ACI Sécurité et Informatique
Projet APRON

APRON et le domaine des octogones

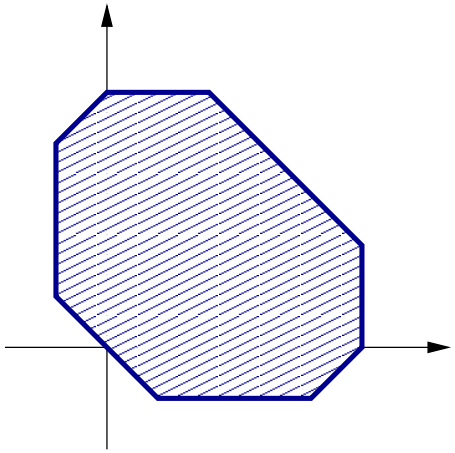
Antoine Miné

École Normale Supérieure

8 novembre 2006

Introduction

Le domaine des **octogones** cherche des invariants de la forme $\pm V_i \pm V_j \leq c$.



- **Précision intermédiaire** entre les intervalles et les polyèdres.
  - Abstraction précise des tests courants.
  - Capable d'inférer des propriétés **relationnelles**.
- **Coût intermédiaire** entre les intervalles (linéaires) et les polyèdres (exponentiel):
  - représentation quadratique en mémoire,
  - coût cubique en temps (au pire).
- Implantation possible en nombre flottants (coût réduit au détriment de la précision).

Exemple d'utilisation des octogones

Exemple 1: (limiteur de vitesse)

```
Y=0;
while (?)  {
  X=rand(-128,128); D=rand(0,16);
  S=Y; Y=X; R=X-S;
  if (R≤-D) Y=S-D;
  if (R≥D)  Y=S+D;
}
```

X: signal d'entrée
Y: signal de sortie
S: sortie précédente
R: dérivée Y−S
D: maximum autorisé pour |R|

- Les intervalles sont impuissants à montrer que $|Y|$ est borné.
- Les polyèdres trouvent $|Y| \leq 128$.
- Les octogones trouvent $|Y| \leq 144$.

Exemple d'utilisation des octogones

Exemple 2: (invariant de boucle)

```
X=0; I=1;
while ● (I<5) {
  if (?)  X=X+1; else X=X-1;
  I=I+1;
} ♦
```

- Les intervalles ne trouvent aucune information sur X en ♦.
- Les octogones et les polyèdres trouvent $X \in [-4, 4]$.

Pour trouver un invariant précis à la sortie d'une boucle ♦,
il faut trouver un invariant de boucle ● de forme plus complexe, **relationnel**:

$$\begin{cases} -I < X < I, \\ I \in [1, 5]. \end{cases}$$

Différences bornées

On s'intéresse tout d'abord aux **contraintes de potentiel**:

$$V_i - V_j \leq c, \quad c \in \mathbb{I}, V_i \in \mathcal{V}$$

- $\mathbb{I} = \mathbb{Q}$ ou $\mathbb{I} = \mathbb{R}$,
- $\mathcal{V}$ est ensemble fini de n variables.

Une conjonction de contraintes de potentiel est représentée par une **matrice de différences bornées (DBM)** $\mathbf{m}$:

- $\mathbf{m}$ est carrée de taille $n \times n$, à valeur dans $\mathbb{I} \cup \{+\infty\}$,
- si $\mathbf{m}_{ij} < +\infty$, c'est la borne supérieure de $V_j - V_i$,
- si $\mathbf{m}_{ij} = +\infty$, $V_j - V_i$ n'est pas borné,
- $\mathbf{m}$ représente l'ensemble de points:

$$\gamma^{\mathsf{DB}}(\mathbf{m}) \stackrel{\text{def}}{=} \{ \vec{x} \in \mathbb{I}^n \mid \forall i, j,\ x_j - x_i \leq \mathbf{m}_{ij} \}.$$

Graphe de potentiel

$\mathbf{m}$ peut être vu comme la matrice d'adjacence d'un **graphe de potentiel**.

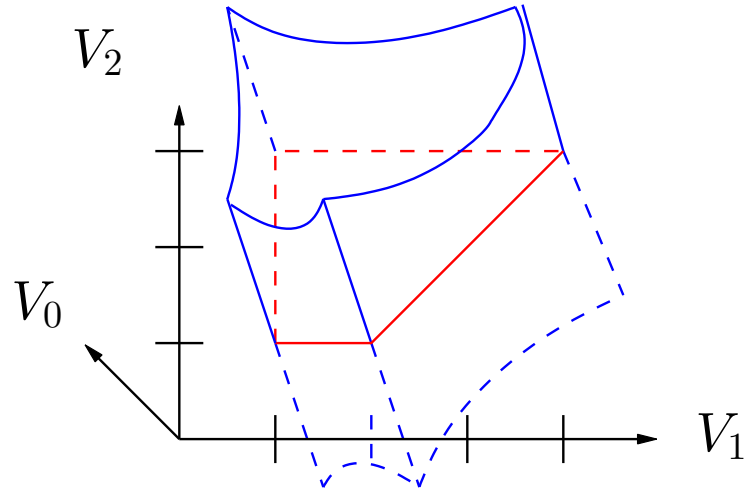
- graphe orienté, de nœuds $\mathcal{V}$,
- si $\mathbf{m}_{ij} < +\infty$, il y a une arête de poids $\mathbf{m}$ de V_i à V_j.

