Calculs d'invariants et applications

Quentin VERMANDE

1 Introduction

L'informatique ayant de très nombreuses applications, il est nécessaire de pouvoir vérifier efficacement le comportement des programmes. Cela permet non seulement d'éliminer les bugs et d'éviter qu'un programme ne plante à un instant critique, comme l'erreur de conversion qui a provoqué la désintégration de la fusée Ariane 5, mais aussi de vérifier qu'un programme ne peut pas retourner de valeur absurde, termine, ou simplement s'exécute assez rapidement. La phase de test n'est en général pas suffisante pour enlever toutes les erreurs ou prouver une propriété d'un programme car on ne peut pas être sûr d'avoir trouvé les pires exécutions. Il faut donc analyser les programmes au niveau de leur code. Les techniques de preuve de correction de programmes et de model-checking ont une efficacité limitée du fait qu'une partie importante du travail ne peut pas être automatisée. On cherche alors à faire de l'analyse statique. Parmi les constructions de base de la plupart des langages de programmation, la plus difficile à analyser est la boucle.

Ce mémoire débute par une présentation de l'objectif recherché. Puis il introduit les domaines abstrait, en particulier le domaine des polyèdres convexes [3]. Il conclut avec les techniques de widening [2] et d'accélération de boucle [1].

2 Définition du problème

On considère une boucle de la forme :

```
1 while(condition) { instructions }
```

Soit n le nombre de variables apparaissant dans cette boucle. On note $X \in \mathcal{M}_{n,1}(K)$ la colonne donnant ces variables où K est l'espace des valeurs possibles pour les variables. En pratique, on a $K = \mathbb{Z}/2^{64}\mathbb{Z}$ pour des entiers 64 bits, mais dans la théorie on considère en général $K = \mathbb{R}$.

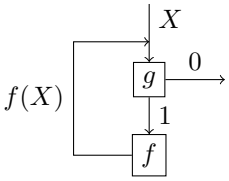
La condition d'exécution de la boucle, appelée par la suite "garde", est modélisée par une application $g : \mathcal{M}_{n,1}(K) \to \{0, 1\}$ où, pour $X \in \mathcal{M}_{n,1}(K), g(X) = 1$ si et seulement si la condition est vraie pour X.

L'exécution des instructions est modélisée par une application $f : \mathcal{M}_{n,1}(K) \to \mathcal{M}_{n,1}(K)$.

On obtient alors la boucle :

```
1 while(c(X)) { X = f(X) }
```

Elle se réécrit sous forme de graphe de flot de contrôle :



Étant donné un ensemble d'états initiaux $\mathcal{X} \in \mathcal{P}(\mathcal{M}_{n,1}(\mathbb{R}))$ des valeurs possibles de X, on cherche l'ensemble des valeurs possibles des variables du programme au moment de l'évaluation de la condition.

Exemple. *Dans tout ce mémoire, on considère l'exemple de la boucle (où x et y sont les variables du programme)*

```
1  while(-42 <= x <= 42) {y = x-y; x = 2x-1;}
```

On prend la matrice $X = \begin{pmatrix} x \\ y \end{pmatrix}$ *et on a alors :*

$$c : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \mathbb{1}_{[-42,42]}(x)$$

$$f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2x-1 \\ x-y \end{pmatrix}$$

On prendra comme espace d'états initiaux :

$$\mathcal{X} = \{ \begin{pmatrix} x \\ y \end{pmatrix}, (x,y) \in [0,3] \times [0,5] \}$$

3 Génération d'invariants

L'invariant de boucle $\mathcal{I}$ cherché est défini par l'équation :

$$\mathcal{I} = \mathcal{X} \cup \{ f(X), X \in \mathcal{I}, g(X) = 1 \}$$

On définit l'opérateur de propagation en avant :

$$\begin{array}{rccc} \mathcal{F}(f,g) : & \mathcal{P}(\mathcal{M}_{n,1}(K)) & \longrightarrow & \mathcal{P}(\mathcal{M}_{n,1}(K)) \\ & \mathcal{X} & \longmapsto & \mathcal{X} \cup \{ f(X), X \in \mathcal{X}, g(X) = 1 \} \end{array}$$

Alors, un ensemble $\mathcal{A} \in \mathcal{P}(\mathcal{M}_{n,1}(K))$ est un invariant de la boucle définie plus haut lorsque $\mathcal{F}(f,g)(\mathcal{A}) \subset \mathcal{A}$, donc lorsque $\mathcal{F}(f,g)(\mathcal{A}) = \mathcal{A}$. En particulier, l'invariant de boucle le plus fort est le plus petit point fixe de $\mathcal{F}(f,g)$:

$$\mathcal{I} = \text{ lfp}(\mathcal{F}(f,g))$$

En pratique, on n'effectue pas le calcul de $\mathcal{I}$ car le nombre d'itérations de $\mathcal{F}(f,g)$ nécessaire pour obtenir l'invariant est trop grand, lorsqu'il n'est pas infini. On cherche alors un invariant plus faible par approximation dans un domaine abstrait.

