Validation par analyse statique

Deuxième partie : Interprétation abstraite, cours 2/3

Pierre Roux

ONERA

Cours commun ENSEEIHT 3A et Master SRLC
2013-2014

Page du cours : `http://perso.ens-lyon.fr/pierre.roux/vas_2013_2014/`

Type de la sémantique concrète

La sémantique concrète d'un programme est de type

$$L \to \mathcal{P}(\mathbb{V} \to \mathbb{Z})$$

- une fonction qui à chaque point du programme (dans L)
- associe un ensemble d'états possibles de la mémoire
  - une fonction qui à chaque variable (dans $\mathbb{V}$)
  - associe sa valeur en mémoire (dans $\mathbb{Z}$)

Exemple

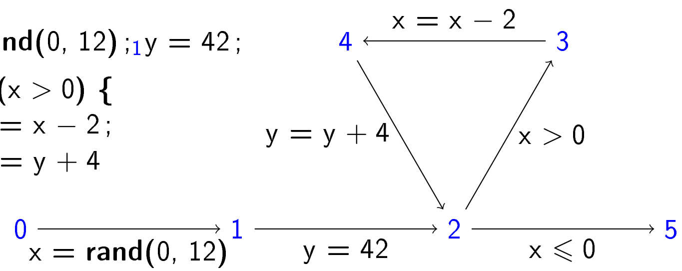
${}_0\mathsf{x} = \textbf{rand}(0, 12)\,;{}_1\mathsf{y} = 42\,;$

$\textbf{while}\ {}_2(\mathsf{x} > 0)\ \{$

$\quad {}_3\mathsf{x} = \mathsf{x} - 2\,;$

$\quad {}_4\mathsf{y} = \mathsf{y} + 4$

$\}_5$



$$\begin{aligned}
R_0 &= \mathbb{V} \to \mathbb{Z} \qquad\qquad (\mathbb{V} = \{x, y\}) \\
R_1 &= \{f \in (\mathbb{V} \to \mathbb{Z}) \mid f(x) \in [\![0, 12]\!]\} \\
R_2 &= \{f \mid f(x) \in [\![-1, 12]\!], f(y) \in [\![42, 66]\!] \cap 4\mathbb{Z} + 2, 2f(x) + f(y) \in [\![42, 66]\!]\} \\
R_3 &= \{f \mid f(x) \in [\![1, 12]\!], f(y) \in [\![42, 66]\!] \cap 4\mathbb{Z} + 2, 2f(x) + f(y) \in [\![42, 66]\!]\} \\
R_4 &= \{f \mid f(x) \in [\![-1, 10]\!], f(y) \in [\![42, 66]\!] \cap 4\mathbb{Z} + 2, 2f(x) + f(y) \in [\![38, 62]\!]\} \\
R_5 &= \{f \mid f(x) \in [\![-1, 0]\!], f(y) \in [\![42, 66]\!] \cap 4\mathbb{Z} + 2, 2f(x) + f(y) \in [\![42, 66]\!]\}
\end{aligned}$$

Abstraire la sémantique concrète

Rappels sur la sémantique concrète

Abstractions relationnelles ou non

Abstractions non relationnelles

Signes

Constantes

Intervalles

Exercices

Abstraire ? oui mais quoi ?

La sémantique concrète est incalculable, on veut la simplifier.
Mais que simplifier ?

- L est fini et on veut savoir ce qui se passe en chaque point
  $\Rightarrow$ on le garde à l'identique
- $\mathbb{V}$ est fini et on s'intéresse à toutes les variables
  $\Rightarrow$ on le garde à l'identique
- $\mathbb{Z}$ (et donc l'ensemble des fonctions $\mathbb{V} \to \mathbb{Z}$) est infini
  $\Rightarrow$ c'est ici qu'on va abstraire

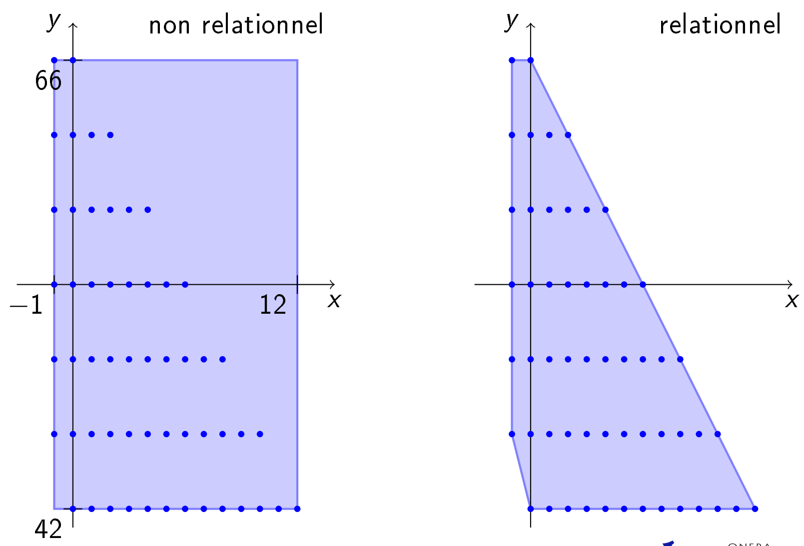
Comment abstraire $\mathcal{P}(\mathbb{V} \to \mathbb{Z})$?

Deux grandes solutions

- Abstraire $\mathcal{P}(\mathbb{V} \to \mathbb{Z})$ en $\mathbb{V} \to \mathcal{P}(\mathbb{Z})$ puis $\mathcal{P}(\mathbb{Z})$ en un $\mathcal{D}^\sharp$
  - *non relationnel* : les valeurs de x et y sont indépendantes
  - cette semaine
- Abstraire $\mathcal{P}(\mathbb{V} \to \mathbb{Z})$ directement en un $\mathcal{D}^\sharp$
  - *relationnel* : certaines combinaisons de x et y sont impossibles
  - \+ plus précis
  - − plus compliqué et plus coûteux
  - la semaine prochaine

Deux petits dessins valent mieux que de longs discours

Exemple précédent au point de programme 2 (invariant de boucle)



Domaine des signes

Définition

Treillis des signes $(\mathcal{D}^\sharp, \sqsubseteq^\sharp)$

$$\begin{tikzcd}[column sep=small] & \top & \\ \leqslant 0 \arrow[ur, dash] & & \geqslant 0 \arrow[ul, dash] \\ & \bot \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$$\begin{aligned} \gamma(\top) &= \mathbb{Z} \\ \gamma(\leqslant 0) &=]\!] -\infty, 0]\!] \\ \gamma(\geqslant 0) &= [\![0, +\infty [\![\\ \gamma(\bot) &= \emptyset \end{aligned}$$

Question

L'ordre $\sqsubseteq^\sharp$ ci dessus est il correct par rapport à l'ordre $\subseteq$ sur $\mathcal{P}(\mathbb{Z})$.

