

## Übungen zu Grundlagen der Softwarezuverlässigkeit

Besprechung am 17.02.06

### Aufgabe 7.1

Es sei

$$C = \{0 : 00, 0 : 01, \dots, 0 : 59, 1 : 00, \dots, 23 : 59\}$$

die Menge von "Uhrzeiten" und die folgende Abstraktion

$$A_0 = \{\text{Morgen, Vormittag, Mittag, Nachmittag, Abend, Nacht, } \perp, \top\}$$

mit den Konkretisierungen

$$\begin{aligned} \gamma(\text{Morgen}) &= \{7 : 30, \dots, 10 : 30\} \\ \gamma(\text{Vormittag}) &= \{10 : 00, \dots, 12 : 00\} \\ \gamma(\text{Mittag}) &= \{11 : 30, \dots, 14 : 00\} \\ \gamma(\text{Nachmittag}) &= \{15 : 00, \dots, 16 : 45\} \\ \gamma(\text{Abend}) &= \{17 : 30, \dots, 22 : 00\} \\ \gamma(\text{Nacht}) &= \{23 : 00, \dots, 23 : 59\} \cup \{00 : 00, \dots, 6 : 00\} \\ \gamma(\perp) &= \emptyset \\ \gamma(\top) &= C \end{aligned}$$

gegeben.

- Erweitern Sie  $A_0$  durch möglichst wenig zusätzliche Elemente zu einem vollständigen Verband  $A$ .
- Falls  $A$  nicht wohlgeformt ist, so ändern Sie  $A$  entsprechend ab. Machen Sie sich klar, dass für je zwei  $a, b \in A$  ein  $c$  derart existieren muss, dass  $\gamma(c) = \gamma(a) \cap \gamma(b)$  gilt (Warum?).
- $A$  wird um das Element  $\text{Uni}$  mit  $\gamma(\text{Uni}) = \{8 : 00, \dots, 17 : 15\}$  zu  $A'$  erweitert.

Überprüfen Sie, ob  $A'$  noch immer ein wohlgeformter, vollständiger Verband ist und passen Sie  $A'$  notfalls an.

Hinweis: Tragen Sie die Zeitintervalle auf einen Kreis (bzw. mehrere konzentrische Kreise) ein. Die Skizze muss dabei nur korrekt die  $\subseteq$ -Relation darstellen, damit an ihr die benötigten Eigenschaften überprüft werden können.

### Aufgabe 7.2

Betrachten Sie folgendes Programm:

```
var
  x      : integer;
  y      : integer;
begin
  (l0) if isEven( x )
  (l1) then y := 2;
  (l2) else y := -2;

  (l3) x := x * ( y - 2 ) * ( y + 2 );

  (l4) if x = 0
  (l5) then y := 1;
  (l6) else y := 3;
  (l7)
end;
```

Zur Konstantenerkennung soll der Wert einer Variable durch einen Wert aus

$$A_0 = \text{integer} \cup \{\top, \perp\}$$

abstrahiert werden. Die Konkretisierung ist durch  $\gamma_0(v) = \{v\}$  für  $v \in \text{integer}$  und  $\gamma_0(\top) = \text{integer}$ ,  $\gamma_0(\perp) = \emptyset$  gegeben.

- (a) Wie lautet die entsprechende Abstraktionsabbildung  $\alpha_0 : 2^{\text{integer}} \rightarrow A_0$ ? Vergleiche auch Aufgabe 7.3 - (f).
- (b) Die möglichen Speicherbelegungen des obigen Programms sind durch  $C := 2^{\text{integer} \times \text{integer}}$  gegeben.  $\pi_x, \pi_y$  bezeichnen die Projektionen auf die  $x$ - bzw.  $y$ -Werte eines Elements  $c \in C$ , z.B. ergibt sich für  $c = \{(4, 5), (3, 4)\} \in C$   $\pi_x(c) = \{4, 3\}$  und  $\pi_y(c) = \{4, 5\}$ .

