Software-Modellierung und Verifikation
Informatik 2
Prof. J.-P. Katoen
RWTH Aachen

Priv.-Doz. T. Noll noll@cs.rwth-aachen.de
D. Klink klink@cs.rwth-aachen.de

10. Exercise sheet *Semantics and Verification of Software 2007*

Due to Wed., 27 June 2007, *before* the exercise course begins.

Exercise 10.1:

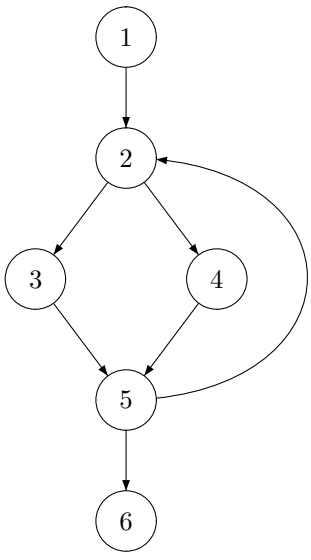
(a) Develop a (non-trivial) *sign analysis* for program variables based on an abstraction that maps all negative numbers to the symbol $-$, zero to the symbol 0 and all positive numbers to $+$. E.g. the set $\{0, 1, 2, \ldots\}$ is abstracted to $\{0, +\}$.

(b) Perform your analysis on the following program:

$x := 0;$
$y := -1;$
$z := x * y;$
while $x \geq y$ **do**
  $x := x + 1;$
  $y := y + x;$
  $z := x * y;$

Exercise 10.2:

Both, *available expression* and *live variable analysis* had transfer functions of the form $\varphi_l(d) = (d \setminus \mathit{kill}(B^l)) \cup \mathit{gen}(B^l)$. Consider the following flowgraph and transfer functions on domain $2^{\{a,b,c,d\}}$ (which can not be converted into *kill-gen* style) and determine the minimal fixpoint using the worklist algorithm from the lecture.



$$\varphi_1(M) = (M \setminus \{a\}) \cup \{c\}$$

$$\varphi_2(M) = \begin{cases} M \cup \{b\} & \text{if } b \in M \vee c \in M \\ M & \text{otherwise} \end{cases}$$

$$\varphi_3(M) = \begin{cases} M \cup \{a, c\} & \text{if } (a \in M \vee d \in M) \wedge (b \in M \vee c \in M) \\ M \cup \{a\} & \text{if } a \in M \vee d \in M \\ M \cup \{c\} & \text{if } b \in M \vee c \in M \\ M & \text{otherwise} \end{cases}$$

$$\varphi_4(M) = \begin{cases} M \cup \{b, d\} & \text{if } b \in M \vee c \in M \vee d \in M \\ M \cup \{b\} & \text{otherwise} \end{cases}$$

$$\varphi_5(M) = (M \setminus \{a\}) \cup \{d\}$$

$$\varphi_6(M) = M$$

Exercise 10.3:

Consider domains of the form $D = 2^M$ where M is a finite set. Transfer function $\varphi_l : D \mapsto D$ is called distributive, iff for any $d_1, d_2 \in D$:

$$\varphi_l(d_1 \sqcup d_2) = \varphi_l(d_1) \sqcup \varphi_l(d_2)$$

(a) Show that any transfer function of the form $\varphi_l(d) = (d \setminus \mathit{kill}(B^l)) \cup \mathit{gen}(B^l)$ is distributive in this setting.

(b) Show that the transfer function from Exercise 10.2 is not representable in *kill-gen* style, but still is distributive.