

Séminaire des élèves du Département d'Informatique

---

# Représentation de contraintes numériques simples et application à l'analyse automatique de programmes

---

Antoine Miné

Doctorant au Département d'Informatique de l'ENS  
Équipe Sémantique et Interprétation Abstraite (P.Cousot)  
bureau S17



6 novembre 2001

# Plan de l'exposé

---

- Introduction à l'analyse statique de programmes
- Construction du domaine abstrait des graphes de potentiel  $x - y \leq c$
- Généralisation aux octogones  $\pm x \pm y \leq c$
- Généralisation à  $x - y \in D$ , où  $D$  est à valeur dans une algèbre quasi-dioïde

# Introduction à la sémantique

Idée : associer à un programme  $p$  un objet mathématique  $\llbracket p \rrbracket$  décrivant son comportement.

Exemple :

$$\begin{array}{ccc} \Sigma^* & \longrightarrow & \mathbb{S} \\ p & \longmapsto & \llbracket p \rrbracket \end{array}$$

```
let fibo a =  
  if a < 2 then 1  
  else fibo(a-1)+fibo(a-2)
```

$$f \in (\mathbb{Z} \mapsto \mathbb{Z})$$

But : prouver formellement la correction d'un programme : absence de bugs, respect d'une spécification, terminaison, etc. par une preuve mathématique sur  $\llbracket p \rrbracket$ .

Analyse statique : construire un programme permettant de calculer **automatiquement**  $\llbracket \cdot \rrbracket$ . Comme  $\llbracket \cdot \rrbracket$  n'est généralement pas calculable, on se contentera d'une **approximation décidable et sûre**  $\llbracket \cdot \rrbracket^\#$ .

# Découverte d'invariants numériques

Hypothèse : programmes sans procédure, les variables  $v \in \mathcal{V}$  sont à valeur dans  $\mathbb{I}$ ,  $\mathbb{I} = \mathbb{Z}, \mathbb{Q}$  ou  $\mathbb{R}$ .

Sémantique : à chaque **point de programme**  $p_i$  on associe un **invariant**  $X_i \in \mathcal{P}(\mathcal{V} \mapsto \mathbb{I})$  valable à tout instant de toute exécution de  $p$  [Floyd 76].

Exemple :

```
int a, x, tab[-max,max]
x := 1; a := 0; (1)
while x < max do (2)
  if rand(2)=0
    then a := a+1 (3)
    else a := a-1 (4)
  (5) x := x+1 (6)
done (7)
tab[a] := tab[a]+1
```

$X_1$ :	$x = 1$	$a = 0$	
$X_2$ :	$0 \leq x < \max$	$-x \leq a \leq x$	$a \equiv x [2]$
$X_3$ :	$0 \leq x < \max$	$-x \leq a \leq x + 1$	$a \equiv x + 1 [2]$
$X_4$ :	$0 \leq x < \max$	$-x - 1 \leq a \leq x$	$a \equiv x + 1 [2]$
$X_5$ :	$0 \leq x < \max$	$-x - 1 \leq a \leq x + 1$	$a \equiv x + 1 [2]$
$X_6$ :	$0 < x \leq \max$	$-x \leq a \leq x$	$a \equiv x [2]$
$X_7$ :	$x = \max$	$-\max \leq a \leq \max$	$a \equiv \max [2]$

Utilité : éviter les divisions par 0, dépassement de bornes de tableau, prouver des exclusions mutuelles, etc.

# Méthode de calcul des invariants

Méthode : propagation des  $X_i$  le long du **graphe du flux de contrôle** jusqu'à obtenir la stabilité.

Algorithme : [Kleene 52]

- initialisation :  $X_i^0 = \emptyset$  ;
- calcul :  $X_i^{k+1} = F_i(X_1^k, \dots, X_N^k)$  ;
- arrêt : quand  $\forall i, X_i^k = X_i^{k-1}$ .

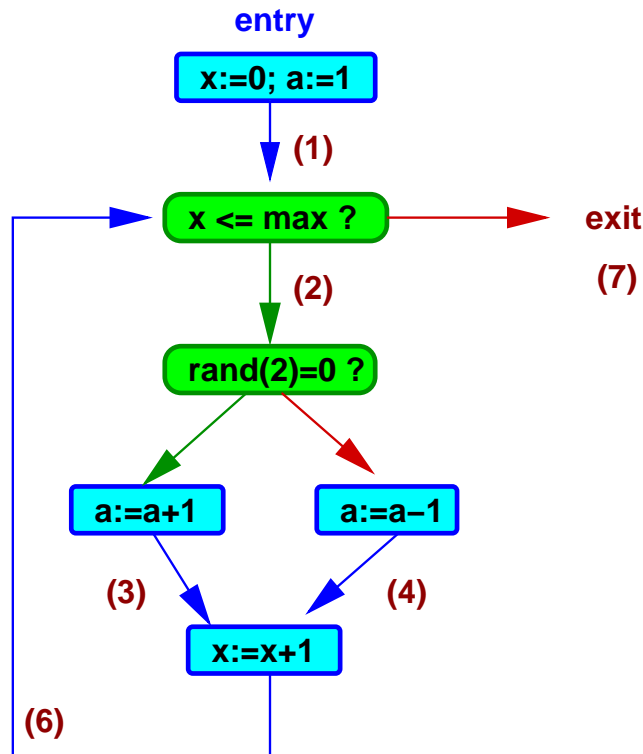
$F_i$  est appelée **fonction de transfert**