Rappel (correction de l'ordre abstrait par rapport au concret)

L'ordre $\sqsubseteq^\sharp$ est correct par rapport à l'ordre $\sqsubseteq$ si γ est croissante

$$\forall x^\sharp, y^\sharp \in \mathcal{D}^\sharp, \quad x^\sharp \sqsubseteq^\sharp y^\sharp \Rightarrow \gamma(x^\sharp) \sqsubseteq \gamma(y^\sharp)$$

Réponse

Domaine des signes, meilleure abstraction

$$\begin{tikzcd}[column sep=small] & \top & \\ \leqslant 0 \arrow[ur, dash] & & \geqslant 0 \arrow[ul, dash] \\ & \bot \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$$\begin{aligned} \gamma(\top) &= \mathbb{Z} \\ \gamma(\leqslant 0) &=]\!] -\infty, 0]\!] \\ \gamma(\geqslant 0) &= [\![0, +\infty [\![\\ \gamma(\bot) &= \emptyset \end{aligned}$$

Question

Toute partie S de $\mathbb{Z}$ (i.e. $S \in \mathcal{P}(\mathbb{Z})$) admet elle une meilleure abstraction dans ce domaine ?

Rappel (meilleure abstraction)

Une partie S de $\mathbb{Z}$ admet une meilleure abstraction si l'ensemble $\left\{ S^\sharp \in \mathcal{D}^\sharp \;\middle|\; S \subseteq \gamma\left(S^\sharp\right) \right\}$ a un minimum.

Réponse

Domaine des signes, meilleure abstraction (suite et fin)

Définition

On corrige en ajoutant un élément

$$\begin{tikzcd}[column sep=small] & \top & \\ \leqslant 0 \arrow[ur, dash] & & \geqslant 0 \arrow[ul, dash] \\ & 0 \arrow[ul, dash] \arrow[ur, dash] & \\ & \bot \arrow[u, dash] & \end{tikzcd}$$

$$\begin{aligned} \gamma(\top) &= \mathbb{Z} \\ \gamma(\leqslant 0) &=]\!] -\infty, 0]\!] \\ \gamma(\geqslant 0) &= [\![0, +\infty [\![\\ \gamma(0) &= \{ 0 \} \\ \gamma(\bot) &= \emptyset \end{aligned}$$

Remarques

- γ reste croissante.
- On a bien une correspondance de Galois avec

$$\alpha(S) = \begin{cases} \top & \text{si } \exists s, s' \in S, s < 0, s' > 0 \\ \leqslant 0 & \text{si } \forall s \in S, s \leqslant 0 \wedge \exists s \in S, s < 0 \\ \geqslant 0 & \text{si } \forall s \in S, s \geqslant 0 \wedge \exists s \in S, s > 0 \\ 0 & \text{si } S = \{ 0 \} \\ \bot & \text{si } S = \emptyset \end{cases}$$

Abstraction non relationnelle

D'une abstraction $\mathcal{D}^\sharp$ de $\mathcal{P}(\mathbb{Z})$,
on déduit une abstraction $\mathcal{D}^\sharp_{\mathrm{nr}}$ de $\mathcal{P}(\mathbb{V} \to \mathbb{Z})$,
en procédant point à point :

- $\mathcal{D}^\sharp_{\mathrm{nr}} = \mathbb{V} \to \mathcal{D}^\sharp$
- $x^\sharp \sqsubseteq^\sharp_{\mathrm{nr}} y^\sharp$ si pour tout $v \in \mathbb{V}$, $x^\sharp(v) \sqsubseteq^\sharp y^\sharp(v)$
- $\gamma_{\mathrm{nr}}\left(x^\sharp\right) = \left\{\rho \in (\mathbb{V} \to \mathbb{Z}) \;\middle|\; \forall v \in \mathbb{V}, \rho(v) \in \gamma\left(x^\sharp(v)\right)\right\}$
- $\alpha_{\mathrm{nr}}(x) = v \mapsto \alpha\left(\{\rho(v) \mid \rho \in x\}\right)$
- $\top_{\mathrm{nr}} = v \mapsto \top$
- $\bot_{\mathrm{nr}} = v \mapsto \bot$
- $x^\sharp \sqcup^\sharp_{\mathrm{nr}} y^\sharp = v \mapsto x^\sharp(v) \sqcup^\sharp y^\sharp(v)$
- $x^\sharp \sqcap^\sharp_{\mathrm{nr}} y^\sharp = v \mapsto x^\sharp(v) \sqcap^\sharp y^\sharp(v)$

Syntaxe de notre langage (rappel)

Syntaxe

stm ::= v = $expr$; | stm stm
  | **if** ($expr$ > 0) **{** stm **}** **else** **{** stm **}**
  | **while** ($expr$ > 0) **{** stm **}**

$expr$ ::= v | n | **rand**(n, n)
  | $expr + expr$ | $expr - expr$ | $expr \times expr$ | $expr / expr$

$v \in \mathbb{V}$, un ensemble de variables

$n \in \mathbb{Z}$ (on ne manipule que des entiers)

rand(n_1, n_2) représente le choix aléatoire d'un entier entre n_1 et n_2 (sert à simuler une entrée).

