Technische Universität Wien
Programmiersprachen und Übersetzer
Prof. Dr. J. Knoop

A-1040 Wien
Argentinierstr. 8
Tel.: 01-58801-18510

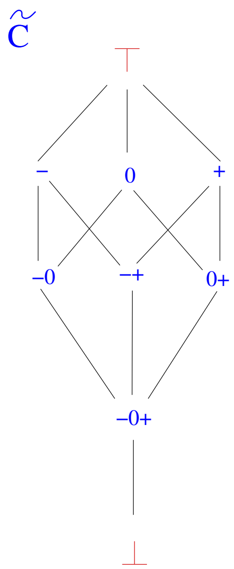
“ Analyse und Verifikation (185.276, VU 2.0, ECTS 3.0) ” SS 2021

Übungsblatt 6

07.05.2021

Die Aufgaben beziehen sich auf *Kapitel 7* und *8* über abstrakte Semantiken, Analysesemantiken und Datenflussanalyse der Vorlesung.

Vorzeichenanalyse. Das Hasse-Diagramm:



legt den Verband $\widetilde{\mathcal{C}} = (C, \sqsubseteq, \sqcap, \sqcup, \perp, \top)$ zur Vorzeichenanalyse über der Elementmenge:

$$C = \{\perp, -, 0, +, -0, 0+, -0+, \top\}$$

fest. Die Verbandselemente $-$, $+$ und 0 repräsentieren dabei die Mengen $\{z \in \mathbb{Z} \,|\, z < \mathbf{0}\}$, $\{z \in \mathbb{Z} \,|\, z > \mathbf{0}\}$ und $\{\mathbf{0}\}$ echt negativer, echt positiver ganzer Zahlen sowie die einelementige Menge mit Null als einzigem Element. Entsprechend repräsentieren die Elemente $-0+$, -0, $0+$ und $-+$ die Mengen $\mathbb{Z}$, $\{z \in \mathbb{Z} \,|\, z \leq 0\}$, $\{z \in \mathbb{Z} \,|\, z \geq \mathbf{0}\}$ und $\{z \in \mathbb{Z} \,|\, z \neq \mathbf{0}\}$ ganzer Zahlen, negativer bxw. positiver ganzer Zahlen einschließlich null sowie die Menge von Null verschiedener ganzer Zahlen.

Das Element $-+$ steht damit für die (Analyse-) Information ‘ungleich null’, die Elemente -0, $0+$ entsprechend für die Informationen ‘kleiner oder gleich null’ bzw. ‘größer oder gleich null’ usw. Die Elemente $\perp$ und $\top$ schließlich stehen für ‘keine Information’, die ‘Nullinformation’ bzw. die ‘Allinformation’, die Verallgemeinerung jeder anderen durch ein Verbandselement dargestellten-Information ist.

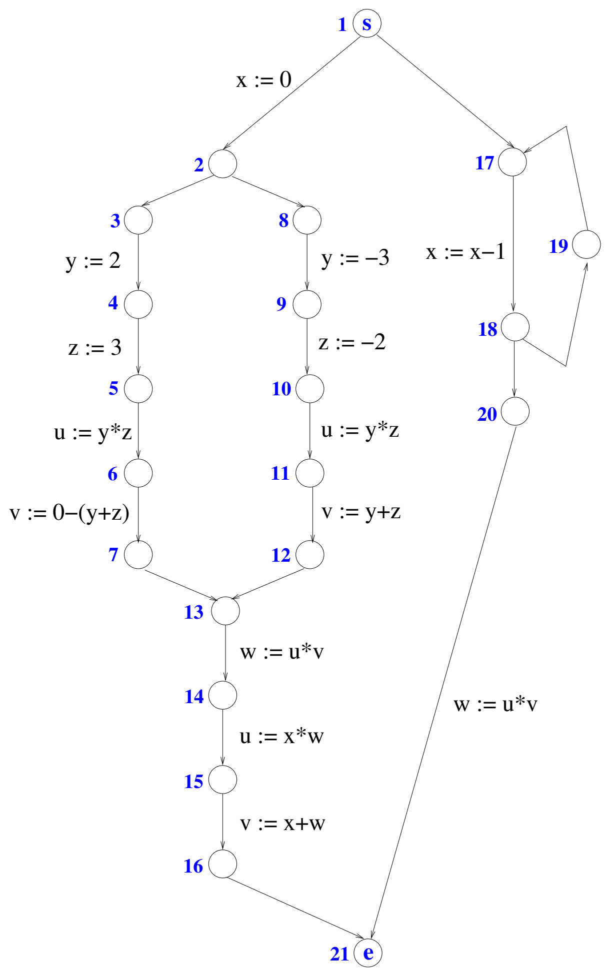
Für die Vorzeichenanalyse (als konkrete Programmanalyse) betrachten wir Programme über einer endlichen Menge $V = \{x_1, x_2, \ldots, x_k\}$ von Variablen und der Menge abstrakter Programmzustände über $\mathcal{C}$:

$$\Sigma = \{\sigma \,|\, \sigma : V \to C\}$$

Weiters bezeichnen wir mit $\mathbf{T}$ die Menge der Terme über V, der Menge $K = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ der Konstantensymbole für ganze Zahlen und der Menge $Op = \{+, -, *, /\}$ zweistelliger Operatoren (oder: Operationssymbole) mit der üblichen Bedeutung der Addition, Subtraktion, Multiplikation und ganzzahligen Division auf der Menge der ganzen Zahlen.

Aufgabe 1 : ((2+2)+2+(1+1)+(2+2) Punkte)

1. Definiere nach dem Vorbild von
   (a) Definition 8.13.2.2.4 die Auswertungsfunktion $\mathcal{A} : \mathbf{T} \to (\Sigma \to C)$.
   (b) Definition 8.13.2.2.5 die abstrakte Instruktionssemantik $\theta_i : \Sigma \to \Sigma$ für ι Instruktion der Form $x := t$ oder der Form *skip*.
2. Spezifiziere nach dem Vorbild der "einfachen-Konstanten"-Analyse aus Kapitel 8.13.2.3 die Vorzeichenanalyse, die für jede Programmstelle für jede Variable möglichst genau deren Vorzeichen bestimmt.
3. Ist die Vorzeichenanalyse (ohne Beweis)
   (a) monoton?
   (b) distributiv?
4. Gib für das Programm G:



und die Anfangszusicherung $\sigma_{\mathbf{S}} \in \Sigma$ mit $\sigma_{\mathbf{S}} = (\lambda\, s.\ +)$ die *MaxFP*-Semantik an, indem die Programmpunkte mit den entsprechenden DFA-Informationen annotiert werden.

5. Unterscheiden sich für das Beispiel aus Aufgabe 1.4 *SUP*- und *MaxFP*-Semantik voneinander?

Aufgabe 2 : (2+2)+2+(1+1)+(2+2) Punkte)

Wiederhole Aufgabe 1, aber ersetze den Zustandsverband Σ durch den 'auf den Kopf gestellten' Potenzmengenverband $\widetilde{\mathcal{P}(\Sigma)} = (\mathcal{P}(\Sigma), \supseteq, \cup, \cap, \Sigma, \emptyset)$ mit kleinstem Element Σ, größtem Element $\emptyset$ Mengenvereinigung $\cup$ und Mengenschnitt $\cap$ als Schnitt- bzw. Vereinigungsoperation, wobei $\mathcal{P}$ den Potenzmengenoperator bezeichne. Im einzelnen:

1. Definiere nach dem Muster von Aufgabe 1
   (a) die Auswertungsfunktion $\mathcal{A} : \mathbf{T} \to (\mathcal{P}(\Sigma) \to \mathcal{C})$.
   (b) die abstrakte Instruktionssemantik $\theta_i : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ für ι Instruktion der Form $x := t$ oder der Form *skip*.
2. Spezifiziere nach dem Vorbild von Aufgabe 1 die Vorzeichenanalyse bezüglich der neuen Anweisungssemantik.
3. Ist die neue Vorzeichenanalyse (ohne Beweis)
   (a) monoton?
   (b) distributiv?
4. Gib für das Programm aus Aufgabe 1 und die Anfangszusicherung $\{\sigma_{\mathbf{S}}\} \in \mathcal{P}(\Sigma)$, $\sigma_{\mathbf{S}} = (\lambda\, v.\ +)$ die *MaxFP*-Semantik an, indem die Programmpunkte mit den entsprechenden DFA-Informationen annotiert werden.
5. Unterscheiden sich für das Beispiel aus Aufgabe 2.4 *SUP*- und *MaxFP*-Semantik voneinander?

