# THÈSE

présentée à l'École Normale Supérieure de Cachan

pour obtenir le grade de

**Docteur de l'École Normale Supérieure de Cachan**

par : Jérôme Leroux

Spécialité : Informatique

# Algorithmique de la vérification des systèmes à compteurs. Approximation et accélération. Implémentation de l'outil Fast.

Soutenue le 12 décembre 2003 devant un jury composé de :

- André Arnold — président du jury
- Bernard Boigelot — rapporteur
- Ahmed Bouajjani — rapporteur
- Alain Finkel — directeur de thèse
- Nicolas Halbwachs — examinateur
- Markus Müller-Olm — examinateur

Merci !

CHAPITRE 1

# Introduction

L'objectif de cette thèse est d'apporter de nouvelles méthodes pour vérifier des propriétés d'accessibilité de systèmes à compteurs. Nous employons le mot "méthode" pour désigner un ensemble de théorèmes fondamentaux situant les problèmes décidables et indécidables ainsi que leurs complexités, un ensemble de théorèmes d'algorithmique ainsi que des heuristiques, choisies après expérimentations, permettant d'implémenter avec efficacité les théorèmes précédents. Ces méthodes ont été implémentées dans un nouvel outil FAST.

Les systèmes à compteurs contiennent tous les automates à compteurs et recouvrent des objets différents comme les programmes et les modèles à variables entières. Les protocoles qui assurent la cohérence des mémoires caches [EN98, EFM99], [Del00a, Del01], les protocoles qui évitent la formation de cliques dans le graphe de communication d'un système embarqué comme le TTP/C [BM02] et les programmes JAVA multithread [DRV01] sont des exemples de programmes qui ont été modélisés par des systèmes à compteurs. On peut aussi abstraire un protocole de communication en un système d'automates où les canaux de communication sont représentés par un ensemble de compteurs (un par type de messages).

Même lorsque l'ensemble des états accessibles d'un système à compteurs est fini, et donc que les problèmes d'accessibilité sont décidables, ces problèmes ne sont pas nécessairement réellement solubles avec les ressources (temps CPU et mémoire vive) limitées habituelles. Or l'ensemble des états accessibles d'un système à compteurs est souvent infini. En effet, la borne des files de communication d'un protocole n'est pas toujours connue à l'avance, les variables entières peuvent aussi être non bornées (par exemple, le nombre de retransmissions d'un message dans le protocole BRP) et l'ensemble des états initiaux peut aussi être infini pour modéliser une infinité de processus ; enfin le modèle peut contenir des paramètres.

Bien que ce modèle des systèmes à compteurs soit très utilisé, il n'existait pas en 2000 d'outil permettant de calculer automatiquement l'ensemble des états accessibles. Seuls LASH et TREX permettaient de calculer l'accélération d'une boucle de contrôle d'un système à compteurs (avec des gardes restreintes à des fragments de la logique de Presburger) ; cependant ces outils ne proposaient pas de procédure de calcul de l'ensemble des états accessibles.

Nous nous sommes fixés comme objectif, dès le début de la thèse, de construire un outil calculant automatiquement l'ensemble des états accessibles (et des approximations supérieures, par union d'espaces affines et des approximations inférieures, par accélérations) de systèmes à une dizaine de compteurs.

## Outils pour représenter des ensembles infinis

La vérification d'un système revient souvent à calculer son ensemble d'accessibilité. Pour vérifier un système infini, il est ainsi important de pouvoir représenter des ensembles infinis d'états.

### Représentations symboliques

Une représentation symbolique décrit de manière finie une partie infinie d'un ensemble. De façon habituelle, une classe de représentations symboliques doit satisfaire deux sortes de propriétés :

- L'ensemble des états accessibles "en une étape" (les Post et Pre) à partir d'un ensemble, symboliquement représenté, doivent aussi pouvoir être décrits symboliquement ; on demande de plus que ces descriptions puissent être calculées par un algorithme (les ensembles sont alors dit effectivement représentables).
- L'union de deux ensembles est effectivement représentable. L'inclusion entre ensembles représentés et le vide de l'intersection entre deux ensembles représentés doivent être décidables.

Parmi les nombreuses représentations existantes, citons :

- les unions finies de contraintes fournissent une représentation symbolique des polyèdres, utilisées pour analyser les systèmes hybrides [HH95] [Hyt].
- Les DBM [Dil90] représentent des ensembles de valeurs d'horloges par une disjonction de "contraintes simples" de la forme $x-y \leqslant c$. Cette représentation a été étendue aux CPDBM [AAB00] pour pouvoir ajouter des paramètres sur les compteurs et des variables entières. Les outils Uppaal et Trex, par exemple, [ABS01, Tre] implémentent cette représentation pour vérifier les automates temporisés.
- Pour les automates à file, des classes d'expressions régulières et la logique de Presburger ont été utilisées comme représentations symboliques : les CQDD [BH99], les QDD [BGWW97], les SRE [ABJ98] et les SLRE [FPS03].
- Enfin, pour les systèmes à compteurs, les représentations symboliques des ensembles semi-linéaires sont bien adaptées [Cia94, DJS99], [DRB02, ADG+02, Bab],[ST98], [BGP97].

On s'intéresse aux trois représentations symboliques permettant de représenter *tous* les semi-linéaires.

- Les formules de Presburger qui peuvent être simplifiées par l'outil Omega [Ome], ont été utilisées dans l'outil de vérification Csl-Alv [Alv].
- Les représentation par bases/périodes [GS66] sont utilisées dans l'outil Brain [RV02, Bra].

- Les automates binaires, appelés NDD, RVA [Boi98, WB00] et DFA [BC96], permettent de représenter tout ensemble semi-linéaire en décomposant un entier en binaire ou plus généralement dans une base de décomposition $r \geqslant 2$ [BHMV94].

La complexité des opérations ensemblistes diffère pour les trois représentations symboliques précédentes. Ainsi, alors que l'union de deux ensembles se représente effectivement en temps polynômial pour ces trois représentations (linéaire pour les deux premières et quadratique pour la dernière), l'inclusion et le test du vide de l'intersection de deux ensembles est 2-expspace-dur pour les formules de Presburger, NP-complet pour les semi-linéaires et quadratique pour les automates binaires.

Dans cette thèse, on étudie la représentation par automates qui est la seule représentation symbolique dont les opérations ensemblistes (sans compter la projection qui peut-être exponentielle en théorie) sont polynômiales.

## Synthèse de formules

Pour comparer la taille des différentes représentations d'un ensemble semi-linéaire, on a étudié le problème de la construction d'une représentation à partir d'une autre. Rappelons que le passage d'une formule de Presburger à une représentation par bases/périodes [GS66, FR74] ou par automates binaires [WB00] se fait en temps élémentaire, et que le passage d'une représentation par bases/périodes à une représentation par formules de Presburger se fait en temps linéaire. Cependant, on ne connaît pas de borne élémentaire de complexité pour construire à partir d'un automate binaire, une formule de Presburger définissant le même ensemble.

Rappelons que les automates binaires permettent de représenter tous les ensembles Presburger-définissables, mais aussi d'autres ensembles dépendant de la base $r \geqslant 2$ de décomposition choisie [BHMV94]. Ainsi, la synthèse d'une formule de Presburger à partir d'un automate n'est pas toujours possible. Le premier problème naturel, est donc de pouvoir décider si un automate représente un ensemble Presburger-définissable. Ce problème a été prouvé décidable dans [Muc03]. Naturellement, en énumérant les formules de Presburger et en construisant les automates associés, on pourrait synthétiser une formule de Presburger à partir de tout automate représentant un ensemble Presburger-définissable. Cependant, la seule borne supérieure connue de cet algorithme est non-élémentaire et la synthèse d'une formule en temps élémentaire reste un problème ouvert.

En remarquant qu'une formule de Presburger est une suite finie de quantificateurs appliqués à une formule non-quantifiée, le problème de la synthèse d'une formule non-quantifiée est un sous-problème naturel de la synthèse d'une formule de Presburger.

Pour ce problème, on a prouvé les deux résultats suivants :

- On peut décider en temps exponentiel si un automate représente un ensemble non quantifié (théorème 5.37).
- On peut synthétiser en temps exponentiel une formule de Presburger non-quantifiée à partir d'un tel automate (théorème 5.40).

Ce dernier résultat est intéressant car il donne une réciproque au théorème de construction d'un automate binaire en temps exponentiel en fonction d'une formule de Presburger non-quantifiée [BC96, WB95, WB00], montrant ainsi que les formules de Presburger et les automates ont des tailles équivalentes, à un facteur exponentiel près, dans le cas non-quantifié.

### Structure et taille asymptotique des automates

Différentes implémentions de la représentation symbolique par automate (Mona, Fast, Lash, Csl-Alv) ont permis de vérifier des systèmes à compteurs avec des temps de calcul et une utilisation mémoire bien en dessous de la complexité théorique attendue [BFLP03, BB02, BB03].

Le calcul de l'automate représentant les états accessibles en une étape (Pre ou Post) à partir d'un ensemble est en général exponentiel en sa représentation. En généralisant le résultat de [BB03], nous avons montré que pour les systèmes à compteurs déterministes, le calcul devient polynômial (théorème 7.3). Nous avons ainsi obtenu *un début de réponse* expliquant la bonne "complexité expérimentale" de la représentation par automates. Cependant, si à chaque étape, la taille de l'automate est doublée, après $k$ étapes, la taille de l'automate est multipliée par un facteur exponentiel en $k$. Pourtant, dans la pratique, on n'observe pas une explosion exponentielle. Pour *expliquer les expérimentations* faites, on s'est ainsi naturellement intéressé à la taille asymptotique de l'automate représentant l'ensemble des états accessibles en au plus $k$ "étapes".

Cette étude nous a permis de prouver deux résultats *inattendus* pour les systèmes à compteurs "à monoïde fini" (une classe de systèmes qui contient tous les automates à compteurs).

- La taille asymptotique en $k$ de l'automate représentant l'ensemble des états accessibles en au plus $k$ étapes est polynômial en $k$ (théorème 7.17).
- Le nombre de composantes fortement connexes non réduites à un état est borné indépendamment de $k$ (proposition 7.15).

Cette dernière caractérisation montre l'intérêt d'implémenter une bibliothèque d'automates utilisant les mêmes techniques que celles utilisées pour les BDD [Bry92].

## Approximation de l'ensemble et de la relation d'accessibilité

Lorsqu'un calcul exact de l'ensemble des états accessibles d'un système a échoué, nous utilisons des méthodes approchées en remarquant les points suivants :

- Le calcul d'une sur-approximation, suffisamment précise, de l'ensemble des états accessibles d'un système, peut permettre de décider une propriété d'accessibilité [BPR02, HJMS02].
- Une sur-approximation de l'ensemble des états "co-accessibles" à partir des états "critiques" du système, permet de restreindre le calcul exact des états accessibles aux états appartenant à cette sur-approximation [DRV01].
- D'une sur-approximation des états accessibles, on déduit des relations entres les variables d'un système permettant de le simplifier [Ler03, MOS04].

Pour des classes d'approximation (qui doivent être stables par intersection quelconque), on peut naturellement approximer un ensemble par le plus petit élément (pour l'inclusion) de la classe d'approximation le contenant. Plusieurs classes d'approximations sont ainsi définies, comme les enveloppes affines [Ler03, MOS04], semi-affine et convexes [Hyt], la clôture par le haut [FS01] et par le bas [BM99], et l'approximation cartésienne [BPR01].

Nous introduisons les représentations “stables par résidus” (si les langages associés sont stables par résidus).

En remarquant que la représentation par NDD n'est pas stable par résidu, nous introduisons les UBA (“Unambiguous Binary Automaton”) qui représentent par des automates ayant toujours moins d'états, les mêmes ensembles que les NDD (théorème 4.40). En montrant que les enveloppes affines, semi-affines, convexes, les clôtures par le haut et par le bas sont des classes d'approximations stables par résidus, on en déduit une méthode générale d'approximation des ensembles représentés par des UBA. Ceci nous permet en particulier :

– de calculer en temps polynômial l'enveloppe affine d'un UBA (corollaire 4.68), et
– de calculer en temps exponentiel l'enveloppe semi-affine d'un UBA (théorème 4.79).

Nous appliquons ces techniques d'approximations, et nous montrons :

– comment généraliser la notion “d'invariants de place” à tout système à compteurs. Comme dans le cas des réseaux de Petri, une base de ces invariants reste calculable en temps polynômial (théorème 8.15).
– comment calculer des “invariants disjonctifs de place”, permettant d'approximer finement les systèmes à compteurs utilisant “des transferts” entre les compteurs (théorème 8.51).

## Calcul de l'ensemble d'accessibilité

Le calcul itératif des états accessibles ne converge pas en général pour un système infini. En effet, même pour des systèmes simples comme les réseaux de Petri reset/transfert, l'accessibilité est indécidable [DFS98]. Pour ces classes de systèmes, il n'existe donc pas d'algorithme permettant de calculer exactement l'ensemble des états accessibles. Nous construisons un semi-algorithme calculant l'ensemble des états accessible, et qui *termine souvent* sur les études de cas.

*L'accélération* consiste à *calculer la limite* des composées d'actions [BW94]. Pour pouvoir utiliser des techniques d'accélération, la représentation symbolique doit être suffisamment expressive pour que l'on puisse représenter l'effet d'une accélération sur un ensemble d'états. L'accélération des “lossy channel systems” utilise les SRE [ABJ98] ; celles des “FIFO channel systems ” utilise les QDD [BGWW97, WB98], les SLRE [FPS03] ou les CQDD [Bou01].

Les NDD permettent d'accélérer les composées d'actions [BW94, Boi, FL02] des systèmes à compteurs à monoïde fini.

L'accélération a fait l'objet de trois implémentations Lash [Las], Trex [Tre, ABS01, APSY02, ASY01] et Fast[Fas, BFLP03]. Cependant Lash et Trex demandent à l'utilisateur de donner les circuits à accélérer.

Nous développons une méthode pour rendre *automatique* le choix des accélérations pour les systèmes à compteurs à monoïde fini. Nous montrons comment réduire les composées d'au plus $k$ actions à un ensemble polynômial en $k$. Nous utilisons alors un algorithme de type “*brute force*” sur l'ensemble réduit.

Nous montrons les deux résultats suivants :

– L'ensemble réduit des composées d'au plus $k$ actions est calculable en temps polynômial en $k$ (théorème 9.58). Ainsi, cet ensemble contient des éléments qui ont une

taille polynômiale en $k$.
- Les accélérations restent effectivement représentables par UBA (théorème 9.24).

## L'outil Fast

FAST calcule automatiquement l'ensemble d'accessibilité de plus de 40 systèmes à compteurs : des abstractions de programmes Java, des protocoles de communication, des systèmes industriels. FAST a aussi permis d'analyser *automatiquement* le protocole embarqué TTP/C à 2 fautes [BM02].

FAST contient notamment :
- Un algorithme de calcul, par accélération, de l'ensemble des états accessibles d'un système à compteurs avec une recherche automatique de l'ensemble réduit des composées d'actions à accélérer.
- Un algorithme de calcul des invariants de places d'un système à compteurs.
- Un algorithme de synthèse de formules de Presburger permettant d'afficher l'ensemble des états accessibles d'un système sous la forme d'une formule de Presburger.

# Table des matières

CHAPITRE 2

# Préliminaires

## 2.1 Les bases

### Les nombres

L'ensemble des entiers positifs (respectivement strictement positifs) est noté $\mathbb{N}$ (respectivement $\mathbb{N}^*$), l'ensemble des entiers relatifs, aussi appelés entiers, est noté $\mathbb{Z}$, l'ensemble des rationnels est noté $\mathbb{Q}$, l'ensemble des rationnels positifs ou nuls est noté $\mathbb{Q}^+$, l'ensemble des réels est noté $\mathbb{R}$ et l'ensemble des complexes est noté $\mathbb{C}$. La relation d'ordre sur $\mathbb{R}$ est notée $\leqslant$. Pour un sous-ensemble fini $F \subseteq \mathbb{R}$, on note $\max(F)$ le plus grand élément de $F$ pour la relation d'ordre $\leqslant$. Pour deux entiers $i$ et $j$, l'ensemble des entiers compris entre $i$ et $j$ est noté $\{i, \ldots, j\} = \{k \in \mathbb{Z};\ i \leqslant k \leqslant j\}$. Le plus grand commun diviseur de deux entiers $p$ et $q$ tels que $(p, q) \neq (0, 0)$ est noté $\mathrm{pgcd}(p, q) \geqslant 1$. Si $\mathrm{pgcd}(p, q) = 1$, les entiers $p$ et $q$ sont dit premiers entre eux. Tout rationnel $q \in \mathbb{Q}$ admet une unique écriture irréductible : $q = n/d$ où $(n, d) \in \mathbb{Z} \times \mathbb{N}^*$ sont premiers entre eux. Le reste de la division euclidienne d'un entier $n$ par un entier $q$ est noté $n[q] \in \{0, \ldots, q-1\}$. La valeur absolue d'un réel $x$ est notée $|x|$.

### Les ensembles

Pour deux ensembles $E$ et $F$, on note $E \cap F$, $E \cup F$, $E \backslash F$ et $E \times F$ respectivement l'intersection, l'union, la différence et le produit cartésien de $E$ et $F$. On note $E \subseteq F$ si $E$ est un sous-ensemble de $F$ et on note $E \subsetneq F$ si $E$ est un sous ensemble strict de $F$. L'ensemble vide est noté $\emptyset$. Le cardinal d'un ensemble fini $X$ est noté $\mathrm{card}(X) \in \mathbb{N}$. L'ensemble des parties d'un ensemble $X$ est noté $\mathcal{P}(X)$ et l'ensemble des parties finies de $X$ est noté $\mathcal{P}_f(X)$.

## Les relations

Une relation $\mathcal{R}$ dans $X \times X'$ est une partie $\mathcal{R} \subseteq X \times X'$. On note $x\mathcal{R}x'$ si $(x, x') \in \mathcal{R}$. La composée d'une relation $\mathcal{R}$ dans $X \times X'$ et d'une relation $\mathcal{R}'$ dans $X' \times X''$, est la relation $\mathcal{R}.\mathcal{R}'$ dans $X \times X''$ définie par $x\mathcal{R}.\mathcal{R}'x''$si et seulement si il existe $x' \in X'$ tel que $x\mathcal{R}x'$ et $x'\mathcal{R}'x''$. L'inverse d'une relation $\mathcal{R}$ dans $X \times X'$, est la relation $\mathcal{R}^{-1}$ définie par $x\mathcal{R}^{-1}x'$si et seulement si $x'\mathcal{R}x$.

Une relation sur un ensemble $X$ est une relation dans $X \times X$. La relation identité $\mathcal{I}_X$ sur $X$ est définie par $\mathcal{I}_X = \{(x, x);\ x \in X\}$. On note $\mathcal{R}^k$ la relation sur $X$ définie par l'induction $\mathcal{R}^k = \mathcal{R}.(\mathcal{R}^{k-1})$ pour $k \geqslant 1$ et par $\mathcal{R}^0 = \mathcal{I}_X$.

Une relation $\mathcal{R}$ sur $X$ est :
- réflexive si $x\mathcal{R}x$ pour tout $x$.
- symétrique si $x\mathcal{R}x'$ implique $x'\mathcal{R}x$ pour tous $x, x'$.
- antisymétrique si $x\mathcal{R}x'$ et $x'\mathcal{R}x$ implique $x = x'$ pour tous $x, x'$.
- transitive si $x\mathcal{R}x'$ et $x'\mathcal{R}x''$ implique $x\mathcal{R}x''$ pour tous $x, x', x''$.
- un pré-ordre partiel si $\mathcal{R}$ est réflexive et transitive.
- un ordre partiel si $\mathcal{R}$ est un ordre partiel antisymétrique.
- un ordre total si $\mathcal{R}$ est un ordre partiel tel que pour tous $x, x'$, on a soit $x\mathcal{R}x'$ soit $x'\mathcal{R}x$.
- une équivalence si $\mathcal{R}$ est réflexive, transitive et symétrique.

