The Calculational Design of a Generic Abstract Interpreter

Corrigendum, April 12, 2004

Patrick COUSOT
LIENS, Département de Mathématiques et Informatique
École Normale Supérieure, 45 rue d'Ulm, 75230 Paris cedex 05, France

Section 8.7, page 447

The backward ternary substraction operation $-^{\triangleleft}$ is de–ned as

$$-^{\triangleleft}(q_1, q_2, p) \;\triangleq\; \text{let } (r_1, r_2) = -^{\triangleleft}(q_1, -^{\triangleright}(q_2), p) \text{ in } (r_1, -^{\triangleright}(r_2))\;.$$

should be:

The backward ternary substraction operation $-^{\triangleleft}$ is de–ned as

$$-^{\triangleleft}(q_1, q_2, p) \;\triangleq\; \text{let } (r_1, r_2) = +^{\triangleleft}(q_1, -^{\triangleright}(q_2), p) \text{ in } (r_1, -^{\triangleright}(r_2))\;.$$

Section 9.2, page 449

In equations (46),

$$b_1 \,\underline{\mathtt{b}}\, b_2 \;\triangleq\; b_1 \,\mathtt{b}\, i_2\;.$$

should be:

$$b_1 \,\underline{\mathtt{b}}\, b_2 \;\triangleq\; b_1 \,\mathtt{b}\, b_2\;.$$

Section 10.3, page 454

The calculational design of the abstract equality operation $\check{\doteq}$ does not depend upon the speci–c choice of L

$$
\begin{array}{ll}
 & \alpha^2(\{\langle i_1,\ i_2\rangle \mid i_1 \in \gamma(p_1)\cap \mathbb{I} \wedge i_2 \in \gamma(p_2)\cap \mathbb{I} \wedge i_1 \underline{=} i_2 = \mathrm{tt}\}) \\
 & \quad \wr \text{def. (45) of } \underline{=} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1)\cap\gamma(p_2)\cap\mathbb{I}\}) \\
\sqsubseteq^2 & \quad \wr \gamma\circ\alpha \text{ is extensive (6) and } \alpha^2 \text{ is monotone} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1)\cap\gamma(p_2)\cap\gamma(\alpha(\mathbb{I}))\}) \\
 & \quad \wr \gamma \text{ preserves meets} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}))\}) \\
 & \quad \wr \text{def. (12) of } \gamma^2 \wr \\
 & \alpha^2(\gamma^2(\langle p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}),\ p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I})\rangle)) \\
\sqsubseteq^2 & \\
 & \quad \wr \alpha^2\circ\gamma^2 \text{ is reductive and let notation} \wr \\
 & \text{let } p = p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}) \text{ in } \langle p,\ p\rangle \\
\sqsubseteq^2 & \quad \wr \text{def. (36) of } ?^{\triangleright} \wr \\
 & \text{let } p = p_1 \sqcap p_2 \sqcap ?^{\triangleright} \text{ in } \langle p,\ p\rangle \\
= & \quad \wr \text{by de–ning } \check{\doteq} \stackrel{\Delta}{=} \text{let } p = p_1 \sqcap p_2 \sqcap ?^{\triangleright} \text{ in } \langle p,\ p\rangle \wr \\
 & \check{\doteq}\,.
\end{array}
$$

_____ should be:

The calculational design of the abstract equality operation $\check{\doteq}$ does not depend upon the speci–c choice of L

$$
\begin{array}{ll}
 & \alpha^2(\{\langle i_1,\ i_2\rangle \mid i_1 \in \gamma(p_1)\cap \mathbb{I} \wedge i_2 \in \gamma(p_2)\cap \mathbb{I} \wedge i_1 \underline{=} i_2 = \mathrm{tt}\}) \\
= & \quad \wr \text{def. (45) of } \underline{=} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1)\cap\gamma(p_2)\cap\mathbb{I}\}) \\
\sqsubseteq^2 & \quad \wr \gamma\circ\alpha \text{ is extensive (6) and } \alpha^2 \text{ is monotone} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1)\cap\gamma(p_2)\cap\gamma(\alpha(\mathbb{I}))\}) \\
= & \quad \wr \gamma \text{ preserves meets} \wr \\
 & \alpha^2(\{\langle i,\ i\rangle \mid i \in \gamma(p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}))\}) \\
= & \quad \wr \text{def. (12) of } \gamma^2 \wr \\
 & \alpha^2(\gamma^2(\langle p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}),\ p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I})\rangle)) \\
\sqsubseteq^2 & \quad \wr \alpha^2\circ\gamma^2 \text{ is reductive and let notation} \wr \\
 & \text{let } p = p_1 \sqcap p_2 \sqcap \alpha(\mathbb{I}) \text{ in } \langle p,\ p\rangle \\
\sqsubseteq^2 & \quad \wr \text{def. (36) of } ?^{\triangleright} \wr \\
 & \text{let } p = p_1 \sqcap p_2 \sqcap ?^{\triangleright} \text{ in } \langle p,\ p\rangle \\
= & \quad \wr \text{by de–ning } \check{\doteq} \stackrel{\Delta}{=} \text{let } p = p_1 \sqcap p_2 \sqcap ?^{\triangleright} \text{ in } \langle p,\ p\rangle \wr \\
 & \check{\doteq}\,.
\end{array}
$$