Exemple :  $X_6^{k+1} = \{ (x+1, a) \mid (x, a) \in X_3^k \cup X_4^k \}$

Le calcul n'est pas automatisable car :

- $X_i^k \in \mathcal{P}(\mathcal{V} \mapsto \mathbb{I})$  pas représentable en machine ;
- les itérations peuvent se stabiliser à  $\omega$ .

Problème : comment définir une méthode approchée **sûre** et **calculable** ?



# Interprétation abstraite pour les invariants numériques

L'**interprétation abstraite** est une théorie de comparaison des sémantiques [Cousot Cousot 77].

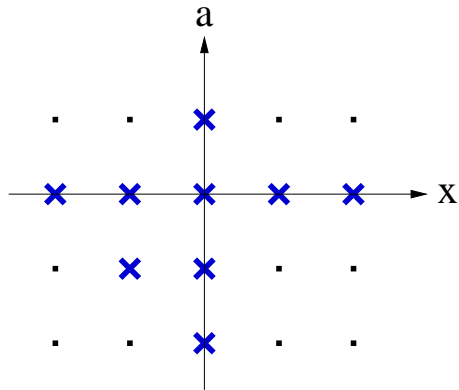
## Méthodologie : définition d'un **domaine numérique abstrait**

- choix d'un **ensemble abstrait**  $\mathbb{D}^\#$  représentable en mémoire : chaque  $D^\# \in \mathbb{D}^\#$  correspond à un invariant par  $\Gamma : \mathbb{D}^\# \mapsto \mathcal{P}(\mathcal{V} \mapsto \mathbb{I})$  ;
- chaque invariant  $D \in \mathcal{P}(\mathcal{V} \mapsto \mathbb{I})$  a une approximation  $D^\#$  dans  $\mathbb{D}^\#$  :  $\Gamma(D^\#) \supseteq D$  ;
- chaque fonction de transfert  $F$  a une approximation  $F^\#$  calculable dans  $\mathbb{D}^\#$  :  $\Gamma(F^\#(D_1^\#, \dots, D_N^\#)) \supseteq F(\Gamma(D_1^\#), \dots, \Gamma(D_N^\#))$  ;
- définition d'une structure d'ordre partiel ou de **treillis** sur  $\mathbb{D}^\#$  ;
- définition d'un opérateur d'**accélération de convergence** (élargissement  $\nabla$ ).

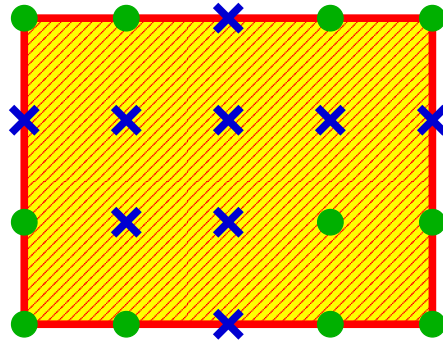
Propriété : l'interprétation abstraite garantit que  $X_i^\#$  est **calculable en temps fini** et vérifie  $\Gamma(X_i^\#) \supseteq X_i$  (sûreté).

Conclusion : les problèmes sémantiques sont résolus, la définition de domaines abstraits adaptés et efficaces relève de l'algorithmique...

# Domaines abstraits classiques



Domaine concret

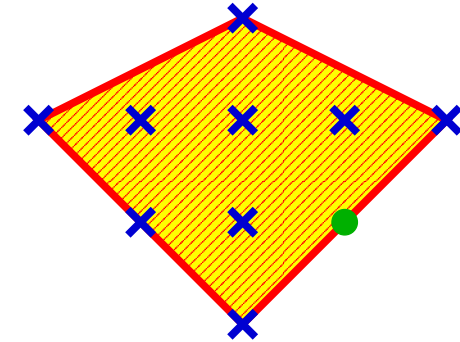


Domaine des intervalles

$\Gamma(\mathbb{D}^\#) = \{ \text{boites} \}$   
[Cousot Cousot 76]

$v \in [a, b]$   
coût linéaire

$$X_7^\# : x \geq 1$$



Domaine des polyèdres

$\Gamma(\mathbb{D}^\#) = \{ \text{polyèdres convexes} \}$   
[Cousot Halbwachs 78]

$\alpha_1 v_0 + \dots + \alpha_n v_{n-1} \leq c$   
coût exponentiel

$$X_7^\# : \begin{cases} x = \mathbf{max} \\ -\mathbf{max} \leq a \leq \mathbf{max} \end{cases}$$

But : enrichir le choix de domaines abstraits pour adapter le ratio coût / précision.

