

Cours « Interprétation abstraite :
application à la vérification et
à l'analyse statique »

Corrigé de l'examen du 17 novembre 2006

P. COUSOT

Quête 1 :

Les conditions syntaxiques sont données
par la grammaire attribuée :

$$\begin{aligned} C ::= & L : \text{skip} & C.E &= \{L\} \\ & | \quad L : X := E & C.E &= \{L\} \\ & | \quad L : \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi} \end{aligned}$$

$$C.E = \{L\} \cup C_1.E \cup C_2.E$$

$$L \notin C_1.E \cup C_2.E$$

$$C_1.E \cap C_2.E = \emptyset$$

$$| \quad L : \text{while } E \text{ do } C_1 \text{ od}$$

$$C.E = \{L\} \cup C_1.E$$

$$L \notin C_1.E$$

$$| \quad C_1 ; \dots ; C_n \quad C.E = \bigcup_{i=1}^n C_i.E$$

$$\forall i, j \in [1, n] : i \neq j \Rightarrow C_i.E \cap C_j.E = \emptyset$$

$$P ::= C ; L :$$

$$P.E = \{L\} \cup C.E$$

$$L \notin C.E$$

L'ensemble des variables du programme est donné par la grammaire attribuée suivante:

$$\begin{array}{ll}
 E ::= 1 & E.V = \emptyset \\
 | X & E.V = \{X\} \\
 | E_1 - E_2 & E.V = E_1.V \cup E_2.V
 \end{array}$$

$$\begin{array}{ll}
 C ::= L; \text{skip} & C.V = \emptyset \\
 | L; X := E & C.V = \{X\} \cup E.V \\
 | \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi} & C.V = E.V \cup C_1.V \cup C_2.V \\
 | \text{while } E \text{ do } C_1 \text{ fi} & C.V = E.V \cup C_1.V \\
 | C_1; \dots; C_n & C.V = \bigcup_{i=1}^n C_i.V
 \end{array}$$

$$\begin{array}{ll}
 P ::= C; L & P.V = C.V
 \end{array}$$

L'ensemble $P.\Sigma$ des états d'un programme P est

$$P.L \times (P.R \rightarrow \mathbb{Z}) \quad P.R = P.V \rightarrow \mathbb{Z}$$

de la forme $\langle L, p \rangle$ où $L \in P.L$ est un point de programme et $p \in (P.V \rightarrow \mathbb{Z})$ indique pour chaque variable $X \in P.V$ du programme P sa valeur entière $p(X) \in \mathbb{Z}$.

La sémantique des expressions E est donnée par

$$S[1]p = 1$$

$$S[X]p = p(X)$$

$$S[E_1 - E_2]p = S[E_1]p - S[E_2]p$$

On définit les étiquettes avant $C.at$, et dans $C.in$ et après $C.after$ une commande C par la grammaire attribuée suivante :

$C ::= L.skip$

$C.at = L$

$C.in = \emptyset$

| $L: X := E$

$C.at = L$

$C.in = \emptyset$

| $L: \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi}$

$C.at = L$

$C.in = \{C_1.at\} \cup C_1.in \cup \{C_2.at\} \cup C_2.in$

$C_1.after = C.after$

$C_2.after = C.after$

| $L: \text{while } E \text{ do } C_1 \text{ od}$

$C.at = L$

$C.in = \{C_1.at\} \cup C_1.in$

$C_1.after = L$

| $C_1; \dots; C_n$

$C.at = C_1.at$

$\bigwedge_{i=1}^{n-1} C_i.after = C_{i+1}.at$

$C.in = C_1.in \cup$

$\bigcup_{i=2}^n \{C_i.at\} \cup C_i.in$

$P := C.L$

$P.at = C.at$

$P.in = C.in$

$P.after = L$

$C.after = L$

La sémantique de transition est donnée par la grammaire attribuée suivante :

$$C ::= L : \text{skip} \quad C.T = \{ \langle L, p \rangle \rightarrow \langle C.\text{after}, p \rangle \mid p \in C.R \} \rightarrow \mathbb{Z}$$

