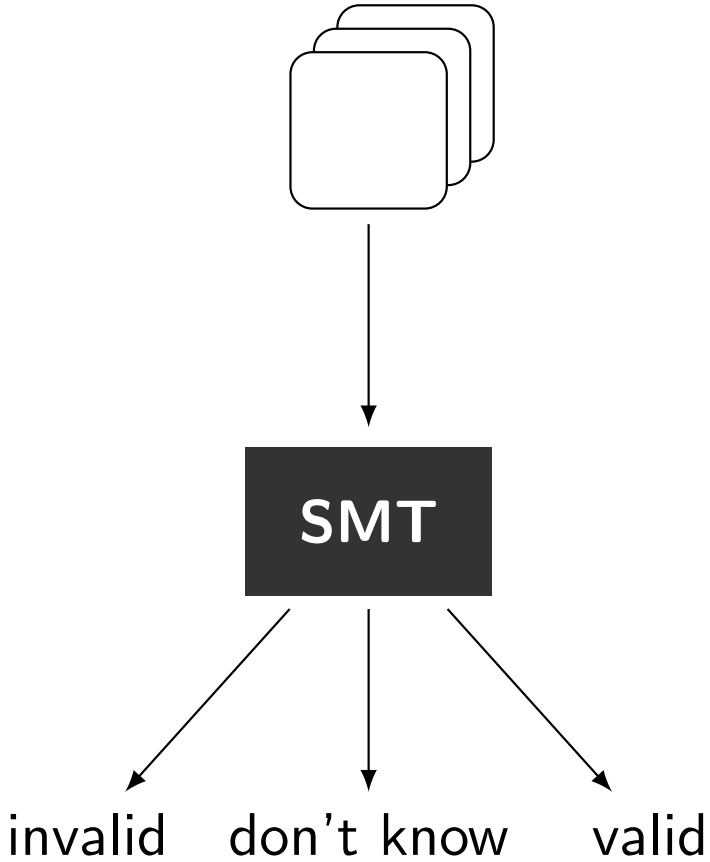
Efficient Proof Reconstruction for the SMT Solver Z3

Sascha Böhme

Technische Universität München

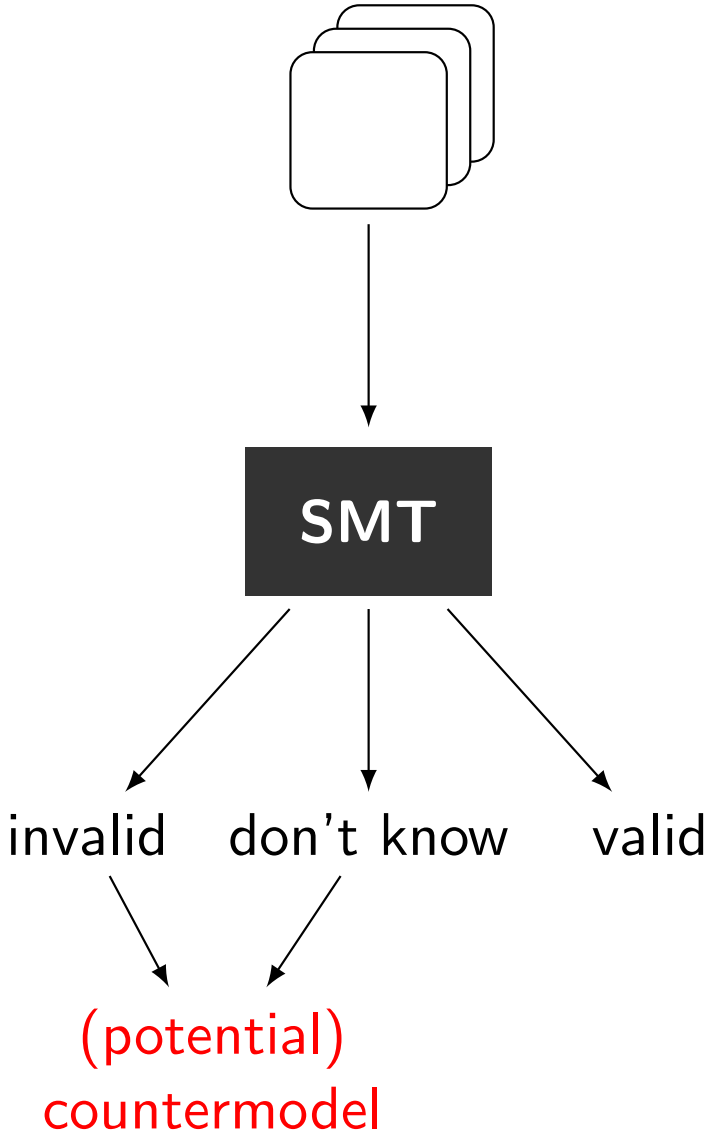
30. January 2010

Joint work with Tjark Weber (University of Cambridge)



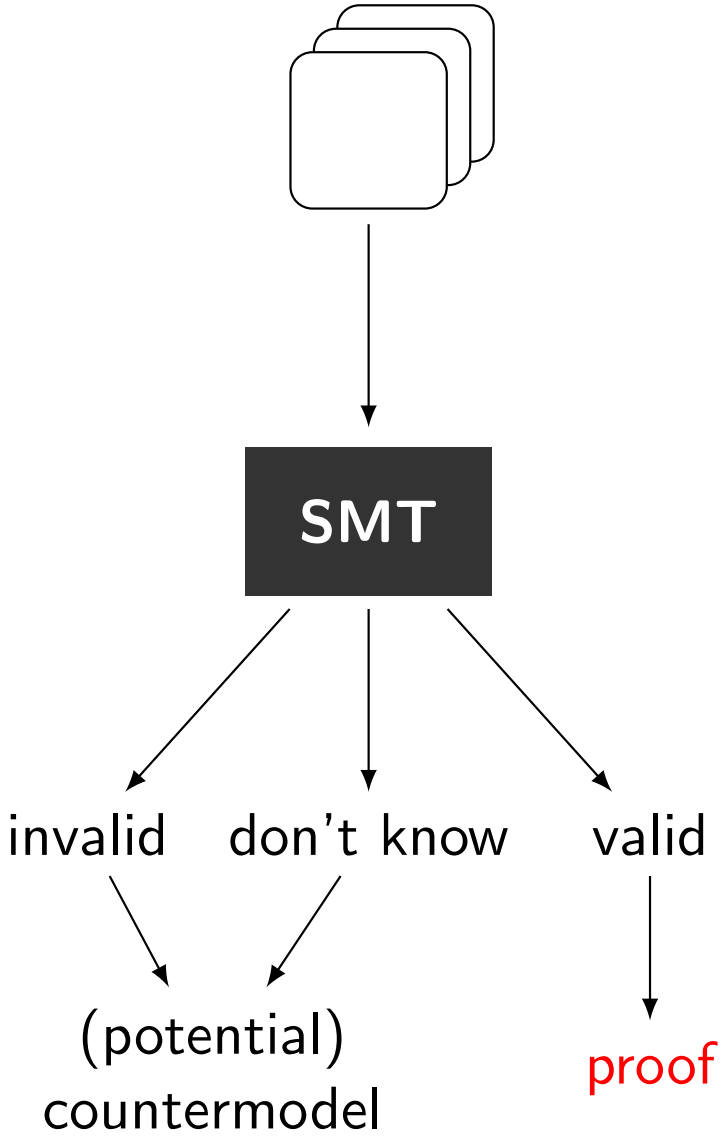
User perspective on SMT:

- "black-box" technology
- solvers contain bugs



User perspective on SMT:

- "black-box" technology
- solvers contain bugs

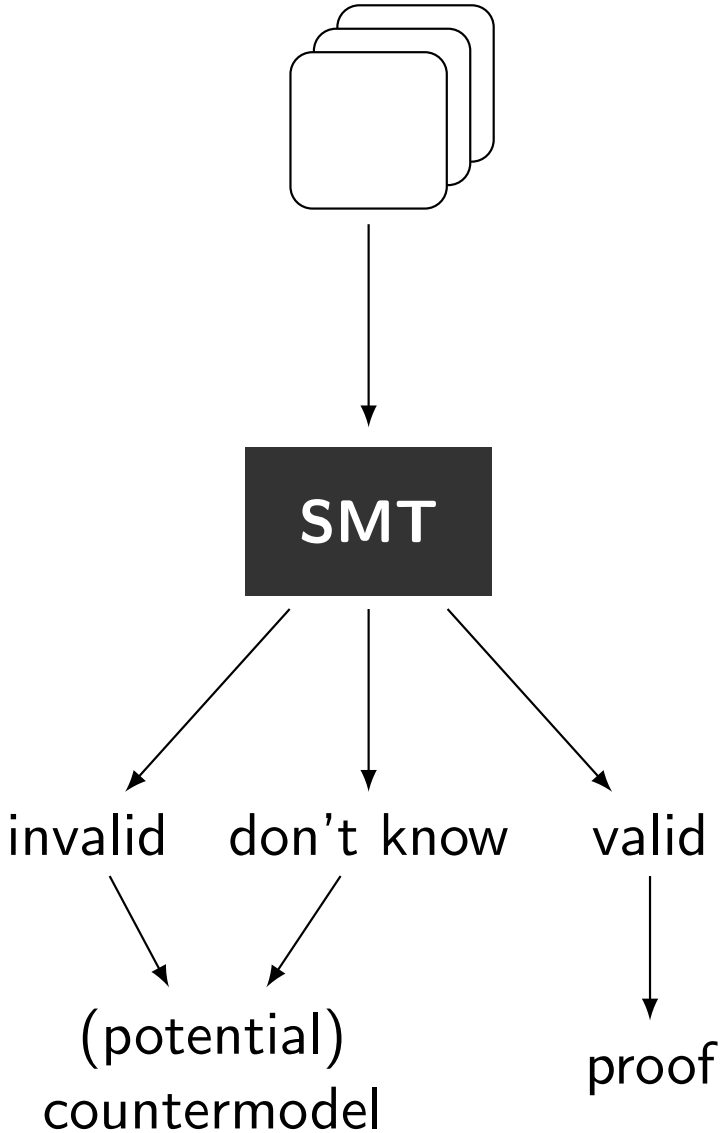


User perspective on SMT:

- "black-box" technology
- solvers contain bugs

Valid:

- checkable certificates
- increased confidence



User perspective on SMT:

- "black-box" technology
- solvers contain bugs

Valid:

- checkable certificates
- increased confidence

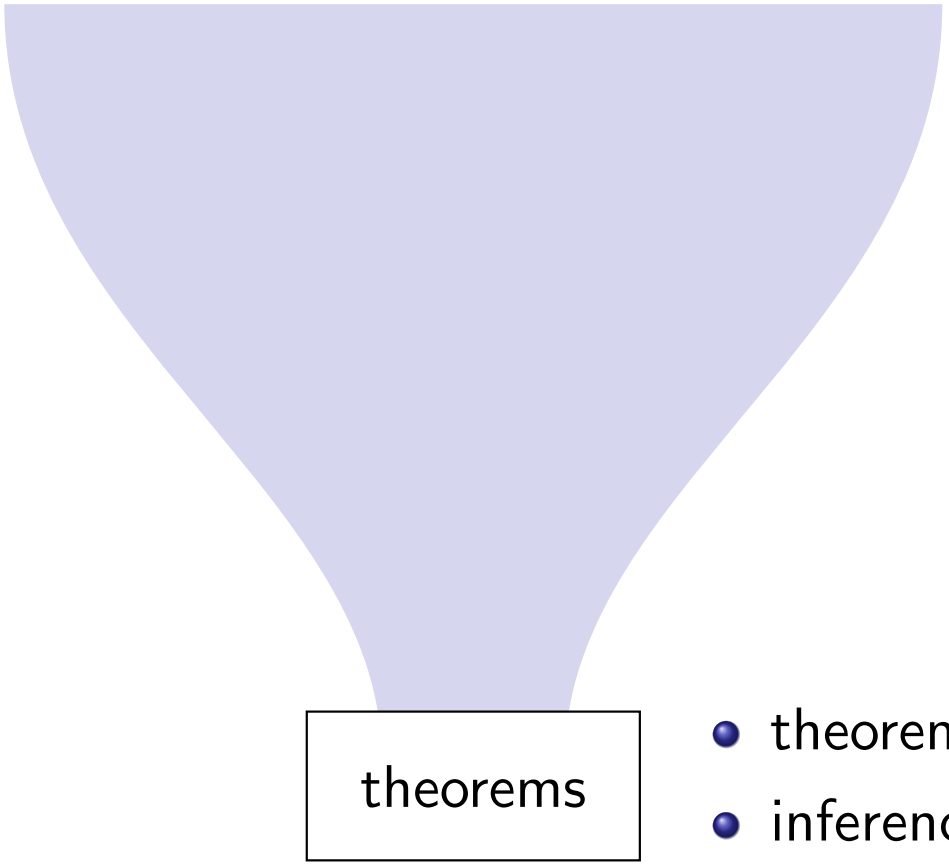
Our aim:

- reconstruct proofs of Z3
- in Isabelle/HOL

Isabelle/HOL

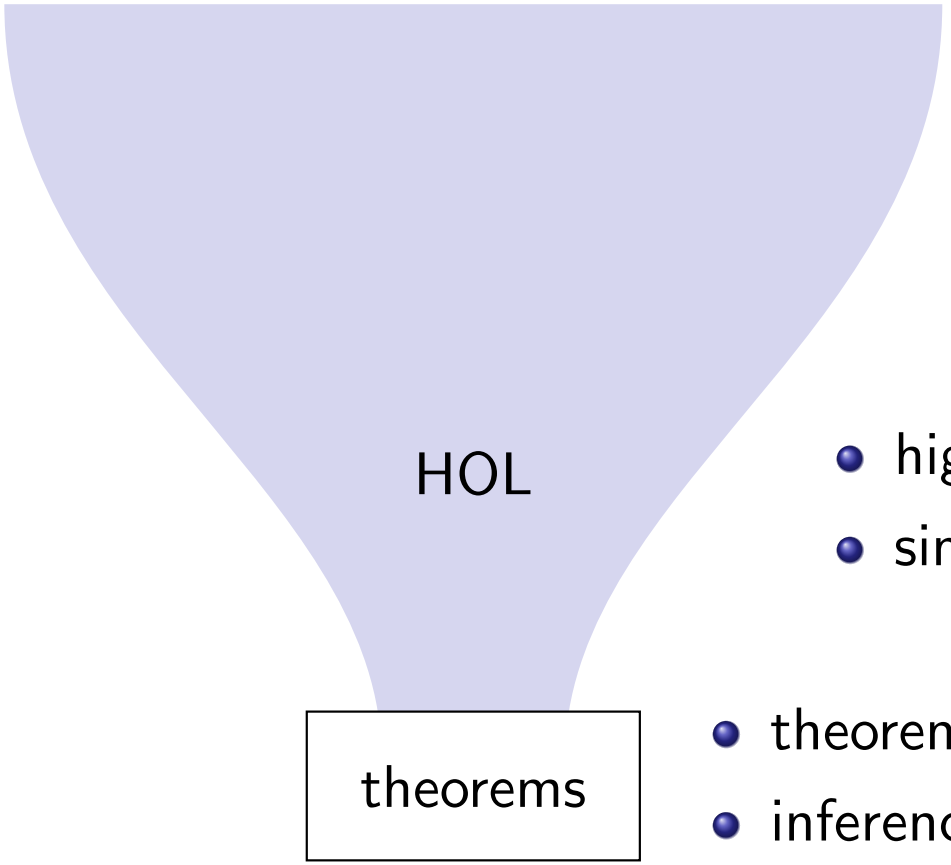
- theorems: abstract type
- inference rules: intuitionistic higher-order logic

Isabelle/HOL



- theorems: abstract type
- inference rules: intuitionistic higher-order logic

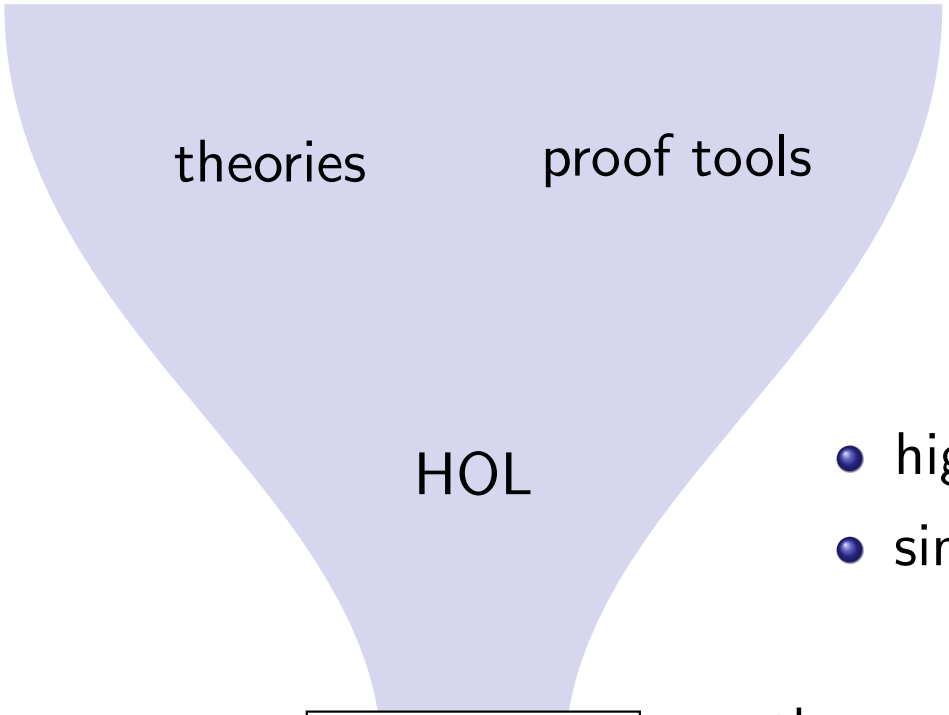
Isabelle/HOL



- higher-order logic
- simply-typed λ-calculus

- theorems: abstract type
- inference rules: intuitionistic higher-order logic

Isabelle/HOL



- term rewriting
- tableaux prover
- arithmetic

- higher-order logic
- simply-typed λ-calculus

- theorems: abstract type
- inference rules: intuitionistic higher-order logic

Z3's Language: Many-Sorted First-Order Logic

Many-sorted:

- *bool*, *int*, *real*
- user-defined sorts
- no polymorphism

Interpreted functions:

- propositional constants and operators
- $\wedge$ and $\vee$ are polyadic
- equality, *distinct*
- numbers and arithmetical operators

Quantifiers

Z3's Proofs

Natural deduction style:

Example

$$\dfrac{\dfrac{}{\neg true \vdash \neg true}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg true \leftrightarrow false}\ \textbf{rewrite}}{\neg true \vdash false}\ \textbf{mp}$$