Die Abstraktion  $\alpha_x$  der Variable  $x$  ergibt sich dann zu  $\alpha_0 \circ \pi_x$ , entsprechend wird  $y$  durch  $\alpha_y := \alpha_0 \circ \pi_y$  abstrahiert. Eine Teilmenge  $c \in C$  wird dann durch  $(\alpha_x(c), \alpha_y(c))$  abstrahiert, für das obige  $c$  ergibt sich also  $(\top, \top)$ .

Entsprechend ist die Konkretisierung  $\gamma((a, b)) = \gamma_0(a) \times \gamma_0(b)$ .

Geben Sie entsprechend der Vorlesung die abstrakten Zuweisungen und Filter für die obigen Anweisungen an.

- (c) Berechnen Sie nun die abstrakten Speicherbelegungen für das obige Programm - die Variablen seien dabei zu Beginn uninitialized.
- (d) Berechnen Sie ebenfalls unter Verwendung der Sammelsemantik die abstrakten Speicherbelegungen an jedem Programmpunkt und vergleichen Sie diese mit den Werten aus der letzten Teilaufgabe.

Beschreiben Sie eine angepasste Abstraktion für `integer`, unter welcher `x` bei `l4` noch als konstant erkannt wird bei Verwendung der Sammelsemantik.

### **Aufgabe 7.3      Galois-Verbindungen - nicht relevant für die Prüfung**

Sei  $(C, \leq)$  ein vollständiger Verband (z.B.  $C = 2^X$ ,  $\leq := \subseteq$  und  $X$  die Menge der möglichen Variablenbelegungen),  $(A, \sqsubseteq)$  eine *partiell geordnete Menge*,  $\alpha : C \rightarrow A$ ,  $\gamma : A \rightarrow C$  Abbildungen mit

$$\forall a \in A, c \in C : \alpha(c) \sqsubseteq a \Leftrightarrow c \leq \gamma(a),$$

d.h.  $(\alpha, \gamma)$  eine Galois-Verbindung zwischen  $(C, \leq)$  und  $(A, \sqsubseteq)$ .

- (a) Zeigen Sie, dass für beliebiges  $a \in A$ ,  $c \in C$  stets  $c \leq \gamma \circ \alpha(c)$  und  $\alpha \circ \gamma(a) \sqsubseteq a$  gilt.

Zur Erinnerung  $\circ$  bezeichnet die Komposition von Funktionen, d.h.  $\alpha \circ \gamma(a) = \alpha(\gamma(a))$ .

Tipp: Beginnen Sie mit der Tautologie  $\gamma(a) \leq \gamma(a)$ .

- (b) Erinnerung: Eine Abbildung  $f : (X, \sqsubseteq_X) \rightarrow (Y, \sqsubseteq_Y)$  zwischen zwei partiell geordneten Mengen heißt *monoton*, falls aus  $x \sqsubseteq_X x'$  stets  $f(x) \sqsubseteq_Y f(x')$  folgt. Die Komposition zweier monotoner Funktionen ist offensichtlich auch wieder monoton.

Zeigen Sie, dass  $\alpha$  und  $\gamma$  monoton sind unter Verwendung der vorangegangenen Aufgabe.

- (c) Zeigen Sie, dass  $\gamma = \gamma \circ \alpha \circ \gamma$  und  $\alpha = \alpha \circ \gamma \circ \alpha$  gilt. Tipp: Wie üblich die Fälle  $\gamma(a) \leq \gamma \circ \alpha \circ \gamma(a)$  und  $\gamma(a) \geq \gamma \circ \alpha \circ \gamma(a)$  getrennt zeigen. Für  $\geq$  sind die ersten beiden Teilaufgaben hilfreich,  $\leq$  folgt direkt aus den Voraussetzungen mit einem ähnlichen Ansatz wie in der ersten Teilaufgabe. Analog für  $\alpha$ .

Folgern Sie damit, dass auch  $\gamma \circ \alpha \circ \gamma \circ \alpha = \gamma \circ \alpha$  und  $\alpha \circ \gamma \circ \alpha \circ \gamma = \alpha \circ \gamma$  gilt.

