Analyse und Verifikation
(185.276, VU 2.0, ECTS 3.0)

Übungsblatt 6

Bernhard Urban
Matr.Nr.: 0725771 KNZ: 067 937
lewurm@gmail.com

Thomas Reinbacher
Matr.Nr.: 0828472 KNZ: 786 881
treinbacher@ecs.tuwien.ac.at

31.05.2011

Aufgabe 1:

Reverse abstrakte Semantik für Dead Code:

- Datenflussanalyseverband:

$$(\mathcal{C}, \sqcap, \sqcup, \sqsubseteq, \bot, \top) =_{df} (\mathbb{B}, \vee, \wedge, \leq, \mathsf{false}, \mathsf{true})$$

  wobei true für "x ist an dieser Stelle tot" steht. Als *join*-Operator wurde das logische UND $\wedge$ verwendet, da x nur dann tot ist wenn dies für alle Pfade der Fall ist.

- Reverses Datenflussanalysefunktional: $[\![\ ]\!]_{dc_R} : E \to (\mathbb{B} \to \mathbb{B})$ ist definiert durch

$$\forall e \in E.\ [\![\ e\ ]\!]_{dc_R}(b) =_{df} \begin{cases} \mathsf{false} & \text{falls } x \text{ frei vorkommt} \\ \mathsf{true} & \text{falls } x \text{ ein neuer Wert zugewiesen wird} \\ b & \text{sonst} \end{cases}$$

Für den Anfangszustand (d.h. der letzte Knoten) gilt, dass x tot ist.

Aufgabe 2:

Definitionen Sei $\hat{\mathcal{C}} = (\mathcal{C}, \sqcap, \sqcup, \sqsubseteq, \bot, \top)$ ein vollständiger Verband und $f : \mathcal{C} \to \mathcal{C}$ eine Funktion auf $\mathcal{C}$. Dann heisst f (Folie 293):

- monoton gdw. $\forall c, c' \in \mathcal{C}.\ c \sqsubseteq c' \Rightarrow f(c) \sqsubseteq f(c')$
- distributiv gdw. $\forall C' \subseteq \mathcal{C}.\ f(\bigsqcap C') = \bigsqcap\{f(c) \mid c \in C'\}$

- additiv gdw. $\forall C' \subseteq \mathcal{C}.\ f(\bigsqcup C') = \bigsqcup\{f(c) \mid c \in C'\}$

Das reverse Datenflussanalysefunktional $[\![\ ]\!]_R : E \to (C \to C)$ ist definiert durch (Folie 324):

$$\forall e \in E\ \forall c \in \mathcal{C}.\ [\![\ e\ ]\!]_R(c) =_{df} \bigsqcap\{c' \mid [\![\ e\ ]\!](c') \sqsupseteq c\}$$

Sprechweisen
$\bigsqcap \ldots$ größte untere Schranke.
$\sqsupseteq \ldots$ "mindestens so groß"

$[\![\ e\ ]\!]_R$ ist wohldefiniert und monoton. $[\![\ e\ ]\!]_R$ ist wohldefiniert, da für jeden vollständigen Verband gilt, dass jede Teilmenge eine kleinste obere und eine größte untere Schranke besitzt (Folie 114, vgl. Lemma A.2 in Principles of Program Analysis, Nielson, Nielson, Hankin, '05).
(Beweisskizze) $[\![\ e\ ]\!]_R$ ist monoton wenn folgendes gilt:

$$\begin{aligned} &\forall c, d \in \mathcal{C}.\ c \sqsupseteq d \Rightarrow \\ [\![\ e\ ]\!]_R(c) = \bigsqcap\{c' \mid [\![\ e\ ]\!](c') \sqsupseteq c\} &\sqsupseteq [\![\ e\ ]\!]_R(d) = \bigsqcap\{d' \mid [\![\ e\ ]\!](d') \sqsupseteq d\} \\ \bigsqcap\{c' \mid [\![\ e\ ]\!](c') \sqsupseteq c\} &\sqsupseteq \bigsqcap\{d' \mid [\![\ e\ ]\!](d') \sqsupseteq d\} \end{aligned}$$

$[\![\ e\ ]\!]_R$ ist additiv, falls $[\![\ e\ ]\!]$ distributiv ist.
(Beweisskizze): Additiv:

$$\forall C' \subseteq \mathcal{C}.\ f(\bigsqcup C') = \bigsqcup\{f(c) \mid c \in C'\}$$

einsetzen von $[\![\ e\ ]\!]_R$:

$$\forall C' \subseteq \mathcal{C}.\ [\![\ e\ ]\!]_R(\bigsqcup C') = \bigsqcup\{[\![\ e\ ]\!]_R(c) \mid c \in C'\}$$

Einsetzen in die Definition von $[\![\ e\ ]\!]_R$:

$$\bigsqcap\{c' \mid [\![\ e\ ]\!](c') \sqsupseteq \bigsqcup C'\} = \bigsqcup\{\bigsqcap\{c' \mid [\![\ e\ ]\!](c') \sqsupseteq c\} \mid c \in C'\}$$

Aufgabe 3:

Aus der Annahme folgt, dass sowohl $[\![\ e\ ]\!]$ als auch $[\![\ e\ ]\!]_R$ monotone Funktionen sind. Es müssen nun die beiden Inklusionen[1] gezeigt werden:

$$\begin{aligned} (1): \quad [\![\ e\ ]\!]_R \ \circ\ [\![\ e\ ]\!] \ &\sqsubseteq\ Id \\ (2): \quad [\![\ e\ ]\!] \ \circ\ [\![\ e\ ]\!]_R \ &\sqsupseteq\ Id \end{aligned}$$

Informell: Die beiden Inklusionen zeigen, dass man die Sicherheitseigenschaft nicht verliert, wenn man zwischen $[\![\ e\ ]\!]$ und $[\![\ e\ ]\!]_R$ hin und hergeht. Dabei muss man einen Genauigkeitsverlust in Kauf nehmen.