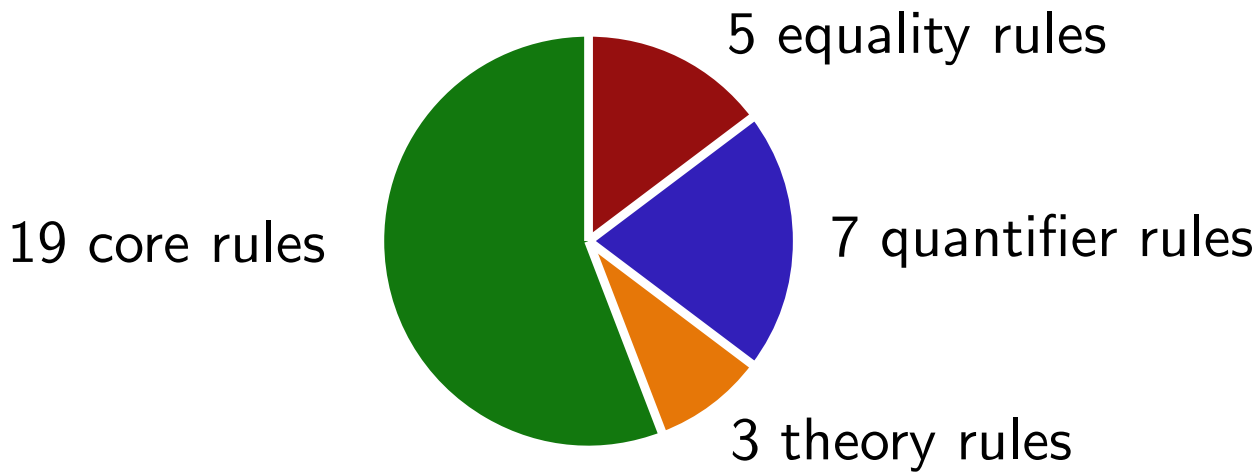
Z3's Proofs

Natural deduction style:

Example

$$\dfrac{\dfrac{}{\neg true \vdash \neg true}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg true \leftrightarrow false}\ \textbf{rewrite}}{\neg true \vdash false}\ \textbf{mp}$$

34 proof rules:



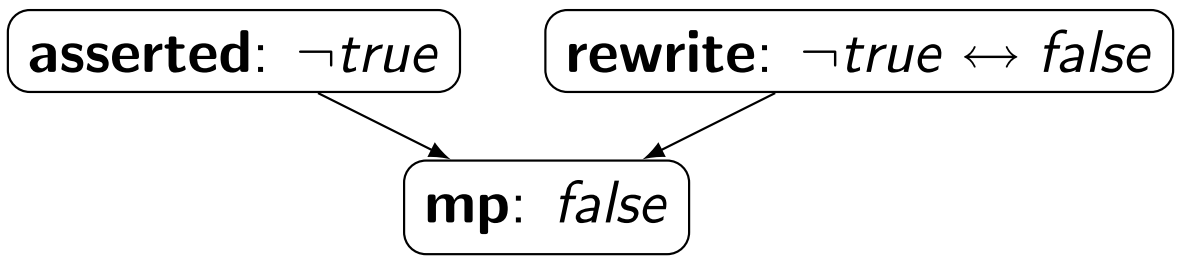
Z3's Proofs

Natural deduction style:

Example

$$\dfrac{\dfrac{}{\neg true \vdash \neg true}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg true \leftrightarrow false}\ \textbf{rewrite}}{\neg true \vdash false}\ \textbf{mp}$$

Graph structure:



Proof Reconstruction

$$\dfrac{\dfrac{}{\neg \mathit{true} \vdash \neg \mathit{true}}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg \mathit{true} \leftrightarrow \mathit{false}}\ \textbf{rewrite}}{\neg \mathit{true} \vdash \mathit{false}}\ \textbf{mp}$$

Proof Reconstruction

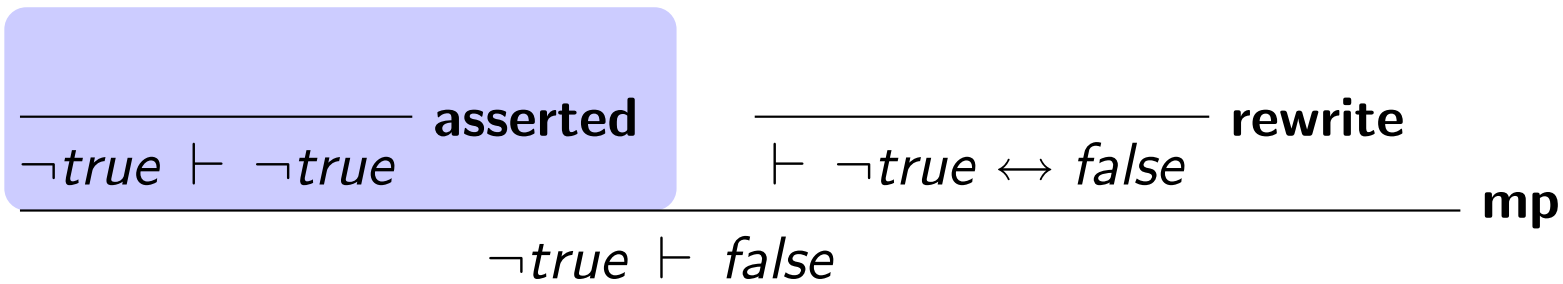
Follows the proof structure:

$$\dfrac{\dfrac{}{\neg \mathit{true} \vdash \neg \mathit{true}}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg \mathit{true} \leftrightarrow \mathit{false}}\ \textbf{rewrite}}{\neg \mathit{true} \vdash \mathit{false}}\ \textbf{mp}$$

Proof Reconstruction

Follows the proof structure:

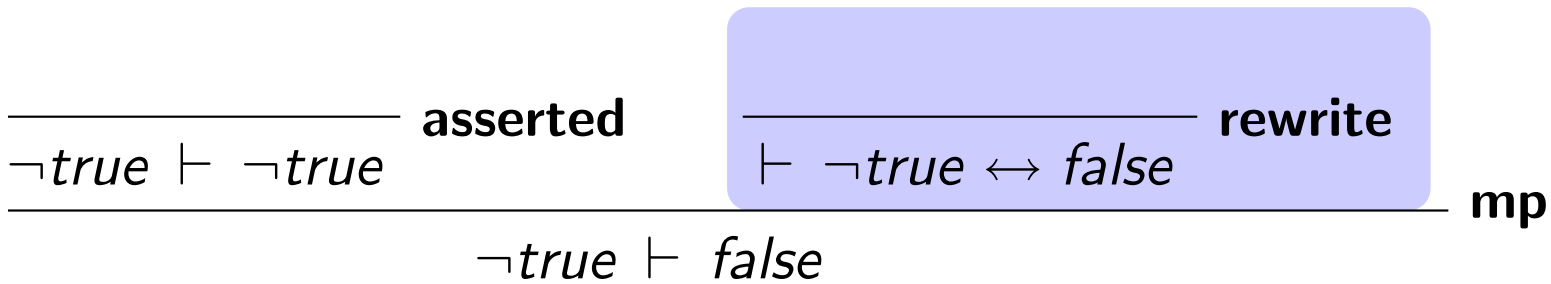
- depth-first, postorder
- one method for every rule



Proof Reconstruction

Follows the proof structure:

- depth-first, postorder
- one method for every rule



Proof Reconstruction

Follows the proof structure:

- depth-first, postorder
- one method for every rule

$$\dfrac{\dfrac{}{\neg \mathit{true} \vdash \neg \mathit{true}}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg \mathit{true} \leftrightarrow \mathit{false}}\ \textbf{rewrite}}{\neg \mathit{true} \vdash \mathit{false}}\ \textbf{mp}$$

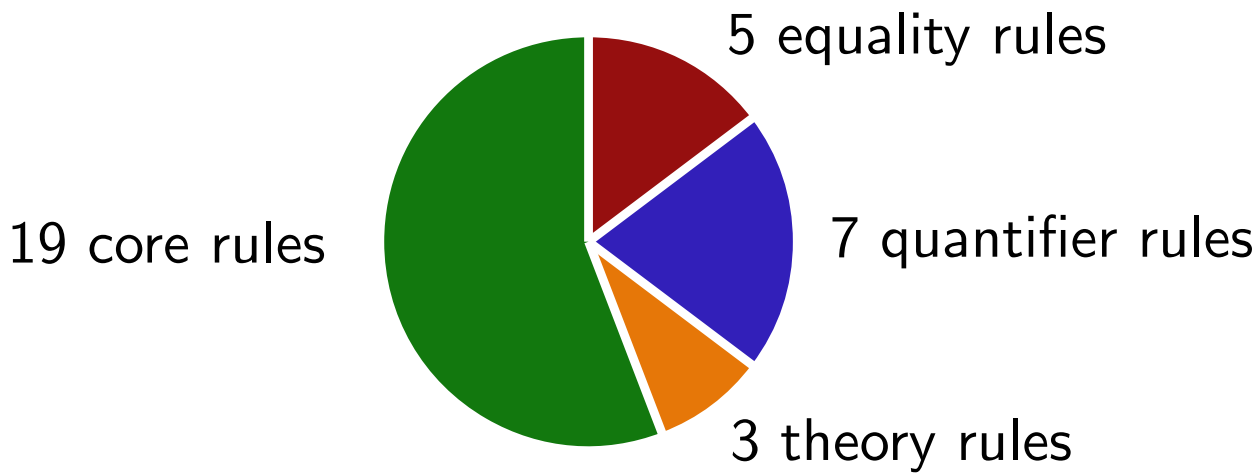
Proof Reconstruction

Follows the proof structure:

- depth-first, postorder
- one method for every rule
- all inferences certified by Isabelle kernel

$$\dfrac{\dfrac{}{\neg \mathit{true} \vdash \neg \mathit{true}}\ \textbf{asserted} \qquad \dfrac{}{\vdash \neg \mathit{true} \leftrightarrow \mathit{false}}\ \textbf{rewrite}}{\neg \mathit{true} \vdash \mathit{false}}\ \textbf{mp}$$

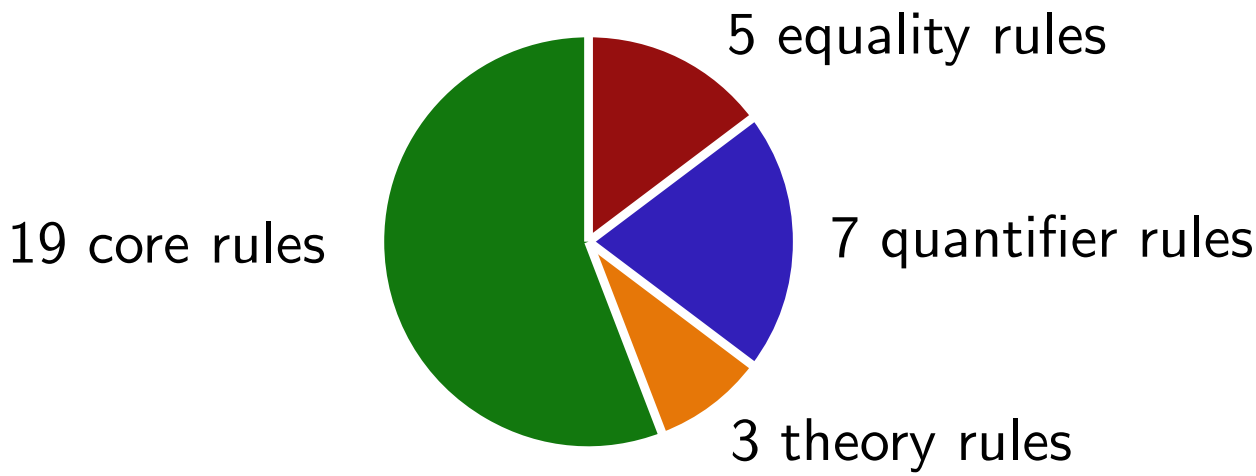
Proof Reconstruction Techniques



Proof Reconstruction Techniques

Example (*modus ponens*)

$$\frac{\neg true \qquad \neg true \leftrightarrow false}{false}\ \textbf{mp} \qquad\qquad P \Longrightarrow P \leftrightarrow Q \Longrightarrow Q$$

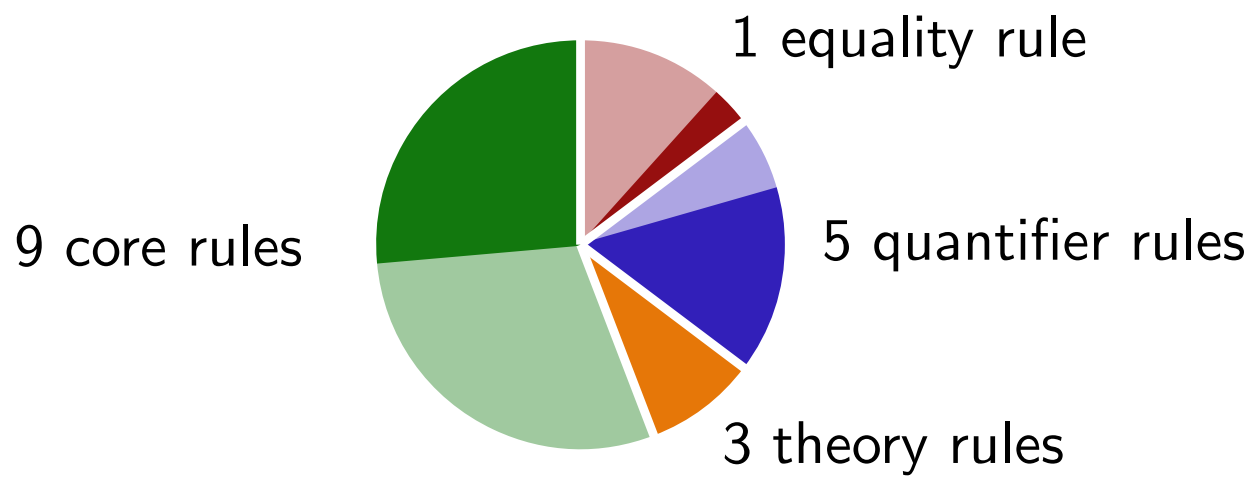


Proof Reconstruction Techniques

Example (*modus ponens*)

$$\frac{\neg true \qquad \neg true \leftrightarrow false}{false}\ \textbf{mp} \qquad\qquad P \Longrightarrow P \leftrightarrow Q \Longrightarrow Q$$