Domaine des signes, opérations arithmétiques abstraites

- $n^\sharp = \alpha(\{\, n \,\}) = \begin{cases} \leqslant 0 & \text{si } n < 0 \\ \geqslant 0 & \text{si } n > 0 \\ 0 & \text{si } n = 0 \end{cases}$
- $\mathbf{rand}^\sharp(n_1, n_2) = \alpha([\![n_1, n_2]\!]) = \begin{cases} \bot & \text{si } n_1 > n_2 \\ 0 & \text{si } n_1 = n_2 = 0 \\ \leqslant 0 & \text{sinon si } n_2 \leqslant 0 \\ \geqslant 0 & \text{sinon si } n_1 \geqslant 0 \\ \top & \text{sinon} \end{cases}$
- $x^\sharp +^\sharp y^\sharp = \alpha\left(\left\{x + y \;\middle|\; x \in \gamma(x^\sharp), y \in \gamma(y^\sharp)\right\}\right) =$

$+^\sharp$	$\top$	$\leqslant 0$	$\geqslant 0$	0	$\bot$
$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$
$\leqslant 0$	$\top$	$\leqslant 0$	$\top$	$\leqslant 0$	$\bot$
$\geqslant 0$	$\top$	$\top$	$\geqslant 0$	$\geqslant 0$	$\bot$
0	$\top$	$\leqslant 0$	$\geqslant 0$	0	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$

- ...

Domaine des signes, opérations arithmétiques abstraites (suite et fin)

Exercice

Compléter la table de la soustraction abstraite

$-^\sharp$	$\top$	$\leqslant 0$	$\geqslant 0$	0	$\bot$
$\top$					
$\leqslant 0$					
$\geqslant 0$					
0					
$\bot$					

Sémantique abstraite, expressions

Sémantique des expressions : $[\![e]\!]^\sharp_{\mathrm{E}} : (\mathbb{V} \to \mathcal{D}^\sharp) \to \mathcal{D}^\sharp$

$$
\begin{array}{ll}
[\![v]\!]^\sharp_{\mathrm{E}}(\rho) & = \rho(v) \\
[\![n]\!]^\sharp_{\mathrm{E}}(\rho) & = n^\sharp \\
[\![\mathbf{rand}(n_1, n_2)]\!]^\sharp_{\mathrm{E}}(\rho) & = \mathbf{rand}^\sharp(n_1, n_2) \\
[\![e_1 + e_2]\!]^\sharp_{\mathrm{E}}(\rho) & = [\![e_1]\!]^\sharp_{\mathrm{E}} +^\sharp [\![e_2]\!]^\sharp_{\mathrm{E}} \\
\dots &
\end{array}
$$

Remarque

Ça se calcule très bien.

Graphe de flot de contrôle (rappel)

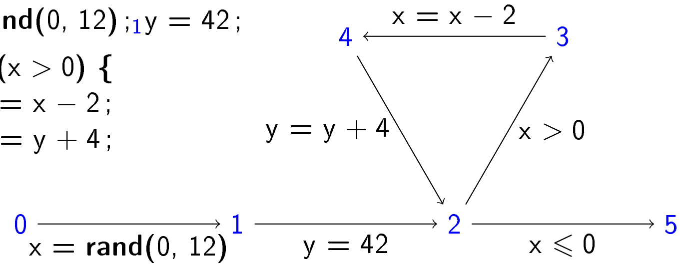
On étudie les graphes de flot de contrôle des programmes.

Définition

Un *graphe de flot de contrôle* (L, A) est composé d'un ensemble de points de programme L, d'un point d'entrée $0 \in L$ et d'arêtes $A \subseteq L \times com \times L$ avec :
$com ::= v = expr \mid expr > 0$

Exemple

$_0$x = **rand**(0, 12) ;$_1$y = 42 ;
while $_2$(x > 0) **{**
  $_3$x = x − 2 ;
  $_4$y = y + 4 ;
}$_5$



Sémantique abstraite, commandes

Sémantique des commandes : $[\![c]\!]^\sharp_{\mathrm{C}} : (\mathbb{V} \to \mathcal{D}^\sharp) \to (\mathbb{V} \to \mathcal{D}^\sharp)$

$$
[\![v = e]\!]^\sharp_{\mathrm{C}}(\rho) = \rho\left[v \mapsto [\![e]\!]^\sharp_{\mathrm{E}}\,\rho\right]
$$

$$
[\![e > 0]\!]^\sharp_{\mathrm{C}}(\rho) = \begin{cases} \rho\left[v \mapsto \rho(v) \sqcap^\sharp \alpha\left([\![1, +\infty[\![\right)\right] & \text{si } e = v \\ \rho & \text{sinon} \end{cases}
$$

...

Remarque

Ça se calcule toujours aussi bien.

Sémantique abstraite, programme

Sémantique des programmes : $[\![(L, A)]\!]^\sharp : L \to (\mathbb{V} \to \mathcal{D}^\sharp)$

C'est la plus petite solution (au sens de l'ordre abstrait $\sqsubseteq^\sharp_{\mathrm{nr}}$) du système

$$
\begin{cases} R^\sharp_0 = \mathbb{V} \to \top & \\ R^\sharp_{l'} = \displaystyle\bigsqcup^\sharp_{\mathrm{nr}\ (l,c,l') \in A} [\![c]\!]^\sharp_{\mathrm{C}}\left(R^\sharp_l\right) & l' \neq 0 \end{cases}
$$

Remarques

- Une telle solution existe (c.f. théorème de Knaster-Tarski).
- Ça semble un peu moins évident à calculer.

Sémantique abstraite, calcul effectif

Théorème

Si S est un treillis complet, f une fonction croissante sur ce treillis et si la suite $(f^n(\bot))_{n\in\mathbb{N}}$ est stationnaire

$$\exists N, \forall n \geqslant N, f^n(\bot) = f^N(\bot)$$

alors sa limite est le plus petit point fixe de f

$$\mathrm{lfp}\, f = f^N(\bot)$$

Démonstration.