La fermeture réflexive et transitive d'une relation $\mathcal{R}$ sur $X$ est la relation $\mathcal{R}^* = \bigcup_{k \geqslant 0} \mathcal{R}^k$.

Un ensemble totalement ordonné est un couple $(X, \leqslant)$ tel que $\leqslant$ est une relation d'ordre total sur $X$. Un ensemble fini totalement ordonné sera noté $X = \{x_1, \dots x_{\mathrm{card}(X)}\}$.

## Les fonctions

Une fonction $f$ est une relation dans $X \times Y$ telle que pour tout $x \in X$, il existe au plus un $y \in Y$ vérifiant $(x, y) \in f$. On note $f(x) = y$ cet élément. Une telle fonction est notée $f : D \to Y$ où $D$ est l'ensemble des $x \in X$ tel qu'il existe $y \in Y$ vérifiant $(x, y) \in f$. L'ensemble de définition de $f$ est $D$ et l'ensemble d'arrivée est $Y$. On dit qu'une fonction $f' : D' \to Y'$ étend une fonction $f : D \to Y$ si $D \subseteq D'$ et $Y \subseteq Y'$ et si pour tout $x \in D$, on a $f(x) = f'(x)$. La restriction d'une fonction $f : D \to Y$ à $D_0 \subseteq D$ est la fonction notée $f|_{D_0} : D_0 \to Y$ définie par $f|_{D_0}(x) = f(x)$ pour tout $x \in D_0$.

La fonction identité $\mathrm{id}_X$ sur un ensemble $X$ est définie par $\mathrm{id}_X(x) = x$ pour tout $x \in X$. Soit $f$ une fonction définie sur un ensemble $D$. L'image $f(X)$ d'un ensemble $X$ est défini par $f(X) = \{f(x);\ x \in D \cap X\}$ et l'image de $f$, noté $\mathrm{Im}(f)$, est $f(D)$. L'image inverse $f^{-1}(Y)$ d'un ensemble $Y$ est défini par $f^{-1}(Y) = \{x \in D;\ f(x) \in Y\}$.

La composée de deux fonctions $f : X \to X'$ et $g : X' \to X''$ est la fonction notée $(g \circ f) : X \to X''$ définie par $(g \circ f)(x) = g(f(x))$ pour tout $x \in X$.

Une fonction est dite :
- surjective si pour tout $y \in Y$ il existe $x \in X$ tel que $y = f(x)$.
- injective si pour tous $x, x' \in X$ tel que $f(x) = f(x')$ on a $x = x'$.
- bijective si elle est injective et surjective.
- inversible à droite s'il existe une fonction $g : Y \to X$ telle que $f \circ g = \mathrm{id}_Y$. Dans ce cas $g$ est appelée un inverse à droite.

- inversible à gauche s'il existe une fonction $g : X \to Y$ telle que $g \circ f = \mathrm{id}_X$. Dans ce cas $g$ est appelée un inverse à gauche.
- inversible si elle est inversible à droite et à gauche.

**Proposition 2.1**
*Une fonction $f$ est bijective si et seulement si elle est inversible. Dans ce cas, l'inverse à droite et l'inverse à gauche coïncident ; on note alors $f^{-1}$ l'inverse de $f$.*

## Les suites

Une suite $u$ indexée par un ensemble $I$ est notée $u = (u_i)_{i \in I}$ où simplement $u = (u_i)_i$ quand il n'y a pas d'ambiguïté sur $I$. Le $i$-ème élément d'une suite $u$ est noté $u_i$. Une suite finie $(u_i)_{i \in I}$ est une suite telle que $I$ est fini. Pour une suite finie $(u_i)_i$ de réels, on note $\max_{i \in I}(u_i)$ ou simplement $\max(u_i)$ le plus grand élément de la suite $(u_i)_i$ pour la relation d'ordre $\leqslant$ sur les réels.

## Les vecteurs

Un vecteur $v$ à $m \geqslant 0$ composantes dans un ensemble $E$ est une suite indexée par $\{1, \ldots, m\}$ telles que $v_i \in E$ pour tout $i$. On note l'ensemble de ces vecteurs $E^m$ (on permet $m = 0$ pour éviter des cas particuliers).

L'ordre partiel $\leqslant$ sur $\mathbb{Q}^m$ est défini pour tout couple de vecteurs $u, v \in \mathbb{Q}^m$ par $u \leqslant v$ si et seulement si $u_i \leqslant v_i$ pour tout $i$. On note $u + v$ le vecteur $w$ défini par $w_i = u_i + v_i$ pour tout $i$. De même pour un rationel $q$, on note $q.u$ le vecteur $w$ défini par $w_i = q.u_i$.

$||x||_\infty = \max(|x_i|)$ est la norme infinie d'un vecteur $x \in \mathbb{Q}^m$ et $||x||_1 = \sum_{i=1}^m |x_i|$ est la norme un.

Le vecteur nul $0$ de $\mathbb{Q}^m$ est le vecteur dont toutes les composantes sont nulles. Le vecteur $e_j$ de $\mathbb{Q}^m$ est défini par $(e_j)_i = 0$ si $j \neq i$ et par $(e_j)_i = 1$ sinon. Les vecteurs $e_j$ sont appelés les vecteurs unitaires de base de $\mathbb{Q}^m$.

Le produit scalaire de $x, y \in \mathbb{Q}^m$ est le rationnel $\langle x, y \rangle = \sum_{i=1}^m x_i.y_i$.

## Les matrices

Une matrice $M$ à $m \geqslant 0$ lignes et $n \geqslant 0$ colonnes et à coefficients dans un ensemble $E$, est une suite indexée par $\{1, \ldots, m\} \times \{1, \ldots, n\}$ telle que $M_{(i,j)} \in E$ pour tout $(i, j)$. L'élément $M_{(i,j)}$ est appelé le coefficient de $M$ en $i$-ème ligne et $j$-ème colonne. Cet élément est aussi noté $M_{ij}$. L'ensemble des matrices à $m$ lignes, $n$ colonnes et à coefficients dans $E$ est noté $\mathcal{M}_{m,n}(E)$. Une matrice colonne est un matrice de $\mathcal{M}_{1,n}(E)$ et une matrice ligne est une matrice de $\mathcal{M}_{m,1}(E)$.

Une matrice carrée de taille $m \geqslant 0$ est une matrice dont le nombre de lignes et le nombre de colonnes sont égaux à $m$. L'ensemble des matrices carrées de taille $m$ est noté $\mathcal{M}_m(E) = \mathcal{M}_{m,m}(E)$.

La transposée d'une matrice $M \in \mathcal{M}_{m,n}(E)$ est la matrice notée $M^t \in \mathcal{M}_{n,m}(E)$ et définie par $M^t_{ji} = M_{ij}$.

Étant données $M \in \mathcal{M}_{m,n}(\mathbb{C})$ et $N \in \mathcal{M}_{n,k}(\mathbb{C})$, la matrice $M.N \in \mathcal{M}_{m,k}(\mathbb{C})$ est définie par $(MN)_{ij} = \sum_l M_{il}.N_{lj}$.

Les vecteurs de $\mathbb{C}^n$ sont identifiés aux matrices colonnes de $\mathcal{M}_{1,n}(\mathbb{C})$. Ainsi, pour une matrice $M \in \mathcal{M}_{m,n}(\mathbb{C})$ et un vecteur $x \in \mathbb{C}^n$, on note $M.x$ le vecteur de $\mathbb{C}^m$ défini par $(M.x)_j = \sum_i M_{ij}x_i$.

La matrice identité de $\mathcal{M}_m(\mathbb{Q})$, notée $I_m$ ou simplement $I$, est définie par $I_{ij} = 1$ si $i \neq j$ et $I_{ij} = 0$ sinon.

Une matrice $M \in \mathcal{M}_m(\mathbb{C})$ est dite inversible s'il existe $M' \in \mathcal{M}_m(\mathbb{C})$ telle que $M.M' = I$ ou $M'.M = I$. Dans ce cas, la matrice $M'$ est unique et est noté $M^{-1}$. On a alors $M^{-1}.M = M.M^{-1} = I$.

### Les polynômes sur $\mathbb{C}$.

On note $\mathbb{C}[X]$ l'ensemble des polynômes sur $\mathbb{C}$ d'indéterminée $X$. Un polynôme de $\mathbb{C}[X]$ est noté $P(X)$ ou simplement $P$. Le degré d'un polynôme $P$ non nul est noté $d^o(P) \in \mathbb{N}$. Le produit de deux polynômes $P$ et $Q$ est noté $P.Q$. La composée d'un polynôme $P$ par un polynôme $Q$ est noté $P(Q)$ où $P \circ Q$.

### Taille des éléments

La taille d'un entier $n \in \mathbb{Z}$ est notée $\text{taille}(n) = \ln(1+|n|)$. On aurrais pu prendre comme définition de la taille d'un entier $n$ la partie entière du logarithme en base 2 de $1 + |n|$. Seulement, à une constante près, cette définition est équivalente à celle donnée. C'est par soucis de simplicité que l'on a choisi une taille qui peut ne pas être entière. La taille d'un rationnel $q$ dont l'écriture irréductible est $q = n/d$ est notée $\text{taille}(q) = \text{taille}(n) + \text{taille}(d)$. La taille d'un vecteur $x \in \mathbb{Q}^m$ est définie par $\text{taille}(x) = \sum_{i=1}^m \text{taille}(x_i)$. La taille d'une matrice $M \in \mathcal{M}_{m,n}(\mathbb{Q})$ est notée $\text{taille}(M) = \sum_{i,j} \text{taille}(M_{ij})$. La taille d'une partie finie $F$ de $\mathbb{Q}^m$ est définie par $\text{taille}(F) = \sum_{x \in F} \text{taille}(x)$. Remarquons que la taille peut-être un réel qui n'est pas un entier.

### Monoïde

Un monoïde est un couple $(E, .)$ où $E$ est un ensemble non vide et $. : E \times E \to E$ une fonction associative $(x.y).z = x.(y.z)$. On note $\Sigma^*$ le monoïde libre sur l'alphabet fini $\Sigma$. Le mot vide de $\Sigma^*$ est noté $\varepsilon$. Le monoïde engendré multiplicativement par une matrice carrée $M \in \mathcal{M}_m(\mathbb{Q})$ est définit par $\langle M \rangle = \{M^i;\ i \geqslant 0\}$.

## 2.2 Les automates finis

Un langage $\mathcal{L}$ est un sous-ensemble de $\Sigma^*$. Un automate finie $\mathcal{A}$ est un quintuplet $\mathcal{A} = (Q, \Sigma, \Delta, I, F)$ où $Q$ est l'ensemble fini des états, $\Sigma$ est l'alphabet fini des actions, $\Delta \subseteq Q \times \Sigma \times Q$ est l'ensemble fini des transitions, $I, F \subseteq Q$ sont respectivement l'ensemble des états initiaux et l'ensemble des états finaux.

**Définition 2.2**
*Pour tout état $q$ d'un automate $\mathcal{A} = (Q, \Sigma, \Delta, I, F)$, on définit l'automate $\mathcal{A}_q$ par $\mathcal{A}_q = (Q, \Sigma, \Delta, \{q\}, F)$.*

En renversant les flèches d'un automate $\mathcal{A}$ et en échangeant les états initiaux avec les états finaux, on obtient un nouvel automate $\mathcal{A}'$, appelé le co-automate de $\mathcal{A} = (Q, \Sigma, \Delta, I, F)$, défini par $\mathcal{A}' = (Q, \Sigma, \Delta', I', F')$ où $\Delta' = \{(q', b, q);\ (q, b, q') \in \Delta\}$, $I' = F$ et $F' = I$.

Comme l'alphabet des automates utilisés dans cette thèse est toujours égal à $\Sigma_r = \{0, \ldots, r-1\}$ pour un entier $r \geqslant 2$ fixé (sauf à quelques passages bien précisés), on ne prend pas en compte les ensembles $\Sigma$ et $\Delta$ pour définir la taille d'un automate. En effet, comme $\Delta$ est un sous ensemble de $\mathbb{Q} \times \Sigma_r \times Q$, son cardinal est majoré par $r.|Q|^2$.

**Définition 2.3**
*La taille d'un automate $\mathcal{A}$ est égale à son nombre d'états :* $\text{taille}(\mathcal{A}) = |Q|$.

Un automate déterministe $\mathcal{A}$ est un automate $\mathcal{A}$ tel que $\text{card}(I) \leqslant 1$ et tel que pour tout état $q \in Q$, et pour tout $b \in \Sigma$, il existe au plus un état $q' \in Q$ tel que $(q, b, q') \in \Delta$. Un automate complet $\mathcal{A}$ est un automate $\mathcal{A}$ tel que $\text{card}(I) \geqslant 1$ et tel que pour tout état $q \in Q$, et pour toute action $a \in \Sigma$, il existe au moins un état $q' \in Q$ tel que $(q, b, q') \in \Delta$.

Un chemin $P$ dans un automate fini $\mathcal{A}$ est une suite finie

$$P = q_0, (q_0, a_1, q_1), \ldots, q_{n-1}, (q_{n-1}, a_n, q_n), q_n$$

telle que $(q_i)_i$ est une suite d'états de $Q$ et $((q_{i-1}, a_i, q_i))_i$ est une suite de transitions de $\Delta$. On dit que $P$ est un chemin étiqueté par le mot $\sigma = a_1 \ldots a_n$ allant de l'état $q_0$ à l'état $q_n$. Un tel chemin est noté par $q_0 \xrightarrow{\sigma} q_n$ ou simplement $q_0 \to q_n$. Étant donnés deux chemins $P = q \xrightarrow{\sigma} q'$ et $P' = q' \xrightarrow{\sigma'} q''$, on note $P.P'$ la concaténation des deux chemins.

Le langage $\mathcal{L}(\mathcal{A})$ accepté par un automate fini $\mathcal{A}$ est l'ensemble des mots $\sigma \in \Sigma^*$ étiquetant au moins un chemin allant d'un état initial à un état final. Deux automates $\mathcal{A}$ et $\mathcal{A}'$ sont dits équivalents s'ils acceptent le même langage. Un langage $\mathcal{L} \subseteq \Sigma^*$ est dit régulier s'il existe un automate $\mathcal{A}$ tel que $\mathcal{L} = \mathcal{L}(\mathcal{A})$.

Un cycle $C$ est un chemin $C = q \to q'$ tel que $q = q'$. Remarquons que pour tout état $q$, le chemin $q \xrightarrow{\varepsilon} q$ est un cycle.

En remarquant que la relation $q \to q'$ est un pré-ordre partiel, on peut définir la classe d'équivalence $[q]_{\mathcal{A}}$ d'un état $q$ par $[q]_{\mathcal{A}} = \{q' \in Q;\ q \to q' \text{ et } q' \to q\}$. Une telle classe d'équivalence est appelée une composante fortement connexe. Le pré-ordre partiel $\to$ induit sur les classes d'équivalence un ordre partiel noté sans ambiguïté par $\to$ ; on a ainsi $C \to C'$ pour deux composantes fortement connexes $C$ et $C'$ si et seulement s'il existe un chemin allant d'un état $q \in C$ à un état $q' \in C'$.

**Définition 2.4**
*Le résidu (à gauche) par un mot $w \in \Sigma^*$ d'un langage $\mathcal{L} \subseteq \Sigma^*$ est la partie $w^{-1}.\mathcal{L}$ de $\Sigma^*$ définie par $w^{-1}.\mathcal{L} = \{\sigma \in \Sigma^*;\ w.\sigma \in \mathcal{L}\}$.*

Le résidu à droite n'étant pas utilisé, on ne rappelle pas sa définition.

**Théorème 2.5 ([Yu97])**
*Un langage $\mathcal{L} \subseteq \Sigma^*$ est régulier si et seulement si l'ensemble de ses résidus est fini. De plus, tous les automates déterministes et complets acceptant $\mathcal{L}$ et ayant un nombre minimal*

*d'états sont égaux, à permutation près des états, à l'automate $\mathcal{A}(\mathcal{L})$ défini par :*

$$\begin{cases} \mathcal{A}(\mathcal{L}) = (Q(\mathcal{L}), \Sigma, \Delta(\mathcal{L}), I(\mathcal{L}), F(\mathcal{L})) \\ Q(\mathcal{L}) = \{\sigma^{-1}\mathcal{L};\ \sigma \in \Sigma^*\} \\ \Delta(\mathcal{L}) = \{(q, a, a^{-1}.q);\ q \in Q(\mathcal{L});\ a \in \Sigma\} \\ I(\mathcal{L}) = \{\mathcal{L}\} \\ F(\mathcal{L}) = \{q \in Q(\mathcal{L});\ \varepsilon \in Q(\mathcal{L})\} \end{cases}$$

## 2.3 Les sous-espaces vectoriels de $\mathbb{Q}^m$

Rappelons qu'un sous-espace vectoriel $V$ de $\mathbb{Q}^m$ est une partie de $\mathbb{Q}^m$ contenant le vecteur nul et telle que pour tous $x, x' \in V$, et pour tous $q, q' \in \mathbb{Q}$, on a $q.x + q'.x' \in V$. D'autre part, toute intersection quelconque de sous-espaces vectoriels est un sous-espace vectoriel. Par suite, pour une partie $X \subseteq \mathbb{Q}^m$, il existe un plus petit espace vectoriel $\text{vec}(X)$ contenant $X$. Une partie $X$ est dite génératrice pour un espace vectoriel $V$ si $V = \text{vec}(X)$. La dimension d'un sous-espace vectoriel $V$ est le plus petit entier $\dim(V) \in \{0, \dots, m\}$ tel qu'il existe une partie génératrice $X$ de $V$ de cardinal $\dim(V)$. Une telle partie $X$ est appelée une base de $V$. Rappelons que pour toute partie $X \subseteq \mathbb{Q}^m$, on a $\text{vec}(X) = \{\sum_{i=1}^m q_i.x_i;\ q_i \in \mathbb{Q};\ x_i \in X\}$. Une partie $X \subseteq \mathbb{Q}^m$ est dite libre si pour toute partie finie $X_0 \subseteq X$ et pour toute suite $(q_x)_{x \in X_0}$ de rationnels tels que $\sum_{x \in X_0} q_x.x = 0$ alors $q_x = 0$ pour tout $x \in X$. Une partie $X$ est une base si et seulement si c'est une partie libre et génératrice. Une fonction linéaire $f : X \to Y$ où $X \subseteq \mathbb{Q}^n$ et $Y \subseteq \mathbb{Q}^m$ est une fonction telle qu'il existe une matrice $M \in \mathcal{M}_m(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^m$ tels que $f(x) = M.x + v$ pour tout $x \in X$.

## 2.4 Les parties convexes

Un convexe $P$ de $\mathbb{Q}^m$ est une partie de $\mathbb{Q}^m$ telle que pour tous $x, x' \in P$ et pour tous $t, t' \in \mathbb{Q}^+$ vérifiant $t + t' = 1$, on a $t.x + t'.x' \in P$. Un convexe de $\mathbb{N}^m$ est l'intersection d'un convexe de $\mathbb{Q}^m$ avec $\mathbb{N}^m$.

## 2.5 Les parties de $\mathbb{N}^m$ définissables dans la logique de Presburger

Un terme $t$ est un couple $t = (q, (q_x)_{x \in X})$ tel que $q \in \mathbb{Z}$ et $(q_x)_{x \in X}$ est une suite finie de $\mathbb{Z}$. L'ensemble $X$ est noté $\text{var}(t)$ et est appelé l'ensemble des variables libres de $t$. Un tel terme $t$ est noté $t = q + \sum_{x \in X} q_x.x$.