Exemple

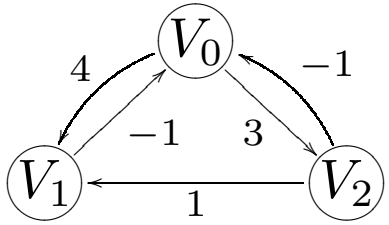
Ensemble de contraintes

$$\begin{cases} V_1 - V_0 \leq 4 \\ V_0 - V_1 \leq -1 \\ V_2 - V_0 \leq 3 \\ V_0 - V_2 \leq -1 \\ V_1 - V_2 \leq 1 \end{cases}$$

Domaine $\gamma^{\mathsf{DB}}(\mathbf{m})$



Graphe de potentiel



Difference-Bound Matrix $\mathbf{m}$

	V_0	V_1	V_2
V_0	$+\infty$	4	3
V_1	−1	$+\infty$	$+\infty$
V_2	−1	1	$+\infty$

Contraintes d'octogones

Soit $\mathcal{V} = \{V_0, \ldots, V_{n-1}\}$ un ensemble de variables.

On note $\mathcal{V}'$ l'ensemble $\mathcal{V}' \stackrel{\text{def}}{=} \{V'_0, \ldots, V'_{2n-1}\}$.

Une contrainte $\pm V_j \pm V_i \leq c$ sur $\mathcal{V}$ est représentée par une contrainte de potentiel sur $\mathcal{V}'$:

$$\begin{array}{lll} V'_{2i} & \text{représente} & +V_i \\ V'_{2i+1} & \text{représente} & -V_i \end{array}$$

La contrainte				est représentée par							
$V_i - V_j$	$\leq$	c	$(i \neq j)$	$V'_{2i} - V'_{2j}$	$\leq$	c	and	$V'_{2j+1} - V'_{2i+1}$	$\leq$	c
$V_i + V_j$	$\leq$	c	$(i \neq j)$	$V'_{2i} - V'_{2j+1}$	$\leq$	c	and	$V'_{2j} - V'_{2i+1}$	$\leq$	c
$-V_i - V_j$	$\leq$	c	$(i \neq j)$	$V'_{2i+1} - V'_{2j}$	$\leq$	c	and	$V'_{2j+1} - V'_{2i}$	$\leq$	c
V_i	$\leq$	c		$V'_{2i} - V'_{2i+1}$	$\leq$	$2c$				
V_i	$\geq$	c		$V'_{2i+1} - V'_{2i}$	$\leq$	$-2c$				

Représentation des octogones

Un octogone peut ainsi être représenté par une DBM de taille $2n \times 2n$.

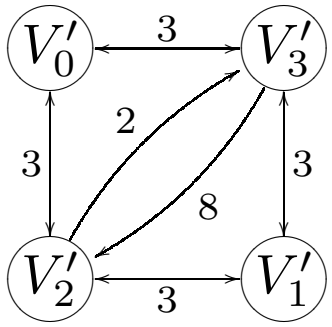
$\mathbf{m}$ représente:

$$\gamma^{\mathsf{Oct}}(\mathbf{m}) \stackrel{\text{def}}{=} \{\ (x_0, \ldots, x_{n-1}) \mid (x_0, -x_0, \ldots, x_{n-1}, -x_{n-1}) \in \gamma^{\mathsf{DB}}(\mathbf{m})\ \}.$$

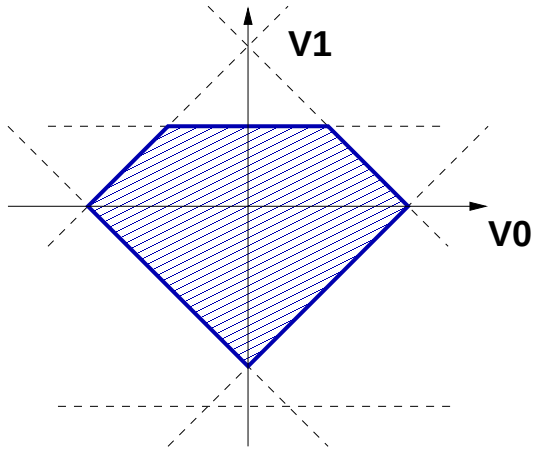
Exemple

$$\begin{cases} V_0 + V_1 \leq 3 \\ V_1 - V_0 \leq 3 \\ V_0 - V_1 \leq 3 \\ -V_0 - V_1 \leq -3 \\ 2V_1 \leq 2 \\ -2V_1 \leq 8 \end{cases}$$

Ensemble de contraintes



Graphe de potentiel



Domaine $\gamma^{\mathsf{Oct}}(\mathbf{m})$

Représentation dans APRON

Note:

Une contrainte binaire peut être représentée par 2 éléments.

$\Longrightarrow$
- On impose: $\mathbf{m}_{ij} = \mathbf{m}_{\bar{j}\bar{i}}$, où $\bar{i} \stackrel{\text{def}}{=} i \texttt{ xor } 1$ $\quad (V'_{2i} \leftrightarrow V'_{2i+1},\ +V_i \leftrightarrow -V_i)$.
- On ne représente que les éléments $\mathbf{m}_{ij}$ tels que $j/2 \leq i/2$.

i \ j

$\times$	$-2V_0$					
$2V_0$	$\times$					
$V_0 - V_1$	$-V_0 - V_1$	$\times$	$-2V_1$			
$V_0 + V_1$	$-V_0 + V_1$	$2V_1$	$\times$			
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$		
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$-2V_{n-1}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$2V_{n-1}$	$\times$

- La diagonale contient des informations sur $V'_i - V'_i$ inutiles $(\times)$.
- $\mathbf{m}$ est représentée par un tableau **plat** de $2n(n+1)$ éléments.
- Si $j/2 \leq i/2$, $\mathbf{m}_{ij}$ se trouve en $j + \frac{(i+1)^2}{2}$ (indépendant de n).