$$\mid L : X := E \quad C.T = \{ \langle L, p \rangle \rightarrow \langle C.\text{after}, p[X \leftarrow S[E]p] \rangle \mid p \in C.R \}$$

$$\mid L : \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi}$$

$$C.T = \{ \langle L, p \rangle \rightarrow \langle C_1.\text{at}, p \rangle \mid p \in C.R \wedge S[E]p \neq 0 \} \\ \cup \{ \langle L, p \rangle \rightarrow \langle C_2.\text{at}, p \rangle \mid p \in C.R \wedge S[E]p = 0 \} \\ \cup C_1.T \cup C_2.T$$

$$C_1.R = C.R$$

$$C_2.R = C.R$$

$$\mid L : \text{while } E \text{ do } C_1 \text{ od}$$

$$C.T = \{ \langle L, p \rangle \rightarrow \langle C.\text{after}, p \rangle \mid p \in C.R \wedge S[E]p \neq 0 \} \\ \cup \{ \langle L, p \rangle \rightarrow \langle C_1.\text{at}, p \rangle \mid p \in C.R \wedge S[E]p = 0 \} \\ \cup C_1.T$$

$$C_1.R = C.R$$

$$P ::= C ; L$$

$$P.T = C.T$$

$$C.R = P.R = (P.V \rightarrow \mathbb{Z})$$

Question 2

On définit la sémantique de traces finies ou infinies en définissant

$$P ::= C, L \quad P.L \times P.R \quad \text{ou} \quad P.R =$$

$$P.\Sigma = P.L \times P.R$$

$$P.R = P.V \rightarrow \mathbb{Z}$$

$$C.\Sigma = P.\Sigma$$

$$P.\Sigma^\infty = C.\Sigma^\infty$$

$$C ::= L : \text{skip} \quad C.\Sigma^\infty = \{s s' \mid s \rightarrow s' \in C.T\}$$

$$| L : X := E \quad C.\Sigma^\infty = \{s s' \mid s \rightarrow s' \in C.T\}$$

$$| L : \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi}$$

$$C.\Sigma^\infty = \{ \langle L, p \rangle s \sigma \mid \langle L, p \rangle \rightarrow s \in C.T \wedge s \sigma \in C_1.\Sigma^\infty \cup C_2.\Sigma^\infty \}$$

$$C_1.\Sigma = C.\Sigma$$

$$C_2.\Sigma = C.\Sigma$$

$$| L : \text{while } E \text{ do } C_1 \text{ od}$$

$$C.\Sigma^\infty = \text{pp}_{\text{c}} \text{ } \mathbb{N} \times \{ \langle L, p \rangle \langle C.\text{after}, p \rangle \mid p \in C.R \wedge S[E] p = 0 \}$$

$$\cup \{ \langle L, p \rangle \langle C_1.\text{at}, p \rangle s s' \mid p \in C.R \wedge S[E] p \neq 0 \wedge \langle C_1.\text{at}, p \rangle s s' \in C_1.\Sigma^\infty \wedge s s' \in X \}$$

$$\cup \{ \langle L, p \rangle \langle C_1.\text{at}, p \rangle \sigma \mid p \in C.R \wedge S[E] p \neq 0 \wedge \langle C_1.\text{at}, p \rangle \sigma \in C_1.\Sigma^\infty \cap (\mathbb{N} \rightarrow C.\Sigma) \}$$

$$C_1.\Sigma = C.\Sigma$$

$$| C_1 ; \dots ; C_n$$

$$C_i \cdot \Sigma = C \cdot \Sigma \text{ pour } i = 1, \dots, n$$

$$C \cdot \Sigma^\infty = \{ s_1 \sigma_1 s_2 \dots s_n \sigma_n s_{n+1} \mid \forall i \in [1, n] : \\ s_i \sigma_i s_{i+1} \in C_i \cdot \Sigma^\infty \} \quad (\text{traces finies})$$

$$\cup \{ s_1 \sigma_1 s_2 \dots s_j \sigma_j \mid \forall i \in [1, j-1] : \\ s_i \sigma_i s_{i+1} \in C_i \cdot \Sigma^\infty \wedge s_j \sigma_j \in C_j \cdot \Sigma^\infty \cap (\Omega \rightarrow C \cdot \Sigma) \} \\ (\text{traces infinies})$$