Une formule de Presburger $\phi$ est un élément de la grammaire :

$$\phi := t\#t|\exists x\ \phi|\forall x\ \phi|\phi \vee \phi|\phi \wedge \phi|\neg\phi|true|false$$

où $t$ est un terme et $\# \in \{\leqslant, \geqslant, <, >, =\}$.

**Définition 2.6**
*Une formule de Presburger étendue aux modulos $\phi$ est un élément de la grammaire :*

$$\phi := t\#t|t\#t[m]|\exists x\ \phi|\forall x\ \phi|\phi \vee \phi|\phi \wedge \phi|\neg\phi|true|false$$

*où* $m \in \mathbb{N}^*$.

On définit par induction l'ensemble $\mathrm{var}(\phi)$ des variables libres d'une formule de Presburger $\phi$ :

$$\begin{cases} \mathrm{var}(t\#t') = \mathrm{var}(t) \cup \mathrm{var}(t') \\ \mathrm{var}(t\#t'[m]) = \mathrm{var}(t) \cup \mathrm{var}(t') \\ \mathrm{var}(\phi \vee \phi') = \mathrm{var}(\phi \wedge \phi') = \mathrm{var}(\phi) \cup \mathrm{var}(\phi') \\ \mathrm{var}(\neg\phi) = \mathrm{var}(\phi) \\ \mathrm{var}(\exists x\ \phi) = \mathrm{var}(\forall x\ \phi) = \mathrm{var}(\phi)\backslash\{x\} \\ \mathrm{var}(true) = \mathrm{var}(false) = \emptyset \end{cases}$$

Pour une formule de Presburger $\phi$ et une fonction $f : \mathrm{var}(\phi) \to \mathbb{N}$, on définit $f \models \phi$ par l'induction suivante :

$$\begin{cases} f \models & q + \sum_{x \in X} q_x.x\#q' + \sum_{x' \in X'} q'_{x'}.x' \\ & \text{si } (q + \sum_{x \in X} q_x f(x)\#q' + \sum_{x' \in X'} q'_{x'} f(x')) \\ f \models & q + \sum_{x \in X} q_x.x\#q' + \sum_{x' \in X'} q'_{x'}.x'[m] \\ & \text{si } \exists k \in \mathbb{Z};\ (q + \sum_{x \in X} q_x f(x)\#q' + \sum_{x' \in X'} q'_{x'} f(x')) + k.m \\ & f \models \phi \vee \phi' \text{ si } (f|_{\mathrm{var}(\phi)} \models \phi) \text{ ou } (f|_{\mathrm{var}(\phi')} \models \phi') \\ f \models & \phi \wedge \phi' \\ & \text{si } (f|_{\mathrm{var}(\phi)} \models \phi) \text{ et } (f|_{\mathrm{var}(\phi')} \models \phi') \\ f \models & \neg\phi \\ & \text{si non } (f \models \phi) \\ f \models & \exists x\ \phi \\ & \text{s'il existe } f' : \mathrm{var}(\phi) \to \mathbb{N} \text{ étendant } f \text{ telle que } f' \models \phi \\ f \models & \forall x\ \phi \\ & \text{si pour toute } f' : \mathrm{var}(\phi) \to \mathbb{N} \text{ étendant } f, \text{ on a } f' \models \phi \\ f \models & true \end{cases}$$

Deux formules de Presburger $\phi$ et $\phi'$ sont dites équivalentes si pour toute fonction $f : \mathrm{var}(\phi) \cup \mathrm{var}(\phi') \to \mathbb{N}$ on a $f|_{\mathrm{var}(\phi)} \models \phi$ si et seulement si $f|_{\mathrm{var}(\phi')} \models \phi'$.

Pour un ensemble fini ordonné $V = \{v_1, \dots, v_m\}$ et un vecteur $x \in \mathbb{N}^m$, on note $f_{V,x} : V \to \mathbb{N}$ la fonction définie par $f_{V,x}(v_i) = x_i$ pour tout $i \in \{1, \dots, m\}$. Soient $V = \{v_1, \dots, v_m\}$ un ensemble totalement ordonné et $\phi$ une formule de Presburger telle que $\mathrm{var}(\phi) \subseteq X$, on définie la partie $[\![\phi]\!]_V$ de $\mathbb{N}^m$ par :

$$[\![\phi]\!]_V = \{x \in \mathbb{N}^m;\ f_{V,x} \models \phi\}$$

**Définition 2.7**
*Une partie $X \subseteq \mathbb{N}^m$ est dite L-définissable pour une sous-logique L de Presburger s'il existe une formule $\phi \in L$ et un ensemble fini V totalement ordonné tel que* $\mathrm{var}(\phi) \subseteq V$ *et* $X = [\![\phi]\!]_V$.

Voici les six fragments dont nous aurons besoin dans la suite :

| | |
|---|---|
| Affine-définissable | $\phi := t = t \vert \phi \vee \phi \vert \phi \wedge \phi \vert true \vert false$ |
| Non-quantifiée-définissable | $\phi := t = t \vert \phi \vee \phi \vert \phi \wedge \phi \vert \neg\phi \vert true \vert false$ |
| Clos-par-le-haut-définissable | $\phi := x \geqslant c \vert \phi \vee \phi \vert \phi \wedge \phi \vert true \vert false$ |
| Clos-par-le-bas-définissable | $\phi := x \leqslant c \vert \phi \vee \phi \vert \phi \wedge \phi \vert true \vert false$ |
| Intervalle-définissable | $\phi := x = c \vert \phi \vee \phi \vert \phi \wedge \phi \vert \neg\phi \vert true \vert false$ |
| Polyèdre-définissable | $\phi := t \leqslant c \vert \phi \vee \phi \vert \phi \wedge \phi \vert \neg\phi \vert true \vert false$ |

**Remarque 2.8**
*Remarquons que l'ensemble $\{x \in \mathbb{N}\ x \geqslant c\}$ est intervalle-définissable pour tout $c \in \mathbb{N}$ car défini par la formule $\bigwedge_{i=0}^{c-1}(x \neq i)$.*

Première PARTIE

# Représentation et approximation des ensembles infinis

CHAPITRE 3

# Parties affines et semi-affines

Ce chapitre a pour objectif d'introduire les notions d'algèbre linéaire utilisées dans cette thèse et d'étudier la classe des parties semi-affines et son algorithmique.

Prendre l'enveloppe affine d'une partie est souvent une sur-approximation trop grossière. Par exemple, l'enveloppe affine de trois points non alignés du plan est le plan tout entier. On étudie dans ce chapitre l'approximation que l'on obtient en considérant des *unions finies* d'espaces affines, appelées espaces semi-affines. En montrant que la classe des semi-affines est stable par intersection quelconque, on définit l'enveloppe semi-affine d'une partie ; l'enveloppe semi-affine de trois points du plan étant alors égale à ces trois points.

Nous étudions l'algorithmique des espaces semi-affines en montrant que tout espace semi-affine s'écrit de manière unique comme une union finie d'espaces affines deux à deux incomparables. En représentant canoniquement les espaces affines, on aura ainsi par cette écriture une représentation canonique des semi-affine dont l'algorithme sera prouvée polynomiale par un algorithme d'élimination de Gauss.

Dans la section 3.1 on définit les enveloppes affines et semi-affines dans une partie $K \subseteq \mathbb{Q}^m$. La stabilité de ces enveloppes pour les opérations d'union, intersection, de somme et d'image par un fonction affine, est étudiée dans la section 3.2 suivante. Enfin, dans la dernière section 3.3, on présente l'algorithmique des espaces semi-affines.

## 3.1 Enveloppe affine et semi-affine

On établit dans cette section l'existence d'une enveloppe affine et d'une enveloppe semi-affine dans $K$. Pour cela, on commence par traiter le cas particulier $K = \mathbb{Q}^m$ et on en déduit le cas général.

Rappelons qu'un espace affine $A$ de $\mathbb{Q}^m$ est soit l'ensemble vide, soit une partie de la forme $A = v + \overrightarrow{A}$ où $v \in \mathbb{Q}^m$ et $\overrightarrow{A}$ est un espace vectoriel de $\mathbb{Q}^m$. Cet espace $\overrightarrow{A}$, unique, est appelé le vectorialisé de $A$. La dimension d'un espace affine est définie par $\dim(A) = -1$ si $A = \emptyset$ et par $\dim(A) = \dim(\overrightarrow{A})$ sinon.

**Définition 3.1**
*Un espace semi-affine de $\mathbb{Q}^m$ est une union finie d'espaces affines de $\mathbb{Q}^m$.*

**Définition 3.2**
*Une partie affine (respectivement semi-affine) de $K \subseteq \mathbb{Q}^m$ est l'intersection d'un espace affine (respectivement semi-affine) de $\mathbb{Q}^m$ avec $K$.*

Pour simplifier la présentation des preuves de cette section on ne fait aucune hypothèse sur $K$. Cependant, dans le reste de cette thèse, on prendra $K = \mathbb{N}^m$.

### 3.1.1 Cas affine

**Définition 3.3**
*Toute partie $X \subseteq \mathbb{Q}^m$ est incluse dans un plus petit espace affine appelé l'enveloppe affine de $X$ et notée $\mathrm{aff}(X)$.*

Pour définir l'enveloppe affine dans une partie $K \subseteq \mathbb{Q}^m$, on commence par établir l'égalité suivante.

**Proposition 3.4**
*Pour toute partie affine $X$ de $K$, on a $X = \mathrm{aff}(X) \cap K$.*

*Démonstration :*
Par définition d'une partie affine de $K$, il existe un espace affine $A$ tel que $X = A \cap K$. Comme $X \subseteq A$, par minimalité de l'enveloppe affine, on déduit $\mathrm{aff}(X) \subseteq A$. En intersectant les inclusions $X \subseteq \mathrm{aff}(X) \subseteq A$ par $K$, on déduit $X \subseteq \mathrm{aff}(X) \cap K \subseteq A \cap K = X$. □

De la proposition précédente, on déduit que toute partie $X \subseteq K$ est incluse dans une plus petite partie affine $\mathrm{aff}(X) \cap K$ de $K$ pour la relation d'inclusion, appelé l'enveloppe affine dans $K$.

**Définition 3.5**
*L'enveloppe affine dans $K$ d'une partie $X \subseteq K$ est notée $\mathrm{aff}_K(X) = \mathrm{aff}(X) \cap K$.*

### 3.1.2 Cas semi-affine

Comme dans le cas affine, on montre l'existence d'une enveloppe semi-affine dans $K$ en commençant par le cas particulier $K = \mathbb{Q}^m$.

**Proposition 3.6**
*La classe des espaces semi-affines est stable par intersection quelconque (finie ou infinie).*

*Démonstration :*

Comme une interstion finie d'espace affine est un espace affine, une intersection finie d'espaces semi-affines est semi-affine. Pour prouver la stabilité par intersection infini, commençons par montrer que toute suite décroissante de semi-affines de $\mathbb{Q}^m$ est stationnaire. Pour cela, on fait une démonstration par récurrence sur $k \in \{-1, \ldots, m\}$ dont l'hypothèse au rang $k$ est : toute suite décroissante de semi-affines de $\mathbb{Q}^m$ inclus dans un espace affine de dimension $k$, est stationnaire. Pour $k = -1$, l'hypothèse de récurrence est établie car on a alors $A = \emptyset$. Supposons donc l'hypothèse de récurrence vraie pour un entier $k \in \{-1, \ldots, m-1\}$ et considérons un espace affine $A$ de dimension $k+1$ et une suite $(T_n)_{n\in\mathbb{N}}$ décroissante de semi-affines de $\mathbb{Q}^m$ inclus dans $A$. Le cas $T_n = A$ pour tout $n$ vérifie la récurrence et on peut donc supposer l'existence d'un indice $n_0 \geqslant 0$ tel que $T_{n_0} \neq A$. Décomposons l'espace semi-affine $T_{n_0}$ en une union finie d'espaces affines $T_{n_0} = \bigcup_{j\in J} A_j$. Pour $n \geqslant n_0$, de l'égalité $T_n = \bigcup_{j\in J}(T_n \cap A_j)$, on déduit qu'il suffit de prouver que chaque suite $(T_n \cap A_j)_n$ est stationnaire. Comme $A_j \subsetneq A$, on a $\dim(A_j) < \dim(A)$. Ainsi la suite de semi-affines $(T_n \cap A_j)_{n\geqslant n_0}$ est décroissante et incluse dans l'espace affine $A_j$ vérifiant $\dim(A_j) \leqslant k$. L'hypothèse de récurrence montre qu'elle est stationnaire. La récurrence est donc établie.

Considérons alors une classe $\mathcal{C}$ d'espaces semi-affines et montrons que l'ensemble $\bigcap_{S\in\mathcal{C}} S$ est semi-affine par l'absurde. Nous allons construire par récurrence une suite croissante $(\mathcal{C}_i)_{i\geqslant 0}$ de sous-ensembles finies de $\mathcal{C}$ tels que $S_i = \bigcap_{S\in\mathcal{C}_i} S$ soit un suite strictement croissante. On considère $\mathcal{C}_0 = \emptyset$. Supposons construit $\mathcal{C}_0$, ..., $\mathcal{C}_n$ et montrons comment construire $\mathcal{C}_{n+1}$. Remarquons que $\bigcap_{S\in\mathcal{C}} S \subseteq S_n$. Or $S_n$ est un semi-affine alors que $\bigcap_{S\in\mathcal{C}} S$ n'en n'est pas un. Ainsi, l'inclusion est stricte. Il existe donc $S \in \mathcal{C}$ tel que $S \not\subseteq S_n$. Considérons $\mathcal{C}_{n+1} = \mathcal{C}_n \cup \{S\}$ et remarquons que l'on a bien $S_n \subsetneq S_{n+1}$. On a ainsi construit une suite strictement décroissante $(S_n)_{n\geqslant 0}$ d'espaces semi-affines. D'ou la contradiction. Ainsi $\bigcap_{S\in\mathcal{C}} S$ est semi-affine. □

Ainsi, en prenant l'intersection de tous les espaces semi-affines contenant une partie $X$ de $\mathbb{Q}^m$, on obtient le plus petit semi-affine contenant $X$, appelé l'enveloppe semi-affine de $X$.

**Définition 3.7**
*L'enveloppe semi-affine d'une partie $X \subseteq \mathbb{Q}^m$ est notée* $\mathrm{saff}(X)$.

Pour prouver l'existence d'une enveloppe semi-affine de $K$, comme pour l'enveloppe affine, on établit l'égalité suivante.

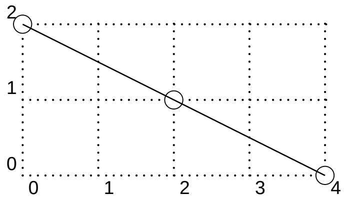
**Proposition 3.8**
*Pour toute partie semi-affine $X$ de $K$, on a $X = \mathrm{saff}(X) \cap K$.*

*Démonstration :*

Même preuve que celle de la proposition 3.4. □

**Remarque 3.9**
*Considérons la partie $X = \{(0,2), (2,1), (4,0)\}$ représentée à la figure 3.1. Remarquons que $X$ est une partie affine de $\mathbb{N}^m$. Cet exemple montre que* $\mathrm{saff}(X) \neq \mathrm{aff}(X)$.

**Figure 3.1** Pour $X = \{(0,2),(2,1),(4,0)\}$, $\mathrm{aff}(X) = (0,2) + \mathbb{Q}.(2,-1)$ et $\mathrm{saff}(X) = X$




On déduit de la proposition 3.8 que toute partie $X$ de $K$ est incluse dans une plus petite partie semi-affine $\mathrm{saff}(X) \cap K$ de $K$ pour la relation d'inclusion, appelé l'enveloppe semi-affine dans $K$.

**Définition 3.10**
*L'enveloppe semi-affine dans $K$ d'une partie $X \subseteq K$ est notée* $\mathrm{saff}_K(X) = \mathrm{saff}(X) \cap K$.

## 3.2 Stabilité des enveloppes

Dans cette section on montre que $\mathrm{aff}(X \cup X')$, $\mathrm{aff}(X + X')$ et $\mathrm{aff}(f(X))$ peuvent se calculer en fonction de $\mathrm{aff}(X)$, $\mathrm{aff}(X')$ et de l'extension affine de $f$ (et symétriquement pour l'enveloppe semi-affine).

### 3.2.1 Union

**Proposition 3.11**
*Soient $X$ et $X'$ deux parties de $\mathbb{Q}^m$. On a :*

$$\mathrm{aff}(X \cup X') = \mathrm{aff}(\mathrm{aff}(X) \cup \mathrm{aff}(X'))$$
$$\mathrm{saff}(X \cup X') = \mathrm{saff}(X) \cup \mathrm{saff}(X')$$

*Démonstration :*
Montrons la première égalité. De $\mathrm{aff}(X) \cup \mathrm{aff}(X') \subseteq \mathrm{aff}(X \cup X')$, on déduit $\mathrm{aff}(\mathrm{aff}(X) \cup \mathrm{aff}(X')) \subseteq \mathrm{aff}(X \cup X')$. Pour l'inclusion inverse, remarquons que $X \cup X' \subseteq \mathrm{aff}(\mathrm{aff}(X) \cup \mathrm{aff}(X')$. Ainsi, on a $\mathrm{aff}(X \cup X') \subseteq \mathrm{aff}(\mathrm{aff}(X) \cup \mathrm{aff}(X')$.

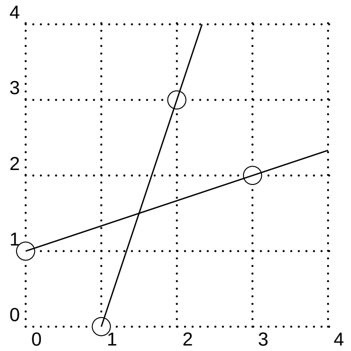
Le cas semi-affine se montre de la même façons. □

### 3.2.2 Somme

**Proposition 3.12**
*Soient $X$ et $X'$ deux parties de $\mathbb{Q}^m$. On a :*

$$\mathrm{aff}(X + X') = \mathrm{aff}(X) + \mathrm{aff}(X')$$
$$\mathrm{saff}(X + X') = \mathrm{saff}(X) + \mathrm{saff}(X')$$

**Figure 3.2** Deux parties affines $X = (0,1) + \mathbb{N}.(3,1)$ et $X' = (1,0) + \mathbb{N}.(1,3)$




*Démonstration :*

Montrons que $\text{aff}(X + X') = \text{aff}(X) + \text{aff}(X')$. Comme $X \subseteq \text{aff}(X)$ et $X' \subseteq \text{aff}(X')$, on a l'inclusion $X + X' \subseteq \text{aff}(X) + \text{aff}(X')$. Comme $\text{aff}(X) + \text{aff}(X')$ est un espace affine contenant $X + X'$, par minimalité de l'enveloppe affine, nous avons $\text{aff}(X+X') \subseteq \text{aff}(X) + \text{aff}(X')$. Pour l'inclusion inverse, pour tout $x \in X$, on a $x + \text{aff}(X') = \text{aff}(x + X') \subseteq \text{aff}(X + X')$. On a donc $X + \text{aff}(X') \subseteq \text{aff}(X + X')$. D'où, pour tout $x' \in \text{aff}(X')$, on a $X + x' \subseteq \text{aff}(X + X')$. Ainsi $\text{aff}(X) + x' = \text{aff}(X + x') \subseteq \text{aff}(X + X')$ pour tout $x' \in \text{aff}(X')$. On a l'inclusion $\text{aff}(X) + \text{aff}(X') \subseteq \text{aff}(X + X')$. On a donc prouvé l'égalité $\text{aff}(X + X') = \text{aff}(X) + \text{aff}(X')$.