Structure de treillis

- On étend point à point l'ordre $\leq$ sur $\mathbb{I} \cup \{+\infty\}$ sur les DBMs:

$$\begin{array}{rcl}
\mathbf{m} \sqsubseteq^\sharp \mathbf{n} & \overset{\text{def}}{\iff} & \forall i,j,\ \mathbf{m}_{ij} \leq \mathbf{n}_{ij} \\
\mathbf{m} =^\sharp \mathbf{n} & \overset{\text{def}}{\iff} & \forall i,j,\ \mathbf{m}_{ij} = \mathbf{n}_{ij} \\
\left[\mathbf{m} \sqcap^\sharp \mathbf{n}\right]_{ij} & \overset{\text{def}}{=} & \min(\mathbf{m}_{ij}, \mathbf{n}_{ij}) \\
\left[\mathbf{m} \sqcup^\sharp \mathbf{n}\right]_{ij} & \overset{\text{def}}{=} & \max(\mathbf{m}_{ij}, \mathbf{n}_{ij}) \\
\left[\top^\sharp\right]_{ij} & \overset{\text{def}}{=} & +\infty
\end{array}$$

- Le domaine abstrait $D^\sharp$ contient toutes les DBMs, plus un plus petit élément $\bot^\sharp$.

Propriétés:

- $(D^\sharp, \sqsubseteq^\sharp, \sqcup^\sharp, \sqcap^\sharp, \bot^\sharp, \top^\sharp)$ est un **treillis**.
- γ^{DB} et γ^{Oct} sont croissantes:

$$\begin{array}{rcl}
\mathbf{m} \sqsubseteq^\sharp \mathbf{n} & \Longrightarrow & \gamma^{\mathsf{DB}}(\mathbf{m}) \subseteq \gamma^{\mathsf{DB}}(\mathbf{n}) \\
\mathbf{m} \sqsubseteq^\sharp \mathbf{n} & \Longrightarrow & \gamma^{\mathsf{Oct}}(\mathbf{m}) \subseteq \gamma^{\mathsf{Oct}}(\mathbf{n})
\end{array}$$

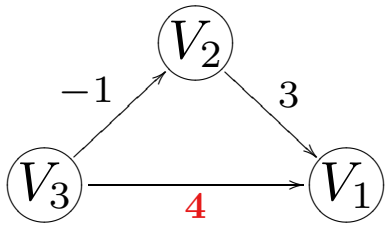
Forme normale pour γ^{DB}

On a: $\gamma^{\mathsf{DB}}(\mathbf{m}) = \gamma^{\mathsf{DB}}(\mathbf{n}) \iff \mathbf{m} =^\sharp \mathbf{n}$
$\gamma^{\mathsf{Oct}}(\mathbf{m}) = \gamma^{\mathsf{Oct}}(\mathbf{n}) \iff \mathbf{m} =^\sharp \mathbf{n}$

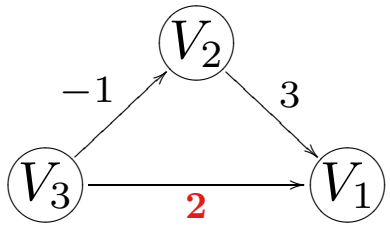
Solution pour les contraintes de potentiel

Propager les contraintes sur des arcs adjacents par addition de poids:

$$\begin{cases} V_1 - V_2 \leq 3 \\ V_2 - V_3 \leq -1 \\ V_1 - V_3 \leq 4 \end{cases}$$



$\Longrightarrow$



$$\begin{cases} V_1 - V_2 \leq 3 \\ V_2 - V_3 \leq -1 \\ V_1 - V_3 \leq 2 \end{cases}$$

Forme normale (si $\gamma^{\mathsf{DB}}(\mathbf{m}) \neq \emptyset$)

Clôture par plus court chemin $\mathbf{m}^*$: $\mathbf{m}^*_{ij} \stackrel{\text{def}}{=} \min_{\langle i=i_1,\ldots,i_N=j\rangle} \sum_{k=1}^{N-1} \mathbf{m}_{i_k\, i_{k+1}}$.

On a: $\mathbf{m}^* = \min_{\sqsubseteq^\sharp} \{\, \mathbf{n} \mid \gamma^{\mathsf{DB}}(\mathbf{m}) = \gamma^{\mathsf{DB}}(\mathbf{n}) \,\}$.

Implantation: algorithme de Floyd-Warshall, en $\mathcal{O}(n^3)$.

Forme normale pour γ^{Oct}

$\mathbf{m}^*$ ne donne pas une forme normale vis-à-vis de γ^{Oct}.

