

Static Analysis Handin #3

Alexander B. Hansen, 20062813

Sivert Bertelsen, 20062179

Søren Løbner, 20050677

{alx,sivert,lobner}@cs.au.dk

February 16, 2010

Exercise 6.7

Først defineres de 6 operatører for den udvidede *Sign* lattice vha. 8 x 8 tabeller og bagefter kontrolleres at de er korrekt monotone.

Operatører

+	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp
1	\perp	+	1	+	-0	+	?	?
0	\perp	1	0	+	-	+0	-0	?
+	\perp	+	+	+	?	+	?	?
-	\perp	-0	-	?	-	?	-	?
+0	\perp	+	+0	+	?	+0	?	?
-0	\perp	?	-0	?	-	?	-0	?
?	\perp	?	?	?	?	?	?	?

-	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp
1	\perp	0	1	-0	+	?	+	?
0	\perp	-	0	-	+	-0	+0	?
+	\perp	+0	+	?	+	?	+	?
-	\perp	-	-	-	?	-	?	?
+0	\perp	?	+0	?	+	?	+0	?
-0	\perp	-	-0	-	+0	-0	?	?
?	\perp	?	?	?	?	?	?	?

*	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	0	\perp	\perp	\perp	\perp	\perp
1	\perp	1	0	+	-	+0	-0	?
0	0	0	0	0	0	0	0	0
+	\perp	+	0	+	?	+0	-0	?
-	\perp	-	0	?	+	-0	+0	?
+0	\perp	+0	0	+0	-0	+0	-0	?
-0	\perp	-0	0	-0	+0	-0	+0	?
?	\perp	?	0	?	?	?	?	?

/	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp
1	\perp	1	?	+0	-0	?	?	?
0	\perp	0	?	0	0	?	?	?
+	\perp	+	?	+0	-0	?	?	?
-	\perp	-	?	-0	+0	?	?	?
+0	\perp	+0	?	+0	-0	?	?	?
-0	\perp	-0	?	-0	+0	?	?	?
?	\perp	?	?	?	?	?	?	?

==	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp
1	\perp	1	0	+0	0	+0	0	+0
0	\perp	0	1	0	0	+0	+0	+0
+	\perp	+0	0	+0	0	+0	0	+0
-	\perp	0	0	0	+0	0	+0	+0
+0	\perp	+0	+0	+0	+0	+0	+0	+0
-0	\perp	0	+0	+0	+0	+0	+0	+0
?	\perp	+0	+0	+0	+0	+0	+0	+0

>	\perp	1	0	+	-	+0	-0	?
\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp	\perp
1	\perp	0	1	0	1	+0	1	+0
0	\perp	0	0	0	1	0	+0	+0
+	\perp	+0	1	+0	1	+0	1	+0
-	\perp	0	0	0	+0	0	+0	+0
+0	\perp	+0	+0	+0	1	+0	+0	+0
-0	\perp	0	+0	0	+0	+0	+0	+0
?	\perp	+0	+0	+0	+0	+0	+0	+0

Monotonicity

For at kontrollere om vores definitioner af de seks operatører er monotone har vi taget nogle stikprøver og kontrolleret dem. Vi har valgt ikke at kontrollere alle kombinationer, da dette vil tage for lang tid. Her er et par eksempler på kontrollen.

$$0 \sqsubseteq -0 \wedge 1 \sqsubseteq +0 \Rightarrow 0 \overline{0p} \ 1 \sqsubseteq -0 \overline{0p} +0 \quad (1)$$

Her kontrollerer vi så for de forskellige operatører:

$$\begin{aligned} == & : 0 \sqsubseteq +0 \\ + & : 1 \sqsubseteq ? \\ / & : 0 \sqsubseteq ? \\ * & : 0 \sqsubseteq -0 \\ - & : - \sqsubseteq -0 \\ > & : 0 \sqsubseteq +0 \end{aligned} \quad (2)$$

Hvor det ses at alle er monotone. Samme kontrol burde laves for alle kombinationer af input, dog helst automatisk med en $O(n^3)$ algoritme.

Exercise 7.1

Se bagerste sider.

Part C

For at udvide Sign Analysis til interprocedural analysis vil vi erstatte laticen *Sign* til $C \mapsto \text{Sign}$, så vi får den fulde lattice:

$$\text{Vars} \mapsto C \mapsto \text{Sign}$$

Vi vælger C til at være call string, som beskrevet på slides. På denne måde kan vi slå variable op, og afhængigt af konteksten få et sign.

Når vi kalder en funktion slår vi parameterværdierne op i den nuværende kontekst, forlænger call string der gives med, og tilføjer værdierne på input parametrener til den nye kontekst.

Når vi returnerer tager man konteksten der er 'et kald mindre', og udfører en assignment på returnværdien og variabelen i den kalende funktions kontekst.

Ved at have en kontekst kan vi skelne variable fra hinanden, selvom de optræder i rekursive kald. Vi vælger dog at begrænse længden af call string'en, for at sikre at analysen slutter.