4 Domaines abstraits

Notons $(D, \leq)$ le domaine étudié (ici $(D, \leq) = (\mathcal{M}_{n,1}(K), \subset)$). Un domaine abstrait approchant $(D, \leq)$ est la donnée d'un ensemble ordonné $(A, \leq)$ et d'une application $\gamma : A \to D$ croissante, appelée fonction de concrétisation.

Si $F : \mathcal{P}(D) \to \mathcal{P}(D)$ est un opérateur de propagation en avant (ici $F = \mathcal{F}(f, g)$), on approche F par un opérateur de propagation en avant $\overline{F} : \mathcal{P}(A) \to \mathcal{P}(A)$ qui vérifie : $F \circ \gamma \leq \gamma \circ \overline{F}$. On a alors, pour $A \in \mathcal{P}(A)$ tel que $\overline{F}(A) \leq A, F(\gamma(A)) \leq \gamma(\overline{F}(A)) \leq \gamma(A)$. Autrement dit, si on dispose d'un invariant pour $\overline{F}$, alors on en déduit un invariant pour F.

5 Les polyèdres convexes

Soit E un $\mathbb{R}-$espace vectoriel de dimension finie. Une introduction aux polyhèdres est donnée dans .

Un polyèdre convexe de E est une intersection finie de demi-espaces affines fermés de E. On note $\mathcal{CP}(E)$ leur ensemble. Ainsi, pour $P \in \mathcal{CP}(E)$, on dispose de $n \in \mathbb{N}^*, f_1, ..., f_n \in \mathcal{L}(E, \mathbb{R})$ et $a_1, ..., a_n \in \mathbb{R}$ tels que :

$$P = \bigcap_{i=1}^{n} f_i^{-1}(]-\infty, a_i]) = \{x \in E, \forall i \in [\![1, n]\!], f_i(x) \leq a_i\}$$

Une telle représentation d'un polyèdre convexe est appelée représentation par contraintes. On dispose aussi d'une représentation par générateurs : si P est un polyèdre convexe, on a $A, U \in \mathcal{P}(E)$ finis tels que :

$$P = conv(A) + cone(U)$$

où $conv(A)$ est l'enveloppe convexe de A et $cone(U) = \sum_{u \in U} \mathbb{R}^+ u$.

$\mathcal{CP}(E)$ est muni d'un opérateur d'union convexe $\sqcup$ défini par, pour $P, Q \in \mathcal{CP}(E)$:

$$P \sqcup Q = conv(P \cup Q)$$

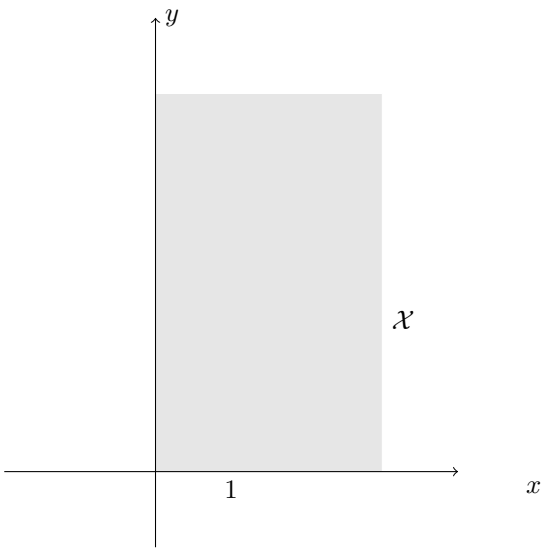
En outre, si on a $A, B, U, V \in \mathcal{P}(E)$ tels que $P = conv(A) + cone(U)$ et $Q = conv(B) + cone(V)$, alors :

$$P \sqcup Q = conv(A \cup B) + cone(U \cup V)$$

Exemple. *Dans l'exemple considéré, $\mathcal{X}$ est un polyèdre convexe :*

$$\mathcal{X} = (\begin{pmatrix} x \\ y \end{pmatrix} \mapsto x)^{-1}(]-\infty, 3]) \cap (\begin{pmatrix} x \\ y \end{pmatrix} \mapsto -x)^{-1}(]-\infty, 0]) \cap (\begin{pmatrix} x \\ y \end{pmatrix} \mapsto y)^{-1}(]-\infty, 5]) \cap (\begin{pmatrix} x \\ y \end{pmatrix} \mapsto -y)^{-1}(]-\infty, 0])$$

$$= conv(\{\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix})$$



$(\mathcal{CP}(E), \gamma)$ est un domaine abstrait approchant $(\mathcal{P}(E), \subset)$ où $\gamma = id_E / \mathcal{CP}(E)$.