Idée

Utiliser **deux** propagations locales:

$$\left\{ \begin{array}{l} V'_i - V'_k \leq c \\ V'_k - V'_j \leq d \end{array} \right. \Longrightarrow V'_i - V'_k \leq c + d \qquad \text{et} \qquad \left\{ \begin{array}{l} V'_i - V'_j \leq c \\ V'_i - V'_{\bar{j}} \leq d \end{array} \right. \Longrightarrow V'_i \leq (c+d)/2$$

Algorithme de Floyd-Warshall modifié

$\mathbf{m}^\bullet$ est défini comme le résultat $\mathbf{m}^{n+1}$ de l'algorithme suivant:

(A) $\left\{ \begin{array}{l} \mathbf{m}^1 = \mathbf{m} \\ \mathbf{m}^{k+1} = S(C^{2k}(\mathbf{m}^k)),\ 1 \leq k \leq n \end{array} \right.$

(B) $[S(\mathbf{n})]_{ij} = \min(\mathbf{n}_{ij}, (\mathbf{n}_{i\,\bar{\imath}} + \mathbf{n}_{\bar{\jmath}j})/2)$

(C) $\left\{ \begin{array}{l} [C^k(\mathbf{n})]_{ij} = \min(\quad \mathbf{n}_{ij}, \\ \qquad\qquad\qquad\quad \mathbf{n}_{ik} + \mathbf{n}_{kj}, \\ \qquad\qquad\qquad\quad \mathbf{n}_{i\bar{k}} + \mathbf{n}_{\bar{k}j}, \\ \qquad\qquad\qquad\quad \mathbf{n}_{ik} + \mathbf{n}_{k\bar{k}} + \mathbf{n}_{\bar{k}j}, \\ \qquad\qquad\qquad\quad \mathbf{n}_{i\bar{k}} + \mathbf{n}_{\bar{k}k} + \mathbf{n}_{kj} \quad) \end{array} \right.$

Forme normale pour γ^{Oct} (suite)

Propriétés de $\mathbf{m}^\bullet$:

- $\gamma^{\mathsf{Oct}}(\mathbf{m}) = \emptyset \iff \exists i,\ \mathbf{m}^\bullet_{ii} < 0.$
- si $\gamma^{\mathsf{Oct}}(\mathbf{m}) \neq \emptyset$, $\mathbf{m}^\bullet$ est une forme normale:
  $$\mathbf{m}^\bullet = \min_{\sqsubseteq^\sharp} \{\ \mathbf{n} \mid \gamma^{\mathsf{Oct}}(\mathbf{n}) = \gamma^{\mathsf{Oct}}(\mathbf{m})\ \}.$$
- $\gamma^{\mathsf{Oct}}(\mathbf{m}) = \gamma^{\mathsf{Oct}}(\mathbf{n}) \iff \mathbf{m}^\bullet =^\sharp \mathbf{n}^\bullet.$
  $\gamma^{\mathsf{Oct}}(\mathbf{m}) \subseteq \gamma^{\mathsf{Oct}}(\mathbf{n}) \iff \mathbf{m}^\bullet \sqsubseteq^\sharp \mathbf{n}.$
- $\mathbf{m}^\bullet$ a un coût **cubique**.
  Une version incrémentale, de coût quadratique existe.

Octogones entiers

$\mathbf{m}^*$ est une forme normale sur γ^{DB} pour $\mathbb{I} = \mathbb{Z}$.

$\mathbf{m}^\bullet$ **n'est pas** une forme normale sur γ^{Oct} pour $\mathbb{I} = \mathbb{Z}$!

Une forme normale en $\mathcal{O}(n^4)$ existe (non implantée).

Opérateurs ensemblistes abstraits

Intersection abstraite (exacte)

- $\sqcap^\sharp$ donne toujours l'intersection **exacte**:
$$\gamma^{\mathsf{Oct}}(\mathbf{m} \sqcap^\sharp \mathbf{n}) = \gamma^{\mathsf{Oct}}(\mathbf{m}) \cap \gamma^{\mathsf{Oct}}(\mathbf{n}).$$
- $(\mathbf{m}^\bullet) \sqcap^\sharp (\mathbf{n}^\bullet)$ n'est généralement pas en forme normale.

Union abstraite (optimale)

- Les octogones sont convexes, donc non clos pas union.
- $\sqcup^\sharp$ est toujours une abstraction valide de l'union:
$$\gamma^{\mathsf{Oct}}(\mathbf{m} \sqcup^\sharp \mathbf{n}) \supseteq \gamma^{\mathsf{Oct}}(\mathbf{m}) \cup \gamma^{\mathsf{Oct}}(\mathbf{n}).$$
mais elle n'est pas toujours optimale...
- $(\mathbf{m}^\bullet) \sqcup^\sharp (\mathbf{n}^\bullet)$ est, par contre, **optimal**:
$$(\mathbf{m}^\bullet) \sqcup^\sharp (\mathbf{n}^\bullet) = \min_{\sqsubseteq^\sharp} \{ \mathbf{o} \mid \gamma^{\mathsf{Oct}}(\mathbf{o}) \supseteq \gamma^{\mathsf{Oct}}(\mathbf{m}) \cup \gamma^{\mathsf{Oct}}(\mathbf{n}) \}$$
en particulier:
$$\gamma^{\mathsf{Oct}}((\mathbf{m}^\bullet) \sqcup^\sharp (\mathbf{n}^\bullet)) = \min_{\subseteq} \{ \gamma^{\mathsf{Oct}}(\mathbf{o}) \mid \gamma^{\mathsf{Oct}}(\mathbf{o}) \supseteq \gamma^{\mathsf{Oct}}(\mathbf{m}) \cup \gamma^{\mathsf{Oct}}(\mathbf{n}) \}.$$
- $(\mathbf{m}^\bullet) \sqcup^\sharp (\mathbf{n}^\bullet)$ est toujours en forme normale.