Le cas semi-affine se montre de la même manière. □

### 3.2.3 Intersection

En général les égalités $\text{aff}(X \cap X') = \text{aff}(X) \cap \text{aff}(X')$ et $\text{saff}(X \cap X') = \text{saff}(X) \cap \text{saff}(X')$ ne sont pas vérifiées comme le montre l'exemple représenté par la figure 3.2.

### 3.2.4 Image par une fonction affine

Une fonction $f : D \to \mathbb{Q}^{m'}$ avec $D \subseteq \mathbb{Q}^m$ est affine s'il existe une matrice $M \in \mathcal{M}_{m',m}(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^{m'}$ tels que $f(x) = M.x + v$ pour tout $x \in D$. L'extension affine d'une fonction affine $f$ définie sur une partie $D$ est l'unique fonction affine $F : \text{aff}(D) \to \mathbb{Q}^{m'}$ étendant $f$ sur $\text{aff}(D)$.

Cette extension affine nous permet d'établir les égalités suivantes.

**Proposition 3.13**
*Soit $f : D \to \mathbb{Q}^{m'}$ une fonction affine et $F$ son extension affine. Pour tout $X \subseteq D$ on a :*

$$\text{aff}(f(X)) = F(\text{aff}(X))$$
$$\text{saff}(f(X)) = F(\text{saff}(X))$$

*Démonstration :*

La preuve du cas semi-affine étant identique à celle du cas affine, on ne prouve que la première égalité. Comme $F$ est une fonction affine, il existe $M \in \mathcal{M}_{m',m}(\mathbb{Q})$ et $v \in \mathbb{Q}^m$ tels que $F(x) = M.x + v$ pour tout $x \in D$. Considérons la fonction affine $g$ définie sur tout $\mathbb{Q}^m$ par $g(x) = M.x + v$. Comme $X \subseteq D$, on a $f(X) = g(X)$. De l'inclusion $X \subseteq D \subseteq \mathrm{aff}(D)$, on déduit par minimalité de l'enveloppe affine, $\mathrm{aff}(X) \subseteq \mathrm{aff}(D)$. Ainsi, on a aussi $F(\mathrm{aff}(X)) = g(\mathrm{aff}(X))$. Il suffit donc de prouver l'égalité $\mathrm{aff}(g(X)) = g(\mathrm{aff}(X))$. De $X \subseteq \mathrm{aff}(X)$, on déduit $g(X) \subseteq g(\mathrm{aff}(X))$. Comme $g(\mathrm{aff}(X))$ est un espace affine, par minimalité de l'enveloppe semi-affine, on a $\mathrm{aff}(g(X)) \subseteq g(\mathrm{aff}(X))$. Montrons l'inclusion réciproque. Puisque $g(X) \subseteq \mathrm{aff}(g(X))$, on a $X \subseteq g^{-1}(g(X)) \subseteq g^{-1}(\mathrm{aff}(g(X)))$. La fonction $g$ étant affine et définie sur tout $\mathbb{Q}^m$, l'ensemble $g^{-1}(\mathrm{aff}(g(X)))$ est un espace affine. Ainsi, $\mathrm{aff}(X) \subseteq g^{-1}(\mathrm{aff}(g(X)))$. En prenant l'image l'inclusion par la fonction $g$, on obtient $g(\mathrm{aff}(X)) \subseteq g(g^{-1}(\mathrm{aff}(g(X))))$. Il reste à montrer l'égalité $g(g^{-1}(\mathrm{aff}(g(X)))) = \mathrm{aff}(g(X))$. Comme $X \subseteq \mathbb{Q}^m$, on a $g(X) \subseteq g(\mathbb{Q}^m)$. Par minimalité de l'enveloppe affine, on déduit de l'inclusion précédente $\mathrm{aff}(g(X)) \subseteq g(\mathbb{Q}^m)$. Comme $g(g^{-1}(\mathrm{aff}(g(X)))) = \mathrm{aff}(g(X)) \cap g(\mathbb{Q}^m)$, on a prouvé $g(g^{-1}(\mathrm{aff}(g(X)))) = \mathrm{aff}(g(X))$. □

## 3.3 Algorithmique des semi-affines

Dans cette section, on montre qu'un espace semi-affine s'écrit comme une union finie d'espaces affines deux à deux incomparables pour la relation d'inclusion, et que cette écriture est unique à permutation près. Ainsi, en donnant une représentation canonique des espaces affines, on obtient naturellement une représentation canonique des espaces semi-affines.

Nous montrons comment décomposer canoniquement un espace semi-affine en une union finie d'espaces affines, puis on étudie l'algorithmique des espaces affines.

### 3.3.1 Composantes d'un semi-affine

On montre qu'un espace affine s'écrit de façon unique comme une union finie d'espaces affines deux à deux incomparables.

**Définition 3.14**
*Une écriture d'un espace semi-affine $S$ est une classe finie $\mathcal{C}$ de parties affines telle que $S = \bigcup_{A \in \mathcal{C}} A$. Elle est dite irréductible si les éléments de $\mathcal{C}$ sont deux à deux incomparables pour la relation d'inclusion.*

De toute écriture d'un semi-affine, on peut effectivement extraire une écriture irréductible. On va montrer que tout espace semi-affine admet une unique écriture irréductible égale à l'ensemble des *composantes affines*.

**Définition 3.15**
*Une composante affine $A$ d'un espace semi-affine $S$ est un espace affine $A \subseteq S$ qui est maximal pour la relation d'inclusion. L'ensemble des composantes affines est noté* $\mathrm{comp}(S)$.

On commence par montrer la proposition suivante.

**Proposition 3.16**
*Soient $A$ un espace affine et $S$ et $S'$ deux espaces semi-affines tels que $A \subseteq S \cup S'$. Alors soit $A \subseteq S$, soit $A \subseteq S'$.*

*Démonstration :*
Il suffit de prouver par récurrence sur $n \geqslant 1$ que pour tout espace affine $A$ et pour toute suite $(A_i)_{1 \leqslant i \leqslant n}$ d'espaces affines tels que $A \subseteq \bigcup_{i=1}^{n} A_i$, il existe $i \in \{1, \ldots, n\}$ tel que $A \subseteq A_i$. Le cas $n = 1$ est évident. Supposons donc la récurrence vraie pour un entier $n \geqslant 1$ et considérons un espace affine $A$ et une suite $(A_i)_{0 \leqslant i \leqslant n}$ tels que $A \subseteq \bigcup_{i=0}^{n} A_i$. Remarquons que si $A \subseteq A_0$ alors la récurrence est montrée. On peut donc supposer que $A \not\subseteq A_0$. On va montrer que $A \subseteq \bigcup_{i=1}^{n} A_i$. Comme $A \not\subseteq A_0$, il existe $a_0 \in A$ tel que $a_0 \notin A_0$. Considérons $a \in A$. Comme $A$ est un espace affine, pour tout $t \in \mathbb{Q}$, on a $a_0 + t.(a - a_0) \in A$. Pour tout $t \in \mathbb{Q}$, il existe donc au moins un indice $i(t) \in \{0, \ldots, n\}$ tel que $a_0 + t.(a - a_0) \in A_{i(t)}$. Pour chaque $i_0 \in \{0, \ldots, n\}$, on note $T_{i_0}$ la partie de $\mathbb{Q}$ définie par $T_{i_0} = \{t \in \mathbb{Q};\ i(t) = i_0\}$. Comme l'ensemble $\mathbb{Q}$ est égal à l'union des $T_{i_0}$ pour $i_0 \in \{0, \ldots, n\}$, il existe un indice $i_0$ tel que $T_{i_0}$ est infini. On a alors $a_0 + T_{i_0}.(a - a_0) \subseteq A_{i_0}$. Comme $A_{i_0}$ est un espace affine, on a alors $a_0 + \mathbb{Q}.(a - a_0) = \mathrm{aff}(a_0 + T_{i_0}.(a - a_0)) \subseteq A_{i_0}$. En particulier, on déduit $a_0, a \in A_{i_0}$. Puisque $a_0 \notin A_0$, on a $i_0 \in \{1, \ldots, n\}$ et $a \in \bigcup_{i=1}^{n} A_i$. On a donc prouvé que $A \subseteq \bigcup_{i=1}^{n} A_i$. En utilisant l'hypothèse de récurrence, il existe un indice $i \in \{1, \ldots, n\}$ tel que $A \subseteq A_i$ et la récurrence est prouvée. □

**Proposition 3.17**
*Tout espace semi-affine $S$ admet une unique écriture irréductible, égale à l'ensemble des composantes affines.*

*Démonstration :*
Soit $\mathcal{C}$ une écriture irréductible d'un espace semi-affine $S$. Il suffit de prouver que $\mathcal{C} = \mathrm{comp}(S)$. Prenons un espace affine $A \in \mathcal{C}$ et montrons que $A$ est un espace affine maximal contenu dans $S$. Soit $A'$ un espace affine tel que $A \subseteq A' \subseteq S$. Comme $A' \subseteq S$, de la proposition 3.16, on déduit l'existence d'un $A'' \in \mathcal{C}$ tel que $A' \subseteq A''$. De $A \subseteq A''$ et $A, A'' \in \mathcal{C}$, on on $A = A''$. Ainsi, on a $A = A' \in \mathrm{comp}(S)$. Réciproquement, considérons $A \in \mathrm{comp}(S)$. Comme $A \subseteq S$, la proposition 3.16 montre l'existence d'un espace affine $A' \in \mathcal{C}$ tel que $A \subseteq A'$. Comme $A \in \mathrm{comp}(S)$ et $A \subseteq A' \subseteq S$, on a $A = A'$. Ainsi, $A \in \mathcal{C}$. □

On peut donc représenter canoniquement les espaces semi-affines par des ensembles finis d'espaces affines incomparables pour la relation d'inclusion. Dans la sous-section suivante, on va montrer qu'il existe une représentation canonique des espaces affines et que pour cette représentation, toutes les opérations intéressantes se réalisent en temps polynomial.

### 3.3.2 Représentation canonique d'un espace affine

On présente dans cette sous-section une représentation canonique des espaces affines. Cette représentation utilise le fait que la projection orthogonale sur un espace affine est une fonction affine définie sur tout $\mathbb{Q}^m$.

**Remarque 3.18**
*Pour représenter canoniquement des polyèdres, on trouvera dans [AFP02] et [Sch87], principalement deux méthodes : une par contraintes utilisant des formules de la logique des polyèdres, et une par points extremaux. L'intérêt de notre représentation est d'être adaptée aux espaces affines et d'être ainsi plus simple à manipuler.*

#### 3.3.2.1 Projection orthogonale sur un espace affine

Rappelons que pour tout espace affine $A$ non vide de $\mathbb{Q}^m$, il existe une unique fonction affine $\Pi_A : \mathbb{Q}^m \to \mathbb{Q}^m$, appelée projection orthogonale sur $A$, telle que pour tout $(x, \overrightarrow{a}) \in \mathbb{Q}^m \times \overrightarrow{A}$, on a :

$$\begin{cases} \Pi_A(x) \in A \\ \langle x - \Pi_A(x), \overrightarrow{a} \rangle = 0 \end{cases}$$

Comme la fonction affine $\Pi_A$ est définie sur tout $\mathbb{Q}^m$, il existe un unique couple $(M_A, v_A) \in \mathcal{M}_m(\mathbb{Q}) \times \mathbb{Q}^m$ tel que $\Pi_A(x) = M_A.x + v_A$ pour tout $x \in \mathbb{Q}^m$. On obtient ainsi une représentation canonique d'un espace affine non vide $A$.

**Définition 3.19**
*La représentation canonique d'un espace affine non vide $A$ est le couple $\rho(A) = (M_A, v_A)$.*

La taille de $\rho(A)$ pour un espace affine non vide $A$ est notée $\text{taille}(\rho(A)) = \text{taille}(M_A) + \text{taille}(v_A)$. Par convention, on note $\text{taille}(\rho(\emptyset)) = 0$.

La proposition suivante montre comment déduire de la représentation $\rho(\overrightarrow{A})$, la représentation d'un espace affine non vide $A$.

**Proposition 3.20**
*Pour tout espace affine non vide $A$ et pour tout $v \in A$, on a :*

$$\begin{cases} M_A = M_{\overrightarrow{A}} \\ v_A = v - M_{\overrightarrow{A}}.v \end{cases}$$

*Démonstration :*
Considérons la fonction affine $f$ définie sur $\mathbb{Q}^m$ par $f(x) = v + M_{\overrightarrow{A}}.(x - v)$ pour tout $x \in \mathbb{Q}^m$. On a alors $f(x) \in A$ et pour tout $\overrightarrow{a} \in \overrightarrow{A}$, on a

$$\langle x - f(x), \overrightarrow{a} \rangle = \left\langle (x - v) - M_{\overrightarrow{A}}.(x - v), \overrightarrow{a} \right\rangle = 0$$

Par unicité de la projection orthogonale, on a $\Pi_A(x) = f(x) = M_{\overrightarrow{A}}.x + v - M_{\overrightarrow{A}}.v$. □

La proposition suivante est utile pour calculer la représentation canonique d'un espace vectoriel.

**Proposition 3.21**
*Soit $N \in \mathcal{M}_{m,m'}(\mathbb{Q})$ une matrice. On suppose que l'ensemble des colonnes de $N$, noté $\mathcal{C}(N) = \{N.e_i;\ i \in \{1, \ldots, m'\}\}$, est une famille libre de $\mathbb{Q}^m$. L'espace vectoriel $V = \text{vec}(\mathcal{C}(N))$ vérifie :*

$$M_V = N^t.(N.N^t)^{-1}.N$$

*Démonstration :*

Considérons un vecteur $x \in \mathbb{Q}^m$. Comme $\Pi_V(x) \in \mathrm{vec}(\mathcal{C}(N))$, il existe un vecteur $y \in \mathbb{Q}^{m'}$ tel que $\Pi_V(x) = N.y$. Pour tout $z \in \mathbb{Q}^{m'}$, de $N.z \in V$, on déduit $\langle x - \Pi_V(x), N.z\rangle = 0$. On a alors $\left\langle N^t.(x - N.y), z\right\rangle = 0$ pour tout $z \in \mathbb{Q}^{m'}$. On a donc $N^t.x = N^t.N.y$. Comme les colonnes de $N$ sont libres, le determinant de $N^t.N$ est non nul (c'est le determinant de Gram [AF88]). On a donc $y = (N^t.N)^{-1}.N^t.x$. Ainsi, pour tout $x \in \mathbb{Q}^m$, on a $\Pi_V(x) = N.(N^t.N)^{-1}.N^t.x$. De cette égalité, on déduit la proposition. □

La proposition suivante montre que la représentation que l'on a choisie à une taille minimale a un facteur multiplicatif $32.m^5$ près.

**Proposition 3.22**
*Pour tout espace affine $A$ de $\mathbb{Q}^m$ non vide et pour toute partie finie $X \subseteq \mathbb{Q}^m$ telle que $A = \mathrm{aff}(X)$, on a*

$$\mathrm{taille}(\rho(A)) \leqslant 32.m^5.(\mathrm{taille}(X) + 1)$$

*Démonstration :*

Soit $A$ un espace affine de $\mathbb{Q}^m$. Comme le cas $A = \emptyset$ est immédiat, on peut supposer que $A \neq \emptyset$. Si $\dim(A) = 0$, il existe $b \in \mathbb{Q}^m$ tel que $A = \{b\}$ et $\rho(A) = (b, 0)$. Considérons une partie finie $X \subseteq \mathbb{Q}^m$ telle que $A = \mathrm{aff}(X)$. Puisque $A = \{b\}$, on a nécéssairement $X = \{b\}$. On peut donc supposer $\dim(A) \geqslant 1$. Soit alors une partie finie $X = \{x_0, \ldots, x_{m'}\} \subseteq \mathbb{Q}^m$ telle que $A = \mathrm{aff}(X)$. Il existe une partie $X_0 \subseteq X$ libre telle que $\mathrm{aff}(X) = \mathrm{aff}(X_0)$. Comme $\mathrm{taille}(X_0) \leqslant \mathrm{taille}(X)$, on peut supposer que $X = X_0$. On a alors $m' = \dim(A) \geqslant 1$ et en particulier $m \geqslant 1$. On note $N \in \mathcal{M}_{m,m'}(\mathbb{Q})$ la matrice dont les colonnes correspondent aux vecteurs de $X$ : pour tout $i \in \{1, \ldots, m'\}$, $N.e_i = x_i - x_0$. D'après la proposition 3.20, $M_A = M_{\overrightarrow{A}}$ et par la proposition 3.21, on déduit $M_A = N^t.(N.N^t)^{-1}.N$.

Posons $s = \mathrm{taille}(X)$ et considérons le produit $d$ de tous les dénominateurs des vecteurs $x_i$. Comme chaque dénominateur est strictement majoré par $e^s$, on a la majoration $d < e^{m.(m+1).s} \leqslant e^{2.m^2.s}$. De plus, pour tout $i \in \{0, \ldots, m'\}$, on a $||d.x_i||_\infty < e^{3.m^2.s}$.

Par construction de $d$ et $N$, la matrice $P = d.N$ est à coefficients dans $\mathbb{Z}$ et $||P||_\infty < 2.e^{3.m^2.s}$. Cette matrice vérifie de plus $M_A = P^t.(P.P^t)^{-1}.P$.

Ainsi, il existe un entier $h \in \mathbb{Z}\backslash\{0\}$ et une matrice $H \in \mathcal{M}_{m'}(\mathbb{Z})$ tels que :

$$\begin{cases} (P.P^t)^{-1} = \frac{1}{h}.H \\ |h| < (4.m^2)^m.e^{6.m^3.s} \\ ||H||_\infty < (4.m^2)^m.e^{6.m^3.s} \end{cases}$$

Comme $||P||_\infty < 2.e^{3.m^2.s}$, on a $\left|\left|P.P^t\right|\right|_\infty < 4.m.e^{6.m^2.s}$. Le déterminant $h$ de la matrice $P.P^t$ peut-être majoré par :

$$|h| < m!.(4.m.e^{6.m^2.s})^m \leqslant (4.m^2)^m.e^{6.m^3.s}$$

Posons $H = h.(P.P^t)^{-1}$. Comme $H$ est égale à la co-matrice de $P.P^t$, on a aussi la majoration : $||H||_\infty < (m-1)!.(4.m.e^{6.m^2.s})^m \leqslant (4.m^2)^m.e^{6.m^3.s}$.

De l'égalité $h.M_A = P^t.H.P$, on déduit $||h.M_A||_\infty < 4.m^3.(4.m^2)^m.e^{12.m^3.s}$. Ainsi, on a la majoration :

$$\begin{aligned}
\text{taille}(M_A) &\leqslant m^2.\left[18.m^3.s + 2.m.\ln(4.m^2) + \ln(4.m^3)\right] \\
&\leqslant m^5.(18.\text{taille}(X) + 8.\frac{\ln(4.m^2)}{4.m^2} + 4.\frac{\ln(4.m^3)}{4.m^3}) \\
&\leqslant m^5.(18.\text{taille}(X) + \frac{12}{e}) \\
&\leqslant 18.m^5.(\text{taille}(X) + 1)
\end{aligned}$$

D'après la proposition 3.20, on a $v_A = x_0 - M_A.x_0$. Comme $d.x_0 \in \mathbb{Z}^m$, on a $d.h.v_A \in \mathbb{Z}^m$. De plus, $||d.h.v_A||_\infty < (4.m^2)^m.e^{6.m^3.s} + 4.m^3.(4.m^2)^m.e^{15.m^3.s} \leqslant 5.m^3.(4.m^2)^m.e^{15.m^3.s}$. Enfin, de la majoration $|d.h| < (4.m^2)^m.e^{8.m^3.s}$, on déduit :

$$\begin{aligned}
\text{taille}(v_A) &\leqslant m.\left[14.m^3.s + m.\ln(4.m^2) + m.\ln(4.m^2) + \ln(5.m^3)\right] \\
&\leqslant 14.m^5.(\text{taille}(X) + 1)
\end{aligned}$$

On a donc prouvé $\text{taille}(\rho(A)) \leqslant 32.m^5.(\text{taille}(X) + 1)$. □

#### 3.3.2.2 Une algorithmique polynomiale

En représentant canoniquement un espace semi-affine $S$ par l'ensemble fini $\{\rho(A);\ A \in \text{comp}(S)\}$, on déduit de l'algorithme de résolution de Gauss des systèmes linéaires, que l'algorithmique des espaces semi-affines est polynomiale pour cette représentation.

