +\infty] \}
\]

\[
i = 0
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
i = i + 1
\]

Neg(i<42)

Pos(i<42)

\[
\{ i \mapsto [0, 0] \}
\]

Neg(0<=i<42)

Pos(0<=i<42)

\[
\bot
\]

M[a+i] = i \times 2

\[
\bot
\]
Example (Revisited)

\[
\{ i \mapsto [-\infty, +\infty] \}
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
\text{Neg}(i<42)
\]

\[
\text{Pos}(i<42)
\]

\[
\text{Neg}(0\leq i<42)
\]

\[
\text{Pos}(0\leq i<42)
\]

\[
M[a+i]=i*2
\]

\[
i=i+1
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
\{ i \mapsto [0, 0] \}
\]

\[
\bot
\]
Example (Revisited)

\[ \{ i \mapsto [-\infty, +\infty] \} \]

\[ i = 0 \]

\[ \{ i \mapsto [0, 0] \} \]

\[ i = i + 1 \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \text{Neg}(i < 42) \]

\[ \text{Pos}(i < 42) \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \text{Neg}(0 \leq i < 42) \]

\[ \text{Pos}(0 \leq i < 42) \]

\[ \{ i \mapsto [0, 0] \} \]

\[ M[a+i] = i \times 2 \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \bot \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \bot \]

\[ \{ i \mapsto [0, 0] \} \]

• Not exactly what we expected :(
Example (Revisited)

\[ M[a+i] = i \times 2 \]

\[ i = i + 1 \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \{ i \mapsto [-\infty, +\infty] \} \]

\[ \{ i \mapsto [0, +\infty] \} \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \{ i \mapsto [0, 0] \} \]

\[ \{ i \mapsto [0, 0] \} \]
Example (Revisited)

\[ \{ i \mapsto [-\infty, +\infty] \} \]

\[ i = 0 \]

\[ \{ i \mapsto [0, +\infty] \} \]

\[ i = i + 1 \]

Neg \( i < 42 \)

Pos \( i < 42 \)

\[ \{ i \mapsto [42, +\infty] \} \]

\[ \{ i \mapsto [0, +\infty] \} \]

Neg \( 0 \leq i < 42 \)

Pos \( 0 \leq i < 42 \)

\[ \{ i \mapsto [0, 0] \} \]

M[a+i] = i*2

\[ \{ i \mapsto [0, 0] \} \]
Example (Revisited)

\[
\begin{align*}
  i &= 0 \\
  \{i \mapsto [0, +\infty]\} & \quad i = i + 1
\end{align*}
\]

\[
\begin{align*}
  \text{Neg}(i < 42) & \quad \{i \mapsto [0, +\infty]\} \\
  \text{Pos}(i < 42) & \quad \{i \mapsto [42, +\infty]\} \\
  \text{Neg}(0 \leq i < 42) & \quad \{i \mapsto [42, +\infty]\} \\
  \text{Pos}(0 \leq i < 42) & \quad \{i \mapsto [0, +\infty]\}
\end{align*}
\]

\[
\begin{align*}
  M[a+i] &= i \times 2 \\
  \{i \mapsto [0, 0]\}
\end{align*}
\]
Example (Revisited)

\[
\{ i \mapsto [-\infty, +\infty] \}
\]

\[
i = 0
\]

\[
\{ i \mapsto [0, +\infty] \}_{i = i + 1}
\]

\[
\text{Neg}(i<42)
\]

\[
\{ i \mapsto [42, +\infty] \}
\]

\[
\{ i \mapsto [0, +\infty] \}
\]

\[
\text{Pos}(i<42)
\]

\[
\text{Neg}(0 \leq i < 42)
\]

\[
\{ i \mapsto [42, +\infty] \}
\]

\[
\{ i \mapsto [0, +\infty] \}
\]

\[
\text{Pos}(0 \leq i < 42)
\]

\[
\{ i \mapsto [42, +\infty] \}
\]

\[
\{ i \mapsto [0, +\infty] \}
\]

\[
M[a+i] = i \times 2
\]

\[
\{ i \mapsto [0, +\infty] \}
\]

• Not exactly what we expected :(
Example (Revisited)

\[ \{i \mapsto [-\infty, +\infty]\} \]

- \( i = 0 \)
- \( \{i \mapsto [0, +\infty]\} \)
  - \( i = i + 1 \)
  - \( \{i \mapsto [42, +\infty]\} \)
  - \( \{i \mapsto [0, +\infty]\} \)

- \( \text{Neg}(i<42) \)
- \( \text{Pos}(i<42) \)

- \( \text{Neg}(0 \leq i < 42) \)
- \( \text{Pos}(0 \leq i < 42) \)

\[ M[a+i] = i \times 2 \]

\[ \{i \mapsto [0, +\infty]\} \]

- Not exactly what we expected :(
Idea

- Only apply widening at loop separators
- A set $S \subseteq V$ is called loop separator, iff each cycle in the CFG contains a node from $S$.
- Intuition: Only loops can cause infinite chains of updates.
- Thus, FP-iteration still terminates
Problem

- How to find suitable loop separator

- We could take $S = \{2\}$, $S = \{4\}$, ...
- Results of FP-iteration are different!
Loop Separator $S = \{2\}$

1. $i=0$
2. $i=i+1$
3. Neg($i<42$)
4. Pos($i<42$)
5. Neg($0\leq i<42$)
6. Pos($0\leq i<42$)
7. $M[a+i] = i \times 2$

$\bot$
Loop Separator $S = \{2\}$

$i \mapsto [\neg\infty, +\infty]$
Loop Separator $S = \{2\}$

\[
\begin{align*}
\{ i \mapsto [-\infty, +\infty] \} \\
\{ i \mapsto [0, 0] \} \\
M[a+i] = i*2
\end{align*}
\]
Loop Separator $S = \{2\}$

\[
\begin{align*}
\{i \mapsto [-\infty, +\infty]\} \\
i=0 \\
\{i \mapsto [0, 0]\} \\
i=i+1 \\
\text{Neg}(i<42) \quad \text{Pos}(i<42)
\end{align*}
\]

\[
\begin{align*}
\{i \mapsto [0, 0]\} \\
\text{Neg}(0\leq i<42) \quad \text{Pos}(0\leq i<42)
\end{align*}
\]

\[
M[a+i]=i \times 2
\]

\[
\bot \quad \bot \quad \bot
\]
Loop Separator $S = \{2\}$

$\{i \mapsto (-\infty, +\infty]\}$

1. $i = 0$

2. $\{i \mapsto [0, 0]\}$

3. Neg($i < 42$)

4. Pos($i < 42$)

5. Neg($0 \leq i < 42$)

6. Pos($0 \leq i < 42$)

7. $M[a+i] = i \times 2$

Fixed point
Loop Separator $S = \{2\}$

1. $i = 0$
   - $\{i \mapsto [-\infty, +\infty]\}$

2. $i = i + 1$
   - $\{i \mapsto [0, 0]\}$

3. Neg($i < 42$)
   - $\perp$
   - $\{i \mapsto [0, 0]\}$

4. Pos($i < 42$)
   - $\{i \mapsto [0, 0]\}$

5. Neg($0 \leq i < 42$)
   - $\perp$
   - $\{i \mapsto [0, 0]\}$

6. Pos($0 \leq i < 42$)
   - $\{i \mapsto [0, 0]\}$

7. $M[a+i] = i \times 2$
   - $\{i \mapsto [0, 0]\}$
Loop Separator $S = \{2\}$

$i \mapsto [-\infty, +\infty]$

1

$i = 0$

$i \mapsto [0, +\infty]$

2

$i = i + 1$

$\neg (i < 42)$

3

$\neg (0 \leq i < 42)$

4

$\neg (0 \leq i < 42)$

5

$\neg (0 \leq i < 42)$

6

$\neg (0 \leq i < 42)$

7

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$

$\vdash$
Loop Separator $S = \{2\}$

$\{i \mapsto [-\infty, +\infty]\}$

$1$

$i = 0$

$\{i \mapsto [0, +\infty]\}$

$2$

$i = i + 1$

$3$

Neg($i < 42$)

$4$

Pos($i < 42$)

$5$

Neg($0 <= i < 42$)

$6$

Pos($0 <= i < 42$)

$7$

$M[a+i] = i \times 2$

$\{i \mapsto [0, 0]\}$

$\bot$

$\{i \mapsto [0, 0]\}$

$\{i \mapsto [0, 41]\}$

$\{i \mapsto [0, +\infty]\}$

$\{i \mapsto [42, +\infty]\}$

$\{i \mapsto [0, +\infty]\}$

$\{i \mapsto [0, 0]\}$
Loop Separator $S = \{2\}$

{\(i \mapsto [-\infty, +\infty]\)}

1

\(i = 0\)

\{\(i \mapsto [0, +\infty]\}\}

2

\(i = i + 1\)

Neg(\(i < 42\))

\{\(i \mapsto [42, +\infty]\}\}

3

Pos(\(i < 42\))

\{\(i \mapsto [0, 41]\}\}

4

Neg(\(0 \leq i < 42\))

\{\(i \mapsto [42, +\infty]\}\}

5

Pos(\(0 \leq i < 42\))

\{\(i \mapsto [0, 41]\}\}

6

\(M[a+i] = i \times 2\)

7

\{\(i \mapsto [0, 0]\}\}
Loop Separator $S = \{2\}$

\[
\{ i \mapsto [\neg i < 42, \neg 0 \leq i < 42, \neg 42 \leq i < 42, \neg 0 \leq i \leq 41] \} \rightarrow \{ i \mapsto [0, +\infty] \} \rightarrow \{ i \mapsto [0, 41] \} \rightarrow \{ i \mapsto [0, 41] \} \rightarrow \{ i \mapsto [0, 41] \} \rightarrow \{ i \mapsto [0, 41] \}
\]
Loop Separator $S = \{2\}$

1. $i = 0$
2. $\{i \rightarrow [0, +\infty]\}$
3. $\text{Neg}(i < 42)$
4. $\text{Pos}(i < 42)$
5. $\{i \rightarrow [42, +\infty]\}$
6. $\{i \rightarrow [0, 41]\}$
7. $\{i \rightarrow [0, 41]\}$

- Fixed point
Loop Separator $S = \{4\}$

1. $i = 0$
2. $i = i + 1$
3. \(\text{Neg}(i < 42)\)
4. \(\text{Pos}(i < 42)\)
5. \(\text{Neg}(0 \leq i < 42)\)
6. \(\text{Pos}(0 \leq i < 42)\)
7. $M[a + i] = i \times 2$
Loop Separator $S = \{4\}$

\[ \{ i \mapsto [-\infty, +\infty]\} \]

\[ i = 0 \]

\[ \perp \]

\[ i = i + 1 \]

\[ \perp \]

\[ \text{Neg}(i < 42) \]

\[ \perp \]

\[ \text{Pos}(i < 42) \]

\[ \perp \]

\[ \text{Neg}(0 \leq i < 42) \]

\[ \perp \]

\[ \text{Pos}(0 \leq i < 42) \]

\[ \perp \]

\[ M[a + i] = i \times 2 \]

\[ \perp \]
Loop Separator $S = \{4\}$

\[
\{ i \mapsto [-\infty, +\infty] \}
\]

\[
\begin{align*}
& 1 \\
& \quad i = 0 \\
& \quad \{ i \mapsto [0, 0] \} \\
& \quad i = i + 1 \\
& \quad \text{Neg}(i < 42) \\
& \quad \text{Pos}(i < 42) \\
& \quad \perp \\
& \quad \text{Neg}(0 \leq i < 42) \\
& \quad \text{Pos}(0 \leq i < 42) \\
& \quad \perp \\
& \quad M[a + i] = i \times 2 \\
& \quad \perp
\end{align*}
\]
Loop Separator $S = \{4\}$

$$\{ i \mapsto [-\infty, +\infty] \}$$

$$i = 0$$

$$\{ i \mapsto [0, 0] \}$$

$$i = i + 1$$

$$\{ i \mapsto [0, 0] \}$$

$\bot$
Loop Separator $S = \{4\}$

1. $i = 0$
   - $\{i \mapsto [-\infty, +\infty]\}$

2. $i = i + 1$
   - $\{i \mapsto [0, 0]\}$

3. Neg($i < 42$)
4. Pos($i < 42$)
   - $\{i \mapsto [0, 0]\}$

5. Neg($0 \leq i < 42$)
6. Pos($0 \leq i < 42$)
   - $\{i \mapsto [0, 0]\}$

7. $M[a+i] = i \times 2$
   - $\bot$
Loop Separator $S = \{4\}$

1. $\{i \mapsto [-\infty, +\infty]\}$

2. $\{i \mapsto [0, 0]\}$

3. $\text{Neg}(i < 42)$

4. $\text{Pos}(i < 42)$

5. $\text{Neg}(0 \leq i < 42)$

6. $\text{Pos}(0 \leq i < 42)$

7. $\{i \mapsto [0, 0]\}$

$i = 0$

$i = i + 1$

\[ M[a + i] = i \times 2 \]
Loop Separator $S = \{4\}$

{i \mapsto [-\infty, +\infty]}
Loop Separator $S = \{4\}$

\[
\begin{align*}
&\{i \mapsto [-\infty, +\infty]\} \\
&i = 0 \\
&\{i \mapsto [0, 1]\} \\
&i = i + 1 \\
\end{align*}
\]

- Neg($i < 42$)
- Pos($i < 42$)

\[
\begin{align*}
&\{i \mapsto [0, +\infty]\} \\
&\{i \mapsto [0, 0]\} \\
&M[a+i] = i \times 2 \\
\end{align*}
\]

\[
\begin{align*}
&\{i \mapsto [0, 0]\} \\
\end{align*}
\]
Loop Separator $S = \{4\}$

$\{i \mapsto [-\infty, +\infty]\}$

1

\[i = 0\]

\(\{i \mapsto [0, 1]\}\)

2

\(i = i + 1\)

3

Neg($i < 42$)

4

Pos($i < 42$)

\(\{i \mapsto [0, +\infty]\}\)

5

Neg($0 \leq i < 42$)

6

Pos($0 \leq i < 42$)

\(\{i \mapsto [42, +\infty]\}\)

\(\{i \mapsto [0, 41]\}\)

7

\(\{i \mapsto [0, 0]\}\)

\(M[a + i] = i \times 2\)
Loop Separator $S = \{4\}$

1. \{ $i \mapsto [-\infty, +\infty]$ \}

2. \{ $i \mapsto [0, 1]$ \} \quad i = i + 1

3. Neg($i < 42$)

4. Pos($i < 42$) \quad \{ $i \mapsto [0, +\infty]$ \}

5. Neg($0 \leq i < 42$)

6. Pos($0 \leq i < 42$) \quad \{ $i \mapsto [0, 41]$ \}

7. \{ $i \mapsto [0, 41]$ \}

\[ M[a+i] = i \times 2 \]
Loop Separator $S = \{4\}$

1. $i=0$

2. $i=i+1$

3. Neg($i<42$)

4. Pos($i<42$)

5. Neg($0\leq i<42$)

6. Pos($0\leq i<42$)

7. $M[a+i]=i*2$

{ $i \mapsto [0, 42] $ }

{ $i \mapsto [0, +\infty] $ }

{ $i \mapsto [42, +\infty] $ }

{ $i \mapsto [0, 41] $ }

{ $i \mapsto [0, 41] $ }

{ $i \mapsto [0, 41] $ }

{ $i \mapsto [-\infty, +\infty] $ }

$\bot$
Loop Separator $S = \{4\}$

\[
\begin{align*}
\{i \mapsto [-\infty, +\infty]\} \\
\{i \mapsto [0, 42]\} & \quad i = i + 1 \\
\{i \mapsto [42, 42]\} & \quad \text{Neg}(i < 42) \\
\{i \mapsto [42, +\infty]\} & \quad \text{Pos}(i < 42) \\
\{i \mapsto [0, +\infty]\} \\
\{i \mapsto [0, 42]\} & \quad \text{Neg}(0 \leq i < 42) \\
\{i \mapsto [42, +\infty]\} & \quad \text{Pos}(0 \leq i < 42) \\
\{i \mapsto [0, 41]\} \\
\{i \mapsto [0, 41]\} \\
\{i \mapsto [0, 41]\} \\
\{i \mapsto [0, 41]\} \\
\end{align*}
\]

\[M[a+i] = i \times 2\]
Loop Separator $S = \{4\}$

\[ \{i \mapsto [-\infty, +\infty]\} \]

- $i = 0$
  - $\{i \mapsto [0, 42]\}$
    - $i = i + 1$
      - $\{i \mapsto [42, 42]\}$
      - $\{i \mapsto [42, +\infty]\}$
    - $\{i \mapsto [0, +\infty]\}$
  - $\text{Neg}(i < 42)$
    - $\{i \mapsto [0, 42]\}$
      - $\{i \mapsto [42, 42]\}$
      - $\{i \mapsto [42, +\infty]\}$
    - $\{i \mapsto [0, +\infty]\}$
  - $\text{Pos}(i < 42)$
    - $\{i \mapsto [0, 42]\}$
      - $\{i \mapsto [42, 42]\}$
      - $\{i \mapsto [42, +\infty]\}$
  - $\text{Pos}(0 \leq i < 42)$
    - $\{i \mapsto [0, 42]\}$
      - $\{i \mapsto [42, 42]\}$
      - $\{i \mapsto [42, +\infty]\}$
    - $\{i \mapsto [0, +\infty]\}$
  - $\text{Neg}(0 \leq i < 42)$
    - $\{i \mapsto [0, 42]\}$
      - $\{i \mapsto [42, 42]\}$
      - $\{i \mapsto [42, +\infty]\}$
    - $\{i \mapsto [0, +\infty]\}$

- $M[a+i] = i \times 2$

- Fixed point
• Only $S = \{2\}$ identifies bounds check as superfluous
Result

- Only $S = \{2\}$ identifies bounds check as superfluous
- Only $S = \{4\}$ identifies $x = 42$ at end of program
Result

- Only $S = \{2\}$ identifies bounds check as superfluous
- Only $S = \{4\}$ identifies $x = 42$ at end of program
- We could combine the information
Result

- Only $S = \{2\}$ identifies bounds check as superfluous
- Only $S = \{4\}$ identifies $x = 42$ at end of program
- We could combine the information
  - But would be costly in general
Narrowing

- Let $\mathbf{x}$ be a solution of (1)
Narrowing

- Let \( \bar{x} \) be a solution of (1)
- I.e., \( x_i \supseteq f_i(\bar{x}) \)
Narrowing

- Let $\vec{x}$ be a solution of (1)
- I.e., $x_i \supseteq f_i(\vec{x})$
- Then, for monotonic $f_i$:
  - $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
Narrowing

- Let $\vec{x}$ be a solution of (1)
- I.e., $x_i \supseteq f_i(\vec{x})$
- Then, for monotonic $f_i$:
  - $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
    - By straightforward induction
Narrowing

- Let $\vec{x}$ be a solution of (1)
- I.e., $x_i \supseteq f_i(\vec{x})$
- Then, for monotonic $f_i$:
  - $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
    - By straightforward induction
- $\implies$ Every $F^k(\vec{x})$ is a solution of (1)!
Narrowing

• Let $\vec{x}$ be a solution of (1)
• I.e., $x_i \supseteq f_i(\vec{x})$
• Then, for monotonic $f_i$:
  • $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
    • By straightforward induction
  $\implies$ Every $F^k(\vec{x})$ is a solution of (1)!
• Narrowing iteration: Iterate until stabilization

• Narrowing iteration: Iterate until stabilization
Narrowing

• Let \( \vec{x} \) be a solution of (1)
• I.e., \( x_i \supseteq f_i(\vec{x}) \)
• Then, for monotonic \( f_i \):
  • \( \vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots \)
    • By straightforward induction
  \( \implies \) Every \( F^k(\vec{x}) \) is a solution of (1)!

• Narrowing iteration: Iterate until stabilization
  • Or some maximum number of iterations reached
    • Note: Need not stabilize within finite number of iterations
Narrowing

- Let \( \bar{x} \) be a solution of (1)
- I.e., \( x_i \supseteq f_i(\bar{x}) \)
- Then, for monotonic \( f_i \):
  - \( \bar{x} \supseteq F(\bar{x}) \supseteq F^2(\bar{x}) \supseteq \ldots \)
    - By straightforward induction
  \[ \implies \] Every \( F^k(\bar{x}) \) is a solution of (1)!

- **Narrowing iteration**: Iterate until stabilization
  - Or some maximum number of iterations reached
    - Note: Need not stabilize within finite number of iterations

- Solutions get smaller (more precise) with each iteration
Narrowing

- Let $\vec{x}$ be a solution of (1)
- I.e., $x_i \supseteq f_i(\vec{x})$
- Then, for monotonic $f_i$:
  - $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
    - By straightforward induction
  $\implies$ Every $F^k(\vec{x})$ is a solution of (1)!
- **Narrowing iteration**: Iterate until stabilization
  - Or some maximum number of iterations reached
    - Note: Need not stabilize within finite number of iterations
- Solutions get smaller (more precise) with each iteration
- Round robin/Worklist iteration also works!
Narrowing

- Let $\vec{x}$ be a solution of (1)
- I.e., $x_i \supseteq f_i(\vec{x})$
- Then, for monotonic $f_i$:
  - $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
    - By straightforward induction
  $\implies$ Every $F^k(\vec{x})$ is a solution of (1)!
- Narrowing iteration: Iterate until stabilization
  - Or some maximum number of iterations reached
    - Note: Need not stabilize within finite number of iterations
- Solutions get smaller (more precise) with each iteration
- Round robin/Worklist iteration also works!
  - Important to have only one constraint per $x_i$!
Example

- Start with over-approximation.

\[
\begin{cases}
  i \mapsto [-\infty, +\infty] \\
  i = 0
\end{cases}
\]

\[
\begin{cases}
  i \mapsto [0, +\infty] \\
  i = i + 1
\end{cases}
\]

\[
\begin{cases}
  i \mapsto [42, +\infty] \\
  \text{Neg}(i < 42)
\end{cases}
\]

\[
\begin{cases}
  i \mapsto [0, +\infty] \\
  \text{Pos}(i < 42)
\end{cases}
\]

\[
\begin{cases}
  i \mapsto [42, +\infty] \\
  \text{Neg}(0 \leq i < 42)
\end{cases}
\]

\[
\begin{cases}
  i \mapsto [0, +\infty] \\
  \text{Pos}(0 \leq i < 42)
\end{cases}
\]

\[
\begin{cases}
  M[a + i] = i \times 2 \\
  \{ i \mapsto [0, +\infty] \}
\end{cases}
\]
Example

- Start with over-approximation.

\[
\begin{align*}
\{ i \mapsto [\infty, +\infty] \} \\
\{ i \mapsto [0, +\infty] \} & \quad (i = i + 1) \\
\text{Neg}(i < 42) & \quad \text{Pos}(i < 42) \\
\{ i \mapsto [42, +\infty] \} & \quad \{ i \mapsto [0, 41] \} \\
\{ i \mapsto [0, 41] \} & \quad \{ i \mapsto [0, +\infty] \} \\
\text{Neg}(0 \leq i < 42) & \quad \text{Pos}(0 \leq i < 42) \\
\{ i \mapsto [42, +\infty] \} & \quad \{ i \mapsto [0, +\infty] \} \\
M[a+i] &= i \times 2 \\
\{ i \mapsto [0, +\infty] \}
\end{align*}
\]
Example

- Start with over-approximation.

\[
\begin{align*}
i &= 0 \\
\{i \mapsto [\infty, +\infty]\} \\
\{i \mapsto [0, +\infty]\} &\xrightarrow{i = i + 1} \{i \mapsto [0, 41]\} \\
\{i \mapsto [42, +\infty]\} &\xrightarrow{\text{Neg}(i < 42)} \{i \mapsto [0, 41]\} \\
\{i \mapsto [0, +\infty]\} &\xrightarrow{\text{Pos}(i < 42)} \{i \mapsto [0, +\infty]\} \\
\text{M}[a+i] &= i \times 2 \\
\{i \mapsto [0, +\infty]\} \\
\end{align*}
\]
Example

- Start with over-approximation.

\[
\{ i \mapsto [0, +\infty] \} \\
\{ i \mapsto [42, +\infty] \} \\
\{ i \mapsto [0, 41] \}
\]

\[
\{ i \mapsto [-\infty, +\infty] \} \\
\{ i \mapsto [0, 41] \}
\]

\[
\begin{align*}
M[a+i] & = i \times 2 \\
\{ i \mapsto [0, 41] \}
\end{align*}
\]
Example

- Start with over-approximation.

\[
\begin{align*}
\{i \mapsto [\neg\infty, +\infty]\} \\
\{i \mapsto [0, 42]\} \\
\{i \mapsto [42, +\infty]\} \\
\{i \mapsto [0, 41]\} \\
\{i \mapsto [0, 41]\} \\
\{i \mapsto [0, 41]\}
\end{align*}
\]
Example

- Start with over-approximation.

\[
\begin{align*}
\{i & \mapsto [-\infty, +\infty]\} \\
i = 0 & \\
\{i & \mapsto [0, 42]\} & i = i + 1 \\
\text{Neg}(i < 42) & \\
\{i & \mapsto [42, 42]\} & \text{Pos}(i < 42) \\
\{i & \mapsto [0, 42]\} & \\
\text{Neg}(0 \leq i < 42) & \\
\{i & \mapsto [42, 42]\} & \text{Pos}(0 \leq i < 42) \\
\{i & \mapsto [0, 41]\} & \\
M[a+i] & = i \times 2 \\
\{i & \mapsto [0, 41]\} & \\
\{i & \mapsto [0, 41]\} & \\
\bot &
\end{align*}
\]
Example

- Start with over-approximation. Stabilized

\[
\begin{align*}
&\{i \mapsto [0, 42]\} \\
&\{i \mapsto [0, 41]\} \\
&\{i \mapsto [42, 42]\} \\
&\{i \mapsto [0, 41]\}
\end{align*}
\]

\[
\begin{align*}
&\text{Neg} (i < 42) \\
&\text{Pos} (i < 42) \\
&\text{Neg} (0 \leq i < 42) \\
&\text{Pos} (0 \leq i < 42)
\end{align*}
\]

\[
\begin{align*}
&M[a+i] = i \times 2 \\
&\{i \mapsto [0, 41]\}
\end{align*}
\]
Discussion

- Not necessary to find good loop separator
Discussion

- Not necessary to find good loop separator
- In our example, it even stabilizes
Discussion

- Not necessary to find good loop separator
- In our example, it even stabilizes
  - Otherwise: Limit number of iterations
Discussion

- Not necessary to find good loop separator
- In our example, it even stabilizes
  - Otherwise: Limit number of iterations
- Narrowing makes solution more precise in each step
Discussion

• Not necessary to find good loop separator
• In our example, it even stabilizes
  • Otherwise: Limit number of iterations
• Narrowing makes solution more precise in each step
• Question: Do we have to accept possible nontermination/large number of iterations?
Accelerated narrowing

- Let $\vec{x} \sqsubseteq F(\vec{x})$ be solution of (1)
Accelerated narrowing

- Let $\vec{x} \sqsupseteq F(\vec{x})$ be solution of (1)
- Consider function $H : \vec{x} \mapsto \vec{x} \cap F(\vec{x})$
Accelerated narrowing

- Let $\vec{x} \sqsupseteq F(\vec{x})$ be solution of (1)
- Consider function $H : \vec{x} \mapsto \vec{x} \sqcap F(\vec{x})$
- For monotonic $F$, we have $\vec{x} \sqsupseteq F(\vec{x}) \sqsupseteq F^2(\vec{x}) \sqsupseteq \ldots$
Accelerated narrowing

- Let \( \vec{x} \supseteq F(\vec{x}) \) be solution of (1)
- Consider function \( H : \vec{x} \mapsto \vec{x} \cap F(\vec{x}) \)
- For monotonic \( F \), we have \( \vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots \)
  - and thus \( H^k(\vec{x}) = F^k(\vec{x}) \)
Accelerated narrowing

- Let $\vec{x} \supseteq F(\vec{x})$ be solution of (1)
- Consider function $H : \vec{x} \mapsto \vec{x} \sqcap F(\vec{x})$
- For monotonic $F$, we have $\vec{x} \supseteq F(\vec{x}) \supseteq F^2(\vec{x}) \supseteq \ldots$
  - and thus $H^k(\vec{x}) = F^k(\vec{x})$
- Now regard $I : (\vec{x}) \mapsto \vec{x} \sqcap F(\vec{x})$, where
Accelerated narrowing

- Let $\vec{x} \sqsupseteq F(\vec{x})$ be solution of (1)
- Consider function $H : \vec{x} \mapsto \vec{x} \sqcap F(\vec{x})$
- For monotonic $F$, we have $\vec{x} \sqsupseteq F(\vec{x}) \sqsupseteq F^2(\vec{x}) \sqsupseteq \ldots$
  - and thus $H^k(\vec{x}) = F^k(\vec{x})$
- Now regard $I : (\vec{x}) \mapsto \vec{x} \sqcap F(\vec{x})$, where
- $\sqcap$: Narrowing operator, whith
  1. $x \sqcap y \sqsubseteq x \sqcap y \sqsubseteq x$
  2. For every sequence $a_0, a_1, \ldots$, the (down)chain $b_0 = a_0$, $b_{i+1} = b_i \sqcap a_{i+1}$ eventually stabilizes
Accelerated narrowing

- Let $\tilde{x} \supseteq F(\tilde{x})$ be solution of (1)
- Consider function $H : \tilde{x} \mapsto \tilde{x} \cap F(\tilde{x})$
- For monotonic $F$, we have $\tilde{x} \supseteq F(\tilde{x}) \supseteq F^2(\tilde{x}) \supseteq \ldots$
  - and thus $H^k(\tilde{x}) = F^k(\tilde{x})$
- Now regard $I : (\tilde{x}) \mapsto \tilde{x} \cap F(\tilde{x})$, where
- $\sqcap$: Narrowing operator, whith
  1. $x \sqcap y \subseteq x \sqcap y \subseteq x$
  2. For every sequence $a_0, a_1, \ldots$, the (down)chain $b_0 = a_0, b_{i+1} = b_i \sqcap a_{i+1}$ eventually stabilizes
- We have: $I^k(\tilde{x}) \supseteq H^k(\tilde{x}) = F^k(\tilde{x}) \supseteq F^{k+1}(\tilde{x})$.
  - I.e., $I^k(\tilde{x})$ greater (valid approx.) than a solution.
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \sqcap [l_2, u_2] := [l, u]\), where

\[
\begin{align*}
l &= \begin{cases} 
  l_2 & \text{if } l_1 = -\infty \\
  l_1 & \text{otherwise}
\end{cases} \\
u &= \begin{cases} 
  u_2 & \text{if } u_1 = \infty \\
  u_1 & \text{otherwise}
\end{cases}
\end{align*}
\]
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \cap [l_2, u_2] := [l, u],\) where

\[
\begin{align*}
l &:= \begin{cases} l_2 & \text{if } l_1 = -\infty \\
l_1 & \text{otherwise} \end{cases} \\
u &:= \begin{cases} u_2 & \text{if } u_1 = \infty \\
u_1 & \text{otherwise} \end{cases}
\end{align*}
\]

- Check:
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \cap [l_2, u_2] := [l, u]\), where

\[
\begin{align*}
l &:= \begin{cases} 
  l_2 & \text{if } l_1 = -\infty \\
  l_1 & \text{otherwise}
\end{cases} \\
u &:= \begin{cases} 
  u_2 & \text{if } u_1 = \infty \\
  u_1 & \text{otherwise}
\end{cases}
\end{align*}
\]

- Check:
  - \([l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1]

- \(\cap\) is not commutative

- For our example: Same result as non-accelerated narrowing!
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \cap [l_2, u_2] := [l, u]\), where

\[
\begin{align*}
l & := \begin{cases} 
l_2 & \text{if } l_1 = -\infty \\
l_1 & \text{otherwise}
\end{cases} \\
u & := \begin{cases} 
u_2 & \text{if } u_1 = \infty \\
u_1 & \text{otherwise}
\end{cases}
\end{align*}
\]

- Check:
  - \([l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1]
  - Stabilizes after at most two narrowing steps

- \(\cap\) is not commutative
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \cap [l_2, u_2] := [l, u]\), where

\[
l := \begin{cases} 
  l_2 & \text{if } l_1 = -\infty \\
  l_1 & \text{otherwise}
\end{cases}
\]

\[
u := \begin{cases} 
  u_2 & \text{if } u_1 = \infty \\
  u_1 & \text{otherwise}
\end{cases}
\]

- Check:
  - \([l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1]\)
  - Stabilizes after at most two narrowing steps

- \(\cap\) is not commutative
For interval analysis

- Preserve (finite) interval bounds: \([l_1, u_1] \cap [l_2, u_2] := [l, u]\), where

\[
    l := \begin{cases} 
        l_2 & \text{if } l_1 = -\infty \\
        l_1 & \text{otherwise}
    \end{cases}
\]

\[
    u := \begin{cases} 
        u_2 & \text{if } u_1 = \infty \\
        u_1 & \text{otherwise}
    \end{cases}
\]

- Check:
  - \([l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1] \cap [l_2, u_2] \subseteq [l_1, u_1]\)
  - Stabilizes after at most two narrowing steps

- \(\cap\) is not commutative

- For our example: Same result as non-accelerated narrowing!
Discussion

- Narrowing only works for monotonic functions
  - Widening worked for all functions
Discussion

- Narrowing only works for monotonic functions
  - Widening worked for all functions
- Accelerated narrowing can be iterated until stabilization
Discussion

- Narrowing only works for monotonic functions
  - Widening worked for all functions
- Accelerated narrowing can be iterated until stabilization
- However: Design of good widening/narrowing remains black magic
Last Lecture

- Interval analysis (ctd)
  - Abstract values: Intervals $[l, u]$ with $l \leq u$, $l \in \mathbb{Z}_{-\infty}$, $u \in \mathbb{Z}^{+\infty}$
  - Abstract operators: Interval arithmetic
Last Lecture

• Interval analysis (ctd)
  • Abstract values: Intervals \([l, u]\) with \(l \leq u\), \(l \in \mathbb{Z}_{-\infty}\), \(u \in \mathbb{Z}^{+\infty}\)
  • Abstract operators: Interval arithmetic

• Main problem: Infinite ascending chains
  • Analysis not guaranteed to terminate

• Widening: Accelerate convergence by over-approximating join
  • Here: Update interval bounds to \(-\infty / +\infty\)

• Problem: makes analysis imprecise

• Idea 1: Widening only at loop separators
• Idea 2: Narrowing

• FP-Iteration on solution preserves solution
  • But may make it smaller

• Accelerated narrowing:
  • Use narrowing operator for update, that lies “in between” \(\sqcap\) and original value
  • ... and converges within finite time
  • Here: Keep finite interval bounds
Last Lecture

- Interval analysis (ctd)
  - Abstract values: Intervals \([l, u]\) with \(l \leq u\), \(l \in \mathbb{Z}_{-\infty}\), \(u \in \mathbb{Z}^{+\infty}\)
  - Abstract operators: Interval arithmetic
- Main problem: Infinite ascending chains
  - Analysis not guaranteed to terminate
- Widening: Accelerate convergence by over-approximating join
  - Here: Update interval bounds to \(-\infty/\infty\)
Last Lecture

• Interval analysis (ctd)
  • Abstract values: Intervals $[l, u]$ with $l \leq u$, $l \in \mathbb{Z}_{-\infty}$, $u \in \mathbb{Z}^{+\infty}$
  • Abstract operators: Interval arithmetic

• Main problem: Infinite ascending chains
  • Analysis not guaranteed to terminate

• Widening: Accelerate convergence by over-approximating join
  • Here: Update interval bounds to $-\infty/+\infty$

• Problem: makes analysis imprecise
  • Idea 1: Widening only at loop separators
  • Idea 2: Narrowing
    • FP-Iteration on solution preserves solution
    • But may make it smaller

  • Accelerated narrowing:
    • Use narrowing operator for update, that lies “in between” $\sqcap$ and original value
      • ... and converges within finite time
      • Here: Keep finite interval bounds
Recipe: Abstract Interpretation (I)

- Define **abstract value domain** $\mathbb{A}$, with partial order $\sqsubseteq$
  - $\sqsubseteq$ must be **totally defined** ($\sqsubseteq$ need not always exists)
- Define **description relation between values**: $\Delta \subseteq \mathbb{Z} \times \mathbb{A}$
  - Show: **Monotonicity**: $\forall a_1 \sqsubseteq a_2, \nu. \nu \Delta a_1 \implies \nu \Delta a_2$
  - Standard: Lift to valuations ($\text{Reg} \rightarrow \mathbb{A}$), domain ($\mathbb{D} := (\text{Reg} \rightarrow \mathbb{A}) \cup \{\bot\}$)
- Define **abstract operators** $\nu^\#: \mathbb{A}$, $\square^\# : \mathbb{A} \times \mathbb{A} \rightarrow \mathbb{A}$, etc.
  - Show soundness wrt. concrete ones:
    \[
    \forall c \in \mathbb{Z}. \nu \Delta \nu^#
    \]
    \[
    \forall \nu_1, \nu_2 \in \mathbb{Z}, d_1, d_2 \in \mathbb{A}. \nu_1 \Delta d_1 \land \nu_2 \Delta d_2 \implies \nu_1 \square \nu_2 \Delta d_1 \square^# d_2
    \]
  - For free: $\rho \Delta \rho^# \implies \llbracket e \rrbracket \rho \Delta \llbracket e \rrbracket^# \rho^#$
- Define **transformation** $\text{tr} :: \text{Act} \times \mathbb{D} \rightarrow \text{Act}$
  - Show correctness: $(\rho, \mu) \Delta d \implies \llbracket a \rrbracket (\rho, \mu) = \llbracket \text{tr}(a, d) \rrbracket (\rho, \mu)$
- Define **abstract effects** $\llbracket \cdot \rrbracket^# : \text{Act} \rightarrow \mathbb{D} \rightarrow \mathbb{D}$, initial value $d_0 \in \mathbb{D}$
  - Usually: Creativity only required on Pos,Neg
  - Show: **Monotonicity**: $\forall d_1 \sqsubseteq d_2, a. \llbracket a \rrbracket^# d_1 \sqsubseteq \llbracket a \rrbracket^# d_2$ and simulation:
    \[
    \forall \rho, \mu. (\rho, \mu) \Delta d_0
    \]
    \[
    \forall (\rho, \mu) \in \text{dom}(\llbracket a \rrbracket), d. (\rho, \mu) \Delta d \implies \llbracket a \rrbracket (\rho, \mu) \Delta \llbracket a \rrbracket^# d
    \]
Recipe: Abstract Interpretation (II)

- Check finite chain height of domain
  - Finite: Done
  - Infinite (or too high)
    - Define widening, narrowing operator
Short recapture of methods so far

- Operational semantics on flowgraphs
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.

- Collecting semantics:

- Program analysis

- Abstract description of

- Forward: States reachable at \( u \)

- Backward: Executions leaving \( u \)

- Abstract effects of edges:
  - Must be compatible with concrete effects
  - Forward: Simulation; Backward: Also (kind of) simulation

- MOP \( [u] \)
  - Abstract effects reachable at \( u \)

- Special case: abstract interpretation — domain describes abstract values

- Transformation: Must be compatible with states/leaving paths described by abstract effects

- Computing analysis result
  - Constraint system. For monotonic abstract effects. Precise if distributive.
  - Solving algorithms: Naive iteration, RR-iteration, worklist algorithm
  - Forcing convergence: Widening, Narrowing
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$. 

Program analysis

- Abstract description of

  - Forward: States reachable at $u$
  - Backward: Executions leaving $u$

Abstract effects of edges:

  - Must be compatible with concrete effects
  - Forward: Simulation; Backward: Also (kind of) simulation

MOP $[u]$ — Abstract effects reachable at $u$

- Special case: abstract interpretation — domain describes abstract values

Transformation: Must be compatible with states/leaving paths described by abstract effects

Computing analysis result

- Constraint system. For monotonic abstract effects. Precise if distributive.
- Solving algorithms: Naive iteration, RR-iteration, worklist algorithm

Forcing convergence: Widening, Narrowing
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: \([u]\) — States reachable at \(u\).
- Program analysis
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $\llbracket u \rrbracket$ — States reachable at $u$.
- Program analysis
  - Abstract description of

\[ \llbracket \] — States reachable at $u$.\]
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $\llbracket u \rrbracket$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $\llbracket u \rrbracket$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: \([u]\) — States reachable at \(u\).

- Program analysis
  - Abstract description of
    - Forward: States reachable at \(u\)
    - Backward: Executions leaving \(u\)
  - Abstract effects of edges:
    - Must be compatible with concrete effects
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $\llbracket u \rrbracket$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $\mathbb{[u]}$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[u]$ — Abstract effects reachable at $u$
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP[$u$] — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[u]$ — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values

- Transformation: Must be compatible with states/leaving paths described by abstract effects
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[u]$ — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values

- Transformation: Must be compatible with states/leaving paths described by abstract effects

- Computing analysis result
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[u]$ — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values

- Transformation: Must be compatible with states/leaving paths described by abstract effects

- Computing analysis result
  - Constraint system. For monotonic abstract effects. Precise if distributive.
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[u]$ — States reachable at $u$.

- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[u]$ — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values

- Transformation: Must be compatible with states/leaving paths described by abstract effects

- Computing analysis result
  - Constraint system. For monotonic abstract effects. Precise if distributive.
  - Solving algorithms: Naive iteration, RR-iteration, worklist algorithm
Short recapture of methods so far

- Operational semantics on flowgraphs
  - Edges have effect on states. Extend to paths.
  - Collecting semantics: $[[u]]$ — States reachable at $u$.
- Program analysis
  - Abstract description of
    - Forward: States reachable at $u$
    - Backward: Executions leaving $u$
  - Abstract effects of edges:
    - Must be compatible with concrete effects
    - Forward: Simulation; Backward: Also (kind of) simulation
  - MOP$[[u]]$ — Abstract effects reachable at $u$
  - Special case: abstract interpretation — domain describes abstract values
- Transformation: Must be compatible with states/leaving paths described by abstract effects
- Computing analysis result
  - Constraint system. For monotonic abstract effects. Precise if distributive.
  - Solving algorithms: Naive iteration, RR-iteration, worklist algorithm
- Forcing convergence: Widening, Narrowing
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D \iff \forall x \in D, \nu. \llbracket \pi \rrbracket (\rho(x := \nu), \mu) = \llbracket \pi \rrbracket (\rho, \mu)\)
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \nu. \llbracket \pi \rrbracket (\rho(x := \nu), \mu) = \llbracket \pi \rrbracket (\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \in \Delta D_0\)
  2. \([a](\rho, \mu), \pi \Delta D \implies (\rho, \mu), a\pi \Delta [a]# D\)
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \nu. \llbracket \pi \rrbracket (\rho(x := \nu), \mu) = \llbracket \pi \rrbracket (\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \in \Delta D_0\)
  2. \([a](\rho, \mu), \pi \Delta D \implies (\rho, \mu), a\pi \Delta [a]^{\#} D\)
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \Delta [\pi]^{\#} D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \nu. \llbracket \pi \rrbracket (\rho(x := \nu), \mu) = \llbracket \pi \rrbracket (\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \in \Delta D_0\)
  2. \([a]\)(\rho, \mu), \pi \Delta D \implies (\rho, \mu), a\pi \Delta [a] \# D
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \Delta [\pi] \# D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).

\[
\left(\rho_n, \mu_n\right), \in \\
\quad \Delta \\
\quad \Delta \\
D_0
\]
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \triangle D\) iff \(\forall x \in D, v. \llbracket \pi \rrbracket (\rho(x := v), \mu) = \llbracket \pi \rrbracket (\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \varepsilon \triangle D_0\)
  2. \([a](\rho, \mu), \pi \triangle D \implies (\rho, \mu), a\pi \triangle [a]\#D\)
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \triangle \llbracket \pi \rrbracket \# D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).

\[
\begin{align*}
(\rho_{n-1}, \mu_{n-1}), a &\rightarrow (\rho_n, \mu_n), \varepsilon \\
D_1 &\leftarrow [a]\# D_0 \quad \Delta
\end{align*}
\]
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \forall v. \llbracket \pi \rrbracket(\rho(x := v), \mu) = \llbracket \pi \rrbracket(\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \varepsilon \Delta D_0\)
  2. \([a]\)(\rho, \mu), \pi \Delta D \implies (\rho, \mu), a\pi \Delta \llbracket a \rrbracket \# D
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \Delta \llbracket \pi \rrbracket \# D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).

\[
\begin{array}{c}
(\rho_{n-1}, \mu_{n-1}), a \xrightarrow{[a]} (\rho_n, \mu_n), \varepsilon \\
\Delta \\
D_1 \leftarrow D_0 \xrightarrow{[a]\#} \Delta
\end{array}
\]
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \nu. \llbracket \pi \rrbracket(\rho(x := \nu), \mu) = \llbracket \pi \rrbracket(\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \varepsilon \Delta D_0\)
  2. \([a] \rho, \mu, \pi \Delta D \implies (\rho, \mu), a\pi \Delta [a]\# D\)
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \Delta [\pi]\# D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).

\[
\cdots \longrightarrow (\rho_{n-1}, \mu_{n-1}), a \longrightarrow (\rho_n, \mu_n), \varepsilon
\]

\[
\begin{array}{cc}
\Delta & \Delta \\
\end{array}
\]

\[
\begin{array}{c}
\cdots \\
D_1 \\
\end{array} \quad [a]# 
\begin{array}{c}
D_0 \\
\end{array}
\]
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - $(\rho, \mu), \pi \Delta D$ iff $\forall x \in D, \forall. \llbracket \pi \rrbracket (\rho(x := \nu), \mu) = \llbracket \pi \rrbracket (\rho, \mu)$
- Proof obligations
  1. $(\rho, \mu), \varepsilon \Delta D_0$
  2. $\llbracket a \rrbracket (\rho, \mu) \Delta D \implies (\rho, \mu), a\pi \Delta \llbracket a \rrbracket # D$
- Yields: $\forall \rho, \mu. (\rho, \mu), \pi \Delta \llbracket \pi \rrbracket # D_0$
  - Note: Could even restrict to reachable states $\rho, \mu$.

\[
(\rho_0, \mu_0), \pi \rightarrow \cdots \rightarrow (\rho_{n-1}, \mu_{n-1}), a \rightarrow (\rho_n, \mu_n), \varepsilon
\]
Remark: Simulation (Backwards)

- Describe execution to end node (state, path)
- Dead variables: Execution does not depend on dead variables
  - \((\rho, \mu), \pi \Delta D\) iff \(\forall x \in D, \pi. [\pi](\rho(x := v), \mu) = [\pi](\rho, \mu)\)
- Proof obligations
  1. \((\rho, \mu), \varepsilon \Delta D_0\)
  2. \([a](\rho, \mu), \pi \Delta D \implies (\rho, \mu), a\pi \Delta [a]# D\)
- Yields: \(\forall \rho, \mu. (\rho, \mu), \pi \Delta [\pi]# D_0\)
  - Note: Could even restrict to reachable states \(\rho, \mu\).

\[
(\rho_0, \mu_0), \pi \rightarrow \cdots \rightarrow (\rho_{n-1}, \mu_{n-1}), a [a] \rightarrow (\rho_n, \mu_n), \varepsilon
\]
<table>
<thead>
<tr>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
</tbody>
</table>
Motivation

- Want to consider memory
Motivation

- Want to consider memory
- E.g. $M[y] = 5; \ x = M[y] + 1 \rightarrow M[y] = 5; \ x=6$
Motivation

• Want to consider memory

E.g. \( M[y] = 5; \ x = M[y] + 1 \mapsto M[y] = 5; \ x=6 \)

• Here: Assume analyzed program is the only one who accesses memory
Motivation

- Want to consider memory
- E.g. $M[y] = 5; \ x = M[y] + 1 \mapsto M[y] = 5; \ x=6$
- Here: Assume analyzed program is the only one who accesses memory
  - In reality: Shared variables (interrupts, threads), DMA, memory-mapped hardware, ...
Motivation

- Want to consider memory
- E.g. \[ M[y] = 5; \ x = M[y] + 1 \mapsto M[y] = 5; \ x=6 \]
- Here: Assume analyzed program is the only one who accesses memory
  - In reality: Shared variables (interrupts, threads), DMA, memory-mapped hardware, ...
  - Compilers provide, e.g., volatile annotation
First Attempt

- Available expressions:
  - Memorize loads: Load: \( x = M[e] \mapsto \{ T_{M[e]} = M[e] ; \ x = T_{M[e]} \} \)
  - Effects

\[
\begin{align*}
[T_e = e] \# A &= [A] \# \cup \{ e \} \\
[T_{M[e]} = M[e]] \# A &= [A] \# \cup \{ M[e] \} \\
[x = e] \# A &= [A] \# \setminus \text{Expr}_x \\
[M[e_1] = e_2] \# A &= [A] \# \setminus \text{loads}
\end{align*}
\]
First Attempt

- Available expressions:
  - Memorize loads: Load: \( x = M[e] \mapsto \{ T_{M[e]} = M[e]; \ x = T_{M[e]} \} \)
  - Effects

\[
\]

\[
\]

- Problem: Need to be conservative on store
  - Store destroys all information about memory
Constant propagation

- Apply constant propagation to addresses?
Constant propagation

- Apply constant propagation to addresses?
- Exact addresses not known at compile time
Constant propagation

- Apply constant propagation to addresses?
- Exact addresses not known at compile time
- Usually, different addresses accessed at same program point
Constant propagation

- Apply constant propagation to addresses?
- Exact addresses not known at compile time
- Usually, different addresses accessed at same program point
  - E.g., iterate over array
Constant propagation

- Apply constant propagation to addresses?
- Exact addresses not known at compile time
- Usually, different addresses accessed at same program point
  - E.g., iterate over array
- Storing at unknown address destroys all information
Last Lecture

- Motivation to consider memory
  - Alias analysis required!
- Changing the semantics of memory
  - Pointers to start of blocks, indexing within blocks
  - No pointer arithmetic
  - Some assumptions about program correctness: Semantics undefined if
    - Program accesses address that has not been allocated
    - Indexes block out of bounds
    - Computes with addresses
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)

- Semantics
  - Value: \( \text{Val} = \mathbb{Z}^\sigma \cup \text{Addr} \)
  - Integer values and block addresses
  - Memory described by \( \mu \): \( \text{Addr} \mapsto \mathbb{Z} \mapsto \text{Val} \)
    - Maps addresses of blocks to arrays of values
    - \( \mapsto \) partial function (Not all addresses/indexes are valid)
  - Assumption: Type correct
  - In reality: Type system

  We write \( \text{null} \) and 0 synonymously
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)

- Semantics
  - Value: \( \text{Val} = \mathbb{Z} \cup \text{Addr} \)
    - Integer values and block addresses
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)

- Semantics
  - Value: \( \text{Val} = \mathbb{Z} \cup \text{Addr} \)
    - Integer values and block addresses
  - Memory described by \( \mu: \text{Addr} \rightarrow \mathbb{Z} \rightarrow \text{Val} \)
    - Maps addresses of blocks to arrays of values
    - \( \rightarrow - \) partial function (Not all addresses/indexes are valid)
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)

- Semantics
  - Value: \( \text{Val} = \mathbb{Z} \cup \text{Addr} \)
    - Integer values and block addresses
  - Memory described by \( \mu : \text{Addr} \rightarrow \mathbb{Z} \rightarrow \text{Val} \)
    - Maps addresses of blocks to arrays of values
    - \( \rightarrow \) - partial function (Not all addresses/indexes are valid)
  - Assumption: Type correct
    - In reality: Type system
Extending semantics by blocked memory

- Organize memory into blocks
  - \( p = \text{new}(e) \) allocates new block of size \( e \)
  - \( x = p[e] \) loads cell \( e \) from block \( p \)
  - \( p[e_1] = e_2 \) writes cell \( e_1 \) from block \( p \)

- Semantics
  - Value: \( \text{Val} = \mathbb{Z} \uplus \text{Addr} \)
    - Integer values and block addresses
  - Memory described by \( \mu : \text{Addr} \rightarrow \mathbb{Z} \rightarrow \text{Val} \)
    - Maps addresses of blocks to arrays of values
    - \( \rightarrow \) partial function (Not all addresses/indexes are valid)
  - Assumption: Type correct
    - In reality: Type system
  - We write \text{null} and 0 synonymously
Semantics

\[\llbracket \text{Nop}\rrbracket (\rho, \mu) = (\rho, \mu)\]
\[\llbracket x = e \rrbracket (\rho, \mu) = (\rho(x \mapsto \llbracket e \rrbracket \rho), \mu)\]
\[\llbracket \text{Pos}(e) \rrbracket (\rho, \mu) = \llbracket e \rrbracket \rho \neq 0? (\rho, \mu) : \text{undefined}\]
\[\llbracket \text{Neg}(e) \rrbracket (\rho, \mu) = \llbracket e \rrbracket \rho = 0? (\rho, \mu) : \text{undefined}\]
\[\llbracket x = p[e] \rrbracket (\rho, \mu) = (\rho(x \mapsto \mu(\llbracket p \rrbracket \rho, \llbracket e \rrbracket \rho)), \mu)\]
\[\llbracket p[e_1] = e_2 \rrbracket (\rho, \mu) = (\rho, \mu(\llbracket p \rrbracket \rho, \llbracket e_1 \rrbracket \rho) \mapsto \llbracket e_2 \rrbracket \rho)\]
\[\llbracket x = \text{new}(e) \rrbracket (\rho, \mu) = (\rho(x \mapsto a), \mu(a \mapsto (i \mapsto 0 \mid 0 \leq i < \llbracket e \rrbracket \rho))) \quad a \notin \text{dom(\mu)}\]

- New initializes the block
Semantics

\[
\begin{align*}
\llbracket \text{Nop} \rrbracket (\rho, \mu) &= (\rho, \mu) \\
\llbracket x = e \rrbracket (\rho, \mu) &= (\rho(x \mapsto \llbracket e \rrbracket \rho), \mu) \\
\llbracket \text{Pos}(e) \rrbracket (\rho, \mu) &= \llbracket e \rrbracket \rho \neq 0?(\rho, \mu) : \text{undefined} \\
\llbracket \text{Neg}(e) \rrbracket (\rho, \mu) &= \llbracket e \rrbracket \rho = 0?(\rho, \mu) : \text{undefined} \\
\llbracket x = p[e] \rrbracket (\rho, \mu) &= (\rho(x \mapsto \mu(\llbracket p \rrbracket \rho, \llbracket e \rrbracket \rho)), \mu) \\
\llbracket p[e_1] = e_2 \rrbracket (\rho, \mu) &= (\rho, \mu(\llbracket p \rrbracket \rho, \llbracket e_1 \rrbracket \rho) \mapsto \llbracket e_2 \rrbracket \rho) \\
\llbracket x = \text{new}(e) \rrbracket (\rho, \mu) &= (\rho(x \mapsto a), \mu(a \mapsto (i \mapsto 0 \mid 0 \leq i < \llbracket e \rrbracket \rho))) \quad a \notin \text{dom}(\mu)
\end{align*}
\]

- New initializes the block
  - Java: OK, C/C++: ???
Semantics

\[ \lbrack \text{Nop} \rbrack (\rho, \mu) = (\rho, \mu) \]
\[ \lbrack x = e \rbrack (\rho, \mu) = (\rho(x \mapsto [e] \rho), \mu) \]
\[ \lbrack \text{Pos}(e) \rbrack (\rho, \mu) = \lbrack e \rbrack \rho \neq 0? (\rho, \mu) : \text{undefined} \]
\[ \lbrack \text{Neg}(e) \rbrack (\rho, \mu) = \lbrack e \rbrack \rho = 0? (\rho, \mu) : \text{undefined} \]
\[ \lbrack x = p[e] \rbrack (\rho, \mu) = (\rho(x \mapsto \mu([p] \rho, [e] \rho)), \mu) \]
\[ \lbrack p[e_1] = e_2 \rbrack (\rho, \mu) = (\rho, \mu([p] \rho, [e_1] \rho) \mapsto [e_2] \rho) \]
\[ \lbrack x = \text{new}(e) \rbrack (\rho, \mu) = (\rho(x \mapsto a), \mu(a \mapsto (i \mapsto 0 \mid 0 \leq i < \lbrack e \rbrack \rho))) \quad a \not\in \text{dom}(\mu) \]

- New initializes the block
  - Java: OK, C/C++: ???
- Assume that only valid addresses are used
  - Otherwise, we formally get undefined
Semantics

\[ \begin{align*}
\llbracket \text{Nop} \rrbracket (\rho, \mu) &= (\rho, \mu) \\
\llbracket x = e \rrbracket (\rho, \mu) &= (\rho(x \mapsto \llbracket e \rrbracket \rho), \mu) \\
\llbracket \text{Pos}(e) \rrbracket (\rho, \mu) &= \llbracket e \rrbracket \rho \neq 0 ? (\rho, \mu) : \text{undefined} \\
\llbracket \text{Neg}(e) \rrbracket (\rho, \mu) &= \llbracket e \rrbracket \rho = 0 ? (\rho, \mu) : \text{undefined} \\
\llbracket x = p[e] \rrbracket (\rho, \mu) &= (\rho(x \mapsto \mu(\llbracket p \rrbracket \rho, \llbracket e \rrbracket \rho)), \mu) \\
\llbracket p[e_1] = e_2 \rrbracket (\rho, \mu) &= (\rho, \mu(\llbracket p \rrbracket \rho, \llbracket e_1 \rrbracket \rho) \mapsto \llbracket e_2 \rrbracket \rho) \\
\llbracket x = \text{new}(e) \rrbracket (\rho, \mu) &= (\rho(x \mapsto a), \mu(a \mapsto (i \mapsto 0 \mid 0 \leq i < \llbracket e \rrbracket \rho))) \quad a \not\in \text{dom}(\mu)
\end{align*} \]

- New initializes the block
  - Java: OK, C/C++: ???
- Assume that only valid addresses are used
  - Otherwise, we formally get undefined
- Assume that no arithmetic on addresses is done
Semantics

\[
\begin{align*}
\sem{\text{Nop}}(\rho, \mu) &= (\rho, \mu) \\
\sem{x = e}(\rho, \mu) &= (\rho(x \mapsto \sem{e}_\rho), \mu) \\
\sem{\text{Pos}(e)}(\rho, \mu) &= \sem{e}_\rho \neq 0?(\rho, \mu) : \text{undefined} \\
\sem{\text{Neg}(e)}(\rho, \mu) &= \sem{e}_\rho = 0?(\rho, \mu) : \text{undefined} \\
\sem{x = p[e]}(\rho, \mu) &= (\rho(x \mapsto \mu([p]_\rho, \sem{e}_\rho)), \mu) \\
\sem{p[e_1] = e_2}(\rho, \mu) &= (\rho, \mu([p]_\rho, \sem{e_1}_\rho) \mapsto \sem{e_2}_\rho) \\
\sem{x = \text{new}(e)}(\rho, \mu) &= (\rho(x \mapsto a), \mu(a \mapsto (i \mapsto 0 \mid 0 \leq i < \sem{e}_\rho))) \quad a \notin \text{dom}(\mu)
\end{align*}
\]

- New initializes the block
  - Java: OK, C/C++: ???
- Assume that only valid addresses are used
  - Otherwise, we formally get undefined
- Assume that no arithmetic on addresses is done
- Assume infinite supply of addresses
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated
- This is irrelevant, consider e.g.
  \[ x = \text{new}(4); \ y = \text{new}(4) \quad \text{and} \quad y = \text{new}(4); \ x = \text{new}(4) \]
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated
- This is irrelevant, consider e.g.
  \[ x = \text{new}(4); \ y = \text{new}(4) \quad \text{and} \quad y = \text{new}(4); \ x = \text{new}(4) \]
  - Programs should be equivalent
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated.
- This is irrelevant, consider e.g.:
  \[ x = \text{new}(4); \ y = \text{new}(4) \quad \text{and} \quad y = \text{new}(4); \ x = \text{new}(4) \]
  - Programs should be equivalent.
  - Although memory manager would probably assign different physical addresses.
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated
- This is irrelevant, consider e.g.
  \[
  x = \texttt{new}(4); \quad y = \texttt{new}(4) \quad \text{and} \quad y = \texttt{new}(4); \quad x = \texttt{new}(4)
  \]
  - Programs should be equivalent
  - Although memory manager would probably assign different physical addresses
- Two states \((\rho, \mu)\) and \((\rho', \mu')\) are considered equivalent, iff they are equivalent up to permutation of addresses
  - We write \((\rho, \mu) \equiv (\rho', \mu')\)
Equivalence

- Note: Semantics does not clearly specify how addresses are allocated
- This is irrelevant, consider e.g.
  \[x = \text{new}(4); \ y = \text{new}(4) \quad \text{and} \quad y = \text{new}(4); \ x = \text{new}(4)\]
  - Programs should be equivalent
  - Although memory manager would probably assign different physical addresses
- Two states \((\rho, \mu)\) and \((\rho', \mu')\) are considered equivalent, iff they are equivalent up to permutation of addresses
  - We write \((\rho, \mu) \equiv (\rho', \mu')\)
- Note: To avoid this nondeterminism in semantics:
  - Choose \texttt{Addr} to be totally ordered
  - Always take the smallest free address
Examples

• Building the linked list [1, 2]

\[
\begin{align*}
  p_1 &= \text{new (2)} \\
  p_2 &= \text{new (2)} \\
  p_1[0] &= 1 \\
  p_1[1] &= p_2 \\
  p_2[0] &= 2 \\
  p_2[1] &= \text{null}
\end{align*}
\]
Examples

- List reversal

```java
R = null
while (T != null) {
    H = T
    T = T[0]
    H[0] = R
    H[0] = R
    R = H
}
```
Examples

- List reversal

```java
R = null
while (T != null) {
    H = T
    T = T[0]
    H[0] = R
    H[0] = R
    R = H
}
```

- Sketch algorithm on whiteboard
Alias analysis

- **May alias**: May two pointers point to the same address
  - On store: Only destroy information for addresses that may alias with stored address
Alias analysis

- **May alias**: May two pointers point to the same address
  - On store: Only destroy information for addresses that may alias with stored address
- **Must alias**: Must two pointers point to the same address
  - If so, store to one can update information for the other
Alias analysis

- May alias: May two pointers point to the same address
  - On store: Only destroy information for addresses that may alias with stored address
- Must alias: Must two pointers point to the same address
  - If so, store to one can update information for the other
- Here: Focus on may-alias
  - Important to limit the destructive effect of memory updates
  - Must alias: Usually only done in local scope, by, e.g., copy propagation
First Idea

- Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  - Use start node of edge in CFG to identify allocation site
  - Abstract values $\text{Addr}^# = V$, $\text{Val}^# = 2^{\text{Addr}^#}$ (Possible targets for pointer)
  - Domain: $(\text{Reg} \to \text{Val}^#) \times (\text{Addr}^# \to \text{Val}^#)$

- Effects

  \[
  \begin{align*}
  \llbracket \_, x = y, \_ \rrbracket^#(R, M) &= (R(x \mapsto R(y)), M) & &\text{for } y \in \text{Reg} \\
  \llbracket \_, x = e, \_ \rrbracket^#(R, M) &= (R(x \mapsto \emptyset), M) & &\text{for } e \notin \text{Reg} \\
  \llbracket u, x = \text{new}(e), v \rrbracket^#(R, M) &= (R(x \mapsto \{u\}), M) \\
  \llbracket \_, x = p[e], \_ \rrbracket^#(R, M) &= (R(x \mapsto \bigcup \{M[a] \mid a \in R[p]\}), M) \\
  \llbracket \_, p[e_1] = y, \_ \rrbracket^#(R, M) &= (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p))) & &\text{for } y \in \text{Reg} \\
  \llbracket \_, p[e_1] = e, \_ \rrbracket^#(R, M) &= (R, M) & &\text{for } e \notin \text{Reg}
  \end{align*}
  \]
First Idea

- Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  - Use start node of edge in CFG to identify allocation site
  - Abstract values $\text{Addr}^\# = V$, $\text{Val}^\# = 2^{\text{Addr}^\#}$ (Possible targets for pointer)
  - Domain: $(\text{Reg} \rightarrow \text{Val}^\#) \times (\text{Addr}^\# \rightarrow \text{Val}^\#)$

- Effects

  \[ \ldots \]

  \[
  \llbracket _, x = y, _\rrbracket^\#(R, M) = (R(x \mapsto R(y)), M) \quad \text{for } y \in \text{Reg}
  \]

  \[
  \llbracket _, x = e, _\rrbracket^\#(R, M) = (R(x \mapsto \emptyset), M) \quad \text{for } e \not\in \text{Reg}
  \]

  \[
  \llbracket u, x = \text{new}(e), v \rrbracket^\#(R, M) = (R(x \mapsto \{u\}), M)
  \]

  \[
  \llbracket _, x = p[e], _\rrbracket^\#(R, M) = (R(x \mapsto \bigcup\{M[a] \mid a \in R[p]\}), M)
  \]

  \[
  \llbracket _, p[e_1] = y, _\rrbracket^\#(R, M) = (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p))) \quad \text{for } y \in \text{Reg}
  \]

  \[
  \llbracket _, p[e_1] = e, _\rrbracket^\#(R, M) = (R, M) \quad \text{for } e \not\in \text{Reg}
  \]

$x$ may point to addresses where $y$ may point to.
First Idea

• Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  • Use start node of edge in CFG to identify allocation site
  • Abstract values $\text{Addr}^\# = V$, $\text{Val}^\# = 2^\text{Addr}^\#$ (Possible targets for pointer)
  • Domain: $(\text{Reg} \to \text{Val}^\#) \times (\text{Addr}^\# \to \text{Val}^\#)$

• Effects

  \[\ldots\]
  
  \[\llbracket \%, x = y, \% \rrbracket^\#(R, M) = (R(x \mapsto R(y)), M)\]
  for $y \in \text{Reg}$
  \[\llbracket \%, x = e, \% \rrbracket^\#(R, M) = (R(x \mapsto \emptyset), M)\]
  for $e \notin \text{Reg}$
  \[\llbracket u, x = \text{new}(e), v \rrbracket^\#(R, M) = (R(x \mapsto \{u\}), M)\]
  \[\llbracket \%, x = p[e], \% \rrbracket^\#(R, M) = (R(x \mapsto \bigcup\{M[a] \mid a \in R[p]\}), M)\]
  \[\llbracket \%, p[e_1] = y, \% \rrbracket^\#(R, M) = (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p)))\]
  for $y \in \text{Reg}$
  \[\llbracket \%, p[e_1] = e, \% \rrbracket^\#(R, M) = (R, M)\]
  for $e \notin \text{Reg}$

Expressions are never pointers.
First Idea

• Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  • Use start node of edge in CFG to identify allocation site
  • Abstract values $\text{Addr}^\# = V$, $\text{Val}^\# = 2^{\text{Addr}^\#}$ (Possible targets for pointer)
  • Domain: $(\text{Reg} \to \text{Val}^\#) \times (\text{Addr}^\# \to \text{Val}^\#)$

• Effects

$$\ldots$$

$$[\_ , x = y , \_]^\# (R , M) = (R (x \mapsto R (y)) , M) \quad \text{for } y \in \text{Reg}$$

$$[\_ , x = e , \_]^\# (R , M) = (R (x \mapsto \emptyset) , M) \quad \text{for } e \notin \text{Reg}$$

$$[u , x = \text{new}(e) , v]^\# (R , M) = (R (x \mapsto \{ u \}) , M)$$

$$[\_ , x = p[e] , \_]^\# (R , M) = (R (x \mapsto \bigcup \{ M [a] \mid a \in R [p] \}) , M)$$

$$[\_ , p[e_1] = y , \_]^\# (R , M) = (R , M (a \mapsto M (a) \cup R (y)) \mid a \in R (p))) \quad \text{for } y \in \text{Reg}$$

$$[\_ , p[e_1] = e , \_]^\# (R , M) = (R , M) \quad \text{for } e \notin \text{Reg}$$

$x$ points to this allocation site.
First Idea

- Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  - Use start node of edge in CFG to identify allocation site
  - Abstract values $\text{Addr}# = V$, $\text{Val}# = 2^{\text{Addr}#}$ (Possible targets for pointer)
  - Domain: $(\text{Reg} \rightarrow \text{Val}#) \times (\text{Addr}# \rightarrow \text{Val}#)$

- Effects

\[
\begin{align*}
\lll, x = y, \lrrr \#(R, M) &= (R(x \mapsto R(y)), M) & \text{for } y \in \text{Reg} \\
\lll, x = e, \lrrr \#(R, M) &= (R(x \mapsto \emptyset), M) & \text{for } e \notin \text{Reg} \\
\lll[u, x = \text{new}(e), v] \#(R, M) &= (R(x \mapsto \{u\}), M) \\
\lll, x = p[e], \lrrr \#(R, M) &= (R(x \mapsto \bigcup \{M[a] \mid a \in R[p]\}), M) \\
\lll, p[e_1] = y, \lrrr \#(R, M) &= (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p))) & \text{for } y \in \text{Reg} \\
\lll, p[e_1] = e, \lrrr \#(R, M) &= (R, M) & \text{for } e \notin \text{Reg}
\end{align*}
\]

$x$ may point to everything that $a$ may point to, for $p$ pointing to $a$
First Idea

- Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  - Use start node of edge in CFG to identify allocation site
  - Abstract values $\text{Addr}^\# = V$, $\text{Val}^\# = 2^{\text{Addr}^\#}$ (Possible targets for pointer)
  - Domain: $(\text{Reg} \rightarrow \text{Val}^\#) \times (\text{Addr}^\# \rightarrow \text{Val}^\#)$
- Effects

\[
\begin{align*}
\llbracket \_, x = y, \_ \rrbracket^\# (R, M) &= (R(x \mapsto R(y)), M) & \text{for } y \in \text{Reg} \\
\llbracket \_, x = e, \_ \rrbracket^\# (R, M) &= (R(x \mapsto \emptyset), M) & \text{for } e \notin \text{Reg} \\
\llbracket u, x = \text{new}(e), v \rrbracket^\# (R, M) &= (R(x \mapsto \{u\}), M) \\
\llbracket \_, x = p[e], \_ \rrbracket^\# (R, M) &= (R(x \mapsto \bigcup \{M[a] \mid a \in R[p]\}), M) \\
\llbracket \_, p[e_1] = y, \_ \rrbracket^\# (R, M) &= (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p))) & \text{for } y \in \text{Reg} \\
\llbracket \_, p[e_1] = e, \_ \rrbracket^\# (R, M) &= (R, M) & \text{for } e \notin \text{Reg}
\end{align*}
\]

Add addresses from $y$ to each possible address of $p$
First Idea

- Summarize (arbitrarily many) blocks of memory by (fixed number of) allocation sites
  - Use start node of edge in CFG to identify allocation site
  - Abstract values $\text{Addr}^# = V$, $\text{Val}^# = 2^{\text{Addr}^#}$ (Possible targets for pointer)
  - Domain: $(\text{Reg} \to \text{Val}^#) \times (\text{Addr}^# \to \text{Val}^#)$

- Effects

  \[
  \begin{align*}
  &\llbracket \_ , x = y , \_ \rrbracket^# (R, M) = (R(x \mapsto R(y)), M) \\
  &\llbracket \_ , x = e , \_ \rrbracket^# (R, M) = (R(x \mapsto \emptyset), M) \\
  &\llbracket u , x = \text{new}(e) , v \rrbracket^# (R, M) = (R(x \mapsto \{u\}), M) \\
  &\llbracket \_ , x = p[e] , \_ \rrbracket^# (R, M) = (R(x \mapsto \bigcup\{M[a] \mid a \in R[p]\}), M) \\
  &\llbracket \_ , p[e_1] = y , \_ \rrbracket^# (R, M) = (R, M(a \mapsto M(a) \cup R(y) \mid a \in R(p))) \quad \text{for } y \in \text{Reg} \\
  &\llbracket \_ , p[e_1] = e , \_ \rrbracket^# (R, M) = (R, M) \quad \text{for } e \notin \text{Reg}
  \end{align*}
  \]

Expressions are never pointers.
Example

\[ u: \ p_1 = \text{new} \ 2 \]
\[ v: \ p_2 = \text{new} \ 2 \]
\[ p_1[0] = 1 \]
\[ p_1[1] = p_2 \]
\[ p_2[0] = 2 \]
\[ p_2[1] = \text{null} \]

- At end of program, we have

\[ R = p_1 \mapsto \{u\}, p_2 \mapsto \{v\} \]
\[ M = u \mapsto \{v\}, v \mapsto \{\} \]
Description Relation

\[(\rho, \mu) \Delta (R, M) \text{ iff } \exists s : \text{Addr } \rightarrow \ V. \ \forall a, a' \in \text{Addr}. \ \forall x, i.\]

\[\rho(x) = a \implies s(a) \in R(x) \quad (1)\]

\[\land \mu(a, i) = a' \implies s(a') \in M(s(a)) \quad (2)\]

Intuitively: There is a mapping \(s\) from addresses to allocation sites, with:

(1) If a register contains an address, its abstract value contains the corresponding allocation site

(2) If a memory block contains an address (at any index), its abstract value contains the corresponding allocation site
\[(\rho, \mu) \Delta (R, M) \text{ iff } \exists s : \text{Addr} \rightarrow \mathcal{V}. \forall a, a' \in \text{Addr. } \forall x, i.
\]
\[
\rho(x) = a \implies s(a) \in R(x) \quad (1)
\]
\[
\mu(a, i) = a' \implies s(a') \in M(s(a)) \quad (2)
\]

Intuitively: There is a mapping \(s\) from addresses to allocation sites, with:

1. If a register contains an address, its abstract value contains the corresponding allocation site.
2. If a memory block contains an address (at any index), its abstract value contains the corresponding allocation site.

From this, we can extract may-alias information: Pointers \(p_1, p_2\) may only alias (i.e., \(\rho(p_1) = \rho(p_2) \in \text{Addr}\)), if \(R(p_1) \cap R(p_2) \neq \emptyset\).

- B/c if \(\rho(p_1) = \rho(p_2) = a \in \text{Addr}\), we have \(s(a) \in R(p_1) \cap R(p_2)\)
Description Relation

\[(\rho, \mu) \triangleq (R, M) \text{ iff } \exists s : \text{Addr} \rightarrow V. \forall a, a' \in \text{Addr}. \forall x, i.\]

\[\rho(x) = a \implies s(a) \in R(x)\]
\[\land \mu(a, i) = a' \implies s(a') \in M(s(a))\]

Intuitively: There is a mapping \(s\) from addresses to allocation sites, with:

(1) If a register contains an address, its abstract value contains the corresponding allocation site

(2) If a memory block contains an address (at any index), its abstract value contains the corresponding allocation site

From this, we can extract may-alias information: Pointers \(p_1, p_2\) may only alias (i.e., \(\rho(p_1) = \rho(p_2) \in \text{Addr}\)), if \(R(p_1) \cap R(p_2) \neq \emptyset\).

- B/c if \(\rho(p_1) = \rho(p_2) = a \in \text{Addr}\), we have \(s(a) \in R(p_1) \cap R(p_2)\)

Correctness of abstract effects (sketch)

- On whiteboard
Discussion

- May-point-to information accumulates for store.
  - If store is not initialized, we find out nothing
Discussion

- May-point-to information accumulates for store.
  - If store is not initialized, we find out nothing
- Analysis can be quite expensive
  - Abstract representation of memory at each program point
  - Does not scale to large programs
Flow insensitive analysis

- Idea: Do not consider ordering of statements
Flow insensitive analysis

- Idea: Do not consider ordering of statements
- Compute information that holds for any program point
Flow insensitive analysis

- Idea: Do not consider ordering of statements
- Compute information that holds for any program point
  - Only one instance of abstract registers/memory needed
Flow insensitive analysis

- Idea: Do not consider ordering of statements
- Compute information that holds for any program point
  - Only one instance of abstract registers/memory needed
- For our simple example: No loss in precision
First attempt

- Each edge \((u, a, v)\) gives rise to constraints

<table>
<thead>
<tr>
<th>(a)</th>
<th>constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x = y)</td>
<td>(R(x) \supseteq R(y))</td>
</tr>
<tr>
<td>(x = \text{new}(e))</td>
<td>(R(x) \supseteq {u})</td>
</tr>
<tr>
<td>(x = p[e])</td>
<td>(R(x) \supseteq \bigcup{M(a) \mid a \in R(p)})</td>
</tr>
<tr>
<td>(p[e_1] = x)</td>
<td>(M(a) \supseteq (a \in R(p) \Rightarrow R(x) : \emptyset)) for all (a \in V)</td>
</tr>
</tbody>
</table>

- Other edges have no effect
- Problem: Too many constraints
- \(O(kn)\) for \(k\) allocation sites and \(n\) edges.
- Does not scale to big programs
First attempt

- Each edge \((u, a, v)\) gives rise to constraints
  \[
  \begin{array}{l|l}
  a & \text{constraints} \\
  \hline
  x = y & R(x) \supseteq R(y) \\
  x = \text{new}(e) & R(x) \supseteq \{u\} \\
  x = p[e] & R(x) \supseteq \bigcup\{M(a) \mid a \in R(p)\} \\
  p[e_1] = x & M(a) \supseteq (a \in R(p) \cap R(x) : \emptyset) \quad \text{for all } a \in V \\
  \end{array}
  \]

- Other edges have no effect
First attempt

- Each edge \((u, a, v)\) gives rise to constraints

<table>
<thead>
<tr>
<th>(a)</th>
<th>constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x = y)</td>
<td>(R(x) \supseteq R(y))</td>
</tr>
<tr>
<td>(x = \text{new}(e))</td>
<td>(R(x) \supseteq {u})</td>
</tr>
<tr>
<td>(x = p[e])</td>
<td>(R(x) \supseteq \bigcup{M(a) \mid a \in R(p)})</td>
</tr>
<tr>
<td>(p[e_1] = x)</td>
<td>(M(a) \supseteq (a \in R(p) \cdot R(x) : \emptyset)) for all (a \in V)</td>
</tr>
</tbody>
</table>

- Other edges have no effect
- Problem: Too many constraints
  - \(O(kn)\) for \(k\) allocation sites and \(n\) edges.
First attempt

- Each edge \((u, a, v)\) gives rise to constraints

<table>
<thead>
<tr>
<th>(a)</th>
<th>constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x = y)</td>
<td>(R(x) \supseteq R(y))</td>
</tr>
<tr>
<td>(x = \text{new}(e))</td>
<td>(R(x) \supseteq {u})</td>
</tr>
<tr>
<td>(x = p[e])</td>
<td>(R(x) \supseteq \bigcup{M(a) \mid a \in R(p)})</td>
</tr>
<tr>
<td>(p[e_1] = x)</td>
<td>(M(a) \supseteq (a \in R(p) \land R(x) : \emptyset)) for all (a \in V)</td>
</tr>
</tbody>
</table>

- Other edges have no effect
- Problem: Too many constraints
  - \(O(kn)\) for \(k\) allocation sites and \(n\) edges.
- Does not scale to big programs
Last Lecture

- Flow sensitive points-to analysis
  - Identify blocks in memory with allocation sites
  - Does not scale. One abstract memory per program point.

- Flow-insensitive points-to analysis
  - Compute one abstract memory that approximates all program points.
  - Does not scale. Too many constraints

- Flow-insensitive alias analysis
  - Compute equivalence classes of $p$ and $p[]$
Alias analysis

• Idea: Maintain equivalence relation between variables $p$ and memory accesses $p[]$
  • $x \sim y$ whenever $x$ and $y$ may contain the same address (at any two program points)

u: $p_1 = \text{new} (2)$
v: $p_2 = \text{new} (2)$
$p_1[0] = 1$
$p_1[1] = p_2$
$p_2[0] = 2$
$p_2[1] = \text{null}$

• $\sim = \{\{p_1[], p_2\}, \{p_1\}, \{p_2[]\}\}$

Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{ p' \in R \mid p \sim p' \}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{ p' \in R \mid p \sim p' \}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  - $\sim \bot :=$
Equivalence relations

• Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
• Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
• The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
• $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  • The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  • $\sim \perp := (=)$
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{ p' \in R \mid p \sim p' \}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  - $\sim_{\bot} := (=)$
  - $\sim_{\top} :=$
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  - $\sim_{\perp} := (=)$
  - $\sim_{\top} := R \times R$
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  - $\sim \bot := (\equiv)$
  - $\sim \top := R \times R$
  - $\bigcup S := \bigcup S$
Equivalence relations

- Relation $\sim \subseteq R \times R$ that is reflexive, transitive, symmetric
- Equivalence class $[p] := \{p' \in R \mid p \sim p'\}$
- The equivalence classes partition $R$. Conversely, any partition of $R$ defines an equivalence relation.
- $\sim \subseteq \sim'$ ($\sim$ finer than $\sim'$)
  - The set of all equivalence relations on $R$ with $\subseteq$ forms a complete lattice
  - $\sim_\perp := (=)$
  - $\sim_T := R \times R$
  - $\sqcup S := (\bigcup S)^*$
Operations on ERs

- `find(\sim, p)`: Return equivalence class of $p$
Operations on ERs

- \texttt{find}(\sim, p): \text{Return equivalence class of } p
- \texttt{union}(\sim, p, p'): \text{Return finest ER } \sim' \text{ with } p \sim' p' \text{ and } \sim \subseteq \sim'
Operations on ERs

- \textbf{find} (\sim, p): Return equivalence class of \( p \)
- \textbf{union} (\sim, p, p'): Return finest ER \( \sim' \) with \( p \sim' p' \) and \( \sim \subseteq \sim' \)
- On partitions of finite sets: Let \( R = [p_1]_{\sim} \cup \ldots \cup [p_n]_{\sim} \)
  - \textbf{union} (\sim, p, p'): Let \( p \in [p_i]_{\sim}, p' \in [p_j]_{\sim} \)
    Result: \( \{[p_i]_{\sim} \cup [p_j]_{\sim}\} \cup \{[p_k] \mid 1 \leq k \leq n \land k \notin \{i, j\}\} \)
Recursive Union

- If $x \sim y$, then also $x[] \sim y[]$ (rec)
Recursive Union

- If $x \sim y$, then also $x[] \sim y[]$ (rec)
- After union, we have to add those equivalences!
Recursive Union

- If \( x \sim y \), then also \( x[] \sim y[] \) (rec)
- After union, we have to add those equivalences!
- \texttt{union}\(^*\)(~\(p\),\(p'\)):
  - The finest ER that is coarser than \texttt{union}(~\(p\),\(p'\)) and satisfies (rec)
Alias analysis

\[ \pi = \{ \{x\}, \{x[]\} \mid x \in \text{Vars} \} // \text{Finest ER} \]

for (_,a,_) in E do {
    case a of
        x=y: \pi = \text{union}*(\pi,x,y)
        | x=y[e]: \pi = \text{union}*(\pi,x,y[]) // y variable
        | y[e]=x: \pi = \text{union}*(\pi,x,y[]) // y variable
}

- Start with finest ER (=)
Alias analysis

\[ \pi = \{ \{x\}, \{x[\}\} \mid x \in \text{Vars} \} \] // Finest ER

for (_,a,_) in E do {
   case a of
      x=y: \( \pi = \text{union}^*(\pi,x,y) \)
      | x=y[e]: \( \pi = \text{union}^*(\pi,x,y[\]) \) // y variable
      | y[e]=x: \( \pi = \text{union}^*(\pi,x,y[\]) \) // y variable
}

- Start with finest ER (\( = \))
- Iterate over edges, and union equivalence classes
Example

1: \( p_1 = \text{new} \ (2) \)
2: \( p_2 = \text{new} \ (2) \)
3: \( p_1[0] = 1 \)
4: \( p_1[1] = p_2 \)
5: \( p_2[0] = 2 \)
6: \( p_2[1] = \text{null} \)

\[
\text{init} \quad \{ \{ p_1 \}, \{ p_2 \}, \{ p_1 \}, \{ p_2 \} \} \\
1 \rightarrow 2 \quad \{ \{ p_1 \}, \{ p_2 \}, \{ p_1 \}, \{ p_2 \} \} \\
2 \rightarrow 3 \quad \{ \{ p_1 \}, \{ p_2 \}, \{ p_1 \}, \{ p_2 \} \} \\
3 \rightarrow 4 \quad \{ \{ p_1 \}, \{ p_2 \}, \{ p_1 \}, \{ p_2 \} \} \\
4 \rightarrow 5 \quad \{ \{ p_1 \}, \{ p_2, p_1 \}, \{ p_2 \} \} \\
5 \rightarrow 6 \quad \{ \{ p_1 \}, \{ p_2, p_1 \}, \{ p_2 \} \} \]
Example

1: $R = \text{null}$
2: if Neg (T != null) goto 8
3: $H = T$
4: $T = T[0]$
5: $H[0] = R$
6: $R = H$
7: goto 2
8:

init $\{\{H\}, \{R\}, \{T\}, \{H[]\}, \{T[]\}\}$
3 $\rightarrow$ 4 $\{\{H, T\}, \{R\}, \{H[], T[]\}\}$
4 $\rightarrow$ 5 $\{\{H, T, H[], T[]\}, \{R\}\}$
5 $\rightarrow$ 6 $\{\{H, T, H[], T[], R\}\}$
6 $\rightarrow$ 7 $\{\{H, T, H[], T[], R\}\}$
• All memory content must have been constructed by analyzed program
Discussion

- All memory content must have been constructed by analyzed program
  - \( p = p[]; \ p = p[]; \ q = q[] \)
Discussion

- All memory content must have been constructed by analyzed program
  - `p=p[]; p=p[]; q=q[]`
  - What if `q` points to third element of linked list at `p`.
Discussion

- All memory content must have been constructed by analyzed program
  - `p=p[]; p=p[]; q=q[]`
  - What if `q` points to third element of linked list at `p`.

⇒ Only works for whole programs, no input via memory
Correctness

- Intuition: Each address ever created represented by a register

- Invariant:
  1. If a register holds an address, it is in the same class as the address's representative.
  2. If memory holds an address, it is in the same class as the address of the address dereferenced.

- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m: \text{Addr} \rightarrow \text{Reg}\), such that
  1. If \(\rho(x) \in \text{Addr}\) then \(x \sim m(\rho(x))\).
  2. If \(\mu(a, i) \in \text{Addr}\) then \(m(a) \sim m(\mu(a, i))\).

- Extracting alias information:
  - \(x, y\) may alias, if \(x \sim y\).
  - If \(\rho(x) = \rho(y) = a \in \text{Addr}\) then \(x \sim m(a) \sim y\).

- To show: Invariant holds initially, and preserved by steps.
Correctness

- Intuition: Each address ever created represented by register
- Invariant:

\[
\begin{align*}
\text{1.} & \quad \text{If register holds address, it is in the same class as address' representative} \\
\text{2.} & \quad \text{If memory holds address, it is in the same class as address of address dereferenced}
\end{align*}
\]

- Formally: For all reachable states \((\rho,\mu)\), there exists a map \(m: \text{Addr} \to \text{Reg}\), such that

\[
\begin{align*}
\text{1.} & \quad \rho(x) \in \text{Addr} \implies x \sim m(\rho(x)) \\
\text{2.} & \quad \mu(a,i) \in \text{Addr} \implies m(a) \sim m(\mu(a,i))
\end{align*}
\]

- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).

\[
\begin{align*}
\rho(x) = \rho(y) = a \in \text{Addr} \implies x \sim m(a) \sim y
\end{align*}
\]

- To show: Invariant holds initially, and preserved by steps

\[
\begin{align*}
\text{Initially:} & \quad \text{By assumption, neither registers nor memory hold addresses!} \\
\text{Preservation:} & \quad \text{On whiteboard}
\end{align*}
\]
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced

Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m: \text{Addr} \to \text{Reg}\), such that

1. \(\rho(x) \in \text{Addr} \Rightarrow x \sim m(\rho(x))\)
2. \(\mu(a, i) \in \text{Addr} \Rightarrow m(a) \sim m(\mu(a, i))\)

- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).
- \(\rho(x) = \rho(y) = a \in \text{Addr} \Rightarrow x \sim m(a) \sim y\)

- To show: Invariant holds initially, and preserved by steps
  - Initially: By assumption, neither registers nor memory hold addresses!
  - Preservation: On whiteboard
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \to \text{Reg}\), such that

\[
\rho(x) \in \text{Addr} \Rightarrow x \sim m(\rho(x)) \\
\mu(a, i) \in \text{Addr} \Rightarrow m(a) \sim m(\mu(a, i))
\]
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \rightarrow \text{Reg}\), such that
  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \rightarrow \text{Reg}\), such that
  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
  2. \(\mu(a, i) \in \text{Addr} \implies m(a)[i] \sim m(\mu(a, i))\)
Correctness

- Intuition: Each address ever created represented by register

- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced

- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \rightarrow \text{Reg}\), such that

  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
  2. \(\mu(a, i) \in \text{Addr} \implies m(a)[i] \sim m(\mu(a, i))\)

- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).
  
  - \(\rho(x) = \rho(y) = a \in \text{Addr} \implies x \sim m(a) \sim y\)
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \rightarrow \text{Reg}\), such that
  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
  2. \(\mu(a, i) \in \text{Addr} \implies m(a)[i] \sim m(\mu(a, i))\)
- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).
  - \(\rho(x) = \rho(y) = a \in \text{Addr} \implies x \sim m(a) \sim y\)
- To show: Invariant holds initially, and preserved by steps
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \rightarrow \text{Reg}\), such that
  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
  2. \(\mu(a, i) \in \text{Addr} \implies m(a)[i] \sim m(\mu(a, i))\)
- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).
  - \(\rho(x) = \rho(y) = a \in \text{Addr} \implies x \sim m(a) \sim y\)
- To show: Invariant holds initially, and preserved by steps
  - Initially: By assumption, neither registers nor memory hold addresses!
Correctness

- Intuition: Each address ever created represented by register
- Invariant:
  1. If register holds address, it is in the same class as address’ representative
  2. If memory holds address, it is in the same class as address of address dereferenced
- Formally: For all reachable states \((\rho, \mu)\), there exists a map \(m : \text{Addr} \to \text{Reg}\), such that
  1. \(\rho(x) \in \text{Addr} \implies x \sim m(\rho(x))\)
  2. \(\mu(a, i) \in \text{Addr} \implies m(a)[i] \sim m(\mu(a, i))\)
- Extracting alias information: \(x, y\) may alias, if \(x \sim y\).
  - \(\rho(x) = \rho(y) = a \in \text{Addr} \implies x \sim m(a) \sim y\)
- To show: Invariant holds initially, and preserved by steps
  - Initially: By assumption, neither registers nor memory hold addresses!
  - Preservation: On whiteboard
Implementation

- Need to implement `union*` operation efficiently
Implementation

- Need to implement `union*` operation efficiently
- Use `Union-Find` data structure
Implementation

• Need to implement \texttt{union}\* operation efficiently
• Use \texttt{Union-Find} data structure
• Equivalence classes identified by unique representative
Implementation

- Need to implement `union*` operation efficiently
- Use `Union-Find` data structure
- Equivalence classes identified by unique representative
- Operations:
Implementation

- Need to implement \textbf{union} operation efficiently
- Use \textbf{Union-Find} data structure
- Equivalence classes identified by unique representative
- Operations:
  - \textbf{find}(x): Return representative of \([x]\)
Implementation

• Need to implement \texttt{union}\* operation efficiently
• Use \texttt{Union-Find} data structure
• Equivalence classes identified by unique representative
• Operations:
  • \texttt{find(x)}: Return representative of [x]
  • \texttt{union(x, y)}: Join equivalence classes represented by \(x\) and \(y\)
    • Destructive update!
Union-Find: Idea

- ER represented as forest.
Union-Find: Idea

- ER represented as forest.
- Each node contains element and parent pointer.
Union-Find: Idea

- ER represented as forest.
- Each node contains element and parent pointer.
- Elements of trees are equivalence classes
Union-Find: Idea

- ER represented as forest.
- Each node contains element and parent pointer.
- Elements of trees are equivalence classes
- Representatives are roots of trees
Union-Find: Idea

• ER represented as forest.
• Each node contains element and parent pointer.
• Elements of trees are equivalence classes
• Representatives are roots of trees
• Find: Follow tree upwards

```
0 1 2 3 6 7 4 5
1 1 3 1 4 7 5 7
```

0
1
3
2
4
7
5
6
Union-Find: Idea

- ER represented as forest.
- Each node contains element and parent pointer.
- Elements of trees are equivalence classes
- Representatives are roots of trees
- Find: Follow tree upwards
- Union: Link root node of one tree to other tree
Union-Find: Idea

- ER represented as forest.
- Each node contains element and parent pointer.
- Elements of trees are equivalence classes
- Representatives are roots of trees
- Find: Follow tree upwards
- Union: Link root node of one tree to other tree
Union-Find: Optimizations

- Complexity: Union: $O(1)$, find: $O(n)$ :(
Union-Find: Optimizations

- Complexity: Union: $O(1)$, find: $O(n)$ :
- Union by size: Connect root of smaller tree to root of bigger one
Union-Find: Optimizations

- Complexity: Union: $O(1)$, find: $O(n)$ :
- Union by size: Connect root of smaller tree to root of bigger one
  - Store size of tree in root node
Union-Find: Optimizations

- Complexity: Union: $O(1)$, find: $O(n)$ :(
- Union by size: Connect root of smaller tree to root of bigger one
  - Store size of tree in root node
  - C - implementation hack: Re/ab-use parent-pointer field for that
Union-Find: Optimizations

- Complexity: Union: $O(1)$, find: $O(n)$ :

- Union by size: Connect root of smaller tree to root of bigger one
  - Store size of tree in root node
  - C - implementation hack: Re/ab-use parent-pointer field for that
  - Complexity: Union: $O(1)$, find: $O(\log n)$ :|
Union by size: Example

0 1 2 3 4 5 6 7
1 1 3 1 4 7 5 7
Union by size: Example

```
0 1 2 3 6 7 4 5
0 1 3 2 4 7 5 6
```

```
0 1 2 3 4 5 6 7
1 1 3 1 7 7 5 7
```
Path compression

- After find, redirect pointers on path to root node

\[
\text{Complexity, amortized for } m \text{ find and } n - 1 \text{ union operations}
\]

\[
\mathcal{O}\left(n + m \alpha(n)\right)
\]

Where \(\alpha\) is the inverse Ackerman-function

\[
\text{Note: This complexity is optimal :)}
\]
Path compression

- After find, redirect pointers on path to root node
- Requires second pass for find

- Complexity, amortized for \( m \) find and \( n - 1 \) union operations
  \[ O(n + m \alpha(n)) \]
  Where \( \alpha \) is the inverse Ackerman function

- Note: This complexity is optimal :)
Path compression

- After find, redirect pointers on path to root node
- Requires second pass for find
  - Alternative: Connect each node on find-path to its grandfather

Complexity, amortized for $m$ find and $n-1$ union operations

$O\left(\frac{m}{\alpha(n)}\right)$

Where $\alpha$ is the inverse Ackerman function

Note: $n < 10^{18} \Rightarrow \alpha(n) < 5$

Note: This complexity is optimal!
Path compression

- After find, redirect pointers on path to root node
- Requires second pass for find
  - Alternative: Connect each node on find-path to its grandfather
- Complexity, amortized for $m$ find and $n - 1$ union operations
  - $O(n + m\alpha(n))$
  - Where $\alpha$ is the inverse Ackerman-function
Path compression

- After find, redirect pointers on path to root node
- Requires second pass for find
  - Alternative: Connect each node on find-path to its grandfather
- Complexity, amortized for $m$ find and $n - 1$ union operations
  - $O(n + m\alpha(n))$
  - Where $\alpha$ is the inverse Ackerman-function
  - Note $n < 10^{80} \implies \alpha(n) < 5$
Path compression

- After find, redirect pointers on path to root node
- Requires second pass for find
  - Alternative: Connect each node on find-path to its grandfather
- Complexity, amortized for $m$ find and $n - 1$ union operations
  - $O(n + m\alpha(n))$
  - Where $\alpha$ is the inverse Ackerman-function
  - Note $n < 10^{80} \iff \alpha(n) < 5$
  - Note: This complexity is optimal :)
Path compression: Example

![Graph Example]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>
Path compression: Example

```
0 1 2 3 4 5 6 7
0 1 3 1 7 7 5 3
```
Path compression: Example

```
0 1 2 3 4 5 6 7
5 1 3 1 7 7 5 3
```
Path compression: Example
Path compression: Example

```
0  1  2  3  4  5  6  7
5  1  3  1  1  7  1  1
```
Placing registers on top

- Try to preserve invariant:
Placing registers on top

- Try to preserve invariant:
  - If equivalence class contains register, its representative (root node) is register
Placing registers on top

- Try to preserve invariant:
  - If equivalence class contains register, its representative (root node) is register
  - On union, if linking register class to non-register class:
Placing registers on top

- Try to preserve invariant:
  - If equivalence class contains register, its representative (root node) is register
  - On union, if linking register class to non-register class:
    - Swap stored values in roots
Placing registers on top

- Try to preserve invariant:
  - If equivalence class contains register, its representative (root node) is register
  - On union, if linking register class to non-register class:
    - Swap stored values in roots
- Then, register equivalence class can be identified by its representative
Implementing union*

union*(x,y):
    x = find(x); y=find(y)
    if x != y then
        union(x,y)
        if x ∈ Regs & y ∈ Regs then
            union*(x[],y[])
Summary

- Complexity:
  - $O(|E| + |\text{Reg}|)$ calls to union*, find. $O(|\text{Reg}|)$ calls to union.