# Introduction aux Graphes de Potentiel

---

Soit  $\mathcal{V} = \{v_0, \dots, v_{n-1}\}$  un ensemble de variables à valeur dans  $\mathbb{I}$  ( $\mathbb{I} = \mathbb{Z}, \mathbb{Q}$  ou  $\mathbb{R}$ ).  
Une **contrainte de potentiel** est de la forme  $x - y \leq c$ ,  $x, y \in \mathcal{V}$ ,  $c \in \mathbb{I}$ .

## Représentations :

Le **graphe de potentiel**  $\mathcal{G}$  est le graphe **orienté, pondéré** défini par

- les noeuds sont étiquetés par les éléments de  $\mathcal{V}$ ;
- il y a un arc de poids  $c$  de  $v_i$  à  $v_j$  si  $(v_j - v_i \leq c) \in D^\#$ .

La **matrice d'adjacence**  $\mathbf{m}$  de  $\mathcal{G}$  est définie par :

- $\mathbf{m}$  est carrée, de dimension  $n \times n$ , d'éléments à valeur dans  $\mathbb{I} \cup \{+\infty\}$ ;
- $\mathbf{m}_{ij} = c < +\infty$  si  $(v_j - v_i \leq c) \in D^\#$ ;
- $\mathbf{m}_{ij} = +\infty$  sinon ;
- $\mathbf{m}$  est aussi appelée **Difference-Bound Matrix** (DBM).

$\mathbf{m}$  représente l'invariant  $\Gamma(\mathbf{m})$  appelé **zone** :

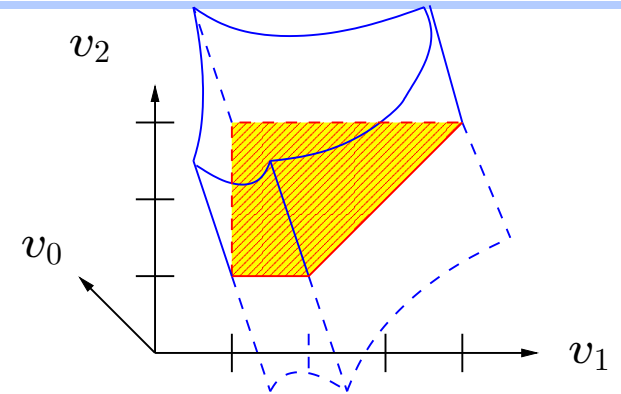
$$\Gamma(\mathbf{m}) = \{ (x_0, \dots, x_{n-1}) \in \mathbb{I}^n \mid \forall i, j, x_j - x_i \leq \mathbf{m}_{ij} \}$$

# Exemple

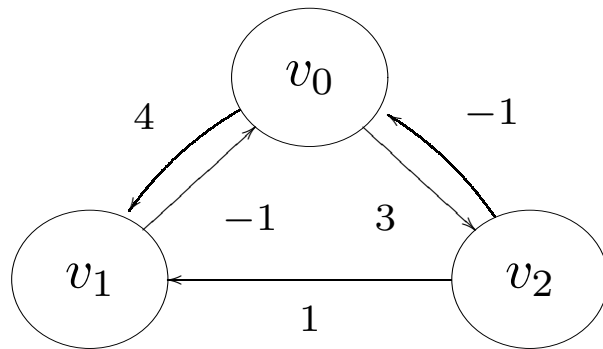
Système de contraintes

$$\begin{cases} v_1 - v_0 \leq 4 \\ v_0 - v_1 \leq -1 \\ v_2 - v_0 \leq 3 \\ v_0 - v_2 \leq -1 \\ v_1 - v_2 \leq 1 \end{cases}$$

Invariant



Graphe de potentiel



Matrice d'adjacence (DBM)

	$v_0$	$v_1$	$v_2$
$v_0$	$+\infty$	4	3
$v_1$	-1	$+\infty$	$+\infty$
$v_2$	-1	1	$+\infty$

Extension : on pose la **contrainte implicite**  $v_0 = 0$  pour permettre à un graphe de potentiel de représenter des contraintes de la forme  $v_i \leq c$  par  $v_i - v_0 \leq v$ .