- $f^N(\bot)$ est un point fixe : $f(f^N)(\bot) = f^{N+1}(\bot) = f^N(\bot)$;
- et c'est le plus petit : soit y un point fixe ($f(y) = y$), $\bot \sqsubseteq y$ donc par croissance de f, $f(\bot) \sqsubseteq f(y) = y$ et par récurrence immédiate $f^N(\bot) \sqsubseteq y$. □

Sémantique abstraite, calcul effectif (suite et fin)

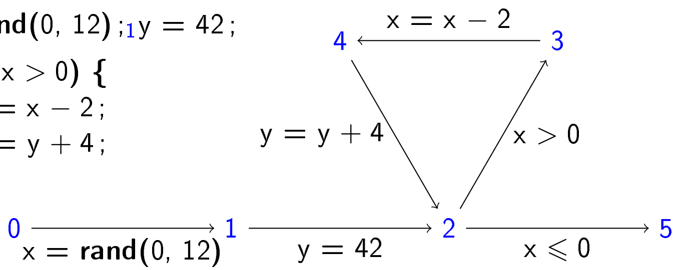
- $L \to (\mathbb{V} \to \mathcal{D}^\sharp)$ est un treillis complet (car $\mathcal{D}^\sharp$ en est un).
- La fonction $F^\sharp : (L \to (\mathbb{V} \to \mathcal{D}^\sharp)) \to (L \to (\mathbb{V} \to \mathcal{D}^\sharp))$

$$F^\sharp(R^\sharp) = \begin{cases} 0 & \mapsto \quad \top_{\mathrm{nr}} \\ l' & \mapsto \quad \displaystyle\bigsqcup^\sharp_{\mathrm{nr}\,(l,c,l')\in A} [\![c]\!]^\sharp_{\mathrm{C}}\,(R^\sharp(l)) \end{cases}$$

  est croissante et calculable.
- Donc si la suite $\left(F^{\sharp^n}(L \to \bot_{\mathrm{nr}})\right)_{n\in\mathbb{N}}$ est stationnaire, on a une méthode de calcul de la sémantique abstraite :
  1. On part de $R^{\sharp^0} := L \to \bot_{\mathrm{nr}}$;
  2. on calcule $R^{\sharp^{k+1}} := F^\sharp\left(R^{\sharp^k}\right)$;
  3. on retourne en 2 jusqu'à atteindre un point fixe.

Exemple de calcul du point fixe abstrait

$_0$x = **rand**(0, 12) ;$_1$y = 42 ;
while $_2$(x > 0) {
  $_3$x = x − 2 ;
  $_4$y = y + 4 ;
}$_5$



$$\begin{aligned}
R_0^{\sharp^{i+1}} &= \top_{\mathrm{nr}} \\
R_1^{\sharp^{i+1}} &= R_0^{\sharp^{i+1}}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp^{i+1}} &= R_1^{\sharp^{i+1}}\,[y \mapsto \geqslant 0] \sqcup^\sharp_{\mathrm{nr}} \\
&\quad R_4^{\sharp^{i}}\left[y \mapsto R_4^{\sharp^{i}}(y) +^\sharp (\geqslant 0)\right] \\
R_3^{\sharp^{i+1}} &= R_2^{\sharp^{i+1}}\left[x \mapsto R_2^{\sharp^{i+1}}(x) \sqcap^\sharp \geqslant 0\right] \\
R_4^{\sharp^{i+1}} &= R_3^{\sharp^{i+1}}\left[x \mapsto R_3^{\sharp^{i+1}}(x) -^\sharp (\geqslant 0)\right] \\
R_5^{\sharp^{i+1}} &= R_2^{\sharp^{i+1}}\left[x \mapsto R_2^{\sharp^{i+1}} \sqcap^\sharp \leqslant 0\right]
\end{aligned}$$

l	$R_l^{\sharp^0}$	$R_l^{\sharp^1}$	$R_l^{\sharp^2}$	$R_l^{\sharp^3}$
0	$(\bot,\bot)$	$(\top,\top)$	$(\top,\top)$	$(\top,\top)$
1	$(\bot,\bot)$	$(\geqslant 0,\top)$	$(\geqslant 0,\top)$	$(\geqslant 0,\top)$
2	$(\bot,\bot)$	$(\geqslant 0,\geqslant 0)$	$(\top,\geqslant 0)$	$(\top,\geqslant 0)$
3	$(\bot,\bot)$	$(\geqslant 0,\geqslant 0)$	$(\geqslant 0,\geqslant 0)$	$(\geqslant 0,\geqslant 0)$
4	$(\bot,\bot)$	$(\top,\geqslant 0)$	$(\top,\geqslant 0)$	$(\top,\geqslant 0)$
5	$(\bot,\bot)$	$(0,\geqslant 0)$	$(\leqslant 0,\geqslant 0)$	$(\leqslant 0,\geqslant 0)$

Correction et terminaison

Théorème (correction)

La sémantique abstraite est une *sur-approximation correcte* de la sémantique concrète : pour tout $l \in L$, on a

$$R_l \subseteq \gamma_{\mathrm{nr}}\left(R_l^\sharp\right)$$

Propriété (terminaison)

Le calcul du point fixe par itérations termine.

Démonstration.

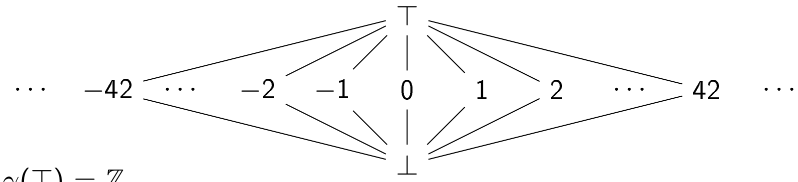
$\mathcal{D}^\sharp$ est fini donc $L \to \left(\mathbb{V} \to \mathcal{D}^\sharp\right)$ également

donc la suite croissante $\left(R^{\sharp^n}\right)_{n\in\mathbb{N}}$ est stationnaire. □

Domaine des constantes

Définition

Treillis des constantes $(\mathcal{D}^\sharp, \sqsubseteq^\sharp)$



$\gamma(\top) = \mathbb{Z}$
$\gamma(n) = \{ n \}$
$\gamma(\bot) = \emptyset$

Remarque

L'ordre $\sqsubseteq^\sharp$ ci dessus est correct par rapport à l'ordre $\subseteq$ sur $\mathcal{P}(\mathbb{Z})$.