- (d) Zeigen Sie, dass  $\alpha$  genau dann surjektiv ist, falls  $\gamma$  injektiv ist. Verwenden Sie die letzte Teilaufgabe hierfür.

Überlegen Sie sich, warum es unter dem Gesichtspunkt einer Abstraktion sinnvoll ist zu fordern, dass  $\alpha$  surjektiv bzw.  $\gamma$  injektiv sein soll.

- (e) Zeigen Sie unter Verwendung der beiden vorangegangenen Teilaufgaben, dass  $\gamma$  genau dann injektiv ist, falls,  $\alpha \circ \gamma = \text{id}_A$  gilt.

Bemerkung: Damit ist äquivalent:  $(\alpha, \gamma)$  reduziert,  $\gamma$  injektiv,  $\alpha$  surjektiv,  $\alpha \circ \gamma = \text{id}_A$ .  $\text{id}_A$  sei dabei die Identität auf  $A$ .

(f) (korregiert) Sei  $(\alpha, \gamma)$  eine Galois-Verbindung. Zeigen Sie, dass

$$\gamma(a) = \bigvee \{c \in C \mid \alpha(c) \sqsubseteq a\}$$

und

$$\alpha(c) = \bigwedge \{a \in A \mid c \leq \gamma(a)\}$$

gilt - wobei in beiden Fällen das Supremum bzw. Infimum existiert, auch wenn  $(C, \leq)$  bzw.  $(A, \sqsubseteq)$  keine vollständige Verbände sein müssen.

Hiermit folgt dann, dass mit  $\alpha$  (bzw.  $\gamma$ ) auch bereits  $\gamma$  (bzw.  $\alpha$ ) eindeutig festgelegt ist - soweit sich  $\alpha$  (bzw.  $\gamma$ ) zu einer Galois-Verbindung ergänzen lässt.

(g) Sei  $\pi : C \rightarrow C$  eine Abbildung mit  $\pi$  monoton,  $c \leq \pi(c)$  und  $\pi \circ \pi(c) = \pi(c)$  für alle  $c \in C$ .  $\pi$  verhält sich also so, wie man es von einer Überapproximation erwarten würde,  $\pi$  verliert keine Zustände, und mehrmalige Approximation derselben Menge führt immer auf dasselbe Ergebnis. Weiter sei  $\iota : \pi(C) \rightarrow C : p \rightarrow p$  die formale Einbettung von  $\pi(C)$  in  $C$  -  $\iota$  dient nur dazu, formal  $(\pi, \iota)$  als Galois-Verbindung schreiben zu können.

Zeigen Sie, dass  $(\pi, \iota)$  tatsächlich eine reduzierte Galois-Verbindung ist zwischen  $(C, \leq)$  und  $(\pi(C), \leq)$ .

Bemerkung: Insbesondere erfüllt  $\gamma \circ \alpha$  diese Bedingungen nach dem bereits Gezeigten. Ist somit erst eine Galois-Verbindung  $(\alpha, \gamma)$  gefunden, so kann man einfach durch Übergang zu  $(\gamma \circ \alpha(C), \leq)$  eine reduzierte Galois-Verbindung erhalten.

(h) Zeigen Sie, dass in einer reduzierten Galois-Verbindung  $a \sqsubseteq b \Leftrightarrow \gamma(a) \leq \gamma(b)$  gilt.

Bemerkung: So war die partielle Ordnung  $\sqsubseteq$  in der Vorlesung gerade definiert worden für die dort betrachtete Abstraktion.

(i) Sei  $(\alpha, \gamma)$  eine reduzierte Galois-Verbindung. Zeigen Sie, dass  $(A, \sqsubseteq)$  mit  $(\gamma \circ \alpha(C), \leq)$  identifiziert werden kann.

D.h. die Abstraktionen, welche üblicherweise betrachtet werden, können stets in  $(C, \leq)$  eingebettet werden.