Projections

Intervalle d'une variable

$$\pi_i(X) \stackrel{\text{def}}{=} \{\ x \in \mathbb{I} \mid \exists \vec{x} \in X, \text{ tel que } x_i = x\ \}$$

est abstrait par:

$$\pi_i^{\mathsf{Oct}}(\mathbf{m}) = \left[-\frac{\mathbf{m}^{\bullet}_{(2i)\,(2i+1)}}{2},\ \frac{\mathbf{m}^{\bullet}_{(2i+1)\,(2i)}}{2} \right]$$

Oubli d'une variable (affectation non déterministe)

$$\{\!|\ V_f \leftarrow ?\ |\!\}(X) \stackrel{\text{def}}{=} \{\ \vec{x}[x_f \mapsto v] \mid \vec{x} \in X,\ v \in \mathbb{I}\ \}$$

est abstrait par:

$$\left[\{\!|\ V_f \leftarrow ?\ |\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=} \begin{cases} \mathbf{m}^{\bullet}_{ij} & \text{si } \lfloor i/2 \rfloor \neq f \text{ et } \lfloor j/2 \rfloor \neq f \\ 0 & \text{si } i = j \text{ et } \lfloor i/2 \rfloor = f \\ +\infty & \text{sinon} \end{cases}$$

- Ces opérateurs sont **exacts**.
- Sans normalisation, ils ne sont plus exacts mais restent sûrs.

Affectations abstraites

On chercher à abstraire l'effet d'une affectation: $V_f \leftarrow [a_0, b_0] + \sum_i [a_i, b_i] V_i$.
(forme affine avec coefficients intervalles)

$$\{\!| V_f \leftarrow [a_0, b_0] + \textstyle\sum_i [a_i, b_i] V_i |\!\}(X) \stackrel{\text{def}}{=} \{ \vec{x}[x_f \mapsto t] \mid \vec{x} \in X,\ t_i \in [a_i, b_i],\ t = t_0 + \textstyle\sum t_i x_i \}$$

Affectations exactes seulement pour $V_f \leftarrow \alpha V_k + [a, b]$ où $\alpha \in \{-1, 0, 1\}$.

Cas non inversibles (perte d'information)

- $\left[\{\!| V_{j_0} \leftarrow [a, b] |\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$

$$\begin{cases} -2a & \text{si } i = 2j_0,\ j = 2j_0 + 1 \\ 2b & \text{si } i = 2j_0 + 1,\ j = 2j_0 \\ \left[\{\!| V_{j_0} \leftarrow ? |\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} & \text{sinon} \end{cases}$$

- $\left[\{\!| V_{j_0} \leftarrow V_{i_0} + [a, b] |\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$ $(j_0 \neq i_0)$

$$\begin{cases} -a & \text{si } i = 2j_0,\ j = 2i_0 \text{ ou } i = 2i_0 + 1,\ j = 2j_0 + 1 \\ b & \text{si } i = 2i_0,\ j = 2j_0 \text{ ou } i = 2j_0 + 1,\ j = 2i_0 + 1 \\ \left[\{\!| V_{j_0} \leftarrow ? |\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} & \text{sinon} \end{cases}$$

Affectations abstraites (suite)

Cas inversibles

- $\left[\!\{\!\{ V_{j_0} \leftarrow V_{j_0} + [a,b] \}\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$

$$\begin{cases} \mathbf{m}_{ij} - a & \text{si } i = 2j_0,\ j \neq 2j_0, 2j_0+1 \text{ ou } j = 2j_0,\ i \neq 2j_0, 2j_0+1 \\ \mathbf{m}_{ij} + b & \text{si } i \neq 2j_0, 2j_0+1,\ j = 2j_0 \text{ ou } j \neq 2j_0, 2j_0+1,\ i = 2j_0+1 \\ \mathbf{m}_{ij} - 2a & \text{si } i = 2j_0,\ j = 2j_0+1 \\ \mathbf{m}_{ij} + 2b & \text{si } i = 2j_0+1,\ j = 2j_0 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

- $\left[\!\{\!\{ V_{j_0} \leftarrow -V_{j_0} \}\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$

$$\begin{cases} \mathbf{m}_{\bar{i}j} & \text{si } i \in \{2j_0, 2j_0+1\} \text{ et } j \notin \{2j_0, 2j_0+1\} \\ \mathbf{m}_{i\bar{j}} & \text{si } i \notin \{2j_0, 2j_0+1\} \text{ et } j \in \{2j_0, 2j_0+1\} \\ \mathbf{m}_{\bar{i}\bar{j}} & \text{si } i \in \{2j_0, 2j_0+1\} \text{ et } j \in \{2j_0, 2j_0+1\} \\ \mathbf{m}_{ij} & \text{si } i \notin \{2j_0, 2j_0+1\} \text{ et } j \notin \{2j_0, 2j_0+1\} \end{cases}$$

Affectations abstraites (suite)

Affectations approchées trois compromis coût / précision

- Abstraction par les intervalles

$$\{\!|\, V_f \leftarrow [a_0, b_0] + \textstyle\sum_i [a_i, b_i] V_i \,|\!\}^{\mathsf{Oct}}(\mathbf{m}) \stackrel{\text{def}}{=} \{\!|\, V_f \leftarrow [a, b] \,|\!\}^{\mathsf{Oct}}(\mathbf{m})$$

où

$$[a, b] \stackrel{\text{def}}{=} [a_0, b_0] + \textstyle\sum_i [a_i, b_i] \times \pi_i^{\mathsf{Oct}}(\mathbf{m})$$

est calculé par **arithmétique d'intervalles**.