6 Les boucles linéaires

//Pourquoi les boucles linéaires, l'abstraction directe plante sur les polyèdres ?

Si f est affine et g est l'indicatrice d'un polyèdre convexe, on dit que la boucle définie par f et g est linéaire. On dispose alors de $A \in \mathcal{M}_n(\mathbb{R}), k \in \mathbb{N}^*, G \in \mathcal{M}_{k,n}(\mathbb{R})$ et $b, h \in \mathcal{M}_{n,1}(\mathbb{R})$ tels que :

$$f = x \mapsto Ax + b$$

$$g = \mathbb{1}_{\{x \in \mathcal{M}_{n,1}(\mathbb{R}), Gx \leq h\}}$$

y = x-y ; x = 2x-1 ;

Exemple. *Dans notre exemple, on a*

$$A = \begin{pmatrix} 2 & 0 \\ 1 & -1 \end{pmatrix}$$

$$b = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

$$G = \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$$

$$h = \begin{pmatrix} 0 \\ 42 \end{pmatrix}$$

Pour simplifier les calculs, on ajoute au programme une variable constante égale à 1. On notera $\mathcal{M}'_{n,1}(\mathbb{R})$ le nouvel ensemble des valeurs possibles pour les variables du programme. On définit alors :

$$A' = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_{n+1}(\mathbb{R})$$

$$G' = \begin{pmatrix} G & -h \end{pmatrix} \in \mathcal{M}_{k,n+1}(\mathbb{R})$$

Et on a :

$$f = x \mapsto A'x$$

$$g = \mathbb{1}_{\{x \in \mathcal{M}'_{n,1}(\mathbb{R}), G'x \leq 0\}}$$

Une telle boucle est appelée boucle linéaire homogène.

Exemple. *On obtient dans l'exemple :*

$$A' = \begin{pmatrix} 2 & 0 & -1 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$G' = \begin{pmatrix} -1 & 0 & -42 \\ 1 & 0 & -42 \end{pmatrix}$$

On munit $\mathcal{CP}(\mathcal{M}'_{n,1}(\mathbb{R}))$ d'une structure de domaine abstrait approchant $\mathcal{P}(\mathcal{M}'_{n,1}(\mathbb{R}))$ en l'ordonnant pas l'inclusion et avec l'inclusion de $\mathcal{CP}(\mathcal{M}'_{n,1}(\mathbb{R}))$ dans $\mathcal{P}(\mathcal{M}'_{n,1}(\mathbb{R}))$. On peut alors approcher $\mathcal{F}(f,g)$ par :

$$\begin{array}{rccc} F(f,g): & \mathcal{CP}(\mathcal{M}'_{n,1}(\mathbb{R})) & \longrightarrow & \mathcal{CP}(\mathcal{M}'_{n,1}(\mathbb{R})) \\ & P & \longmapsto & P \sqcup conv(\{A'x, x \in P, G'x \leq 0\}) \end{array}$$

On peut supposer que $\mathcal{X}$ est un polyèdre convexe.

Exemple. *Soit G l'ensemble des $x \in \mathcal{M}'_{n,1}(\mathbb{R})$ tels que $Gx \leq 0$. G est un polyèdre convexe. On peut effectuer le calcul direct de $\mathcal{I}$ dans le domaine des polyèdres convexes. On définit $P \in \mathcal{CP}(\mathcal{M}'_{n,1}(\mathbb{R}))^{\mathbb{N}}$ par récurrence par $P_0 = \mathcal{X}$ et $\forall n \in \mathbb{N}, P_{n+1} = P_n \sqcup A'(G \cap P_n)$:*