(j) Sei  $(\alpha, \gamma)$  eine reduzierte Galois-Verbindung ist. Zeigen Sie, dass dann  $(A, \sqsubseteq)$  ein vollständiger Verband ist.

Hinweis: Nach dem letzten Ergebnis müssen Sie nur zeigen, dass  $(\gamma(A), \leq)$  ein vollständiger Verband ist. Jede Teilmenge  $T$  von  $\gamma(A)$  hat nach Voraussetzung ein Supremum  $\bigvee T$  in  $(C, \leq)$ . Im Allgemeinen wird  $\bigvee T$  jedoch nicht in  $(\gamma(A), \leq)$  existieren (siehe z.B. 7.2). Zeigen Sie, dass aber  $\gamma \circ \alpha(\bigvee T)$  das Supremum von  $T$  in  $(\gamma(A), \leq)$  ist.

Untersuchen Sie ebenfalls, wie es sich mit dem Infimum verhält, d.h. stimmt das Infimum auf  $\gamma(A)$  mit dem auf  $C$  überein, oder gilt dasselbe wie im Fall des Supremums?

Zusammenfassung:

Aus den vorangegangenen Teilaufgaben wissen Sie nun, dass im Fall einer reduzierten Galois-Verbindung  $(\alpha, \gamma)$  folgende Eigenschaften erfüllt sind:

- $(A, \sqsubseteq)$  ist ein vollständiger Verband.
- $a \sqsubseteq b \Leftrightarrow \gamma(a) \leq \gamma(b)$ .
- $\alpha(c) = \bigwedge \{a \in A \mid c \leq \gamma(a)\}$ .

Das heißt, jede reduzierte Galois-Verbindung ist eine wohlgeformte Abstraktion im Sinne der Vorlesung.

Auf den Folien 331 und 334 (in Acroread: 339 und 342) finden Sie die entsprechenden Beweise dafür, dass jede wohlgeformte Abstraktion bereits eine reduzierte Galois-Verbindung ist.

(k) Bei der Abstraktion von Programmen hat man u.U. mehrere Galois-Verbindungen  $(\alpha_i, \gamma_i)$  zwischen  $(C, \leq)$  und  $(A_i, \sqsubseteq_i)$  für  $i \in I$ , vergleiche z.B. Aufgabe 7.2, dort waren die  $A_i$  gleich, jedoch die Abstraktionen  $\alpha_i$  verschieden.

Die kanonische Konstruktion der Abstraktion  $(A, \sqsubseteq)$ , welche alle  $(A_i, \sqsubseteq_i)$  umfasst, ist (wie üblich) über das mengentheoretische Produkt  $A := \prod_{i \in I} A_i$  definiert, wobei die Ordnung  $\sqsubseteq$  auf  $A$  wieder punktweise definiert ist, d.h. es gilt  $(a_i)_{i \in I} \sqsubseteq (b_i)_{i \in I}$  genau dann, wenn für alle  $i \in I$   $a_i \sqsubseteq_i b_i$  gilt.

Die Abstraktion  $\alpha$  geschieht dann ebenfalls punktweise:  $\alpha(c) := (\alpha_i(c))_{i \in I}$ . Wie Sie in dieser Aufgabe bereits gezeigt haben, muss dann  $\gamma((a_i)_{i \in I}) = \bigvee \{c \in C \mid \alpha(c) \sqsubseteq (a_i)_{i \in I}\}$  gelten, damit  $(\alpha, \gamma)$  eine Galois-Verbindung sein kann.

Zeigen Sie, dass genauer  $\gamma((a_i)_{i \in I}) = \bigwedge \{\gamma_i(a_i) \mid i \in I\}$  gilt.

Hinweis: Auf Grund der Eindeutigkeit von  $\gamma$  reicht es zu zeigen, dass es sich bei  $(\alpha, \gamma)$  um eine Galois-Verbindung handelt, *falls*  $\gamma$  gerade durch die letzte Gleichung definiert wird.