Idée : peut-on utiliser cette représentation pour définir un nouveau domaine numérique abstrait correspondant à des **invariants de la forme  $x - y \leq c$  et  $\pm x \leq c$ ?**

Pour cela : définir une structure de treillis, des fonctions de transfert et d'accélération de convergence.

# Structure mathématique des matrices d'adjacence

Treillis : extension point-à-point de l'ordre partiel  $(\mathbb{I} \cup \{+\infty\}, \min, \max)$ .

$$\begin{aligned} \mathbf{m} \trianglelefteq \mathbf{n} &\iff \forall i, j, \mathbf{m}_{ij} \leq \mathbf{n}_{ij} && \text{ordre partiel} \\ [\mathbf{m} \wedge \mathbf{n}]_{ij} &= \min(\mathbf{m}_{ij}, \mathbf{n}_{ij}) && \text{plus grand minorant} \\ [\mathbf{m} \vee \mathbf{n}]_{ij} &= \max(\mathbf{m}_{ij}, \mathbf{n}_{ij}) && \text{plus petit majorant} \end{aligned}$$

En ajoutant un plus petit élément  $\perp$ , l'ensemble des matrices d'adjacence forme un **treillis**.

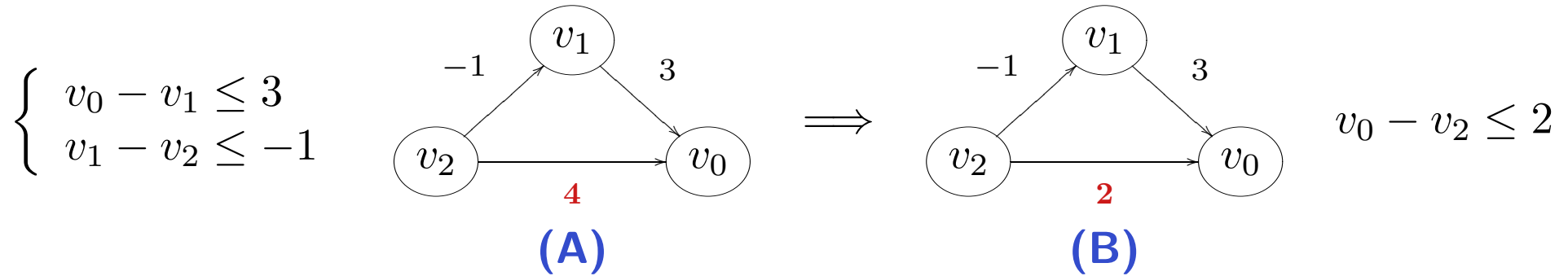
## Passage à $\Gamma$ :

- $\Gamma$  n'est **pas injective** :  $\Gamma(\mathbf{m}) = \Gamma(\mathbf{n}) \not\Rightarrow \mathbf{m} = \mathbf{n}$  ;
- $\mathbf{m} \trianglelefteq \mathbf{n} \implies \Gamma(\mathbf{m}) \subseteq \Gamma(\mathbf{n})$ , mais pas la réciproque ;
- $\Gamma(\mathbf{m} \wedge \mathbf{n}) = \Gamma(\mathbf{m}) \cap \Gamma(\mathbf{n})$  ;
- $\Gamma(\mathbf{m} \vee \mathbf{n}) \supseteq \Gamma(\mathbf{m}) \cup \Gamma(\mathbf{n})$ .

Problèmes : comment déterminer  $\Gamma(\mathbf{m}) \stackrel{?}{=} \emptyset$ ,  $\Gamma(\mathbf{m}) \stackrel{?}{=} \Gamma(\mathbf{n})$ ,  $\Gamma(\mathbf{m}) \stackrel{?}{\subseteq} \Gamma(\mathbf{n})$  ?  
existe-t-il une **meilleure approximation** pour  $\cup$  ?

# Forme normale et test du vide

Idée : dériver des contraintes **implicites** par sommation de poids sur des chemins



Théorème :

- $\Gamma(\mathbf{m}) = \emptyset \iff \mathcal{G}$  a un cycle de poids total strictement négatif;
- si  $\Gamma(\mathbf{m}) \neq \emptyset$ , le graphe de plus court chemin  $\mathbf{m}^*$  **est une forme normale** :  $\mathbf{m}^* = \min_{\triangleleft} \{ \mathbf{n} \mid \Gamma(\mathbf{m}) = \Gamma(\mathbf{n}) \}$ ;
- si  $\Gamma(\mathbf{m}), \Gamma(\mathbf{n}) \neq \emptyset$ , alors  $\Gamma(\mathbf{m}) \subseteq \Gamma(\mathbf{n}) \iff \mathbf{m}^* \triangleleft \mathbf{n}^*$ ,  $\Gamma(\mathbf{m}) = \Gamma(\mathbf{n}) \iff \mathbf{m}^* = \mathbf{n}^*$  et  $\Gamma(\mathbf{m}^* \vee \mathbf{n}^*)$  est la **meilleure approximation** de  $\Gamma(\mathbf{m}) \cup \Gamma(\mathbf{n})$ .