Domaine des constantes, meilleure abstraction

Remarque

On a bien une correspondance de Galois avec

$$\alpha(S) = \begin{cases} \top & \text{si } \mathrm{card}(S) \geqslant 2 \\ n & \text{si } S = \{ n \} \\ \bot & \text{si } S = \emptyset \end{cases}$$

Domaine des constantes, opérations arithmétiques abstraites

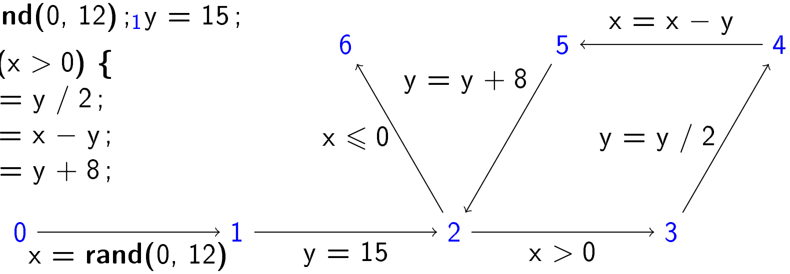
- $n^\sharp = \alpha(\{ n \}) = n$
- $\mathbf{rand}^\sharp(n_1, n_2) = \alpha([\![n_1, n_2]\!]) = \begin{cases} \top & \text{si } n_1 < n_2 \\ n_1 & \text{si } n_1 = n_2 \\ \bot & \text{si } n_1 > n_2 \end{cases}$
- $x^\sharp +^\sharp y^\sharp = \alpha\left(\left\{ x + y \;\middle|\; x \in \gamma(x^\sharp), y \in \gamma(y^\sharp) \right\}\right) =$

$$\begin{cases} \top & \text{si } x^\sharp = \top \text{ ou } y^\sharp = \top \\ n_1 + n_2 & \text{si } x^\sharp = n_1 \text{ et } y^\sharp = n_2 \\ \bot & \text{si } x^\sharp = \bot \text{ ou } y^\sharp = \bot \end{cases}$$

- ...

Exemple de calcul du point fixe abstrait

$_0$x = **rand**(0, 12) ;$_1$y = 15 ;
while $_2$(x > 0) {
  $_3$y = y / 2 ;
  $_4$x = x − y ;
  $_5$y = y + 8 ;
}$_6$



$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}}\\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \top]\\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto 15] \sqcup^\sharp_{\mathrm{nr}}\\
&\quad R_5^{\sharp\,i}\left[y \mapsto R_5^{\sharp\,i}(y) +^\sharp 8\right]\\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[y \mapsto R_3^{\sharp\,i+1}(y) /^\sharp 2\right]\\
R_5^{\sharp\,i+1} &= R_4^{\sharp\,i+1}\left[x \mapsto R_4^{\sharp\,i+1}(x) -^\sharp R_4^{\sharp\,i+1}(y)\right]\\
R_6^{\sharp\,i+1} &= R_2^{\sharp\,i+1}
\end{aligned}
$$

l	$R_l^{\sharp\,0}$	$R_l^{\sharp\,1}$	$R_l^{\sharp\,2}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$
2	$(\bot, \bot)$	$(\top, 15)$	$(\top, 15)$
3	$(\bot, \bot)$	$(\top, 15)$	$(\top, 15)$
4	$(\bot, \bot)$	$(\top, 7)$	$(\top, 7)$
5	$(\bot, \bot)$	$(\top, 7)$	$(\top, 7)$
6	$(\bot, \bot)$	$(\top, 15)$	$(\top, 15)$

Correction et terminaison

Théorème (correction, *pareil que pour les signes*)

La sémantique abstraite est une *sur-approximation correcte* de la sémantique concrète : pour tout $l \in L$, on a

$$R_l \subseteq \gamma_{\mathrm{nr}}\left(R_l^\sharp\right)$$

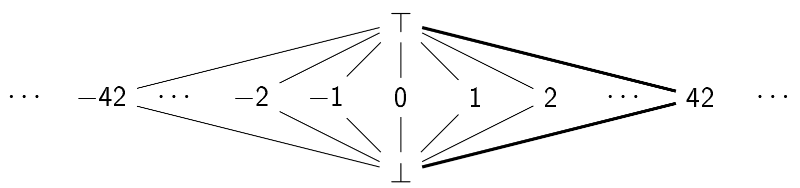
Propriété (terminaison)

Le calcul du point fixe par itérations termine.

Démonstration.

$\mathcal{D}^\sharp$ est infini mais n'a pas de chaîne strictement croissante infinie donc $L \to \left(\mathbb{V} \to \mathcal{D}^\sharp\right)$ non plus donc la suite croissante $\left(R^{\sharp\,n}\right)_{n\in\mathbb{N}}$ est stationnaire. □

Le treillis des constantes n'a pas de chaîne croissante infinie



Remarques

- Le domaine des constantes est souvent appelé Kildall.
- Il est utilisé en compilation pour faire du constant folding.
- Démo GCC.
- Le domaine des constantes est en fait le domaine des singletons de $\mathcal{P}(\mathbb{Z})$.
- Sur le même principe, on peut construire pour un $n \in \mathbb{N}$ quelconque un domaine « ensembles d'au plus n éléments ».

Domaine des intervalles

Définition

Treillis des intervalles $(\mathcal{D}^\sharp, \sqsubseteq^\sharp)$

$$
\begin{array}{ccccccc}
 & & &]\!\!]-\infty,+\infty[\![& & & \\
 & & & \vdots & & & \\
 & & \cdots & [\![-1,1]\!] & \cdots & & \\
 & \cdots & [\![-1,0]\!] & & [\![0,1]\!] & \cdots & \\
\cdots & [\![-1,-1]\!] & & [\![0,0]\!] & & [\![1,1]\!] & \cdots \\
 & & & \bot & & &
\end{array}
$$

$$
\begin{array}{ll}
\gamma(]\!\!]-\infty,+\infty[\![) & =]\!\!]-\infty,+\infty[\![\\
\gamma(]\!\!]-\infty,n]\!]) & =]\!\!]-\infty,n]\!] \\
\gamma([\![n,+\infty[\![) & = [\![n,+\infty[\![\\
\gamma([\![n_1,n_2]\!]) & = [\![n_1,n_2]\!] \\
\gamma(\bot) & = \emptyset
\end{array}
$$

Remarque

L'ordre est correct.