L'ordre du pont fixe pour une commande C est

$$C \cdot \Sigma^+ = C \cdot \Sigma^\infty \cap \bigcup_{n \geq 0} \{ [0, n[\rightarrow C \cdot \Sigma \}$$

$$C \cdot \Sigma^\omega = C \cdot \Sigma^\infty \cap \Omega \rightarrow C \cdot \Sigma$$

$$T_1 \sqsubseteq_c T_2 = (T_1 \cap C \cdot \Sigma^+) \subseteq (T_2 \cap C \cdot \Sigma^+) \wedge \\ (T_1 \cap C \cdot \Sigma^\infty) \supseteq (T_2 \cap C \cdot \Sigma^\infty).$$

Question 3

α est un morphisme complet pour l'union
 $\alpha(\bigcup X_i) = \bigcup \alpha(X_i)$ et donc l'adjoint
 inférieur d'un correspondance de Galois
 donnée par :

$$\langle \mathcal{F}(\Sigma^\infty), \subseteq \rangle \xrightleftharpoons[\alpha]{\delta} \langle \mathcal{F}(\Sigma) \rightarrow \mathcal{F}(\Sigma), \subseteq \rangle$$

où $\subseteq$ est l'inclusion point par point.

Question 4

On pose $C.wlp = \alpha_C(C.\Sigma^\infty)$.

Par cas :

- $C \equiv L : \text{skip}$.

$$\begin{aligned} & \alpha(C.\Sigma^\infty) \\ &= \lambda R. \{p \mid \exists p' \in R : \exists \sigma : \langle C.at, p \rangle \sigma \langle C.after, p' \rangle \in C.\Sigma^+\} \\ &= \lambda R. \{p \mid \exists p' \in R : \langle C.at, p \rangle \rightarrow \langle C.after, p' \rangle \in C.T\} \\ &= \lambda R. \{p \mid \exists p' \in R : p' = p\} \\ &= \lambda R. R \end{aligned}$$

- $C \equiv X := E$

$$\begin{aligned} & \alpha(C.\Sigma^\infty) \\ &= \lambda R. \{p \mid \exists p' \in R : \exists \sigma : \langle C.at, p \rangle \sigma \langle C.after, p' \rangle \in C.\Sigma^+\} \\ &= \lambda R. \{p \mid \exists p' \in R : \langle C.at, p \rangle \rightarrow \langle C.after, p' \rangle \in C.T\} \\ &= \lambda R. \{p \mid \exists p' \in R : p' = p[x \leftarrow S[E]p]\} \\ &= \lambda R. \{p \mid p[x \leftarrow S[E]p] \in R\} \end{aligned}$$

- $C \equiv \text{if } E \text{ then } C_1 \text{ else } C_2 \text{ fi}$

$$\begin{aligned} & \alpha(C.\Sigma^\infty) \\ &= \lambda R. \{p \mid \exists p' \in R : \exists \sigma : \langle C.at, p \rangle \sigma \langle C.after, p' \rangle \in C.\Sigma^+\} \\ &= \lambda R. \{p \mid \exists p' \in R : \exists s, \sigma : \langle C.at, p \rangle \rightarrow s \in C.T \wedge \\ & \quad \wedge \sigma \langle C.after, p' \rangle \in C_1.\Sigma^\infty \cup C_2.\Sigma^\infty\} \\ &= \lambda R. \{p \mid \exists p' \in R : S[E]p \neq 0 \wedge \langle C_1.at, p \rangle \sigma \langle C.after, p' \rangle \in \\ & \quad C_1.\Sigma^\infty \cup C_2.\Sigma^\infty\} \cup \{\text{idem si faux}\} \end{aligned}$$