- Abstraction par les polyèdres

Exact, mais coûteux, et implémenté seulement pour $V_f \leftarrow a_0 + \sum_i a_i V_i$.

- Abstraction semi-relationnelle

Pour tous les $i \neq k$ on calcule une borne de $\pm V_f \pm V_k$ par intervalles.
e.g.: $\mathbf{m}'_{(2i)\,f} = \max\left([a_0, b_0] + \left(\sum_{k \neq i} [a_k, b_k] \times \pi_k^{\mathsf{Oct}}(\mathbf{m})\right) + [a_i - 1, b_i - 1] \times \pi_i^{\mathsf{Oct}}(\mathbf{m})\right)$.
(coût total linéaire, si $\mathbf{m}$ est déjà en forme normale)

Affectations abstraites (suite)

Exemple d'affectations approchées:

Argument

$$\begin{cases} 0 \leq Y \leq 10 \\ 0 \leq Z \leq 10 \\ 0 \leq Y - Z \leq 10 \end{cases}$$

$$\Downarrow \; X \leftarrow Y - Z$$

$$\begin{cases} -10 \leq X \leq 10 \\ -20 \leq X - Y \leq 10 \\ -10 \leq X + Y \leq 20 \\ -20 \leq X - Z \leq 10 \\ -10 \leq X + Z \leq 20 \end{cases}$$

Intervalles

$$\begin{cases} -5 \leq X \leq 10 \\ -10 \leq X - Y \leq 0 \\ 0 \leq X + Y \leq 20 \\ -10 \leq X - Z \leq 10 \\ 0 \leq X + Z \leq 10 \end{cases}$$

Semi-relationnel

$$\begin{cases} 0 \leq X \leq 10 \\ -10 \leq X - Y \leq 0 \\ 0 \leq X + Y \leq 20 \\ -10 \leq X - Z \leq 10 \\ 0 \leq X + Z \leq 10 \end{cases}$$

Meilleur abstraction
(par les polyèdres)

Utilisation des coefficients intervalles

Application: analyse des calculs en **virgule flottante**.

Chaque opérateur flottant $\oplus$, $\ominus$, $\otimes$, $\oslash$ induit un arrondi non linéaire.

Exemple: $Z \leftarrow X \ominus (0.25 \otimes Y)$

$\{\!|\, Z \leftarrow X - (0.25 \times Y) \,|\!\}^{\mathsf{Oct}}(\mathbf{m})$ n'est pas une abstraction sûre!

Solution

L'arrondi est approximé par une erreur non-déterministe:

- erreur relative d'amplitude 2^{-23} (`float` simple précision normalisé),
- erreur absolue d'amplitude 2^{-159} (`float` simple précision dénormalisé).

Exemple:

$X \ominus (0.25 \otimes Y)$ est approximé **sur** $\mathbb{Q}$ en:
$[0.99999980790710449 22, 1.00000011920928955 08] \times X$
$+[-0.25000005960464832 81, -0.24999994039535167 19] \times Y$
$+[-1.17549442088721072 42e^{-38}, 1.17549442088721072 42e^{-38}]$.

Tests abstrait

On chercher à abstraire l'effet d'une garde: $[a_0, b_0] + \sum_i [a_i, b_i] V_i \leq 0$?.

$$\{\!\!\{ [a_0, b_0] + \textstyle\sum_i [a_i, b_i] V_i \leq 0 \ ? \}\!\!\}(X) \stackrel{\text{def}}{=}$$
$$\{ \vec{x} \in X \mid \exists t_i \in [a_i, b_i] \text{ tels que } v_0 + \textstyle\sum_i t_i x_i \leq 0 \}.$$

Tests exacts

Seulement pour $\alpha V_i + \beta V_j + [a, b] \geq 0$ où $\alpha, \beta \in \{-1, 0, 1\}$.

- $\left[\{\!\!\{ V_{j_0} + [a, b] \leq 0 \ ? \}\!\!\}^{\text{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$

$$\begin{cases} \min(\mathbf{m}_{ij}, -2a) & \text{si } i = 2j_0 + 1,\ j = 2j_0 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

- $\left[\{\!\!\{ -V_{j_0} + [a, b] \leq 0 \ ? \}\!\!\}^{\text{Oct}}(\mathbf{m})\right]_{ij} \stackrel{\text{def}}{=}$

$$\begin{cases} \min(\mathbf{m}_{ij}, -2a) & \text{si } i = 2j_0,\ j = 2j_0 + 1 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

Tests abstraits (suite)

- $\left[\{\!\!\{ V_{j_0} - V_{i_0} + [a,b] \leq 0 \ ? \}\!\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \overset{\text{def}}{=}$

$$\begin{cases} \min(\mathbf{m}_{ij}, -a) & \text{si } i = 2i_0,\ j = 2j_0 \text{ ou } i = 2j_0+1,\ j = 2i_0+1 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

- $\left[\{\!\!\{ V_{j_0} + V_{i_0} + [a,b] \leq 0 \ ? \}\!\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \overset{\text{def}}{=}$

$$\begin{cases} \min(\mathbf{m}_{ij}, -a) & \text{si } i = 2i_0+1,\ j = 2j_0 \text{ ou } i = 2j_0+1,\ j = 2i_0 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

- $\left[\{\!\!\{ -V_{j_0} - V_{i_0} + [a,b] \leq 0 \ ? \}\!\!\}^{\mathsf{Oct}}(\mathbf{m})\right]_{ij} \overset{\text{def}}{=}$

$$\begin{cases} \min(\mathbf{m}_{ij}, -a) & \text{si } i = 2i_0,\ j = 2j_0+1 \text{ ou } i = 2j_0,\ j = 2i_0+1 \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

Coût en $\mathcal{O}(1)$.