**Théorème 3.23**
*La représentation canonique des espaces semi-affines suivants, est calculable en temps polynomial :*
- *L'enveloppe affine d'un semi-affine.*
- *L'intersection de deux espaces semi-affines.*
- *Le produit cartésien de deux espaces semi-affines.*
- *L'espace affine engendré par une partie finie $F \subseteq \mathbb{Q}^m$.*
- *L'orthogonal d'un espace semi-affine.*
- *La somme de deux espaces semi-affines.*
- *L'image d'un espace semi-affine par une fonction affine.*
- *La composition de deux relations semi-affines.*

*De plus, on peut décider en temps polynomial l'inclusion de deux espaces semi-affines.*

*Démonstration :*
Il suffit d'appliquer l'algorithme de Gauss. □

**Remarque 3.24**
*Expérimentalement, on a remarqué qu'il fallait représenter en machine une matrice $M \in \mathcal{M}_m(\mathbb{Q})$ sous la forme $M = \frac{1}{d}.M'$ où $d \in \mathbb{N}^*$ est premier avec les coefficients de la matrice $M' \in \mathcal{M}_m(\mathbb{Z})$. En effet, dans le cas d'une représentation sous la forme $M_{ij} = \frac{n_{ij}}{d_{ij}}$ où*

*$n_{ij} \in \mathbb{Z}$ et $d_{ij} \in \mathbb{N}^*$ sont premiers entre eux, on a observé une explosion du nombre de pgcd à calculer.*

CHAPITRE 4

# Couverture d'un automate

Dans ce chapitre, on présente une méthode pour sur-approximer un ensemble représenté symboliquement par un automate binaire.

Les représentations symboliques jouent un rôle important dans le domaine de la vérification des systèmes infinis. En effet, une des méthodes pour vérifier un tel système, consiste à calculer une représentation finie de l'ensemble infini des états accessibles. Suivant la structure du système à analyser, différentes représentations symboliques ont été développées. Les "SRE" sont utilisés pour représenter des contenus de file d'un "lossy channel system" [AJ93] [ABJ98] ; les "CST" [DRV01] permettent de représenter des ensembles clos par le haut ou par le bas pour vérifier des réseaux de Petri (avec ou sans perte [BM99]). Pour vérifier les systèmes à compteurs, des représentations par automates ont été développées. Appelés "NDD" [Boi98], [WB00] ou "DFA" (nom donné à la bibliothèque d'automates de Mona : "Deterministic Finite Automaton") [KMS02] [BC96], ces automates permettent de représenter *canoniquement* une large classe de sous-ensemble de $\mathbb{N}^m$, et en particulier toutes les parties Presburger-définissables. Remarquons que hors du contexte des systèmes à compteurs, cette *représentation* a aussi permis de vérifier des protocoles paramétrés de communication en anneau [BJNT00], [BF], [AJNd02], [ABJN99].

Cependant, l'ensemble des états accessibles d'un système complexe peut ne pas être représentable par la représentation symbolique que l'on a choisie. Comme la découverte et l'implémentation d'une représentation symbolique est un travail de recherche important, on a souvent recours à l'approximation ([BF99]). Par exemple l'outil Hytech approxime une union finie de polyèdres par son enveloppe convexe [Hyt]. Cette technique permet aussi de terminer un calcul de points fixes [BGP99]. Enfin, la sur-approximation permet d'analyser qualitativement un ensemble. On peut en effet juste chercher à prouver qu'une certaine relation affine reliant les compteurs d'un système est valide [MOS04] [Ler03].

L'objectif de ce chapitre est de présenter une méthode d'approximation des ensembles représentés par automates. Remarquons que parallèlement à notre étude, le théorie des "structures automatiques" [BG02] s'applique à caractériser les représentations par automates permettant de "résoudre" les logiques du premier ordre [Bar77] par des méthodes généralisant celles que l'on utilise habituellement pour la logique de Presburger ([BC96], [WB95]).

On a obtenu les résultats suivants :
- Caractérisation des représentations par automates, stables par résidus. celles-ci possèdent la bonne propriété pour pouvoir sur-approximer l'ensemble représenté.
- Nous avons étendu la représentation par NDD pour obtenir une nouvelle représentation stable par résidu, appelée UBA.
- Nous présentons un algorithme de calcul en temps polynomial (respectivement exponentiel) de l'enveloppe affine (respectivement semi-affine) d'un ensemble représenté par un UBA.

Dans la section 4.1, on définit la notion de représentation et on introduit les représentations régulières et/ou stables par résidu. En s'intéressant plus particulièrement aux représentations des parties de $\mathbb{N}^m$, on montre dans la section 4.2 qu'en étendant la représentation par NDD, on obtient une nouvelle représentation stable par résidu. En section 4.3 on montre comment à partir d'une "couverture" d'un automate, on déduit une sur-approximation de l'ensemble représenté par cet automate dans le cadre des représentations stables par résidu. Enfin, en appliquant cette technique au cas des NDD, on déduit dans la section 4.4 un algorithme de calcul de l'enveloppe affine (respectivement semi-affine) d'un ensemble représenté par un NDD.

Dans tout ce chapitre, $E$ est un ensemble non vide.

## 4.1 Les représentations

On montre comment représenter les éléments d'un ensemble $E$ par des mots sur un alphabet $\Sigma$. Cette représentation induit naturellement une représentation des parties de $E$ par des langages sur $\Sigma$. Pour que les opérations ensemblistes (union, intersection et complémentaire) sur les langages se traduisent en opérations ensemblistes sur les parties de $E$, on définit la classe des langages non-ambigus dans la section 4.1.1. Dans la section 4.1.2 on définit la classe des représentations régulières et la classe des représentations stables par résidu, deux classes de représentations adaptées aux langages à la fois réguliers et non-ambigus.

Comme l'on souhaite que tout élément de $E$ puisse être représenté par au moins un mot de $\Sigma^*$, il est naturel de considérer la définition suivante.

**Définition 4.1**
*Une représentation est un triplet $(\Sigma, E, \rho)$ tel que $\Sigma$ est un alphabet fini et $\rho$ est une fonction surjective définie sur une partie de $\Sigma^*$ et à valeur dans un ensemble $E$.*

Sans ambiguïté, on notera de la même façon la fonction $\rho$ et la représentation $(\Sigma, E, \rho)$.

### 4.1.1 Les langages non-ambigus

Une représentation $\rho$ permet naturellement d'associer à un langage $\mathcal{L}$ sur $\Sigma$ la partie $\rho(\mathcal{L})$ de $E$. Remarquons que l'opération d'union sur les langages "se transporte" par $\rho$ en opération d'union sur les parties de $E$ ; en effet, pour tout couple de langages $(\mathcal{L}, \mathcal{L}')$ sur $\Sigma$ on a $\rho(\mathcal{L} \cup \mathcal{L}') = \rho(\mathcal{L}) \cup \rho(\mathcal{L}')$. Cependant, il n'en va pas de même pour l'opération d'intersection comme le montre le lemme 4.2 suivant.

**Lemme 4.2**
*Il existe une représentation $\rho$ et deux langages $\mathcal{L}$ et $\mathcal{L}'$ tels que $\rho(\mathcal{L} \cap \mathcal{L}') \subsetneq \rho(\mathcal{L}) \cap \rho(\mathcal{L}')$.*

*Démonstration :*
On se place dans le cas $E = \mathbb{N}$ et $\Sigma = \{0, 1\}$. La fonction $\rho$ est définie sur tout $\Sigma^*$ par $\rho(\sigma) = |\sigma|$. On considère $\mathcal{L} = \{0\}$ et $\mathcal{L}' = \{1\}$. On a alors $\emptyset = \rho(\mathcal{L} \cap \mathcal{L}') \subsetneq \rho(\mathcal{L}) \cap \rho(\mathcal{L}') = \{1\}$. □

Pour que l'opération d'intersection sur les langages "se transporte" par $\rho$ en opération d'intersection sur les parties de $E$, on introduit la classe des langages non-ambigus.

**Définition 4.3**
*Un langage $\mathcal{L}$ est dit non-ambigu pour une représentation $\rho$ s'il existe une partie $X \subseteq E$ telle que $\mathcal{L} = \rho^{-1}(X)$.*

Intuitivement, un langage non ambigu $\mathcal{L}$ est tel qu'un élément $x \in E$ est "représenté" par un mot de $\mathcal{L}$ ($x = \rho(\sigma)$ pour $\sigma \in \mathcal{L}$), alors toutes les représentations de $x$ sont dans $\mathcal{L}$ (pour tout $\sigma \in \rho^{-1}(\{x\})$, on a $\sigma \in \mathcal{L}$).

Les langages non-ambigus permettent de représenter "canoniquement" les parties de $E$.

**Proposition 4.4**
*L'application $X \to \rho^{-1}(X)$ est une bijection de l'ensemble des parties de $E$ dans l'ensemble des langages non-ambigus, de réciproque $\mathcal{L} \to \rho(\mathcal{L})$.*

*Démonstration :*
Il suffit de montrer que :
– pour toute partie $X$ de $E$, on a $\rho(\rho^{-1}(X)) = X$, et
– pour tout langage non-ambigu $\mathcal{L}$, on a $\rho^{-1}(\rho(\mathcal{L})) = \mathcal{L}$.

Le premier point est immédiat car la fonction $\rho$ est surjective. Prouvons le deuxième point en considérant un langage non-ambigu $\mathcal{L}$. Il existe une partie $X \subseteq E$ telle que $\mathcal{L} = \rho^{-1}(X)$. D'après le premier point, $\rho(\mathcal{L}) = \rho(\rho^{-1}(X)) = X$. Ainsi $\rho^{-1}(\rho(\mathcal{L})) = \rho^{-1}(X) = \mathcal{L}$ et on a prouvé le deuxième point. □

Il est alors naturel de définir la notion de codage d'une partie et de complété d'un langage.

**Définition 4.5**
*Le codage d'une partie $X$ est le langage non-ambigu $\mathcal{L} = \rho^{-1}(X)$.*

**Définition 4.6**
*Le complété d'un langage $\mathcal{L}$ est le langage $\rho^{-1}(\rho(\mathcal{L}))$.*

On montre que les opérations d'union, d'intersection et de complémentaire sur les langages non-ambigus se traduisent en opérations sur les parties de $E$.

**Corollaire 4.7**
*Pour tout couple de langages non-ambigus $\mathcal{L}$ et $\mathcal{L}'$ :*
- *l'union $\mathcal{L} \cup \mathcal{L}'$ est non-ambigu et vérifie $\rho(\mathcal{L} \cup \mathcal{L}') = \rho(\mathcal{L}) \cup \rho(\mathcal{L}')$,*
- *l'intersection $\mathcal{L} \cap \mathcal{L}'$ est non-ambigu et vérifie $\rho(\mathcal{L} \cap \mathcal{L}') = \rho(\mathcal{L}) \cap \rho(\mathcal{L}')$, et*
- *le complémentaire $\rho^{-1}(E)\backslash\mathcal{L}$ est non-ambigu et vérifie $\rho(\rho^{-1}(E)\backslash\mathcal{L}) = E\backslash\rho(\mathcal{L})$.*

*Démonstration :*
Considérons deux langages non-ambigus $\mathcal{L}$ et $\mathcal{L}'$. On note $X$ et $X'$ les parties de $E$ définies par $X = \rho(\mathcal{L})$ et $X' = \rho(\mathcal{L}')$. La proposition 4.4 montre que l'on on a $\mathcal{L} = \rho^{-1}(X)$ et $\mathcal{L}' = \rho^{-1}(X')$.

$\rho^{-1}(X \cup X') = \rho^{-1}(X) \cup \rho^{-1}(X') = \mathcal{L} \cup \mathcal{L}'$ montre que $\mathcal{L} \cup \mathcal{L}'$ est non-ambigu et que $\rho(\mathcal{L} \cup \mathcal{L}') = \rho^{-1}(X \cup X') = X \cup X' = \rho(\mathcal{L}) \cup \rho(\mathcal{L}')$.

De même, $\rho^{-1}(X \cap X') = \rho^{-1}(X) \cap \rho^{-1}(X') = \mathcal{L} \cap \mathcal{L}'$montre que $\mathcal{L} \cap \mathcal{L}'$ est non-ambigu et que $\rho(\mathcal{L} \cap \mathcal{L}') = \rho^{-1}(X \cap X') = X \cap X' = \rho(\mathcal{L}) \cap \rho(\mathcal{L}')$.

Enfin $\rho^{-1}(E\backslash X) = \rho^{-1}(E)\backslash\mathcal{L}$ implique $\rho^{-1}(E)\backslash\mathcal{L}$ est non-ambigu et que $\rho(\rho^{-1}(E)\backslash\mathcal{L}) = \rho(\rho^{-1}(E\backslash X)) = E\backslash X = E\backslash\rho(\mathcal{L})$. □

**Remarque 4.8**
*Le corollaire précédent étend des résultats de [Boi98]. Cette extension sera détaillée dans la section suivante.*

### 4.1.2 Stabilité des langages non-ambigus

Dans la section 4.1.1, on a introduit la classe des langages non-ambigus et on a montré que cette classe possède de bonnes propriétés pour représenter les parties de $E$. On présente maintenant deux conditions suffisantes pour que la théorie des automates finis puisse être utilisée dans le cadre des langages non-ambigus :
- On étudie les représentations telles que les langages réguliers et les langages réguliers non-ambigus représentent exactement les mêmes parties de $E$.
- On étudie les représentations pour lesquelles les langages non-ambigus sont stables par résidu.

#### 4.1.2.1 Les représentations régulières : structures automatiques

On caractérise les représentations telles que les langages réguliers et les langages réguliers non-ambigus représentent exactement les mêmes parties de $E$ et on établit le lien avec les structures automatiques.

**Proposition 4.9**
*Considérons une représentation $\rho$. Les langages réguliers et les langages réguliers non-ambigus représentent exactement les mêmes parties de $E$ si et seulement si le complété de tout langage régulier est régulier.*

*Démonstration :*
Supposons que les deux classes représentent les mêmes parties de $E$ et montrons que le complété de tout langage régulier est régulier. Pour cela, on considère un langage régulier $\mathcal{L}$. Par hypothèse, il existe un langage régulier non-ambigu $\mathcal{L}'$ tel que $\rho(\mathcal{L}) = \rho(\mathcal{L}')$. Or $\mathcal{L}'$ étant non-ambigu, on a $\mathcal{L}' = \rho^{-1}(\rho(\mathcal{L}')) = \rho^{-1}(\rho(\mathcal{L}))$. On a donc montré que le complété de $\mathcal{L}$ est régulier. Réciproquement, supposons que le complété de tout langage régulier soit régulier et montrons que les deux classes représentent les mêmes parties de $E$. Il suffit de montrer que pour tout langage régulier $\mathcal{L}$, il existe un langage régulier non-ambigu $\mathcal{L}'$ tel que $\rho(\mathcal{L}') = \rho(\mathcal{L})$. Or le complété $\mathcal{L}'$ de $\mathcal{L}$ est régulier, non-ambigu et vérifie cette égalité.
$\square$

**Définition 4.10**
*Une représentation régulière est une représentation telle que le complété de tout langage régulier est régulier.*

Établissons le lien entre les structures automatiques et les représentations régulières. Rappelons informellement qu'une structure automatique d'un ensemble $E$ est une représentation régulière $(\Sigma, E, \rho)$ telle que la relation d'égalité $\{(\sigma, \sigma') \in \rho^{-1}(E) \times \rho^{-1}(E);\ \rho(\sigma) = \rho(\sigma')\}$ est un "langage régulier" ([BG02]).

**Remarque 4.11**
*Les structures automatiques sont adaptées aux logiques du premier ordre [Bar77] (la logique de Presburger en est un cas particulier) que l'on peut "résoudre" par des automates. Ainsi, en plus d'imposer à la relation d'égalité d'être un langage régulier, on impose à tous les "prédicats" de la logique d'être réguliers.*

Pour pouvoir définir la notion de langage régulier pour des parties de $\Sigma^* \times \Sigma^*$, on doit pouvoir associer à un couple de mots $(\sigma, \sigma')$ un mot unique. L'idée est d'entrelacer les mots $\sigma$ et $\sigma'$ lettre par lettre. Comme ils n'ont a priori pas la même longueur, on utilise un symbole de "bourrage" $\square \not\in \Sigma$.

Ainsi, pour un mot $\sigma \in \Sigma^*$ et un entier $i \in \mathbb{N}^*$, on note $\sigma_i = \square$ si $i > |\sigma|$ et $\sigma_i$ la $i$-ème lettre de $\sigma$ sinon. Pour deux mots $\sigma$ et $\sigma'$ de $(\Sigma \cup \{\square\})^*$, on considère le mot $\sigma \otimes \sigma'$ de $((\Sigma \cup \{\square\}) \times (\Sigma \cup \{\square\}))^*$ de longueur $l = \max(|\sigma|, |\sigma'|)$ défini par $(\sigma \otimes \sigma')_i = (\sigma_i, \sigma'_i)$ pour $i \in \{1, \ldots, l\}$.

**Définition 4.12 ([BG02])**
*Une structure automatique d'un ensemble $E$ est une représentation $(\Sigma, E, \rho)$ telle que le langage $\mathcal{L}_=$ suivant est régulier :*

$$\{\sigma \otimes \sigma';\ \sigma, \sigma' \in \rho^{-1}(E);\ \rho(\sigma) = \rho(\sigma')\}$$

**Proposition 4.13**
*Toute structure automatique est une représentation régulière.*

*Démonstration :*
Considérons une structure automatique $(\Sigma, E, \rho)$. Comme $\mathcal{L}_=$ est régulier, il est accepté par un automate $\mathcal{A}^= = (Q^=, (\Sigma \cup \{\square\})^2, \Delta^=, Q_0^=, F^=)$ tel que $\mathcal{L}(\mathcal{A}^=) = \mathcal{L}_=$. Considérons alors un langage régulier $\mathcal{L}$. Le langage $\mathcal{L}.\square^*$ reste régulier et est donc accepté par un automate $\mathcal{A} = (Q, \Sigma \cup \{\square\}, \delta, Q_0, F)$. Montrons que le langage $\rho^{-1}(\rho(\mathcal{L}))$ est régulier en construisant effectivement un automate $\mathcal{A}'$ acceptant ce langage.

On définit l'automate $\mathcal{A}^\square = (Q^= \times Q, \Sigma \cup \{\square\}, \Delta^\square, Q_0^= \times Q_0, F^= \times F)$ par :

$$\Delta^\square = \{(q_1^=, q_1), a, (q_2^=, q_2);\ \exists b \in \Sigma \cup \{\square\};\ (q_1^=, (a, b), q_2^=) \in \Delta^=;\ (q_1, b, q_2) \in \Delta\}$$

Soit $F'$ l'ensemble des états $(q^=, q) \in Q^= \times Q$ tels qu'il existe un chemin étiqueté par un mot de $\square^*$ dans l'automate $\mathcal{A}^\square$ allant de cet état à un état final de $F^= \times F$. Notons $\Delta' = \Delta \cap (Q^= \times Q \times \Sigma \times Q^= \times Q)$, les transitions de $\Delta'$ n'utilisant pas le symbole $\square$. On va montrer que l'automate $\mathcal{A}' = (Q^= \times Q, \Sigma, \Delta', Q_0^= \times Q_0, F')$ accepte le langage $\rho^{-1}(\rho(\mathcal{L}))$.