Du fait que les traces de C_i commencent en $C_i.at$

$$\begin{aligned} &= \lambda R. \{p \mid \exists p' \in R : S[E]p \neq 0 \wedge \langle C_1.at, p \rangle \sigma \langle C.after, p' \rangle \in C_1.\Sigma^\infty\} \\ & \quad \cup \{\text{idem si faux}\} \end{aligned}$$

Du fait que $C_1.after = C.after$

$$= \downarrow R. \{ p \mid \exists p' \in R : \exists \sigma : S[E] p \neq 0 \wedge \langle C_1.at, p \rangle \sigma \langle C_1.after, p' \rangle \in C_1.\Sigma^\infty \} \cup \{ \text{idem si faux} \}$$

$$= \downarrow R. \{ p \mid S[E] p \neq 0 \wedge p \in \{ p \mid \exists p' \in R : \exists \sigma : \langle C_1.at, p \rangle \sigma \langle C_1.after, p' \rangle \in C_1.\Sigma^\infty \} \} \cup \{ \text{idem si faux} \}$$

$$= \downarrow R. \{ p \mid S[E] p \neq 0 \wedge p \in \alpha_{C_1}(C_1.\Sigma^\infty)R \} \cup \{ \text{idem si faux} \}$$

et donc par hypothèse d'inducte :

$$= \downarrow R. \{ p \mid S[E] p \neq 0 \wedge p \in C_1.wlp(R) \} \cup \{ p \mid S[E] p = 0 \wedge p \in C_2.wlp(R) \}$$

- Pour la boucle while on utilise le théorème de transfert de point fixe pour

$$F(X) = F_f(X) \cup F_i(X) \cup F_w(X)$$

ou

$$F_f(X) = \{ \langle L, p \rangle \langle C.after, p \rangle \mid S[E] p = 0 \}$$

$$F_i(X) = \{ \langle L, p \rangle \langle C_1.at, p \rangle \sigma \sigma' \mid S[E] p \neq 0 \wedge \langle C_1.at, p \rangle \sigma \sigma' \in C_1.\Sigma^\infty \wedge \sigma' \in X \}$$

$$F_w(X) = \{ \langle L, p \rangle \langle C_1.at, p \rangle \sigma \mid S[E] p \neq 0 \wedge \langle C_1.at, p \rangle \sigma \in C_1.\Sigma^\infty(\Omega \rightarrow C.\Sigma) \}$$

on observe que

$$\alpha_c(F_w(X)) = \downarrow R. \emptyset$$

et donc

$$\alpha_c(F(X)) = \alpha_c(F_f(X)) \cup \alpha_c(F_i(X))$$

puisque α est un morphisme pour $\cup$.

$$- \alpha_c(F_f(x)) \mid R$$

$$= \{p \mid \exists p' \in R : \exists \sigma : \langle c.at, p \rangle \sigma \langle c.after, p' \rangle \in F_f(x) \cap c.\Sigma^+\}$$

$$= \{p \mid p \in R \wedge \langle c.at, p \rangle \langle c.after, p \rangle \in c.\Sigma^+ \wedge S[\mathbb{E}] p = 0\}$$

$$= \{p \in R \mid S[\mathbb{E}] p = 0\}$$

$$- \alpha_c(F_i(x)) \mid R \quad \alpha_c(F_i(x)) \mid R \text{ est identique au}$$

$$= \{p \mid \exists p' \in R : \exists \sigma : \langle c.at, p \rangle \sigma \langle c.after, p' \rangle \in F_i(x) \cap c.\Sigma^+\}$$

$$= \{p \mid \exists p' \in R : \langle l, p \rangle \langle c_1.at, p \rangle \sigma s' \sigma' \langle c.after, p' \rangle \in F_i(x)\}$$

$$= \{p \mid \exists p' \in R : S[\mathbb{E}] p \neq \emptyset \wedge \langle c_1.at, p \rangle \sigma s' \in c_1.\Sigma^\infty \wedge s' \sigma' \langle c.after, p' \rangle \in X \cap c.\Sigma^+\}$$

