Technische Universität München
Institut für Informatik
Prof. Tobias Nipkow, Ph.D.
Brian Huffman, Peter Lammich

WS 2011/12
3. 02. 2012

Semantics of Programming Languages

Exercise Sheet 14

Exercise 14.1 Abstract Boolean Expressions

Finnish exercise 13.3!

Exercise 14.2 Galois Connections

Given an abstraction function $\alpha{::}'c \Rightarrow {}'a$ and a concretization function $\gamma{::}'a \Rightarrow {}'c$, they form a Galois-Connection, iff

$\alpha\ c \leq a \longleftrightarrow c \leq \alpha\ a$

Intuitively, this means that abstraction and concretization can be used interchangeably.

Your task is to prove some properties of Galois-Connections. Warning: Not all properties we propose here are actually true! Give a counterexample for those cases.

locale *galois_connection* =
  fixes α:: "$'a$::*complete_lattice* ⇒ $'b$::*complete_lattice*" **and** γ
  assumes *galois*: "$c \leq \gamma(a) \longleftrightarrow \alpha(c) \leq a$"
begin

Intuition: Concretization followed by abstraction yields a more precise value.

lemma *αγ_defl*: "$\alpha(\gamma(x)) \leq x$"

Intuition: Abstraction followed by concretization yields a more precise value.

lemma *γα_defl*: "$\gamma(\alpha(x)) \leq x$"

Intuition: Abstraction followed by concretization yields a less precise value.

lemma *γα_infl*: "$x \leq \gamma(\alpha(x))$"

Intuition: Concretization followed by abstraction yields a less precise value.

lemma *αγ_infl*: "$x \leq \alpha(\gamma(x))$"

lemma α*_mono*: *"mono* α*"*

lemma γ*_mono*: *"mono* γ*"*

Intuition: Concretization of the greatest lower bound is the same as the greatest lower bound of concretizations.

lemma *dist_*γ[*simp*]:
"γ (*inf a b*) = *inf* (γ *a*) (γ *b*)"

Intuition: Abstraction of the least upper bound (join) is the same as the least upper bound of abstractions.

lemma *dist_*α[*simp*]:
"α (*sup a b*) = *sup* (α *a*) (α *b*)"

end

Intuition: γ is already uniquely determined by α

lemma γ*_determ*:
assumes *"galois_connection* α γ*"* **and** *"galois_connection* α γ'*"*
shows "γ=γ'"
proof −
interpret *a*: *galois_connection* α γ + *b*: *galois_connection* α γ' **by** *fact+*

show *?thesis*
qed

Intuition: α is already uniquely determined by γ

lemma α*_determ*:
assumes *"galois_connection* α γ*"* **and** *"galois_connection* α' γ*"*
shows "α=α'"
proof −
interpret *a*: *galois_connection* α γ + *b*: *galois_connection* α' γ **by** *fact+*

show *?thesis*
qed

Recipe for counterexamples (by example):

Assume we would have asked you to show

lemma (**in** *galois_connection*) α*_antimono*: "$y \le x \Longrightarrow \alpha\ x \le \alpha\ y$" **oops**

First find an appropriate Galois-Connection. In our case, we take the trivial one (*id*,*id*) over the complete lattice of sets of booleans. Hint: The complete lattice of sets of booleans *bool set* and the lattice of sets of unit-type *unit set* are good candidates for finding counterexamples!

definition "$\alpha c \equiv$ *id*::(*bool set* $\Rightarrow$ *bool set*)"

definition "$\gamma c \equiv id$::(*bool set* $\Rightarrow$ *bool set*)"
interpretation *c*!: *galois_connection* αc γc
  apply (*unfold_locales*)
  unfolding αc*_def* γc*_def* **by** *auto*

Then prove a lemma that provides a counterexample

lemma
  defines "$x \equiv UNIV$" **and** "$y \equiv \{\}$"
  shows "$\neg$ ($y \leq x \longrightarrow \alpha c\ x \leq \alpha c\ y$)"
  unfolding αc*_def* γc*_def* *x_def* *y_def* **by** *auto*