Domaine des intervalles, meilleure abstraction

Remarque

On a bien une correspondance de Galois avec

$$\alpha(S) = \begin{cases} [\![n_1, n_2]\!] & \text{avec } n_1 = \min S \text{ et } n_2 = \max S \\ \bot & \text{si } S = \emptyset \end{cases}$$

Domaine des intervalles, opérations arithmétiques abstraites

- $n^\sharp = \alpha(\{\, n \,\}) = [\![n, n]\!]$
- $\mathbf{rand}^\sharp(n_1, n_2) = \alpha([\![n_1, n_2]\!]) = \begin{cases} [\![n_1, n_2]\!] & \text{si } n_1 \leqslant n_2 \\ \bot & \text{si } n_1 > n_2 \end{cases}$
- $x^\sharp +^\sharp y^\sharp = \alpha\left(\left\{x + y \;\middle|\; x \in \gamma(x^\sharp), y \in \gamma(y^\sharp)\right\}\right) =$

$$\begin{cases} [\![a + c, b + d]\!] & \text{avec } x^\sharp = [\![a, b]\!] \text{ et } y^\sharp = [\![c, d]\!] \\ \bot & \text{si } x^\sharp = \bot \text{ ou } y^\sharp = \bot \end{cases}$$

- ...

Domaine des intervalles, opérations arithmétiques abstraites (suite et fin)

Exercice

- Donner la soustraction d'intervalles.
- Donner la multiplication d'intervalles.

Exemple de calcul du point fixe abstrait

$_0$x = **rand**(0, 12) ; $_1$y = 42 ;
while $_2$(x > 0) **{**
  $_3$x = x − 2 ;
  $_4$y = y + 4 ;
}$_5$

$$\begin{tikzcd}
 & & & 4 \arrow[dr, "y = y + 4"'] & & 3 \arrow[ll, "x = x - 2"'] & \\
0 \arrow[rr, "x = \mathbf{rand}(0,\ 12)"'] & & 1 \arrow[rr, "y = 42"'] & & 2 \arrow[ur, "x > 0"'] \arrow[rr, "x \leqslant 0"'] & & 5
\end{tikzcd}$$

$$\begin{aligned}
{R_0^\sharp}^{i+1} &= \top \\
{R_1^\sharp}^{i+1} &= {R_0^\sharp}^{i+1}\,[x \mapsto [\![0,12]\!]] \\
{R_2^\sharp}^{i+1} &= {R_1^\sharp}^{i+1}\,[y \mapsto [\![42,42]\!]] \sqcup^\sharp_{\mathrm{nr}} \\
&\quad {R_4^\sharp}^{i}\left[y \mapsto {R_4^\sharp}^{i}(y) +^\sharp [\![4,4]\!]\right] \\
{R_3^\sharp}^{i+1} &= {R_2^\sharp}^{i+1}\left[x \mapsto {R_2^\sharp}^{i+1}(x) \right. \\
&\qquad\qquad \left. \sqcap^\sharp [\![1,+\infty[\![\right] \\
{R_4^\sharp}^{i+1} &= {R_3^\sharp}^{i+1}\left[x \mapsto {R_3^\sharp}^{i+1}(x) -^\sharp [\![2,2]\!]\right] \\
{R_5^\sharp}^{i+1} &= {R_2^\sharp}^{i+1}\left[x \mapsto {R_2^\sharp}^{i+1}(x) \right. \\
&\qquad\qquad \left. \sqcap^\sharp]\!]-\infty,0]\!]\right]
\end{aligned}$$

l	${R_l^\sharp}^0$	${R_l^\sharp}^1$	${R_l^\sharp}^2$	...
0				
1				
2				
3				
4				
5				

Correction et terminaison

Théorème (correction, *encore le même*)

La sémantique abstraite est une *sur-approximation correcte* de la sémantique concrète : pour tout $l \in L$, on a

$$R_l \subseteq \gamma_{\mathrm{nr}}\left(R_l^\sharp\right)$$

Remarques

- De manière générale, ca ne termine pas !
  Car le treillis a des chaînes croissantes infinies (ex. $([\![0,n]\!])_{n\in\mathbb{N}}$).
- Et quand bien même ça termine, ça peut être long...

Accélération de convergence

On va donc intercaler entre chaque itération un *élargissement* (widening en anglais) qui va empêcher de suivre des chaînes croissantes infinies en « sautant » plus haut.

Définition (élargissement)

Un élargissement ∇ est une opération binaire ($\nabla : \mathcal{D}^\sharp \times \mathcal{D}^\sharp \to \mathcal{D}^\sharp$) vérifiant

- $\forall x^\sharp, y^\sharp, \quad x^\sharp \sqcup^\sharp y^\sharp \ \sqsubseteq^\sharp\ x^\sharp \nabla y^\sharp$;
- pour toute suite $\left(x_n^\sharp\right)_{n\in\mathbb{N}}$, la suite croissante

$$\begin{cases} y_0^\sharp &= x_0^\sharp \\ y_{i+1}^\sharp &= y_i^\sharp \nabla x_{i+1}^\sharp \end{cases}$$

est stationnaire.

Élargissement, illustration

$$R^\sharp = {F^\sharp}^N(\bot) = \operatorname{lfp} F^\sharp$$
$$\vdots$$
$${R^\sharp}^2 = F^\sharp\left({R^\sharp}^1\right) = {F^\sharp}^2(\bot)$$
$${R^\sharp}^1 = F^\sharp\left({R^\sharp}^0\right) = F^\sharp(\bot)$$
$${R^\sharp}^0 = \bot$$

$F^\sharp$ stationnaire

$$R^\sharp = R^\sharp \triangledown F^\sharp(R^\sharp)$$
$$\operatorname{lfp} F^\sharp$$
$$\vdots$$
$${R^\sharp}^2 = {R^\sharp}^1 \triangledown F^\sharp\left({R^\sharp}^1\right)$$
$${R^\sharp}^1 = {R^\sharp}^0 \triangledown F^\sharp\left({R^\sharp}^0\right)$$
$${R^\sharp}^0 = \bot$$

$F^\sharp$ non stationnaire, élargissement

Remarque : $\operatorname{lfp} F^\sharp \sqsubseteq^\sharp R^\sharp$

On s'arrête avec $R^\sharp = R^\sharp \triangledown F^\sharp(R^\sharp)$ donc $F^\sharp(R^\sharp) \sqsubseteq^\sharp R^\sharp$ donc

$$\operatorname{lfp} F^\sharp = \bigsqcap^\sharp \left\{ x \;\middle|\; F^\sharp(x) \sqsubseteq^\sharp x \right\} \sqsubseteq^\sharp R^\sharp.$$

Exemple d'élargissement

Si les bornes de l'intervalle sont stables, on les conserve, sinon on les remplace par ∞.