Définition du plus court chemin :

$$\mathbf{m}_{ij}^* = \min_{\langle i=i_1, \dots, i_N=j \rangle} \sum_{k=1}^{N-1} \mathbf{m}_{i_k i_{k+1}}$$

# Algorithme de Floyd-Warshall

Algorithme de Floyd-Warshall : clôture par plus court chemin

$$\begin{cases} \mathbf{m}_{ij}^0 = \mathbf{m}_{ij} \\ \mathbf{m}_{ij}^{k+1} = \min(\mathbf{m}_{ij}^k, \mathbf{m}_{ik}^k + \mathbf{m}_{kj}^k) \end{cases}$$

Théorème :

- $\Gamma(\mathbf{m}) = \emptyset \iff \exists i, \mathbf{m}_{ii}^n < 0$ ;
- Si  $\Gamma(\mathbf{m}) \neq \emptyset$ , alors  $\mathbf{m}^* = \mathbf{m}^n$ ;
- $\mathbf{m}^n$  se calcule en temps  $\mathcal{O}(n^3)$ .

Treillis des matrices closes :

- on considère l'ensemble des matrices closes :  $\mathbf{m}^* = \mathbf{m}$ ;
- on ajoute un plus petit élément  $\perp^*$  et on étend  $\Gamma$  par  $\Gamma(\perp^*) = \emptyset$ ;
- le plus petit majorant est  $\mathbf{m} \vee \mathbf{n}$ , le plus grand minorant est  $(\mathbf{m} \wedge \mathbf{n})^*$  (ou  $\perp^*$ );
- on obtient un treillis isomorphe par  $\Gamma$  à un sous-treillis de  $\mathcal{P}(\mathcal{V} \mapsto \mathbb{I})$ .

## Modélisation d'un test : $e(v_0, \dots, v_{n-1}) \leq 0$

$$\Gamma(\mathbf{m}_{(e \leq 0)}) \supseteq \{ (x_0, \dots, x_{n-1} \mid (x_0, \dots, x_{n-1}) \in \Gamma(\mathbf{m}), e(x_0, \dots, x_{n-1}) \leq 0 \}$$

## Exemples de définitions :

- $\left[ \mathbf{m}_{(x_{j_0} - x_{i_0} \leq c)} \right]_{ij} = \begin{cases} \min(\mathbf{m}_{ij}, c) & \text{si } (i, j) = (i_0, j_0), \\ \mathbf{m}_{ij} & \text{sinon.} \end{cases}$
- $\mathbf{m}_{(? \leq 0)} = \mathbf{m}$

## Modélisation de l'affectation : $v_i \leftarrow e(v_0, \dots, v_{n-1})$

$$\Gamma(\mathbf{m}_{(v_i \leftarrow e)}) \supseteq \{ (x_0, \dots, x'_i, \dots, x_{n-1} \mid (x_0, \dots, x_{n-1}) \in \Gamma(\mathbf{m}), x'_i = e(x_0, \dots, x_{n-1}) \}$$

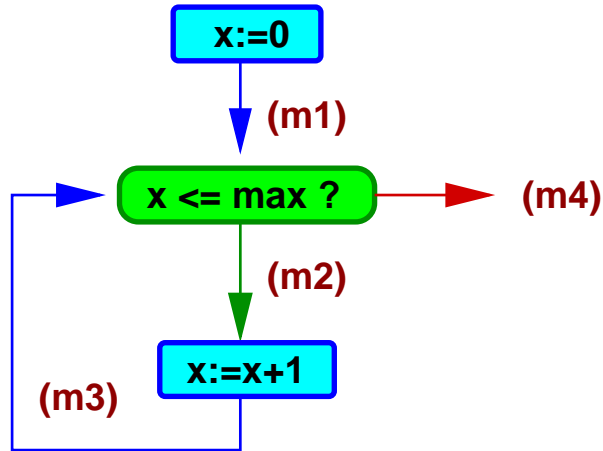
## Exemples de définitions :

- $\left[ \mathbf{m}_{(x_{j_0} \leftarrow ?)} \right]_{ij} = \begin{cases} +\infty & \text{si } i = j_0 \text{ ou } j = j_0, \\ \mathbf{m}_{ij}^* & \text{sinon.} \end{cases}$
- $\mathbf{m}_{(x_{j_0} \leftarrow x_{i_0} + c)} = ((\mathbf{m}_{(x_{j_0} \leftarrow ?)})_{(x_{j_0} - x_{i_0} \leq c)})_{(x_{i_0} - x_{j_0} \leq -c)}$  quand  $i_0 \neq j_0$

Il est possible de modéliser tout le langage à partir de ces fonctions,  $\cup$  et  $\cap$ .