  Analysis is fast. But may be imprecise. More precise analysis too expensive for compilers.
Summary

- Complexity:
  - $O(|E| + |Reg|)$ calls to union*, find. $O(|Reg|)$ calls to union.
- Analysis is fast. But may be imprecise.
Summary

- Complexity:
  - \(O(|E| + |\text{Reg}|)\) calls to union*, find. \(O(|\text{Reg}|)\) calls to union.
- Analysis is fast. But may be imprecise.
- More precise analysis too expensive for compilers.
Last Lecture

- Alias analysis by merging equivalence classes
- Implementation by union-find structure
  - Optimizations: Union-by-size, path-compression
  - Implementing union*
Evaluation

Please fill out evaluation forms online.
Table of Contents

1. Introduction
2. Removing Superfluous Computations
3. Abstract Interpretation
4. Alias Analysis
5. Avoiding Redundancy (Part II)
6. Interprocedural Analysis
7. Analysis of Parallel Programs
8. Replacing Expensive by Cheaper Operations
9. Exploiting Hardware Features
10. Optimization of Functional Programs
Idea

```c
if * {
    x = M[5]
} else {
    y_1 = x + 1
}
```

\[
M[1] = y_1 + y_2
\]
if * {
    x = M[5]
} else {
    y_1 = x + 1
}

y_2 = x + 1
M[1] = y_1 + y_2

• x+1 is evaluated on every path
Idea

```plaintext
if * {
    x = M[5]
} else {
    y_1 = x + 1
}

y_2 = x + 1
M[1] = y_1 + y_2
```

- $x+1$ is evaluated on every path
- On else-path even two times
Goal

if * {
    x = M[5]
} else {
    y_1 = x + 1
}

y_2 = x + 1
M[1] = y_1 + y_2
Goal

if * {
  x = M[5]
} else {
  y_1 = x + 1
}
y_2 = x + 1
M[1] = y_1 + y_2

if * {
  x = M[5]
  T = x + 1
} else {
  T = x + 1
  y_1 = T
}
y_2 = T
M[1] = y_1 + T
Idea

- Insert assignments $T_e = e$, such that $e$ is available at all program points where it is required.
Idea

- Insert assignments $T_e = e$, such that $e$ is available at all program points where it is required.
- Insert assignments as early as possible.
Idea

- Insert assignments $T_e = e$, such that $e$ is available at all program points where it is required.
- Insert assignments as early as possible.
- Do not add evaluations of $e$ that would not have been executed at all.
  - $\text{if } x \neq 0 \text{ then } y = 6 \text{ div } x \rightarrow T = 6 \text{ div } x; \text{ if } x \neq 0 \text{ then } y = T$
Very busy expressions

• An expression $e$ is busy on path $\pi$, if it is evaluated on $\pi$ before a variable of $e$ is changed.

• An expression $e$ is very busy at $u$, if it is busy for all path from $u$ to an end node.

• Backwards must analysis, i.e., $\sqsubseteq = \sqsupseteq$, $\sqcup = \sqcap$.

• Semantic intuition:
  • $e$ busy on $\pi$ — evaluation of $e$ can be placed at start of path $\pi$.
  • $e$ very busy at $u$ — evaluation can be placed at $u$.
  • Without inserting unwanted additional evaluations.
Very busy expressions

- An expression $e$ is **busy** on path $\pi$, if it is evaluated on $\pi$ before a variable of $e$ is changed.
- $e$ is **very busy** at $u$, if it is busy for all path from $u$ to an end node.
Very busy expressions

- An expression $e$ is **busy** on path $\pi$, if it is evaluated on $\pi$ before a variable of $e$ is changed.
- $e$ is **very busy** at $u$, if it is busy for all path from $u$ to an end node.
- Backwards must analysis, i.e., $\subseteq \supseteq$, $\sqcup = \sqcap$
An expression $e$ is **busy** on path $\pi$, if it is evaluated on $\pi$ before a variable of $e$ is changed.

- $e$ is **very busy** at $u$, if it is busy for all path from $u$ to an end node.

- Backwards must analysis, i.e., $\sqsubseteq = \supseteq$, $\sqcup = \cap$

- Semantic intuition:
  - $e$ busy on $\pi$ — evaluation of $e$ can be placed at start of path
  - $e$ very busy at $u$ — evaluation can be placed at $u$
    - Without inserting unwanted additional evaluations
Abstract effects

$$\llbracket \text{Nop} \rrbracket^\# B = B$$

$$\llbracket \text{Pos}(e) \rrbracket^\# B = B \cup \{e\}$$

$$\llbracket \text{Neg}(e) \rrbracket^\# B = B \cup \{e\}$$

$$\llbracket x := e \rrbracket^\# B = (B \setminus \text{Expr}_x) \cup \{e\}$$

$$\llbracket x := M[e] \rrbracket^\# B = (B \setminus \text{Expr}_x) \cup \{e\}$$

$$\llbracket M[e_1] = e_2 \rrbracket^\# B = B \cup \{e_1, e_2\}$$

- Initial value: $\emptyset$
  - No very busy expressions at end nodes
Abstract effects

\[ [\text{Nop}]^\# B = B \]
\[ [\text{Pos}(e)]^\# B = B \cup \{e\} \]
\[ [\text{Neg}(e)]^\# B = B \cup \{e\} \]
\[ [x := e]^\# B = (B \setminus \text{Expr}_x) \cup \{e\} \]
\[ [x := M[e]]^\# B = (B \setminus \text{Expr}_x) \cup \{e\} \]
\[ [M[e_1] = e_2]^\# B = B \cup \{e_1, e_2\} \]

- Initial value: \( \emptyset \)
  - No very busy expressions at end nodes
- Kill/Gen analysis, i.e., distributive
  - \( \text{MOP} = \text{MFP} \), if end node reachable from every node
Example (Very Busy Expressions)

\[ x = M[5] \]

\[ y_1 = x + 1 \]

\[ y_2 = x + 1 \]

\[ M[1] = y_1 + y_2 \]
Example (Very Busy Expressions)

\[
x = M[5] \\
y_1 = x + 1 \\
y_2 = x + 1 \\
M[1] = y_1 + y_2 \\
\]

{}
Example (Very Busy Expressions)

\[ x = M[5] \]

\[ y_1 = x + 1 \]

\[ y_2 = x + 1 \]

\[ \{ y_1 + y_2 \} \]

\[ M[1] = y_1 + y_2 \]

\[ \{ \} \]
Example (Very Busy Expressions)

\[ x = M[5] \]
\[ y_1 = x + 1 \]
\[ y_2 = x + 1 \]
\[ M[1] = y_1 + y_2 \]
Example (Very Busy Expressions)

\[ \{x + 1\} \]

\[ x = M[5] \]

\[ y_1 = x + 1 \]

\[ y_2 = x + 1 \]

\[ y_1 + y_2 \]

\[ M[1] = y_1 + y_2 \]

\[ \} \]
Example (Very Busy Expressions)

\[
x = M[5]
\]

\[
y_1 = x + 1
\]

\[
y_2 = x + 1
\]

\[
M[1] = y_1 + y_2
\]
Available expressions

- Recall: Available expressions before memo-transformation

\[
\begin{align*}
\llbracket \text{Nop} \rrbracket_A A & := A \\
\llbracket \text{Pos}(e) \rrbracket_A A & := A \cup \{e\} \\
\llbracket \text{Neg}(e) \rrbracket_A A & := A \cup \{e\} \\
\llbracket R = e \rrbracket_A A & := (A \cup \{e\}) \setminus \text{Expr}_R \\
\llbracket R = M[e] \rrbracket_A A & := (A \cup \{e\}) \setminus \text{Expr}_R \\
\llbracket M[e_1] = e_2 \rrbracket_A A & := A \cup \{e_1, e_2\}
\end{align*}
\]
Transformation

- Insert $T_e = e$ after edge $(u, a, v)$, if

Note: Order does not matter
Transformation

- Insert $T_e = e$ after edge $(u, a, v)$, if
  - $e$ is very busy at $v$
Transformation

- Insert $T_e = e$ after edge $(u, a, v)$, if
  - $e$ is very busy at $v$
  - Evaluation could not have been inserted before, b/c
    - $e$ destroyed by $a$, or
    - $e$ neither available, nor very busy at $u$
Transformation

- Insert $T_e = e$ after edge $(u, a, v)$, if
  - $e$ is very busy at $v$
  - Evaluation could not have been inserted before, b/c
    - $e$ destroyed by $a$, or
    - $e$ neither available, nor very busy at $u$
  - Formally: $e \in B[v] \setminus \llbracket a \rrbracket^\#_A(A[u] \cup B[u])$

- At program start, insert evaluations of $B[v_0]$
Transformation

- Insert $T_e = e$ after edge $(u, a, v)$, if
  - $e$ is very busy at $v$
  - Evaluation could not have been inserted before, b/c
    - $e$ destroyed by $a$, or
    - $e$ neither available, nor very busy at $u$
  - Formally: $e \in B[v] \setminus \{a\}^{\#}(A[u] \cup B[u])$
- At program start, insert evaluations of $B[v_0]$
• Insert $T_e = e$ after edge $(u, a, v)$, if
  • $e$ is very busy at $v$
  • Evaluation could not have been inserted before, b/c
    • $e$ destroyed by $a$, or
    • $e$ neither available, nor very busy at $u$
  • Formally: $e \in B[v] \setminus \#_A (A[u] \cup B[u])$
• At program start, insert evaluations of $B[v_0]$
  • Note: Order does not matter
Transformation

- Place evaluations of expressions
  - \((u, a, v) \mapsto \{(u, a, w), (w, T_e = e, v)\} \text{ for } e \in B[v] \setminus \llbracket a \rrbracket^\#_A(A[u] \cup B[u])\)
  - For fresh node \(w\)

- Note: Multiple memo-assignments on one edge
  - Can just be expanded in any order

- Replace usages of expressions
  - \((u, x = e, v) \mapsto (u, x = T_e, v)\)
  - analogously for other uses of \(e\)
Transformation

- Place evaluations of expressions
  - \((u, a, v) \mapsto \{(u, a, w), (w, T_e = e, v)\} \text{ for } e \in B[v] \setminus \llbracket a \rrbracket^\#_A(A[u] \cup B[u])\)
  - For fresh node \(w\)
- \(v_0 \mapsto v_0' \text{ with } (v_0', T_e = e, v_0) \text{ for } e \in B[v_0]\)
Transformation

- Place evaluations of expressions
  - $(u, a, v) \mapsto \{(u, a, w), (w, T_e = e, v)\}$ for $e \in B[v] \setminus \llbracket a \rrbracket^\#(A[u] \cup B[u])$
  - For fresh node $w$
- $v_0 \mapsto v_0'$ with $(v_0', T_e = e, v_0)$ for $e \in B[v_0]$
- Note: Multiple memo-assignments on one edge
  - Can just be expanded in any order
Transformation

- Place evaluations of expressions
  - \((u, a, v) \mapsto \{(u, a, w), (w, T_e = e, v)\} \text{ for } e \in B[v] \setminus \llbracket a \rrbracket_A^\#(A[u] \cup B[u])\)
  - For fresh node \(w\)
- \(v_0 \mapsto v_0'\) with \((v_0', T_e = e, v_0)\) for \(e \in B[v_0]\)
- Note: Multiple memo-assignments on one edge
  - Can just be expanded in any order
- Replace usages of expressions
  - \((u, x = e, v) \mapsto (u, x = T_e, v)\)
  - analogously for other uses of \(e\)
Example

- For expression $x + 1$ only

\[
x = M[5] \\
y_1 = x + 1 \\
y_2 = x + 1 \\
M[1] = y_1 + y_2
\]
Example

- For expression $x + 1$ only

\[ B = \{\}, A = \{\} \]

\[ B = \{\}, A = \{\} \]

\[ B = \{x + 1\}, A = \{\} \]

\[ B = \{\}, A = \{\} \]

\[ B = \{x + 1\}, A = \{\} \]

\[ B = \{x + 1\}, A = \{x + 1\} \]

\[ B = \{x + 1\}, A = \{\} \]

\[ B = \{\}, A = \{\} \]

\[ B = \{\}, A = \{\} \]

\[ B = \{y_1 + y_2\}, A = \{x + 1\} \]

\[ B = \{\}, A = \{x + 1, y_1 + y_2\} \]
Example

- For expression $x + 1$ only
Example

- For expression $x + 1$ only

$$x = M[5]$$

$$y_1 = x + 1$$

$$y_2 = x + 1$$

$$M[1] = y_1 + y_2$$
Example

- For expression $x + 1$ only

\[ T = x + 1 \]

\[ y_1 = x + 1 \]

\[ x = M[5] \]

\[ y_2 = x + 1 \]

\[ M[1] = y_1 + y_2 \]
Example

- For expression $x + 1$ only

$x = M[5]$

$T = x + 1$

$y_1 = T$

$y_2 = T$

$M[1] = y_1 + y_2$
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

→ Required expressions are very busy at start node of edge
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

⇒ Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$

Correctness (Sketch)

• Assumption: Same set of expressions occur at all outgoing edges of a node
  • True for our translation scheme
  • Be careful in general!

⇒ Required expressions are very busy at start node of edge

• Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  • Assume expression $e$ required by $a$
  • $e \in B[u]$

• Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

⇒ Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
    - $e \in B[u]$
  - Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$
  - Induction on $\pi$. 
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

⇒ Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$
- Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$
- Induction on $\pi$.
  - Empty path: Evaluation placed before start node
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

  $\Rightarrow$ Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$

- Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$

- Induction on $\pi$.
  - Empty path: Evaluation placed before start node
  - $\pi = \pi'(u, a, v)$:
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

  ➞  Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: $\pi_1(u, a, v) \pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$

- Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$

- Induction on $\pi$.
  - Empty path: Evaluation placed before start node
  - $\pi = \pi'(u, a, v)$:
    - Case $a$ modifies $e$ $\implies e \notin \llbracket a \rrbracket_A^\#(\ldots)$ $\implies$ Evaluation placed here.
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

→ Required expressions are very busy at start node of edge

- Regard path from start node over edge to end node: \( \pi_1(u, a, v) \pi_2 \)
  - Assume expression \( e \) required by \( a \)
  - \( e \in B[u] \)

- Show: On any path \( \pi \) from \( v_0 \) to \( v \) with \( e \in B[v] \), evaluation of \( e \) is placed such that it is available at \( v \)

- Induction on \( \pi \).
  - Empty path: Evaluation placed before start node
  - \( \pi = \pi'(u, a, v) \):
    - Case \( a \) modifies \( e \) \( \implies e \notin [a]_A^#(\ldots) \implies \) Evaluation placed here.
    - Case \( e \notin A[u] \cup B[u] \implies \) Evaluation placed here.
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

→ Required expressions are very busy at start node of edge
- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$
- Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$
- Induction on $\pi$.
  - Empty path: Evaluation placed before start node
  - $\pi = \pi'(u, a, v)$:
    - Case $a$ modifies $e$ $\implies$ $e \notin \llbracket a \rrbracket^\#(\ldots)$ $\implies$ Evaluation placed here.
    - Case $e \notin A[u] \cup B[u]$ $\implies$ Evaluation placed here.
    - Assume: $a$ does not modify $e$
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

⇒ Required expressions are very busy at start node of edge
- Regard path from start node over edge to end node: $\pi_1(u, a, v)\pi_2$
  - Assume expression $e$ required by $a$
  - $e \in B[u]$

- Show: On any path $\pi$ from $v_0$ to $v$ with $e \in B[v]$, evaluation of $e$ is placed such that it is available at $v$
- Induction on $\pi$.
  - Empty path: Evaluation placed before start node
  - $\pi = \pi'(u, a, v)$:
    - Case $a$ modifies $e \Rightarrow e \notin [\lceil a\rceil]^\#_A(\ldots) \Rightarrow$ Evaluation placed here.
    - Case $e \notin A[u] \cup B[u] \Rightarrow$ Evaluation placed here.
    - Assume: $a$ does not modify $e$
    - Case $e \in B[u]$. Induction hypothesis.
Correctness (Sketch)

- Assumption: Same set of expressions occur at all outgoing edges of a node
  - True for our translation scheme
  - Be careful in general!

⇒ Required expressions are very busy at start node of edge
- Regard path from start node over edge to end node: \( \pi_1(u, a, v)\pi_2 \)
  - Assume expression \( e \) required by \( a \)
  - \( e \in B[u] \)
- Show: On any path \( \pi \) from \( v_0 \) to \( v \) with \( e \in B[v] \), evaluation of \( e \) is placed such that it is available at \( v \)
- Induction on \( \pi \).
  - Empty path: Evaluation placed before start node
  - \( \pi = \pi'(u, a, v) \):
    - Case \( a \) modifies \( e \) \( \implies \) \( e \notin \[a\]_A^\#(\ldots) \implies \) Evaluation placed here.
    - Case \( e \notin A[u] \cup B[u] \) \( \implies \) Evaluation placed here.
    - Assume: \( a \) does not modify \( e \)
    - Case \( e \in B[u] \). Induction hypothesis.
    - Case \( e \in A[u] \) \( \implies \) \( \pi' = \pi'_1(u', a', v')\pi'_2 \), such that \( \pi'_2 \) does not modify \( e \), and \( e \) required by \( a' \) \( \implies \) \( e \in B[u'] \). Induction hypothesis.
Non-degradation of performance

- On any path: Placement of $T_e = e$ corresponds to replacing an $e$ by $T_e$
  - $e$ not evaluated more often than in original program
Non-degradation of performance

- On any path: Placement of $T_e = e$ corresponds to replacing an $e$ by $T_e$
  - $e$ not evaluated more often than in original program
- Proof sketch: Placement only done where $e$ is very busy
Non-degradation of performance

- On any path: Placement of $T_e = e$ corresponds to replacing an $e$ by $T_e$
  - $e$ not evaluated more often than in original program
- Proof sketch: Placement only done where $e$ is very busy
  - I.e., every path from placement contains evaluation of $e$, which will be replaced
Non-degradation of performance

- On any path: Placement of $T_e = e$ corresponds to replacing an $e$ by $T_e$
  - $e$ not evaluated more often than in original program
- Proof sketch: Placement only done where $e$ is very busy
  - I.e., every path from placement contains evaluation of $e$, which will be replaced
  - Moreover, no path contains two evaluations of $e$, without usage of $e$ in between

By contradiction. Sketch on board.
Non-degradation of performance

- On any path: Placement of $T_e = e$ corresponds to replacing an $e$ by $T_e$
  - $e$ not evaluated more often than in original program
- Proof sketch: Placement only done where $e$ is very busy
  - I.e., every path from placement contains evaluation of $e$, which will be replaced
  - Moreover, no path contains two evaluations of $e$, without usage of $e$ in between
    - By contradiction. Sketch on board.
Partial Redundancy Elimination
  - Place evaluations such that
    - They are evaluated as early as possible, such that:
      - Expressions are only evaluated if also evaluated in original program

Analysis: Very Busy Expressions
Transformation: Placement on edges
  - where expression stops to be very busy
  - or is destroyed (and very busy at target)
Placement only if expression is not available
Application: Moving loop-invariant code

```c
for (i=0; i<N; ++i)
    a[i] = b + 3
```

- `b+3` evaluated in every iteration.
Application: Moving loop-invariant code

```c
for (i=0; i<N; ++i)
    a[i] = b + 3
```

- $b+3$ evaluated in every iteration.
- To the same value
Application: Moving loop-invariant code

```c
for (i=0; i<N; ++i)
    a[i] = b + 3
```

- $b+3$ evaluated in every iteration.
- To the same value
- Should be avoided!
Example (CFG)

CFG of previous example

1: i=0;
2: if (i<N) {
3:     a[i] = b + 3
4:     i=i+1
5:     goto 2
6: }


Analysis results for expression $b + 3$

1: i=0;
2: if (i<N) {
3:   a[i] = b + 3  // B
4:   i=i+1         // A
5:   goto 2       // A
6: }

Example (CFG)
Example (CFG)

Placement happens inside loop, on edge $(2, \text{Pos}(i < N), 3)$ :

1: \( i=0; \)
2: \( \text{if } (i<N) \) \{  
\hspace{1em} T=b+3  
3: \ a[i] = T  
4: \ i=i+1  
5: \ \text{goto 2}  
6: \  

Example (CFG)

There is no node outside loop for placing e!

1: i=0;
2: if (i<N) {
3:     T=b+3
4:     a[i] = T
5:     i=i+1
6:     goto 2
}
Solution: Loop inversion

- Idea: Convert while-loop to do-while loop

```plaintext
while (b) do c  \rightarrow \text{if (b) \{do c while (b)\}}
```
Solution: Loop inversion

- Idea: Convert while-loop to do-while loop

  \[
  \text{while (b) do c} \quad \rightarrow \quad \text{if (b) \{do c while (b)\}}
  \]

- Does not change semantics
Solution: Loop inversion

- Idea: Convert while-loop to do-while loop

```plaintext
while (b) do c  \rightarrow if (b) {do c while (b)}
```

- Does not change semantics
- But creates node for placing loop invariant code
Example

CFG after loop inversion

1: \texttt{i=0;}
2: \texttt{if (i<N) \{}
3: \texttt{a[i] = b + 3}
4: \texttt{i=i+1}
5: \texttt{if (i<N) goto 3}
6: \texttt{\}}
Example

Analysis results for expression $b + 3$

1: $i=0$;
2: if (i<N) {
3:   $a[i] = b + 3$  // B
4:   $i=i+1$       // A
5:   if (i<N) goto 3  // A
6: }

Example

Placement happens outside loop, on edge \((2, \text{Pos}(i < N), 3) :\)

1: i=0;
2: if (i<N) {
  x: T=b+3;
3:   a[i] = T
4:   i=i+1
5:   if (i<N) goto 3
6: }

Conclusion

• PRE may move loop-invariant code out of the loop
Conclusion

- PRE may move loop-invariant code out of the loop
- Only for do-while loops
Conclusion

- PRE may move loop-invariant code out of the loop
- Only for do-while loops
- To also cover while-loops: Apply loop-inversion first
Conclusion

- PRE may move loop-invariant code out of the loop
- Only for do-while loops
- To also cover while-loops: Apply loop-inversion first
- Loop inversion: No additional statements executed.
  - But slight increase in code size.
  - Side note: Better pipelining behavior (Less jumps executed)
Detecting loops in CFG

- Loop inversion can be done in AST
Detecting loops in CFG

- Loop inversion can be done in AST
  - But only if AST is available
Detecting loops in CFG

- Loop inversion can be done in AST
  - But only if AST is available
  - What if some other CFG-based transformations have already been run?
Detecting loops in CFG

- Loop inversion can be done in AST
  - But only if AST is available
  - What if some other CFG-based transformations have already been run?
- Need CFG-based detection of loop headers
Detecting loops in CFG

- Loop inversion can be done in AST
  - But only if AST is available
  - What if some other CFG-based transformations have already been run?
- Need CFG-based detection of loop headers
- Idea: Predominators
Predominators

- A node $u$ pre-dominates $v$ ($u \Rightarrow v$), iff every path $v_0 \rightarrow^* v$ contains $u$. 
Predominators

- A node $u$ pre-dominates $v$ ($u \Rightarrow v$), iff every path $v_0 \rightarrow^* v$ contains $u$.
- $\Rightarrow$ is a partial order.
  - reflexive, transitive, anti-symmetric
Predominator example
Predominator example
Remark: Immediate Predominator

- The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
Remark: Immediate Predominator

- The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, $v_0$ dominates every node (root of tree)
Remark: Immediate Predominator

- The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, $v_0$ dominates every node (root of tree)
  - Every node has at most one immediate predecessor:
Remark: Immediate Predominator

- The ⇒-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, $v_0$ dominates every node (root of tree)
  - Every node has at most one immediate predecessor:
    - Assume $u_1 \Rightarrow v$, $u_2 \Rightarrow v$, and neither $u_1 \Rightarrow u_2$ nor $u_2 \Rightarrow u_1$
Remark: Immediate Predominator

- The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, $v_0$ dominates every node (root of tree)
  - Every node has at most one immediate predecessor:
    - Assume $u_1 \Rightarrow v$, $u_2 \Rightarrow v$, and neither $u_1 \Rightarrow u_2$ nor $u_2 \Rightarrow u_1$
    - Regard path $\pi$ to $v$. Assume, wlog, $\pi = \pi_1 u_1 \pi_2 v$, such that $u_1, u_2 \notin \pi_2$
Remark: Immediate Predominator

• The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
  • Clearly, $v_0$ dominates every node (root of tree)
  • Every node has at most one immediate predecessor:
    • Assume $u_1 \Rightarrow v$, $u_2 \Rightarrow v$, and neither $u_1 \Rightarrow u_2$ nor $u_2 \Rightarrow u_1$
    • Regard path $\pi$ to $v$. Assume, wlog, $\pi = \pi_1 u_1 \pi_2 v$, such that $u_1, u_2 \notin \pi_2$
    • Then, every path $\pi'$ to $u_1$ gives rise to path $\pi'\pi_2$ to $v$. 
Remark: Immediate Predominator

- The ⇒-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, \( v_0 \) dominates every node (root of tree)
  - Every node has at most one immediate predecessor:
    - Assume \( u_1 \Rightarrow v \), \( u_2 \Rightarrow v \), and neither \( u_1 \Rightarrow u_2 \) nor \( u_2 \Rightarrow u_1 \)
    - Regard path \( \pi \) to \( v \). Assume, wlog, \( \pi = \pi_1 u_1 \pi_2 v \), such that \( u_1, u_2 \notin \pi_2 \)
    - Then, every path \( \pi' \) to \( u_1 \) gives rise to path \( \pi' \pi_2 \) to \( v \).
    - Thus, \( u_2 \in \pi' \pi_2 \). By asm, not in \( \pi_2 \). I.e. \( u_2 \in \pi' \).
Remark: Immediate Predominator

- The $\Rightarrow$-relation, with reflexivity and transitivity removed, is a tree
  - Clearly, $v_0$ dominates every node (root of tree)
  - Every node has at most one immediate predecessor:
    - Assume $u_1 \Rightarrow v$, $u_2 \Rightarrow v$, and neither $u_1 \Rightarrow u_2$ nor $u_2 \Rightarrow u_1$
    - Regard path $\pi$ to $v$. Assume, wlog, $\pi = \pi_1 u_1 \pi_2 v$, such that $u_1, u_2 \notin \pi_2$
    - Then, every path $\pi'$ to $u_1$ gives rise to path $\pi' \pi_2$ to $v$.
    - Thus, $u_2 \in \pi' \pi_2$. By asm, not in $\pi_2$. I.e. $u_2 \in \pi'$.
    - Thus, $u_2 \Rightarrow u_1$, contradiction.
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$. 
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $\llbracket (\_, \_, v) \rrbracket^\# P = P \cup \{ v \}, \quad d_0 = \{ v_0 \}$
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $[[(_, _, v)]]^# P = P \cup \{v\}$, $d_0 = \{v_0\}$
  - Collects nodes on paths
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $\llbracket(\_,\_,v)\rrbracket^\# P = P \cup \{v\}, \ d_0 = \{v_0\}$
  - Collects nodes on paths
  - Distributive, i.e. MOP can be precisely computed
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $\llbracket(\_\_, \_\_, v)\rrbracket \# P = P \cup \{v\}, \ d_0 = \{v_0\}$
  - Collects nodes on paths
  - Distributive, i.e. MOP can be precisely computed
- $\text{MOP}[u] = \bigcap\{\llbracket\pi\rrbracket \# \{v_0\} \mid v_0 \rightarrow^* u\}$

Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $\llbracket(\_\_, \_\_, v)\rrbracket^\# P = P \cup \{v\}, \ d_0 = \{v_0\}$
  - Collects nodes on paths
  - Distributive, i.e. MOP can be precisely computed
- $\text{MOP}[u] = \bigcap \{\llbracket\pi\rrbracket^\# \{v_0\} \mid v_0 \to^* u\}$
  - Which is precisely the set of nodes occurring on all paths to $u$
Computing predominators

- Use a (degenerate) dataflow analysis. Forward, Must. Domain $2^V$.
- $\llbracket (\_,\_, v) \rrbracket^# P = P \cup \{ v \}$, $d_0 = \{ v_0 \}$
  - Collects nodes on paths
  - Distributive, i.e. MOP can be precisely computed
- $\text{MOP}[u] = \bigcap\{ \llbracket \pi \rrbracket^# \{ v_0 \} \mid v_0 \rightarrow^* u \}$
  - Which is precisely the set of nodes occurring on all paths to $u$
  - I.e. the predominators of $u$
Detecting loops using predominators

- Observation: Entry node of loop predominates all nodes in loop body.

\[
\begin{align*}
\text{Neg}(e) & \quad \text{Pos}(e) \\
\text{Neg}(e) & \quad \text{Pos}(e)
\end{align*}
\]

\[v \in P[u] \implies \]

\[
\begin{align*}
\text{Neg}(e) & \quad \text{Pos}(e) \\
\text{Neg}(e) & \quad \text{Pos}(e)
\end{align*}
\]
Detecting loops using predominators

- Observation: Entry node of loop predominates all nodes in loop body.
  - In particular the start node of the back edge

\[ \text{if } v \in P[u] \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]

\[ \text{Neg}(e) \quad \text{Pos}(e) \]
Detecting loops using predominators

- Observation: Entry node of loop predominates all nodes in loop body.
  - In particular the start node of the back edge
- Loop inversion transformation

\[
\text{if } v \in P(u) \rightarrow
\]

\[
\begin{align*}
\text{Neg}(e) & \quad \text{Pos}(e) \\
\text{Pos}(e) & \quad \text{Neg}(e)
\end{align*}
\]
Detecting loops using predominators

- Observation: Entry node of loop predominates all nodes in loop body.
  - In particular the start node of the back edge
- Loop inversion transformation

\[
\begin{align*}
  v & \in P[u] \\
  & \mapsto \\
  & \begin{cases} 
    v & \text{Neg}(e) \\
    u & \text{Pos}(e)
  \end{cases}
\end{align*}
\]

- Obviously correct
Example

CFG of running example

1. $i = 0$
2. $\text{Neg}(i < N)$
3. $a[i] = b + 3$
4. $\text{Pos}(i < N)$
5. $i = i + 1$
6. Loop back to 2
Example

$2 \in P[6]$, identified pattern for transformation
Example
Inverted loop

1. i = 0
2. Neg(i < N)  Pos(i < N)
3. Neg(i < N)  Pos(i < N)
4. a[i] = b + 3
5. i = i + 1
6.
Warning

- Transformation fails to invert all loops
Warning

- Transformation fails to invert all loops
- E.g., if evaluation of condition is more complex
Warning

- Transformation fails to invert all loops
- E.g., if evaluation of condition is more complex
  - E.g., condition contains loads
  - `while (M[0])` ...
Warning

- Transformation fails to invert all loops
- E.g., if evaluation of condition is more complex
  - E.g., condition contains loads
  - `while (M[0]) ...

\[x = M[0]\]
\[\text{Neg}(x)\]
\[\text{Pos}(x)\]
Warning

- Transformation fails to invert all loops
- E.g., if evaluation of condition is more complex
  - E.g., condition contains loads
  - \texttt{while (M[0])} ...

- We would have to duplicate the load-edge, too
Partial redundancy elimination
- Very busy expressions
- Place evaluations as early as possible

Loop inversion
- \texttt{while} $\rightarrow$ \texttt{do-while}
- Enables moving loop-invariant code out of loops
- Computation on CFG: Use pre-dominators
# Table of Contents

1. Introduction

2. Removing Superfluous Computations

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)
   - Partial Redundancy Elimination
   - Partially Dead Assignments

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Motivation

- Consider program

  \[
  T = x+1
  \]

  \[
  \text{if (*) then } M[0] = T
  \]

  - Assume (*) does not use \( T \), and \( T \) dead at end
Motivation

- Consider program
  
  \[
  T = x + 1 \\
  \text{if (*) then } M[0] = T
  \]
  
  - Assume (*) does not use \( T \), and \( T \) dead at end
  - Assignment \( T = x + 1 \) only required on one path
Motivation

- Consider program

\[
T = x+1 \\
\text{if}(\ast) \text{ then } M[0]=T
\]

- Assume (\ast) does not use \( T \), and \( T \) dead at end
- Assignment \( T = x + 1 \) only required on one path
- Would like to move assignment into this path

\[
\text{if}(\ast) \text{ then } \{T = x+1; \ M[0]=T\}
\]
Idea

- Delay assignments as long as possible
Idea

- Delay assignments as long as possible
- Can delay assignment $x := e$ over edge $k$, if
  - $x$ is not used, nor defined by $k$
  - No variable of $e$ is defined by $k$
Delayable Assignments Analysis

- Domain: \( \{ x = e \mid x \in \text{Reg} \land e \in \text{Expr} \} \), Ordering: \( \sqsubseteq \sqsupseteq \), forward
- I.e. forward must analysis
Delayable Assignments Analysis

- Domain: \{ x = e \mid x \in \text{Reg} \land e \in \text{Expr} \}, Ordering: \sqsubseteq \subseteq, forward
  - I.e. forward must analysis
- \( d_0 = \emptyset \), no delayable assignments at program start

\[
\begin{align*}
\mathbb{[Nop]} \# D &= D \\
\mathbb{[x = e]} \# D &= D \setminus (\text{Ass}(e) \cup \text{Occ}(x)) \cup \{x = e\} \\
\mathbb{[\text{Pos}(e)]} \# D &= D \setminus \text{Ass}(e) \\
\mathbb{[\text{Neg}(e)]} \# D &= D \setminus \text{Ass}(e) \\
\mathbb{[x = M[e]]} \# D &= D \setminus (\text{Ass}(e) \cup \text{Occ}(x)) \\
\mathbb{[M[e_1] = e_2]} \# D &= D \setminus (\text{Ass}(e_1) \cup \text{Ass}(e_2))
\end{align*}
\]

where

- \( \text{Ass}(e) := \{ x = e' \mid x \in \text{Reg}(e) \} \) Assignments to variable in \( e \)
- \( \text{Occ}(x) := \{ x' = e \mid x = x' \lor x \in \text{Reg}(e) \} \) Assignments in which \( x \) occurs
Intuition

- $x = e \in D[u]$: On every path reaching $u$, the assignment $x = e$ is executed, and no edge afterwards:
  - Depends on $x$
  - Changes $x$ or a variable of $e$
Intuition

- $x = e \in D[u]$: On every path reaching $u$, the assignment $x = e$ is executed, and no edge afterwards:
  - Depends on $x$
  - Changes $x$ or a variable of $e$

- Thus, this assignment can be safely moved to $u$
Transformation

• Delay assignments as far as possible
Transformation

- Delay assignments as far as possible
- Do not place assignments to dead variables
Transformation

- Delay assignments as far as possible
- Do not place assignments to dead variables
- \((u, x = e, v) \mapsto (u, ss_1, w), (w, ss_2, v)\) where
  - \(ss_1\) Assignments to live variables that cannot be delayed over action \(x = e\)
  - \(ss_2\) Assignments to live variables delayable due to edge, but not at \(v\) (Other paths over \(v\))
  - \(w\) is fresh node
Transformation

- Delay assignments as far as possible
- Do not place assignments to dead variables
- \((u, x = e, v) \mapsto (u, ss_1, w), (w, ss_2, v)\) where
  - \(ss_1\) Assignments to live variables that cannot be delayed over action \(x = e\)
  - \(ss_2\) Assignments to live variables delayable due to edge, but not at \(v\) (Other paths over \(v\))
  - \(w\) is fresh node
  - Formally

\[
ss_1 := \{ x' = e' \in D[u] \setminus \llbracket x = e \rrbracket^* D[u] \mid x' \in L[u] \}
\]

\[
ss_2 = \{ x' = e' \in \llbracket x = e \rrbracket^* D[u] \setminus D[v] \mid x' \in L[v] \}
\]
Transformation

- Delay assignments as far as possible
- Do not place assignments to dead variables
- $(u, x = e, v) \mapsto (u, ss_1, w), (w, ss_2, v)$ where
  - $ss_1$ Assignments to live variables that cannot be delayed over action $x = e$
  - $ss_2$ Assignments to live variables delayable due to edge, but not at $v$ (Other paths over $v$)
- $w$ is fresh node
- Formally
  
  $ss_1 := \{x' = e' \in D[u] \setminus [x = e]^\#D[u] \mid x' \in L[u]\}$
  $ss_2 = \{x' = e' \in [x = e]^\#D[u] \setminus D[v] \mid x' \in L[v]\}$

- $(u, a, v) \mapsto (u, ss_1, w_1), (w_1, a, w_2), (w_2, ss_2, v)$ for $a$ not assignment
  
  $ss_1 := \{x' = e' \in D[u] \setminus [a]^\#D[u] \mid x' \in L[u]\}$
  $ss_2 = \{x' = e' \in [a]^\#D[u] \setminus D[v] \mid x' \in L[v]\}$
Transformation

- Delay assignments as far as possible
- Do not place assignments to dead variables
- \((u, x = e, v) \mapsto (u, ss_1, w), (w, ss_2, v)\) where
  - \(ss_1\) Assignments to live variables that cannot be delayed over action \(x = e\)
  - \(ss_2\) Assignments to live variables delayable due to edge, but not at \(v\) (Other paths over \(v\))
  - \(w\) is fresh node
  - Formally
    \[
    ss_1 := \{ x' = e' \in D[u] \setminus \llbracket x = e \rrbracket^# D[u] \mid x' \in L[u] \}
    \[
    ss_2 = \{ x' = e' \in \llbracket x = e \rrbracket^# D[u] \setminus D[v] \mid x' \in L[v] \}
    \]
- \((u, a, v) \mapsto (u, ss_1, w_1), (w_1, a, w_2), (w_2, ss_2, v)\) for \(a\) not assignment
  - \(ss_1 := \{ x' = e' \in D[u] \setminus \llbracket a \rrbracket^# D[u] \mid x' \in L[u] \}
  - \(ss_2 = \{ x' = e' \in \llbracket a \rrbracket^# D[u] \setminus D[v] \mid x' \in L[v] \}
- \(v_e \in V_{\text{end}} \mapsto (v_e, D[v_e], v'_e)\)
  - where \(v'_e\) is fresh end node, and \(v_e\) no end node any more.
Dependent actions

- Two actions $a_1, a_2$ are independent, iff $[a_1 a_2] = [a_2 a_1]$
- Actions may be swapped
Dependent actions

- Two actions $a_1, a_2$ are independent, iff $[a_1 a_2] = [a_2 a_1]$
  - Actions may be swapped
- Assignments only delayed over independent actions
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant

Proof sketch:

$x = e$ only inserted by $\{ \}$, after all dependent assignments removed

Regard path with assignment $(u, x = e, v)$.

We have $x = e \in \{ x = e \} \# D[u]$. (1) Either placed here, (2) $x$ dead, (3) or delayable at $v$.

(1) No change of path
(2), not (3): Assignment dropped, but was dead anyway
(3). Three subcases: Sketch on whiteboard!

(3.1) $x = e$ stops being delayable due to dependent action
$\Rightarrow$ Assignment placed before this action, if live
(3.2) $x = e$ stops being delayable at node
$\Rightarrow$ Assignment placed after edge to this node, if live
(3.3) $x = e$ delayable until end
$\Rightarrow$ Assignment placed at end node, if live
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $[\cdot\cdot\cdot]#$, after all dependent assignments removed
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $\llbracket \cdot \rrbracket^\#$, after all dependent assignments removed
- Regard path with assignment $(u, x = e, v)$. 

Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $[\cdot]^\#$, after all dependent assignments removed
- Regard path with assignment $(u, x = e, v)$.
- We have $x = e \in [x = e]^\# D[u]$. (1) Either placed here, (2) $x$ dead, (3) or delayable at $v$
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $[\cdot]$#, after all dependent assignments removed
- Regard path with assignment $(u, x = e, v)$.
- We have $x = e \in [x = e]^# D[u]$. (1) Either placed here, (2) $x$ dead, (3) or delayable at $v$
  - (1) No change of path
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $[[\cdot]]^\#$, after all dependent assignments removed
- Regard path with assignment $(u, x = e, v)$.
- We have $x = e \in [[x = e]]^\# D[u]$. (1) Either placed here, (2) $x$ dead, (3) or delayable at $v$
  - (1) No change of path
  - (2), not (3): Assignment dropped, but was dead anyway
Correctness (Rough Sketch)

- First: $D[u]$ does never contain dependent assignments
  - Placement order is irrelevant
  - Proof sketch: $x = e$ only inserted by $[\cdot]^{\#}$, after all dependent assignments removed
- Regard path with assignment $(u, x = e, v)$.
- We have $x = e \in [x = e]^{\#} D[u]$. (1) Either placed here, (2) $x$ dead, (3) or delayable at $v$
  - (1) No change of path
  - (2), not (3): Assignment dropped, but was dead anyway
  - (3). Three subcases: Sketch on whiteboard!
    - (3.1) $x = e$ stops being delayable due to dependent action
      $\implies$ Assignment placed before this action, if live
    - (3.2) $x = e$ stops being delayable at node
      $\implies$ Assignment placed after edge to this node, if live
    - (3.3) $x = e$ delayable until end
      $\implies$ Assignment placed at end node, if live
Example

1: $T = x+1$  \hspace{1cm} D: {}  \hspace{1cm} L: \{x\}
2: if (*) then \{}  \hspace{1cm} D: \{T=x+1\}  \hspace{1cm} L: \{T\}
3: \hspace{1cm} M[0]=T  \hspace{1cm} D: \{T=x+1\}  \hspace{1cm} L: \{T\}
4: \hspace{1cm} Nop  \hspace{1cm} D: {}  \hspace{1cm} L: {}
5: \}  \hspace{1cm} D: {}  \hspace{1cm} L: {}
Example

1: T = x+1          D: {}          L: {x}
2: if (*) then {    D: {T=x+1}    L: {T}
3: M[0]=T           D: {T=x+1}    L: {T}
4: Nop              D: {}          L: {}
5: }                D: {}          L: {}

• Placement of $T = x + 1$ before edge (3, 4)
  • We have $T = x + 1 \in D[3] \setminus \{M[0] = T\} \# D[4]$, and $T \in L[3]$
Example

1: T = x+1  D: {}  L: {x}
2: if (*) then {  D: {T=x+1}  L: {T}
3: M[0]=T  D: {T=x+1}  L: {T}
4: Nop  D: {}  L: {}
5: }

• Placement of $T = x + 1$ before edge (3, 4)
  • We have $T = x + 1 \in D[3] \setminus [M[0] = T] \# D[4]$, and $T \in L[3]$

1:
2: if (*) then {
3: T = x+1
x: M[0]=T
4: Nop
5: }
Summary

- PDE is generalization of DAE
  - Assignment to dead variable will not be placed
  - As variable is dead on all paths leaving that assignment
Summary

- PDE is generalization of DAE
  - Assignment to dead variable will not be placed
  - As variable is dead on all paths leaving that assignment
- May also use true liveness.
Summary

- PDE is generalization of DAE
  - Assignment to dead variable will not be placed
  - As variable is dead on all paths leaving that assignment
- May also use true liveness.
- Non degradation of performance
  - Number of assignments on each path does not increase (without proof)
  - In particular: Assignments not moved into loops (Whiteboard)
Summary

- PDE is generalization of DAE
  - Assignment to dead variable will not be placed
  - As variable is dead on all paths leaving that assignment
- May also use true liveness.
- Non degradation of performance
  - Number of assignments on each path does not increase (without proof)
  - In particular: Assignments not moved into loops (Whiteboard)
- Profits from loop inversion (Whiteboard)
Conclusion

- Design of meaningful optimization is nontrivial
- Optimizations may only be useful in connection with others
- Order of optimization matters
- Some optimizations can be iterated
## A meaningful ordering

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINV</td>
<td>Loop inversion</td>
</tr>
<tr>
<td>ALIAS</td>
<td>Alias analysis</td>
</tr>
<tr>
<td>AI</td>
<td>Constant propagation</td>
</tr>
<tr>
<td></td>
<td>Intervals</td>
</tr>
<tr>
<td>RE</td>
<td>(Simple) redundancy elimination</td>
</tr>
<tr>
<td>CP</td>
<td>Copy propagation</td>
</tr>
<tr>
<td>DAE</td>
<td>Dead assignment elimination</td>
</tr>
<tr>
<td>PRE</td>
<td>Partial redundancy elimination</td>
</tr>
<tr>
<td>PDE</td>
<td>Partially dead assignment elimination</td>
</tr>
</tbody>
</table>
Table of Contents

1 Introduction
2 Removing Superfluous Computations
3 Abstract Interpretation
4 Alias Analysis
5 Avoiding Redundancy (Part II)
6 Interprocedural Analysis
7 Analysis of Parallel Programs
8 Replacing Expensive by Cheaper Operations
9 Exploiting Hardware Features
10 Optimization of Functional Programs
• Partially dead assignments
• Started semantics with procedures
Motivation

• So far:
  • Only regarded single procedure
  • But program typically has many procedures
  • Need to be pessimistic about their effect
Motivation

- So far:
  - Only regarded single procedure
  - But program typically has many procedures
  - Need to be pessimistic about their effect

- Now:
  - Analyze effects of procedures
  - Restrict to procedures without parameters/return values
  - But with local and global variables!
  - Can emulate parameters/return values!
Extending the semantics

- Each procedure $f$ represented by control flow graph $G^f$. Assume these are distinct!
Extending the semantics

- Each procedure $f$ represented by control flow graph $G_f$. Assume these are distinct!
- Add edge label $f()$ for call of procedure $f$
Extending the semantics

- Each procedure \( f \) represented by control flow graph \( G^f \). Assume these are distinct!
- Add edge label \( f() \) for call of procedure \( f \)
- Procedure main must exist

\[
\begin{align*}
\text{Conf} &= \text{Stack} \times \text{Globals} \times \text{Store} \\
\text{Globals} &= \text{Glob} \rightarrow \text{Val} \\
\text{Store} &= \text{Addr} \rightarrow \text{Val} \\
\text{Stack} &= \text{Frame}^+ \\
\text{Frame} &= \mathcal{V} \times \text{Locals} \\
\text{Locals} &= \text{Loc} \rightarrow \text{Val}
\end{align*}
\]

- where \( \text{Glob} \) are global variable names, and \( \text{Loc} \) are local variable names
Execution, small-step semantics

- $\llbracket e \rrbracket(\rho_l, \rho_g) : \text{Val. Value of expression.}$
Execution, small-step semantics

- $\llbracket e \rrbracket(\rho_l, \rho_g)$: Val. Value of expression.
- $\llbracket a \rrbracket(\rho_l, \rho_g, \mu)$: Locals $\times$ Globals $\times$ Store. Effect of (non-call) action.
Execution, small-step semantics

- $\llbracket e \rrbracket (\rho_l, \rho_g)$ : Val. Value of expression.
- $\llbracket a \rrbracket (\rho_l, \rho_g, \mu)$ : Locals $\times$ Globals $\times$ Store. Effect of (non-call) action.
- Initial configuration: $((v_0^{main}, \lambda x. 0), \rho, \mu)$
Execution, small-step semantics

- $\llbracket e \rrbracket(\rho_l, \rho_g) : \text{Val. Value of expression.}$
- $\llbracket a \rrbracket(\rho_l, \rho_g, \mu) : \text{Locals } \times \text{Globals } \times \text{Store. Effect of (non-call) action.}$
- Initial configuration: $([v_0^{\text{main}}, \lambda x. 0], \rho_g, \mu)$
- $\rightarrow \subseteq \text{Conf } \times \text{Conf}$

$$\left((u, \rho_l)\sigma, \rho_g, \mu\right) \rightarrow \left((v, \rho_l)'\sigma, \rho_g', \mu'\right) \quad \text{(basic)}$$

if $(u, a, v) \in E$ $\land \llbracket a \rrbracket(\rho_l, \rho_g, \mu) = (\rho_l', \rho_g', \mu')$

$$\left((u, \rho_l)\sigma, \rho_g, \mu\right) \rightarrow \left((v_0^f, \lambda x. 0)(v, \rho_l)\sigma, \rho_g, \mu\right) \quad \text{(call)}$$

if $(u, f(), v) \in E$

$$\left((u, \_\_)\sigma, \rho_g, \mu\right) \rightarrow (\sigma, \rho_g, \mu) \quad \text{(return)}$$

if $u \in V_{\text{end}} \land \sigma \neq \varepsilon$
Example (factorial)

main():
    M[0] = fac(3)

fac(x):
    if (x <= 1) return 1
    else return x * fac(x-1)
Example (factorial)

main():
   M[0] = fac(3)

fac(x):
   if (x <= 1) return 1
   else return x * fac(x-1)

Translation to no arguments and return values

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
f3: Gret = 1
   } else {
f4: Gx = x-1
f5: fac()
f6: Gret = x*Gret
f7: }
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
f3: Gret = 1
} else {
f4: Gx = x-1
f5: fac()
f6: Gret = x*Gret
f7: }

A run:
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
f3:   Gret = 1
   } else {
   f4:   Gx = x-1
   f5:   fac()
   f6:   Gret = x*Gret
   f7:   }

A run:

<table>
<thead>
<tr>
<th>(m1, -)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gx: -</td>
</tr>
<tr>
<td>Gret: -</td>
</tr>
<tr>
<td>M[0]: -</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
  f3: Gret = 1
} else {
  f4: Gx = x-1
  f5: fac()
  f6: Gret = x*Gret
  f7: }

A run:

<table>
<thead>
<tr>
<th>(m2, −)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gx : 3, Gret : −, M[0] : −</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
    f3: Gret = 1
} else {
    f4: Gx = x-1
    f5: fac()
    f6: Gret = x*Gret
    f7: }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f1, x : 0)</td>
<td></td>
</tr>
<tr>
<td>(m3, −)</td>
<td></td>
</tr>
<tr>
<td>Gx : 3, Gret : −, M[0] : −</td>
<td></td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
 f1: x = Gx
 f2: if (x <= 1) {
 f3:   Gret = 1
 } else {
 f4:   Gx = x-1
 f5:   fac()
 f6:   Gret = x*Gret
 f7: }

A run:

<table>
<thead>
<tr>
<th>(f2, x : 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m3, −)</td>
</tr>
<tr>
<td>Gx : 3, Gret : −, M[0] : −</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:

fac():
f1:  x = Gx
f2:  if (x <= 1) {
    f3:    Gret = 1
f3:    } else {
    f4:    Gx = x-1
f5:    fac()
    f6:    Gret = x*Gret
f7:    }

A run:

\[
\begin{array}{|c|}
\hline
(f4, x : 3) \\
(m3, -) \\
Gx : 3, Gret : -, M[0] : - \\
\hline
\end{array}
\]
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
f3:  Gret = 1
} else {
f4:  Gx = x-1
f5:  fac()
f6:  Gret = x*Gret
f7:  }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f5, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, −)</td>
<td></td>
</tr>
<tr>
<td>Gx : 2, Gret : −, M[0] : −</td>
<td></td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
  f3:   Gret = 1
} else {
  f4:   Gx = x-1
  f5:   fac()
  f6:   Gret = x*Gret
  f7: }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f1, x : 0)</td>
<td></td>
</tr>
<tr>
<td>(f6, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, −)</td>
<td></td>
</tr>
<tr>
<td>Gx : 2, Gret : −, M[0] : −</td>
<td></td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
  f3: Gret = 1
} else {
  f4: Gx = x-1
  f5: fac()
  f6: Gret = x*Gret
  f7: }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f2, x : 2)</td>
<td></td>
</tr>
<tr>
<td>(f6, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, −)</td>
<td></td>
</tr>
</tbody>
</table>

Gx : 2, Gret : −, M[0] : −
Example (factorial)

main():
m1:  Gx = 3;
m2:   fac()
m3:  M[0] = Gret
m4:

fac():
f1:  x = Gx
f2:  if (x <= 1) {
  f3:    Gret = 1
} else {
  f4:    Gx = x-1
  f5:     fac()
  f6:     Gret = x*Gret
  f7:   }

A run:

<table>
<thead>
<tr>
<th>(f4, x : 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f6, x : 3)</td>
</tr>
<tr>
<td>(m3, -)</td>
</tr>
<tr>
<td>Gx : 2, Gret : - , M[0] : -</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:

fac():
f1:  x = Gx
f2:  if (x <= 1) {
  f3:    Gret = 1
  } else {
  f4:    Gx = x-1
  f5:    fac()
  f6:    Gret = x*Gret
  f7:  }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f5, x: 2)</td>
<td></td>
</tr>
<tr>
<td>(f6, x: 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, -)</td>
<td></td>
</tr>
</tbody>
</table>

Gx: 1, Gret: -, M[0]: -
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
f3:  Gret = 1
} else {
  f4:  Gx = x-1
  f5:  fac()
  f6:  Gret = x*Gret
  f7:  }

A run:

| (f1, x: 0) |
| (f6, x: 2) |
| (f6, x: 3) |
| (m3, −) |
| Gx : 1, Gret : −, M[0] : − |
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:  

fac():
f1:  x = Gx
f2:  if (x <= 1) {
    f3:    Gret = 1
} else {
    f4:    Gx = x-1
    f5:    fac()
    f6:    Gret = x*Gret
    f7:  }

A run:

\[(f2, x : 1)\]
\[(f6, x : 2)\]
\[(f6, x : 3)\]
\[(m3, -)\]
\[Gx : 1, Gret : -, M[0] : -\]
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
  f3: Gret = 1
  } else {
  f4: Gx = x-1
  f5: fac()
  f6: Gret = x*Gret
  f7: }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f3, x : 1)</td>
<td></td>
</tr>
<tr>
<td>(f6, x : 2)</td>
<td></td>
</tr>
<tr>
<td>(f6, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, –)</td>
<td></td>
</tr>
</tbody>
</table>

Gx : 1, Gret : –, M[0] : –
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
f1: x = Gx
f2: if (x <= 1) {
  f3: Gret = 1
} else {
  f4: Gx = x-1
  f5: fac()
  f6: Gret = x*Gret
  f7: }

A run:

<table>
<thead>
<tr>
<th>(f7, x : 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f6, x : 2)</td>
</tr>
<tr>
<td>(f6, x : 3)</td>
</tr>
<tr>
<td>(m3, −)</td>
</tr>
<tr>
<td>Gx : 1, Gret : 1, M[0] : −</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:  

fac():
f1:  x = Gx
f2:  if (x <= 1) {
  f3:    Gret = 1
  } else {
  f4:    Gx = x-1
  f5:    fac()
  f6:    Gret = x*Gret
  f7:  }

A run:

\[
(f6, x : 2)
\]

\[
(f6, x : 3)
\]

\[
(m3, -)
\]

\[
Gx : 1, \, Gret : 1, \, M[0] : -
\]
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:

fac():
f1:  x = Gx
f2:  if (x <= 1) {
    f3:    Gret = 1
    } else {
    f4:    Gx = x-1
    f5:    fac()
    f6:    Gret = x*Gret
    f7:    }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f7, x : 2)</td>
<td></td>
</tr>
<tr>
<td>(f6, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, −)</td>
<td></td>
</tr>
<tr>
<td>Gx : 1, Gret : 2, M[0] : −</td>
<td></td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1:  Gx = 3;
m2:  fac()
m3:  M[0] = Gret
m4:

fac():
f1:  x = Gx
f2:  if (x <= 1) {
  f3:    Gret = 1
  } else {
  f4:    Gx = x-1
  f5:    fac()
  f6:    Gret = x*Gret
  f7: }

A run:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(f6, x : 3)</td>
<td></td>
</tr>
<tr>
<td>(m3, –)</td>
<td></td>
</tr>
<tr>
<td>Gx : 1, Gret : 2, M[0] : –</td>
<td></td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
  f1: x = Gx
  f2: if (x <= 1) {
    f3: Gret = 1
    } else {
    f4: Gx = x-1
    f5: fac()
    f6: Gret = x*Gret
    f7: }

A run:

| (f7, x : 3)  |
| (m3, −)      |
| Gx : 1, Gret : 6, M[0] : − |
Example (factorial)

main():
m1: Gx = 3;
m2: fac() 
m3: M[0] = Gret
m4: 

fac():
f1: x = Gx
f2: if (x <= 1) {
    f3: Gret = 1
} else {
    f4: Gx = x-1
    f5: fac() 
    f6: Gret = x*Gret
    f7: }

A run:

<table>
<thead>
<tr>
<th>(m3, -)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gx : 1, Gret : 6, M[0] : -</td>
</tr>
</tbody>
</table>
Example (factorial)

main():
m1: Gx = 3;
m2: fac()
m3: M[0] = Gret
m4:

fac():
  f1: x = Gx
  f2: if (x <= 1) {
  f3:   Gret = 1
  } else {
  f4:   Gx = x-1
  f5:   fac()
  f6:   Gret = x*Gret
  f7: }

A run:

<table>
<thead>
<tr>
<th>(m4, −)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gx : 1, Gret : 6, M[0] : 6</td>
</tr>
</tbody>
</table>
Realistic Call Semantic

• On real machine, procedure call involves
  • Save registers
  • Create stack frame
    • Push parameters, return address
    • Allocate stack space for local variables
  • Jump to procedure body
Realistic Call Semantic

- On real machine, procedure call involves
  - Save registers
  - Create stack frame
    - Push parameters, return address
    - Allocate stack space for local variables
  - Jump to procedure body
- Procedure return
  - Free stack frame
    - Jump to return address
    - Remove parameters from stack
  - Restore registers
  - Handle result
Realistic Call Semantic

- On real machine, procedure call involves
  - Save registers
  - Create stack frame
    - Push parameters, return address
    - Allocate stack space for local variables
  - Jump to procedure body
- Procedure return
  - Free stack frame
    - Jump to return address
    - Remove parameters from stack
  - Restore registers
  - Handle result
- Short demo: cdecl calling convention on x86
Inlining

- Procedure call is quite expensive

```c
int f(int a, int b) {  
    int l = a + b  
    return l + l  
}

int g (int a) {  
    return f(a,a)  
}
```
Inlining

- Procedure call is quite expensive
- Idea: Copy procedure body to call-site

```c
int f(int a, int b) {
    int l = a + b
    return l + l
}

int g (int a) {
    int l = a + a
    return l + l
}
```
Problems

- Have to keep distinct local variables
Problems

- Have to keep distinct local variables
  - Our simple language has no parameters/ returns
Problems

- Have to keep distinct local variables
  - Our simple language has no parameters/ returns
- Be careful with recursion
  - Inlining optimization might not terminate
Problems

- Have to keep distinct local variables
  - Our simple language has no parameters/ returns
- Be careful with recursion
  - Inlining optimization might not terminate
- Too much inlining of (non-recursive procedures) may blow up the code

```c
void m0() {x=x+1}
void m1() {m0();m0()}
void m2() {m1();m1()}
...
void mN() {mN-1(); mN-1()}
```

$$O(2^N)$$
Problems

- Have to keep distinct local variables
  - Our simple language has no parameters/returns
- Be careful with recursion
  - Inlining optimization might not terminate
- Too much inlining of (non-recursive procedures) may blow up the code
  - Exponentially!

```cpp
void m0() {x=x+1}
void m1() {m0(); m0();}
void m2() {m1(); m1();}
...
void mN() {mN-1(); mN-1();}
```
Problems

- Have to keep distinct local variables
  - Our simple language has no parameters/returns
- Be careful with recursion
  - Inlining optimization might not terminate
- Too much inlining of (non-recursive procedures) may blow up the code
  - Exponentially!

```c
void m0() { x=x+1 }
void m1() { m0(); m0() }
void m2() { m1(); m1() }
...
void mN() { mN-1(); mN-1() }
```

- Inlining everything, program gets size $O(2^N)$
Call Graph

- Graph over procedures
Call Graph

- Graph over procedures
- Edge from $f$ to $g$, if body of $f$ contains call to $g$
Call Graph

- Graph over procedures
- Edge from $f$ to $g$, if body of $f$ contains call to $g$
- In our examples

```
main → fac
    ↘
    ↗
    ↘
    ↗
  g → f
```

- Inline strategies
  - Leaf: Only leaf procedures
  - Everything: Every non-recursive procedure
  - Real compilers use complex heuristics
    - Based on code size, register pressure, ...
Call Graph

- Graph over procedures
- Edge from $f$ to $g$, if body of $f$ contains call to $g$
- In our examples

- Inline strategies
Call Graph

- Graph over procedures
- Edge from $f$ to $g$, if body of $f$ contains call to $g$
- In our examples

- Inline strategies
  - Leaf: Only leaf procedures
Call Graph

• Graph over procedures
• Edge from $f$ to $g$, if body of $f$ contains call to $g$
• In our examples

• Inline strategies
  • Leaf: Only leaf procedures
  • Everything: Every non-recursive procedure
Call Graph

- Graph over procedures
- Edge from $f$ to $g$, if body of $f$ contains call to $g$
- In our examples

- Inline strategies
  - Leaf: Only leaf procedures
  - Everything: Every non-recursive procedure
  - Real compilers use complex heuristics
    - Based on code size, register pressure, ...
Inlining transformation

- For edge \((u, f(), v)\)
Inlining transformation

- For edge \((u, f(), v)\)
- Make a copy of \(G^f\), rename locals to fresh names \(l^f_1, \ldots, l^f_n\)
Inlining transformation

- For edge \((u, f(), v)\)
- Make a copy of \(G^f\), rename locals to fresh names \(l^f_1, \ldots, l^f_n\)
- Replace by edges:
Inlining transformation

• For edge \((u, f(), v)\)
• Make a copy of \(G^f\), rename locals to fresh names \(l_1^f, \ldots, l_n^f\)
• Replace by edges:
  • \((u, l_1^f = \vec{0}, v_0^f)\) (Initialize locals, goto start node of copy)
Inlining transformation

- For edge \((u, f(), v)\)
- Make a copy of \(G^f\), rename locals to fresh names \(l^f_1, \ldots, l^f_n\)
- Replace by edges:
  - \((u, l^f = \vec{0}, v^f_0)\) (Initialize locals, goto start node of copy)
  - \((v^f_e, \text{Nop}, v)\), for all \(v^f_e \in V^f_{\text{end}}\) (Link end nodes of copy with \(v\))
Inlining transformation

- For edge \((u, f(), v)\)
- Make a copy of \(G^f\), rename locals to fresh names \(l_{f1}^f, \ldots, l_{fn}^f\)
- Replace by edges:
  - \((u, l_{f}^f = \vec{0}, v_0^f)\) (Initialize locals, goto start node of copy)
  - \((v_e^f, \text{Nop}, v)\), for all \(v_e^f \in V_{\text{end}}^f\) (Link end nodes of copy with \(v\))
Tail call optimization

- Idea: If after recursive call, the procedure returns
- Re-use the procedure’s stack frame, instead of allocating a new one

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi]=a[Gi]+t
        f()
    }
}
```
Tail call optimization

- Idea: If after recursive call, the procedure returns
- Re-use the procedure’s stack frame, instead of allocating a new one

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi] = a[Gi] + t
        f()
    }
}
```

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi] = a[Gi] + t
        t = 0; goto f
    }
}
```
Tail call optimization

- Idea: If after recursive call, the procedure returns
- Re-use the procedure's stack frame, instead of allocating a new one

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi]=a[Gi]+t
        f()
    }
}
```

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi]=a[Gi]+t
        t=0; goto f
    }
}
```

- Requires no code duplication
Tail call optimization

- Idea: If after recursive call, the procedure returns
- Re-use the procedure’s stack frame, instead of allocating a new one

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi]=a[Gi]+t
        f()
    }
}
```

```c
void f() {
    if (Gi < Gn-1) {
        t = a[Gi]
        Gi = Gi+1
        a[Gi]=a[Gi]+t
        t=0; goto f
    }
}
```

- Requires no code duplication
- Have to re-initialize local variables, according to semantics
  - Target for DAE ;)

Tail-Call Transformation

f: $v_0^f$ → u

f()

ve

f: $v_0^f$ → u

$l_f = \vec{0}$

ve
Discussion

- Crucial optimization for languages without loop construct
  - E.g., functional languages
Discussion

- Crucial optimization for languages without loop construct
  - E.g., functional languages
- No duplication of code or additional local variables
Discussion

• Crucial optimization for languages without loop construct
  • E.g., functional languages

• No duplication of code or additional local variables

• The optimization may also be profitable for non-recursive calls
  • Re-use stack-space of current frame for new stack frame
  • But not expressable in our semantics (Too high-level view on locals)
Interprocedural Analysis

• Want to extend our program analysis to procedures
• For example, constant propagation
Interprocedural Analysis

• Want to extend our program analysis to procedures
• For example, constant propagation

```c
main() { int t;
    t = 0;
    if (t) M[17] = 3;
    a1 = t;
    work();
    ret = 1 - ret;
}

work() {
    if (a1) work();
    ret = a1 ;
}
```
Interprocedural Analysis

- Want to extend our program analysis to procedures
- For example, constant propagation

```c
main() { int t;
    t = 0;
    if (t) M[17] = 3;
    a1 = t;
    work();
    ret = 1 - ret;
}

work() {
    if (a1) work();
    ret = a1;
}
```

```c
main() { int t;
    t = 0;
    //if (t) M[17] = 3;
    a1 = 0;
    work0();
    ret = 1;
}

work0() {
    //if (a1) work();
    ret = 0;
}
```
Last Lecture

- Stack-based semantics with procedures
- Inlining optimization
- Tail-call optimization
- Path-based semantics
Generalization of Paths

- Recall: Paths were sequences of actions

\[ \text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \]
Generalization of Paths

• Recall: Paths were sequences of actions

\[ \text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \]

• Now: We can call procedures. A procedure call may
  • Return on path
  • Not return on path

\[ \text{slpath} = \varepsilon \mid \text{Act} \cdot \text{slpath} \mid f(\text{slpath}) \cdot \text{slpath} \]

\[ \text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \mid f(\text{slpath}) \cdot \text{path} \mid f< \cdot \text{path} \]

• Intuitively:
  • \( f(\pi) \): Call to procedure \( f \), which executes \( \pi \) and returns
  • \( f< \): Call to procedure \( f \), which does not return

• slpath: Same level paths, which end on same stack-level as they begin

• Note: Inside returning call, all calls must return.
Generalization of Paths

• Recall: Paths were sequences of actions

\[
\text{path} = \varepsilon \mid \text{Act} \cdot \text{path}
\]

• Now: We can call procedures. A procedure call may
  - Return on path
  - Not return on path
  - Advantageous to make this visible in path structure

\[
\text{slpath} = \varepsilon \mid \text{Act} \cdot \text{slpath} \mid f(\text{slpath}) \cdot \text{slpath}
\]

\[
\text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \mid f(\text{slpath}) \cdot \text{path} \mid f_\prec \cdot \text{path}
\]
Generalization of Paths

- Recall: Paths were sequences of actions

  \[ \text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \]

- Now: We can call procedures. A procedure call may
  - Return on path
  - Not return on path
  - Advantageous to make this visible in path structure

  \[ \text{slpath} = \varepsilon \mid \text{Act} \cdot \text{slpath} \mid f(\text{slpath}) \cdot \text{slpath} \]

  \[ \text{path} = \varepsilon \mid \text{Act} \cdot \text{path} \mid f(\text{slpath}) \cdot \text{path} \mid f_< \cdot \text{path} \]

- Intuitively:
  - \( f(\pi) \): Call to procedure \( f \), which executes \( \pi \) and returns
  - \( f_< \): Call to procedure \( f \), which does not return
  - slpath: **Same level paths**, which end on same stack-level as they begin
  - Note: Inside returning call, all calls must return.
Generalization of Paths

- Recall: Paths between nodes

\[
\begin{align*}
[\text{empty}] \quad & \xrightarrow{\varepsilon} \quad u \xrightarrow{} u \\
[\text{app}] \quad & \frac{k = (u, a, v) \in E}{v \xrightarrow{\pi} w} \\
& \quad u \xrightarrow{k\pi} w
\end{align*}
\]
Generalization of Paths

- Recall: Paths between nodes

\[
\begin{align*}
\text{[empty]} & \quad u \overset{\varepsilon}{\rightarrow} u \\
\text{[app]} & \quad k = (u, a, v) \in E \\
& \quad v \overset{\pi}{\rightarrow} w
\end{align*}
\]

- Now

\[
\begin{align*}
\text{[empty]} & \quad u \overset{\varepsilon}{\rightarrow}_{sl} u \\
\text{[app]} & \quad k = (u, a, v) \in E \\
& \quad v \overset{\pi_{sl}}{\rightarrow} w
\end{align*}
\]

\[
\begin{align*}
\text{[call]} & \quad (u, f(), v) \in E \\
& \quad v_0^f \overset{\pi_1}{\rightarrow}_{sl} v_e^f \in V_{end} \\
& \quad v \overset{\pi_2}{\rightarrow}_{sl} w
\end{align*}
\]
Generalization of Paths

- Recall: Paths between nodes

\[
\begin{align*}
[\text{empty}] & \quad \varepsilon \rightarrow u \\
[\text{app}] & \quad k = (u, a, v) \in E \quad v \xrightarrow{\pi} w
\end{align*}
\]

- Now

\[
\begin{align*}
[\text{empty}] & \quad \varepsilon \rightarrow_{sl} u \\
[\text{app}] & \quad k = (u, a, v) \in E \quad v \xrightarrow{\pi_{sl}} w
\end{align*}
\]

\[
\begin{align*}
[\text{call}] & \quad (u, f(), v) \in E \quad v_0^f \xrightarrow{\pi_1_{sl}} v_v^f \in V_{\text{end}} \quad v \xrightarrow{\pi_{sl}} w
\end{align*}
\]

- And

\[
\begin{align*}
[\text{emp}] & \quad \varepsilon \rightarrow u \\
[\text{app}] & \quad k = (u, a, v) \in E \quad v \xrightarrow{\pi} w
\end{align*}
\]

\[
\begin{align*}
[\text{call}] & \quad (u, f(), v) \in E \quad v_0^f \xrightarrow{\pi_1_{sl}} v_v^f \in V_{\text{end}} \quad v \xrightarrow{\pi_{sl}} w
\end{align*}
\]

\[
\begin{align*}
[\text{ncall}] & \quad (u, f(), v) \in E \quad v_0^f \xrightarrow{\pi} w
\end{align*}
\]
Executions of paths

• Recall

\[ [\varepsilon]s = s \quad [k\pi]s = [\pi]([k]s) \]
Executions of paths

- Recall

\[ [\varepsilon]s = s \quad [k\pi]s = [\pi](k[s]) \]

- Now

\[ [\varepsilon]s = s \quad [k\pi]s = [\pi](k[s]) \]

\[ [f(\pi)]s = H [\pi] s \quad [f_<]s = \text{enter } s \]

where

\[
\text{enter}(\rho_l, \rho_g, \mu) := (\vec{0}, \rho_g, \mu) \\
\text{combine}((\rho_l, \rho_g, \mu), (\rho'_l, \rho'_g, \mu')) := (\rho_l, \rho'_g, \mu') \\

H e s := \text{combine}(s, (e(\text{enter } s)))
\]
Executions of paths

• Recall

\[ [\varepsilon]s = s \quad [k\pi]s = [\pi]([k]s) \]

• Now

\[ [\varepsilon]s = s \quad [k\pi]s = [\pi]([k]s) \]

\[ [f(\pi)]s = H [\pi] s \quad [f<]s = \text{enter } s \]

where

\[
\text{enter}(\rho_l, \rho_g, \mu) := (\vec{0}, \rho_g, \mu) \\
\text{combine}((\rho_l, \rho_g, \mu), (\rho'_l, \rho'_g, \mu')) := (\rho_l, \rho'_g, \mu') \\
H e s := \text{combine}(s, (e(\text{enter } s)))
\]

• Intuition:

\begin{align*}
\text{enter} & \quad \text{Set up stack frame} \\
\text{combine} & \quad \text{Combine procedure result with old frame}
\end{align*}
Example

```plaintext
f () {
    if x>0 then {
        x = x - 1
        f ()
        x = x + 1
    } else {
        u: Nop
    }
}

main () {
    x = 1;
    f ()
    x = 0
}
```
Example

```plaintext
f () {
  if x>0 then {
    x = x - 1
    f ()
    x = x + 1
  } else {
    u: Nop
  }
}

main () {
  x = 1;
  f ()
  x = 0
}
```

SL-path through main:

```
x=1
f()
  Pos(x>0)
  x=x-1
  f()
    Neg(x>0)
    Nop
  )
    x = x + 1
)
  x = 0
```
Example

```plaintext
f () {
    if x>0 then {
        x = x - 1
        f ()
        x = x + 1
    } else {
        u: Nop
    }
}

main () {
    x = 1;
    f ()
    x = 0
}
```

---

**SL-path through main**

```
x=1
f()
```

**Path from main to u**

```
x=1
f<
```

```
Pos(x>0)
```

```
x=x-1
```

```
f(
    Pos(x>0)
    x=x-1
    f(
        Pos(x>0)
        Nop
    )
    x = x + 1
)
```

```
Neg(x>0)
```
Theorem

The stack-based and path-based semantics are equivalent:

\[
(\exists \sigma. ([u, \rho_l], \rho_g, \mu) \xrightarrow{}^* ([v, \rho'_l] \sigma, \rho'_g, \mu'))
\]

\[\iff\]

\[\exists \pi. u \xrightarrow{\pi} v \land \llbracket \pi \rrbracket(\rho_l, \rho_g, \mu) = (\rho'_l, \rho'_g, \mu')\]
Proof sketch (Whiteboard)

- Auxiliary lemma: Same-level paths

\[ (([u, \rho_l], \rho_g, \mu)) \to^* ([v, \rho'_l], \rho'_g, \mu') \]

\[ \iff (\exists \pi. \ u \overset{\pi}{\to}_{sl} v \land [\pi](\rho_l, \rho_g, \mu) = (\rho'_l, \rho'_g, \mu')) \]
Proof sketch (Whiteboard)

- Auxiliary lemma: Same-level paths

\[ (((u, \rho_l], \rho_g, \mu)) \rightarrow^* ([v, \rho'_l], \rho'_g, \mu') \]

\[ \iff (\exists \pi. u \xrightarrow{\pi}_{sl} v \land [\pi](\rho_l, \rho_g, \mu) = (\rho'_l, \rho'_g, \mu')) \]

- Main ideas (\implies)
  - Induction on length of execution
  - Identify non-returning calls:
    - Execution in between yields same-level paths (aux-lemma)
Proof sketch (Whiteboard)

- **Auxiliary lemma: Same-level paths**

\[
((\{u, \rho_l\}, \rho_g, \mu)) \rightarrow^* (\{v, \rho'_l\}, \rho'_g, \mu') \iff (\exists \pi. \ u \xrightarrow{\pi}_{s1} v \land [\pi](\rho_l, \rho_g, \mu) = (\rho'_l, \rho'_g, \mu'))
\]

- **Main ideas (⇒)**
  - Induction on length of execution
  - Identify non-returning calls:
    - Execution in between yields same-level paths (aux-lemma)

- **Main ideas (⇐)**
  - Induction on path structure
  - Executions can be repeated with stack extended at the bottom

\[
(\sigma, \rho_g, \mu) \rightarrow^* (\sigma', \rho'_g, \mu') \implies (\sigma \hat{\sigma}, \rho_g, \mu) \rightarrow^* (\sigma' \hat{\sigma}, \rho'_g, \mu')
\]
Abstraction of paths

- Recall: Abstract effects of actions: $[a]^\# : \mathbb{D} \rightarrow \mathbb{D}$
Abstraction of paths

- Recall: Abstract effects of actions: \([a]^{\#} : D \rightarrow D\)
- Actions: Nop, Test, Assign, Load, Store
Abstraction of paths

- Recall: Abstract effects of actions: \([a]_\# : \mathbb{D} \rightarrow \mathbb{D}\)
  - Actions: Nop, Test, Assign, Load, Store
- Now: Additional actions: Returning/non-returning procedure call
Abstraction of paths

- Recall: Abstract effects of actions: $[a]^{\#} : \mathbb{D} \rightarrow \mathbb{D}$
  - Actions: Nop, Test, Assign, Load, Store
- Now: Additional actions: Returning/non-returning procedure call
- Require: Abstract effects for $f(\pi)$ and $f_<$
Abstraction of paths

- Recall: Abstract effects of actions: $\llbracket a \rrbracket^\# : D \rightarrow D$
  - Actions: Nop, Test, Assign, Load, Store
- Now: Additional actions: Returning/non-returning procedure call
- Require: Abstract effects for $f(\pi)$ and $f_<$
  - Define abstract $\text{enter}_f^\#$, $\text{combine}_f^\#$
Abstraction of paths

- Recall: Abstract effects of actions: \([a]^\# : D \rightarrow D\)
  - Actions: Nop, Test, Assign, Load, Store
- Now: Additional actions: Returning/non-returning procedure call
- Require: Abstract effects for \(f(\pi)\) and \(f_<\)
  - Define abstract enter\(_f^\#\), combine\(_f^\#
  - \(H_f^# e d = \text{combine}_f^# (d, e(\text{enter}_f^# (d)))\)
Abstraction of paths

- Recall: Abstract effects of actions: $\llbracket a \rrbracket^\#: D \rightarrow D$
  - Actions: Nop, Test, Assign, Load, Store
- Now: Additional actions: Returning/non-returning procedure call
- Require: Abstract effects for $f(\pi)$ and $f_<$
  - Define abstract $\text{enter}^\#, \text{combine}^\#
  - $H^\#_f \ e \ d = \text{combine}^\#_f (d, e(\text{enter}^\#_f (d)))$
  - $\llbracket f(\pi) \rrbracket^\# d = H^\#_f \ llbracket \pi \rrbracket^\# d$
Abstraction of paths

• Recall: Abstract effects of actions: $[a]^\# : \mathbb{D} \rightarrow \mathbb{D}$
  • Actions: Nop, Test, Assign, Load, Store
• Now: Additional actions: Returning/non-returning procedure call
• Require: Abstract effects for $f(\pi)$ and $f_<$
  • Define abstract $\text{enter}^f_\#$, $\text{combine}^f_\#
  • $H^f_\# e d = \text{combine}^f_\# (d, e(\text{enter}^f_\# (d)))$
  • $[f(\pi)]^\# d = H^f_\# [\pi]^\# d$
  • $[f_<]^\# d = \text{enter}^f_\# (d)$
Example: Copy constants

• Simplified constant propagation
Example: Copy constants

- Simplified constant propagation
  - Conditions not exploited
Example: Copy constants

- Simplified constant propagation
  - Conditions not exploited
  - Only assignments of form $x = y$ and $x = c, c \in \mathbb{Z}$
Example: Copy constants

- Simplified constant propagation
  - Conditions not exploited
  - Only assignments of form $x = y$ and $x = c$, $c \in \mathbb{Z}$
- Domain: $\mathbb{D} := \text{Reg} \rightarrow \mathbb{Z}^\top$
Example: Copy constants

- Simplified constant propagation
  - Conditions not exploited
  - Only assignments of form $x = y$ and $x = c, c \in \mathbb{Z}$
- Domain: $\mathbb{D} := \text{Reg} \rightarrow \mathbb{Z}^\top$
- Initially: $d_0 \ l := 0, l \in \text{Loc}, d_0 \ g := \top, g \in \text{Glob}$
Example: Copy constants

- Simplified constant propagation
  - Conditions not exploited
  - Only assignments of form $x = y$ and $x = c$, $c \in \mathbb{Z}$

- Domain: $\mathbb{D} := \text{Reg} \rightarrow \mathbb{Z}^\top$

- Initially: $d_0 \ l := 0$, $l \in \text{Loc}$, $d_0 \ g := \top$, $g \in \text{Glob}$

- Abstract effects

\[
\begin{align*}
[x := c]^\# d &= d(x := c) \quad \text{for } c \in \mathbb{Z} \\
[x := y]^\# d &= d(x := d(y)) \quad \text{for } y \in \text{Reg} \\
[x := e]^\# d &= d(x := \top) \quad \text{for } e \in \text{Expr} \setminus (\mathbb{Z} \cup \text{Reg}) \\
[x := M(e)]^\# d &= d(x := \top) \\
[\text{Pos}(e)]^\# d &= [\text{Neg}(e)]^\# d = [\text{Nop}]^\# d = [M(e_1) = e_2]^\# d = d \\
\text{enter}_f^# d &= d(l := 0 \mid l \in \text{Loc}) \\
\text{combine}_f^# d \ d' &= \lambda x. \ x \in \text{Loc}?d(x) : d'(x)
\end{align*}
\]
Correctness

- Description relation \((\rho_l, \rho_g, \mu) \Delta d\)
  - iff \(\rho_l \Delta d|_{\text{Loc}}\) and \(\rho_g \Delta d|_{\text{Glob}}\)
Correctness

- Description relation \( (\rho_l, \rho_g, \mu) \Delta d \)
  - iff \( \rho_l \Delta d|_{\text{Loc}} \) and \( \rho_g \Delta d|_{\text{Glob}} \)
- Show: \( \forall \rho_g, \mu. [\pi](\vec{0}, \rho_g, \mu) \Delta [\pi]|^\# d_0 \)
Correctness

- Description relation \((\rho_l, \rho_g, \mu) \triangle d\)
  - iff \(\rho_l \triangle d|_{\text{Loc}}\) and \(\rho_g \triangle d|_{\text{Glob}}\)

- Show: \(\forall \rho_g, \mu. \llbracket \pi \rrbracket (\vec{0}, \rho_g, \mu) \triangle \llbracket \pi \rrbracket \# d_0\)
  - By induction on path
Correctness

- Description relation \((\rho_l, \rho_g, \mu) \Delta d\)
  - iff \(\rho_l \Delta d|_{\text{Loc}}\) and \(\rho_g \Delta d|_{\text{Glob}}\)
- Show: \(\forall \rho_g, \mu. \llbracket \pi \rrbracket (\vec{0}, \rho_g, \mu) \Delta \llbracket \pi \rrbracket \# d_0\)
  - By induction on path
  - Then, case distinction on edges
Correctness

- Description relation \((\rho_l, \rho_g, \mu) \triangleq d\)
  - iff \(\rho_l \triangleq d|_{\text{Loc}}\) and \(\rho_g \triangleq d|_{\text{Glob}}\)
- Show: \(\forall \rho_g, \mu. \llbracket \pi \rrbracket (\vec{0}, \rho_g, \mu) \triangleq \llbracket \pi \rrbracket \# d_0\)
  - By induction on path
  - Then, case distinction on edges
  - Generalization of simulation proofs for intraprocedural case
Computing Solutions

- Interested in $\text{MOP}[u] := \bigsqcup \{ [[\pi]]^d_0 \mid v_0^{\text{main}} \xrightarrow{\pi} u \}$
Computing Solutions

- Interested in \( \text{MOP}[u] := \bigcup \{ [\pi]^d | v_0^{\text{main}} \xrightarrow{\pi} u \} \)
- Idea: Constraint system for same-level effects of functions

\[
\begin{align*}
S[v_0^f] & \supseteq \text{id} \\
S[v] & \supseteq [k]^{d} \circ S[u] & k = (u, a, v) \in E \\
S[v] & \supseteq H^d(S[f]) \circ S[u] & k = (u, f(), v) \in E \\
S[f] & \supseteq S[v_e^f] & v_e^f \in V_{\text{end}}
\end{align*}
\]
Computing Solutions

- Interested in \( \text{MOP}\{u\} := \bigcup \{ [[\pi]]^{\#} d_0 \mid v_{0\text{main}}^{\pi} \rightarrow u \} \)
- Idea: Constraint system for same-level effects of functions
  \[
  S[v_0^f] \supseteq \text{id}
  
  S[v] \supseteq [k]^{\#} \circ S[u]
  \]
  \[
  S[v] \supseteq H^{\#}(S[f]) \circ S[u]
  \]
  \[
  S[f] \supseteq S[v_e^f]
  \]

- And for effects of paths reaching \( u \)
  \[
  R[v_0^{\text{main}}] \supseteq \text{enter}^{\#} d_0
  \]
  \[
  R[v] \supseteq [k]^{\#} R[u]
  \]
  \[
  R[v] \supseteq H^{\#} S[f] R[u]
  \]
  \[
  R[v_0^f] \supseteq \text{enter}^{\#} R[u]
  \]

\( k = (u, a, v) \in E \) (edge)
\( k = (u, f(), v) \in E \) (call)
\( v_e^f \in V_{\text{end}}^f \) (end)

\( k = (u, a, v) \in E \) (edge)
\( k = (u, f(), v) \in E \) (call)
\( (u, f(), v) \in E \) (calln)
Coincidence Theorems

- Let MFP be the least solution of $R$, then we have
  \[ MOP \sqsubseteq MFP \]

- For monotonic effects
Coincidence Theorems

- Let $\text{MFP}$ be the least solution of $R$, then we have
  \[ \text{MOP} \subseteq \text{MFP} \]

- For monotonic effects
- If each program point is reachable, and all effects as well as $H^#$ are distributive:
  \[ \text{MOP} = \text{MFP} \]
Coincidence Theorems

- Let \( MFP \) be the least solution of \( R \), then we have

\[
MOP \subseteq MFP
\]

- For monotonic effects

- If each program point is reachable, and all effects as well as \( H^\# \) are distributive:

\[
MOP = MFP
\]

- Generalization of corresponding intra-procedural theorems
Coincidence Theorems

- Let $MFP$ be the least solution of $R$, then we have

\[ \text{MOP} \subseteq \text{MFP} \]

- For monotonic effects
- If each program point is reachable, and all effects as well as $H\#$ are distributive:

\[ \text{MOP} = \text{MFP} \]

- Generalization of corresponding intra-procedural theorems
- Intuition: Constraint system joins early
Coincidence Theorems

- Let \( MFP \) be the least solution of \( R \), then we have
  \[
  \text{MOP} \sqsubseteq \text{MFP}
  \]

  - For monotonic effects

- If each program point is reachable, and all effects as well as \( H^\# \) are distributive:
  \[
  \text{MOP} = \text{MFP}
  \]

- Generalization of corresponding intra-procedural theorems

  - Intuition: Constraint system joins early
    - Information from multiple incoming edges
Coincidence Theorems

- Let $MFP$ be the least solution of $R$, then we have

  $$MOP \sqsubseteq MFP$$

- For monotonic effects
- If each program point is reachable, and all effects as well as $H\#$ are distributive:

  $$MOP = MFP$$

- Generalization of corresponding intra-procedural theorems
- Intuition: Constraint system joins early
  - Information from multiple incoming edges
  - All paths through procedure on returning call
Remaining problem

- How to compute effects of call efficiently?
Remaining problem

- How to compute effects of call efficiently?
  - How to represent functions \( D \rightarrow D \)
Remaining problem

• How to compute effects of call efficiently?
  • How to represent functions $\mathbb{D} \rightarrow \mathbb{D}$
  • efficiently?
Remaining problem

- How to compute effects of call efficiently?
  - How to represent functions $\mathbb{D} \to \mathbb{D}$
  - efficiently?
- For copy constants:
Remaining problem

- How to compute effects of call efficiently?
  - How to represent functions $\mathbb{D} \rightarrow \mathbb{D}$
  - efficiently?
- For copy constants:
  - Domain is actually finite: Only need to consider constants that actually occur in the program
Remaining problem

- How to compute effects of call efficiently?
  - How to represent functions $\mathbb{D} \rightarrow \mathbb{D}$
  - efficiently?

- For copy constants:
  - Domain is actually finite: Only need to consider constants that actually occur in the program
  - But this would yield huge tables for functions
Remaining problem

• How to compute effects of call efficiently?
  • How to represent functions $\mathbb{D} \rightarrow \mathbb{D}$
  • efficiently?
• For copy constants:
  • Domain is actually finite: Only need to consider constants that actually occur in the program
  • But this would yield huge tables for functions
• Possible solutions:
Remaining problem

• How to compute effects of call efficiently?
  • How to represent functions \( D \rightarrow D \)
  • efficiently?

• For copy constants:
  • Domain is actually finite: Only need to consider constants that actually occur in the program
  • But this would yield huge tables for functions

• Possible solutions:
  • Find efficient representation for functions
Remaining problem

• How to compute effects of call efficiently?
  • How to represent functions $\mathbb{D} \rightarrow \mathbb{D}$
  • efficiently?