- $P_0 = conv(\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}\})$
- $P_1 = P_0 \sqcup conv(\{\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ -2 \end{pmatrix}\})$
  $= conv(\{\begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ -2 \end{pmatrix}\})$
- $P_2 = P_0 \sqcup conv(\{\begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \begin{pmatrix} -3 \\ -1 \end{pmatrix}, \begin{pmatrix} -3 \\ 4 \end{pmatrix}, \begin{pmatrix} 9 \\ 2 \end{pmatrix}, \begin{pmatrix} 9 \\ 7 \end{pmatrix}\})$
  $= conv(\{\begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 5 \\ -2 \end{pmatrix}\}, \begin{pmatrix} -3 \\ -1 \end{pmatrix}, \begin{pmatrix} -3 \\ 4 \end{pmatrix}, \begin{pmatrix} 9 \\ 2 \end{pmatrix}, \begin{pmatrix} 9 \\ 7 \end{pmatrix}\})$
- ...
- $P_5 = conv(\{\begin{pmatrix} -31 \\ -15 \end{pmatrix}, \begin{pmatrix} -31 \\ -10 \end{pmatrix}, \begin{pmatrix} -15 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 33 \\ 15 \end{pmatrix}, \begin{pmatrix} 65 \\ 18 \end{pmatrix}, \begin{pmatrix} 65 \\ 23 \end{pmatrix}\})$
  $P_5 \cap G = conv(\{\begin{pmatrix} -31 \\ -15 \end{pmatrix}, \begin{pmatrix} -31 \\ -10 \end{pmatrix}, \begin{pmatrix} -15 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 33 \\ 15 \end{pmatrix}, \begin{pmatrix} 42 \\ \frac{69}{4} \end{pmatrix}, \begin{pmatrix} 42 \\ \frac{659}{66} \end{pmatrix}\})$
- $P_6 = P_5 \sqcup conv(\{\begin{pmatrix} -63 \\ -21 \end{pmatrix}, \begin{pmatrix} -63 \\ -16 \end{pmatrix}, \begin{pmatrix} 83 \\ \frac{99}{4} \end{pmatrix}, \begin{pmatrix} 83 \\ \frac{2113}{66} \end{pmatrix}\})$
  $= conv(\{\begin{pmatrix} -63 \\ -21 \end{pmatrix}, \begin{pmatrix} -63 \\ -16 \end{pmatrix}, \begin{pmatrix} -31 \\ -15 \end{pmatrix}, \begin{pmatrix} -15 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 65 \\ 18 \end{pmatrix}, \begin{pmatrix} 83 \\ \frac{99}{4} \end{pmatrix}, \begin{pmatrix} 83 \\ \frac{2113}{66} \end{pmatrix}\})$
  $P_6 \cap G = conv(\{\begin{pmatrix} -42 \\ -\frac{37}{3} \end{pmatrix}, \begin{pmatrix} -42 \\ -\frac{491}{32} \end{pmatrix}, \begin{pmatrix} -31 \\ -15 \end{pmatrix}, \begin{pmatrix} -1 \\ -5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 65 \\ 18 \end{pmatrix}, \begin{pmatrix} 42 \\ \frac{17046}{913} \end{pmatrix}, \begin{pmatrix} 42 \\ \frac{659}{66} \end{pmatrix}\})$

— $P_7 = P_6 \sqcup conv(\begin{pmatrix}-85\\-\frac{89}{3}\end{pmatrix}, \begin{pmatrix}-85\\-\frac{853}{32}\end{pmatrix}, \begin{pmatrix}83\\\frac{21300}{913}\end{pmatrix}, \begin{pmatrix}83\\\frac{2113}{66}\end{pmatrix}\})$
$= conv(\{\begin{pmatrix}-85\\-\frac{89}{3}\end{pmatrix}, \begin{pmatrix}-85\\-\frac{853}{32}\end{pmatrix}, \begin{pmatrix}-63\\-16\end{pmatrix}, \begin{pmatrix}-31\\-15\end{pmatrix}, \begin{pmatrix}-1\\-5\end{pmatrix}, \begin{pmatrix}0\\5\end{pmatrix}, \begin{pmatrix}83\\\frac{21300}{913}\end{pmatrix}, \begin{pmatrix}83\\\frac{2113}{66}\end{pmatrix}\})$

On peut montrer que P est strictement croissante et que $\bigcup_{n\in\mathbb{N}} P_n = conv(\{\begin{pmatrix}-85\\-33\end{pmatrix}, \begin{pmatrix}-85\\-\frac{70}{3}\end{pmatrix}, \begin{pmatrix}83\\23\end{pmatrix}, \begin{pmatrix}83\\\frac{98}{3}\end{pmatrix}\})$.

7 Widening

Comme on a pu le remarquer dans les calculs précédents, l'itération directe ne termine pas. On utilise la technique du widening pour assurer la convergence.

Définition 7.1. *Soient $(A, \leq)$ un ensemble ordonné et $\nabla : A^2 \to A$ une loi de composition interne définie sur A. On dit que ∇ est un opérateur de widening sur A lorsque :*
— $\forall x, y \in A, x \leq x\nabla y \wedge y \leq x\nabla y$
— *pour toute suite $x \in A^{\mathbb{N}}$ croissante, la suite $y \in A^{\mathbb{N}}$ définie par $y_0 = x_0$ et $\forall n \in \mathbb{N}, y_{n+1} = x_{n+1}\nabla y_n$ est stationnaire.*

Le widening fonctionne lorsque f est Scott-continue :

Définition 7.2. *Soient $(E, \leq)$ et $(F, \leq)$ deux ensembles ordonnés. On dit que $f \in F^E$ est Scott-continue lorsque, pour toute partie A de E admettant un supremum $s \in E$, $f(s)$ est le supremum de $f(A)$.*