# Élargissement

Problème : même dans  $\mathbb{D}^\#$ , les itérations peuvent se stabiliser à  $\omega$ .



$$\begin{cases} \mathbf{m}2^0 : x = 0 \\ \mathbf{m}2^{k+1} : (\mathbf{m}2^k)^* \vee (((\mathbf{m}2^k)_{(x \leftarrow x+1)})_{(x \leq \max)})^* \end{cases}$$

$$\mathbf{m}2^k : 0 \leq x, x \leq k, x \leq \max$$

$$\mathbf{m}2^\omega : 0 \leq x \leq \max$$

Solution : opérateur d'élargissement  $\nabla$  [Cousot 77]

- $\Gamma(\mathbf{m} \nabla \mathbf{n}) \supseteq \Gamma(\mathbf{m}) \cup \Gamma(\mathbf{n})$  ;
- $\forall \mathbf{m}_0, (\mathbf{n}_i)_{i \in \mathbb{N}}$ , la suite  $(\mathbf{m}_i)_{i \in \mathbb{N}}$  définie par  $\mathbf{m}_{i+1} = \mathbf{m}_i \nabla \mathbf{n}_i$  est **ultimement stationnaire**.

Définition :  $[\mathbf{m} \nabla \mathbf{n}]_{ij} = \begin{cases} \mathbf{m}_{ij} & \text{si } \mathbf{n}_{ij} \leq \mathbf{m}_{ij}, \\ +\infty & \text{sinon.} \end{cases}$

# Représentation des octogones

But : étendre des graphes de potentiel à la représentation de contraintes  $\pm x \pm y \leq c$ .

Idée : se ramener à des contraintes de la forme  $x' - y' \leq c$  par changement de variables.

Soit  $\mathcal{V}' = \{ v'_0, \dots, v'_{2n-1} \}$ .

Un ensemble de contraintes de la forme  $\pm x \pm y \leq c$  sur  $\mathcal{V}$  s'écrit comme un **graphe de potentiel** sur  $\mathcal{V}'$  où

la contrainte	est représentée par
$v_i - v_j \leq c \quad (i \neq j)$	$v'_{2i} - v'_{2j} \leq c$ et $v'_{2j+1} - v'_{2i+1} \leq c$
$v_i + v_j \leq c \quad (i \neq j)$	$v'_{2i} - v'_{2j+1} \leq c$ et $v'_{2j} - v'_{2i+1} \leq c$
$-v_i - v_j \leq c \quad (i \neq j)$	$v'_{2j+1} - v'_{2i} \leq c$ et $v'_{2i+1} - v'_{2j} \leq c$
$v_i \leq c$	$v'_{2i} - v'_{2i+1} \leq 2c$
$v_i \geq c$	$v'_{2i+1} - v'_{2i} \leq -2c$

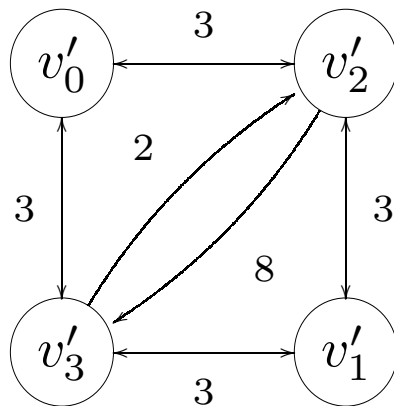
Contrainte :  $\forall i, j, \mathbf{m}_{ij} = \mathbf{m}_{\bar{j}\bar{i}} \quad \bar{i} = i \oplus 1$

$\mathbf{m}$  représente l'invariant  $\Gamma'(\mathbf{m})$  appelé **octogone** :