[1] Wir definieren $Id := Id_{\mathcal{C}}$

Definitionen Das Rückwärtsfunktional $[\![e]\!]_R$ ist definiert als:

$$\forall e \in E\ \forall c \in \mathcal{C}.\ [\![e]\!]_R(c) =_{df} \bigsqcap \{c' \mid [\![e]\!](c') \sqsupseteq c\}$$

Inklusion (1) $[\![e]\!]_R \circ [\![e]\!] \sqsubseteq Id$
Aus der Monotonie folgt (man beachte die umgedrehte Relation):

$$\forall c, c' \in \mathcal{C}.\ c' \sqsupseteq c \Rightarrow [\![e]\!](c') \sqsupseteq [\![e]\!](c)$$

Unter Verwendung der Beziehung:

$$\forall c' \in \mathcal{C}.\ (A(c') \Rightarrow B(c')) \Rightarrow (\{c' | B(c')\} \supseteq \{c' | A(c')\})$$

gilt somit auf folgendes:

$$\{c' \mid [\![e]\!](c') \sqsupseteq [\![e]\!](c)\} \supseteq \{c' | c' \sqsupseteq c\}$$

Und durch die Verwendung der Beziehung zwischen Set inklusion und $\bigsqcap$:

$$(A \supseteq B) \Rightarrow (\bigsqcap A \sqsubseteq \bigsqcap B)$$

und daraus folgt:

$$\bigsqcap \{c' \mid [\![e]\!](c') \sqsupseteq [\![e]\!](c)\} \sqsubseteq \bigsqcap \{c' | c' \sqsupseteq c\}$$

Unter Ausnützung der Beziehung

$$\forall x \in M : \bigsqcap M \sqsubseteq x$$

erhalten wir:

$$\forall c \in \mathcal{C}.\ \bigsqcap \{c' | c' \sqsupseteq c\} \sqsubseteq c$$

Durch einsetzen:

$$\begin{aligned} \bigsqcap \{c \mid [\![e]\!](c') \sqsupseteq [\![e]\!](c)\} &\sqsubseteq \bigsqcap \{c' | c' \sqsupseteq c\} \sqsubseteq c \\ \bigsqcap \{c' \mid [\![e]\!](c') \sqsupseteq [\![e]\!](c)\} &\sqsubseteq c \\ [\![e]\!]_R([\![e]\!](c)) &\sqsubseteq c \\ [\![e]\!]_R \circ [\![e]\!] &\sqsubseteq Id \end{aligned}$$

Was zu zeigen war.

Inklusion (2) $[\![e]\!] \circ [\![e]\!]_R \sqsupseteq Id$
Aus der Distributivität folgt:

$$\forall e \in E\ \forall C' \subseteq \mathcal{C}.\ [\![e]\!](\bigsqcap C') = \bigsqcap \{[\![e]\!](c) \mid c \in C'\}$$

Wir setzen nun für $C' =_{df} \{c' \mid [\![e]\!](c') \sqsupseteq d\}$ ein und erhalten:

$$[\![e]\!](\bigsqcap \{c' \mid [\![e]\!](c') \sqsupseteq d\}) = \bigsqcap \underbrace{\{[\![e]\!](c) \mid c \in \{c' \mid [\![e]\!](c') \sqsupseteq d\}\}}_{B}$$

Informales Argument: Für die Menge B wählen wir nur jene Elemente c aus für die folgendes gilt:

$$\forall x \in C' : [\![e]\!](x) \sqsupseteq d$$

Wir stellen folgendes fest:

- d ist die untere Schranke von B
- $\bigsqcap B$ ist die größte untere Schranke von B

Eine größte untere Schranke ist definiert als:

$$(1)\forall x \in B : \bigsqcap B \sqsubseteq x$$
$$(2)\forall c \in B : (\forall x \in B : c \sqsubseteq x \Rightarrow \bigsqcap B \sqsubseteq x)$$

und folgern daraus

$$\bigsqcap B \sqsupseteq d$$

Somit erhalten wir:

$$[\![e]\!](\bigsqcap \{c' \mid 22[\![e]\!](c') \sqsupseteq d\}) = \bigsqcap \underbrace{\{[\![e]\!](c) \mid c \in \{c' \mid [\![e]\!](c') \sqsupseteq d\}\}}_{B} \sqsupseteq d$$

und weiters durch Umformungen:

$$[\![e]\!](\bigsqcap \{c' \mid [\![e]\!](c') \sqsupseteq d\}) \sqsupseteq d$$
$$[\![e]\!]([\![e]\!]_R(d)) \sqsupseteq d$$
$$[\![e]\!] \circ [\![e]\!]_R \sqsupseteq Id$$

was zu zeigen war.