La forme normale n'est jamais nécessaire.

Tests abstraits (suite)

Tests approchés

- Abstraction par l'identité.
- Abstraction par les intervalles.
- Abstraction par les polyèdres.
  (seulement pour $a_0 + \sum_i a_i V_i \geq 0$)
- Abstraction semi-relationnelle.

  Pour chaque $i \neq j$, $\pm V_i \pm V_j$ est approximé dans les intervalles.
  e.g.: $\mathbf{m}'_{(2i)\,(2j)} = \min(\mathbf{m}_{(2i)\,(2j)}, x)$ où

$$\begin{aligned} x = \max \{ & -[a_0, b_0] \\ & - \textstyle\sum_{k \neq i,j} [a_k, b_k] \times \pi_k^{\mathsf{Oct}}(\mathbf{m}) \\ & -[a_i + 1, b_i + 1] \times \pi_i^{\mathsf{Oct}}(\mathbf{m}) \\ & -[a_j - 1, b_j - 1] \times \pi_j^{\mathsf{Oct}}(\mathbf{m}) \ \}. \end{aligned}$$

  (coût quadratique, si $\mathbf{m}$ est déjà en forme normale)

Substitutions abstraites

On chercher à abstraire l'effet d'une substitution dans l'ensemble des contraintes:
$V_f \longrightarrow [a_0, b_0] + \sum_i [a_i, b_i] V_i$.

$$\{\!\!\{ V_f \longrightarrow [a_0, b_0] + \sum_i [a_i, b_i] V_i \}\!\!\}(X) \stackrel{\text{def}}{=}$$
$$\{\ \vec{x} \mid \exists t_i \in [a_i, b_i] \text{ tels que } \vec{x}[x_f \longrightarrow t_0 + \sum t_i x_i] \in X\ \}$$

Abstractions

Similaires au cas des affectations:

- Cas exacts: $V_f \longrightarrow \alpha V_i + [a, b]$ où $\alpha \in \{-1, 0, 1\}$.
  Les cas inversibles $(i = f)$ se réduisent à des affectations.
- Cas approchés:
  - par projection $(V_f \leftarrow ?)$,
  - par les intervalles,
  - par les polyèdres (seulement pour $V_f \longrightarrow a_0 + \sum_i a_i V_i$),
  - par approximation semi-relationnelle (coût cubique...).

Élargissements

Élargissement classique

Extension point à point de l'élargissement sur les intervalles:

On enlève les contraintes non stables:

$$[\mathbf{m} \triangledown \mathbf{n}]_{ij} \stackrel{\text{def}}{=} \begin{cases} \mathbf{m}_{ij} & \text{si } \mathbf{m}_{ij} \geq \mathbf{n}_{ij} \\ +\infty & \text{sinon} \end{cases}$$

Élargissement étagé

Paramétré par un ensemble **fini** $\mathbb{T} \subseteq \mathbb{I}$ d'étages:

$$[\mathbf{m} \triangledown \mathbf{n}]_{ij} \stackrel{\text{def}}{=} \begin{cases} \mathbf{m}_{ij} & \text{si } \mathbf{m}_{ij} \geq \mathbf{n}_{ij} \\ \min \{ x \in \mathbb{T} \cup \{+\infty\} \mid x \geq \mathbf{n}_{ij} \} & \text{sinon} \end{cases}$$

Plus précis, mais peut nécessiter plus d'itérations pour la stabilisation.

Élargissements et forme normale

Attention à l'interaction entre élargissement et la normalisation:

- $\mathbf{m}_{i+1} \overset{\text{def}}{=} \mathbf{m}_i \triangledown \mathbf{n}_i$ converge,
- $\mathbf{m}_{i+1} \overset{\text{def}}{=} \mathbf{m}_i \triangledown (\mathbf{n}_i^\bullet)$ converge,
- $\mathbf{m}_{i+1} \overset{\text{def}}{=} (\mathbf{m}_i \triangledown \mathbf{n}_i)^\bullet$ **ne converge plus**!

Intuition: $\triangledown$ augmente les coefficients de $\mathbf{m}_i$, $\bullet$ les diminue.