Si $\sigma' \in \mathcal{L}(\mathcal{A}')$, par construction, il existe $i \geqslant 0$ tel que $\sigma'.\square^i \in \mathcal{L}(\mathcal{A}^\square)$. Ainsi, il existe $w \in \mathcal{L}.\square^*$ tel que $|w| = |\sigma|$ et $\sigma \otimes w \in \mathcal{L}_=$. Considérons $\sigma \in \mathcal{L}$ et $i' \geqslant 0$ tels que $w = \sigma.\square^{i'}$. Par définition de $\mathcal{L}_=$, on a $\rho(\sigma) = \rho(\sigma')$. Ainsi $\sigma' \in \rho^{-1}(\rho(\mathcal{L}))$.

Réciproquement, soit $\sigma' \in \rho^{-1}(\rho(\mathcal{L}))$. Il existe $\sigma \in \mathcal{L}(\mathcal{A})$ tel que $\rho(\sigma) = \rho(\sigma')$. Comme $\sigma.\square^{|\sigma'|}$ et $\sigma'.\square^{|\sigma|}$ sont des mots de la même longueur, et que $\sigma.\square^{|\sigma'|} \in \mathcal{L}.\square^*$, on a $\sigma'.\square^{|\sigma|} \in \mathcal{L}(\mathcal{A}^\square)$. Par construction de $\mathcal{A}'$, on a alors $\sigma' \in \mathcal{L}(\mathcal{A}')$.

Le langage $\rho^{-1}(\rho(\mathcal{L}))$ étant régulier pour tout langage régulier $\mathcal{L}$, la représentation $\rho$ est régulière. $\square$

**Proposition 4.14**
*Il existe une représentation régulière qui n'est pas une structure automatique.*

*Démonstration :*
Considérons la représentation $(\{a, b\}, \mathbb{N}, \rho)$ où $\rho(\sigma)$ est le nombre de changement de lettres dans $\sigma$ défini par $\rho(\sigma) = \mathrm{card}(\{i \in \mathbb{N}^*;\ \sigma_i \neq \sigma_{i+1}\})$. Remarquons que $\rho$ est régulière et il suffit ainsi de prouver que $\rho$ n'est pas une structure automatique. Supposons que le langage $\mathcal{L}_=$ soit régulier. Il existe alors un automate déterministe et complet $\mathcal{A} = (Q, \Sigma, \delta, \{q_0\}, F)$ reconnaissant $\mathcal{L}_=$. On note $n$ le nombre d'états de l'automate. On définit les mots $\sigma = (ab)^n b^{2.n}$ et $\sigma' = a^{2.n}(ab)^n$. Ayant la même longueur, on a $\sigma \otimes \sigma' = ((a, a).(b, a))^n.((b, a).(b, b))^n$. Comme $\rho(\sigma) = \rho(\sigma')$, on a prouvé que $((a, a).(b, a))^n.((b, a).(b, b))^n \in \mathcal{L}_=$. On va alors appliquer "le lemme de l'étoile". Comme $\{\delta(q_0, ((a, a).(b, a))^i);\ i \in \{0, \ldots, n\}\} \subseteq Q$, il existe $i < i'$ tels que $\delta(q_0, ((a, a).(b, a))^i) = \delta(q_0, ((a, a).(b, a))^{i'})$. En particulier $((a, a).(b, a))^{n+i'-i}.((b, a).(b, b))^n \in \mathcal{L}_=$. On a une contradiction et la représentation $\rho$ n'est donc pas une structure automatique. $\square$

#### 4.1.2.2 Stabilité des non-ambigus par résidu

On étudie les représentations $\rho$ qui sont telles que la classe des langages non-ambigus est stable par résidu. On montre que la définition de résidu sur les langages "se transporte" par $\rho$ en une définition de résidus sur les parties de $E$. On prouve alors que le codage d'une partie de $E$ est régulier si et seulement si l'ensemble de ses résidus est fini.

Rappelons que l'automate minimal associé à un langage régulier est caractérisé par ses résidus, il est donc naturel de s'intéresser aux représentations dont la classe des langages non-ambigus est stable par résidu.

**Définition 4.15**
*Une représentation est stable par résidu si tout résidu d'un langage non-ambigu est non-ambigu.*

Considérons une représentation $\rho$ stable par résidu. En utilisant la proposition 4.4, on transporte facilement l'opération de résidu sur les langages non-ambigus en opération de résidu sur les parties de $E$.

**Définition 4.16**
*Le résidu d'une partie $X \subseteq E$ par un mot $\sigma$ est la partie de $E$ notée $\sigma^{-1}.X$ et définie par :*

$$\sigma^{-1}.X = \rho(\sigma^{-1}.\rho^{-1}(X))$$

Prendre le résidu d'une partie $X$ par un mot $\sigma_2$ puis par un mot $\sigma_1$ correspond en fait à prendre directement le résidu de $X$ par le mot $\sigma_1.\sigma_2$ comme le montre la proposition 4.17 suivante.

**Proposition 4.17**
*Pour toute partie $X \subseteq E$ et pour tout couple de mots $(\sigma_1, \sigma_2)$, on a :*

$$(\sigma_1\sigma_2)^{-1}.X = \sigma_2^{-1}.(\sigma_1^{-1}.X)$$

*Démonstration :*
On a $\sigma_2^{-1}.(\sigma_1^{-1}.X) = \rho(\sigma_2^{-1}.\rho^{-1}(\rho(\sigma_1^{-1}.\rho^{-1}(X))))$. Comme la représentation $\rho$ est stable par résidu, le langage $\sigma_1^{-1}.\rho^{-1}(X)$ est non-ambigu. La proposition 4.4 montre alors que $\rho^{-1}(\rho(\sigma_1^{-1}.\rho^{-1}(X))) = \sigma_1^{-1}.\rho^{-1}(X)$. On a donc $\sigma_2^{-1}.(\sigma_1^{-1}.X) = \rho(\sigma_2^{-1}.\sigma_1^{-1}.\rho^{-1}(X)) = (\sigma_1\sigma_2)^{-1}.X$. □

Quand l'ensemble des résidus d'une partie $X \subseteq E$ est fini, on peut associer à $X$ un automate fini $\mathcal{A}(X)$.

**Définition 4.18**
*Pour une partie $X \subseteq E$ dont l'ensemble des résidus est fini, on définit l'automate $\mathcal{A}(X)$ par :*
- *un ensemble d'états $Q(X) = \{\sigma^{-1}.X;\ \sigma \in \Sigma^*\}$,*
- *un alphabet égal à $\Sigma$,*
- *un ensemble de transitions $\Delta(X) = \{q \xrightarrow{b} (b^{-1}.q);\ q \in Q(X);\ b \in \Sigma\}$,*
- *un ensemble d'états initiaux $Q_0(X) = \{X\}$, et*
- *un ensemble d'états finaux $F(X) = \{q \in Q(X);\ \rho(\varepsilon) \in q\}$.*

**Remarque 4.19**
*Remarquons que $\rho(\varepsilon)$ est bien défini. En effet, comme la représentation $\rho$ est stable par résidu, pour tout $\sigma \in \rho^{-1}(E)$, l'ensemble $\sigma^{-1}.\rho^{-1}(E)$ est non-ambigu et contient $\varepsilon$. Or par définition des non-ambigus, on a $\sigma^{-1}.\rho^{-1}(E) \subseteq \rho^{-1}(E)$ ce qui montre que $\varepsilon \in \rho^{-1}(E)$.*

On peut alors caractériser les parties de $E$ qui ont un codage régulier.

**Théorème 4.20**
*Soit $\rho$ une représentation stable par résidu. Le codage d'une partie $X$ de $E$ est régulier si et seulement si l'ensemble des résidus de $X$ est fini. De plus, dans ce cas, l'unique automate déterministe, complet et minimal acceptant le codage de $X$ est l'automate $\mathcal{A}(X)$.*

*Démonstration :*

Considérons une partie $X \subseteq E$.

Supposons que l'ensemble des résidus de $X$ soit fini et montrons alors que $\mathcal{A}(X)$ accepte le codage de $X$ égale à $\rho^{-1}(X)$. Soit $\sigma \in \mathcal{L}(\mathcal{A}(X))$ et montrons que $\sigma \in \rho^{-1}(X)$. On note $q_0 \xrightarrow{\sigma} q_f$ un chemin acceptant $\sigma$ dans l'automate $\mathcal{A}(X)$. La proposition 4.17 montre que $q_f = \sigma^{-1}.q_0$. De $q_0 = X$ et $\rho(\varepsilon) \in q_f$, on déduit $\rho(\varepsilon) \in \sigma^{-1}.X$. On a alors $\varepsilon \in \sigma^{-1}.\rho^{-1}(X)$. D'où $\sigma \in \rho^{-1}(X)$. Réciproquement, considérons $\sigma \in \rho^{-1}(X)$ et montrons que $\sigma \in \mathcal{L}(\mathcal{A}(X))$. On déduit de $\sigma \in \rho^{-1}(X)$ que $\rho(\varepsilon) \in \sigma^{-1}.X$. Ainsi, le chemin $X \xrightarrow{\sigma} \sigma^{-1}.X$ est un chemin acceptant de l'automate $\mathcal{A}(X)$ et on a montré que $\sigma \in \mathcal{L}(\mathcal{A}(X))$. On a donc montré que si l'ensemble des résidus de $X$ est fini, l'automate $\mathcal{A}(X)$ accepte le codage de $X$ qui est donc régulier.

Réciproquement, supposons que le codage de $X$ soit régulier et montrons que l'ensemble des résidus de $X$ est fini. L'ensemble des résidus de $X$ est donné par $\{\rho(\sigma^{-1}.\rho^{-1}(X))\ \sigma \in \Sigma^*\}$. Comme le langage $\rho^{-1}(X)$ est régulier, cet ensemble est fini.

Supposons maintenant que l'ensemble des résidus de $X$ soit fini et montrons que $\mathcal{A}(X)$ est l'unique automate déterministe, complet et minimal acceptant le codage de $X$. Par unicité d'un tel automate, il suffit de montrer que le nombre d'états de l'automate $\mathcal{A}(X)$ est au plus égal au nombre de résidus de $\rho^{-1}(X)$. Or, l'ensemble des résidus de $X$ étant égal à $\{\rho(\sigma^{-1}.\rho^{-1}(X));\ \sigma \in \Sigma^*\}$, cette propriété est vérifiée. L'automate $\mathcal{A}(X)$ est donc l'automate déterministe, complet et minimal reconnaissant $X$. □

Le théorème 4.20 a un corollaire intéressant quand la représentation $\rho$ est de plus régulière.

**Corollaire 4.21**
*Considérons une représentation $\rho$ régulière et stable par résidu. Une partie $X \subseteq E$ est représentable par un langage régulier si et seulement si l'ensemble des résidus de $X$ est fini. De plus, dans ce cas, l'unique automate déterministe, complet et minimal acceptant le codage de $X$ est l'automate $\mathcal{A}(X)$.*

*Démonstration :*

Remarquons que si $X$ est représentable par un langage régulier, comme $\rho$ est une représentation régulière, le codage de $X$ est régulier. Il suffit alors d'appliquer le théorème 4.20. □

## 4.2 Représentations régulières de $\mathbb{N}^m$

Dans la section précédente, on a introduit la notion de représentation d'un ensemble $E$. Dans cette section, on s'intéresse au cas particulier $E = \mathbb{N}^m$. Dans la sous-section 4.2.1, on rappelle deux représentations classiques de $\mathbb{N}^m$ : celle de Boudet et Comon [BC96] et celle de Boigelot et Wolper [WB95]. En étudiant ces représentations, on montre que l'on peut en déduire une nouvelle, plus algébrique qui rentre exactement dans le cadre théorique de la section 4.1. On pourra ainsi appliquer à cette représentation les résultats d'approximations prouvés dans la section 4.3. Une telle représentation est obtenue dans la sous-section 4.2.2 en montrant que l'on peut étendre naturellement la représentation de Boigelot et Wolper. Enfin, dans la sous-section 4.2.3, on montre que cette nouvelle représentation définit une nouvelle classe d'automates, les UBA, qui représentent les mêmes parties de $\mathbb{N}^m$ que les automates associés à la représentation de Boigelot et Wolper, les NDD. On prouve aussi que les UBA sont toujours plus petits que les NDD.

On se donne pour cette section un entier $r \geqslant 2$, appelé la base de l'écriture et un entier $m \geqslant 1$ appelé la dimension des vecteurs. L'ensemble $\{0, \dots, r-1\}$ est noté $\Sigma_r = \{0, \dots, r-1\}$ et ses éléments sont appelés des bits.

Un tableau récapitulatif des trois représentations étudiées dans cette section est donné ci-dessous. On remarque que la nouvelle représentation proposée est la seule stable par résidu à avoir un alphabet de taille ne dépendant pas de $m$.

| Représentation | Boudet Comon | Boigelot Wolper | Nouvelle |
|---|---|---|---|
| régularité effective | oui | oui | oui |
| stable par résidu | oui | non | oui |
| taille de l'alphabet | $r^m$ | $r$ | $r$ |

### 4.2.1 Les représentations régulières classiques de $\mathbb{N}^m$

On commence par étudier la représentation proposée par Boudet et Comon dans [BC96]. On montre que cette représentation est régulière et stable par résidu. Cependant, comme l'alphabet de cette représentation à une taille exponentielle en la dimension $m$, elle n'est pas utilisable en pratique. On rappelle ensuite la représentation de Boigelot et Wolper, les NDD [WB95] qui utilise une représentation régulière dont la taille de l'alphabet ne dépend pas de $m$. On montre cependant que cette représentation n'est pas stable par résidu.

#### 4.2.1.1 Vecteur de digits par vecteur de digits

Boudet et Comon [BC96] se sont intéressés plus particulièrement à la représentation $(\Sigma_r^m, \mathbb{N}^m, \rho_{BC})$ où la fonction $\rho_{BC}$ est définie pour tout mot $\sigma = \overrightarrow{b_1} \dots \overrightarrow{b_n}$ avec $\overrightarrow{b_i} \in \Sigma_r^m$ par :

$$\rho_{BC}(\sigma) = r^0.\overrightarrow{b_1} + r^1.\overrightarrow{b_2} + \dots + r^{n-1}.\overrightarrow{b_n}$$

Cette représentation par mots possède les deux propriétés suivantes [BC96] :

– la représentation $\rho_{BC}$ est régulière et même effective (le complété d'un langage régulier est effectivement calculable), et
– le codage de toute partie de $\mathbb{N}^m$ définissable dans la logique de Presburger est effectivement calculable.

Une autre propriété importante est la stabilité par résidu :

**Proposition 4.22**
*La représentation $\rho_{BC}$ est stable par résidu. De plus le résidu d'une partie $X \subseteq \mathbb{N}^m$ pour un mot $\sigma$ est égal à :*

$$\sigma^{-1}.X = \left[\frac{1}{r^{|\sigma|}}(X - \rho_{BC}(\sigma))\right] \cap \mathbb{N}^m$$

*Démonstration :*

On note $\rho$ la représentation $\rho_{BC}$. Il suffit de montrer que pour toute partie $X \subseteq \mathbb{N}^m$ et pour tout mot $\sigma$ on a $\sigma^{-1}.\rho^{-1}(X) = \rho^{-1}([\frac{1}{r^{|\sigma|}}(X - \rho(\sigma))] \cap \mathbb{N}^m)$. Pour cela, considérons $w \in \sigma^{-1}.\rho^{-1}(X)$. On a donc $r^{|\sigma|}.\rho(w) + \rho(\sigma) = \rho(\sigma.w) \in X$. Ainsi, $w \in \rho^{-1}([\frac{1}{r^{|\sigma|}}(X - \rho(\sigma))] \cap \mathbb{N}^m)$. Réciproquement, soit $w \in \rho^{-1}([\frac{1}{r^{|\sigma|}}(X - \rho(\sigma))] \cap \mathbb{N}^m)$. On a alors $\rho(\sigma.w) = r^{|\sigma|}.\rho(w) + \rho(\sigma) \in X$ et $w \in \sigma^{-1}.\rho^{-1}(X)$. $\square$

En utilisant le corollaire 4.21 on obtient une caractérisation de l'automate minimal reconnaissant une partie $X \subseteq \mathbb{N}^m$ en fonction des résidus de $X$. Malheureusement, en pratique, la représentation $\rho_{BC}$ n'est pas utilisable car l'alphabet $\Sigma = \Sigma_r^m$ a une taille exponentielle en $m$.

#### 4.2.1.2 Les NDD

Pour contourner le problème de la taille exponentielle en $m$ de l'alphabet $\Sigma_r^m$, l'outil MONA [KMS02], [Mon], utilise un BDD à $m$ variables pour représenter la relation de transition d'un automate travaillant sur l'alphabet $\Sigma_r^m$. En remarquant qu'un BDD n'est qu'un automate fini et en remplacent les transitions d'un tel automate par le BDD associé, on obtient exactement (à quelques transitions inutiles près, augmentant la taille du BDD d'un facteur $m$) la classe d'automates étudiée par Boigelot et Wolper : les NDD (Number Decision Diagram), des automates qui reconnaissent des mots de longueur divisible par $m$ sur l'alphabet $\Sigma_r$.

La représentation correspondante est notée $(\Sigma_r, \mathbb{N}^m, \rho_{BW})$ où $\rho_{BW}$ est définie pour tout mot $\sigma = b_1 \dots b_m b_{m+1} \dots b_{2m} \dots b_{(n-1).m+1} \dots b_{nm}$ de longueur divisible par $m$ avec $b_i \in \Sigma_r$ par :

$$\rho_{BW}(\sigma) = r^0.\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} + r^1.\begin{pmatrix} b_{m+1} \\ \vdots \\ b_{2m} \end{pmatrix} + \dots + r^{n-1}.\begin{pmatrix} b_{(n-1).m+1} \\ \vdots \\ b_{nm} \end{pmatrix}$$

**Remarque 4.23**
*Le lien entre $\rho_{BC}$ et $\rho_{BW}$ est naturellement donné pour tout $b_1, \dots, b_m \in \Sigma_r$ par :*

$$\rho_{BC}((b_1, \dots, b_m)) = \rho_{BW}(b_1 \dots b_m)$$

En utilisant les notations introduites dans ce chapitre, on peut redonner la définition des NDD.

**Définition 4.24 ([WB95])**
*Un NDD est un automate déterministe et complet sur l'alphabet $\Sigma_r$ acceptant un langage régulier non-ambigu pour $\rho_{BW}$.*

**Remarque 4.25**
*En fait, la définition des NDD par Boigelot et Wolper permet de représenter des vecteurs de $\mathbb{Z}^m$ en utilisant le complément à 2 pour représenter un entier négatif par un mot. Dans la section 9.2, on présentera une extension à $\mathbb{Z}^m$.*

**Remarque 4.26**
*La représentation digit de poids fort en premier, possible avec les NDD n'est pas présentée car c'est une représentation "qui ne peut-être étendue" à une représentation stable par résidu.*

Tout comme les automates de Boudet et Comon, les NDD possèdent les deux propriétés suivantes :
- la représentation par mots $\rho_{BW}$ est régulière et même effective (le complété d'un langage régulier est effectivement calculable),
- le codage de toute partie de $\mathbb{N}^m$ définissable dans la logique de Presburger est effectivement calculable.

Cependant, la représentation $\rho_{BW}$ n'est pas stable par résidu. En effet, seul le langage vide a tous ses résidus inclus dans $(\Sigma_r^m)^*$. On ne peut donc plus appliquer le corollaire 4.21.