On a alors le théorème suivant :

Théorème 7.1. *Soient $(A, \leq)$ un ensemble ordonné, ∇ un opérateur de widening sur A, $f \in A^A$ une application Scott-continue et $y \in A^{\mathbb{N}}$ telle que $y_0 \leq lfp(f)$ et, pour tout $n \in \mathbb{N}, y_{n+1} = y_n\nabla f(y_n)$. Alors y est stationnaire et $lfp(f) \leq \lim_{n\to+\infty} y_n$.*

Considérons (A, γ) un domaine abstrait. On peut remarquer que, si $\mathcal{X}$ est un élément abstrait et si $\gamma(\mathcal{X})$ est l'ensemble des valeurs possibles en entrée du programme et I est la limite obtenue par widening en itérant $\overline{\mathcal{F}}$ à partir de $\mathcal{X}$, alors d'après le théorème, on a $\mathcal{I} = lfp(\mathcal{F}(f, g)) \subset I$.

Définition 7.3. *Soient $P = \bigcap_{a\in A} a$ et $Q = \bigcap_{b\in B} b$ deux polyèdres convexes représentés par contraintes. Alors on définit $P\nabla Q = \bigcap_{c\in A\cap B} c$.*

Lemme 7.1. *∇ est un opérateur de widening sur les polyèdres convexes.*

Démonstration. *Soient $P = \bigcap_{a\in A} a$ et $Q = \bigcap_{b\in B} b$ deux polyèdres convexes représentés par contraintes. Alors $A \subset A \cap B$ donc $P = \bigcap_{a\in A} a \subset \bigcap_{c\in A\cap B} c = P\nabla Q$. Symétriquement, $B \subset A \cap B$ donc $Q \subset P\nabla Q$.*

Soit $P \in \mathcal{CP}(\mathbb{R}^n)^{\mathbb{N}}$ croissante. On définit $Q \in \mathcal{CP}(\mathbb{R}^n)^{\mathbb{N}}$ par récurrence par $Q_0 = P_0$ et $\forall k \in \mathbb{N}, Q_{k+1} = P_{k+1}\nabla Q_k$. On peut écrire la représentation par contraintes de P_0 : $P_0 = \bigcap_{a\in A} a$. On montre alors par récurrence immédiate que, pour $k \in \mathbb{N}$, il existe $B \subset A$ tel que $Q_k = \bigcap_{b\in B} b$. Soit donc, pour $k \in \mathbb{N}$, $B_k \subset A$ tel que $Q_k = \bigcap_{b\in B_k} b$. On montre alors par récurrence immédiate que B est décroissante. Or A est fini, donc B est stationnaire. Donc Q est stationnaire.

Exemple. *On reprend les calculs précédents. Si on applique l'opérateur de widening pour le calcul de :*

— $P_k, k \in \{1,2\}$, *on trouve* $P_k = \mathcal{M}'_{n,1}$

— P_3, *on obtient* $P_3 = \{(\begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}'_{n,1}(\mathbb{R}), 3y - x \leq 15\}$.

— $P_k, k \in [\![4,6]\!]$, *on a* $P_k = \{(\begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}'_{n,1}(\mathbb{R}), 3y - x \in [-14,15]\}$

— P_7, *on trouve* $P_7 = \{(\begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}'_{n,1}(\mathbb{R}), x \in [-\infty,83], 3y - x \in [-14,15]\}$

— $P_k, 8 \leq k$, *on obtient* $P_k = \{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}'_{n,1}(\mathbb{R}), x \in [-85,83], 3y - x \in [-14,15]\}$

8 Accélération

Dans le domaine des polyèdres convexes, on dispose d'une technique plus précise que le widening, l'accélération. On calcule plutôt une autre approximation de $\mathcal{I}$, donnée par le théorème qui suit.

Théorème 8.1. *Soit* $n = \min(\{k \in \mathbb{N}, \forall x \in \mathcal{X}, 0 < G'A'^k x\})$ *(où* $\min(\varnothing) = +\infty$*). Alors :*

$$lfp(F(f,g)) \subset \bigcup_{k=0}^{n} \{A'^k x, x \in \mathcal{X}\}$$

Démonstration. *Soient* $\mathcal{I}_0 = \mathcal{X}$ *et, pour* $k \in \mathbb{N}, \mathcal{I}_{k+1} = \{A'x, x \in \mathcal{I}_k, G'x \leq 0\}$. *Alors* $\mathcal{I} = \bigcup_{k \in \mathbb{N}} \mathcal{I}_k$. *Montrons par récurrence que, pour tout* $k \in \mathbb{N}, \mathcal{I}_k \subset \bigcup_{k=0}^{n} \{A'x, x \in \mathcal{X}\}$.