Exemple:

```
X=0; Y=rand(-1,1);
while ● (rand(0,1)=0) {
  R=rand(-1,1);
  if (X=Y) Y=X+R
  else X=Y+R
}
```

itération $2j$ en ●	itération $2j+1$ en ●
$X \in [-2j, 2j]$	$X \in [-2j-2, 2j+2]$
$Y \in [-2j-1, 2j+1]$	$Y \in [-2j-1, 2j+1]$
$X - Y \in [-1, 1]$	$X - Y \in [-1, 1]$

Rétrécissement

Rétrécissement classique

Extension point à point du rétrécissement sur les intervalles:

On ne raffine que les contraintes infinies:

$$[\mathbf{m} \vartriangle \mathbf{n}]_{ij} \stackrel{\text{def}}{=} \begin{cases} \mathbf{n}_{ij} & \text{si } \mathbf{m}_{ij} = +\infty \\ \mathbf{m}_{ij} & \text{sinon} \end{cases}$$

Interaction avec la forme normale

Pas de problème:

- $\mathbf{m}_{i+1} \stackrel{\text{def}}{=} \mathbf{m}_i \vartriangle \mathbf{n}_i$ converge,
- $\mathbf{m}_{i+1} \stackrel{\text{def}}{=} \mathbf{m}_i \vartriangle (\mathbf{n}_i^\bullet)$ converge,
- $\mathbf{m}_{i+1} \stackrel{\text{def}}{=} (\mathbf{m}_i \vartriangle \mathbf{n}_i)^\bullet$ converge.

Tableau des opérateurs abstraits

opérateur	coût	précision	argument en forme normale	résultat en forme normale
$\cap$	$\mathcal{O}(n^2)$	**exact**	non	non
$\cup$	$\mathcal{O}(n^2)$	optimal	oui	oui
$V \leftarrow ?$	$\mathcal{O}(n)$	**exact**	oui	non†
$V \leftarrow \pm V' + [a,b]$	$\mathcal{O}(n)$	**exact**	oui/non	non†
$V \rightarrow \pm V' + [a,b]$	$\mathcal{O}(n)$	**exact**	oui/non	non†
$\pm V' + \pm V''[a,b] \leq 0\,?$	$\mathcal{O}(1)$	**exact**	non	non
$V \leftarrow l$	$\mathcal{O}(n)$	moyenne	oui	non†
$V \rightarrow l$	$\mathcal{O}(n^3)$	moyenne	oui	non
$l \leq 0\,?$	$\mathcal{O}(n^2)$	moyenne	oui	non
∇	$\mathcal{O}(n^2)$	-	non‡	non
$\triangle$	$\mathcal{O}(n^2)$	-	oui	non

† La forme normale peut être calcule incrémentalement en $\mathcal{O}(n^2)$.

‡ Les itérés ne doivent pas être clos.

Utilisation de la clôture dans APRON

Stratégie utilisée dans APRON:

- Par défaut, **clore l'argument seulement si cela améliore la précision**.
  (modifiable par l'utilisateur: `algorithme` < 0)
- À cause de ∇, on ne remplace jamais subrepticement une DBM par sa forme normale.
  ($\neq$ polyèdres)
- On garde les formes closes en **cache**.
  Chaque DBM $\mathbf{m}$ garde un pointeur vers $\mathbf{m}^\bullet$ (`NULL` si non calculée).
  Le cache est détruit quand $\mathbf{m}$ est détruit.
- Si l'opérateur respecte la clôture, le résultat a automatiquement un cache.
- Si l'opérateur est de coût quadratique au moins,
  et que la **clôture incrémentale** s'applique,
  le cache du résultat est calculé. (temps quadratique)

Domaine numérique sous-jacent

Deux choix pour $\mathbb{I}$.

Rationnels multi-précision

- Arithmétique exacte sur $\mathbb{Q}$ grâce à GMP.
- Optimalité garantie si on abstrait des rationnels.
- Optimalité non garantie si on abstrait des entiers, mais sans conséquence pratique.
  (cf. polyèdres)

Flottants machine

- Sûreté garantie par l'arrondi vers $+\infty$ des opérations de base.
  ($+$, $\min$, $\max$, division et division par 2)
- Très rapide!
  (coût indépendant de la taille des coefficients, $+\infty$ gratuit, etc.)
- Optimalité non garantie, mais précision suffisante en pratique.
- Idéals pour abstraire des calculs flottants, après abstraction sûre des erreurs d'arrondis.

Implantation

- Module `octagons` dans APRON: **4771** lignes de C.
- Test de régression unitaire: 1566 lignes de C
  - tests de sûreté et d'optimalité par comparaison avec le résultat sur les polyèdres,
  - tests sur des entrées aléatoires,
  - a permis de trouver aussi des bogues dans les polyèdres!
- **Intégration expérimentale** dans `Astrée`:
  - remplace la 'vielle' implantation `octlib`,
  - glue: 992 lignes de OCaml,
  - résultats encourageants, mais à améliorer:

	lignes de code	**itérations**	**temps**	**mémoire**	**alarmes**
`octlib`	68535	21	24mn	494 Mo	2
APRON	68535	21	24mn	473 Mo	2
`octlib`	237546	73	6h40	1.5 Go	2
APRON	237546	69	14h50	1.2 Go	2
`octlib`	420886	80	11h50	2.5 Go	0
APRON	420886	78	29h40	1.8 Go	0

Travaux futurs

- Profiler et améliorer le coût des octogones (et d'APRON).

- Grâce à l'interface commune, comparer expérimentalement octogones et polyèdres:
  - intégrer les octogones aux projets polyèdres (e.g., NBac),
  - intégrer les polyèdres à Astrée,
  - contacter les projets hors APRON utilisant NewPolka ou les octogones,
  - intégrer à APRON un analyseur académique.

- Expérimenter de nouveaux opérateurs:
  - abstractions semi-relationnelles plus précises,
  - opérateurs d'élargissement et d'extrapolation.