### 4.2.2 Extension des NDD : les UBA

Pour obtenir une représentation efficace (sans explosion due à la taille de l'alphabet) et stable par résidu, on commence par prouver que $\rho_{BW}$ admet une unique extension naturelle à tout $\Sigma_r^*$ notée $\rho_m$. On prouve que $\rho_m$ est une représentation régulière stable par résidu. On introduit les classes d'automates BA, UBA et CBA adaptées aux langages réguliers non-ambigus. Enfin, on caractérise les parties de $\mathbb{N}^m$ représentables par ces automates.

#### 4.2.2.1 Extension de $\rho_{BW}$ à $\Sigma_r^*$

Pour étendre la fonction $\rho_{BW}$, on remarque que les mots $\sigma$ et $\sigma.0^{i.m}$ représentent le même vecteur pour tout entier $i \geqslant 0$ et pour tout mot $\sigma$ de longueur divisible par $m$. Il est donc naturel de chercher à étendre la fonction $\rho_{BW}$ de sorte que $\sigma$ et $\sigma.0^i$ représentent le même vecteur quelque soit l'entier $i \geqslant 0$ et le mot $\sigma$. La proposition 4.27 montre qu'une telle extension existe et qu'elle est unique.

**Proposition 4.27**
*Il existe une unique fonction $\rho$ qui étend $\rho_{BW}$ sur $\Sigma_r^*$ telle que pour tout mot $\sigma$ et pour tout entier $i \geqslant 0$, on a $\rho(\sigma.0^i) = \rho(\sigma)$.*

*Démonstration :*

Pour un entier $i \in \mathbb{N}$, on note $i[m]$ le reste de la division euclidienne de $i$ par $m$. Pour l'unicité, considérons un mot $\sigma$. Le mot $\sigma' = \sigma.0^{m-|\sigma|[m]}$ a une longueur divisible par $m$. Ainsi, on a $\rho(\sigma) = \rho(\sigma.0^{m-|\sigma|[m]}) = \rho_{BW}(\sigma.0^{m-|\sigma|[m]})$. Pour l'existence, considérons la fonction $\rho$ définie pour tout $\sigma$ par $\rho(\sigma) = \rho_{BW}(\sigma.0^{m-|\sigma|[m]})$ et remarquons que $\rho$ convient. $\square$

**Définition 4.28**
*L'unique extension naturelle de $\rho_{BW}$ à $\Sigma_r^*$ est notée $\rho_m$.*

Pour étudier cette extension, on introduit une famille de fonctions affines $(\gamma_\sigma)_{\sigma \in \Sigma_r^*}$.

**Définition 4.29**
*La fonction affine $\gamma_\sigma : \mathbb{N}^m \to \mathbb{N}^m$ est définie pour tout $\sigma \in \Sigma_r^*$ par la récurrence :*

$$\gamma_\sigma(x_1, \ldots, x_m) = \begin{cases} (x_1, \ldots, x_m) & \text{si } \sigma = \varepsilon \\ \gamma_{\sigma'}(r.x_m + b, x_1, \ldots, x_{m-1}) & \text{si } \sigma = \sigma' b \text{ avec } b \in \Sigma_r \end{cases}$$

L'extension affine de $\gamma_\sigma$ à $\mathbb{Q}^m$ joue un rôle important :

**Définition 4.30**
*L'extension affine de $\gamma_\sigma$ à $\mathbb{Q}^m$ est notée $\lambda_\sigma : \mathbb{Q}^m \to \mathbb{Q}^m$.*

La proposition 4.31 suivante montre comment calculer $\rho_m(\sigma)$ en fonction de $\gamma_\sigma$.

**Proposition 4.31**
*On a $\rho_m(\sigma) = \gamma_\sigma(\overrightarrow{0})$ pour tout mot $\sigma$.*

*Démonstration :*

La proposition 4.27 montre que $\rho_m$ est l'unique fonction qui étend $\rho_{BW}$ et telle que $\rho_m(\sigma.0^i) = \rho_m(\sigma)$ pour tout mot $\sigma$ et pour tout $i \geqslant 0$. Pour montrer que $\rho_m(\sigma) = \gamma_\sigma(\overrightarrow{0})$, il suffit donc de montrer que la fonction $\sigma \to \gamma_\sigma(\overrightarrow{0})$ vérifie les deux mêmes propriétés.

Commençons par prouver par récurrence sur la longueur de $\sigma \in (\Sigma_r^m)^*$ que $\rho_m(\sigma) = \gamma_\sigma(\overrightarrow{0})$. La récurrence est immédiate en remarquant que pour tout mot $\sigma = b_1 \ldots b_m$ sur l'alphabet $\Sigma_r$, on a $\gamma_\sigma(x) = r.x + (b_1, \ldots, b_m)$.

Enfin, comme $\gamma_0(\overrightarrow{0}) = \overrightarrow{0}$, on a bien pour tout $i \geqslant 0$ et pour tout $\sigma \in \Sigma_r^*$, $\gamma_{\sigma.0^i}(\overrightarrow{0}) = \gamma_\sigma(\overrightarrow{0})$. $\square$

#### 4.2.2.2 Régularité de $\rho_m$

On montre que la représentation $\rho_m$ est régulière et effective. On commence par caractériser les couples de mots représentant le même vecteur, puis on caractérise le complété d'un langage $\mathcal{L}$ en fonction de $\mathcal{L}$. On prouve ainsi que $\rho_m$ est effectivement régulière.

Caractérisons les couples de mots $\sigma$ et $\sigma'$ représentant le même vecteur de $\mathbb{N}^m$.

**Lemme 4.32**
*Pour tous mots $\sigma$ et $\sigma'$, on a $\rho_m(\sigma) = \rho_m(\sigma')$ si et seulement si*

$$\begin{cases} \sigma \in \sigma' 0^* & \text{si } |\sigma| \leqslant |\sigma'| \\ \sigma = \sigma' & \text{si } |\sigma| = |\sigma'| \\ \sigma' \in \sigma 0^* & \text{si } |\sigma'| \leqslant |\sigma| \end{cases}$$

*Démonstration :*
Considérons deux mots $\sigma$ et $\sigma'$ vérifiant $\rho_m(\sigma) = \rho_m(\sigma')$ et montrons $\sigma.0^* \cap \sigma'.0^* \neq \emptyset$. Il existe deux entiers $i$ et $i'$ tels que $\sigma.0^i$ et $\sigma'.0^{i'}$ sont deux mots de même longueur divisible par $m$. De $\rho_{BW}(\sigma.0^i) = \rho_{BW}(\sigma'.0^{i'})$, on déduit par unicité de l'écriture binaire que $\sigma.0^i = \sigma'.0^{i'}$.

Réciproquement, prenons deux mots $\sigma$ et $\sigma'$ vérifiant $\sigma.0^* \cap \sigma'.0^* \neq \emptyset$ et montrons que $\rho_m(\sigma) = \rho_m(\sigma')$. Il existe deux entiers $i$ et $i'$ tels que $\sigma.0^i = \sigma'.0^{i'}$. On a alors $\rho_m(\sigma) = \rho_m(\sigma.0^i) = \rho_m(\sigma'.0i') = \rho_m(\sigma')$. □

Caractérisons mainteant le complété d'un langage $\mathcal{L}$ en fonction de $\mathcal{L}$.

**Proposition 4.33**
*Pour tout langage $\mathcal{L}$, on a :*

$$\rho_m^{-1}(\rho_m(\mathcal{L})) = \bigcup_{i \geqslant 0} (\mathcal{L}.0^*).(0^i)^{-1}$$

*Démonstration :*
Considérons $\sigma \in \bigcup_{i \geqslant 0} (\mathcal{L}.0^*).(0^i)^{-1}$. Il existe $i \geqslant 0$ tel que $\sigma.0^i \in \mathcal{L}.0^*$. Ainsi, il existe $\sigma' \in \mathcal{L}$ et $i' \geqslant 0$ tels que $\sigma.0^i = \sigma'.0^{i'}$. On a alors $\rho_m(\sigma) = \rho_m(\sigma')$ et on a prouvé que $\sigma \in \rho_m^{-1}(\rho_m(\mathcal{L}))$. Réciproquement, si $\sigma \in \rho_m^{-1}(\rho_m(\mathcal{L}))$, il existe alors $\sigma' \in \mathcal{L}$ tel que $\rho_m(\sigma) = \rho_m(\sigma')$. Le lemme 4.32 montre qu'il existe $i, i' \geqslant 0$ tels que $\sigma.0^i = \sigma'.0^{i'}$. On a donc $\sigma \in \bigcup_{i \geqslant 0} (\mathcal{L}.0^*).(0^i)^{-1}$. □

Montrons enfin que $\rho_m$ est régulière et effective.

**Corollaire 4.34**
*La représentation $\rho_m$ est régulière. De plus le complété d'un langage régulier est effectivement calculable.*

*Démonstration :*
Prenons sidérons une partie $X$ de $\mathbb{N}^m$ représentée par un automate $\mathcal{A} = (Q, \Sigma_r, \Delta, Q_0, F)$ et montrons qu'il existe un automate $\mathcal{A}' = (Q', \Sigma_r, \Delta', Q_0', F')$ effectivement calculable tel que $\mathcal{L}(\mathcal{A}') = \rho_m^{-1}(X)$. On note $q_\perp$ un état tel que $q_\perp \notin Q$. On définit alors l'automate $\mathcal{A}'$ par $Q' = Q \cup \{q_\perp\}$, $\Delta' = \Delta \cup \{q_f \xrightarrow{0} q_\perp;\ q_f \in F\}$, $Q_0' = Q_0$, $F' = \{q_\perp\} \cup \{q \in Q;\ \exists q_f \in F;\ \exists q \xrightarrow{0^*} q_f\}$. Montrons l'inclusion $\rho_m^{-1}(X) \subseteq \mathcal{L}(\mathcal{A}')$. Pour cela, considérons un mot $\sigma \in \rho_m^{-1}(X)$. Il existe alors $\sigma' \in \mathcal{L}(\mathcal{A})$ tel que $\rho_m(\sigma) = \rho_m(\sigma')$. D'où l'existence de deux entiers $i, i'$ tels que $\sigma.0^i = \sigma'.0^{i'}$. On sépare la preuve en deux cas, le cas $i \leqslant i'$

et le cas $i > i'$. Pour le cas $i \leqslant i'$, de $\sigma = \sigma'.0^{i'-i}$, on déduit l'existence de deux chemins $q_0 \xrightarrow{\sigma'} q'$ et $q' \xrightarrow{0^{i'-i}} q_f$ dans $\mathcal{A}$ tels que $q_0 \in Q_0$ et $q_f \in F$. Par définition de $F'$, on a $q' \in F'$. Ainsi, on a prouvé que $\sigma' \in \mathcal{L}(\mathcal{A}')$. Dans le cas $i > i'$, on a $\sigma' = \sigma.0^{i-i'}$. Comme $\sigma \in \mathcal{L}$, il existe un chemin $q_0 \xrightarrow{\sigma} q_f$ dans l'automate $\mathcal{A}$ tel que $q_0 \in Q_0$ et $q_f \in F$. Par définition de $\mathcal{A}'$, il existe un chemin $q_f \xrightarrow{0^{i-i'}} q_\perp$ dans l'automate $\mathcal{A}'$. Ainsi, $q_0 \xrightarrow{\sigma.0^{i-i'}} q_\perp$ est un chemin acceptant de $\mathcal{A}'$. On a donc prouvé l'inclusion $\rho_m^{-1}(X) \subseteq \mathcal{L}(\mathcal{A}')$. Pour montrer l'inclusion réciproque, prenons $\sigma \in \mathcal{L}(\mathcal{A}')$ et un chemin $q_0 \xrightarrow{\sigma} q'$ dans l'automate $\mathcal{A}'$ tel que $q' \in F'$. On sépare la preuve en deux cas : $q \neq q_\perp$ et $q = q_\perp$. Supposons que $q \neq q_\perp$. Comme $q' \in F' \backslash \{q_\perp\}$, il existe un chemin $q' \xrightarrow{0^i} q_f$ avec $q_f \in F$ et $i \geqslant 0$ dans l'automate $\mathcal{A}$. On a alors $\rho_m(\sigma) = \rho_m(\sigma.0^i) \in X$ et $\sigma \in \rho_m^{-1}(X)$. Considérons enfin le cas $q' = q_\perp$. Le chemin $q \xrightarrow{\sigma} q_\perp$ se décompose alors en deux chemins de $\mathcal{A}'$, $q \xrightarrow{\sigma'} q_f$ et $q_f \xrightarrow{0^i} q_\perp$ avec $q_f \in F$. Le chemin $q \xrightarrow{\sigma'} q_f$ est alors un chemin acceptant de $\mathcal{A}$ et on a donc $\rho_m(\sigma') \in X$. De $\rho_m(\sigma) = \rho_m(\sigma'.0^i) = \rho_m(\sigma') \in X$, on déduit $\sigma \in \rho_m^{-1}(X)$. On a donc prouvé que $\mathcal{L}(\mathcal{A}') = \rho^{-1}(X)$. □

#### 4.2.2.3 Stabilité par résidu

On montre que la représentation par mots $\rho_m$ est stable par résidu.

**Proposition 4.35**
*La représentation par mots $\rho_m$ est stable par résidu. De plus, le résidu d'une partie $X \subseteq \mathbb{N}^m$ par un mot $\sigma$ est égal à :*

$$\sigma^{-1}.X = \gamma_\sigma^{-1}(X)$$

*Démonstration :*

Il suffit de montrer que $\sigma^{-1}.\rho_m^{-1}(X) = \rho_m^{-1}(\gamma_\sigma^{-1}(X))$. Considérons donc un mot $w \in \sigma^{-1}.\rho_m^{-1}(X)$ et montrons que $w \in \rho_m^{-1}(\gamma_\sigma^{-1}(X))$. On a $\rho_m(\sigma w) \in X$. Or $\rho_m(\sigma.w) = \gamma_\sigma(\rho_m(w))$. Ainsi, $w \in \rho_m^{-1}(\gamma_\sigma^{-1}(X))$. Réciproquement, considérons un mot $w \in \rho_m^{-1}(\gamma_\sigma^{-1}(X))$ et montrons que $w \in \sigma^{-1}.\rho_m^{-1}(X)$. On a $\gamma_\sigma(\rho_m(w)) \in X$. Donc $\rho_m(\sigma w) = \gamma_\sigma(\rho_m(w)) \in X$ et $w \in \sigma^{-1}.\rho_m^{-1}(X)$. □

#### 4.2.2.4 Les différents automates binaires

On définit maintenant la classe des automates binaires. En utilisant la régularité et la stabilité par résidu de la représentation $\rho_m$, on caractérise les parties de $\mathbb{N}^m$ représentables par automates binaires.

On commence par définir trois classes d'automates.

**Définition 4.36**
*On définit les trois classes suivantes d'automates :*

- *Un automate binaire (BA pour "Binary Automaton") est un automate sur l'alphabet $\Sigma_r$.*

– *Un automate binaire non-ambigu (UBA pour "Unambiguous Binary Automaton") est un automate binaire déterministe, complet qui accepte un langage régulier non-ambigu de $\rho_m$.*
– *Un automate binaire canonique (CBA pour "Canonical Binary Automaton") est un automate binaire non-ambigu minimal.*

On peut alors caractériser les parties de $\mathbb{N}^m$ représentables par un automate binaire.

**Théorème 4.37**
*Une partie $X \subseteq \mathbb{N}^m$ est représentable par un automate binaire si et seulement si, l'ensemble des résidus de $X$ est fini. De plus, dans ce cas $\mathcal{A}(X)$ est l'unique automate binaire canonique représentant $X$.*

*Démonstration :*
Il suffit d'appliquer le corollaire 4.21 à la représentation $\rho_m$. □

Remarquons de plus que la proposition 4.35 permet de caractériser l'automate $\mathcal{A}(X)$.

**Proposition 4.38**
*L'ensemble des résidus d'une partie $X$ est l'ensemble $\{\gamma_\sigma^{-1}(X);\ \sigma \in \Sigma_r^*\}$. Quand cet ensemble est fini, l'automate $\mathcal{A}(X)$ est défini par :*
– *l'ensemble d'états $Q(X) = \{\gamma_\sigma^{-1}(X);\ \sigma \in \Sigma_r^*\}$,*
– *l'alphabet $\Sigma_r$,*
– *l'ensemble de transitions $\Delta(X) = \{q \xrightarrow{b} \gamma_b^{-1}(q);\ q \in Q(X);\ b \in \Sigma_r\}$,*
– *l'ensemble d'états initiaux $Q_0(X) = \{X\}$, et*
– *l'ensemble d'états finaux $F(X) = \{q \in Q(X);\ \overrightarrow{0} \in q\}$.*

*Démonstration :*
Il suffit de remarquer que $\rho_m(\varepsilon) = \overrightarrow{0}$ et d'appliquer la proposition 4.35. □

### 4.2.3 Comparaison NDD et UBA

On montre que les NDD et les UBA représentent les mêmes parties de $\mathbb{N}^m$. Pour cela, on commence par prouver que l'on peut déduire d'un BA, un UBA représentant le même ensemble simplement en modifiant l'ensemble des états finaux.

**Lemme 4.39**
*Soit $\mathcal{A}$ un automate binaire déterministe et complet tel que $\delta(q_f, 00^*) \cap F \neq \emptyset$ pour tout $q_f \in F$. En remplaçant dans l'automate $\mathcal{A}$ l'ensemble $F$ par l'ensemble $F' = \{q \in Q;\ \delta(q, 0^*) \cap F \neq \emptyset\}$, on obtient un automate binaire non-ambigu $\mathcal{A}'$ représentant le même ensemble de vecteurs que $\mathcal{A}$.*

*Démonstration :*
Considérons un tel automate binaire $\mathcal{A} = (Q, \Sigma_r, \delta, \{q_0\}, F)$ et posons $F' = \{q \in$

$Q;\ \delta(q,0^*) \cap F \neq \emptyset\}$ et $\mathcal{A}' = (Q, \Sigma_r, \delta, \{q_0\}, F')$. Il suffit de montrer que $\mathcal{L}(\mathcal{A}') = \rho_m^{-1}(\rho_m(\mathcal{L}(\mathcal{A})))$.

Soit $\sigma' \in \mathcal{L}(\mathcal{A}')$ et montrons que $\sigma' \in \rho_m^{-1}(\rho_m(\sigma'))$. On a $\delta(q_0, \sigma') \in F'$. Par définition de $F'$, on a $\delta(q_0, \sigma' 0^*) \cap F \neq \emptyset$. Ainsi, il existe $i \geqslant 0$ tel que $\delta(q_0, \sigma' 0^i) \in F$. De $\sigma' 0^i \in \mathcal{L}(\mathcal{A})$ et $\rho_m(\sigma' 0^i) = \rho_m(\sigma')$, on déduit $\sigma' \in \rho_m^{-1}(\rho_m(\mathcal{L}(\mathcal{A})))$.