• For copy constants:
  • Domain is actually finite: Only need to consider constants that actually occur in the program
  • But this would yield huge tables for functions

• Possible solutions:
  • Find efficient representation for functions
  • Function actually not applied to all values $d \in \mathbb{D}$. $\implies$ compute on demand.
Efficient representation of same-level effects

- Observation: Functions $S[u] \neq \bot$ are of form $\langle m \rangle$ where

$$\langle m \rangle := \lambda D x. m_1 x \sqcup \bigsqcup_{y \in m_2 x} D y$$

- $m_1 x : \mathbb{Z}^\top_\bot$ - Join of constants that may be assigned to $x$
- $m_2 x : 2^{\text{Reg}}$ - set of variables that may be assigned to $x$ (non-empty)
Efficient representation of same-level effects

• Observation: Functions $S[u] \neq \bot$ are of form $\langle m \rangle$ where

$$\langle m \rangle := \lambda D \ x. \ m_1 \ x \sqcup \bigsqcup_{y \in m_2} D \ y$$

• $m_1 \ x : \mathbb{Z}_\bot^\top$ - Join of constants that may be assigned to $x$
• $m_2 \ x : 2^{\text{Reg}}$ - set of variables that may be assigned to $x$ (non-empty)
• Let $F := \{ \langle m \rangle | m : \text{Reg} \rightarrow \mathbb{Z}_\bot^\top \times 2^{\text{Reg}} \}$ be the set of those functions
Efficient representation of same-level effects

- Observation: Functions $S[u] \neq \perp$ are of form $\langle m \rangle$ where

  $$\langle m \rangle := \lambda D \ x. \ m_1 \ x \sqcup \bigcup_{y \in m_2 \ x} D \ y$$

  - $m_1 \ x : \mathbb{Z}_{\perp}^+$ - Join of constants that may be assigned to $x$
  - $m_2 \ x : 2^{\text{Reg}}$ - set of variables that may be assigned to $x$ (non-empty)

- Let $F := \{ \langle m \rangle | m : \text{Reg} \rightarrow \mathbb{Z}_{\perp}^+ \times 2^{\text{Reg}} \}$ be the set of those functions

- To show: $\text{id}, \left[ a \right]^\# \in F$, and $F$ closed under $\circ, \sqcup, \text{enter}^\#$, and $H^\#$
Identity and effects representable

\[ \text{id} = \langle \lambda x. (\bot, \{x\}) \rangle \]

\[ \llbracket x := e \rrbracket^\# = \begin{cases} 
\langle \text{id}(x \mapsto (c, \emptyset)) \rangle & \text{for } e = c \in \mathbb{Z} \\
\langle \text{id}(x \mapsto (\bot, \{y\})) \rangle & \text{for } e = y \in \text{Reg} \\
\langle \text{id}(x \mapsto (\top, \emptyset)) \rangle & \text{otherwise}
\end{cases} \]
Identity and effects representable

\[ \text{id} = \langle \lambda x. (\bot, \{x\}) \rangle \]

\[ \llbracket x := e \rrbracket^\# = \begin{cases} 
\langle \text{id}(x \mapsto (c, \emptyset)) \rangle & \text{for } e = c \in \mathbb{Z} \\
\langle \text{id}(x \mapsto (\bot, \{y\})) \rangle & \text{for } e = y \in \text{Reg} \\
\langle \text{id}(x \mapsto (\top, \emptyset)) \rangle & \text{otherwise}
\end{cases} \]

- Effects of other actions similarly
Closed under function composition and join

\[ \langle m \rangle \circ \langle m' \rangle = \langle \lambda x. (m_1 x \sqcup \bigsqcup_{y \in m_2} m'_1 y, \bigsqcup_{y \in m_2} m'_2 y) \rangle \]

\[ \langle m \rangle \sqcup \langle m' \rangle = \langle m \sqcup m' \rangle \]
Closed under function composition and join

\[ \langle m \rangle \circ \langle m' \rangle = \langle \lambda x. (m_1 \ x \ \sqcup \ \bigsqcup_{y \in m_2 \ x} m'_1 \ y, \ \bigcup_{y \in m_2 \ x} m'_2 \ y) \rangle \]

\[ \langle m \rangle \sqcup \langle m' \rangle = \langle m \sqcup m' \rangle \]

- Intuition: Assigned constants by \( m_1 \), or by \( m'_1 \), and variable goes through \( m_2 \)
  - \([x := c; \ text{foo}] \#\), or \([x := y; y := c] \#\)
  - Note: If \( x \) not touched, we have \( m_2 \ x = \{x\} \)

- Note: \( \sqcup \) defined pointwise: \((m \sqcup m') \ x = (m_1 \ x \ \sqcup \ m'_1 \ x, m_2 \ x \ \sqcup \ m'_2 \ x)\)
Closed under $\text{enter}^\#$ and $H^#$

$$\text{enter}^\# = \langle (\lambda x. (0, \emptyset)) \rangle_{\text{Loc}} \oplus \text{id}_{\text{Glob}}$$

$$H^#(\langle m \rangle) = \text{id}_{\text{Loc}} \oplus (\langle m \rangle \circ \text{enter}^\#)_{\text{Glob}}$$

$$\langle m \rangle_{\text{Loc}} \oplus \langle m' \rangle_{\text{Glob}} := \langle \lambda x. x \in \text{Loc}?m\ x : m'\ x \rangle$$
Closed under $\text{enter}^\#$ and $H^#$

\[
\text{enter}^\# = \langle (\lambda x. (0, \emptyset))\rangle_{\text{Loc}} \oplus \text{id}_{\text{Glob}}
\]

\[
H^#(\langle m \rangle) = \text{id}_{\text{Loc}} \oplus (\langle m \rangle \circ \text{enter}^\#)_{\text{Glob}}
\]

\[
\langle m \rangle_{\text{Loc}} \oplus \langle m' \rangle_{\text{Glob}} := \langle \lambda x. x \in \text{Loc}?m x : m' x \rangle
\]

- **Intuition**
  - Function call only affects globals
  - $\text{enter}^\#$ is effect of entering function (set locals to 0)
  - $f_{\text{Loc}} \oplus f'_{\text{Glob}}$ - Use $f$ for local variables, $f'$ for global variables
Recall initial example

```c
main() {
    int t;
    t = 0; // t=0, a1=T, ret=T
    if (t) { // t=0, a1=T, ret=T
        M[17] = 3; // t=0, a1=T, ret=T
        a1 = t; // t=0, a1=T, ret=T
        work (); // t=0, a1=0, ret=T
        ret = 1 - ret; // t=0, a1=0, ret=0
    }
    // t=0, a1=0, ret=T
}

work() {
    if (a1) { // id
        work (); // id
        Nop } // id[ ret->(⊥, {a1}) ] a1=0, ret=0
    ret = a1 ; // id[ ret->(⊥, {ret,a1}) ] a1=0, ret=T
} // id[ ret->(⊥, {a1}) ] a1=0, ret=0
```
Discussion

- At least copy-constants can be determined interprocedurally
- For that, we had to ignore conditions and complex assignments
- However, for the reaching paths, we could have been more precise
- Extra abstractions were required as
  1. Set of abstract same-level effects must be finite
  2. and efficiently implementable
Last Lecture

- Copy-Constant propagation
- Functional approach to interprocedural analysis
  - Compute same-level effects by constraint system
  - Find efficient representation for same-level effects
Idea: Evaluation on demand

- Procedures often called only for few distinct abstract arguments
  - Observed early (Sharir/Pneuli’81, Cousot’77)
- Only analyze procedures for these
- Intuition: $[f, a]^\# -$ effect of $f$ if called in abstract state $a$
- Put up constraint system
  
  $[v_0^f, a]^\# \subseteq a$

  $[v, a]^\# \subseteq [k]^\#([u, a]^\#)$ for basic edge $k = (u, -, v)$

  $[v, a]^\# \subseteq \text{combine}^\#([u, a]^\#, [g, \text{enter}^\#([u, a]^\#)]^\#)$ for call edge $k = (u, g(), v)$

  $[f, a]^\# \subseteq [v_e^f, a]^\#$ for $v_e^f \in V_{\text{end}}$

- Idea: Keep track of effect for any node of procedure
Evaluation on demand

- This constraint system may be huge
- Idea: Only evaluate $\mathbb{F}_f, a\#$ for values $a$ that actually occur
  - Local fixed-point algorithms (not covered)
- But, we can do an example nevertheless :)
Example: Full constant propagation

```c
// al, ret | locals
main() { int t;
    t = 0;  \ T,\ T | 0
    if (t) \ T,\ T | 0
        M[17] = 3; \ \bot
    al = t; \ T,\ T | 0
work(); \ 0,\ T | 0
ret = 1 - ret; \ 0,0 | 0
} \ 0,1 | 0

work() { \ [work, (0, T)]#
    if (al) \ 0,\ T
        work() \ \bot
    ret = al; \ 0,\ T
} \ 0,0
```

- Only need to keep track of \( a_1 \) for calling context of `work`
Discussion

- This analysis terminates, if
This analysis terminates, if

- $\mathcal{D}$ has finite height,
Discussion

- This analysis terminates, if
  - $\mathcal{D}$ has finite height,
  - and every procedure only analyzed for finitely many arguments
Discussion

- This analysis terminates, if
  - $\mathbb{D}$ has finite height,
  - and every procedure only analyzed for finitely many arguments
- Analogous algorithms have proved efficient for analysis of PROLOG
Discussion

- This analysis terminates, if
  - $\mathcal{D}$ has finite height,
  - and every procedure only analyzed for finitely many arguments
- Analogous algorithms have proved efficient for analysis of PROLOG
- Together with points-to analysis, algorithms of this kind used in the Goblint-Tool
Discussion

- This analysis terminates, if
  - $\mathbb{D}$ has finite height,
  - and every procedure only analyzed for finitely many arguments
- Analogous algorithms have proved efficient for analysis of PROLOG
- Together with points-to analysis, algorithms of this kind used in the Goblint-Tool
  - Data-race detection for C with POSIX-Threads
Crude approximation

- Start with very crude approximation:

\[ D[v_0 f] \leq \text{enter} \] 
\[ D[u] \leq \text{combine} \]

\( D[v f e] \in V_f \) 

end
Crude approximation

- Start with very crude approximation:
  - Just insert edges from function-call to procedure start

\[ D[v_0f] \preceq \text{enter} \]
\[ D[u] D[v] \preceq \text{combine} \]
\[ f \in V_f \text{end} \]

- Clearly covers all possible paths
- But also infeasible ones
Crude approximation

- Start with very crude approximation:
  - Just insert edges from function-call to procedure start
  - And from return of procedure to target-node of function call

\[
\begin{align*}
  D[v_0 \ f] &\leq \text{enter} \\
  D[v] &\leq \text{combine} \\
  D[u] &\in V_f
\end{align*}
\]

- Clearly covers all possible paths
- But also infeasible ones
Crude approximation

- Start with very crude approximation:
  - Just insert edges from function-call to procedure start
  - And from return of procedure to target-node of function call
- I.e, for \((u, f(), v)\), generate constraints

\[
D[v_0^f] \equiv \text{enter}_f^# D[u] \\
D[v] \equiv \text{combine}_f^# (D[u], D[v_e^f]) \quad v_e^f \in V_{end}^f
\]
Crude approximation

- Start with very crude approximation:
  - Just insert edges from function-call to procedure start
  - And from return of procedure to target-node of function call
- I.e, for \((u, f(), v)\), generate constraints

\[
D[v_0^f] \supseteq \text{enter}_f^# D[u] \\
D[v] \supseteq \text{combine}_f^# (D[u], D[v_e^f])
\]

- Clearly covers all possible paths
Crude approximation

- Start with very crude approximation:
  - Just insert edges from function-call to procedure start
  - And from return of procedure to target-node of function call
- I.e, for \((u, f(), v)\), generate constraints

\[
D[v_0^f] \equiv \text{enter}_f^\# D[u]
\]
\[
D[v] \equiv \text{combine}_f^\# (D[u], D[v_e^f]) \quad \forall v_e^f \in V_{\text{end}}^f
\]

- Clearly covers all possible paths
- But also infeasible ones
Crude approximation, example

```c
f () { ... }
g () { f() }

main () {
    f ();
    g ()
}
```

---

Infeasible paths: 326 / 471
Crude approximation, example

f () {...}
g () { f() }  

main () {
    f ();
    g ()
}

main: f: ...  
   f()       
       ↓       
   f()  
   g()  
   g: f()
Crude approximation, example

```c
f () {...}
g () { f() }

main () {
    f ();
    g ()
}
```

Infeasible paths 326 / 471
Crude approximation, example

\[
f() \{ ... \}
g() \{ f() \}
\]

main () {
  f ();
  g ()
}

main: \[\text{-} \]
f: \[\text{-} \]
\[ \]
g: \[\text{-} \]
Crude approximation, example

```c
f () {...}
g () { f() } 

main () {
    f ();
    g ()
}
```

Infeasible paths
Crude approximation, example

```c
f () {
...
}
g () { f() }

main () {
    f ();
    g ()
}
```

Infeasible paths
Crude approximation, example

```c
f () {...}
g () { f() }

main () {
    f ();
    g ()
}
```

Infeasible paths
Call strings

- Idea: Call string contains sequence of up to \( k \) program points
Call strings

- Idea: Call string contains sequence of up to $k$ program points
- These are the topmost $k$ return addresses on the stack
Call strings

- Idea: Call string contains sequence of up to $k$ program points
- These are the topmost $k$ return addresses on the stack
- Analyze procedures for every (feasible) call-string
Call strings

- Idea: Call string contains sequence of up to $k$ program points
- These are the topmost $k$ return addresses on the stack
- Analyze procedures for every (feasible) call-string
- Only create edges that match call-string
Call strings

\[ D[v_0^f, (\nu \omega)|_k] \equiv \text{enter}^\#(D[u, \omega]) \]  \hspace{5cm} \text{where } (\cdot)|_k \text{ limits string size to } k, \text{ cutting off nodes from the end.}

\[ D[v, \omega] \equiv \text{combine}^\#(D[u, \omega], D[f, (\nu \omega)|_k]) \]  \hspace{5cm} \nu_e \in V_{end}^f \]

\[ D[f, \omega] \equiv D[v_e, \omega] \]  \hspace{5cm} (u, f(), v) \in E

\[ D[v_0^{main}, \varepsilon] \equiv d_0 \]  \hspace{5cm} \nu_{v_0^{main}, \varepsilon} \equiv d_0

\[ D[v, \omega] \equiv [k]^\# D[u, \omega] \]  \hspace{5cm} k = (u, a, v) \in E

\[ (u, f(), v) \in E \]  \hspace{5cm} (u, f(), v) \in E
Example

```c
f () {...}
g () { f() }

main () {
    f ();
    g ()
}
```

```
main: 1           f2: 4 → 5
      f()          f7: 4' → 5'
  2   3   g()      g3: 6 → 7
```
Example

```plaintext
f () {...}
g () { f() }

main () {
    f ();
    g ();
}
```
Discussion

- Analysis terminates if $D$ has finite height
Discussion

- Analysis terminates if $D$ has finite height
- Call strings with $k = 0$ matches crude approximation
Discussion

- Analysis terminates if $D$ has finite height
- Call strings with $k = 0$ matches crude approximation
- Can increase precision by eliminating (some) infeasible paths
Discussion

- Analysis terminates if $D$ has finite height
- Call strings with $k = 0$ matches crude approximation
- Can increase precision by eliminating (some) infeasible paths
- Cost increases exponentially with size of $k$
Discussion

- Analysis terminates if $D$ has finite height
- Call strings with $k = 0$ matches crude approximation
- Can increase precision by eliminating (some) infeasible paths
- Cost increases exponentially with size of $k$
- In practice $k = 0$ or $k = 1$
Discussion

- Analysis terminates if $D$ has finite height
- Call strings with $k = 0$ matches crude approximation
- Can increase precision by eliminating (some) infeasible paths
- Cost increases exponentially with size of $k$
- In practice $k = 0$ or $k = 1$
- Correctness proof: Simulation wrt. stack-based semantics
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
    - Requires efficient representation of effects
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
    - Requires efficient representation of effects
  - Evaluation on demand: Same-level effects for finite number of arguments
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
    - Requires efficient representation of effects
  - Evaluation on demand: Same-level effects for finite number of arguments
    - Requires finite/small number of abstract arguments for each function
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
    - Requires efficient representation of effects
  - Evaluation on demand: Same-level effects for finite number of arguments
    - Requires finite/small number of abstract arguments for each function
  - Call-Strings: Limit stack-depth, add extra (stack-insensitive) paths above depth limit
Summary: Interprocedural Analysis

- Semantics: Stack-based, path-based
- Analysis:
  - Functional: Compute same-level effects
    - Requires efficient representation of effects
  - Evaluation on demand: Same-level effects for finite number of arguments
    - Requires finite/small number of abstract arguments for each function
  - Call-Strings: Limit stack-depth, add extra (stack-insensitive) paths above depth limit
    - Adds extra imprecision, exponentially cost in depth-limit
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Removing Superfluous Computations</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Interpretation</td>
</tr>
<tr>
<td>4</td>
<td>Alias Analysis</td>
</tr>
<tr>
<td>5</td>
<td>Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6</td>
<td>Interprocedural Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8</td>
<td>Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Hardware Features</td>
</tr>
<tr>
<td>10</td>
<td>Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Analysis of Parallel Programs

- Concurrency gets more important nowadays
Analysis of Parallel Programs

- Concurrency gets more important nowadays
- Admits new classes of bugs
Concurrency gets more important nowadays
Admits new classes of bugs
  - E.g, data races
Analysis of Parallel Programs

- Concurrency gets more important nowadays
- Admits new classes of bugs
  - E.g, data races
- These are hard to find/ hard to reproduce
Analysis of Parallel Programs

- Concurrency gets more important nowadays
- Admits new classes of bugs
  - E.g, data races
- These are hard to find/ hard to reproduce
- Can program analysis help?
Data races

- Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

What will the program print?

Assuming sequential consistency?

Answer: In most cases: 2

But in very rare cases: 1

Depends on machine, other programs, OS, start time, ...
Data races

- Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

- What will the program print?
Data races

- Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

- What will the program print?
  - Assuming sequential consistency?
Data races

- Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

- What will the program print?
  - Assuming sequential consistency?

- Answer: In most cases: 2

But in very rare cases: 1
Depends on machine, other programs, OS, start time, ...
Data races

- Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

- What will the program print?
  - Assuming sequential consistency?
  - Answer: In most cases: 2
  - But in very rare cases: 1
Data races

• Concurrent accesses to global data, one is a write

```c
int g = 0;
t1 () {
    g = g + 1
}
main () {
    fork t1;
    g = g + 1
    join;
    print g
}
```

• What will the program print?
  • Assuming sequential consistency?

• Answer: In most cases: 2
• But in very rare cases: 1
• Depends on machine, other programs, OS, start time, ...
Locks

- Threads can acquire/release locks

```c
int g = 0; lock lg;
t1 () {
  acquire(lg); g = g + 1; release(lg);
}
main () {
  fork t1;
  acquire(lg); g = g + 1; release(lg);
  join;
  print g
}
```
Locks

- Threads can acquire/release locks
- Each lock can only be acquired by one thread at the same time

```c
int g = 0; lock lg;
t1 () {
    acquire(lg); g = g + 1; release(lg);
}
main () {
    fork t1;
    acquire(lg); g = g + 1; release(lg);
    join;
    print g
}
```
Locks

- Threads can acquire/release locks
- Each lock can only be acquired by one thread at the same time
- Other threads that want to acquire the lock have to wait

```c
int g = 0; lock lg;
t1 () {
    acquire(lg); g = g + 1; release(lg);
}
main () {
    fork t1;
    acquire(lg); g = g + 1; release(lg);
    join;
    print g
}
```
Locks

- Threads can acquire/release locks
- Each lock can only be acquired by one thread at the same time
- Other threads that want to acquire the lock have to wait
- Used to prevent data races

```c
int g = 0; lock lg;
t1 () {
    acquire(lg); g = g + 1; release(lg);
}
main () {
    fork t1;
    acquire(lg); g = g + 1; release(lg);
    join;
    print g
}
Demo: Goblint data race analyzer

- Program with data race
- Try to show bad reproducibility + dependence on machine load, etc.
- Show goblint-analyzer to find the race

http://goblint.in.tum.de
Abstract semantics with locks

- We will regard an abstract semantics with locks
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
  - E.g., pointer analysis to identify locks

- Analysis results are safe
  - If we find no datarace, there is none
  - But there may be false positives
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
  - E.g., pointer analysis to identify locks
- Has more possible executions than concrete program
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
  - E.g., pointer analysis to identify locks
- Has more possible executions than concrete program
- Analysis results are safe
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
  - E.g., pointer analysis to identify locks
- Has more possible executions than concrete program
- Analysis results are safe
  - If we find no datarace, there is none
Abstract semantics with locks

- We will regard an abstract semantics with locks
- I.e., it contains no state beyond the current program points and status of locks
- Concrete program mapped to this semantics
  - E.g., pointer analysis to identify locks
- Has more possible executions than concrete program
- Analysis results are safe
  - If we find no data race, there is none
  - But there may be false positives
Parallel flowgraphs with fork

- Add $\text{fork}(v)$ edge label, that forks new thread starting at $v$
Parallel flowgraphs with fork

- Add \( \text{fork}(v) \) edge label, that forks new thread starting at \( v \)
- For now, we ignore joins!
Parallel flowgraphs with fork

- Add $\text{fork}(v)$ edge label, that forks new thread starting at $v$
  - For now, we ignore joins!
- Abstract semantics: State is multiset of nodes.
Parallel flowgraphs with fork

- Add $\text{fork}(\nu)$ edge label, that forks new thread starting at $\nu$
  - For now, we ignore joins!
- Abstract semantics: State is multiset of nodes.
  - Initial state: $\{\nu_0\}$

\[
\begin{align*}
\{u\} \cup s &\rightarrow \{v\} \cup s & (u, a, \nu) \in E \\
\{u\} \cup s &\rightarrow \{v, w\} \cup s & (u, \text{fork}(w), \nu) \in E
\end{align*}
\]
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks $\mathbb{L}$, actions $\text{acq}(l)$ and $\text{rel}(l)$
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks $\mathbb{L}$, actions $\text{acq}(l)$ and $\text{rel}(l)$
- State: Each thread together with its acquired locks

$$\text{State: Each thread together with its acquired locks}$$
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks $L$, actions $\text{acq}(l)$ and $\text{rel}(l)$
- State: Each thread together with its acquired locks
- Initial state: $\{(v_0, \emptyset)\}$

\[
\begin{align*}
((u, L) \cup s) &\rightarrow ((v, L) \cup s) & (u, a, v) &\in E \\
((u, L) \cup s) &\rightarrow (((v, L), (w, \emptyset)) \cup s) & (u, \text{fork}(w), v) &\in E \\
((u, L) \cup s) &\rightarrow (((v, L \cup \{l\}) \cup s) & (u, \text{acq}(l), v) &\in E \text{ and } l \notin s|_2 \\
((u, L) \cup s) &\rightarrow (((v, L \setminus \{l\}) \cup s) & (u, \text{rel}(l), v) &\in E
\end{align*}
\]
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks \( L \), actions \( \text{acq}(l) \) and \( \text{rel}(l) \)
- State: Each thread together with its acquired locks
- Initial state: \( \{(v_0, \emptyset)\} \)

\[
\begin{align*}
\{(u, L)\} \cup s &\rightarrow \{(v, L)\} \cup s \quad (u, a, v) \in E
\{(u, L)\} \cup s &\rightarrow \{(v, L), (w, \emptyset)\} \cup s \quad (u, \text{fork}(w), v) \in E
\{(u, L)\} \cup s &\rightarrow \{(v, L \cup \{l\})\} \cup s \quad (u, \text{acq}(l), v) \in E \text{ and } l \notin s \mid_2
\{(u, L)\} \cup s &\rightarrow \{(v, L \setminus \{l\})\} \cup s \quad (u, \text{rel}(l), v) \in E
\end{align*}
\]

- Note: We assume that a thread only releases locks that it possesses.
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks $\mathbb{L}$, actions $\text{acq}(l)$ and $\text{rel}(l)$
- State: Each thread together with its acquired locks
- Initial state: $\{(v_0, \emptyset)\}$

\[
\begin{align*}
\{(u, L)\} \cup s & \rightarrow \{(v, L)\} \cup s & (u, a, v) \in E \\
\{(u, L)\} \cup s & \rightarrow \{(v, L), (w, \emptyset)\} \cup s & (u, \text{fork}(w), v) \in E \\
\{(u, L)\} \cup s & \rightarrow \{(v, L \cup \{l\})\} \cup s & (u, \text{acq}(l), v) \in E \text{ and } l \notin s|_2 \\
\{(u, L)\} \cup s & \rightarrow \{(v, L \setminus \{l\})\} \cup s & (u, \text{rel}(l), v) \in E
\end{align*}
\]

- Note: We assume that a thread only releases locks that it possesses.
- We assume that a thread does not acquire a lock it already possesses.
Parallel flowgraphs with fork and locks

- Additionally: Finite set of locks $\mathbb{L}$, actions $\text{acq}(l)$ and $\text{rel}(l)$
- State: Each thread together with its acquired locks
- Initial state: $\{(v_0, \emptyset)\}$

\[
\begin{align*}
\{(u, L)\} \cup s &\rightarrow \{(v, L)\} \cup s & (u, a, v) \in E \\
\{(u, L)\} \cup s &\rightarrow \{(v, L), (w, \emptyset)\} \cup s & (u, \text{fork}(w), v) \in E \\
\{(u, L)\} \cup s &\rightarrow \{(v, L \cup \{l\})\} \cup s & (u, \text{acq}(l), v) \in E \text{ and } l \not\in s_2 \\
\{(u, L)\} \cup s &\rightarrow \{(v, L \setminus \{l\})\} \cup s & (u, \text{rel}(l), v) \in E
\end{align*}
\]

- Note: We assume that a thread only releases locks that it possesses.
- We assume that a thread does not acquire a lock it already possesses.
- Invariant: For each reachable state, the thread’s lock-sets are disjoint

\[
\{(v_0, \emptyset)\} \rightarrow^* \{(u_1, L_1), (u_2, L_2)\} \cup s \implies L_1 \cap L_2 = \emptyset
\]
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
- Lock-sets
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
- Lock-sets
  - Sets of locks that must be allocated at program point
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
- Lock-sets
  - Sets of locks that must be allocated at program point
  - Used to make MHP more precise
Analysis Plan

• Lock-insensitive may-happen in parallel (MHP)
  • Sets of program points that may be executed in parallel

• Lock-sets
  • Sets of locks that must be allocated at program point
  • Used to make MHP more precise
    • \( \text{MHP}(u, v) \) only if \( u \) and \( v \) have disjoint lock sets
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
- Lock-sets
  - Sets of locks that must be allocated at program point
  - Used to make MHP more precise
    - \( MHP(u, \nu) \) only if \( u \) and \( \nu \) have disjoint lock sets
- Data-Races
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel
- Lock-sets
  - Sets of locks that must be allocated at program point
  - Used to make MHP more precise
    - MHP\((u, v)\) only if \(u\) and \(v\) have disjoint lock sets
- Data-Races
  - Identify conflicting program points, with outgoing actions that read/write the same global variable
Analysis Plan

- Lock-insensitive may-happen in parallel (MHP)
  - Sets of program points that may be executed in parallel

- Lock-sets
  - Sets of locks that must be allocated at program point
  - Used to make MHP more precise
    - MHP\((u, v)\) only if \(u\) and \(v\) have disjoint lock sets

- Data-Races
  - Identify conflicting program points, with outgoing actions that read/write the same global variable
  - Check whether they may happen in parallel
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \quad \text{(R.node)}
\]
\[
R[u] \supseteq R[v] \quad \text{if } (u, _, v) \in E \quad \text{(R.edge)}
\]
\[
R[u] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(R.trans)}
\]
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
\begin{align*}
R[u] & \supseteq \{u\} & \text{if } u \text{ interesting} & \text{(R.node)} \\
R[u] & \supseteq R[v] & \text{if } (u, \_, v) \in E & \text{(R.edge)} \\
R[u] & \supseteq R[w] & \text{if } (u, \text{fork}(w), \_) \in E & \text{(R.trans)} \\
\end{align*}
\]

\[
\begin{align*}
\text{MHP}[v] & \supseteq \text{MHP}[u] & \text{if } (u, \_, v) \in E & \text{(MHP.edge)} \\
\text{MHP}[w] & \supseteq \text{MHP}[u] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.trans)} \\
\text{MHP}[v] & \supseteq R[w] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.fork1)} \\
\text{MHP}[w] & \supseteq R[v] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.fork2)} \\
\end{align*}
\]
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \quad \text{(R.node)}
\]
\[
R[u] \supseteq R[v] \quad \text{if } (u, _, v) \in E \quad \text{(R.edge)}
\]
\[
R[u] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(R.trans)}
\]

\[
\text{MHP}[v] \supseteq \text{MHP}[u] \quad \text{if } (u, _, v) \in E \quad \text{(MHP.edge)}
\]
\[
\text{MHP}[w] \supseteq \text{MHP}[u] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.trans)}
\]
\[
\text{MHP}[v] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.fork1)}
\]
\[
\text{MHP}[w] \supseteq R[v] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.fork2)}
\]

(R.node) Interesting node reachable from itself
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \quad \text{(R.node)}
\]
\[
R[u] \supseteq R[v] \quad \text{if } (u,_,v) \in E \quad \text{(R.edge)}
\]
\[
R[u] \supseteq R[w] \quad \text{if } (u,\text{fork}(w),_) \in E \quad \text{(R.trans)}
\]
\[
\text{MHP}[v] \supseteq \text{MHP}[u] \quad \text{if } (u,_,v) \in E \quad \text{(MHP.edge)}
\]
\[
\text{MHP}[w] \supseteq \text{MHP}[u] \quad \text{if } (u,\text{fork}(w),v) \in E \quad \text{(MHP.trans)}
\]
\[
\text{MHP}[v] \supseteq R[w] \quad \text{if } (u,\text{fork}(w),v) \in E \quad \text{(MHP.fork1)}
\]
\[
\text{MHP}[w] \supseteq R[v] \quad \text{if } (u,\text{fork}(w),v) \in E \quad \text{(MHP.fork2)}
\]

$(R.edge)$ Propagate reachability over edge
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \\
R[u] \supseteq R[v] \quad \text{if } (u,_,v) \in E \\
R[u] \supseteq R[w] \quad \text{if } (u,\text{fork}(w),_) \in E
\]

(MH\$P[v] \supseteq MH\$P[u] \quad \text{if } (u,_,v) \in E \\
MH\$P[w] \supseteq MH\$P[u] \quad \text{if } (u,\text{fork}(w),v) \in E \\
MH\$P[v] \supseteq R[w] \quad \text{if } (u,\text{fork}(w),v) \in E \\
MH\$P[w] \supseteq R[v] \quad \text{if } (u,\text{fork}(w),v) \in E
\]

(R.trans) Propagate reachability over fork
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
- Reachable also over forks

\[
\begin{align*}
R[u] &\supseteq \{u\} & \text{if } u \text{ interesting} & \quad (R.\text{node}) \\
R[u] &\supseteq R[v] & \text{if } (u, _, v) \in E & \quad (R.\text{edge}) \\
R[u] &\supseteq R[w] & \text{if } (u, \text{fork}(w), _) \in E & \quad (R.\text{trans}) \\
\end{align*}
\]

\[
\begin{align*}
\text{MHP}[v] &\supseteq \text{MHP}[u] & \text{if } (u, _, v) \in E & \quad (\text{MHP.\text{edge}}) \\
\text{MHP}[w] &\supseteq \text{MHP}[u] & \text{if } (u, \text{fork}(w), v) \in E & \quad (\text{MHP.\text{trans}}) \\
\text{MHP}[v] &\supseteq R[w] & \text{if } (u, \text{fork}(w), v) \in E & \quad (\text{MHP.\text{fork1}}) \\
\text{MHP}[w] &\supseteq R[v] & \text{if } (u, \text{fork}(w), v) \in E & \quad (\text{MHP.\text{fork2}}) \\
\end{align*}
\]

$(\text{MHP.\text{edge}})$ If this edge executed, other threads still at same positions
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

  \[
  R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \quad \text{(R.node)}
  \]
  \[
  R[u] \supseteq R[v] \quad \text{if } (u, _, v) \in E \quad \text{(R.edge)}
  \]
  \[
  R[u] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(R.trans)}
  \]

  \[
  \text{MHP}[v] \supseteq \text{MHP}[u] \quad \text{if } (u, _, v) \in E \quad \text{(MHP.edge)}
  \]
  \[
  \text{MHP}[w] \supseteq \text{MHP}[u] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.trans)}
  \]
  \[
  \text{MHP}[v] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.fork1)}
  \]
  \[
  \text{MHP}[w] \supseteq R[v] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.fork2)}
  \]

(MHP.trans) Start node of forked thread parallel to other threads
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
R[u] \supseteq \{u\} \quad \text{if } u \text{ interesting} \quad \text{(R.node)}
\]
\[
R[u] \supseteq R[v] \quad \text{if } (u, _, v) \in E \quad \text{(R.edge)}
\]
\[
R[u] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(R.trans)}
\]

\[
\text{MHP}[v] \supseteq \text{MHP}[u] \quad \text{if } (u, _, v) \in E \quad \text{(MHP.edge)}
\]
\[
\text{MHP}[w] \supseteq \text{MHP}[u] \quad \text{if } (u, \text{fork}(w), v) \in E \quad \text{(MHP.trans)}
\]
\[
\text{MHP}[v] \supseteq R[w] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(MHP.fork1)}
\]
\[
\text{MHP}[w] \supseteq R[v] \quad \text{if } (u, \text{fork}(w), _) \in E \quad \text{(MHP.fork2)}
\]

(MHP.fork1) Forking thread parallel to everything that may be reached from forked thread
Lock-insensitive MHP

- Put up constraint system, $R[u]$: Set of (interesting) nodes reachable from $u$
  - Reachable also over forks

\[
\begin{align*}
R[u] & \supseteq \{u\} & \text{if } u \text{ interesting} & \text{(R.node)} \\
R[u] & \supseteq R[v] & \text{if } (u, _, v) \in E & \text{(R.edge)} \\
R[u] & \supseteq R[w] & \text{if } (u, \text{fork}(w), _) \in E & \text{(R.trans)} \\
\end{align*}
\]

\[
\begin{align*}
\text{MHP}[v] & \supseteq \text{MHP}[u] & \text{if } (u, _, v) \in E & \text{(MHP.edge)} \\
\text{MHP}[w] & \supseteq \text{MHP}[u] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.trans)} \\
\text{MHP}[v] & \supseteq R[w] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.fork1)} \\
\text{MHP}[w] & \supseteq R[v] & \text{if } (u, \text{fork}(w), v) \in E & \text{(MHP.fork2)} \\
\end{align*}
\]

(MHP.fork2) Forked thread parallel to everything that may be reached from forking thread
Correctness

- For interesting nodes $u$ and $v$ (also $u=v$), we have:

$$\exists s. \{v_0\} \rightarrow^* \{u, v\} \cup s \implies u \in \text{MHP}[v]$$
Correctness

- For interesting nodes $u$ and $v$ (also $u=\nu$), we have:

  $$\exists s. \{v_0\} \rightarrow^* \{u, v\} \cup s \implies u \in \text{MHP}[v]$$

- Proof sketch
Correctness

• For interesting nodes $u$ and $v$ (also $u=v$), we have:

$$\exists s. \{v_0\} \rightarrow^* \{u, v\} \cup s \implies u \in \text{MHP}[v]$$

• Proof sketch
  • Auxiliary: $\{u\} \rightarrow^* \{v\} \cup s \implies v \in \text{R}[u]$
Correctness

- For interesting nodes $u$ and $v$ (also $u$=v), we have:

  $$\exists s. \{v_0\} \rightarrow^* \{u, v\} \cup s \implies u \in \text{MHP}[v]$$

- Proof sketch
  - Auxiliary: $\{u\} \rightarrow^* \{v\} \cup s \implies v \in R[u]$
  - Find the crucial fork, where $u$ is reached from, wlog, the forked thread, and $v$ is reached from the forking thread
Correctness

• For interesting nodes $u$ and $v$ (also $u=v$), we have:

$$\exists s. \{v_0\} \rightarrow^* \{u, v\} \cup s \implies u \in \text{MHP}[v]$$

• Proof sketch
  • Auxiliary: $\{u\} \rightarrow^* \{v\} \cup s \implies v \in R[u]$
  • Find the crucial fork, where $u$ is reached from, wlog, the forked thread, and $v$ is reached from the forking thread
    • $\{v_0\} \rightarrow^* \{a\} \cup \ldots$, and $(a, \text{fork}(c), b) \in E$, and $\{b\} \rightarrow^* \{u\} \cup \ldots$, and $\{c\} \rightarrow^* \{v\} \cup \ldots$
Lock-set analysis

- Forward, must analysis (standard)

\[
\begin{align*}
LS[v_0] \subseteq \emptyset \\
LS[w] \subseteq \emptyset & \quad \quad (u, \text{fork}(w), v) \in E \\
LS[v] \subseteq LS[u] & \quad \quad (u, a, v) \in E, \text{ a no lock-action} \\
LS[v] \subseteq LS[u] \cup \{l\} & \quad \quad (u, \text{acq}(l), v) \in E \\
LS[v] \subseteq LS[u] \setminus \{l\} & \quad \quad (u, \text{rel}(l), v) \in E
\end{align*}
\]
Lock-set analysis

- Forward, must analysis (standard)

\[
\begin{align*}
LS[v_0] & \subseteq \emptyset \\
LS[w] & \subseteq \emptyset \quad \text{for } (u, \text{fork}(w), v) \in E \\
LS[v] & \subseteq LS[u] \quad \text{for } (u, a, v) \in E, \text{ a no lock-action} \\
LS[v] & \subseteq LS[u] \cup \{l\} \quad \text{for } (u, \text{acq}(l), v) \in E \\
LS[v] & \subseteq LS[u] \setminus \{l\} \quad \text{for } (u, \text{rel}(l), v) \in E
\end{align*}
\]

- Correctness:

\[
l \in LS[u] \implies (\forall s. \{(v_0, \emptyset)\} \rightarrow^* \{(u, L)\} \cup s \implies l \in L)
\]
Data-Race analysis

- Interesting nodes:
Data-Race analysis

- Interesting nodes:
  - Nodes with actions that read or write global variables
Data-Race analysis

- Interesting nodes:
  - Nodes with actions that read or write global variables
- For each pair \((u, v)\) of conflicting nodes, check
  \[ u \in \text{MHP}[v] \implies LS[u] \cap LS[v] \neq \emptyset \]
Data-Race analysis

- Interesting nodes:
  - Nodes with actions that read or write global variables
- For each pair \((u, v)\) of conflicting nodes, check
  \[ u \in \text{MHP}[v] \implies \text{LS}[u] \cap \text{LS}[v] \neq \emptyset \]
- If satisfied, report „definitely no data race”
Data-Race analysis

- Interesting nodes:
  - Nodes with actions that read or write global variables
- For each pair \((u, v)\) of conflicting nodes, check
  \[ u \in \text{MHP}[v] \implies \text{LS}[u] \cap \text{LS}[v] \neq \emptyset \]
- If satisfied, report „definitely no data race”
- Otherwise, report possible data race
Example

```c
int g = 0; lock lg;
t1 () {
  1:   acquire(lg);            R: 2          MHP: {7,11} L: {} 
  2:   g = g + 1;              R: 2          MHP: {7,11} L: {lg} 
  3:   release(lg);            R: {}         MHP: {7,11} L: {lg} 
  4: }                          MHP: {7,11} L: {} 
main () {
  5:   fork t1;                R: 2,7,11    MHP: {} L: {} 
  6:   acquire(lg);            R: 7,11      MHP: {2} L: {} 
  7:   g = g + 1;              R: 7,11      MHP: {2} L: {lg} 
  8:   release(lg);            R: 11        MHP: {2} L: {lg} 
  9:   join;                   R: 11        MHP: {2} L: {} 
10:   acquire(lg);            R: 11        MHP: {2} L: {} 
11:   print g                 R: 11        MHP: {2} L: {lg} 
12:   release(lg);            R: {}         MHP: {2} L: {lg} 
13: }                          R: {}         MHP: {2} L: {} 
```

- Check lock-sets for 2/7 and 2/11
Example

```c
int g = 0; lock lg;

void t1 () {
    acquire(lg); R: 2 MHP: {7,11} L: {} 
    g = g + 1; R: 2 MHP: {7,11} L: {lg} 
    release(lg); R: {} MHP: {7,11} L: {lg} 
}

void main () {
    fork t1; R: 2,7,11 MHP: {} L: {} 
    acquire(lg); R: 7,11 MHP: {2} L: {} 
    g = g + 1; R: 7,11 MHP: {2} L: {lg} } 
    release(lg); R: 11 MHP: {2} L: {lg} 
    join; R: 11 MHP: {2} L: {} 
    acquire(lg); R: 11 MHP: {2} L: {lg} 
    print g R: 11 MHP: {2} L: {lg} 
    release(lg); R: {} MHP: {2} L: {lg} 
}
```

- Check lock-sets for 2/7 and 2/11
- Lock `lg` contained in all of them
Example

```c
int g = 0; lock lg;

void t1() {
    acquire(lg); R: 2 MHP: {7,11} L: {}
    g = g + 1; R: 2 MHP: {7,11} L: {lg}
    release(lg); R: {} MHP: {7,11} L: {lg}
}

void main() {
    fork t1; R: 2,7,11 MHP: {} L: {}
    acquire(lg); R: 7,11 MHP: {2} L: {}
    g = g + 1; R: 7,11 MHP: {2} L: {lg}
    release(lg); R: 11 MHP: {2} L: {lg}
    join; R: 11 MHP: {2} L: {}
    acquire(lg); R: 11 MHP: {2} L: {lg}
    print g R: 11 MHP: {2} L: {lg}
    release(lg); R: {} MHP: {2} L: {lg}
}
```

- Check lock-sets for 2/7 and 2/11
- Lock lg contained in all of them
- Program is safe!
Discussion

- Simple (and relatively cheap) analysis
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
  - Fork inside lock
  - Deadlocks

Goblint:
- Interprocedural
- Pointer-analysis
- Constant propagation
- Equality/inequality of indexes
- ...
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
- Goblint:
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
- Goblint:
  - Interprocedural
Discussion

• Simple (and relatively cheap) analysis
• Can prove programs data-race free
• But may return false positives, due to:
  • Not handling joins
  • Ignoring data completely
  • Not handling interaction of locks and control flow
    • Fork inside lock
    • Deadlocks

• Goblint:
  • Interprocedural
  • Pointer-analysis
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
- Goblint:
  - Interprocedural
  - Pointer-analysis
  - Constant propagation
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
- Goblint:
  - Interprocedural
  - Pointer-analysis
  - Constant propagation
  - Equality/inequality of indexes
Discussion

- Simple (and relatively cheap) analysis
- Can prove programs data-race free
- But may return false positives, due to:
  - Not handling joins
  - Ignoring data completely
  - Not handling interaction of locks and control flow
    - Fork inside lock
    - Deadlocks
- Goblint:
  - Interprocedural
  - Pointer-analysis
  - Constant propagation
  - Equality/inequality of indexes
  - ...
Discussion

- Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```
Discussion

• Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

• Thread-safe?
Discussion

- Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

- Thread-safe? No!
Discussion

• Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

• Thread-safe? No!

⇒ Transactionality
Discussion

- Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

- Thread-safe? No!
  ⇒ Transactionality

- Advanced locking patterns
Discussion

- Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

- Thread-safe? No!

  ➞ Transactionality

- Advanced locking patterns
  - E.g., lock chains:

    ```c
    lock 1; lock 2; unlock 1; lock 3; unlock 2 ...
    ```
Discussion

- Freedom of data races often not enough

```c
int x[N];
void norm() {
    lock l; n = length(x); unlock l;
    lock l; x = 1/n * x; unlock l;
}
```

- Thread-safe? No!

⇒ Transactionality

- Advanced locking patterns
  - E.g., lock chains:

    ```c
    lock 1; lock 2; unlock 1; lock 3; unlock 2 ...
    ```

  - Two lock-chains executed simultaneously will never overtake
Last Lecture

- Analysis of parallel programs
  - Intraprocedural with thread creation
  - May-happen in parallel + lockset analysis = datarace analysis

- Caveats
  - Need to abstract program into model with fixed locks
    - Problematic if locks are addressed via pointers/arrays
  - Datarace freedom may no be enough
    - Transactions
    - Advanced locking patterns like lockchains
# Table of Contents

1. Introduction

2. Removing Superfluous Computations

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations
   - Strength Reduction
   - Peephole Optimization
   - Linearization

9. Exploiting Hardware Features

10. Optimization of Functional Programs
Motivating Example

```c
for (i=l; i<r; i=i+h) {
    a=a0 + b*i
    M[a] = ...
}
```

- Initialize array in range: $[l, r[$, every $h$th element
Motivating Example

```c
for (i=l; i<r; i=i+h) {
    a=a0 + b*i
    M[a] = ...
}
```

- Initialize array in range: \([l, r[\), every \(h\)th element
- Element size of array: \(b\)
Motivating Example

for (i=l; i<r; i=i+h) {
    a = a_0 + b * i
    M[a] = ...  
}

- Initialize array in range: [l, r[, every hth element
- Element size of array: b
- Loop requires r – l multiplications
Motivating Example

```c
for (i=l; i<r; i=i+h) {
    a=a_0 + b*i
    M[a] = ...
}
```

- Initialize array in range: \([l, r[\), every \(h\)th element
- Element size of array: \(b\)
- Loop requires \(r - l\) multiplications
- Multiplications are expensive, addition much cheaper
Motivating Example

for (i=l; i<r; i=i+h) {
    a = a₀ + b*i
    M[a] = ...
}

- Initialize array in range: [l, r[, every hth element
- Element size of array: b
- Loop requires r − l multiplications
- Multiplications are expensive, addition much cheaper
- Observation: From one iteration of the loop to the next:
  - Difference between as is constant: $(a₀ + b(i + h)) − (a₀ + bi) = bh$
Optimization

- First, loop inversion

```java
i=l;
if (i<r) {
    do {
        a=a0 + b*i
        M[a] = ...
        i=i+h
    } while (i<r)
}
```
Optimization

- First, loop inversion
- Second, pre-compute difference and replace computation of $a$
  - No multiplication left in loop

```c
i=1;
if (i<r) {
    delta = b*h
    a=a0 + b*i
    do {
        M[a] = ...
        i=i+h
        a=a+delta
    } while (i<r)
}
```
Optimization

- First, loop inversion
- Second, pre-compute difference and replace computation of $a$
  - No multiplication left in loop
- If
  - $i$ not used elsewhere in the loop, and
  - $i$ dead after loop
  - $b$ not zero

```c
i=l;
if (i<r) {
    delta = b*h
    a=a0 + b*i
    do {
        M[a] = ...
        i=i+h
        a=a+delta
    } while (i<r)
}
```
Optimization

- First, loop inversion
- Second, pre-compute difference and replace computation of $a$
  - No multiplication left in loop
- If
  - $i$ not used elsewhere in the loop, and
  - $i$ dead after loop
  - $b$ not zero
  - Get rid of $i$ altogether