Pour $k = 0$, *on a* $\mathcal{I}_0 = \mathcal{X} = \{A'^0 x, x \in \mathcal{X}\} \subset \bigcup_{k=0}^{n} \{A'x, x \in \mathcal{X}\}$.

Soit $k \in \mathbb{N}$ *tel que* $\mathcal{I}_k \subset \bigcup_{k=0}^{n} \{A'x, x \in \mathcal{X}\}$. *Soit* $x \in \mathcal{I}_k$ *tel que* $G'x \leq 0$. *Alors on dispose de* $i \in [\![0,n]\!]$ *tel que* $x \in \{A'^i y, y \in \mathcal{X}\}$. *Soit* $y \in \mathcal{X}$ *tel que* $x = A'^i y$. *On a* $G'A'^i y \leq 0$, *donc* $i < n$. *Donc* $A'x = A'^{i+1} y \in \bigcup_{k=0}^{n} \{A'x, x \in \mathcal{X}\}$. *Donc* $\mathcal{I}_{k+1} \subset \bigcup_{k=0}^{n} \{A'x, x \in \mathcal{X}\}$.

Il faut faire du calcul matriciel avec des polyèdres convexes (car les calculs demandent de calculer $A'^k \mathcal{X}, k \in [\![0,n]\!]$).

Définition 8.1. *Soient* $n, p, q \in \mathbb{N}^*, M_1 = conv(V_1) + cone(R_1) \in \mathcal{CP}(\mathcal{M}_{n,p}(\mathbb{R}))$ *et* $M_2 = conv(V_2) + cone(R_2) \in \mathcal{CP}(\mathcal{M}_{p,q})$. *On définit* $M_1 \otimes M_2 = conv(V_1 V_2) + cone(V_1 R_2 \cup V_2 R_1 \cup R_1 R_2)$.

Propriété 8.1. *Soient* $n, p, q \in \mathbb{N}^*, M_1 \mathcal{CP}(\mathcal{M}_{n,p}(\mathbb{R}))$ *et* $M_2 \in \mathcal{CP}(\mathcal{M}_{p,q})$. *Alors* $M_1 M_2 \subset M_1 \otimes M_2$.

Démonstration. *On peut écrire* $M_1 = conv(V_1) + cone(R_1)$ *et* $M_2 = conv(V_2) + cone(R_2)$ *avec* $V_1, R_1 \in \mathcal{P}(\mathcal{M}_{n,p}(\mathbb{R}))$ *finis et* $V_2, R_2 \in \mathcal{P}(\mathcal{M}_{p,q}(\mathbb{R}))$ *finis.*
Soient $A = \sum_{U \in V_1} s_U U + \sum_{V \in R_1} \mu_V V \in M_1$ *et* $B = \sum_{X \in V_2} t_X X + \sum_{Y \in R_2} \nu_Y Y \in M_2$ *où* $s \in [0,1]^{V_1}, \sum_{U \in V_1} t_U = 1, \mu \in (\mathbb{R}^+)^{R_1}, t \in [0,1]^{V_2}, \sum_{X \in V_1} t_X = 1$ *et* $\nu \in (\mathbb{R}^+)^{R_2}$.

Alors : $AB = \sum_{(U,X) \in V_1 \times V_2} s_U t_X UX + \sum_{(U,Y) \in V_1 \times R_2} s_U \nu_Y UY + \sum_{(V,X) \in R_1 \times V_2} t_V \mu_X VX + \sum_{(V,Y) \in R_1 \times R_2} \mu_V \nu_Y VY.$

Or, $\forall (U,X) \in V_1 \times V_2, s_U t_X \in [0,1]$ *et* $\sum_{(U,X)\in V_1\times V_2} s_U t_X = \sum_{U\in V_1} s_U \sum_{X\in V_2} t_X = 1$ *donc* $\sum_{(U,X)\in V_1\times V_2} s_U t_X UX \in conv(V_1V_2)$. *De plus,* $\forall (U,Y) \in V_1 \times R_2, s_U\nu_Y \in \mathbb{R}^+, \forall (V,X) \in R_1 \times V_2, \mu_V t_X \in \mathbb{R}^+$ *et* $\forall (V,Y) \in R_1\times R_2, \mu_V\nu_Y \in \mathbb{R}^+$, *donc* $\sum_{(U,Y)\in V_1\times R_2} s_U\nu_Y UY + \sum_{(V,X)\in R_1\times V_2} t_V\mu_X VX + \sum_{(V,Y)\in R_1\times R_2} \mu_V\nu_Y VY \in cone(V_1R_2 + R_1V_2 + R_1R_2)$.

Donc $AB \in M_1 \otimes M_2$. *Donc* $M_1M_2 \subset M_1 \otimes M_2$.