Définition

$$x^\sharp \triangledown y^\sharp = \begin{cases} [\![a, b]\!] & \text{si } x^\sharp = [\![a, b]\!], y^\sharp = [\![c, d]\!], c \geqslant a, d \leqslant b \\ [\![a, +\infty[\![& \text{si } x^\sharp = [\![a, b]\!], y^\sharp = [\![c, d]\!], c \geqslant a, d > b \\ ]\!]-\infty, b]\!] & \text{si } x^\sharp = [\![a, b]\!], y^\sharp = [\![c, d]\!], c < a, d \leqslant b \\ ]\!]-\infty, +\infty[\![& \text{si } x^\sharp = [\![a, b]\!], y^\sharp = [\![c, d]\!], c < a, d > b \\ y^\sharp & \text{si } x^\sharp = \bot \\ x^\sharp & \text{si } y^\sharp = \bot \end{cases}$$

Exemple

- $[\![0, 2]\!] \triangledown [\![0, 1]\!] = [\![0, 2]\!]$
- $[\![0, 1]\!] \triangledown [\![0, 2]\!] = [\![0, +\infty[\![$ ($\triangledown$ n'est pas symétrique)

Exemple d'élargissement (suite et fin)

Exercice

Reprendre le calcul précédent en remplaçant l'equation de $R_2^\sharp$ par

$${R_2^\sharp}^{i+1} = {R_2^\sharp}^{i} \triangledown_{\mathrm{nr}} \left({R_1^\sharp}^{i+1} [y \mapsto \{42\}] \sqcup^\sharp_{\mathrm{nr}} {R_4^\sharp}^{i} \left[y \mapsto {R_4^\sharp}^{i}(y) +^\sharp \{4\} \right] \right)$$

(ça devrait s'arrêter après trois étapes).

Résultat

Après calcul on obtient :

$R_0^\sharp =$

$R_1^\sharp =$

$R_2^\sharp =$

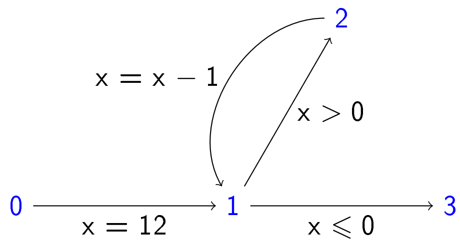
$R_3^\sharp =$

$R_4^\sharp =$

$R_5^\sharp =$

Exemple de calcul du point fixe abstrait

$_0$x = 12 ;
while $_1$(x > 0) **{**
    $_2$ x = x − 1 ;
}$_3$



$${R_0^\sharp}^{i+1} = \top$$
$${R_1^\sharp}^{i+1} = {R_1^\sharp}^{i} \triangledown_{\mathrm{nr}} \left({R_0^\sharp}^{i+1} [x \mapsto [\![12, 12]\!]] \sqcup^\sharp_{\mathrm{nr}} {R_2^\sharp}^{i} \left[y \mapsto {R_2^\sharp}^{i}(x) -^\sharp [\![1, 1]\!] \right] \right)$$
$${R_3^\sharp}^{i+1} = {R_1^\sharp}^{i+1} \left[x \mapsto {R_1^\sharp}^{i+1}(x) \sqcap^\sharp]\!]-\infty, 0]\!] \right]$$

I	${R_I^\sharp}^0$	${R_I^\sharp}^1$	${R_I^\sharp}^2$	${R_I^\sharp}^3$
0				
1				
2				
3				
4				
5				

Regagner de la précision

- L'élargissement permet au calcul de terminer.
- Mais entraîne une perte de précision.
- On peut en regagner un peu par des itérations descendantes.

Définition (rétrécissement)

Un rétrécissement (narrowing en anglais) $\triangle$ est une opération binaire ($\triangle\colon \mathcal{D}^\sharp \times \mathcal{D}^\sharp \to \mathcal{D}^\sharp$) vérifiant

- $\forall x^\sharp, y^\sharp, \quad x^\sharp \sqcap^\sharp y^\sharp \sqsubseteq^\sharp x^\sharp \triangle y^\sharp \sqsubseteq^\sharp x^\sharp$;
- pour toute suite $\left(x^\sharp\right)_{n\in\mathbb{N}}$, la suite décroissante

$$\left\{\begin{array}{lcl} y_0^\sharp & = & x_0^\sharp \\ y_{i+1}^\sharp & = & y_i^\sharp \triangle x_{i+1}^\sharp \end{array}\right.$$

est stationnaire.

Rétrécissement, illustration

$$R^\sharp = R^\sharp \triangledown F^\sharp(R^\sharp)$$

$$R^{\sharp'1} = R^\sharp \triangle F^\sharp(R^\sharp)$$

$$\vdots$$

$$R^{\sharp'} = R^{\sharp'} \triangle F^\sharp\left(R^{\sharp'}\right)$$

$$\mathrm{lfp}\ F^\sharp$$

$$\vdots$$

$$R^{\sharp 0} = \bot$$

Remarque : $\mathrm{lfp}\ F^\sharp \sqsubseteq^\sharp R^{\sharp'}$

On part de $R^\sharp \sqsupseteq^\sharp \mathrm{lfp}\ F^\sharp$
donc par croissance de $F^\sharp$,

$$F^\sharp(R^\sharp) \sqsupseteq^\sharp F^\sharp\left(\mathrm{lfp}\ F^\sharp\right) = \mathrm{lfp}\ F^\sharp$$

donc par propriété du rétrécissement $\triangle$,

$$R^{\sharp'1} = R^\sharp \triangle F^\sharp(R^\sharp) \sqsupseteq^\sharp \mathrm{lfp}\ F^\sharp.$$

Finalement, par récurrence immédiate,

$$R^{\sharp'} \sqsupseteq \mathrm{lfp}\ F^\sharp.$$

Exemple de rétrécissement

Pour garantir la convergence, on ne raffine que les bornes infinies.