```c
if (l<r) {
  delta = b*h
  a=a0 + b*l
  N = a0 + b*r
  do {
    M[a] = ...
    a=a+delta
  } while (a<N)
}
```
In general

- Identify
  - loops
  - iteration variables
  - constants
  - Matching use structures
Loops

- Identify loop by node $v$ where back-edge leads to, i.e., $(u, a, v) \in E$ with $v \Rightarrow u$
- Nodes of loop:

$$\text{loop}[[v]] = \{ w \mid w \rightarrow^* v \land v \Rightarrow w \}$$

- I.e., nodes which can only be reached via $v$, and from which $v$ can be reached again
Example
Example
Iteration variable

- Variable $i$, such that
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
    - where $h$ is loop constant
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
    - where $h$ is loop constant
- Loop constant: Plain constant, or, more sophisticated:
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
    - where $h$ is loop constant
- Loop constant: Plain constant, or, more sophisticated:
  - Expression that does not depend on variables modified in loop
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
    - where $h$ is loop constant
- Loop constant: Plain constant, or, more sophisticated:
  - Expression that does not depend on variables modified in loop
- Heuristics for application:
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
  - where $h$ is loop constant
- Loop constant: Plain constant, or, more sophisticated:
  - Expression that does not depend on variables modified in loop
- Heuristics for application:
  - There is an assignment to $i$ in loop
Iteration variable

- Variable $i$, such that
  - All assignments to $i$ in loop have form $i := i + h$
    - where $h$ is loop constant
- Loop constant: Plain constant, or, more sophisticated:
  - Expression that does not depend on variables modified in loop
- Heuristics for application:
  - There is an assignment to $i$ in loop
  - Assignment to $i$ executed in every iteration
Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \cdot i$, such that

  - $a_0$, $b$ are loop constants
  - $i$ is iteration variable with increment $h$
  - Introduce temporary variables $a$ and $\Delta$
  - Initialize $a = a_0 + b \cdot i$ and $\Delta = b \cdot h$ right before loop
  - Note: Loop must be inverted, to avoid extra evaluations!
  - Add $a = a + \Delta$ after assignments to $i$
  - Replace expression $a_0 + b \cdot i$ by $a$
Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \cdot i$, such that
  - $a_0, b$ are loop constants
Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \times i$, such that
  - $a_0, b$ are loop constants
  - $i$ is iteration variable with increment $h$

Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \times i$, such that
  - $a_0, b$ are loop constants
  - $i$ is iteration variable with increment $h$

- Introduce temporary variables $a$ and $\Delta$

- Note: Loop must be inverted, to avoid extra evaluations!

- Add $a = a + \Delta$ after assignments to $i$

- Replace expression $a_0 + b \times i$ by $a$
Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \cdot i$, such that
  - $a_0, b$ are loop constants
  - $i$ is iteration variable with increment $h$
- Introduce temporary variables $a$ and $\Delta$
- Initialize $a = a_0 + b \cdot i$ and $\Delta = b \cdot h$ right before loop
  - Note: Loop must be inverted, to avoid extra evaluations!
• Strength reduction possible for expressions of the form $a_0 + b \times i$, such that
  • $a_0, b$ are loop constants
  • $i$ is iteration variable with increment $h$
• Introduce temporary variables $a$ and $\Delta$
• Initialize $a = a_0 + b \times i$ and $\Delta = b \times h$ right before loop
  • Note: Loop must be inverted, to avoid extra evaluations!
• Add $a = a + \Delta$ after assignments to $i$
Strength reduction

- Strength reduction possible for expressions of the form $a_0 + b \times i$, such that
  - $a_0, b$ are loop constants
  - $i$ is iteration variable with increment $h$
- Introduce temporary variables $a$ and $\Delta$
- Initialize $a = a_0 + b \times i$ and $\Delta = b \times h$ right before loop
  - Note: Loop must be inverted, to avoid extra evaluations!
- Add $a = a + \Delta$ after assignments to $i$
- Replace expression $a_0 + b \times i$ by $a$
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: \( I_u \) for all \( u \in V \)
Excursus: Floyd-Style verification

- Establish invariants for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: $l_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory

E.g., $a = a_0 + b \ast i$ describes $\{(\rho,\mu) | \rho(a) = \rho(a_0) + b \ast \rho(i)\}$

- Show:
  - $(\rho_0,\mu_0) \in I_0$
  - for states $(\rho_0,\mu_0)$ that satisfy precondition (Here: all states)
  - For all edges $(u, a, v)$, we have $(\rho,\mu) \in I_u \cap \text{dom}(a) = \Rightarrow [u](\rho,\mu) \in I_v$
  - Then, we have, for all nodes $u$: $[u] \subseteq I_u$

Proof: Induction on paths.

Recall $[u] = \{(\rho,\mu) | \exists \rho_0,\mu_0, \pi. v_0 \xrightarrow{\pi} u \land [\pi](\rho_0,\mu_0) = (\rho,\mu)\}$

Intuition: All states reachable at $u$

Collecting semantics

And can use this fact to

Show correctness of program

Justify transformations

...
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., $a = a_0 + b \cdot i$ describes $\{(\rho, \mu) | \rho(a) = \rho(a_0) + b \cdot \rho(i)\}$
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., $a = a_0 + b \times i$ describes $\{(\rho, \mu) \mid \rho(a) = \rho(a_0) + b \times \rho(i)\}$
- Show:
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., $a = a_0 + b \times i$ describes $\{(\rho, \mu) | \rho(a) = \rho(a_0) + b \times \rho(i)\}$
- Show:
  - $(\rho_0, \mu_0) \in I_{v_0}$
    - for states $(\rho_0, \mu_0)$ that satisfy precondition (Here: all states)
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: \( I_u \) for all \( u \in V \)
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., \( a = a_0 + b \cdot i \) describes \( \{ (\rho, \mu) \mid \rho(a) = \rho(a_0) + b \cdot \rho(i) \} \)
- Show:
  - \( (\rho_0, \mu_0) \in I_{v_0} \)
    - for states \( (\rho_0, \mu_0) \) that satisfy precondition (Here: all states)
  - For all edges \( (u, a, v) \), we have
    \[
    (\rho, \mu) \in I_u \cap \text{dom}(\llbracket a \rrbracket) \implies \llbracket a \rrbracket(\rho, \mu) \in I_v
    \]
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: \( I_u \) for all \( u \in V \)
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., \( a = a_0 + b \times i \) describes \( \{(\rho, \mu) \mid \rho(a) = \rho(a_0) + b \times \rho(i)\} \)

- **Show:**
  - \( (\rho_0, \mu_0) \in I_{v_0} \)
    - for states \( (\rho_0, \mu_0) \) that satisfy precondition (Here: all states)
  - For all edges \( (u, a, v) \), we have
    \[
    (\rho, \mu) \in I_u \cap \text{dom}([a]) \implies [a](\rho, \mu) \in I_v
    \]

- Then, we have, for all nodes \( u \): \( [u] \subseteq I_u \)
- **Proof:** Induction on paths.
  - Recall \( [u] := \{(\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \quad \nu_0 \xrightarrow{\pi} u \land [\pi](\rho_0, \mu_0) = (\rho, \mu)\} \)
  - Intuition: All states reachable at \( u \)
  - Collecting semantics
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., $a = a_0 + b \ast i$ describes $\{(\rho, \mu) \mid \rho(a) = \rho(a_0) + b \ast \rho(i)\}$
- Show:
  - $(\rho_0, \mu_0) \in I_v$
    - for states $(\rho_0, \mu_0)$ that satisfy precondition (Here: all states)
  - For all edges $(u, a, v)$, we have
    $$ (\rho, \mu) \in I_u \cap \text{dom}(\llbracket a \rrbracket) \implies \llbracket a \rrbracket(\rho, \mu) \in I_v $$
- Then, we have, for all nodes $u$: $\llbracket u \rrbracket \subseteq I_u$
  - Proof: Induction on paths.
    - Recall $\llbracket u \rrbracket := \{(\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \nu_0 \xrightarrow{\pi} u \land \llbracket \pi \rrbracket(\rho_0, \mu_0) = (\rho, \mu)\}$
    - Intuition: All states reachable at $u$
    - Collecting semantics
- And can use this fact to
Excursus: Floyd-Style verification

- Establish invariants for CFG-nodes: $I_u$ for all $u \in V$
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., $a = a_0 + b \times i$ describes $\{(\rho, \mu) | \rho(a) = \rho(a_0) + b \times \rho(i)\}$
- Show:
  - $(\rho_0, \mu_0) \in I_v$
    - for states $(\rho_0, \mu_0)$ that satisfy precondition (Here: all states)
  - For all edges $(u, a, v)$, we have
    $$(\rho, \mu) \in I_u \cap \text{dom}([a]) \implies [a](\rho, \mu) \in I_v$$

- Then, we have, for all nodes $u$: $[u] \subseteq I_u$
  - Proof: Induction on paths.
    - Recall $[u] := \{(\rho, \mu) | \exists \rho_0, \mu_0, \pi. \nu_0 \xrightarrow{\pi} u \land [\pi](\rho_0, \mu_0) = (\rho, \mu)\}$
    - Intuition: All states reachable at $u$
    - Collecting semantics
  - And can use this fact to
    - Show correctness of program
Excursus: Floyd-Style verification

- Establish invariants for CFG-nodes: \( I_u \) for all \( u \in V \)
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., \( a = a_0 + b \cdot i \) describes \( \{ (\rho, \mu) \mid \rho(a) = \rho(a_0) + b \cdot \rho(i) \} \)
- Show:
  - \( (\rho_0, \mu_0) \in I_v \)
    - for states \( (\rho_0, \mu_0) \) that satisfy precondition (Here: all states)
  - For all edges \( (u, a, v) \), we have
    \[
    (\rho, \mu) \in I_u \cap \text{dom}(\llbracket a \rrbracket) \implies \llbracket a \rrbracket(\rho, \mu) \in I_v
    \]

- Then, we have, for all nodes \( u \): \( \llbracket u \rrbracket \subseteq I_u \)
  - Proof: Induction on paths.
    - Recall \( \llbracket u \rrbracket := \{ (\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \nu_0 \xrightarrow{\pi} u \land \llbracket \pi \rrbracket(\rho_0, \mu_0) = (\rho, \mu) \} \)
    - Intuition: All states reachable at \( u \)
    - Collecting semantics
- And can use this fact to
  - Show correctness of program
  - Justify transformations
Excursus: Floyd-Style verification

- Establish **invariants** for CFG-nodes: \( I_u \) for all \( u \in V \)
- Invariant is set of states
  - Equivalent notation: Characteristic formula over variables/memory
  - E.g., \( a = a_0 + b \cdot i \) describes \( \{ (\rho, \mu) \mid \rho(a) = \rho(a_0) + b \cdot \rho(i) \} \)

- Show:
  - \( (\rho_0, \mu_0) \in I_{v_0} \)
    - for states \( (\rho_0, \mu_0) \) that satisfy precondition (Here: all states)
  - For all edges \((u, a, v)\), we have
    \[
    (\rho, \mu) \in I_u \cap \text{dom}([a]) \implies [a](\rho, \mu) \in I_v
    \]

- Then, we have, for all nodes \( u \): \([u] \subseteq I_u \)
  - Proof: Induction on paths.
    - Recall \([u] := \{ (\rho, \mu) \mid \exists \rho_0, \mu_0, \pi. \ n_0 \xrightarrow{\pi} u \wedge [\pi](\rho_0, \mu_0) = (\rho, \mu) \} \)
    - Intuition: All states reachable at \( u \)
    - Collecting semantics

- And can use this fact to
  - Show correctness of program
  - Justify transformations
  - ...
Correctness

• Prove that $a = a_0 + b \cdot i \land \Delta = b \cdot h$ is invariant for all nodes in loop
  • Except the target nodes of assignments to $i$
    • There, we have $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h$
Correctness

- Prove that $a = a_0 + b \times i \land \Delta = b \times h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \times (i - h) \land \Delta = b \times h$

- Proof:
Correctness

- Prove that $a = a_0 + b \cdot i \land \Delta = b \cdot h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h$

- Proof:
  - Entering loop: Have put initialization right before loop!
Correctness

- Prove that $a = a_0 + b \times i \land \Delta = b \times h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \times (i - h) \land \Delta = b \times h$

- Proof:
  - Entering loop: Have put initialization right before loop!
  - Edge inside loop:
Correctness

- Prove that $a = a_0 + b \times i \land \Delta = b \times h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \times (i - h) \land \Delta = b \times h$

- Proof:
  - Entering loop: Have put initialization right before loop!
  - Edge inside loop:
    - No assignments to $\Delta$, $b$, and $h$
Correctness

- Prove that $a = a_0 + b \cdot i \land \Delta = b \cdot h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h$
- Proof:
  - Entering loop: Have put initialization right before loop!
  - Edge inside loop:
    - No assignments to $\Delta$, $b$, and $h$
    - Assignment $i := i + h$: Check $a = a_0 + b \cdot i \implies a = a_0 + b \cdot (i + h - h)$.
Correctness

- Prove that $a = a_0 + b \cdot i \land \Delta = b \cdot h$ is invariant for all nodes in loop
  - Except the target nodes of assignments to $i$
    - There, we have $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h$

- Proof:
  - Entering loop: Have put initialization right before loop!
  - Edge inside loop:
    - No assignments to $\Delta$, $b$, and $h$
    - Assignment $i := i + h$: Check $a = a_0 + b \cdot i \implies a = a_0 + b \cdot (i + h - h)$.
    - Assignment $a := a + \Delta$. Only occurs directly after assignment to $i$.
      Check $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h \implies a + \Delta = a_0 + b \cdot i$
Correctness

• Prove that $a = a_0 + b \cdot i \land \Delta = b \cdot h$ is invariant for all nodes in loop
  • Except the target nodes of assignments to $i$
    • There, we have $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h$

• Proof:
  • Entering loop: Have put initialization right before loop!
  • Edge inside loop:
    • No assignments to $\Delta$, $b$, and $h$
    • Assignment $i := i + h$: Check $a = a_0 + b \cdot i \implies a = a_0 + b \cdot (i + h - h)$.
    • Assignment $a := a + \Delta$. Only occurs directly after assignment to $i$.
      Check $a = a_0 + b \cdot (i - h) \land \Delta = b \cdot h \implies a + \Delta = a_0 + b \cdot i$
    • Other edges: Do not modify variables in invariant
Table of Contents

1 Introduction
2 Removing Superfluous Computations
3 Abstract Interpretation
4 Alias Analysis
5 Avoiding Redundancy (Part II)
6 Interprocedural Analysis
7 Analysis of Parallel Programs
8 Replacing Expensive by Cheaper Operations
   Strength Reduction
   Peephole Optimization
   Linearization
9 Exploiting Hardware Features
10 Optimization of Functional Programs
Peephole Optimization

- Idea: Slide a small window over the code

\[ x = x \times 2 \rightarrow x = x + x \]
\[ x = x + 1 \rightarrow x + x = 5 + a - a \rightarrow x = 5 \]
\[ x = 0 \rightarrow x = x \oplus x \]
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:

\[ x = x \times 2 \quad \rightarrow \quad x = x + x \]
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:

\[ x = x \times 2 \quad \rightarrow \quad x = x + x \]
\[ x = x + 1 \quad \rightarrow \quad x + + \]
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:

\[
\begin{align*}
    x &= x \times 2 \quad \rightarrow \quad x &= x + x \\
    x &= x + 1 \quad \rightarrow \quad x &= +
\end{align*}
\]

\[
\begin{align*}
    x &= 5 + a - a \quad \rightarrow \quad x &= 5
\end{align*}
\]
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:

\[
\begin{align*}
x &= x \times 2 &\rightarrow& & x &= x + x \\
x &= x + 1 &\rightarrow& & x &= + + \\
x &= 5 + a - a &\rightarrow& & x &= 5 \\
x &= x &\rightarrow& & \text{Nop}
\end{align*}
\]
Peephole Optimization

- Idea: Slide a small window over the code
- Optimize aggressively inside this window
- Examples:

\[
\begin{align*}
x &= x \times 2 & \rightarrow & & x &= x + x \\
x &= x + 1 & \rightarrow & & x &= + + \\
x &= 5 + a - a & \rightarrow & & x &= 5 \\
x &= x & \rightarrow & & \text{Nop} \\
x &= 0 & \rightarrow & & x &= x \oplus x
\end{align*}
\]
Sub-Problem: Elimination of Nop

- For edge $(u, \text{Nop}, v)$, such that $u$ has no further outgoing edges
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops
- Implementation

1. For each node:
   - Follow chain of \(\text{Nop}\)-edges. (Check for loop)
   - Then redirect all edges on this chain to its end

2. For each edge \((u, a, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes:
   - Replace by \((u, a, w)\)

Complexity: Linear, \(O(|E|)\)

1. No edge redirected twice.
   (For each newly discovered edge, at most one more edge followed)
2. For each edge, only one more edge followed
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse Nop-loops
- Implementation
  1. For each node:

1. For each edge \((u, \text{Nop}, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes: Replace by \((u, a, w)\)

Complexity: Linear, \(O(|E|)\)

1. No edge redirected twice. (For each newly discovered edge, at most one more edge followed)
2. For each edge, only one more edge followed
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse Nop-loops

- Implementation
  1. For each node:
     - Follow chain of Nop-edges. (Check for loop)
Sub-Problem: Elimination of Nop

• For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  • Identify \(u\) and \(v\)
  • Attention: Do not collapse \(\text{Nop}\)-loops

• Implementation
  1. For each node:
     • Follow chain of \(\text{Nop}\)-edges. (Check for loop)
     • Then redirect all edges on this chain to its end
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops

Implementation

1. For each node:
   - Follow chain of \(\text{Nop}\)-edges. (Check for loop)
   - Then redirect all edges on this chain to its end

2. For each edge \((u, a, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes:
   Replace by \((u, a, w)\)
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops

Implementation

1. For each node:
   - Follow chain of \(\text{Nop}\)-edges. (Check for loop)
   - Then redirect all edges on this chain to its end

2. For each edge \((u, a, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes:
   - Replace by \((u, a, w)\)

- Complexity: Linear, \(O(|E|)\)
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops

Implementation

1. For each node:
   - Follow chain of \(\text{Nop}\)-edges. (Check for loop)
   - Then redirect all edges on this chain to its end

2. For each edge \((u, a, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes:
   Replace by \((u, a, w)\)

- Complexity: Linear, \(O(|E|)\)

  1. No edge redirected twice.
     (For each newly discovered edge, at most one more edge followed)
Sub-Problem: Elimination of Nop

- For edge \((u, \text{Nop}, v)\), such that \(u\) has no further outgoing edges
  - Identify \(u\) and \(v\)
  - Attention: Do not collapse \(\text{Nop}\)-loops

Implementation

1. For each node:
   - Follow chain of \(\text{Nop}\)-edges. (Check for loop)
   - Then redirect all edges on this chain to its end

2. For each edge \((u, a, v)\) with \((v, \text{Nop}, w)\) and \(v\) no other outgoing nodes:
   Replace by \((u, a, w)\)

- Complexity: Linear, \(O(|E|)\)
  1. No edge redirected twice.
     (For each newly discovered edge, at most one more edge followed)
  2. For each edge, only one more edge followed
Table of Contents

1. Introduction
2. Removing Superfluous Computations
3. Abstract Interpretation
4. Alias Analysis
5. Avoiding Redundancy (Part II)
6. Interprocedural Analysis
7. Analysis of Parallel Programs
8. Replacing Expensive by Cheaper Operations
   - Strength Reduction
   - Peephole Optimization
   - Linearization
9. Exploiting Hardware Features
10. Optimization of Functional Programs
Motivation

- Translate CFG to instruction list
- Need to insert jumps. No unique translation.
- Crucial for performance

```c
while (b) {
    ...
    if (b_1) {
        c_1;
        break;
    }
    ...
}
```
Motivation

- Translate CFG to instruction list
- Need to insert jumps. No unique translation.
- Crucial for performance

```plaintext
while (b) {
    ...
    if (b1) {
        c1;
        break;
    }
    ...
}
```

Bad linearization, jump in loop
Motivation

- Translate CFG to instruction list
- Need to insert jumps. No unique translation.
- Crucial for performance

```java
while (b) {
    ...
    if (b1) {
        c1;
        break;
    }
    ...
}
```

Good linearization, jump out of loop
Heuristics

• Avoid jumps inside loops
Heuristics

- Avoid jumps inside loops
- Assign each node its loop nesting depth (temperature)
Heuristics

- Avoid jumps inside loops
- Assign each node its loop nesting depth (temperature)
  - Hotter nodes are in inner loops
Heuristics

- Avoid jumps inside loops
- Assign each node its loop nesting depth (temperature)
  - Hotter nodes are in inner loops
- If jump needs to be inserted: Jump to colder node (out of loop)
Implementation

1. Compute temperatures

• Compute predominators
• Identify back edges
• For each loop head $v$ (i.e., $(u, _, v)$ is back edge)
• Increase temperature of nodes in loop $[v]$
• Recall: $\text{loop}[v] = \{ w | w \rightarrow^* v \land v \Rightarrow w \}$

2. Linearize
• Pre-order DFS to number nodes
• Visit hotter successors first
Implementation

1. Compute temperatures
   - Compute predominators
Implementation

Compute temperatures

- Compute predominators
- Identify back edges

For each loop head $v$ (i.e., $(u, _v, v)$ is back edge)

- Increase temperature of nodes in loop $[v]$

Recall: $\text{loop}[v] = \{ w | w \rightarrow^* v \land v \Rightarrow w \}$
Compute temperatures

- Compute predominators
- Identify back edges
- For each loop head \( v \) (i.e., \((u, _, v)\) is back edge)
  - Increase temperature of nodes in \( \text{loop}[v] \)
  - Recall:

\[
\text{loop}[v] = \{ w \mid w \xrightarrow{*} v \land v \Rightarrow w \}
\]
Implementation

1. Compute temperatures
   - Compute predominators
   - Identify back edges
   - For each loop head \( v \) (i.e., \((u, _, v)\) is back edge)
     - Increase temperature of nodes in \( \text{loop}[v] \)
     - Recall:
       \[
       \text{loop}[v] = \{ w \mid w \rightarrow^* v \land v \Rightarrow w \}
       \]

2. Linearize
Implementation

1. Compute temperatures
   - Compute predominators
   - Identify back edges
   - For each loop head $v$ (i.e., $(u, _, v)$ is back edge)
     - Increase temperature of nodes in $\text{loop}[v]$
     - Recall:
       \[
       \text{loop}[v] = \{ w \mid w \to^* v \land v \Rightarrow w \}
       \]

2. Linearize
   - Pre-order DFS to number nodes
Implementation

1. **Compute temperatures**
   - Compute predominators
   - Identify back edges
   - For each loop head \( v \) (i.e., \( (u, _, v) \) is back edge)
     - Increase temperature of nodes in \( \text{loop}[v] \)
     - Recall:

\[
\text{loop}[v] = \{ w \mid w \rightarrow^* v \land v \Rightarrow w \}
\]

2. **Linearize**
   - Pre-order DFS to number nodes
   - Visit hotter successors first
Example
Example
Example
# Table of Contents

1. Introduction
2. Removing Superfluous Computations
3. Abstract Interpretation
4. Alias Analysis
5. Avoiding Redundancy (Part II)
6. Interprocedural Analysis
7. Analysis of Parallel Programs
8. Replacing Expensive by Cheaper Operations
9. Exploiting Hardware Features
10. Optimization of Functional Programs
Motivation

- Program needs to be compiled to specific hardware
Motivation

- Program needs to be compiled to specific hardware
- Which has some features that can be exploited for optimization, e.g.
Motivation

- Program needs to be compiled to specific hardware
- Which has some features that can be exploited for optimization, e.g.
  - Registers
Motivation

- Program needs to be compiled to specific hardware
- Which has some features that can be exploited for optimization, e.g.
  - Registers
  - Pipelines
Motivation

- Program needs to be compiled to specific hardware
- Which has some features that can be exploited for optimization, e.g.
  - Registers
  - Pipelines
  - Caches
Motivation

- Program needs to be compiled to specific hardware
- Which has some features that can be exploited for optimization, e.g.
  - Registers
  - Pipelines
  - Caches
  - Multiple Processors
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Removing Superfluous Computations</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Interpretation</td>
</tr>
<tr>
<td>4</td>
<td>Alias Analysis</td>
</tr>
<tr>
<td>5</td>
<td>Avoiding Redundancy (Part II)</td>
</tr>
<tr>
<td>6</td>
<td>Interprocedural Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Analysis of Parallel Programs</td>
</tr>
<tr>
<td>8</td>
<td>Replacing Expensive by Cheaper Operations</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Hardware Features</td>
</tr>
<tr>
<td></td>
<td>Register Allocation</td>
</tr>
<tr>
<td></td>
<td>Single Static Assignment Form</td>
</tr>
<tr>
<td></td>
<td>Exploiting Instruction Level Parallelism</td>
</tr>
<tr>
<td></td>
<td>Improving Memory/Cache Behaviour</td>
</tr>
<tr>
<td>10</td>
<td>Optimization of Functional Programs</td>
</tr>
</tbody>
</table>
Nomenclature

- Variables \( \text{Var} \), e.g. \( x, y, z, \ldots \): Variables in source program (formerly also called registers)
Nomenclature

- Variables $\text{Var}$, e.g. $x, y, z, \ldots$: Variables in source program (formerly also called registers)
- Registers $\text{Reg}$, e.g. $R_1, R_2, \ldots$: Registers after register allocation
Motivation

• Processor only has limited number of registers
Motivation

- Processor only has limited number of registers
- Variables need to be mapped to those registers
Motivation

- Processor only has limited number of registers
- Variables need to be mapped to those registers
- If no more registers free: Spill to memory
Motivation

- Processor only has limited number of registers
- Variables need to be mapped to those registers
- If no more registers free: Spill to memory
  - Expensive!
Motivation

- Processor only has limited number of registers
- Variables need to be mapped to those registers
- If no more registers free: Spill to memory
  - Expensive!
- Want to map as much variables as possible to registers
Example

1: x=M[a]
2: y=x+1
3: if (y=0) {
4:     z=x*x
5:     M[a]=z
6: } else {
7:     t=-y*y
8:     M[a]=t
9: }

• How many registers are needed?
Example

1: x=M[a]
2: y=x+1
3: if (y=0) {
4:   z=x*x
5:   M[a]=z
    } else {
7:   t=-y*y
8:   M[a]=t
9:   }

• How many registers are needed? Assuming all variables dead at 9
Example

1: x=M[a]
2: y=x+1
3: if (y=0) {
4:   z=x*x
5:   M[a]=z
6: } else {
7:   t=-y*y
8:   M[a]=t
9: }

• How many registers are needed? Assuming all variables dead at 9
• Variables: $a, x, y, z, t$. 
Example

1: \( R_1 = M[R_3] \)
2: \( R_2 = R_1 + 1 \)
3: if (\( R_2 = 0 \)) {
   4: \( R_1 = R_1 \times R_1 \)
   5: \( M[R_3] = R_1 \)
} else {
   7: \( R_1 = -R_2 \times R_2 \)
   8: \( M[R_3] = R_1 \)
   9: }

- How many registers are needed? Assuming all variables dead at 9
- Variables: \( a, x, y, z, t \).
- Three registers suffice: \( x, z, t \mapsto R_1, \ y \mapsto R_2, \ a \mapsto R_3 \)
Live Ranges

- Live range of variable $x$: $L[x] := \{ u \mid x \in L[u] \}$
Live Ranges

- Live range of variable $x$: $L[x] := \{u \mid x \in L[u]\}$
  - Set of nodes where $x$ is alive:
Live Ranges

- Live range of variable $x$: $L[x] := \{u \mid x \in L[u]\}$
  - Set of nodes where $x$ is alive:
  - Analogously: True live range
Live Ranges

- **Live range** of variable $x$: $L[x] := \{ u \mid x \in L[u] \}$
  - Set of nodes where $x$ is alive:
  - Analogously: **True live range**
- Observation: Two variables can be mapped to same register, if their live ranges do not overlap
Example

// L a x y z t
1: x=M[a]  // {a} 1
2: y=x+1  // {a,x} 1 1
3: if (y=0) {  // {a,x,y} 1 1 1
  4: z=x*x  // {a,x} 1 1
  5: M[a]=z  // {a,z} 1 1
  } else {
    7: t=-y*y  // {a,y} 1 1
    8: M[a]=t  // {a,t} 1 1
  9: }  // {}
Interference graph

- $I = (\text{Var}, E_I)$, with $(x, y) \in E_I$ iff $x \neq y$ and $L[x] \cap L[y] \neq \emptyset$
Interference graph

- \( I = (\text{Var}, E_i) \), with \((x, y) \in E_i\) iff \( x \neq y \) and \( L[x] \cap L[y] \neq \emptyset \)
  
  - Graph over variables. Edge iff live ranges overlap.
Interference graph

- \( I = (\text{Var}, E_I) \), with \((x, y) \in E_I\) iff \( x \neq y \) and \( L[x] \cap L[y] \neq \emptyset \)
  - Graph over variables. Edge iff live ranges overlap.
  - \( I \) is called interference graph
Interference graph

- \( I = (\text{Var}, E_I) \), with \( (x, y) \in E_I \) iff \( x \neq y \) and \( L[x] \cap L[y] \neq \emptyset \)
  - Graph over variables. Edge iff live ranges overlap.
  - \( I \) is called interference graph

- In our example:
Last lecture

- Peephole optimization, removal of NOP-edges
- Linearization
  - Temperature of nodes = loop nesting depth
  - Preferably jump to colder nodes
- Register allocation
  - Minimal coloring of interference graph
    - NP-hard
Background: Minimal graph coloring

- Given: Graph \((V, E)\)
Background: Minimal graph coloring

- Given: Graph \((V, E)\)
- Find coloring of nodes \(c : V \rightarrow \mathbb{N}\), such that
  - \((u, v) \in E \Rightarrow c(u) \neq c(v)\)
  - \(\text{max}\{c(v) | v \in V\}\) is minimal

Example:
Background: Minimal graph coloring

- Given: Graph \((V, E)\)
- Find coloring of nodes \(c : V \rightarrow \mathbb{N}\), such that
  - \((u, v) \in E \implies c(u) \neq c(v)\)
  - I.e., adjacent nodes have different colors
- \(\max\{c(v) | v \in V\}\) is minimal
Background: Minimal graph coloring

• Given: Graph \((V, E)\)
• Find \textbf{coloring} of nodes \(c: V \rightarrow \mathbb{N}\), such that
  • \((u, v) \in E \implies c(u) \neq c(v)\)
    • I.e., adjacent nodes have different colors
  • \(\max\{c(v) \mid v \in V\}\) is minimal
Background: Minimal graph coloring

- Given: Graph \( (V, E) \)
- Find coloring of nodes \( c : V \to \mathbb{N} \), such that
  - \( (u, v) \in E \implies c(u) \neq c(v) \)
    - i.e., adjacent nodes have different colors
  - \( \max\{c(v) \mid v \in V\} \) is minimal

Example:
Complexity

- Finding a minimum graph coloring is hard
  - Precisely: NP-complete to determine whether there is a coloring with at most \( k \) colors, for \( k > 2 \).
Finding a minimum graph coloring is hard
  Precisely: NP-complete to determine whether there is a coloring with at most \( k \) colors, for \( k > 2 \).
  Need heuristics
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors

Regard crown graph $C_{2n}$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.

$C_{2n} = (a_i, b_i | i ∈ 1...n, (a_i, b_j) | i \neq j)$

Minimal coloring uses two colors: One for the $a$s, and one for the $b$s

Greedy coloring with order $a_1, b_1, a_2, b_2, ...$ uses $n$ colors

Node ordering heuristics
- Nodes of high degree first
- Here: Pre-order DFS
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i \mid i \in 1 \ldots n, (a_i, b_j) \mid i \neq j)$
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i | i \in 1 \ldots n, (a_i, b_j) | i \neq j)$
  - Minimal coloring uses two colors: One for the $a$s, and one for the $b$s
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i \mid i \in 1 \ldots n, (a_i, b_j) \mid i \neq j)$
  - Minimal coloring uses two colors: One for the $a$s, and one for the $b$s
  - Greedy coloring with order $a_1, b_1, a_2, b_2, \ldots$ uses $n$ colors
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i \mid i \in 1 \ldots n, (a_i, b_j) \mid i \neq j)$
  - Minimal coloring uses two colors: One for the $a$s, and one for the $b$s
  - Greedy coloring with order $a_1, b_1, a_2, b_2, \ldots$ uses $n$ colors
- Node ordering heuristics
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i \mid i \in 1 \ldots n, (a_i, b_j) \mid i \neq j)$
  - Minimal coloring uses two colors: One for the $a$s, and one for the $b$s
  - Greedy coloring with order $a_1, b_1, a_2, b_2, \ldots$ uses $n$ colors

- Node ordering heuristics
  - Nodes of high degree first
Greedy Heuristics

- Iterate over nodes, and assign minimum color different from already colored neighbors
- Can be implemented using DFS
- In theory, result may be arbitrarily far from optimum
  - Regard crown graph $C_n$, which is a complete bipartite graph over $2n$ nodes, with a perfect matching removed.
  - $C_n = (a_i, b_i \mid i \in 1 \ldots n, (a_i, b_j) \mid i \neq j)$
  - Minimal coloring uses two colors: One for the $a$s, and one for the $b$s
  - Greedy coloring with order $a_1, b_1, a_2, b_2, \ldots$ uses $n$ colors
- Node ordering heuristics
  - Nodes of high degree first
  - Here: Pre-order DFS
Greedy heuristics, pseudocode

color(u):
    n = { v | (u,v) in E }
    c(u) = min i. i>=0 and forall v in n. i != c(v)
    for v in n
        if (c(v)==-1) color(v)

main:
    for u in V do c(u) = -1;

    for u in V do
        if c(u)==-1 then color(u)
Live Range Splitting

- Consider **basic block**,
  - i.e., sequence of statements, no jumps in/from in between
  - \((u, a_1, v_1), (v_1, a_2, v_2), \ldots, (v_{n-1}, a_n, v)\), with no other edges touching the \(v_i\).
Live Range Splitting

- Consider basic block,
  - i.e., sequence of statements, no jumps in/from in between
  - \((u, a_1, v_1), (v_1, a_2, v_2), \ldots, (v_{n-1}, a_n, v)\), with no other edges touching the \(v_i\).

- Example:

  ```
  x=M[0] //
  y=M[1] // x
  t=x+y // xy
  M[2]=t // t
  x=M[4] //
  z=M[5] // x
  t=x+z // x z
  M[6]=t // t
  y=M[7] //
  z=M[8] // y
  t=y+z // yz
  M[9]=t // t
  ```

- Requires 3 registers
  - But can do same program with two registers!
Live Range Splitting

- Consider basic block,
  - i.e., sequence of statements, no jumps in/from in between
  - \((u, a_1, v_1), (v_1, a_2, v_2), \ldots, (v_{n-1}, a_n, v)\), with no other edges touching the \(v_i\).

- Example:

```plaintext
x=M[0]  //
y=M[1]  // x
y=x+y // xy
M[2]=t //  t
x=M[4]  //
z=M[5]  // x
z=x+z // x z
M[6]=t //  t
y=M[7]  //
z=M[8]  // y
z=y+z // yz
M[9]=t //  t
```

- Requires 3 registers
Live Range Splitting

- Consider **basic block**, i.e., sequence of statements, no jumps in/from in between
  - \((u, a_1, v_1), (v_1, a_2, v_2), \ldots, (v_{n-1}, a_n, v)\), with no other edges touching the \(v_i\).

- **Example:**

  ```
  x = M[0] //
  y = M[1] // x
  t = x + y // xy
  M[2] = t // t
  x = M[4] //
  z = M[5] // x
  t = x + z // x z
  M[6] = t // t
  y = M[7] //
  z = M[8] // y
  t = y + z // yz
  M[9] = t // t
  ```

- Requires 3 registers
- But can do same program with two registers!
Live range splitting

\[ x_1 = M[0] \] //
\[ y_1 = M[1] \] // \( x_1 \)
\[ t_1 = x_1 + y_1 \] // \( x_1 y_1 \)
\[ M[2] = t_1 \] // \( t_1 \)
\[ x_2 = M[4] \] //
\[ z_1 = M[5] \] // \( x_2 \)
\[ t_2 = x_2 + z_1 \] // \( x_2 z_1 \)
\[ M[6] = t_2 \] // \( t_2 \)
\[ y_2 = M[7] \] //
\[ z_2 = M[8] \] // \( y_2 \)
\[ t_3 = y_2 + z_2 \] // \( y_2 z_2 \)
\[ M[9] = t_3 \] // \( t_3 \)
Live range splitting

\[
x_1 = M[0] // x_1
y_1 = M[1] // x_1
\]
\[
t_1 = x_1 + y_1 // x_1 y_1
M[2] = t_1 // t_1
x_2 = M[4] // x_2
z_1 = M[5] // x_2
\]
\[
t_2 = x_2 + z_1 // x_2 z_1
M[6] = t_2 // t_2
y_2 = M[7] // y_2
z_2 = M[8] // y_2
\]
\[
t_3 = y_2 + z_2 // y_2 z_2
M[9] = t_3 // t_3
\]

- In general: Rename variable if it is redefined
Live range splitting

\[ x_1 = M[0] \] //
\[ y_1 = M[1] \] // \( x_1 \)
\[ t_1 = x_1 + y_1 \] // \( x_1 y_1 \)
\[ M[2] = t_1 \] // \( t_1 \)
\[ x_2 = M[4] \] //
\[ z_1 = M[5] \] // \( x_2 \)
\[ t_2 = x_2 + z_1 \] // \( x_2 z_1 \)
\[ M[6] = t_2 \] // \( t_2 \)
\[ y_2 = M[7] \] //
\[ z_2 = M[8] \] // \( y_2 \)
\[ t_3 = y_2 + z_2 \] // \( y_2 z_2 \)
\[ M[9] = t_3 \] // \( t_3 \)

- In general: Rename variable if it is redefined
- The interference graph forms an interval graph.
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between $[i, j]$ and $[k, l]$, iff $[i, j] \cap [k, l] \neq \emptyset$
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
  - Use greedy algorithm, order intervals by left endpoints
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
  - Use greedy algorithm, order intervals by left endpoints
  - Proof idea:
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
  - Use greedy algorithm, order intervals by left endpoints
  - Proof idea:
    - After coloring all nodes with left endpoint \(i\), there are exactly \(o(i)\) colors allocated.
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - I.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
  - Use greedy algorithm, order intervals by left endpoints
  - Proof idea:
    - After coloring all nodes with left endpoint \(i\), there are exactly \(o(i)\) colors allocated.
    - Where \(o(i) := |\{v \in V \mid i \in v\}|\) - number of nodes containing \(i\).
Interval Graphs

- Nodes are intervals over the real numbers (here: natural numbers).
- Edge between \([i, j]\) and \([k, l]\), iff \([i, j] \cap [k, l] \neq \emptyset\)
  - i.e., edges between overlapping intervals
- On interval graphs, coloring can be determined efficiently
  - Use greedy algorithm, order intervals by left endpoints
  - Proof idea:
    - After coloring all nodes with left endpoint \(i\), there are exactly \(o(i)\) colors allocated.
    - Where \(o(i) := |\{v \in V \mid i \in v\}|\) - number of nodes containing \(i\).
    - Obviously, there is no coloring with less than \(\max\{o(i) \mid i \in \mathbb{N}\}\) colors
Wrap-up

- Heuristics required for register allocation
Wrap-up

- Heuristics required for register allocation
- If number of available registers not sufficient
Wrap-up

- Heuristics required for register allocation
  - If number of available registers not sufficient
    - Spill registers into memory (usually into stack)
Wrap-up

- Heuristics required for register allocation
- If number of available registers not sufficient
  - Spill registers into memory (usually into stack)
  - Preferably, hold variables from inner loops in registers
Heuristics required for register allocation

If number of available registers not sufficient
  - Spill registers into memory (usually into stack)
  - Preferably, hold variables from inner loops in registers

For basic blocks:
Wrap-up

- Heuristics required for register allocation
- If number of available registers not sufficient
  - Spill registers into memory (usually into stack)
  - Preferably, hold variables from inner loops in registers
- For basic blocks:
  - Efficient optimal register allocation
Wrap-up

- Heuristics required for register allocation
- If number of available registers not sufficient
  - Spill registers into memory (usually into stack)
  - Preferably, hold variables from inner loops in registers
- For basic blocks:
  - Efficient optimal register allocation
  - Only if live ranges are split
Wrap-up

- Heuristics required for register allocation
- If number of available registers not sufficient
  - Spill registers into memory (usually into stack)
  - Preferably, hold variables from inner loops in registers
- For basic blocks:
  - Efficient optimal register allocation
  - Only if live ranges are split
- Splitting live ranges for complete program
Wrap-up

• Heuristics required for register allocation
• If number of available registers not sufficient
  • Spill registers into memory (usually into stack)
  • Preferably, hold variables from inner loops in registers
• For basic blocks:
  • Efficient optimal register allocation
  • Only if live ranges are split
• Splitting live ranges for complete program
  $\Rightarrow$ Single static assignment form (SSA)
# Table of Contents

1. Introduction

2. Removing Superfluous Computations

3. Abstract Interpretation

4. Alias Analysis

5. Avoiding Redundancy (Part II)

6. Interprocedural Analysis

7. Analysis of Parallel Programs

8. Replacing Expensive by Cheaper Operations

9. Exploiting Hardware Features
   - Register Allocation
   - Single Static Assignment Form
   - Exploiting Instruction Level Parallelism
   - Improving Memory/Cache Behaviour

10. Optimization of Functional Programs
Idea

• Generalize live-range splitting to programs
Idea

- Generalize live-range splitting to programs
- Proceed in two steps

1. Transform program such that every program point $v$ is reached by at most one definition of variable $x$ which is live at $v$.
2. Introduce a separate variant $x_i$ for each definition of $x$, and replace occurrences of $x$ by the reaching variants.
Idea

- Generalize live-range splitting to programs
- Proceed in two steps
  1. Transform program such that every program point $v$ is reached by at most one definition of variable $x$ which is live at $v$. 


Idea

• Generalize live-range splitting to programs
• Proceed in two steps
  1. Transform program such that every program point \( v \) is reached by at most one definition of variable \( x \) which is live at \( v \).
  2. Introduce a separate variant \( x_i \) for each definition of \( x \), and replace occurrences of \( x \) by the reaching variants.
SSA, first transformation

- Assume that start node has no incoming edges.
SSA, first transformation

- Assume that start node has no incoming edges.
  - Otherwise, add new start node before transformation
SSA, first transformation

- Assume that start node has no incoming edges.
  - Otherwise, add new start node before transformation
- At incoming edges to join points \( v \), i.e., nodes with \( > 1 \) incoming edges:
SSA, first transformation

- Assume that start node has no incoming edges.
  - Otherwise, add new start node before transformation
- At incoming edges to join points $v$, i.e., nodes with $> 1$ incoming edges:
  - Introduce new edges, labeled with $\Psi_v$
SSA, first transformation

- Assume that start node has no incoming edges.
  - Otherwise, add new start node before transformation
- At incoming edges to join points $v$, i.e., nodes with $> 1$ incoming edges:
  - Introduce new edges, labeled with $\Psi_v$
  - For now: $\Psi_v := \text{Nop}$
SSA, first transformation

- Assume that start node has no incoming edges.
  - Otherwise, add new start node before transformation
- At incoming edges to join points $v$, i.e., nodes with $> 1$ incoming edges:
  - Introduce new edges, labeled with $\Psi_v$
  - For now: $\Psi_v := \text{Nop}$

![Diagram](image)
Reaching definitions

- Compute reaching definitions for each variable \( x \) and program point \( v \).
Reaching definitions

• Compute reaching definitions for each variable \( x \) and program point \( v \).
  • Intuitively: The definitions that determined the value of \( x \)
Reaching definitions

- Compute **reaching definitions** for each variable \( x \) and program point \( v \).
  - Intuitively: The definitions that determined the value of \( x \)
- Analyzed by forward may analysis, over domain \( 2^{\text{Defs}} \)
Reaching definitions

- Compute reaching definitions for each variable $x$ and program point $v$.
  - Intuitively: The definitions that determined the value of $x$
- Analyzed by forward may analysis, over domain $2^{\text{Defs}}$
  - where $\text{Defs} = \text{Var} \times V$

Initial value: $R_0 = \{(x, v_0) | x \in \text{Var}\}$

- Intuitively: Interpret program start as end-point of definition for every variable
Reaching definitions

- Compute reaching definitions for each variable $x$ and program point $v$.
  - Intuitively: The definitions that determined the value of $x$
- Analyzed by forward may analysis, over domain $2^{\text{Defs}}$
  - where $\text{Defs} = \text{Var} \times \mathbb{V}$

\[
\begin{align*}
\llbracket (u, x := e, v) \rrbracket R &= R \setminus \text{Defs}(x) \cup \{(x, v)\} \\
\llbracket (u, x := M[e], v) \rrbracket R &= R \setminus \text{Defs}(x) \cup \{(x, v)\} \\
\llbracket (u, a, v) \rrbracket R &= R
\end{align*}
\]

for other edges
**Reaching definitions**

- Compute **reaching definitions** for each variable $x$ and program point $v$.
  - Intuitively: The definitions that determined the value of $x$
- Analyzed by forward may analysis, over domain $2^{\text{Defs}}$
  - where $\text{Defs} = \text{Var} \times V$

\[
\begin{align*}
\llbracket (u, x := e, v) \rrbracket^\# R &= R \setminus \text{Defs}(x) \cup \{(x, v)\} \\
\llbracket (u, x := M[e], v) \rrbracket^\# R &= R \setminus \text{Defs}(x) \cup \{(x, v)\} \\
\llbracket (u, a, v) \rrbracket^\# R &= R
\end{align*}
\]

for other edges

- Initial value: $R_0 := \{(x, v_0) | x \in \text{Var}\}$
Reaching definitions

- Compute **reaching definitions** for each variable \( x \) and program point \( v \).
  - Intuitively: The definitions that determined the value of \( x \)
- Analyzed by forward may analysis, over domain \( 2^{\text{Defs}} \)
  - where \( \text{Defs} = \text{Var} \times \mathcal{V} \)
    
    \[
    \llbracket (u, x := e, v) \rrbracket^\# R = R \setminus \text{Defs}(x) \cup \{ (x, v) \}
    \]
    
    \[
    \llbracket (u, x := M[e], v) \rrbracket^\# R = R \setminus \text{Defs}(x) \cup \{ (x, v) \}
    \]
    
    \[
    \llbracket (u, a, v) \rrbracket^\# R = R \quad \text{for other edges}
    \]

- Initial value: \( R_0 := \{(x, v_0) \mid x \in \text{Var}\} \)
  - Intuitively: Interpret program start as end-point of definition for every variable
Simultaneous assignments

- At incoming edges to join points $v$: 

  $\Psi_v := \{ x = x | x \in L[v] \land x \in R[v] \cap \text{Defs}(x) > 1 \}$

- Assignment $x = x$ for each live variable that has more than one reaching definition.
Simultaneous assignments

- At incoming edges to join points \( v \):
- Set \( \psi_v := \{ x = x \mid x \in L[v] \land |R[v] \cap \text{Defs}(x)| > 1 \} \)
Simultaneous assignments

- At incoming edges to join points $v$:
- Set $\psi_v := \{ x = x \mid x \in L[v] \land |R[v] \cap \text{Defs}(x)| > 1 \}$
  - Assignment $x = x$ for each live variable that has more than one reaching definition
Simultaneous assignments

- At incoming edges to join points \( v \):
  - Set \( \psi_v := \{ x = x \mid x \in L[v] \land |R[v] \cap \text{Defs}(x)| > 1 \} \)
    - Assignment \( x = x \) for each live variable that has more than one reaching definition
    - **Simultaneous** assignment
Example

1: x := M[I]
2: y := 1
3: while (x > 0) {
4:   y = x * y
5:   x = x - 1
6: } 
7: M[R] = y
Example

1: \( x := M[I] \)
2: \( y := 1 \)
3: \( \text{if not (} x > 0 \text{) goto 6;} \)
4: \( y = x \times y \)
5: \( x = x - 1; \)
   \hspace{1em} \text{goto 3}
6: \( M[R] = y \)
7: \
Example

1: x := M[I]
2: y := 1
A: Nop       // Psi3
3: if not (x > 0) goto 6
4: y := x * y
5: x := x - 1
B: Nop       // Psi3
goto 3
6: M[R] := y
7:
Example

1: x:=M[I]    // {}    {(x,1), (y,1)}
2: y:=1       // {x}    {(x,2), (y,1)}
A: Nop        // {x,y}  {(x,2), (y,A)}
3: if not (x>0) goto 6; // {x,y}  {(x,2), (x,B), (y,A), (y,5)}
4: y=x*y      // {x,y}  {(x,2), (x,B), (y,A), (y,5)}
5: x=x-1      // {x,y}  {(x,2), (x,B), (y,5)}
B: Nop        // {x,y}  {(x,B), (y,5)}
goto 3
6: M[R]=y     // {y}    {(x,2), (x,B), (y,A), (y,5)}
7:             // {}    {(x,2), (x,B), (y,A), (y,5)}
Example

1: $x := M[I]$  // {}  
\{(x,1), (y,1)\}

2: $y := 1$  // \{x\}  
\{(x,2), (y,1)\}

A: $x = x \mid y = y$  // \{x, y\}  
\{(x,2), (y,A)\}

3: if not ($x > 0$) goto 6;  // \{x, y\}  
\{(x,2), (x,B), (y,A), (y,5)\}

4: $y = x \ast y$  // \{x, y\}  
\{(x,2), (x,B), (y,A), (y,5)\}

5: $x = x - 1$  // \{x, y\}  
\{(x,2), (x,B), (y,5)\}

B: $x = x \mid y = y$  // \{x, y\}  
\{(x,B), (y,5)\}

goto 3

6: $M[R] = y$  // \{y\}  
\{(x,2), (x,B), (y,A), (y,5)\}

7:  // {}  
\{(x,2), (x,B), (y,A), (y,5)\}
This ensures that only one definition of a variable reaches each program point.
• This ensures that only one definition of a variable reaches each program point
  • Identifying the definitions by simultaneous assignments on edges to same join points
Discussion

- This ensures that only one definition of a variable reaches each program point
  - Identifying the definitions by simultaneous assignments on edges to same join points
- However, we may introduce superfluous simultaneous definitions
Discussion

- This ensures that only one definition of a variable reaches each program point
  - Identifying the definitions by simultaneous assignments on edges to same join points
- However, we may introduce superfluous simultaneous definitions
- Consider, e.g.
Discussion

- This ensures that only one definition of a variable reaches each program point
  - Identifying the definitions by simultaneous assignments on edges to same join points

- However, we may introduce superfluous simultaneous definitions

- Consider, e.g.