Aufgabe 3 : (8 Punkte)

Beweise mithilfe von Lemma 1 (s.u.):

Für Funktionen $f : C \to C$ auf einem vollständigen Verband $\mathcal{C} = (C, \sqcap, \sqcup, \sqsubseteq, \bot, \top)$ gilt:

1. f distributiv $\Longrightarrow \forall\, \emptyset \neq C' \subseteq C.\ f(\bigsqcup C') \sqsupseteq \bigsqcup\{f(c) \,|\, c \in C'\}$
2. f additiv $\Longrightarrow \forall\, \emptyset \neq C' \subseteq C.\ f(\bigsqcap C') \sqsubseteq \bigsqcap\{f(c) \,|\, c \in C'\}$

Hinweis: Es reicht, entweder Aussage 1) oder Aussage 2) zu zeigen (der Beweis der jeweils anderen Aussage ist vollkommen analog). Lemma 1 darf für den Beweis vorausgesetzt werden.

Für einen vollständigen Verband $\mathcal{C} = (C, \sqcap, \sqcup, \sqsubseteq, \bot, \top)$ und eine Teilmenge $C' \subseteq C$ von C bezeichnen:

– $OS(C') =_{\text{df}} \{c \in C \,|\, C' \sqsubseteq c\} =_{\text{df}} \{c \in C \,|\, \forall\, c' \in C'.\ c' \sqsubseteq c\}$ die Menge der oberen Schranken von C'.

Mit diesen Bezeichnungen gilt:

Lemma 1 Für $\mathcal{C} = (C, \sqcap, \sqcup, \sqsubseteq, \perp, \top)$ vollständiger Verband gilt:

1. $\forall\, C' \subseteq C.\ OS(C') \neq \emptyset \ \wedge\ US(C') \neq \emptyset$
2. $\forall\, C_1, C_2 \subseteq C.\ C_1 \subseteq C_2 \ \Rightarrow\ OS(C_2) \subseteq OS(C_1) \ \wedge\ US(C_2) \subseteq US(C_1)$
3. $\forall\, C_1, C_2 \subseteq C.\ C_1 \subseteq C_2 \ \Rightarrow\ \bigsqcup C_2 \sqsupseteq \bigsqcup C_1 \ \wedge\ \bigsqcap C_2 \sqsubseteq \bigsqcap C_1$
4. $\forall\, C' \subseteq C.\ OS(US(OS(C'))) \ = \ OS(C') \ \wedge\ US(OS(US(C'))) \ = \ US(C')$
5. $\forall\, C' \subseteq C.\ \bigsqcup C' \ = \ \bigsqcap OS(C') \ \wedge\ \bigsqcap C' \ = \ \bigsqcup US(C')$
6. $\forall\, C' \subseteq C.\ \forall\, f \in [C \stackrel{monoton}{\longrightarrow} C].\ f(C') \sqsubseteq f(OS(C')) \ \wedge\ f(US(C')) \sqsubseteq f(C')$
7. $\forall\, C' \subseteq C.\ \forall\, f \in [C \stackrel{monoton}{\longrightarrow} C].\ f(OS(C')) \subseteq OS(f(C')) \ \wedge\ f(US(C')) \subseteq US(f(C'))$

Iucundi acti labores.
Getane Arbeiten sind angenehm.
Cicero (106 - 43 v.Chr.)
röm. Staatsmann und Schriftsteller

Abgabe: Mittwoch, den 19.05.2021, im TUWEL-Kurs zur Lehrveranstaltung.