Corollaire 8.1. *Soit* $\mathcal{G} \in \mathcal{CP}(\mathcal{M}_{n+1}(\mathbb{R}))$ *tel que* $\{A \in \mathcal{M}_{n+1}(\mathbb{R}), \exists x \in \mathcal{X}, G'Ax \leq 0\} \subset \mathcal{G}$. *Soient* $n = \min(\{k \in \mathbb{N}, A'^k \notin \mathcal{G}\})$ *et* $\mathcal{A} \in \mathcal{CP}(\mathcal{M}_{n+1}(\mathbb{R}))$ *tel que* $\forall k \in [\![0,n]\!], A'^k \in \mathcal{A}$. *Alors*

$$\mathcal{I} \subset \mathcal{A} \otimes \mathcal{X}$$

Exemple. *On a une expression des puissances de* A' *(obtenue par diagonalisation) :*

$$\forall n \in \mathbb{N}, A'^n = \begin{pmatrix} 2^n & 0 & 1-2^n \\ \frac{1}{3}((-1)^{n+1}+2^n) & (-1)^n & \frac{1}{2}+\frac{(-1)^{n+1}}{6}-\frac{2^n}{3} \\ 0 & 0 & 1 \end{pmatrix}$$

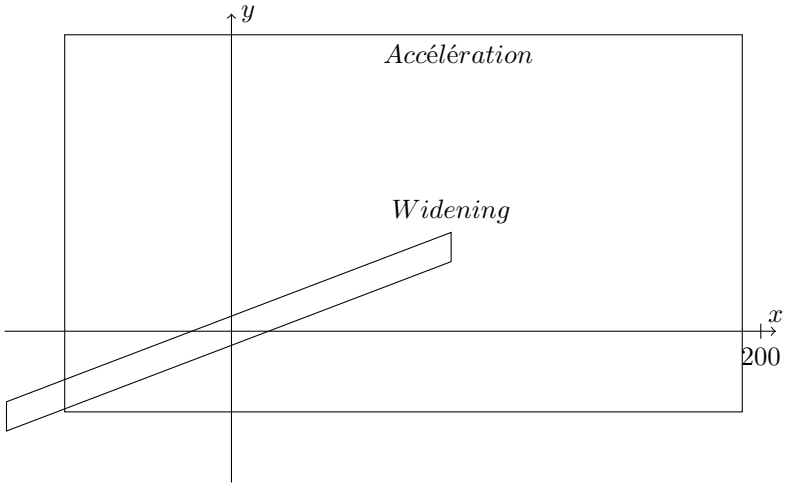
Soit $n \in \mathbb{N}$. *On a* $A'^n\mathcal{X} = conv(\{\begin{pmatrix} 1-2^n \\ \frac{1}{2}+\frac{(-1)^{n+1}}{6}-\frac{2^n}{3} \end{pmatrix}, \begin{pmatrix} 1-2^n \\ 5\cdot(-1)^n+\frac{1}{2}+\frac{(-1)^{n+1}}{6}-\frac{2^n}{3} \end{pmatrix}, \begin{pmatrix} 2^{n+1}-1 \\ \frac{1}{2}+\frac{7}{6}(-1)^{n+1}+\frac{2^{n+1}}{3} \end{pmatrix}, \begin{pmatrix} 2^{n+1}-1 \\ \frac{1}{2}+\frac{23}{6}(-1)^n+\frac{2^{n+1}}{3} \end{pmatrix}\})$. *On a, pour* $n \in \mathbb{N}, 1-2^n \in [-42,42] \Leftrightarrow -42 \leq 1-2^n \Leftrightarrow n \leq log_2(43) \Leftrightarrow n \leq 5$.
On a, pour $n \in \mathbb{N}, 2^{n+1}-1 \in [-42,42] \Leftrightarrow 2^{n+1}-1 \leq 42 \Leftrightarrow n \leq log_2(43)-1 \Leftrightarrow n \leq 4$.
Ici, $n = 5$ *est une borne du nombre d'itérations de la boucle.*

On pose $\mathcal{A} = \{\begin{pmatrix} a & 0 & b \\ c & d & e \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}), a \in [0,64], b \in [-63,1], c \in [-\frac{1}{3},21], d \in [-1,1], e \in [-\frac{62}{3},0]\}$)