```plaintext
1: if (*) goto 3
2: x=1
goto 4
3: x=2
4: if (*) goto 6
5: M[0]=x
6: M[1]=x
7: HALT
```
Discussion

- This ensures that only one definition of a variable reaches each program point
  - Identifying the definitions by simultaneous assignments on edges to same join points
- However, we may introduce superfluous simultaneous definitions
- Consider, e.g.

```plaintext
1: if (*) goto 3
2:   x=1
A:   x=x
goto 4
3:   x=2
B:   x=x
4: if (*) goto C
5:   M[0]=x
D:   x=x
6:   M[1]=x
7:   HALT

C:   x=x
goto 6
```
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ.
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$.
  - Extend analysis for reaching definitions by
    
    $$\llbracket (u, \{ x = x \mid x \in X \}, v) \rrbracket \# R := R \setminus \text{Defs}(X) \cup X \times \{ v \}$$

**Theorem**

For a CFG with $n$ variables, and $m$ nodes with in-degree greater one, the above algorithm terminates after at most $n(m + 1)$ rounds.
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$
  - Extend analysis for reaching definitions by
    $$\lbrack (u, \{x = x \mid x \in X\}, v) \rbrack^\# R := R \setminus \text{Defs}(X) \cup X \times \{v\}$$

Theorem

For a CFG with $n$ variables, and $m$ nodes with in-degree greater one, the above algorithm terminates after at most $n(m + 1)$ rounds.

- The efficiency depends on the number of rounds
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$
  - Extend analysis for reaching definitions by
    $\llbracket (u, \{x = x \mid x \in X\}, v) \rrbracket \# R := R \setminus \text{Defs}(X) \cup X \times \{v\}$

Theorem

For a CFG with $n$ variables, and $m$ nodes with in-degree greater one, the above algorithm terminates after at most $n(m + 1)$ rounds.

- The efficiency depends on the number of rounds
  - For well-structured CFGs, we only need one round
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$
  - Extend analysis for reaching definitions by
    $$\llbracket(u, \{x = x \mid x \in X\}, v)\rrbracket^\# R := R \setminus \text{Defs}(X) \cup X \times \{v\}$$

Theorem

For a CFG with $n$ variables, and $m$ nodes with in-degree greater one, the above algorithm terminates after at most $n(m + 1)$ rounds.

- The efficiency depends on the number of rounds
  - For well-structured CFGs, we only need one round
    - Example where 2 rounds are required on board.
Improved Algorithm

- Introduce assignment $x = x$ before node $v$ only if reaching definitions of $x$ at incoming edges to $v$ differ.
- Repeat until each node $v$ is reached by exactly one definition for each variable live at $v$.
  - Extend analysis for reaching definitions by
    \[
    \left[ (u, \{ x = x \mid x \in X \}, v) \right]^R := R \setminus \text{Defs}(X) \cup X \times \{ v \} \]

Theorem

For a CFG with $n$ variables, and $m$ nodes with in-degree greater one, the above algorithm terminates after at most $n(m + 1)$ rounds.

- The efficiency depends on the number of rounds.
  - For well-structured CFGs, we only need one round.
    - Example where 2 rounds are required on board.
  - We always may terminate after $k$ rounds by using naive algorithm.
Well-structured CFGs

- A CFG is well-structured, if it can be reduced to a single edge or vertex by the following transformations
Examples

- Flowgraphs produced by only using the following control-flow commands are well-structured
  - if, while, do-while, for
Examples

- Flowgraphs produced by only using the following control-flow commands are well-structured
  - if, while, do-while, for
- Break/Continue may break well-structuredness
Examples

• Flowgraphs produced by only using the following control-flow commands are well-structured
  • if, while, do-while, for
• Break/Continue may break well-structuredness
• Some examples on board
Second phase

- Assume, each program point $u$ is reached by exactly one definition $\langle x, w \rangle \in R[u]$ for each variable $x$ live at $u$
Second phase

- Assume, each program point $u$ is reached by exactly one definition $(x, w) \in R[u]$ for each variable $x$ live at $u$
- Define $\Phi_u(x) := x_w$ for the $w$ with $(x, w) \in R[u]$
Second phase

• Assume, each program point $u$ is reached by exactly one definition $(x, w) \in R[u]$ for each variable $x$ live at $u$
• Define $\Phi_u(x) := x_w$ for the $w$ with $(x, w) \in R[u]$
• Transform edge $(u, a, v)$ to $(u, T_{u,v}(a), v)$, where

\[
T_{u,v}(\text{Nop}) = \text{Nop}
\]
\[
T_{u,v}(\text{Neg}(e)) = \text{Neg}(\Phi_u(e))
\]
\[
T_{u,v}(\text{Pos}(e)) = \text{Pos}(\Phi_u(e))
\]
\[
T_{u,v}(x = e) = x_v = \Phi_u(e)
\]
\[
T_{u,v}(x = M[e]) = x_v = M[\Phi_u(e)]
\]
\[
T_{u,v}(M[e_1] = e_2) = M[\Phi_u(e_1)] = \Phi_u(e_2)
\]
\[
T_{u,v}(\{x = x \mid x \in X\}) = \{x_v = \Phi_u(x) \mid x \in X\}
\]

and $\Phi_u(e)$ applies $\Phi_u$ to every variable in $e$
Example

1: \texttt{x:=M[0]}
2: \texttt{y:=1}
A: \texttt{x=x\mid y=y}
3: \texttt{if not (x>0) goto 6;}
4: \texttt{y=x\times y}
5: \texttt{x=x-1}
B: \texttt{x=x\mid y=y}
goto 3
6: \texttt{M[1]=y}
7:
Example

1: \(x_2 := M[0]\)
2: \(y_A := 1\)
A: \(x_3 = x_2 \mid y_3 = y_A\)
3: if not \((x_3 > 0)\) goto 6;
4: \(y_5 = x_3 \times y_3\)
5: \(x_B = x_3 - 1\)
B: \(x_3 = x_B \mid y_3 = y_5\)
    goto 3
6: \(M[1] = y_3\)
7:
Register Allocation for SSA form

**Theorem**

Assume that every program point is reachable from start and the program is in SSA form without assignments to dead variables.

Let $\lambda$ denote the maximal number of simultaneously live variables and $G$ the interference graph of the program variables. Then:

$$\lambda = \omega(G) = \chi(G)$$

where $\omega(G), \chi(G)$ are the maximal size of a clique in $G$ and the minimal number of colors for $G$, respectively.

A minimal coloring of $G$, i.e., an optimal register allocation can be found in polynomial time.
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are chordal.

A chordal graph is one in which every cycle of length greater than 3 has a chord, i.e., an edge between two nodes of the cycle that is, itself, not part of the cycle. A graph is chordal, iff it has a perfect elimination order, i.e., an ordering of the nodes, such that each node and all adjacent nodes form a clique. Using a reverse perfect elimination ordering as node ordering for the greedy algorithm yields a minimal coloring. For graphs in SSA form, the dominance relation induces a perfect elimination ordering on the interference graph. Thus, we do not even need to construct the interference graph: Just traverse CFG with pre-order DFS, and assign registers first-come first-serve.
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - i.e., every cycle of length $> 3$ has a **chord**
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - i.e., every cycle of length > 3 has a **chord**
  - i.e., an edge between two nodes of the cycle that is, itself, not part of the cycle
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - i.e., every cycle of length > 3 has a **chord**
  - i.e., an edge between two nodes of the cycle that is, itself, not part of the cycle

- A graph is chordal, iff it has a **perfect elimination order**
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - I.e., every cycle of length > 3 has a **chord**
  - I.e., an edge between two nodes of the cycle that is, itself, not part of the cycle
- A graph is chordal, iff it has a **perfect elimination order**
  - I.e., an ordering of the nodes, such that each node $u$ and all adjacent nodes $v > u$ form a clique.
Interference graphs of program in SSA-form are **chordal**
- I.e., every cycle of length > 3 has a **chord**
- I.e., an edge between two nodes of the cycle that is, itself, not part of the cycle

A graph is chordal, iff it has a **perfect elimination order**
- I.e., an ordering of the nodes, such that each node $u$ and all adjacent nodes $v > u$ form a clique.

Using a reverse perfect elimination ordering as node ordering for the greedy algorithm yields a minimal coloring.
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - I.e., every cycle of length > 3 has a **chord**
  - i.e., an edge between two nodes of the cycle that is, itself, not part of the cycle
- A graph is chordal, iff it has a **perfect elimination order**
  - I.e., an ordering of the nodes, such that each node $u$ and all adjacent nodes $v > u$ form a clique.
- Using a reverse perfect elimination ordering as node ordering for the greedy algorithm yields a minimal coloring
- For graphs in SSA form, the dominance relation induces a perfect elimination ordering on the interference graph
Interference graphs of program in SSA-form are **chordal**
- I.e., every cycle of length $> 3$ has a **chord**
- I.e., an edge between two nodes of the cycle that is, itself, not part of the cycle

A graph is chordal, iff it has a **perfect elimination order**
- I.e., an ordering of the nodes, such that each node $u$ and all adjacent nodes $v > u$ form a clique.

Using a reverse perfect elimination ordering as node ordering for the greedy algorithm yields a minimal coloring

For graphs in SSA form, the dominance relation induces a perfect elimination ordering on the interference graph
- Thus, we do not even need to construct the interference graph:
Background: Register allocation for SSA

- Interference graphs of program in SSA-form are **chordal**
  - I.e., every cycle of length > 3 has a **chord**
  - I.e., an edge between two nodes of the cycle that is, itself, not part of the cycle
- A graph is chordal, iff it has a **perfect elimination order**
  - I.e., an ordering of the nodes, such that each node $u$ and all adjacent nodes $v > u$ form a clique.
- Using a reverse perfect elimination ordering as node ordering for the greedy algorithm yields a minimal coloring
- For graphs in SSA form, the dominance relation induces a perfect elimination ordering on the interference graph
  - Thus, we do not even need to construct the interference graph:
  - Just traverse CFG with pre-order DFS, and assign registers first-come first serve.
Background: Adjusting register pressure

- Via $\lambda$, we can simply estimate the amount of required registers (register pressure)
Background: Adjusting register pressure

- Via $\lambda$, we can simply estimate the amount of required registers (register pressure)
- And only perform optimizations that increase register pressure if still enough registers available
Discussion

- With SSA form, we get a cheap, optimal register allocation
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments

\[
\begin{align*}
R_1 &= R_2 | R_2 &= R_1 \\
R_1 &= R_3 & R_2 &= R_3 & R_1 &= R_3 \\
R_1 &= R_1 \oplus R_2 & R_2 &= R_1 \oplus R_2 & R_1 &= R_1 \oplus R_2
\end{align*}
\]

- But what about more than two registers?
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
  - Note: Original variables may be mapped to arbitrary registers
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
  - Note: Original variables may be mapped to arbitrary registers
  - I.e., $R_1 = R_2 \mid R_2 = R_1$ swaps registers $R_1$ and $R_2$
• With SSA form, we get a cheap, optimal register allocation
• But: We still have the simultaneous assignments
  • Which are meant to be executed simultaneously
  • Note: Original variables may be mapped to arbitrary registers
  • I.e., $R_1 = R_2 \mid R_2 = R_1$ swaps registers $R_1$ and $R_2$
• We need to translate these to machine instructions
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
  - Note: Original variables may be mapped to arbitrary registers
  - I.e., $R_1 = R_2 \lor R_2 = R_1$ swaps registers $R_1$ and $R_2$
- We need to translate these to machine instructions
  - Use auxiliary register: $R_3 = R_1; R_1 = R_2; R_2 = R_3$
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
  - Note: Original variables may be mapped to arbitrary registers
  - I.e., \( R_1 = R_2 \lor R_2 = R_1 \) swaps registers \( R_1 \) and \( R_2 \)
- We need to translate these to machine instructions
  - Use auxiliary register: \( R_3 = R_1; R_1 = R_2; R_2 = R_3 \)
  - Use XOR-swap: \( R_1 = R_1 \oplus R_2; R_2 = R_1 \oplus R_2; R_1 = R_1 \oplus R_2 \)
Discussion

- With SSA form, we get a cheap, optimal register allocation
- But: We still have the simultaneous assignments
  - Which are meant to be executed simultaneously
  - Note: Original variables may be mapped to arbitrary registers
  - I.e., \( R_1 = R_2 \) \( R_2 = R_1 \) swaps registers \( R_1 \) and \( R_2 \)
- We need to translate these to machine instructions
  - Use auxiliary register: \( R_3 = R_1; R_1 = R_2; R_2 = R_3 \)
  - Use XOR-swap: \( R_1 = R_1 \oplus R_2; R_2 = R_1 \oplus R_2; R_1 = R_1 \oplus R_2 \)
- But what about more than two registers?
Discussion (ctd)

- Cyclic shifts: $R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1$
Discussion (ctd)

- Cyclic shifts: $R_1 = R_2 | R_2 = R_3 | \ldots | R_n = R_1$
  - Require $n - 1$ swaps: $R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n$
• Cyclic shifts: \( R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1 \)
  • Require \( n - 1 \) swaps: \( R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n \)
• Permutations: Consider permutation \( \pi \), i.e., bijection \( \{0, \ldots n\} \rightarrow \{0, \ldots n\} \)
Discussion (ctd)

- Cyclic shifts: \( R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1 \)
  - Require \( n - 1 \) swaps: \( R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n \)

- Permutations: Consider permutation \( \pi \), i.e., bijection \( \{0, \ldots n\} \rightarrow \{0, \ldots n\} \)
  - Cycle in a permutation: Sequence \( p_1, \ldots, p_k \) such that \( \pi(p_1) = p_2, \ldots, \pi(p_k) = p_1 \), and \( i \neq j \implies p_i \neq p_j \)
  - Cayley distance: \( n - \# \text{cycles} \). Equals number of required swaps

- Process each cycle separately

- General case: Each register occurs on LHS at most once
  - Decompose into sequence of linear assignments and cyclic shifts
• Cyclic shifts: \( R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1 \)
  • Require \( n - 1 \) swaps: \( R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n \)
• Permutations: Consider permutation \( \pi \), i.e., bijection \( \{0, \ldots n\} \rightarrow \{0, \ldots n\} \)
  • Cycle in a permutation: Sequence \( p_1, \ldots, p_k \) such that
    \[ \pi(p_1) = p_2, \ldots, \pi(p_k) = p_1, \text{ and } i \neq j \implies p_i \neq p_j \]
  • Cayley distance: \( n - \#\text{cycles} \). Equals number of required swaps
Discussion (ctd)

- Cyclic shifts: \( R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1 \)
  - Require \( n - 1 \) swaps: \( R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n \)
- Permutations: Consider permutation \( \pi \), i.e., bijection \( \{0, \ldots n\} \rightarrow \{0, \ldots n\} \)
  - Cycle in a permutation: Sequence \( p_1, \ldots, p_k \) such that \( \pi(p_1) = p_2, \ldots, \pi(p_k) = p_1 \), and \( i \neq j \implies p_i \neq p_j \)
  - Cayley distance: \( n - \#\text{cycles} \). Equals number of required swaps
    - Process each cycle separately
• Cyclic shifts: $R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1$
  • Require $n - 1$ swaps: $R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n$

• Permutations: Consider permutation $\pi$, i.e., bijection $\{0, \ldots n\} \rightarrow \{0, \ldots n\}$
  • Cycle in a permutation: Sequence $p_1, \ldots, p_k$ such that
    $\pi(p_1) = p_2, \ldots, \pi(p_k) = p_1$, and $i \neq j \implies p_i \neq p_j$
  • Cayley distance: $n - \#cycles$. Equals number of required swaps
    • Process each cycle separately

• General case: Each register occurs on LHS at most once
• Cyclic shifts: $R_1 = R_2 \mid R_2 = R_3 \mid \ldots \mid R_n = R_1$
  • Require $n - 1$ swaps: $R_1 \leftrightarrow R_2; R_2 \leftrightarrow R_3; \ldots; R_{n-1} \leftrightarrow R_n$

• Permutations: Consider permutation $\pi$, i.e., bijection $\{0, \ldots n\} \rightarrow \{0, \ldots n\}$
  • Cycle in a permutation: Sequence $p_1, \ldots, p_k$ such that $\pi(p_1) = p_2, \ldots, \pi(p_k) = p_1$, and $i \neq j \implies p_i \neq p_j$
  • Cayley distance: $n - \#\text{cycles}$. Equals number of required swaps
    • Process each cycle separately

• General case: Each register occurs on LHS at most once
  • Decompose into sequence of linear assignments and cyclic shifts
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
- Sometimes, there is hardware support for this
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
- Sometimes, there is hardware support for this
- Otherwise, we have to insert load and stores. We may ...
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
- Sometimes, there is hardware support for this
- Otherwise, we have to insert load and stores. We may ...
  - Save only registers which may actually be overwritten
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
- Sometimes, there is hardware support for this
- Otherwise, we have to insert load and stores. We may ...
  - Save only registers which may actually be overwritten
  - Save only registers which are live after the call
Interprocedural Register Allocation

- For every local variable, there is an entry in the stack frame
- Save locals to stack before call, restore after call
- Sometimes, there is hardware support for this
- Otherwise, we have to insert load and stores. We may ...
  - Save only registers which may actually be overwritten
  - Save only registers which are live after the call
  - May restore into different registers $\implies$ reduction of live ranges
Motivation

- Modern processors do not execute instructions one after the other
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
Motivation

- Modern processors do not execute instructions one after the other.
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
  - Independent instructions can be executed simultaneously
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
  - Independent instructions can be executed simultaneously
  - Usually combined with pipelining
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
  - Independent instructions can be executed simultaneously
  - Usually combined with pipelining
- Who decides what instructions to parallelize
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
  - Independent instructions can be executed simultaneously
  - Usually combined with pipelining
- Who decides what instructions to parallelize
  - The compiler. \(\Rightarrow\) VLIW - architectures
    - E.g., IA64, on Itanium processors
Motivation

- Modern processors do not execute instructions one after the other
- Each instruction passes multiple phases
  - which are independent, and thus can be done in parallel for multiple instructions
  - Pipelining
- Hardware for executing instructions is duplicated (superscalar processors)
  - Independent instructions can be executed simultaneously
  - Usually combined with pipelining
- Who decides what instructions to parallelize
  - The compiler. \(\Rightarrow\) VLIW - architectures
    - E.g., IA64, on Itanium processors
  - The processor (e.g. x86)
    - Compiler should arrange instructions accordingly
Pipelining

- Execute instruction in multiple phases

- Example: 
  - $R_2 = 0$
  - $R = R + 1$
  - $R = R + R$

  The execute phase of the second instruction cannot start until the write phase of the first instruction is completed, causing a pipeline stall. If the compiler could re-arrange the instructions:
  - $R = R + 1$
  - $R_2 = 0$
  - $R = R + R$
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write

- Which are handled by different parts of the processor

- Idea: Keep all parts busy by having multiple instructions in the pipeline

- Problem: Instructions may depend on each other
  - e.g., \( R_2 = 0; R = R + 1; R = R + R \)
    - execute phase of second instruction cannot start until write-phase of first instruction completed

- Pipeline stall.

- But compiler could have rearranged instructions
  - \( R = R + 1; R_2 = 0; R = R + R \)
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor

Problem: Instructions may depend on each other
- e.g., \( R_2 = 0; R = R + 1; R = R + R \)
  - execute phase of second instruction cannot start, until write-phase of first instruction completed
  - Pipeline stall.

But compiler could have rearranged instructions
- \( R = R + 1; R_2 = 0; R = R + R \)
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
  - e.g., \( R_2 = 0; \ R = R + 1; \ R = R + R \)
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
  - e.g., $R_2 = 0; R = R+1; R = R+R$
    - execute phase of second instruction cannot start, until write-phase of first instruction completed
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
  - e.g., $R_2 = 0; R = R + 1; R = R + R$
    - execute phase of second instruction cannot start, until write-phase of first instruction completed
- Pipeline stall.
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
  - e.g., $R_2 = 0; R = R+1; R = R+R$
    - execute phase of second instruction cannot start, until write-phase of first instruction completed
- Pipeline stall.
- But compiler could have re-arranged instructions
Pipelining

- Execute instruction in multiple phases
  - e.g., fetch, decode, execute, write
  - Which are handled by different parts of the processor
- Idea: Keep all parts busy by having multiple instructions in the pipeline
- Problem: Instructions may depend on each other
  - e.g., \( R_2 = 0; \) \( R = R+1; \) \( R = R+R \)
    - execute phase of second instruction cannot start, until write-phase of first instruction completed
- Pipeline stall.
- But compiler could have re-arranged instructions
  - \( R = R+1; \) \( R_2 = 0; \) \( R = R+R \)
Superscalar architectures

- Fetch > 1 instruction per cycle.
Superscalar architectures

- Fetch $> 1$ instruction per cycle.
- Execute them in parallel if independent
Superscalar architectures

- Fetch > 1 instruction per cycle.
- Execute them in parallel if independent
- Processor checks independence
Superscalar architectures

- Fetch > 1 instruction per cycle.
- Execute them in parallel if independent
- Processor checks independence
  - Out-of-order execution: Processor may re-order instructions
Superscalar architectures

- Fetch > 1 instruction per cycle.
- Execute them in parallel if independent
- Processor checks independence
  - Out-of-order execution: Processor may re-order instructions
- Or compiler checks independence (VLIW)
Exam

- You may bring in two handwritten A4 sheets
- We will not ask you to write OCaml programs
Last Lecture

- Register allocation
  - by coloring interference graph
  - by going to SSA-form
- Instruction level parallelism
  - Pipelining, superscalar architectures
Observation

- These architectures are profitable if there are enough independent instructions available
Observation

- These architectures are profitable if there are enough independent instructions available
- Here:
Observation

- These architectures are profitable if there are enough independent instructions available
- Here:
  1. Re-arrange independent instructions (in basic blocks)
Observation

- These architectures are profitable if there are enough independent instructions available
- Here:
  1. Re-arrange independent instructions (in basic blocks)
  2. Increase size of basic blocks, to increase potential for parallelizing
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
  - read-write $a_i$ reads register written by $a_j$
Data dependence graph

- Consider basic block \( a_1; \ldots; a_n \)
- Instructions \( a_i \) and \( a_j \), \( i < j \), are dependent, iff
  - read-write \( a_i \) reads register written by \( a_j \)
  - write-read \( a_i \) writes register read by \( a_j \)
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
  - read-write $a_i$ reads register written by $a_j$
  - write-read $a_i$ writes register read by $a_j$
  - write-write $a_i$ and $a_j$ both write same register
Data dependence graph

- Consider basic block $a_1; \ldots ; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
  - read-write $a_i$ reads register written by $a_j$
  - write-read $a_i$ writes register read by $a_j$
  - write-write $a_i$ and $a_j$ both write same register
- Dependence graph: Directed graph with
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
  - read-write $a_i$ reads register written by $a_j$
  - write-read $a_i$ writes register read by $a_j$
  - write-write $a_i$ and $a_j$ both write same register
- Dependence graph: Directed graph with
  - $V := \{a_1, \ldots, a_n\}$
Data dependence graph

- Consider basic block \( a_1; \ldots; a_n \)
- Instructions \( a_i \) and \( a_j \), \( i < j \), are dependent, iff
  - read-write: \( a_i \) reads register written by \( a_j \)
  - write-read: \( a_i \) writes register read by \( a_j \)
  - write-write: \( a_i \) and \( a_j \) both write same register
- Dependence graph: Directed graph with
  - \( V := \{a_1, \ldots, a_n\} \)
  - \((a_i, a_j) \in E \) iff \( a_i \) and \( a_j \) are dependent
Data dependence graph

- Consider basic block \( a_1; \ldots; a_n \)
- Instructions \( a_i \) and \( a_j \), \( i < j \), are dependent, iff
  - read-write \( a_i \) reads register written by \( a_j \)
  - write-read \( a_i \) writes register read by \( a_j \)
  - write-write \( a_i \) and \( a_j \) both write same register
- Dependence graph: Directed graph with
  - \( V := \{a_1, \ldots, a_n\} \)
  - \((a_i, a_j) \in E\) iff \( a_i \) and \( a_j \) are dependent
- Instructions in basic block can be reordered
Data dependence graph

- Consider basic block $a_1; \ldots; a_n$
- Instructions $a_i$ and $a_j$, $i < j$, are dependent, iff
  - read-write $a_i$ reads register written by $a_j$
  - write-read $a_i$ writes register read by $a_j$
  - write-write $a_i$ and $a_j$ both write same register
- Dependence graph: Directed graph with
  - $V := \{a_1, \ldots, a_n\}$
  - $(a_i, a_j) \in E$ iff $a_i$ and $a_j$ are dependent
- Instructions in basic block can be reordered
  - As long as ordering respects dependence graph
Example

1: x=x+1
2: y=M[A]
3: t=z
4: z=M[A+x]
5: t=y+z
Example

1: \(x = x + 1\)
2: \(y = M[A]\)
3: \(t = z\)
4: \(z = M[A + x]\)
5: \(t = y + z\)
Example

1: \( x = x + 1 \)
2: \( y = M[A] \)
3: \( t = z \)
4: \( z = M[A + x] \)
5: \( t = y + z \)

Possible re-ordering:

2: \( y = M[A] \)
1: \( x = x + 1 \)
3: \( t = z \)
4: \( z = M[A + x] \)
5: \( t = y + z \)
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
Instruction Scheduling

• Goal: Find topological ordering that stalls pipeline as few as possible
  • Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem

Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
- Requires (more or less precise) model of processor architecture
- Assign priorities to source nodes in graph
  - Schedule node with highest priority first
  - Heuristics for priorities:
    - If required resources are blocked: Lower priority
    - If dependencies not yet available: Lower priority
    - If node creates many new sources: Rise priority
    - If node lies on critical path: Rise priority
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem
- Common heuristics: List scheduling
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem

- Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
Instruction Scheduling

- **Goal:** Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem
- **Common heuristics:** List scheduling
- **While scheduling, keep track of used processor resources**
  - Requires (more or less precise) model of processor architecture
Instruction Scheduling

- **Goal:** Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem

- Common heuristics: List scheduling

- While scheduling, keep track of used processor resources
  - Requires (more or less precise) model of processor architecture

- Assign priorities to source nodes in graph
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem
- Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
  - Requires (more or less precise) model of processor architecture
- Assign priorities to source nodes in graph
- Schedule node with highest priority first
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem
- Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
  - Requires (more or less precise) model of processor architecture
- Assign priorities to source nodes in graph
- Schedule node with highest priority first
- Heuristics for priorities
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem
- Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
  - Requires (more or less precise) model of processor architecture
- Assign priorities to source nodes in graph
- Schedule node with highest priority first
- Heuristics for priorities
  - If required resources are blocked: Lower priority
Instruction Scheduling

- Goal: Find topological ordering that stalls pipeline as few as possible
  - Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  - In general: NP-hard problem

- Common heuristics: List scheduling
- While scheduling, keep track of used processor resources
  - Requires (more or less precise) model of processor architecture
- Assign priorities to source nodes in graph
- Schedule node with highest priority first
- Heuristics for priorities
  - If required resources are blocked: Lower priority
  - If dependencies not yet available: Lower priority
Instruction Scheduling

• Goal: Find topological ordering that stalls pipeline as few as possible
  • Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  • In general: NP-hard problem
• Common heuristics: List scheduling
• While scheduling, keep track of used processor resources
  • Requires (more or less precise) model of processor architecture
• Assign priorities to source nodes in graph
• Schedule node with highest priority first
• Heuristics for priorities
  • If required resources are blocked: Lower priority
  • If dependencies not yet available: Lower priority
  • If node creates many new sources: Rise priority
Instruction Scheduling

• Goal: Find topological ordering that stalls pipeline as few as possible
  • Problems: Data dependencies, limited processor resources (e.g., only single floating-point unit)
  • In general: NP-hard problem
• Common heuristics: List scheduling
• While scheduling, keep track of used processor resources
  • Requires (more or less precise) model of processor architecture
• Assign priorities to source nodes in graph
• Schedule node with highest priority first
• Heuristics for priorities
  • If required resources are blocked: Lower priority
  • If dependencies not yet available: Lower priority
  • If node creates many new sources: Rise priority
  • If node lies on critical path: Rise priority
Example: Live-range splitting

- Live-range splitting helps to decrease dependencies
Example: Live-range splitting

- Live-range splitting helps to decrease dependencies
- No re-ordering possible

1: \( x=r \)
2: \( y=x+1 \)
3: \( x=s \)
4: \( z=x+1 \)
Example: Live-range splitting

- Live-range splitting helps to decrease dependencies
- Can be re-ordered

1: \( x_1 = r \)
2: \( y = x_1 + 1 \)
3: \( x_2 = s \)
4: \( z = x_2 + 1 \)
Example: Live-range splitting

- Live-range splitting helps to decrease dependencies
- Can be re-ordered

1: \( x_1 = r \)
2: \( y = x_1 + 1 \)
3: \( x_2 = s \)
4: \( z = x_2 + 1 \)

- Re-ordering

1: \( x_1 = r \)
3: \( x_2 = s \)
2: \( y = x_1 + 1 \)
4: \( z = x_2 + 1 \)
Example: Live-range splitting

- Live-range splitting helps to decrease dependencies
- Can be re-ordered
- Re-ordering

1: \( x_1 = r \)
2: \( y = x_1 + 1 \)
3: \( x_2 = s \)
4: \( z = x_2 + 1 \)

1: \( x_1 = r \)
3: \( x_2 = s \)
2: \( y = x_1 + 1 \)
4: \( z = x_2 + 1 \)

- Some processors do that dynamically
  \(\Rightarrow\) Register renaming
Loop unrolling

- Consider the example

```c
short M [...];
for (i=0; i<n; ++i) {
    M[i] = 0
}
```
Loop unrolling

• Consider the example

```c
short M [...];
for (i=0; i<n; ++i) {
    M[i] = 0
}
```

• On 32 bit architecture: Writing 16 bit words
Loop unrolling

• Consider the example

```c
short M [...];
for (i=0; i<n; ++i) {
    M[i] = 0
}
```

• On 32 bit architecture: Writing 16 bit words
  • Expensive!
Loop unrolling

- Consider the example

```c
short M [...];
for (i=0; i<n; ++i) {
    M[i] = 0
}
```

- On 32 bit architecture: Writing 16 bit words
  - Expensive!

- Consider unrolled loop (unroll factor 2)

```c
short M [...];
for (i=0; i+1<n; ) {
    M[i] = 0
    i= i+1
    M[i] = 0
    i= i+1
}
if (i<n) {M[i]=0; i=i+1}  // For odd n
```
Loop unrolling

- Consider the example

  ```
  short M [...];
  for (i=0; i<n; ++i) {
      M[i] = 0
  }
  ```

- On 32 bit architecture: Writing 16 bit words
  - Expensive!

- Consider unrolled loop (unroll factor 2)

  ```
  short M [...];
  for (i=0; i+1<n; ) {
      M[i] = 0
      i=i+1
      M[i] = 0
      i=i+1
  }
  if (i<n) {M[i]=0; i=i+1}  // For odd n
  ```

- Loop body can now easily be optimized, e.g., by peephole optimization
Loop unrolling

- Consider the example

  ```
  short M [...];
  for (i=0; i<n; ++i) {
      M[i] = 0
  }
  ```

- On 32 bit architecture: Writing 16 bit words
  - Expensive!

- Consider unrolled loop (unroll factor 2)

  ```
  short M [...];
  for (i=0; i+1<n; i=i+2) {
      (int)M[i] = 0
  }
  if (i<n) {M[i]=0; i=i+1}  // For odd n
  ```

- Loop body can now easily be optimized, e.g., by peephole optimization
Discussion

- Loop unrolling creates bigger basic blocks
Discussion

- Loop unrolling creates bigger basic blocks
- Which open more opportunities for parallelization
Discussion

- Loop unrolling creates bigger basic blocks
- Which open more opportunities for parallelization
- Quick demo with gcc -O2 -funroll-loops
Loop fusion

- Fuse together two successive loops
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- \( \text{for (...)} \{ c_1 \}; \text{for (...)} \{ c_2 \} \rightarrow \text{for (...)} \{ c_1; c_2 \} \)
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent

- \texttt{for (...) \{c_1\}; for (...) \{c_2\}} $\mapsto$ \texttt{for (...) \{c_1; c_2\}}

- In general:
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- \( \text{for } (...) \{ c_1 \}; \text{for } (...) \{ c_2 \} \mapsto \text{for } (...) \{ c_1; c_2 \} \)
- In general:
  - \( i \)th iteration of \( c_1 \) must not read data, that is written in \( < i \)th iteration of \( c_2 \)
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent

\[
\text{for ( ... ) \{ } c_1 \text{\}; for ( ... ) \{ } c_2 \text{\} } \mapsto \text{for ( ... ) \{ } c_1 ; c_2 \text{\} }
\]

- In general:
  - \(i\)th iteration of \(c_1\) must not read data, that is written in \(< \) \(i\)th iteration of \(c_2\)
  - \(i\)th iteration of \(c_2\) must not read data, that is written in \(> \) \(i\)th iteration of \(c_1\)
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- $\text{for ( ... ) \{ c_1 \} ; \text{for ( ... ) \{ c_2 \} } \mapsto \text{for ( ... ) \{ c_1 ; c_2 \}}$
- In general:
  - $i$th iteration of $c_1$ must not read data, that is written in $< i$th iteration of $c_2$
  - $i$th iteration of $c_2$ must not read data, that is written in $> i$th iteration of $c_1$
- Heuristics
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- \texttt{for (...) \{c_1\}; for (...) \{c_2\}} $\mapsto$ \texttt{for (...) \{c_1;c_2\}}
- In general:
  - $i$th iteration of $c_1$ must not read data, that is written in $< i$th iteration of $c_2$
  - $i$th iteration of $c_2$ must not read data, that is written in $> i$th iteration of $c_1$
- Heuristics
  - Data written to disjoint places
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- \texttt{for (...) \{c_1\}; for (...) \{c_2\}} \rightarrow \texttt{for (...) \{c_1; c_2\}}
- In general:
  - \textit{i}th iteration of \( c_1 \) must not read data, that is written in \( < \textit{i} \)th iteration of \( c_2 \)
  - \textit{i}th iteration of \( c_2 \) must not read data, that is written in \( > \textit{i} \)th iteration of \( c_1 \)
- Heuristics
  - Data written to disjoint places
    - E.g., different, statically allocated arrays
Loop fusion

- Fuse together two successive loops
  - With the same iteration scheme
  - That are not data-dependent
- \( \texttt{for (\ldots) \{c_1\}; for (\ldots) \{c_2\} \mapsto for (\ldots) \{c_1; c_2\}} \)
- In general:
  - \(i\)th iteration of \(c_1\) must not read data, that is written in \(< i\)th iteration of \(c_2\)
  - \(i\)th iteration of \(c_2\) must not read data, that is written in \(> i\)th iteration of \(c_1\)
- Heuristics
  - Data written to disjoint places
    - E.g., different, statically allocated arrays
  - More sophisticated analyses, e.g., based on integer linear programming
Consider the following loop, assume $A, B, C, D$ are guaranteed to be different

\[
\text{for } (i=0; i<n; ++i) \quad C[i] = A[i] + B[i]; \\
\text{for } (i=0; i<n; ++i) \quad D[i] = A[i] - B[i];
\]
Example

- Consider the following loop, assume $A, B, C, D$ are guaranteed to be different

```c
for (i=0; i<n; ++i) C[i] = A[i] + B[i];
for (i=0; i<n; ++i) D[i] = A[i] - B[i];
```

- Loop fusion yields

```c
for (i=0; i<n; ++i) {
    R1 = A[i]; R2 = B[i];
    C[i] = R1 + R2;
    D[i] = R1 - R2
}
```
Example

- Consider the following loop, assume $A, B, C, D$ are guaranteed to be different

  ```
  for (i=0; i<n; ++i) C[i] = A[i] + B[i];
  for (i=0; i<n; ++i) D[i] = A[i] - B[i];
  ```

- Loop fusion yields

  ```
  for (i=0; i<n; ++i) {
    C[i] = A[i] + B[i];
    D[i] = A[i] - B[i];
  }
  ```

- Which may be further optimized to

  ```
  for (i=0; i<n; ++i) {
    R1 = A[i]; R2 = B[i];
    C[i] = R1 + R2;
    D[i] = R1 - R2;
  }
  ```
Warning

- The opposite direction, loop fission, splits one loop into two
Warning

- The opposite direction, **loop fission**, splits one loop into two
- May be profitable for large loops
Warning

- The opposite direction, loop fission, splits one loop into two
- May be profitable for large loops
  - Smaller loops may fit into cache entirely
Warning

- The opposite direction, *loop fission*, splits one loop into two
- May be profitable for large loops
  - Smaller loops may fit into cache entirely
  - Accessed memory more local, better cache behavior
Motivation

- Aligning of data
Motivation

- Aligning of data
- Cache-aware data access
Motivation

- Aligning of data
- Cache-aware data access
- Reduction of allocation/deallocation cost
Alignment of data

- Processor usually loads 32/64 bit words from memory
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive
- So compilers can align data in memory accordingly
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive

- So compilers can align data in memory accordingly
  - Data on stack (parameters, local variables)
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive

- So compilers can align data in memory accordingly
  - Data on stack (parameters, local variables)
  - Code (labels, functions, loop-heads)
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive
- So compilers can align data in memory accordingly
  - Data on stack (parameters, local variables)
  - Code (labels, functions, loop-heads)
  - Layout of structures
Alignment of data

- Processor usually loads 32/64 bit words from memory
  - But only from address which is multiple of 4/8
  - Read from odd addresses needs to be split
  - Expensive
- So compilers can align data in memory accordingly
  - Data on stack (parameters, local variables)
  - Code (labels, functions, loop-heads)
  - Layout of structures
- At the cost of wasting more memory
Cache-aware data access

- Load instruction loads whole cache-line

- Subsequent loads within the same cache-line much faster

- Re-arrange memory accesses accordingly

- Important case: Multi-dimensional arrays
  - Iteration should iterate according to memory layout
Cache-aware data access

- Load instruction loads whole cache-line
- Subsequent loads within the same cache-line much faster
Cache-aware data access

- Load instruction loads whole cache-line
- Subsequent loads within the same cache-line much faster
- Re-arrange memory accesses accordingly
Cache-aware data access

- Load instruction loads whole cache-line
- Subsequent loads within the same cache-line much faster
- Re-arrange memory accesses accordingly
- Important case: Multi-dimensional arrays
Cache-aware data access

- Load instruction loads whole cache-line
- Subsequent loads within the same cache-line much faster
- Re-arrange memory accesses accordingly
- Important case: Multi-dimensional arrays
  - Iteration should iterate according to memory layout
Example

- **Array** $A[N][M]$
Example

- **Array** $A[N][M]
- **Assume layout:** $&(A[i, j]) = i + j*N$
Example

• **Array** $A[N][M]$

• **Assume layout:** $&(A[i, j]) = i + j*N$

• **for** $(i=0; i<N; ++i)$ **for** $(j=0; j<M; ++j)$ $x = x + A[i, j]$

• **Bad locality,** when arriving at $A[1][0]N$, cache-line loaded on $A[0][0]N$ probably already overwritten

• **Better:**

  • **for** $(j=0; j<M; ++j)$ **for** $(i=0; i<N; ++i)$ $x = x + A[i, j]$

  • **Good locality,** $A[1][0]N$ probably already in cache
Example

- **Array** \( A[N][M] \)
- **Assume layout:** \( (A[i,j]) = i + j*N \)
- **for** \((i=0; i<N; ++i)\) **for** \((j=0; j<M; ++j)\) \( x = x + A[i,j] \)
  - **Memory accesses:**
    \( A + 0 + 0N, A + 0 + 1N, A + 0 + 2N, \ldots, A + 1 + 0N, A + 1 + 1N, \ldots \)
Example

- **Array** \( A[N][M] \)
- **Assume layout:** \( \&(A[i, j]) = i + j*N \)
- **for** \((i=0; i<N; ++i)\) **for** \((j=0; j<M; ++j)\) \( x=x+A[i, j] \)
  - Memory accesses:
    \( A[0]*0*N, A[0]*1*N, A[0]*2*N, \ldots, A[1]*0*N, A[1]*1*N, \ldots \)
  - Bad locality, when arriving at \( A[1]*0*N \), cache-line loaded on \( A[0]*0*N \) probably already overwritten
Example

- **Array** $A[N][M]$
- **Assume layout**: $(A[i,j]) = i + j*N$
- **for** $(i=0; i<N; ++i)$ **for** $(j=0; j<M; ++j)$ $x = x + A[i,j]$
  - Memory accesses:
    - $A + 0 + 0N, A + 0 + 1N, A + 0 + 2N, ..., A + 1 + 0N, A + 1 + 1N, ...$
  - Bad locality, when arriving at $A + 1 + 0N$, cache-line loaded on $A + 0 + 0N$ probably already overwritten
- **Better**: **for** $(j=0; j<M; ++j)$ **for** $(i=0; i<N; ++i)$ $x = x + A[i,j]$
Example

- **Array** $A[N][M]
- **Assume layout:** $(A[i,j]) = i + j \times N$
- **for** $(i=0; i<N; ++i)$ **for** $(j=0; j<M; ++j)$ $x = x + A[i,j]$
  - Memory accesses:
    - $A + 0 + 0N, A + 0 + 1N, A + 0 + 2N, \ldots, A + 1 + 0N, A + 1 + 1N, \ldots$
  - Bad locality, when arriving at $A + 1 + 0N$, cache-line loaded on $A + 0 + 0N$ probably already overwritten
- **Better:** **for** $(j=0; j<M; ++j)$ **for** $(i=0; i<N; ++i)$ $x = x + A[i,j]$
  - Memory accesses: $A + 0 + 0N, A + 1 + 0N, \ldots, A + 0 + 1N, A + 1 + 1N, \ldots$
Example

- **Array** $A[N][M]$
- **Assume layout**: $(A[i, j]) = i + j \times N$
- **for** ($i=0; i<N; ++i$) **for** ($j=0; j<M; ++j$) $x = x + A[i, j]$
  - Memory accesses: $A + 0 + 0N, A + 0 + 1N, A + 0 + 2N, ..., A + 1 + 0N, A + 1 + 1N, ...$
  - Bad locality, when arriving at $A + 1 + 0N$, cache-line loaded on $A + 0 + 0N$ probably already overwritten
- **Better**: **for** ($j=0; j<M; ++j$) **for** ($i=0; i<N; ++i$) $x = x + A[i, j]$
  - Memory accesses: $A + 0 + 0N, A + 1 + 0N, ..., A + 0 + 1N, A + 1 + 1N, ...$
  - Good locality, $A + 1 + 0N$ probably already in cache
Loop interchange

- Swap inner and outer loop
Loop interchange

• Swap inner and outer loop
  • If they iterate over multi-dimensional array ...

The required dependency analysis is automatable

To some extend for arrays

Not so much for more complex structures
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order

Illustration on board!

The required dependency analysis is automatable

To some extend for arrays

Not so much for more complex structures
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
    - Iteration for index $i, j$, must only depend on iterations $\leq i, \leq j$
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
    - Iteration for index $i, j$, must only depend on iterations $\leq i, \leq j$
    - Illustration on board!
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
    - Iteration for index $i, j$, must only depend on iterations $\leq i, \leq j$
    - Illustration on board!

- The required dependency analysis is automatable
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
    - Iteration for index $i, j$, must only depend on iterations $\leq i, \leq j$
    - Illustration on board!
- The required dependency analysis is automatable
  - To some extend for arrays
Loop interchange

- Swap inner and outer loop
  - If they iterate over multi-dimensional array ...
  - ... in wrong order
  - And loop iterations are sufficiently independent
    - Iteration for index $i, j$, must only depend on iterations $\leq i, \leq j$
    - Illustration on board!

- The required dependency analysis is automatable
  - To some extend for arrays
  - Not so much for more complex structures
Organizing data-structures block-wise

- Warning: No automation in general
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory

- Alternative: Array-List
  - Keep list in array, store index of last element
  - If array overflows: Double the size of the array
  - If array less than quarter-full: Halve the size of the array
  - This adds amortized constant extra cost
  - But makes cache-locality much better
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
- Alternative: Array-List
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
- Alternative: Array-List
  - Keep list in array, store index of last element
Organizing data-structures block-wise

- **Warning:** No automation in general
- **Example:** Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
- **Alternative:** Array-List
  - Keep list in array, store index of last element
  - If array overflows: Double the size of the array
Organizing data-structures block-wise

- **Warning:** No automation in general
- **Example:** Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
- **Alternative:** Array-List
  - Keep list in array, store index of last element
  - If array overflows: Double the size of the array
  - If array less than quarter-full: Halve the size of the array
Organizing data-structures block-wise

- Warning: No automation in general
- Example: Stack-data structure with push, pop
  - Possible implementation: Linked list
  - Disadvantage: Data items distributed over memory
  - Bad cache behavior
  - And extra memory for link-pointers
- Alternative: Array-List
  - Keep list in array, store index of last element
  - If array overflows: Double the size of the array
  - If array less than quarter-full: Halve the size of the array
  - This adds amortized constant extra cost
Organizing data-structures block-wise

• Warning: No automation in general
• Example: Stack-data structure with push, pop
  • Possible implementation: Linked list
  • Disadvantage: Data items distributed over memory
  • Bad cache behavior
  • And extra memory for link-pointers
• Alternative: Array-List
  • Keep list in array, store index of last element
  • If array overflows: Double the size of the array
  • If array less than quarter-full: Halve the size of the array
  • This adds amortized constant extra cost
  • But makes cache-locality much better
Moving heap-allocated blocks to the stack

- Idea: Allocate block of memory on stack, instead of heap
Moving heap-allocated blocks to the stack

- Idea: Allocate block of memory on stack, instead of heap
  - If pointers to this block cannot escape the current stack frame
Moving heap-allocated blocks to the stack

- Idea: Allocate block of memory on stack, instead of heap
  - If pointers to this block cannot escape the current stack frame
  - Important for languages like Java, where almost everything is allocated on heap
Abstract example