Par induction, s' est en $c_1.after = c.at$ dans certain environnement intermédiaire p''

$$= \{p \mid \exists p' \in R : S[\mathbb{E}] p \neq \emptyset \wedge \langle c_1.at, p \rangle \sigma \langle c_1.after, p'' \rangle \in c_1.\Sigma^\infty \wedge \langle c.at, p'' \rangle \sigma' \langle c.after, p' \rangle \in X \cap c.\Sigma^+\}$$

$$= \{p \mid S[\mathbb{E}] p \neq 0 \wedge \exists p'' : p \in \{p \mid \exists p''' \in \{p''\} : \exists \sigma \langle c_1.at, p \rangle \sigma \langle c_1.after, p''' \rangle \in c_1.\Sigma^\infty \cap c_1.\Sigma^+\} \wedge$$

$$p'' \in \{p'' \mid \exists p' \in R : \exists \sigma' :$$

$$\langle c.at, p'' \rangle \sigma' \langle c.after, p' \rangle \in X \cap c.\Sigma^+\}\}$$

$$= \{p \mid S[\mathbb{E}] p \neq 0 \wedge \exists p'' : p \in \alpha_{c_1}(c_1.\Sigma^\infty)(\{p''\}) \wedge p'' \in \alpha_c(x)(R)\}$$

par hypothèse d'induction pour c_1

$$= \{p \mid S[\mathbb{E}] p \neq 0 \wedge \exists p'' : p \in c_1 \circ \omega_p(\{p''\}) \wedge p'' \in \alpha_c(x)(R)\}$$

On remarque que

$$C_1.wlp = \alpha_{C_1}(C_1.\Sigma^\omega)$$

est, d'après la définition de α_{C_1} , un morphisme complet pour elms et donc

$$= \{p \mid S[E]p \neq 0 \wedge p \in C_1.wlp(\alpha_C(X)(R))\}$$

De ce fait en posant :

$$F^\#(X) = \lambda R. \{p \in R \mid S[E]p = 0\} \cup \{p \mid S[E]p \neq 0 \wedge p \in C_1.wlp(X(R))\}$$

on a établi la propriété de commutation

$$F^\#(\alpha(X)) = \alpha(F(X))$$

et donc $\alpha(\ell_p^E F) = \ell_p^E F^\#$, ce qui donne

$$C.wlp = \ell_p^E \lambda X. \lambda R. \{p \in R \mid S[E]p = 0\} \cup \{p \in C_1.wlp(X(R)) \mid S[E]p \neq 0\}$$

- Finalement, pour la composition $C = C_1; \dots; C_n$, on a

$$\begin{aligned} & \alpha_C(C.\Sigma^\omega) R \\ &= \{p \mid \exists p' \in R : \exists \sigma : \langle C.at, p \rangle \sigma \langle C.after, p' \rangle \in C.\Sigma^\omega \cap C.\Sigma^+\} \\ &= \{p \mid \exists p' \in R : \langle C.at, p \rangle \sigma_1 \sigma_2 \dots \sigma_n \sigma_n \langle C.after, p' \rangle \in C.\Sigma^+\} \\ &= C.at = C_1.at \text{ et } C.after = C_1.after \end{aligned}$$

$$\begin{aligned} &= \{p \mid \exists p' \in R : \sigma_1 = \langle C_1.at, p \rangle \wedge \sigma_{n+1} = \langle C_n.after, p' \rangle \wedge \\ & \quad \forall i \in [1, n] : \sigma_i \sigma_{i+1} \in C_i.\Sigma^\omega \cap C_i.\Sigma^+\} \end{aligned}$$