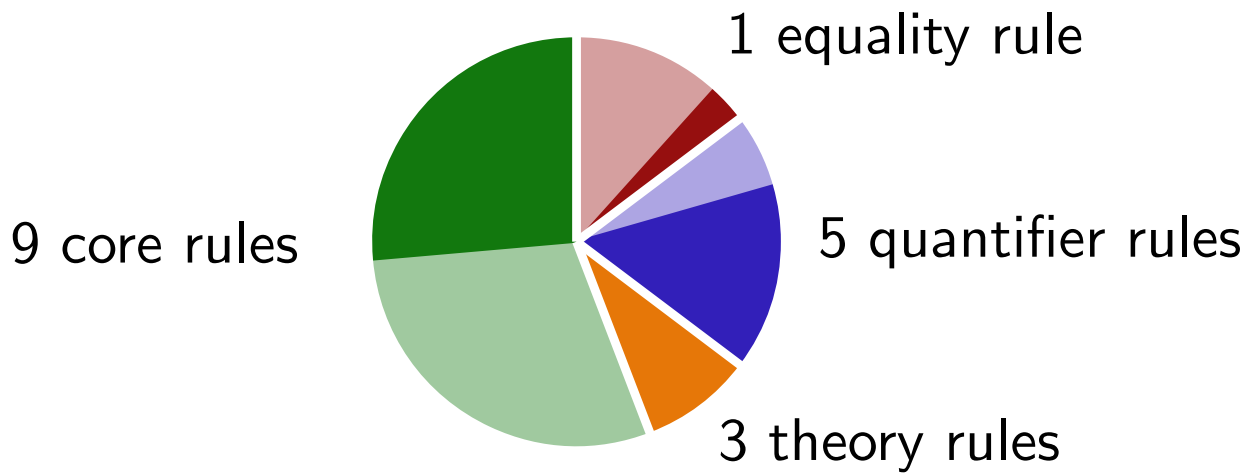
Schematic theorems, inference rules, combinations: 16 proof rules



Proof Reconstruction Techniques

Custom-made proof methods:

- straightforward or irrelevant for efficiency



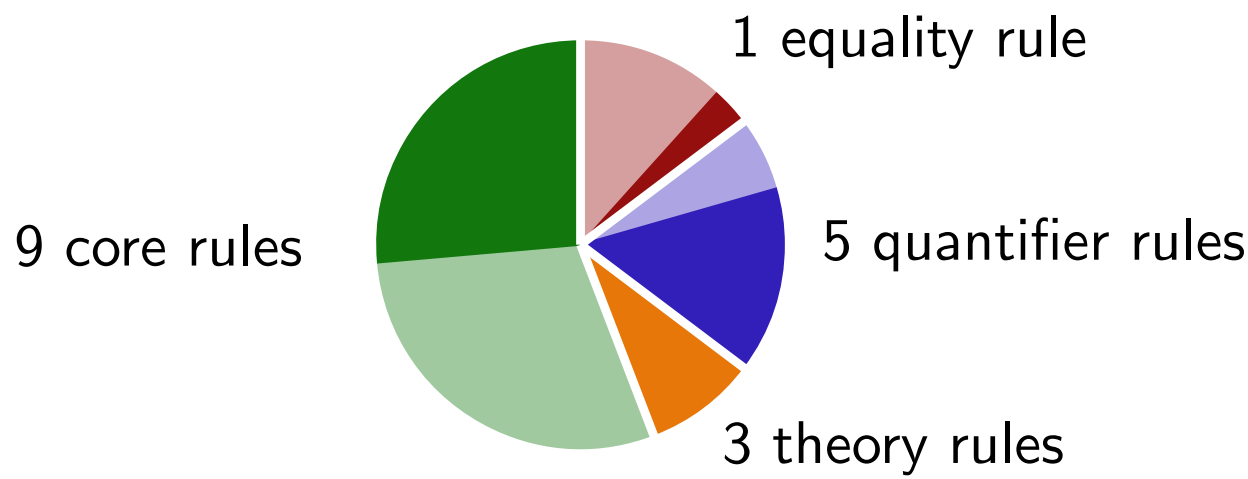
Proof Reconstruction Techniques

Custom-made proof methods:

- straightforward or irrelevant for efficiency

Automated proof tools of Isabelle:

- for rules occurring seldom or never



Proof Reconstruction Techniques

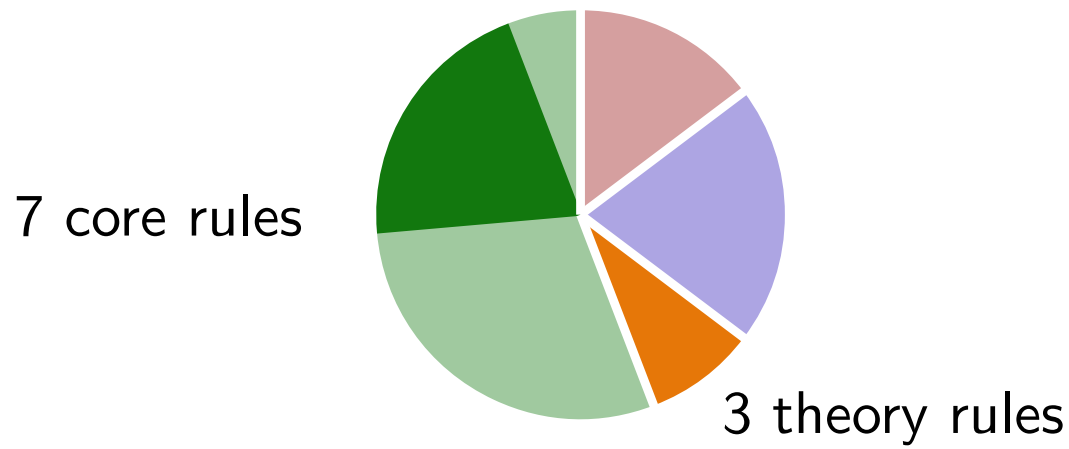
Custom-made proof methods:

- straightforward or irrelevant for efficiency

Automated proof tools of Isabelle:

- for rules occurring seldom or never

Altogether: 8 proof rules



Bottlenecks and Challenges

Huge formulas:

- generic automated proof tools easily get lost
- especially due to polyadic conjunction/disjunction and *distinct*

Rewriting:

- undocumented set of rules
- several different flavors
- propositional and theory-specific reasoning

Linerar arithmetic:

- conjunction of linear inequalities
- requires expensive proof search

Nested Conjunctions and Disjunctions

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_i}$$

Nested Conjunctions and Disjunctions

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_1} \quad \ldots \quad \frac{P_1 \wedge \ldots \wedge P_n}{P_n}$$

Nested Conjunctions and Disjunctions

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_1} \quad \ldots \quad \frac{P_1 \wedge \ldots \wedge P_n}{P_n}$$

$$\Downarrow$$

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_1 \quad \ldots \quad P_n}$$

Nested Conjunctions and Disjunctions

Explosion:

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_1 \quad \ldots \quad P_n} \qquad \frac{\neg(P_1 \vee \ldots \vee P_n)}{\neg P_1 \quad \ldots \quad \neg P_n}$$

$$P \wedge Q \Longrightarrow P \qquad \neg(P \vee Q) \Longrightarrow \neg P$$
$$P \wedge Q \Longrightarrow Q \qquad \neg(P \vee Q) \Longrightarrow \neg Q$$

Nested Conjunctions and Disjunctions

Explosion:

$$\frac{P_1 \wedge \ldots \wedge P_n}{P_1 \quad \ldots \quad P_n} \qquad \frac{\neg(P_1 \vee \ldots \vee P_n)}{\neg P_1 \quad \ldots \quad \neg P_n}$$

$$P \wedge Q \Longrightarrow P \qquad \neg(P \vee Q) \Longrightarrow \neg P$$
$$P \wedge Q \Longrightarrow Q \qquad \neg(P \vee Q) \Longrightarrow \neg Q$$

Join:

$$\frac{P_1 \quad \ldots \quad P_n}{P_1 \wedge \ldots \wedge P_n} \qquad \frac{\neg P_1 \quad \ldots \quad \neg P_n}{\neg(P_1 \vee \ldots \vee P_n)}$$

$$P \Longrightarrow Q \Longrightarrow P \wedge Q \qquad \neg P \Longrightarrow \neg Q \Longrightarrow \neg(P \vee Q)$$

Literal Elimination

$\wedge$-elimination:

Example

$$\frac{P_1 \wedge P_2 \wedge P_3 \wedge Q \wedge P_4}{Q}$$

- explosion
- literal memoization

$\neg\vee$-elimination:

- dually

Equivalence

Conjunctions:

Example

$$(P_1 \wedge P_2 \wedge \mathit{true} \wedge P_3) \leftrightarrow (P_3 \wedge P_1 \wedge P_2)$$

$\Longrightarrow$ explosion of left-hand side, join to right-hand side

$\Longleftarrow$ dually

Equivalence

Conjunctions:

Example

$$(P_1 \wedge P_2 \wedge \mathit{true} \wedge P_3) \leftrightarrow (P_3 \wedge P_1 \wedge P_2)$$

$\Longrightarrow$ explosion of left-hand side, join to right-hand side

$\Longleftarrow$ dually

Disjunctions:

- negate both sides
- similar to case of conjunctions

Contradiction and Excluded Middle

Contradiction:

Example

$$(P_1 \wedge \neg Q \wedge P_2 \wedge Q \wedge P_3) \leftrightarrow \mathit{false}$$

$\Longrightarrow$ explode left-hand side, apply $P \Longrightarrow \neg P \Longrightarrow \mathit{false}$

$\Longleftarrow$ trivial

Contradiction and Excluded Middle

Contradiction:

Example

$$(P_1 \wedge \neg Q \wedge P_2 \wedge Q \wedge P_3) \leftrightarrow \mathit{false}$$

$\Longrightarrow$ explode left-hand side, apply $P \Longrightarrow \neg P \Longrightarrow \mathit{false}$

$\Longleftarrow$ trivial

Excluded middle:

Example

$$(P_1 \vee Q \vee P_2 \vee \neg Q) \leftrightarrow \mathit{true}$$

negate both sides, then similar to contradiction

Unit Resolution

Example

$$\frac{P_1 \vee Q_1 \vee \neg P_2 \vee \neg Q_2 \qquad \neg Q_1 \qquad Q_2}{\neg P_2 \vee P_1}$$

Unit Resolution

Example

$$\frac{P_1 \vee Q_1 \vee \neg P_2 \vee \neg Q_2 \qquad \neg Q_1 \qquad Q_2}{\neg P_2 \vee P_1}$$

Show instead:

$$\frac{\neg(\neg P_2 \vee P_1) \qquad \neg Q_1 \qquad Q_2}{\neg(P_1 \vee Q_1 \vee \neg P_2 \vee \neg Q_2)}$$