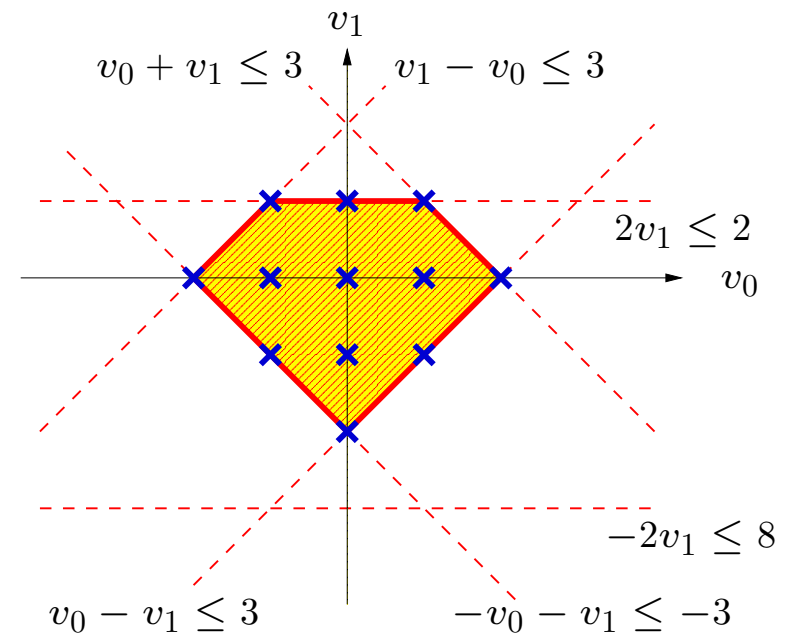
$$\Gamma'(\mathbf{m}) = \{ (x_0, \dots, x_{n-1}) \in \mathbb{I}^n \mid (x_0, -x_0, \dots, x_{n-1}, -x_{n-1}) \in \Gamma(\mathbf{m}) \}$$

# Exemple

Graphe de potentiel



Invariant



Problème : peut-on adapter les algorithmes du domaine des graphes de potentiel aux octogones ?

Solution : une fois le problème de la forme normale résolu, les opérateurs d'union, d'intersection, d'élargissement, le test d'inclusion, d'égalité, de vide et les fonctions de transferts s'adaptent facilement.

# Forme normale pour les octogones

Problème : la clôture  $\mathbf{m}^*$  n'est pas une forme normale !

Idée : utiliser deux transformations locales

$$\begin{cases} v'_i - v'_k \leq c \\ v'_k - v'_j \leq d \end{cases} \implies v'_i - v'_j \leq c + d$$

$$\begin{cases} v'_i - v'_j \leq c \\ v'_i - v'_j \leq d \end{cases} \implies v'_i \leq (c + d)/2$$

Algorithme de Floyd-Warshall modifié :

$$(A) \begin{cases} \mathbf{m}^0 = \mathbf{m} \\ \mathbf{m}^{k+1} = S(C^{2k}(\mathbf{m}^k)), \quad 0 \leq k < n \end{cases}$$

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

$$(C) \begin{cases} [C^k(\mathbf{n})]_{ij} = \min( & \mathbf{n}_{ij}, \\ & \mathbf{n}_{ik} + \mathbf{n}_{kj}, \\ & \mathbf{n}_{i\bar{k}} + \mathbf{n}_{\bar{k}j}, \\ & \mathbf{n}_{ik} + \mathbf{n}_{k\bar{k}} + \mathbf{n}_{\bar{k}j}, \\ & \mathbf{n}_{i\bar{k}} + \mathbf{n}_{\bar{k}k} + \mathbf{n}_{kj} ) \end{cases}$$

Théorème : valable si  $\mathbb{I} \neq \mathbb{Z}$

- $\Gamma'(\mathbf{m}) = \emptyset \iff \exists i, \mathbf{m}_{ii}^n < 0$  ;
- Si  $\Gamma'(\mathbf{m}) \neq \emptyset$ , alors  $\mathbf{m}^n = \min_{\triangleleft} \{ \mathbf{n} \mid \Gamma'(\mathbf{m}) = \Gamma'(\mathbf{n}) \}$ .

Si  $\mathbb{I} = \mathbb{Z}$  on n'a qu'une forme **semi-normale**

# Autre généralisation des graphes de potentiel

Idée : choisir un sous-ensemble  $\mathbb{C}$  de  $\mathcal{P}(\mathbb{I})$  et représenter un ensemble de contraintes de la forme  $x - y \in C$ ,  $C \in \mathbb{C}$ , par une matrice  $n \times n$  d'éléments de  $\mathbb{C}$ .

Exemples :

- $\mathbb{C} = \{ [a, b], \emptyset, \mathbb{I} \}$  donne les contraintes de potentiel ;
- $\mathbb{C} = \{ a\mathbb{Z} + b, \emptyset \}$  donne des contraintes de la forme  $x \equiv y + a \pmod{b}$ .

Algorithme Floyd-Warshall étendu :

$$\begin{cases} \mathbf{m}_{ij}^0 = \mathbf{m}_{ij} \\ \mathbf{m}_{ij}^{k+1} = \mathbf{m}_{ij}^k \cap (\mathbf{m}_{ik}^k \oplus \mathbf{m}_{kj}^k) \end{cases} \quad (A \oplus B = \{ a + b \mid a \in A, b \in B \})$$

Problème : est-ce une forme normale ?