--- par un argument similaire au cas du while

$$= \alpha_{C_n}(C_n.\Sigma^\omega) (\alpha_{C_1}(C_1.\Sigma^\omega)(R) \dots)$$

$$= C_n.wlp(\dots (C_1.wlp(R)) \dots)$$

En résumé, on a :

$$C ::= \text{L: skip} \quad C.\text{wlp} = \lambda R. R$$

$$| \text{L: } X := E \quad C.\text{wlp} = \lambda R. \{p \mid p[X \leftarrow S[E]p] \in R\}$$

$$| \text{L: if } E \text{ then } C_1 \text{ else } C_2 \text{ fi.}$$

$$C.\text{wlp} = \lambda R. \{p \mid S[E]p \neq 0 \wedge p \in C_1.\text{wlp}(R)\} \cup \{p \mid S[E]p = 0 \wedge p \in C_2.\text{wlp}(R)\}$$

$$| \text{L: while } E \text{ do } C_1 \text{ od}$$

$$C.\text{wlp} = \text{Cfp}_p \subseteq \lambda X. \lambda R. \{p \in R \mid S[E]p = 0\} \cup \{p \in C_1.\text{wlp}(X(R)) \mid S[E]p \neq 0\}$$

$$| C_1; \dots; C_n$$

$$C.\text{wlp} = C_n.\text{wlp} \circ \dots \circ C_1.\text{wlp}$$

On note que $C.\text{wlp} \in \mathcal{P}(C.R) \rightarrow \mathcal{P}(C.R)$

et que par définition de α , c'est un morphisme complet pour l'union.

Question 5

On prend le treillis des signes $\langle \mathcal{L}, \sqsubseteq \rangle$ comme donné par le diagramme de Hasse que l'on étend point par point à $\langle X \rightarrow \mathcal{L}, \sqsubseteq \rangle$ pour affecter un signe aux variables puis

$\bar{\alpha}$:

$$\langle \mathcal{P}(C.R) \xrightarrow{\cup} \mathcal{P}(C.R), \sqsubseteq \rangle \xrightleftharpoons[\alpha]{\sigma} \langle (X \rightarrow \mathcal{L})^n \rightarrow (X \rightarrow \mathcal{L}), \bar{\sqsubseteq} \rangle$$

ou $\bar{\sqsubseteq}$ étend $\sqsubseteq$ point par point

$$\alpha_c(x) = \lambda p. \alpha_c(x(\delta_c(p)))$$

$$\delta_c(p) = \{p' \mid \forall x \in C. \forall : p'(x) \in \delta(p(x))\}$$

δ défini dans $\uparrow$ δ de l'énonce

On procède par induction sur le langage

$$- C \equiv L : \text{skip}$$

$$\begin{aligned} & \alpha_c(C. \text{wlp}) \\ &= \lambda p. \alpha_c(C. \text{wlp}(\delta_c(p))) \\ &= \lambda p. \alpha_c(\delta_c(p)) \quad \text{car } C. \text{wlp} \text{ est l'identité} \\ &= \lambda p. p = C. \text{sign} \end{aligned}$$

$$- C \equiv L : X := E$$

$$\begin{aligned} & \alpha_c(C. \text{wlp}) \\ &= \lambda p. \alpha_c(C. \text{wlp}(\delta_c(p))) \\ &= \lambda p. \alpha_c(\{p' \mid p'[X \leftarrow S[E] p'] \in \delta_c(p)\}) \\ &= \lambda p. \alpha_c(\{p' \mid \forall y \in C. \forall : p'[X \leftarrow S[E] p'] y \in \delta(p(y))\}) \\ &= \lambda p. \alpha_c(\{p' \mid \forall y \neq X : p'(y) \in \delta(p(y)) \wedge \\ & \quad S[E] p' \in \delta(p(x))\}) \end{aligned}$$

Par cas, à nouveau

$$- \text{Si } E = 1, \text{ on a } 1 \in \delta(p(x)) \Leftrightarrow p(x) \in \{+, \tau\}$$

$$= \lambda p. \alpha_c(\{p' \mid \forall y \neq X : p'(y) \in \delta(p(y)) \wedge 1 \in \delta(p(x))\})$$

$$= \lambda p. \alpha_c(\{p' \mid \forall y \neq X : p'(y) \in \delta(p(y)) \wedge p(x) \in \{+, \tau\}\})$$

$$= \lambda p. (p(x) \notin \{+, \tau\} \text{ ? } \lambda z. \perp \text{ ? } p[x \leftarrow \tau])$$