_____ Section Theorem 1, page 456 ______________________________

If $\langle M,\ \preceq\rangle$ is poset, $f \in M \mapsto M$ is monotone and reductive, …

_____ should be:

If $\langle M,\ \preceq\rangle$ is poset, $f \in M \mapsto M$ is monotone and idempotent, …

_____ Section Proof of Theorem 1, page 456 ______________________________

$$
\begin{array}{ll}
 & \alpha \circ f \circ \gamma(x) \\
\sqsubseteq & \quad \wr f \text{ reductive (so that } f(f(\gamma(x))) \sqsubseteq f(\gamma(x))\text{) and } \alpha \text{ monotone} \wr \\
 & \alpha \circ f \circ f \circ \gamma(x)
\end{array}
$$

should be:

$$
\begin{array}{ll}
 & \alpha \circ f \circ \gamma(x) \\
= & \quad \wr f \text{ idempotent} \wr \\
 & \alpha \circ f \circ f \circ \gamma(x)
\end{array}
$$

Section 12.5, –gure 12, page 462

Equation (75):

$$
Program\ P = S\ ;;
$$

$$
\frac{\langle \ell,\ \rho \rangle \models\!\!=\![\![S]\!]\!\!\Longrightarrow \rho}{\langle \ell',\ \rho' \rangle \models\!\!=\![\![S\ ;;]\!]\!\!\Longrightarrow \langle \ell',\ \rho' \rangle}\ . \tag{1}
$$

should be:

$$
Program\ P = S\ ;;
$$

$$
\frac{\langle \ell,\ \rho \rangle \models\!\!=\![\![S]\!]\!\!\Longrightarrow \rho'}{\langle \ell,\ \rho \rangle \models\!\!=\![\![S\ ;;]\!]\!\!\Longrightarrow \langle \ell',\ \rho' \rangle}\ . \tag{2}
$$

Section 12.8, page 470

$$
\begin{array}{lll}
\tau^\star[\![C]\!] & = & \tau[\![S]\!]^0 \cup (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^+ \cup (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^B \circ \tau[\![S]\!]^\star \\
 & & \cup\ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^{\bar{B}} \cup \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \\
 & & \cup\ \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^B \circ \tau[\![S]\!]^\star \\
 & & \cup\ \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^{\bar{B}} \\
 & = & (1_{\Sigma[\![P]\!]} \cup \tau[\![S]\!]^\star \circ \tau^R) \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ (1_{\Sigma[\![P]\!]} \cup \tau^B \circ \tau[\![S]\!]^\star \cup \tau^{\bar{B}})\ .
\end{array}
$$

should be:

$$
\begin{array}{lll}
\tau^\star[\![C]\!] & = & \tau[\![S]\!]^0 \cup (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^+ \cup (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^B \circ \tau[\![S]\!]^\star \\
 & & \cup\ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^{\bar{B}} \cup \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \\
 & & \cup\ \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^B \circ \tau[\![S]\!]^\star \\
 & & \cup\ \tau[\![S]\!]^\star \circ \tau^R \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ \tau^{\bar{B}} \\
 & & \cup\ \tau[\![S]\!]^\star \\
 & = & ((1_{\Sigma[\![P]\!]} \cup \tau[\![S]\!]^\star \circ \tau^R) \circ (\tau^B \circ \tau[\![S]\!]^\star \circ \tau^R)^\star \circ (1_{\Sigma[\![P]\!]} \cup \tau^B \circ \tau[\![S]\!]^\star \cup \tau^{\bar{B}})) \cup \tau[\![S]\!]^\star\ .
\end{array}
$$

Section Figure 13, page 476

In equations (94),

- $$\tau^\star[\![\texttt{while}\ B\ \texttt{do}\ S\ \texttt{od}]\!] = (1_{\Sigma[\![P]\!]} \cup \tau^\star[\![S]\!] \circ \tau^R) \circ (\tau^B \circ \tau^\star[\![S]\!] \circ \tau^R)^\star \circ (1_{\Sigma[\![P]\!]} \cup \tau^B \circ \tau^\star[\![S]\!] \cup \tau^{\bar{B}})$$

should be:

- $$\tau^\star[\![\texttt{while}\ B\ \texttt{do}\ S\ \texttt{od}]\!] = ((1_{\Sigma[\![P]\!]} \cup \tau^\star[\![S]\!] \circ \tau^R) \circ (\tau^B \circ \tau^\star[\![S]\!] \circ \tau^R)^\star \circ (1_{\Sigma[\![P]\!]} \cup \tau^B \circ \tau^\star[\![S]\!] \cup \tau^{\bar{B}})) \cup (\tau^\star[\![S]\!])$$

Section 13.9, page 496

The third example shows the imprecision on reachability resulting from the choice to have $\gamma()\,\mathrm{BOT} \neq \emptyset)$.

should be:

The third example shows the imprecision on reachability resulting from the choice to have $\gamma(\mathrm{BOT}) \neq \emptyset)$.

Section "References", page 504

[18] P. Cousot and R. Cousot. Re–ning model checking by abstract interpretation. *Automated Software Engineering Journal, special issue on Automated Software Analysis*, 6(1), 1999. To appear.

should be:

[18] P. Cousot and R. Cousot. Re–ning model checking by abstract interpretation. *Automated Software Engineering Journal, special issue on Automated Software Analysis*, 6(1):69–95, 1999.

End of corrigendum