```c
int do_computation(...) {
    AuxData aux = new AuxData();
    ...
    return ...
}
```
Abstract example

int do_computation(...) {
    AuxData aux = new AuxData()
    ...
    return ...
}

- If no pointer to aux is returned or stored in global memory ...

Abstract example

int do_computation(...) {
  AuxData aux = new AuxData()
  ...
  return ...
}

- If no pointer to aux is returned or stored in global memory ...
- ... aux can be allocated on method’s stack-frame
Example

- Recall our simple pointer-language. *Ret* is global variable.

  1: x=new()
  2: y=new()
      x[A] = y
      z=x[A]
      Ret = z
Example

- Recall our simple pointer-language. Ret is global variable.

  1: \texttt{x=new()}
  2: \texttt{y=new()}
  \hspace{1em} \texttt{x[A] = y}
  \hspace{1em} \texttt{z=x[A]}
  \hspace{1em} \texttt{Ret = z}

- Allocation at 1 may not escape
Example

• Recall our simple pointer-language. *Ret* is global variable.

1: x=new()
2: y=new()
   x[A] = y
   z=x[A]
   Ret = z

• Allocation at 1 may not escape
• Thus we may do the allocation on the stack
In general

- Memory block may escape, which is
In general

- Memory block may escape, which is
  - Assigned to global variable
In general

- Memory block may escape, which is
  - Assigned to global variable
  - Reachable from global variable
In general

- Memory block may escape, which is
  - Assigned to global variable
  - Reachable from global variable
- Forward may analysis. Same as pointer-analysis
In general

- Memory block may escape, which is:
  - Assigned to global variable
  - Reachable from global variable
- Forward may analysis. Same as pointer-analysis:
  - Identify memory blocks with allocation sites
In general

- Memory block may escape, which is
  - Assigned to global variable
  - Reachable from global variable
- Forward may analysis. Same as pointer-analysis
  - Identify memory blocks with allocation sites
  - Analyze where variables/blocks may point to
In general

- Memory block may escape, which is
  - Assigned to global variable
  - Reachable from global variable
- Forward may analysis. Same as pointer-analysis
  - Identify memory blocks with allocation sites
  - Analyze where variables/blocks may point to
  - If global variable/unknown memory block may point to block: Possible escape
Applying the optimization, heuristics

- Only makes sense for small blocks
Applying the optimization, heuristics

- Only makes sense for small blocks
- That are allocated only once
Applying the optimization, heuristics

- Only makes sense for small blocks
- That are allocated only once
  - e.g., not inside loop
Handling procedures more precisely

- Require interprocedural points-to analysis
Handling procedures more precisely

- Require interprocedural points-to analysis
  - Expensive
Handling procedures more precisely

- Require interprocedural points-to analysis
  - Expensive
  - We do not always know whole program
Handling procedures more precisely

- Require interprocedural points-to analysis
  - Expensive
  - We do not always know whole program
    - E.g. Java loads classes at runtime
Handling procedures more precisely

- Require interprocedural points-to analysis
  - Expensive
  - We do not always know whole program
    - E.g. Java loads classes at runtime
- In worst case: Assume everything visible to called procedure may escape
Handling procedures more precisely

- Require interprocedural points-to analysis
  - Expensive
  - We do not always know whole program
    - E.g. Java loads classes at runtime
- In worst case: Assume everything visible to called procedure may escape
  - Which is consistent with parameter passing by global variables and previous analysis
Wrap-Up

• Several optimizations that exploit hardware utilization
Wrap-Up

- Several optimizations that exploit hardware utilization
- A meaningful ordering
Wrap-Up

- Several optimizations that exploit hardware utilization
- A meaningful ordering
  - Restructuring of procedures/loops for better cache-behaviour
Wrap-Up

- Several optimizations that exploit hardware utilization
- A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
     - Loop interchange, fission
Wrap-Up

• Several optimizations that exploit hardware utilization
• A meaningful ordering
  
  1 Restructuring of procedures/loops for better cache-behaviour
    • Loop interchange, fission
    • Tail-recursion/inlining, stack-allocation
Wrap-Up

- Several optimizations that exploit hardware utilization
- A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
     - Loop interchange, fission
     - Tail-recursion/inlining, stack-allocation
  2. Basic-block optimizations, to exploit instruction-level parallelism
Wrap-Up

• Several optimizations that exploit hardware utilization
• A meaningful ordering
  ① Restructuring of procedures/loops for better cache-behaviour
    • Loop interchange, fission
    • Tail-recursion/inlining, stack-allocation
  ② Basic-block optimizations, to exploit instruction-level parallelism
    • Live-range splitting
Wrap-Up

• Several optimizations that exploit hardware utilization
• A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
     • Loop interchange, fission
     • Tail-recursion/inlining, stack-allocation
  2. Basic-block optimizations, to exploit instruction-level parallelism
     • Live-range splitting
     • Instruction scheduling
Wrap-Up

- Several optimizations that exploit hardware utilization
- A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
     - Loop interchange, fission
     - Tail-recursion/inlining, stack-allocation
  2. Basic-block optimizations, to exploit instruction-level parallelism
     - Live-range splitting
     - Instruction scheduling
     - Loop unrolling, fusion
Wrap-Up

• Several optimizations that exploit hardware utilization
• A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
     • Loop interchange, fission
     • Tail-recursion/inlining, stack-allocation
  2. Basic-block optimizations, to exploit instruction-level parallelism
     • Live-range splitting
     • Instruction scheduling
     • Loop unrolling, fusion
  3. Then register allocation
Wrap-Up

• Several optimizations that exploit hardware utilization
• A meaningful ordering
  1. Restructuring of procedures/loops for better cache-behaviour
  • Loop interchange, fission
  • Tail-recursion/inlining, stack-allocation
  2. Basic-block optimizations, to exploit instruction-level parallelism
  • Live-range splitting
  • Instruction scheduling
  • Loop unrolling, fusion
  3. Then register allocation
  4. And finally peephole optimization + instruction selection
Last Lecture

- Optimizations to re-arrange memory access wrt. cache
  - Loop interchange
  - Lists vs. array-list
- Wrap-Up: Optimizations targeted towards features of hardware
- Started with functional languages
We consider simple functional language

\[
\text{prg ::= let rec } f_1 = e_1 \mid \ldots \mid f_n = e_n \text{ in } e \\
\text{e ::= } b \mid c \mid x \mid f_i \mid \text{op} \mid e \ e \mid \text{fn } x.\ e \ \\
\quad \mid \text{let } x=e \text{ in } e \\
\quad \mid \text{match } e \text{ with } p_1 \Rightarrow e_1 \mid \ldots \mid p_n \Rightarrow e_n \\
\text{p ::= } b \mid c \ x_1 \ldots \ x_n
\]
We consider simple functional language

\[
\text{prg ::= let rec } f_1 = e_1 \mid \ldots \mid f_n = e_n \text{ in e}
\]

\[
e ::= b \mid c \mid x \mid f_i \mid \text{op} \mid e \; e \mid \text{fn} \; x. \; e
\]

\[
\mid \text{let } x = e \text{ in } e
\]

\[
\mid \text{match } e \text{ with } p_1 \Rightarrow e_1 \mid \ldots \mid p_n \Rightarrow e_n
\]

\[
p ::= b \mid c \; x_1 \; \ldots \; x_n
\]

where

- \( b \) is primitive constant
- \( c \) is constructor
- \( x \) is variable
- \( f_i \) is recursive function
- \( \text{op} \) is primitive operation
Semantics

- Values $b, c v_1 \ldots v_n, fn \ x. \ e$ (Convention: $v$ denotes values)
Semantics

- Values $b, c \ nar v_1 \ldots v_n, fn \times. e$ (Convention: $v$ denotes values)
- Goal of semantics: Evaluate main expression to value
Semantics

- Values $b, c, v_1 \ldots v_n, fn \ x. \ e$ (Convention: $v$ denotes values)
- Goal of semantics: Evaluate main expression to value
- Done by the following rules

\[
\begin{align*}
\text{[rec]} & \quad \text{let rec } f_i = e_i \\
& \quad f_i \rightarrow e_i \\
\text{[op]} & \quad op \ b_1 \ldots b_n \rightarrow [op](b_1, \ldots, b_n) \\
\text{[app1]} & \quad e_1 \rightarrow e'_1 \\
& \quad e_1 e_2 \rightarrow e'_1 e_2 \\
\text{[app2]} & \quad e_2 \rightarrow e'_2 \\
& \quad \nu_1 e_2 \rightarrow \nu_1 e'_2 \\
\text{[β-red]} & \quad (fn \ x. \ e) \ \nu \rightarrow e[x \mapsto \nu] \\
\text{[match1]} & \quad \text{match } e \text{ with } \ldots \rightarrow \text{match } e' \text{ with } \ldots \\
\text{[match2]} & \quad \text{match } \nu \text{ with } \ldots \rightarrow e_i \sigma \quad (*) \\
\text{[app-op]} & \quad op \ \nu_1 \ldots \nu_{k-1} e_k \ldots e_n \rightarrow op \ \nu_1 \ldots \nu_{k-1} e'_k \ldots e_n
\end{align*}
\]

- where \text{let } x = e_1 \text{ in } e_2 \text{ is syntax for } (fn \ x. \ e_2) \ e_1
- \text{(*)}: p_i \Rightarrow e_i \text{ is the first pattern with } p_i \sigma = \nu
Semantics

- Eager evaluation
Semantics

- Eager evaluation
  - Arguments are evaluated before function is called
Semantics

• Eager evaluation
  • Arguments are evaluated before function is called
• No types: Evaluation of badly-typed program just gets stuck
Semantics

- Eager evaluation
  - Arguments are evaluated before function is called
- No types: Evaluation of badly-typed program just gets stuck
  - Example: `match 5 with True => ... | False => ...`
let
    rec fac = fn x. match x with
      0 => 1
    | x => x * fac (x-1)
in fac 2

fac 2
Example

let
    rec fac = fn x. match x with
         0 => 1
    | x => x * fac (x-1)
in fac 2

(fn x. ...) 2
Example

let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in fac 2

match 2 with ...
Example

let
    rec fac = fn x. match x with
      0 => 1
    | x => x * fac (x-1)
in fac 2

(*) 2 (fac (2-1))
let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
  in fac 2

(*) 2 ((fn x. ...) (2-1))
Example

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in fac 2

(*) 2 ((fn x. ...) 1)
let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in fac 2

(*) 2 (match 1 with ...)
Example

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in fac 2

(*) 2 (((*) 1 (fac (1-1))))
Example

let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in fac 2

(*) 2 ((*) 1 (((fn x. ...) (1-1))))
let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in fac 2

(*) 2 ((*) 1 ((fn x. ...) 0))
let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in fac 2

(*) 2 ((*) 1 (match 0 with ...))
let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in fac 2

(*) 2 ((*) 1 1)
Example

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in fac 2

(*) 2 1
Example

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in fac 2

2
Lazy evaluation

- Evaluate arguments only when needed, as far as needed
Lazy evaluation

- Evaluate arguments only when needed, as far as needed
  - I.e., on match or built-in function call

\[
\begin{align*}
\text{[rec]} & \quad \text{let rec } f_i = e_i \\
& \quad f_i \to e_i \\
\text{[op]} & \quad op \ b_1 \ldots b_n \to [op](b_1, \ldots, b_n)
\end{align*}
\]

\[
\begin{align*}
\text{[app1]} & \quad e_1 \to e'_1 \\
& \quad e_2 \to e'_1 e_2 \\
\mathbf{[\beta-\text{red}]} & \quad (fn \ x. \ e_1) e_2 \to e_1[x \mapsto e_2]
\end{align*}
\]

\[
\begin{align*}
\text{[match1]} & \quad \text{match } e \text{ with } \ldots \to \text{match } e' \text{ with } \ldots \\
\text{[match2]} & \quad \text{match } c \hat{e}_1 \ldots \hat{e}_k \text{ with } \ldots \to e_i\sigma \quad (*)
\end{align*}
\]

\[
\begin{align*}
\text{[match3]} & \quad \text{match } b \text{ with } \ldots \to e_i\sigma \quad (*)
\end{align*}
\]

\[
\begin{align*}
\text{[app-op]} & \quad op \ v_1 \ldots v_{k-1} e_k \ldots e_n \to op \ v_1 \ldots v_{k-1} e'_k \ldots e_n
\end{align*}
\]

Note: Only simple patterns allowed in match.
Lazy evaluation

- Evaluate arguments only when needed, as far as needed
  - I.e., on match or built-in function call

\[
\begin{align*}
\text{[rec]} & \quad \text{let rec } f_i = e_i \quad \quad & \text{[op]} & \quad \text{op } b_1 \ldots b_n \rightarrow \text{[op]}(b_1, \ldots, b_n) \\
& \quad f_i \rightarrow e_i \quad & & \\
\text{[app1]} & \quad e_1 \rightarrow e'_1 \quad & \text{[β-red]} & \quad (\text{fn } x. \ e_1) \ e_2 \rightarrow e_1[x \mapsto e_2] \\
& \quad e_1 \ e_2 \rightarrow e'_1 \ e_2 \quad & & \\
\text{[match1]} & \quad \text{match } e \text{ with } \ldots \rightarrow \text{match } e' \text{ with } \ldots \\
\text{[match2]} & \quad \text{match } c \ \hat{e}_1 \ldots \hat{e}_k \text{ with } \ldots \rightarrow e_i\sigma \quad (*) \\
\text{[match3]} & \quad \text{match } b \text{ with } \ldots \rightarrow e_i\sigma \quad (*) \\
\text{[app-op]} & \quad e_k \rightarrow e'_k \\
& \quad \text{op } v_1 \ldots v_{k-1} \ e_k \ldots e_n \rightarrow \text{op } v_1 \ldots v_{k-1} \ e'_k \ldots e_n
\end{align*}
\]

- Note: Only simple patterns allowed in match
Example (lazy)

```haskell
let 
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in (fac 2)

(fac 2)
```
Example (lazy)

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in (fac 2)

((fn x. ...) 2)
Example (lazy)

```ocaml
let rec fac = fn x. match x with
  0 => 1
| x => x * fac (x-1)
in (fac 2)

(match 2 with ...)```
Example (lazy)

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in (fac 2)

((*) 2 (fac (2-1)))
let
  rec fac = fn x. match x with
    0 => 1
  | x => x * fac (x-1)
in (fac 2)

((*) 2 ((fn x. ...) (2-1)))
Example (lazy)

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)

in (fac 2)

((*) 2 (match (2-1) with ...))
Example (lazy)

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in (fac 2)

((*) 2 (match 1 with ...))
Example (lazy)

let
    rec fac = fn x. match x with
        0 => 1
    | x => x * fac (x-1)
in (fac 2)

and so on ...
Eager vs. Lazy

- **Eager**: Argument evaluated before function call
- **Lazy**: Function call before argument
  - Argument of match only until constructor is at top
    - Weak head normal form
  - Arguments of primitive operator: Completely
Optimization Plan

- Optimize on functional level
Optimization Plan

- Optimize on functional level
- Translate to imperative language/IR
Optimization Plan

- Optimize on functional level
- Translate to imperative language/IR
- Use optimizations for imperative code
Optimization Plan

- Optimize on functional level
- Translate to imperative language/IR
- Use optimizations for imperative code
- Now: Optimizations on functional level
# Table of Contents

1. Introduction
2. Removing Superfluous Computations
3. Abstract Interpretation
4. Alias Analysis
5. Avoiding Redundancy (Part II)
6. Interprocedural Analysis
7. Analysis of Parallel Programs
8. Replacing Expensive by Cheaper Operations
9. Exploiting Hardware Features
10. Optimization of Functional Programs
   - Semantics
   - Simple Optimizations
   - Specialization
   - Deforestation
Simple optimizations

- Idea: Move some evaluation from run-time to compile-time
Simple optimizations

• Idea: Move some evaluation from run-time to compile-time
• Function-application to let

\[(\text{fn } x. \ e_1) \ e_2 \rightarrow \text{let } x=e_2 \ \text{in } e_1\]
Simple optimizations

- Idea: Move some evaluation from run-time to compile-time
- Function-application to let
  
  \[(\text{fn } x. \ e_1) \ e_2 \rightarrow \text{let } x=e_2 \text{ in } e_1\]

- Matches, where part of the pattern is already known

  \[
  \text{match } c \ e_1 \ldots \ e_n \text{ with } \ldots \ c \ x_1 \ldots \ x_n \Rightarrow e \\
  > \text{let } x_1=e_1; \ldots; x_n=e_n \text{ in } e
  \]
Simple optimizations

- Idea: Move some evaluation from run-time to compile-time
- Function-application to let
  
  \( (\text{fn } x. \ e_1) \ e_2 \rightarrow \text{let } x=e_2 \text{ in } e_1 \)

- Matches, where part of the pattern is already known
  
  \[
  \text{match } c \ e_1 \ldots \ e_n \text{ with } \ldots c \ x_1 \ldots x_n \Rightarrow e \\
  > \text{let } x_1=e_1; \ldots; x_n=e_n \text{ in } e
  \]

- Let-reduction
  
  \[
  \text{let } x=e_1 \text{ in } e \rightarrow e[x\mapsto e_1]
  \]
Substitution

• Beware of name-capture

```plaintext
let x = 1 in
let f = fn y. x+y in
let x = 4 in
  f x
```
Substitution

• Beware of name-capture

```plaintext
let x = 1 in
let f = fn y. x+y in
let x = 4 in
  f x
```

• Consider reduction of $f = \ldots$.
Substitution

- Beware of name-capture

```latex
let x = 1 in
let f = fn y. x+y in
let x = 4 in
  f x
```

- Consider reduction of $f = \ldots$

- $\alpha$-conversion: (Consistent) renaming of (bound) variables does not change meaning of program
Substitution

- Beware of name-capture

```nutrition
let x = 1 in
let f = fn y. x+y in
let x = 4 in
  f x
```

- Consider reduction of $f = \ldots$

- $\alpha$-conversion: (Consistent) renaming of (bound) variables does not change meaning of program

- Convention: Substitution uses $\alpha$-conversion to avoid name-capture
Substitution

- Beware of name-capture

```hs
let x = 1 in
let f = fn y. x+y in
let x = 4 in
  f x
```

- Consider reduction of \( f = \ldots \),

- \( \alpha \)-conversion: (Consistent) renaming of (bound) variables does not change meaning of program

- Convention: Substitution uses \( \alpha \)-conversion to avoid name-capture
  
  - Here: Convert `let x=4 in f x` to `let x_1=4 in f x_1`
Termination issues

- Let-reduction may change semantics

```ocaml
let rec f = fn x. 1 + f x in
let _ = f 0 in
  42
```

- This program does not terminate
- But, applying let-reduction, we get
  ```ocaml
  let rec f = fn x. 1 + f x in
  42
  ```
- For eager evaluation, non-terminating programs may be transformed to terminating ones
- For lazy evaluation, semantics is preserved
Termination issues

• Let-reduction *may* change semantics

```plaintext
let rec f = fn x. 1 + f x in
let _ = f 0 in
42
```

• This program does not terminate
Termination issues

- Let-reduction may change semantics

```ocaml
let rec f = fn x. 1 + f x in
let _ = f 0 in
42
```

- This program does not terminate
- But, applying let-reduction, we get

```ocaml
let rec f = fn x. 1 + f x in
42
```
Termination issues

- Let-reduction may change semantics

```plaintext
let rec f = fn x. 1 + f x in
let _ = f 0 in
42
```

- This program does not terminate
- But, applying let-reduction, we get

```plaintext
let rec f = fn x. 1 + f x in
42
```

- which returns 42
Termination issues

- Let-reduction may change semantics

```ocaml
let rec f = fn x. 1 + f x in
let _ = f 0 in
42
```

- This program does not terminate
- But, applying let-reduction, we get

```ocaml
let rec f = fn x. 1 + f x in
 42
```

- which returns 42

- For eager evaluation, non-terminating programs may be transformed to terminating ones
Termination issues

- Let-reduction may change semantics

```plaintext
let rec f = fn x. 1 + f x in
let _ = f 0 in
42
```

- This program does not terminate
- But, applying let-reduction, we get

```plaintext
let rec f = fn x. 1 + f x in
42
```

- which returns 42

- For eager evaluation, non-terminating programs may be transformed to terminating ones
- For lazy evaluation, semantics is preserved
Side-effects

- Languages like SML/OCaml/F# have side-effects
Side-effects

- Languages like SML/OCaml/F# have side-effects
- Side-effecting expressions must not be let-reduced

```ocaml
let _ = print "Hello"
in ()
```
Application of let-reduction

- May make program less efficient

```plaintext
let x = \expensive-op in x + x
```

- May blow up program code exponentially

```plaintext
let x = x + x in let x = x + x in ... in x
```

- Heuristics for application: reduce

  - if \( x_1 \) is a variable (or constant)
  - if \( x_1 \) does not occur in \( e \)
  - if \( x_1 \) occurs exactly once in \( e \)
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    
    ```
    let x = expensive-op in x + x
    ```
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    \[
    \text{let } x = \text{expensive-op in } x + x
    \]
- May blow up program code exponentially
  \[
  \text{let } x = x + x \text{ in let } x = x + x \text{ in } \ldots \text{ in } x
  \]
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    \[
    \text{let } x = \text{expensive-op in } x+x
    \]
- May blow up program code exponentially
  \[
  \text{let } x = x+x \text{ in let } x = x+x \text{ in ... in } x
  \]
- Heuristics for application: reduce
  \[
  \text{let } x_1 = e_1 \text{ in } e
  \]
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    \[
    \text{let } x = \text{expensive-op in } x+x
    \]
- May blow up program code exponentially
  \[
  \text{let } x = x+x \text{ in let } x = x+x \text{ in } \ldots \text{ in } x
  \]
- Heuristics for application: reduce \[
  \text{let } x_1 = e_1 \text{ in } e
  \]
  - if \( e_1 \) is a variable (or constant)
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    \[
    \text{let } x = \text{expensive-op in } x+x
    \]

- May blow up program code exponentially
  \[
  \text{let } x = x+x \text{ in let } x = x+x \text{ in } \ldots \text{ in } x
  \]

- Heuristics for application: reduce \[
  \text{let } x_1 = e_1 \text{ in } e
  \]
  - if \( e_1 \) is a variable (or constant)
  - if \( x_1 \) does not occur in \( e \)
Application of let-reduction

- May make program less efficient
  - Re-computing values instead of storing them in variable
    \[
    \text{let } x = \text{expensive-op} \text{ in } x + x
    \]
- May blow up program code exponentially
  \[
  \text{let } x = x + x \text{ in let } x = x + x \text{ in } \ldots \text{ in } x
  \]
- Heuristics for application: reduce \[
\text{let } x_1 = e_1 \text{ in } e
\]
  - if \( e_1 \) is a variable (or constant)
  - if \( x_1 \) does not occur in \( e \)
  - if \( x_1 \) occurs exactly once in \( e \)
More transformations

- Valid for programs (fragments) with no side-effects

\[(\text{let } x = e \text{ in } e_1) \ e_2 \rightarrow \text{let } x = e \text{ in } e_1 \ e_2\]

// Renaming x to avoid name capture

let \( x_1 = e_1 \) in let \( x_2 = e_2 \) in e

\rightarrow \text{let } x_2 = e_2 \text{ in let } x_1 = e_1 \text{ in } e

// If \( x_1 \) not free in \( e_2 \)

// Renaming \( x_2 \) to avoid name capture

let \( x_1 = (\text{let } x_2 = e_2 \text{ in } e_1) \) in e

\rightarrow \text{let } x_2 = e_2 \text{ in let } x_1 = e_1 \text{ in } e

// Renaming \( x_2 \) to avoid name capture
More transformations

- Valid for programs (fragments) with no side-effects

\[
\text{(let } x = e \text{ in } e_1) \ e_2 \rightarrow \text{let } x = e \text{ in } e_1 \ e_2 \\
\quad // \text{ Renaming } x \text{ to avoid name capture}
\]

\[
\text{let } x_1 = e_1 \text{ in let } x_2 = e_2 \text{ in } e \\
\rightarrow \text{let } x_2 = e_2 \text{ in let } x_1 = e_1 \text{ in } e \\
\quad // \text{ If } x_1 \text{ not free in } e_2 \\
\quad // \text{ Renaming } x_2 \text{ to avoid name capture}
\]

\[
\text{let } x_1 = (\text{let } x_2 = e_2 \text{ in } e_1) \text{ in } e \\
\rightarrow \text{let } x_2 = e_2 \text{ in let } x_1 = e_1 \text{ in } e \\
\quad // \text{ Renaming } x_2 \text{ to avoid name capture}
\]

- May open potential for other optimizations
Inlining

- Consider program \[\text{let } f = \text{fn } x. \text{ e}_1 \text{ in } e\]
Inlining

- Consider program \( \text{let } f = \text{fn } x. \ e_1 \text{ in } e \)
- Inside \( e \), replace \( f \ e_2 \) by \( \text{let } x = e_2 \text{ in } e_1 \)

Goal: Save overhead for function call

Warning: May blow up the code
Inlining

- Consider program \( \text{let } f = \text{fn } x. \ e_1 \text{in } e \)
- Inside \( e \), replace \( f \ e_2 \) by \( \text{let } x = e_2 \text{in } e_1 \)
  - Goal: Save overhead for function call
Inlining

- Consider program \( \text{let } f=fn \ x. \ e_1 \text{ in } e \)
- Inside \( e \), replace \( f \ e_2 \) by \( \text{let } x=e_2 \text{ in } e_1 \)
  - Goal: Save overhead for function call
  - Warning: May blow up the code
Example

let fmax = fn f. fn x. fn y.
    if x>y then f x else f y in
let max = fmax (fn x. x) in
...
Example

let fmax = fn f. fn x. fn y.
  if x>y then f x else f y in
let max = (let f = (fn x. x) in
  fn x. fn y. if x>y then f x else f y) in
...

(inlined fmax)
Example

let fmax = fn f. fn x. fn y.
    if x>y then f x else f y in
let max = (let f = (fn x. x) in
    fn x. fn y. if x>y then let x=x in x else let x=y in x) in
  ...

(inlined f)
Example

let fmax = fn f. fn x. fn y.
    if x>y then f x else f y in
let max = (fn x. fn y. if x>y then x else y) in
...

(Let-reduction for single-var expressions and unused variables)
Note

- Inlining can be seen as special case of let-reduction
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form $\text{fn } x. \ e$, which are not evaluated, unless applied to an argument
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form fn x. e, which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form \( \text{fn } x. \ e \), which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate

```
let w = fn f. fn y. f (y f y) in
let fix = fn f. w f w
```
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form \( \text{fn } x. \ e \), which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate

```plaintext
let w = fn f. fn y. f (y f y) in
let fix = fn f. let f=f in let y=w in f (y f y)
(Inlined w)
```
Note

- Inlining can be seen as a special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form `fn x. e`, which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate

```ocaml
let w = fn f. fn y. f (y f y) in
let fix = fn f. f (w f w)
```

((Safe) let-reduction (copy variables))
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form `fn x. e`, which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate

```plaintext
let w = fn f. fn y. f (y f y) in
let fix = fn f. f (f (f (... f (w f w))))
(...)
```
Note

- Inlining can be seen as special case of let-reduction
- However: Does not change termination behavior or side-effects
  - Only inlining terms of form $\text{fn} \ x. \ e$, which are not evaluated, unless applied to an argument
- In untyped languages (e.g., LISP), the inlining optimization may not terminate
- In typed languages like OCaml or Haskell, however, we have
  - Inlining always terminates
Specialization of recursive functions

- Function to square all elements of a list
- Note: Dropping the restriction that let-rec occurs outermost

```ocaml
let rec map = fn f. fn l.
    match l with
    [] => []
    | x#l => f x # map f l
in
let f = fn x. x*x in
let sqrl = map f in ...
```
Specialization of recursive functions

- Function to square all elements of a list
  - Note: Dropping the restriction that let-rec occurs outermost
- Requires many function calls to $f$

```
let rec map = fn f. fn l.
  match l with
  [] => []
  | x#l => f x # map f l
in
let f = fn x. x*x in
let sqrl = map f in ...
```
Specialization of recursive functions

- Function to square all elements of a list
  - Note: Dropping the restriction that let-rec occurs outermost
- Requires many function calls to \( f \)
- Idea: Replace \texttt{map} \( f \) by new function \texttt{mapf}

```ml
let rec map = fn f. fn l.
    match l with
    | [] => []
    | x#l => f x # map f l
in
let f = fn x. x*x in
let sqrl = map f in ...
```
Specialization of recursive functions

- Function to square all elements of a list
  - Note: Dropping the restriction that let-rec occurs outermost
- Requires many function calls to $f$
- Idea: Replace $\text{map } f$ by new function $\text{map}_f$
- Specialization of $\text{map}$ for argument $f$

```ml
let rec map = fn f. fn l.
    match l with
    [] => []
  | x#l => f x # map f l

let f = fn x. x*x in
let sqrl = map f in ...
```
Specialization of recursive functions

- Function to square all elements of a list
  - Note: Dropping the restriction that let-rec occurs outermost
- Requires many function calls to $f$
- Idea: Replace $\text{map } f$ by new function $\text{mapf}$
- Specialization of $\text{map}$ for argument $f$

```
let rec map = fn f. fn l.
  match l with
  | [] => []
  | x#l => f x # map f l
in
let f = fn x. x*x in
let rec mapf = fn l.
  match l with
  | [] => []
  | x#l => f x # mapf l
in
let sqrl = mapf in ...
```

(Specialization)
Specialization of recursive functions

- Function to square all elements of a list
  - Note: Dropping the restriction that let-rec occurs outermost
- Requires many function calls to $f$
- Idea: Replace $\text{map } f$ by new function $\text{mapf}$
- Specialization of $\text{map}$ for argument $f$

```ml
let rec map = fn f. fn l.
    match l with
    [ ] => [ ]
    | x#l => f x # map f l
in
let f = fn x. x*x in
let rec mapf = fn l.
    match l with
    [ ] => [ ]
    | x#l => x*x # mapf l
in
let sqrl = mapf in ...
```

(Inlining)
Function folding

- When specializing function $f \ a$ to $fa$,
Function folding

- When specializing function \( f \ a \) to \( f a \),
  - we may replace \( f \ a \) by \( f a \) in definition of \( fa \)
Function folding

- When specializing function $f \ a$ to $fa$,
  - we may replace $f \ a$ by $fa$ in definition of $fa$
  - Beware of name-captures!
Function folding

- When specializing function \( f \) to \( f_a \),
  - we may replace \( f \) by \( f_a \) in definition of \( f_a \)
  - Beware of name-captures!
- If recursive function calls alter the specialized argument:
Function folding

- When specializing function \( f \) to \( f_a \),
  - we may replace \( f \) \( a \) by \( f_a \) in definition of \( f_a \)
  - Beware of name-captures!
- If recursive function calls alter the specialized argument:
  - Potential for new specializations may be created
Function folding

- When specializing function \( f \ a \) to \( f a \),
  - we may replace \( f \ a \) by \( f a \) in definition of \( fa \)
  - Beware of name-captures!
- If recursive function calls alter the specialized argument:
  - Potential for new specializations may be created
  - Infinitely often ...
Function folding

• When specializing function \( f \) a to \( f_a \),
  • we may replace \( f \) a by \( f_a \) in definition of \( f_a \)
  • Beware of name-captures!

• If recursive function calls alter the specialized argument:
  • Potential for new specializations may be created
  • Infinitely often ...
  • \( \text{let rec } f = \text{fn } g. \text{fn } l. \ldots f (\text{fn } x. g (g x)) \ldots \)
Function folding

- When specializing function \( f \ a \) to \( f a \),
  - we may replace \( f \ a \) by \( f a \) in definition of \( f a \)
  - Beware of name-captures!

- If recursive function calls alter the specialized argument:
  - Potential for new specializations may be created
  - Infinitely often ...
  - \( \text{let rec } f = \text{fn } g. \text{ fn } l. \ldots f (f \text{n } x. g (g x)) \ldots \)

- Safe and simple heuristics:
Function folding

- When specializing function \( f \ a \) to \( fa \),
  - we may replace \( f \ a \) by \( fa \) in definition of \( fa \)
  - Beware of name-captures!

- If recursive function calls alter the specialized argument:
  - Potential for new specializations may be created
  - Infinitely often ...
  - \( \text{let rec } f = \text{fn } g. \text{fn } l. \ldots f (\text{fn } x. g (g x)) \ldots \)

- Safe and simple heuristics:
  - Only specialize functions of the form
    
    \[
    \text{let rec } f = \text{fn } x. e
    \]

    such that recursive occurrences of \( f \) in \( e \) have the form \( f \ x \)
Deforestation

• Idea: Often, lists are used as intermediate data structures
Deforestation

- Idea: Often, lists are used as intermediate data structures
- Standard list functions

```ocaml
let rec map = fn f. fn l. match l with
  | [] => []
  | x#xs => f x # map f xs

let rec filter = fn P. fn l. match l with
  | [] => []
  | x#xs => if P x then x#filter P xs else filter P xs

let rec foldl = fn f. fn a. fn l. match l with
  | [] => []
  | x#xs => foldl f (f a x) xs
```
Deforestation

- Examples of derived functions

```haskell
let sum = foldl (+) 0

let length = sum o map (fn x. 1)

let der = fn l.
  let n = length l in
  let mean = sum l / n in
  let s2 = (sum
    o map (fn x. x*x)
    o map (fn x. x-mean)) l
  in
  s2 / n
```
Idea

- Avoid intermediate list structures
Idea

- Avoid intermediate list structures
- E.g., we could define

\[
\text{length} = \text{foldl} \ (\text{fn} \ a. \ \text{fn} \ _. \ a+1) \ 0
\]
Idea

- Avoid intermediate list structures
- E.g., we could define
  
  \[
  \text{length} = \text{foldl} \ (\text{fn} \ a. \ \text{fn} \ _._. \ a+1) \ 0
  \]

- In general, we can define rules for combinations of the basic list functions like fold, map, filter, ...

  \[
  \text{map} \ f \circ \text{map} \ g = \text{map} \ (f \circ g)
  \]
  \[
  \text{foldl} \ f \ a \circ \text{map} \ g = \text{foldl} \ (\text{fn} \ a. \ f \ a \circ g) \ a
  \]
  \[
  \text{filter} \ P \circ \text{filter} \ Q = \text{filter} \ (\text{fn} \ x. \ P \ x \ & \ Q \ x)
  \]
  
  ...
Idea

- Avoid intermediate list structures
- E.g., we could define
  \[
  \text{length} = \text{foldl} \ (\text{fn} \ a. \ \text{fn} \ _._. \ a+1) \ 0
  \]
- In general, we can define rules for combinations of the basic list functions like fold, map, filter, ...
  \[
  \text{map} \ f \ o \ \text{map} \ g = \text{map} \ (f \ o \ g) \\
  \text{foldl} \ f \ a \ o \ \text{map} \ g = \text{foldl} \ (\text{fn} \ a. \ f \ a \ o \ g) \ a \\
  \text{filter} \ P \ o \ \text{filter} \ Q = \text{filter} \ (\text{fn} \ x. \ P \ x \ & \ Q \ x)
  \]
  ...
- We may also need versions of these rules in first-order form, e.g.
  \[
  \text{map} \ f \ (\text{map} \ g \ l) = ...
  \]
Example

let der = fn l.
    let n = length l in
    let mean = sum l / n in
    let s2 = (sum
        o map (fn x. x*x)
        o map (fn x. x-mean)) l
    in
    s2 / n
Example

let der = fn l.
    let n = length l in
let mean = sum l / length l in
    let s2 = (foldl (+) 0
            o map (fn x. x*x)
            o map (fn x. x-mean)) l
    in
    s2 / n

Let-optimization/ inlining
Example

```
let der = fn l.
    let n = length l in
    let mean = sum l / length l in
    let s2 = (foldl (+) 0
       o map ((fn x. x*x) o (fn x. x-mean))) l
    in
    s2 / n

map-map rule
```
Example

let der = fn l.
    let n = length l in
    let mean = sum l / length l in
    let s2 = foldl (fn a. (+) a o (fn x. x*x) o (fn x. x-mean)) 0 l
    in
    s2 / n

fold-map rule
let der = fn l.
    let n = length l in
let mean = sum l / length l in
let s2 = foldl (fn a. fn x. let x=x-mean in let x=x*x in a+x ) 0 l
in
    s2 / n

function-application, unfolding of o, let-optimization.
Discussion

- Beware of side-effects!
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
  - Does not scale
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
  - Does not scale
- Only works for built-in functions
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
  - Does not scale
- Only works for built-in functions
  - Could try to automatically recognize user-defined functions
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
  - Does not scale
- Only works for built-in functions
  - Could try to automatically recognize user-defined functions
- Can be extended to algebraic datatypes in general
Discussion

- Beware of side-effects!
- Need rules for many combinations of functions.
  - Does not scale
- Only works for built-in functions
  - Could try to automatically recognize user-defined functions
- Can be extended to algebraic datatypes in general
  - They all have standard map and fold functions
Reducing the number of required rules

- Try to find standard representation

  \[
  \text{foldr} \ f \ a \ [] = a \\
  \text{foldr} \ f \ a \ (x \#xs) = f \ x \ (\text{foldr} \ f \ a \ xs)
  \]

  We can represent \text{map}, \text{filter}, \text{sum}, ... 

  But no list-reversal, as \text{foldl} can

  Problem: How to compose two foldr-calls?

  \[
  \text{foldr} \ f_1 \ a_1 \ (\text{foldr} \ f_2 \ a_2 \ l) = ???
  \]
Reducing the number of required rules

- Try to find standard representation
- `foldr` seems to be a good candidate:

\[
\begin{align*}
\text{foldr } f \ a \ [] &= a \\
\text{foldr } f \ a \ (x\#xs) &= f \ x \ (\text{foldr } f \ a \ xs)
\end{align*}
\]
Reducing the number of required rules

- Try to find standard representation
- `foldr` seems to be a good candidate:
  
  ```
  foldr \ f \ a \ [] = a \\
  foldr \ f \ a \ (x#xs) = f \ x \ (foldr \ f \ a \ xs)
  ```

- We can represent `map`, `filter`, `sum`, ...
Reducing the number of required rules

- Try to find standard representation
- `foldr` seems to be a good candidate:
  \[
  \text{foldr } f \ a \ [ ] = a \\
  \text{foldr } f \ a \ (x\#xs) = f \ x \ (\text{foldr } f \ a \ xs)
  \]
- We can represent `map`, `filter`, `sum`, ...
  - But no list-reversal, as `foldl` can
Reducing the number of required rules

- Try to find standard representation
- \texttt{foldr} seems to be a good candidate:

  \[
  \text{foldr } f \ a \ [\ ] = a \\
  \text{foldr } f \ a \ (x # x: s) = f \ x \ (\text{foldr } f \ a \ x: s)
  \]

- We can represent \textit{map}, \textit{filter}, \textit{sum}, ...
  - But no list-reversal, as \texttt{foldl} can
- Problem: How to compose two \texttt{foldr}-calls?
Reducing the number of required rules

- Try to find standard representation
- `foldr` seems to be a good candidate:
  
  \[
  \text{foldr } f \ a \ [] = a \\
  \text{foldr } f \ a \ (x#xs) = f \ x \ (\text{foldr } f \ a \ xs)
  \]

- We can represent `map`, `filter`, `sum`, ...
  - But no list-reversal, as `foldl` can

- Problem: How to compose two `foldr`-calls?
  - `foldr \ f1 \ a1 \ (foldr \ f2 \ a2 \ l) = ???`
Composition of \textit{foldr}

- Idea: Abstract over constructors

\[
\text{map } f \ l = \text{foldr} \ (\text{fn } l. \ \text{fn } x. \ f \ x \# l) \ [ ] \ l
\]

\[
\text{map' } f \ l = \text{fn } c. \ \text{fn } n. \\
\quad \text{foldr} \ (\text{fn } l. \ \text{fn } x. \ c \ (f \ x) \ l) \ n \ l
\]

\[
\text{build } g = g \ (\#) \ [ ]
\]

\[
\text{map } f \ l = \text{build} \ (\text{map' } f \ l)
\]
Composition of \textit{foldr}

- Idea: Abstract over constructors
  
  \[
  \text{map } f \text{ } l = \text{foldr } (\text{fn } l. \text{fn } x. \text{ } f \text{ } x#l) \text{ } [] \text{ } l
  \]

  \[
  \text{map}^{'} \text{ } f \text{ } l = \text{fn } c. \text{fn } n.
  \quad \text{foldr } (\text{fn } l. \text{fn } x. \text{ } c \text{ } (f \text{ } x) \text{ } l) \text{ } n \text{ } l
  \]

  \[
  \text{build } g = g \text{ } (\#) \text{ } []
  \]

  \[
  \text{map } f \text{ } l = \text{build } (\text{map}^{'} \text{ } f \text{ } l)
  \]

- Have
  
  \[
  \text{foldr } f \text{ } a \text{ } (\text{build } g) = g \text{ } f \text{ } a
  \]
Composition of \textit{foldr}

- Idea: Abstract over constructors

\[
\text{map } f \ l = \text{foldr (fn } l. \text{ fn } x. \ f \ x#l) \ [\] \ l
\]

\[
\text{map'} f \ l = \text{fn } c. \text{ fn } n. \\
\quad \text{foldr (fn } l. \text{ fn } x. \ c \ (f \ x) \ l) \ n \ l
\]

\[
\text{build } g = g \ (#) \ []
\]

\[
\text{map } f \ l = \text{build (map'} f \ l)
\]

- Have

\[
\text{foldr } f \ a \ (\text{build } g) = g \ f \ a
\]

- If abstraction over list inside \( g \) done properly
  - I.e., \( g \) actually produces list using its arguments
Example

```
map f (map g l)
```
Example

\[
\text{map } f \ (\text{map } g \ l) \\
= \text{build } (\text{map'} \ f \ (\text{build } (\text{map'} \ g \ l)))
\]
Example

map f (map g l)

= build (map' f (build (map' g l)))

= build (fn c. fn n.
    foldr (fn l. fn x. c (f x) l) n (build (map' g l)))
map f (map g l)

= build (map’ f (build (map’ g l)))

= build (fn c. fn n.
    foldr (fn l. fn x. c (f x) l) n (build (map’ g l)))

= build (fn c. fn n. map’ g l (fn l. fn x. c (f x) l) n)
Intuition

- Functions may consume lists ($\text{foldr}$), produce lists ($\text{build}$), or both
Intuition

- Functions may consume lists ($\text{foldr}$), produce lists ($\text{build}$), or both
- Applying a chain of functions: ($\text{build foldr}$) ($\text{build foldr}$) \ldots ($\text{build foldr}$)
• Functions may consume lists \((\text{foldr})\), produce lists \((\text{build})\), or both
• Applying a chain of functions: \((\text{build} \ \text{foldr}) \ (\text{build} \ \text{foldr}) \ \ldots \ (\text{build} \ \text{foldr})\)
• Can be re-bracketed to \(\text{build} \ (\text{foldr} \ \text{build}) \ \ldots \ (\text{foldr} \ \text{build}) \ \text{foldr}\)
Intuition

- Functions may consume lists \((foldr)\), produce lists \((build)\), or both
- Applying a chain of functions: \((build \ foldr) \ (build \ foldr) \ldots \ (build \ foldr)\)
- Can be re-bracketed to \(build \ (foldr \ build) \ldots \ (foldr \ build) \ foldr\)
- And the inner pairs cancel out, leaving a single \(build \ foldr\)
Discussion

- Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
Discussion

- **Single rule for deforestation:** \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  - Only correct if \( g \) is abstracted over list correctly
Discussion

- Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  - Only correct if \( g \) is abstracted over list correctly
  - Consider, e.g., \( \text{foldr } f \ a \ (\text{build } (\text{fn } _. \ \text{fn } _. \ [\text{True}])) \)
Discussion

- Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  - Only correct if \( g \) is abstracted over list correctly
  - Consider, e.g., \( \text{foldr } f \ a \ (\text{build } (\text{fn } _. \ \text{fn } _. \ \text{[True]})) \)
    - Which is, in general, not the same as \( (\text{fn } _. \ \text{fn } _. \ \text{[True]}) \ f \ a \)
Discussion

- Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  - Only correct if \( g \) is abstracted over list correctly
  - Consider, e.g., \( \text{foldr } f \ a \ (\text{build } (\text{fn } _. \ \text{fn } _. \ [\text{True}])) \)
    - Which is, in general, not the same as \( (\text{fn } _. \ \text{fn } _. \ [\text{True}]) \ f \ a \)
- If language is parametric, can be enforced via type:
Discussion

- Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  - Only correct if \( g \) is abstracted over list correctly
  - Consider, e.g., \( \text{foldr } f \ a \ (\text{build } (\text{fn } _. \ \text{fn } _. \ [\text{True}])) \)
    - Which is, in general, not the same as \( (\text{fn } _. \ \text{fn } _. \ [\text{True}]) \ f \ a \)
- If language is parametric, can be enforced via type:
  - If \( g \) has type \( \forall \beta.(A \rightarrow \beta \rightarrow \beta) \rightarrow \beta \rightarrow \beta \)
• Single rule for deforestation: \( \text{foldr } f \ a \ (\text{build } g) = g \ f \ a \)
  
  • Only correct if \( g \) is abstracted over list correctly
  
  • Consider, e.g., \( \text{foldr } f \ a \ (\text{build } (\text{fn } _. \ \text{fn } _. \ [\text{True}])) \)
    
    • Which is, in general, not the same as \( (\text{fn } _. \ \text{fn } _. \ [\text{True}]) f a \)

• If language is parametric, can be enforced via type:
  
  • If \( g \) has type \( \forall \beta.(A \rightarrow \beta \rightarrow \beta) \rightarrow \beta \rightarrow \beta \)
  
  • It can only produce its result of type \( \beta \) by using its arguments
• Single rule for deforestation:  \( \text{foldr} \ f \ a \ (\text{build} \ g) = g \ f \ a \)
  
  • Only correct if \( g \) is abstracted over list correctly
  
  • Consider, e.g.,  \( \text{foldr} \ f \ a \ (\text{build} \ (\text{fn} \ _ \ . \ \text{fn} \ _ \ . \ [\text{True}])) \)
    
    • Which is, in general, not the same as  \( (\text{fn} \ _ \ . \ \text{fn} \ _ \ . \ [\text{True}]) \ f \ a \)

• If language is parametric, can be enforced via type:
  
  • If \( g \) has type  \( \forall \beta. (A \rightarrow \beta \rightarrow \beta) \rightarrow \beta \rightarrow \beta \)
  
  • It can only produce its result of type \( \beta \) by using its arguments
  
  • Which is exactly the required abstraction over the list constructors
Wrap-up

- Transformations for functional programs

- Let-optimization
- Inlining
- Specialization
- Deforestation
...
Wrap-up

- Transformations for functional programs
  - Let-optimization

On (imperative) IR, all former optimizations of this lecture can be done.

Important one: Tail-call optimization

There are no loops in functional languages.
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation

Aim at reducing complexity before translation to IR

On (imperative) IR, all former optimizations of this lecture can be done

Important one: Tail-call optimization

There are no loops in functional languages
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation
  - ...

Aim at reducing complexity before translation to IR

On (imperative) IR, all former optimizations of this lecture can be done

Important one: Tail-call optimization

There are no loops in functional languages
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation
  - ...
- Aim at reducing complexity before translation to IR
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation
  - ...

- Aim at reducing complexity before translation to IR
- On (imperative) IR, all former optimizations of this lecture can be done
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation
  - ...

- Aim at reducing complexity before translation to IR

- On (imperative) IR, all former optimizations of this lecture can be done
  - Important one: Tail-call optimization
Wrap-up

- Transformations for functional programs
  - Let-optimization
  - Inlining
  - Specialization
  - Deforestation
  - ...

- Aim at reducing complexity before translation to IR
- On (imperative) IR, all former optimizations of this lecture can be done
  - Important one: Tail-call optimization
    - There are no loops in functional languages
That’s it!

Questions?