- Si $E = X$, on a

$$\lambda p. \lambda c. (\{p' \mid \forall y \neq x : p'(y) \in \delta(p(y)) \wedge p'(x) \in \delta(p(x))\})$$

$$= \lambda p. p[x \leftarrow \tau]$$

- Si $E = z$, $z \neq x$, on a

$$\lambda p. \lambda c. (\{p' \mid \forall y \neq x : p'(y) \in \delta(p(y)) \wedge p'(z) \in \delta(p(x))\})$$

$$= \lambda p. p[z \leftarrow p(x)]$$

- Si $E = E_1 - E_2$, on peut transformer $X := E_1 - E_2$ en $X_1 := E_1$; $X_2 := E_2$; $X = X_1 - X_2$ où X_1 et X_2 sont deux nouvelles variables. De ce fait, il reste à étudier l'affectation $X = X_1 - X_2$.

Noter que cette solution a le mérite de la simplicité mais n'est pas la plus précise possible, voir par exemple une solution meilleure dans :

P. Cousot
The Computational Design of a Generic Abstract Interpreter.

In Computational System Design

IOS Press, 1999, H. Broy & R. Steinbrüggen
Editors.

- Si $X \notin \{X_1, X_2\}$, on connaît le signe de X, X_1, X_2 après l'évaluation de $X := X_1 - X_2$ et l'on cherche le signe de X, X_1, X_2 avant l'évaluation de $X := X_1 - X_2$ qui rend ce résultat possible.

- si c'est impossible, par exemple

$$X_1 := + \quad X_2 := - \quad X := -$$

après l'affectation, aucune valeur de X, X_1, X_2 ne permet d'obtenir ce résultat car

$$+ \ominus - = + \neq - \quad \text{avec} \quad \delta(+)\cap\delta(-) = \emptyset!$$

Dans ce cas on a $p(z) = \perp \quad \forall z \in \mathbb{X}$ avant.

- Dans les autres cas, c'est possible.

- Dans un premier sous-cas, il est possible d'améliorer la connaissance sur le signe de X_1 et/ou X_2 avant l'affectation par exemple, si

$$X_1 = 0 \quad X_2 = T \quad X = +$$

après l'affectation, alors comme $0 - x = -x$ on sait que $X_2 = -$ avant l'affectation

- Dans le cas général, toutes les combinaisons sont possibles, par exemple

$$X_1 = + \quad X_2 = - \quad X = T$$

aujourd'hui on ne sait rien de mieux avant l'affectation

Par l'affectation $X = X_1 - X_2$, il vient :

$$C \equiv L : X := X_1 - X_2$$

$$\alpha(C, w \in \mathcal{P})$$

$$= \lambda p. \mathcal{Q}_C(\{p' \mid \forall y \neq x : p'(y) \in \delta(p(y)) \wedge \exists [X_1 - X_2] p' \in \delta(p(x))\})$$

$$= \lambda p. \mathcal{Q}_C(\{p' \mid \forall y \neq x : p'(y) \in \delta(p(y)) \wedge p'(x_1) - p'(x_2) \in \delta(p(x))\})$$

— Dans le cas $x \notin \{x_1, x_2\}$ on a $p'(x_1) = p(x_1)$ et $p'(x_2) = p(x_2)$. Il faut donc étudier

$$\delta(B(x, y, z)) \supseteq \{ \langle u, v \rangle \mid u \in \delta(x) \wedge v \in \delta(y) \wedge u - v \in \delta(z) \}$$