On a alors : $\mathcal{I} \subset \mathcal{A} \otimes \mathcal{X}$

$= conv(\{\begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ -5 \end{pmatrix}, \begin{pmatrix} -63 \\ -1 \end{pmatrix}, \begin{pmatrix} -63 \\ -6 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix},$
$\begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{50}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ 5 \end{pmatrix}, \begin{pmatrix} -63 \\ -1 \end{pmatrix}, \begin{pmatrix} -63 \\ 4 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ \frac{217}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ \frac{202}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix},$
$\begin{pmatrix} -63 \\ -5 \end{pmatrix}, \begin{pmatrix} -63 \\ 93 \end{pmatrix}, \begin{pmatrix} -63 \\ 88 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ \frac{217}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ \frac{232}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ 5 \end{pmatrix}, \begin{pmatrix} -63 \\ 93 \end{pmatrix}, \begin{pmatrix} -63 \\ 98 \end{pmatrix},$
$\begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -5 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -6 \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix},$
$\begin{pmatrix} 1 \\ -\frac{50}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{217}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{202}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -5 \end{pmatrix}, \begin{pmatrix} 1 \\ 93 \end{pmatrix}, \begin{pmatrix} 1 \\ 88 \end{pmatrix},$
$\begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{217}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{232}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 93 \end{pmatrix}, \begin{pmatrix} 1 \\ 98 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ -\frac{62}{3} \end{pmatrix},$
$\begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ -5 \end{pmatrix}, \begin{pmatrix} 129 \\ -1 \end{pmatrix}, \begin{pmatrix} 129 \\ -6 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ -\frac{50}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ 5 \end{pmatrix}, \begin{pmatrix} 129 \\ -1 \end{pmatrix}, \begin{pmatrix} 129 \\ 4 \end{pmatrix},$
$\begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ \frac{217}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ \frac{202}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ -5 \end{pmatrix}, \begin{pmatrix} 129 \\ 93 \end{pmatrix}, \begin{pmatrix} 129 \\ 88 \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 129 \\ \frac{217}{3} \end{pmatrix},$
$\begin{pmatrix} 129 \\ \frac{232}{3} \end{pmatrix}, \begin{pmatrix} -63 \\ 0 \end{pmatrix}, \begin{pmatrix} -63 \\ 5 \end{pmatrix}, \begin{pmatrix} 129 \\ 93 \end{pmatrix}, \begin{pmatrix} 129 \\ 98 \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 193 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 193 \\ -\frac{62}{3} \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -5 \end{pmatrix}, \begin{pmatrix} 193 \\ -1 \end{pmatrix},$

$\binom{193}{-6}, \binom{1}{-\frac{62}{3}}, \binom{1}{-\frac{62}{3}}, \binom{193}{-\frac{62}{3}}, \binom{193}{-\frac{50}{3}}, \binom{1}{0}, \binom{1}{5}, \binom{193}{-1}, \binom{193}{4}, \binom{1}{-\frac{62}{3}}, \binom{1}{-\frac{62}{3}}, \binom{193}{\frac{217}{3}},$
$\binom{193}{\frac{202}{3}}, \binom{1}{0}, \binom{1}{-5}, \binom{193}{93}, \binom{193}{88}, \binom{1}{-\frac{62}{3}}, \binom{1}{-\frac{62}{3}}, \binom{193}{\frac{217}{3}}, \binom{193}{\frac{232}{3}}, \binom{1}{0}, \binom{1}{5}, \binom{193}{93}, \binom{193}{98}\})$
$= conv(\binom{-63}{-\frac{80}{3}}, \binom{-63}{98}, \binom{193}{-\frac{80}{3}}, \binom{193}{98}\}).$



Dans cet exemple, l'accélération est moins efficace que le widening pour les x positifs mais plus efficaces pour les x négatifs. Cela est dû au fait qu'il faut 5 itérations pour atteindre la borne inférieure et 4 pour la borne supérieure. Or, dans ce cas, il faut considérer 5 itérations de la boucle pour obtenir une approximation correcte de l'invariant, donc on en fait une de trop en ce qui concerne les x positifs.

9 Application à l'analyse WCET

L'analyse Worst Case Execution Time d'un programme consiste à déterminer le temps d'exécution de la plus longue exécution possible de ce programme. Cette borne étant souvent impossible à trouver, on se contente en général d'approximations correctes (i.e. qui surestiment le résultat).

Le calcul d'invariants permet d'estimer, en chaque point d'un programme, la valeur des variables. Cela peut servir à calculer des bornes sur le nombre d'exécutions d'une boucle, ou de manière plus générale le nombre de fois qu'on passe par un point du programme.

Exemple. *Dans notre exemple, on a trouvé par accélération la borne $n = 5$ sur le nombre d'itérations de la boucle.*

Combinées à une évaluation du temps d'exécution de chaque instruction, on en déduit une approximation correcte du pire temps d'exécution.

Références

[1] Sriram Sankaranarayanan Bertrand Jeannet, Peter Schrammel. Abstract acceleration of general linear loops. In *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 529–540. ACM, 11 2013.

[2] P. Cousot and R. Cousot. Abstract interpretation : a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, NY.

[3] P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 84–97, Tucson, Arizona, 1978. ACM Press, New York, NY.