Définition

$$x^\sharp \triangle y^\sharp = \left\{\begin{array}{ll} [\![a, d]\!] & \text{si } x^\sharp = [\![a, +\infty[\![\,, y^\sharp = [\![c, d]\!] \\ [\![c, b]\!] & \text{si } x^\sharp =]\!]-\infty, b]\!]\,, y^\sharp = [\![c, d]\!] \\ [\![c, d]\!] & \text{si } x^\sharp =]\!]-\infty, +\infty[\![\,, y^\sharp = [\![c, d]\!] \\ x^\sharp & \text{sinon} \end{array}\right.$$

Exemple

- $[\![0, +\infty[\![\triangle [\![0, 1]\!] = [\![0, 1]\!]$
- $[\![0, 2]\!] \triangle [\![0, 1]\!] = [\![0, 2]\!]$

Exemple de rétrécissement (suite et fin)

Exercice

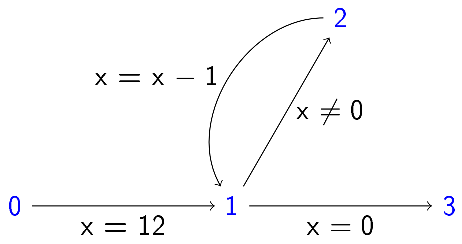
Raffiner le résultat du calcul précédent avec le rétrécissement (i.e. partir du point fixe $R_I^{\sharp 3}$ et itérer en remplaçant $\triangledown_{\mathrm{nr}}$ par $\triangle_{\mathrm{nr}}$ dans les equations).

Résultat

Après calcul on obtient :
$R_0^\sharp =$
$R_1^\sharp =$
$R_2^\sharp =$
$R_3^\sharp =$

Limitations du narrowing et élargissement à seuil

$_0$x $=12$;
while $_1$(x $\neq 0$) **{**
$_2$ x $=$ x -1 ;
}$_3$



- Même avec le narrowing, on ne peut pas trouver $x \geqslant 0$.
- Alors que le domaine des signes y parvient.
- On peut améliorer l'élargissement : au lieu de passer directement d'une borne positive à $-\infty$, on s'arrête d'abord à 0.
- C'est l'idée de l'élargissement à seuil : on peut ainsi utiliser n'importe quel nombre fini de constantes comme seuils.
- Encore faut il avoir le bon seuil (si on avait utilisé -1 ici, on n'aurait pas obtenu l'intervalle $[\![-1, 12]\!]$).

Exercice : analyse en arrière

On avait défini la sémantique abstraite des gardes comme

$$[\![e > 0]\!]^\sharp_{\mathrm{C}}\,\rho = \begin{cases} \rho\left[v \mapsto \rho(v)\ \sqcap^\sharp \alpha\left([\![1, +\infty[\![\right)\right] & \text{si } e = v \\ \rho & \text{sinon} \end{cases}$$

Comment faire pour $x - 4 > 0$?

On va utiliser une analyse en arrière des expressions :
partant du résultat de l'expression,
on en déduit les valeurs possibles des variables.

Exercice : analyse en arrière (suite)

Sémantique en arrière des expressions :
$[\![e]\!]{\downarrow}^\sharp : (\mathbb{V} \to \mathcal{D}^\sharp) \times \mathcal{D}^\sharp \to (\mathbb{V} \to \mathcal{D}^\sharp)$

$$[\![v]\!]{\downarrow}^\sharp(\rho, r) = \rho\left[v \mapsto \rho(v) \sqcap r\right](v)$$

$$[\![n]\!]{\downarrow}^\sharp(\rho, r) = \begin{cases} \bot & \text{si } n^\sharp \sqcap^\sharp r = \bot \\ \rho & \text{sinon} \end{cases}$$

$$[\![\mathbf{rand}(n_1, n_2)]\!]{\downarrow}^\sharp(\rho, r) = \begin{cases} \bot & \text{si } \mathbf{rand}^\sharp(n_1, n_2) \sqcap^\sharp r = \bot \\ \rho & \text{sinon} \end{cases}$$

$$[\![e_1 + e_2]\!]{\downarrow}^\sharp(\rho, r) = [\![e_1]\!]{\downarrow}^\sharp(\rho, r_1) \sqcap^\sharp_{\mathrm{nr}} [\![e_2]\!]{\downarrow}^\sharp(\rho, r_2)$$
$$\text{avec } (r_1, r_2) = +{\downarrow}^\sharp\left([\![e_1]\!]^\sharp_{\mathrm{E}}(\rho), [\![e_2]\!]^\sharp_{\mathrm{E}}(\rho), r\right)$$

...

Exercice : analyse en arrière, arithmétique

Exemple

Dans le domaine des signes :
$+\downarrow^\sharp(\geqslant 0, \geqslant 0, \leqslant 0) = (0, 0)$
(si $x \geqslant 0$, $y \geqslant 0$ et $x + y \leqslant 0$ alors $x = y = 0$)

Exemple

Dans le domaine des intervalles :
$+\downarrow^\sharp(\llbracket 0, 2 \rrbracket, \llbracket 3, 8 \rrbracket, \llbracket 4, 7 \rrbracket) = (\llbracket 0, 2 \rrbracket, \llbracket 3, 7 \rrbracket)$

Exercices

- Donner la table de $+\downarrow^\sharp$ pour le domaine des signes (tout au moins une partie, la table ayant 125 entrées).
- Définir $-\downarrow^\sharp$ pour le domaine des intervalles.

Exercice : analyse en arrière, arithmétique (suite et fin)

Réponse

Exercice, analyse en arrière (suite et fin)

Exercice

- Avec la sémantique en arrière des expressions, définir une sémantique abstraite pour les gardes plus précise.
- Puis calculer cette sémantique dans le domaine des intervalles pour la garde $x + y \leqslant z$ avec $\rho(x) = \llbracket 1, 10 \rrbracket$, $\rho(y) = \llbracket 3, 10 \rrbracket$ et $\rho(z) = \llbracket 3, 5 \rrbracket$.

Réponse

Exercice : domaine des congruences

Exercice

- Concevoir un domaine abstrait non relationnel pour les congruences (exemple : x est congru à 2 modulo 4 : $x \in 4\mathbb{Z} + 2$).
- Analyser avec le programme du premier exemple :

```
x = rand(0, 12) ; y = 42 ;
while (x > 0) {
    x = x - 2 ;
    y = y + 4 ;
}
```