Une manière simple est de construire la table de la règle des signes

		y				
x-y		+	-	0	+	-
x	+	+	+	+	+	+
	-	+	-	-	-	-
	0	+	+	0	-	-
	+	+	+	+	+	+
	-	+	-	-	-	-

et de démontrer pour les 25 cas $\langle x, y \rangle$ de la table qu'à chaque fois

$$\alpha(\{a - b \mid a \in \delta(x) \wedge b \in \delta(y)\}) \subseteq x \ominus y$$

--- à compléter ---

- Dans le cas où

$$C = L, \text{ if } \in \text{ the } C_1 \text{ et } C_2 \text{ si}$$

on a

$$\alpha_C(C, wlp)$$

$$= \lambda p. \alpha_C(C, wlp(\sigma_C(p)))$$

$$= \lambda p. \alpha_C(\{p \mid S[E] p \neq 0 \wedge p \in C_1, wlp(\sigma_C(p))\} \cup \{p \mid S[E] p = 0 \wedge p \in C_2, wlp(\sigma_C(p))\})$$

$$= \lambda \alpha_C \text{ est un morphisme complet pour l'union } S$$

$$\lambda p. \alpha_C(\{p \mid S[E] p \neq 0 \wedge p \in C_1, wlp(\sigma_C(p))\})$$

$$\sqcup \alpha_C(\{p \mid S[E] p = 0 \wedge p \in C_2, wlp(\sigma_C(p))\})$$

Pour choisir une solution simpliste, on peut ignorer le test. Par monnaie

$$\sqsupseteq \lambda p. \alpha_C(C_1, wlp(\sigma_C(p))) \sqcup \alpha_C(C_2, wlp(\sigma_C(p)))$$

Par définition de α_C et σ_C

$$= \lambda p. \alpha_{C_1}(C_1, wlp(\sigma_{C_1}(p))) \sqcup \alpha_{C_2}(C_2, wlp(\sigma_{C_2}(p)))$$

Par hypothèse d'inducte

$$\sqsupseteq C_1, \text{ sign } \sqcup C_2, \text{ sign.}$$

Pour une solution moins simpliste, on peut ignorer $S[E] p \neq 0$ mais restreindre les valeurs possibles des variables dans E telles que $S[E] p = 0$.

$$= \lambda p. \lambda c. \left(\left\{ p' \mid S[x]p' \neq 0 \wedge p' \in c_1. \text{wlp}(\tau_c(p)) \right\} \cup \left\{ p' \mid S[x]p' = 0 \wedge p' \in c_2. \text{wlp}(\tau_c(p)) \right\} \right)$$

$$= \lambda p. \lambda c. \left(\left\{ p' \mid p'(x) \neq 0 \wedge p' \in c_1. \text{wlp}(\tau_c(p)) \right\} \cup \left\{ p' \mid p'(x) = 0 \wedge p' \in c_2. \text{wlp}(\tau_c(p)) \right\} \right)$$

car τ_c est un morphisme complet pour l'union

$$\sqsubseteq \lambda p. \lambda c. \left(\left\{ p' \mid p'(x) \neq 0 \wedge p' \in \tau_{c_1}(\alpha_{c_1}(c_1. \text{wlp}(\tau_{c_1}(p)))) \right\} \cup \left\{ p' \mid p'(x) = 0 \wedge p' \in \tau_{c_2}(\alpha_{c_2}(c_2. \text{wlp}(\tau_{c_2}(p)))) \right\} \right)$$

Par hypothèse d'inductivité et notation

$$\sqsubseteq \lambda p. \lambda c. \left(\left\{ p' \mid p'(x) \neq 0 \wedge p' \in \tau_{c_1}(c_1. \text{sign}(p)) \right\} \cup \left\{ p' \mid p'(x) = 0 \wedge p' \in \tau_{c_2}(c_2. \text{sign}(p)) \right\} \right)$$

$$\sqsubseteq \lambda p. \overline{\mathbb{Z}}(c_1. \text{sign}(p)) \sqcup \mathbb{Z}(c_2. \text{sign}(p))$$

$$\stackrel{\Delta}{=} c. \text{sign}(p).$$

--- à compléter ---