- explode first assumption
- join assumptions to conclusion

Theory-Specific Reasoning

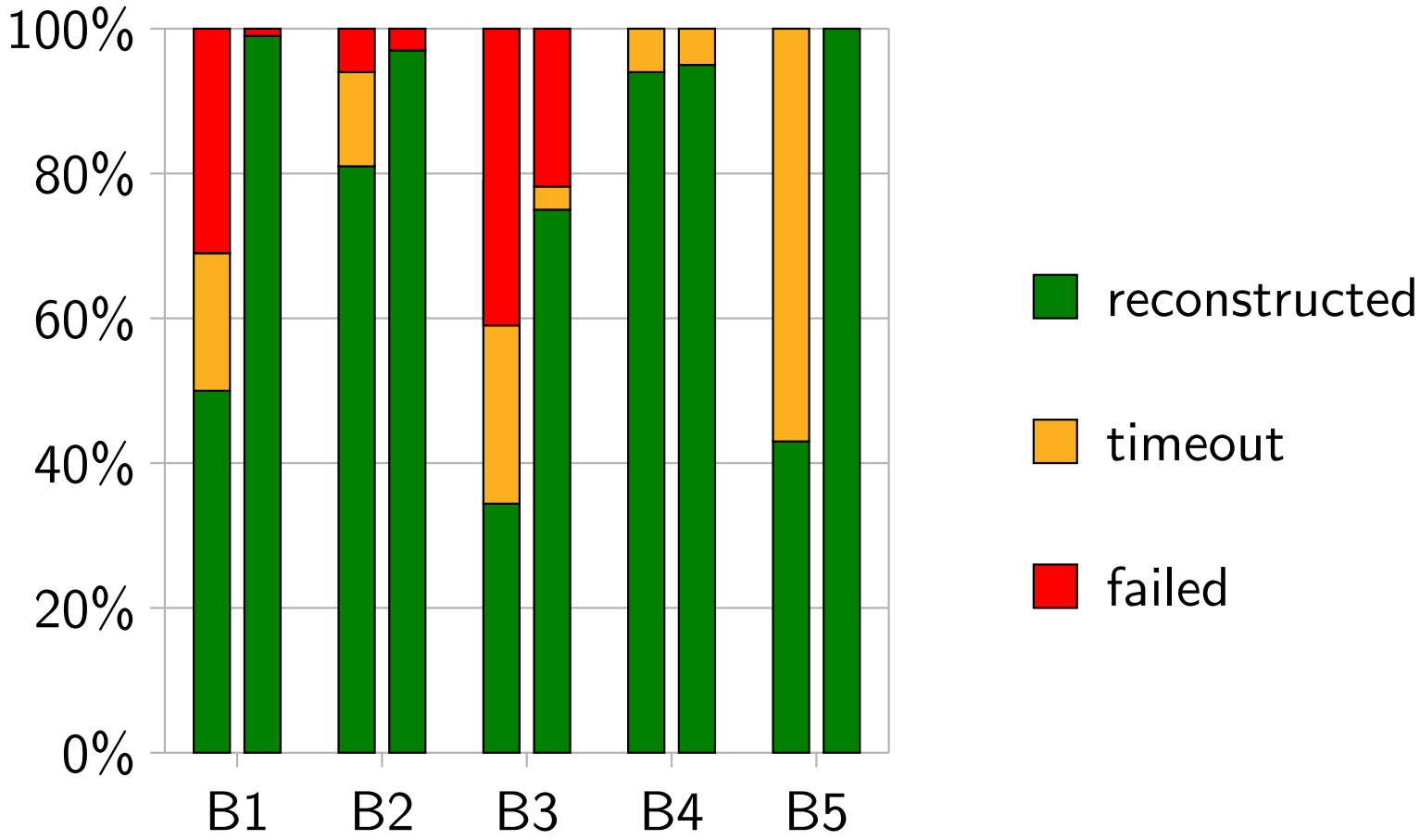
Schematic theorems:

- 120 rewrite rules identified

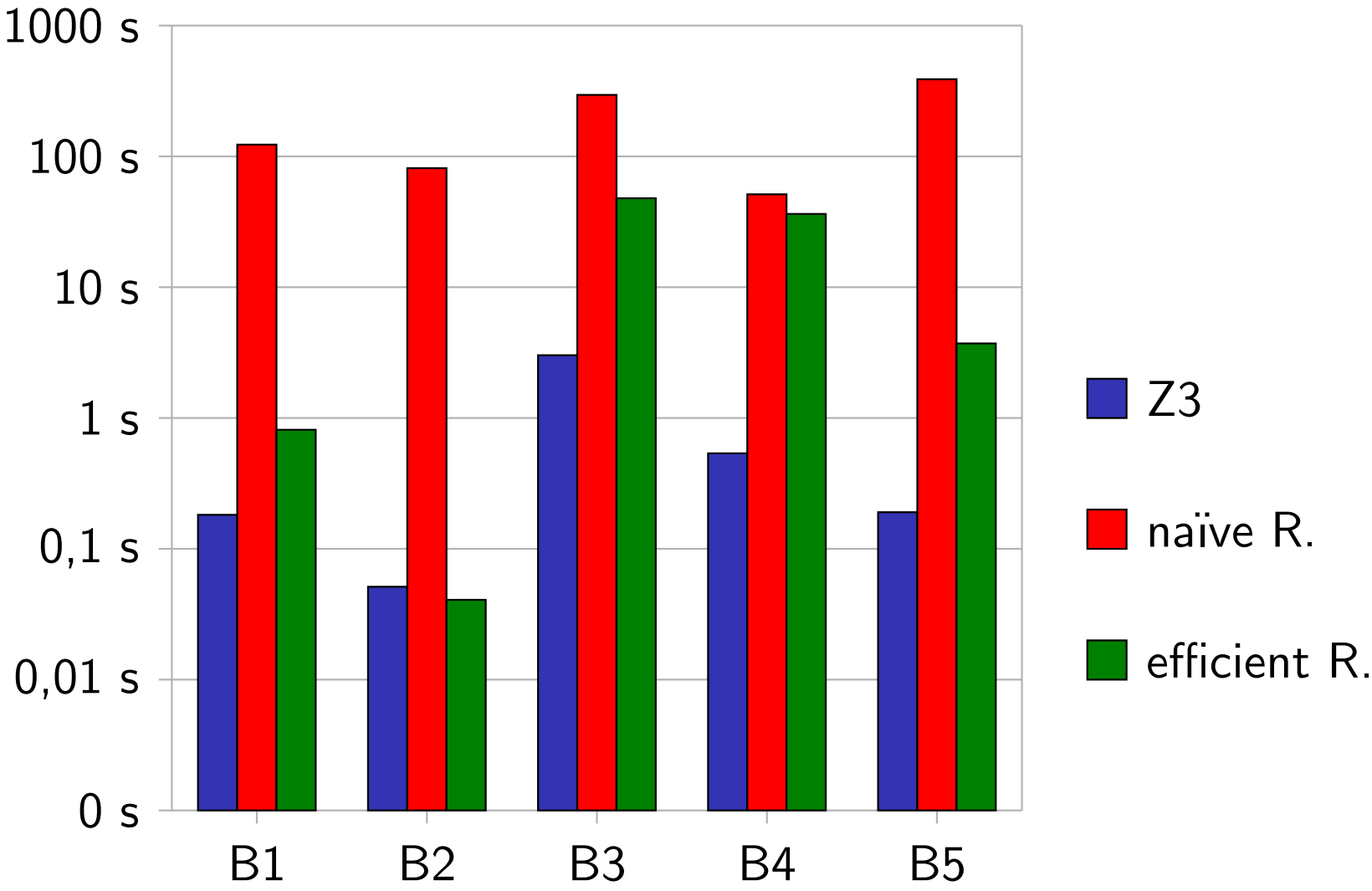
Generalization:

- prepare for generic automated proof tools
- replace “unsupported” terms by variables
- applied for linear arithmetic and propositional reasoning

Results: Proof Reconstruction



Results: Runtimes



Conclusion

Proof reconstruction with Isabelle:

- feasible and efficient
- can be faster than proof search
- required specialized proof procedures
- identified (non-critical) bugs in Z3

Practical implications:

- powerful automation available for Isabelle
- included in latest Isabelle release