Théories existantes : théorie spectrale sur les semi-anneaux

	$\mathbb{C}$	$\cap$	$\oplus$	$\mathbb{I}$	$\emptyset$	$\emptyset \cap \mathbb{I} = \emptyset$
algèbres tropicales	$\mathbb{Z} \cup \{-\infty\}$	max	+	$-\infty$		
algèbres dioides	$\mathbb{Z} \cup \{+\infty, -\infty\}$	max	+	$-\infty$	$+\infty$	$(+\infty) + (-\infty) = -(\infty)$

# Proposition d'extension

Définition :  $\mathbb{C}$  est un sous-ensemble de  $\mathcal{P}(\mathbb{I})$

- **stable** par  $\cap$  et  $\oplus$  ;
- si  $A \in \mathbb{C}$ , alors  $\{ -a \mid a \in A \} \in \mathbb{C}$  ;
- si  $A \cap B, A \cap C, B \cap C \neq \emptyset$ , alors  $A \cap B \cap C \neq \emptyset$  ;
- pour toute famille  $(A_i)_{i \in I}$ , si  $\bigcap_{i \in I} A_i \neq \emptyset$  alors  $\bigcap_{i \in I} (A \oplus A_i) = A \oplus (\bigcap_{i \in I} A_i)$ .

Théorème : gestion du caractère **relationnel** du domaine

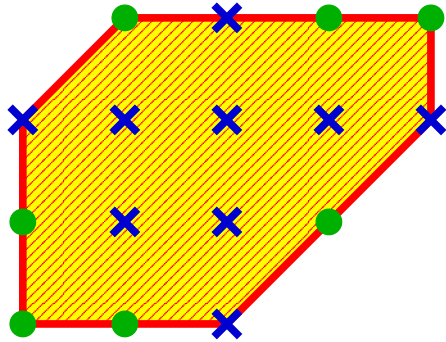
Si  $\mathbf{m}$  vérifie  $\forall i, j, \mathbf{m}_{ij} = -\mathbf{m}_{ji}$ , alors

- $\Gamma(\mathbf{m}) = \emptyset \iff \exists i, 0 \notin \mathbf{m}_{ii}^n$  ;
- Si  $\Gamma(\mathbf{m}) \neq \emptyset$ , alors  **$\mathbf{m}^n$  est la clôture par plus court chemin de  $\mathbf{m}$**  ;

Reste à déterminer : est-ce une forme normale ?

Construction du domaine abstrait : les opérateurs booléens et les fonctions de transfert se fabriquent au cas par cas par extension des opérations naturelles sur  $\mathbb{C}$ .

# Résultats



Domaine des contraintes  
de potentiel

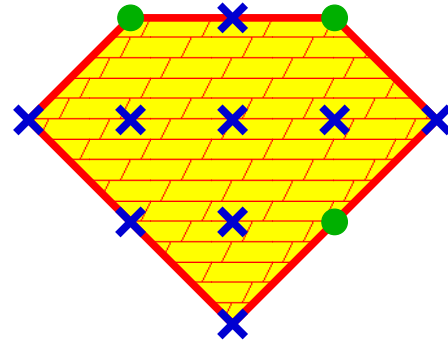
$$\Gamma(\mathbb{D}^\#) = \{ \text{zones} \}$$

[Miné 01]

$$x - y \leq c$$

coût cubique

$$X_7^\# : \begin{cases} x = \mathbf{max} \\ a \leq \mathbf{max} \end{cases}$$



Domaine des octogones

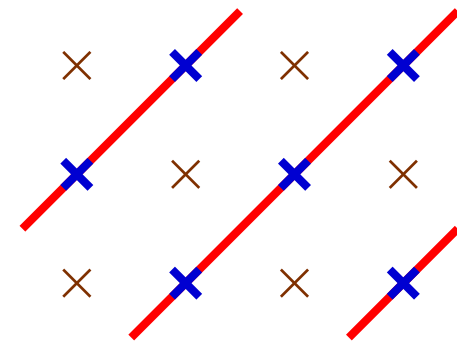
$$\Gamma'(\mathbb{D}^\#) = \{ \text{octogones} \}$$

[Miné 01]

$$\pm x \pm y \leq c$$

coût cubique

$$X_7^\# : \begin{cases} x = \mathbf{max} \\ -\mathbf{max} \leq a \leq \mathbf{max} \end{cases}$$



Domaine des congruences  
de différence

$$\Gamma''(\mathbb{D}^\#) = \{ \text{congruences} \}$$

$$x \equiv y + a [b]$$

coût cubique

$$X_7^\# : \begin{cases} x = \mathbf{max} \\ a \equiv \mathbf{max} [2] \end{cases}$$