Réciproquement, soit $\sigma' \in \rho_m^{-1}(\rho_m(\mathcal{L}(\mathcal{A})))$ et montrons que $\sigma' \in \mathcal{L}(\mathcal{A}')$. Il existe $\sigma \in \mathcal{L}(\mathcal{A})$ tel que $\rho_m(\sigma') = \rho_m(\sigma)$. On commence par montrer que l'on peut supposer $|\sigma| \geqslant |\sigma'|$. Comme $\sigma \in \mathcal{L}(\mathcal{A})$, on a $\delta(q_0, \sigma) \in F$. Comme pour tout $q_f \in F$, on a $\delta(q_f, 00^*) \cap F \neq \emptyset$, une récurrence immédiate montre que pour tout $i \geqslant 0$, on a $\delta(q_0, \sigma 0^i 0^*) \cap F \neq \emptyset$. Ainsi, en prenant $i = |\sigma'|$, on déduit l'existence d'un entier $i' \geqslant 0$ tel que $\delta(q_0, \sigma 0^i 0^{i'}) \in F$. Comme $\rho(\sigma 0^i 0^{i'}) = \rho(\sigma) = \rho(\sigma')$ et $|\sigma 0^i 0^{i'}| \geqslant |\sigma'|$, on peut supposer, quitte à remplacer $\sigma$ par $\sigma 0^i 0^{i'}$, que $|\sigma| \geqslant |\sigma'|$. Le lemme 4.32 montre qu'il existe un entier $i \geqslant 0$ tel que $\sigma = \sigma' 0^i$. Comme $\sigma \in \mathcal{L}(\mathcal{A})$, il existe un chemin $q_0 \xrightarrow{\sigma'} q' \xrightarrow{0^i} q_f$ tel que $q_f \in F$. Par définition de $F'$, on a $q' \in F'$. Ainsi $\sigma' \in \mathcal{L}(\mathcal{A}')$. □

**Théorème 4.40**
*Les NDD et les UBA reconnaissent les mêmes parties de $\mathbb{N}^m$. Plus précisément :*
- *De tout NDD $\mathcal{A}$ , on construit en temps $O(r.\text{taille}(\mathcal{A}))$ un UBA $\mathcal{A}'$ représentant la même partie de $\mathbb{N}^m$ et tel que* $\text{taille}(\mathcal{A}') \leqslant \text{taille}(\mathcal{A})$
- *De tout UBA $\mathcal{A}$, on construit en temps $O(r.m.\text{taille}(\mathcal{A}))$ un NDD $\mathcal{A}'$ représentant la même partie de $\mathbb{N}^m$ et tel que* $\text{taille}(\mathcal{A}') \leqslant m.\text{taille}(\mathcal{A})$.

*Démonstration :*

Considérons un NDD $\mathcal{A} = (Q, \Sigma_r, \Delta, \{q_0\}, F)$ reconnaissant un ensemble $X$ de vecteurs. Le lemme 4.39 montre que l'on peut construire un UBA $\mathcal{A}'$ à partir de $\mathcal{A}$ simplement en changeant l'ensemble des états finaux $F$ en temps $O(r.\text{taille}(\mathcal{A}))$.

Considérons un UBA $\mathcal{A} = (Q, \Sigma_r, \Delta, \{q_0\}, F)$ reconnaissant un ensemble de vecteurs $X$ et construisons un NDD $\mathcal{A}'$ reconnaissant aussi $X$. Le reste de la division euclidienne d'un entier $k$ par $m$ est noté $k[m] \in \{0, \dots, m-1\}$. On note $\mathcal{A}' = (Q \times \{0, \dots, m-1\}, \Sigma_r, \Delta', \{q_0, 0\}, F')$ où $\Delta' = \{(q,i), b, (q', [i+1]);\ (q,b,q') \in \Delta;\ i \in \{0, \dots, m-1\}\}$ et $F' = F \times \{0\}$. Montrons que $\mathcal{A}'$ est un NDD reconnaissant $X$. Il suffit de montrer que $\mathcal{L}(\mathcal{A}') = \rho_{BW}^{-1}(X)$. Par définition de $\mathcal{A}'$, pour tout $\sigma \in \mathcal{L}(\mathcal{A}')$, on a $\sigma \in \mathcal{L}(\mathcal{A})$ et donc $\rho_{BW}(\sigma) = \rho_m(\sigma) \in X$. On a donc prouvé l'inclusion $\mathcal{L}(\mathcal{A}') \subseteq \rho_{BW}^{-1}(X)$. Il suffit donc d'établir l'inclusion réciproque. Considérons $\sigma \in (\Sigma_r^m)^*$ vérifiant $\rho_{BW}(\sigma') \in X$. De $\rho_L(\sigma) = \rho_{BW}(\sigma) \in X$, on déduit $\sigma \in \mathcal{L}(\mathcal{A})$. Ainsi $\sigma$ est l'étiquette d'un chemin de $\mathcal{A}$. Comme la longueur de $\sigma$ est divisible par $m$, $\sigma$ est aussi l'étiquette d'un chemin de $\mathcal{A}'$. D'où l'inclusion $\rho_{BW}^{-1}(X) \subseteq \mathcal{L}(\mathcal{A}')$. On a donc montré que $\mathcal{A}'$ est un NDD reconnaissant le même ensemble de vecteurs que $\mathcal{A}$. □

**Remarque 4.41**
*Les automates associés aux représentations $\rho_{BC}$ et $\rho_{BW}$ représentent exactement les mêmes parties de $\mathbb{N}^m$. Ainsi, d'un point de vue expressivité, les trois représentations $\rho_{BC}$, $\rho_{BW}$ et $\rho_m$ sont équivalentes.*

Le théorème précédent montre que de tout NDD à $n$ états, on peut calculer un UBA dont le nombre d'états est compris entre $\frac{n}{m}$ et $n$. Ainsi, même si les UBA sont toujours plus concis que les NDD, en pratique comme $m$ reste petit, on obtient des tailles relativement équivalentes. Le point vraiment positif avec les UBA est leur définition algébrique simple qui nous permettra dans les sections suivantes de calculer des sur-approximations d'ensemble représenté en utilisant les suites de fonctions affines $(\gamma_\sigma)_{\sigma\in\Sigma_r^*}$ et $(\lambda_\sigma)_{\sigma\in\Sigma_r^*}$.

## 4.3 Enveloppe d'une partie et couverture minimale d'un automate

Dans la section 4.1, on a étudié la notion de représentation permettant d'associer à un automate une partie d'un ensemble $E$. Dans cette section, on étudie comment sur-approximer une telle partie. Dans la sous-section 4.3.1, on introduit la notion de classe d'approximation permettant d'approximer toute partie $X$ de $E$ par une autre partie contenant $X$ et appelée enveloppe de $X$. La notion de couverture minimale d'un automate est présentée dans la sous-section 4.3.2. Enfin, dans la sous-section 4.3.3, on montre comment utiliser la couverture minimale d'un automate pour en déduire l'enveloppe de la partie représentée par cet automate.

*Les représentations $\rho$ de cette section sont toutes supposées stables par résidus.*

### 4.3.1 Enveloppe d'une partie

Pour sur-approximer les parties d'un ensemble $E$, on introduit la notion de classe d'approximation.

**Définition 4.42**
*Une classe d'approximation $\mathcal{C}$ d'un ensemble $E$ est une classe $\mathcal{C}$ de parties de $E$ contenant $E$ et stable par intersection quelconque.*

**Exemple 4.43**
*La classe des parties affines de $\mathbb{N}^m$ est une classe d'approximation. La classe des parties de $\mathbb{N}^m$ dont le complémentaire est fini, n'est pas une classe d'approximation.*

La proposition 4.44 suivante montre que toute partie de $E$ est incluse dans un plus petit élément de $\mathcal{C}$ pour l'inclusion.

**Proposition 4.44**
*Considérons une classe d'approximation $\mathcal{C}$ d'un ensemble $E$. Pour toute partie $X \subseteq E$, il existe une unique partie $C \in \mathcal{C}$ minimale pour l'inclusion et contenant $X$.*

*Démonstration :*
On note $C$ l'intersection de toutes les parties $C' \in \mathcal{C}$ vérifiant $X \subseteq C'$. Remarquons qu'il existe au moins un tel $C'$ car $C' = E$ convient. Ainsi, cette intersection est bien définie. De plus, par définition, on a $C \in \mathcal{C}$. Par construction on a de plus $X \subseteq C$ et pour tout $C' \in \mathcal{C}$, vérifiant $X \subseteq C'$, on a $C \subseteq C'$. □

On peut alors définir l'enveloppe d'une partie $X$ de $E$.

**Définition 4.45**
*L'enveloppe d'une partie $X$ de $E$ pour une classe d'approximation $\mathcal{C}$ de $E$ est la plus petite partie de $\mathcal{C}$ contenant $X$, notée $\mathrm{env}(X)$.*

**Remarque 4.46**
*La définition précédente généralise la notion d'enveloppe affine et semi-affine.*

### 4.3.2 Couverture minimale d'un automate

Pour calculer l'enveloppe d'une partie de $E$ représentée par un automate, on introduit la notion de couverture minimale d'un automate. On montrera comment l'utiliser dans la sous-section 4.3.3. On se donne une représentation $\rho$ stable par résidu et une classe d'approximation $\mathcal{C}$.

On souhaite étiqueter chaque état $q$ d'un automate binaire par une partie de $\mathcal{C}$ qui correspond à une sur-approximation de l'ensemble représenté par l'automate $\mathcal{A}_q$ (rapellons que $\mathcal{A}_q$ est l'automate obtenu à partir de $\mathcal{A}$ en remplaçant l'ensemble des états initiaux par le singleton $\{q\}$).

**Définition 4.47**
*Une couverture d'un automate $\mathcal{A} = (Q, \Sigma, \Delta, Q_0, F)$ est une suite $(C_q)_{q\in Q}$ d'éléments de $\mathcal{C}$ telle que :*
- *pour toute transition $q \xrightarrow{b} q'$ dans $\Delta$, on a $C_{q'} \subseteq b^{-1}.C_q$, et*
- *pour tout état $q_f \in F$, on a $\rho(\varepsilon) \in C_{q_f}$.*

**Remarque 4.48**
*Remarquons que tout automate admet la couverture triviale qui consiste à étiqueter tous ses états par l'ensemble $E$.*

Pour définir la notion de couverture minimale, on introduit la relation d'ordre partiel $\subseteq_Q$ sur les suites de parties de $E$ indexées par un ensemble $Q$.

**Définition 4.49**
*Pour un ensemble $Q$, la relation d'ordre partiel $\subseteq_Q$ sur les suites de parties de $E$ indexées par $Q$ est définie par $(X_q)_{q\in Q} \subseteq_Q (X'_q)_{q\in Q}$ si et seulement si $X_q \subseteq X'_q$ pour tout $q \in Q$.*

La proposition suivante montre l'existence et l'unicité d'une couverture minimale pour la relation d'ordre partiel $\subseteq_Q$.

**Proposition 4.50**
*Tout automate $\mathcal{A}$ admet une unique couverture plus petite pour la relation d'ordre partiel $\subseteq_Q$ que toute autre couverture.*

*Démonstration :*
On note $S$ l'ensemble des couvertures de l'automate $\mathcal{A}$. On considère la suite $(C_q)_{q\in Q}$

définie par $C_q = \bigcap_{C' \in S} C'_q$. Ces intersections sont bien définies car $S$ contenant la suite identiquement égale à $E$, n'est pas vide. De plus, par définition de $\mathcal{C}$, on $C_q \in \mathcal{C}$. Montrons que $(C_q)_{q \in Q}$ est une couverture de $\mathcal{A}$. Remarquons que par construction, on a $\rho(\varepsilon) \in C_{q_f}$ pour tout $q_f \in F$. Il suffit donc de prouver que pour toute transition $q \xrightarrow{b} q'$ on a $C_{q'} \subseteq b^{-1}.C_q$. Or $\rho^{-1}(C_{q'}) = \rho^{-1}(\bigcap_{C' \in S} C'_{q'}) = \bigcap_{C' \in S} \rho^{-1}(C'_{q'}) \subseteq \bigcap_{C' \in S} b^{-1}.\rho^{-1}(C'_q) = b^{-1}.\rho^{-1}(\bigcap_{C' \in S} C'_q) = b^{-1}.\rho^{-1}(C_q)$. Donc, $b^{-1}.C_{q'} \subseteq C_q$. □

**Remarque 4.51**
*Une relation d'ordre partiel, comme $\subseteq_Q$, peut admettre un unique élément minimal sans pour autant qu'il soit comparable avec tous les autres éléments. Ainsi, dire que la couverture minimale est plus petite que toutes les autres couvertures n'est pas redondant avec le fait de dire qu'il existe une unique couverture minimale.*

On peut ainsi définir la notion de couverture minimale d'un automate $\mathcal{A}$.

**Définition 4.52**
*La couverture minimale d'un automate $\mathcal{A}$ est la plus petite couverture pour l'inclusion $\subseteq_Q$, notée $\mathrm{cov}(\mathcal{A}) = (\mathrm{cov}(\mathcal{A})_q)_{q \in Q}$.*

### 4.3.3 Utilisation de la couverture minimale

Dans cette sous-section, on donne une méthode pour déduire de la couverture minimale d'un automate, une sur-approximation de l'enveloppe de la partie représentée par cet automate. On montre que cette sur-approximation est exacte si la classe d'approximation est stable par résidu.

#### 4.3.3.1 Cas général

On montre que sans aucune hypothèse sur la classe d'approximation $\mathcal{C}$, on déduit de la couverture d'un automate $\mathcal{A}$ une sur-approximation de l'enveloppe de la partie de $E$ représentée par $\mathcal{A}$.

**Lemme 4.53**
*Pour tout automate $\mathcal{A}$ et pour tout état $q \in Q$, on a :*

$$\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_q))) \subseteq \mathrm{cov}(\mathcal{A})_q$$

*Démonstration :*
Considérons un mot $\sigma \in \mathcal{L}(\mathcal{A}_q)$. Il existe un chemin $q \xrightarrow{\sigma} q_f$ dans l'automate $\mathcal{A}$ tel que $q_f \in F$. Comme $\mathrm{cov}(\mathcal{A})$ est une couverture, on a $\mathrm{cov}(\mathcal{A})_{q_f} \subseteq \sigma^{-1}.\mathrm{cov}(\mathcal{A})_q$. On déduit de $\rho(\varepsilon) \in \mathrm{cov}(\mathcal{A})_{q_f}$ que $\rho(\sigma) \in \mathrm{cov}(\mathcal{A})_q$. On a donc prouvé l'inclusion $\rho(\mathcal{L}(\mathcal{A}_q)) \subseteq \mathrm{cov}(\mathcal{A})_q$. En passant à l'enveloppe, comme $\mathrm{cov}(\mathcal{A})_q \in \mathcal{C}$, on obtient l'inclusion recherchée. □

Le corollaire suivant montre comment utiliser la couverture minimale d'un automate $\mathcal{A}$ pour obtenir une sur-approximation de l'enveloppe de la partie de $E$ représentée par $\mathcal{A}$.

**Corollaire 4.54**
*Pour tout automate $\mathcal{A}$, on a*

$$\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}))) \subseteq \mathrm{env}\left(\bigcup_{q_0 \in Q_0} \mathrm{cov}(\mathcal{A})_{q_0}\right)$$

*Démonstration :*
Le lemme 4.53 montre que $\mathrm{env}(\rho(\mathcal{L}(\mathcal{A})_q)) \subseteq \mathrm{cov}(\mathcal{A})_q$ pour tout état $q \in Q$. De $\mathcal{L}(\mathcal{A}) = \bigcup_{q_0 \in Q_0}(\mathcal{L}(\mathcal{A})_{q_0})$, on déduit :

$$\begin{aligned}
\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}))) &= \mathrm{env}(\bigcup_{q_0 \in Q_0} \rho(\mathcal{L}(\mathcal{A}_{q_0}))) \\
&= \mathrm{env}(\bigcup_{q_0 \in Q_0} \mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_{q_0})))) \\
&\subseteq \mathrm{env}(\bigcup_{q_0 \in Q_0} \mathrm{cov}(\mathcal{A})_{q_0})
\end{aligned}$$

□

Cependant, comme le montre le lemme suivant, l'inclusion prouvée dans le corollaire 4.54 n'est en général pas une égalité.

**Lemme 4.55**
*Il existe une représentation $\rho$ stable par résidu, une classe d'approximation $\mathcal{C}$, un automate $\mathcal{A}$ tels que l'inclusion du corollaire 4.54 est stricte.*

*Démonstration :*
On reprend l'exemple du lemme 4.2. On se place dans le cas $E = \mathbb{N}$ et $\Sigma = \{a, b\}$. La fonction $\rho$ est définie sur tout $\Sigma^*$ par $\rho(\sigma) = |\sigma|$. La classe d'approximation $\mathcal{C}$ est donnée par $\mathcal{C} = \{\mathbb{N}, P\}$ où $P$ est l'ensemble des entiers pairs. L'automate $\mathcal{A}$ est donné par $Q = \{q_0, q, q_f\}$, $\Delta = \{q_0 \xrightarrow{a} q,\ q \xrightarrow{a} q_f\}$, $Q_0 = \{q_0\}$ et $F = \{q_f\}$. Remarquons que $\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}))) = P \subsetneq \mathrm{cov}(\mathcal{A})_{q_0} = \mathbb{N}$. □

**Remarque 4.56**
*Dans la preuve du lemme 4.55, si l'on avait pris la classe d'approximation $\mathcal{C} = \{\mathbb{N}, P, I\}$ où $I$ est l'ensemble des entiers impairs, on aurait obtenu l'égalité dans le corollaire 4.54. Cette classe d'approximation est un cas particulier des classes d'approximation que nous allons étudier à partir de maintenant : les classes d'approximation stables par résidu.*

#### 4.3.3.2 Cas stable par résidu.

Pour obtenir l'égalité dans le corollaire 4.54, on définit la classe des approximations stables par résidus.

**Définition 4.57**
*Une classe d'approximation $\mathcal{C}$ d'un ensemble $E$ est stable par résidu pour une représentation $\rho$ si tout résidu d'un élément de $\mathcal{C}$ est un élément de $\mathcal{C}$.*

On a alors la réciproque du lemme 4.53.

**Lemme 4.58**
*Considérons une classe d'approximation stable par résidu. Pour tout automate $\mathcal{A}$ et pour tout état $q \in Q$, on a :*

$$\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_q))) \supseteq \mathrm{cov}(\mathcal{A})_q$$

*Démonstration :*
On note $(C_q)_{q\in Q}$ la suite définie par $C_q = \mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_q)))$. Pour montrer que $\mathrm{cov}(\mathcal{A})_q \subseteq C_q$, il suffit de montrer que $(C_q)_{q\in Q}$ est une couverture de l'automate $\mathcal{A}$. Pour tout $q_f \in F$, on a $\varepsilon \in \mathcal{L}(\mathcal{A}_{q_f})$, donc $\rho(\varepsilon) \in C_{q_f}$. Reste à montrer que pour toute transition $q \xrightarrow{b} q'$, on a $C_{q'} \subseteq b^{-1}.C_q$. On a $\mathcal{L}(\mathcal{A})_{q'} \subseteq b^{-1}.\mathcal{L}(\mathcal{A}_q) \subseteq b^{-1}.\rho^{-1}(\rho(\mathcal{L}(\mathcal{A}_q))) \subseteq b^{-1}.\rho^{-1}(C_q)$. Ainsi $\rho(\mathcal{L}(\mathcal{A}_{q'})) \subseteq b^{-1}.C_q$. Comme $\mathcal{C}$ est stable par résidu, on a $b^{-1}.C_q \in \mathcal{C}$. Par minimalité de l'enveloppe, on obtient l'inclusion $C_{q'} = \mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_{q'}))) \subseteq b^{-1}.C_q$. Cela montre que la suite $(C_q)_{q\in Q}$ est une couverture de l'automate $\mathcal{A}$. □

Le théorème suivant permet déduire l'enveloppe d'une partie représentée par un automate $\mathcal{A}$ à partir de la couverture minimale de $\mathcal{A}$.

**Théorème 4.59**
*Considérons une classe d'approximation stable par résidu. Pour tout automate $\mathcal{A}$, on a*

$$\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}))) = \mathrm{env}(\bigcup_{q_0\in Q_0} \mathrm{cov}(\mathcal{A})_{q_0})$$

*Démonstration :*
Les propositions 4.53 et 4.58 montrent que $\mathrm{env}(\rho(\mathcal{L}(\mathcal{A})_q)) = \mathrm{cov}(\mathcal{A})_q$ pour tout état $q \in Q$. De $\mathcal{L}(\mathcal{A}) = \bigcup_{q_0\in Q_0}(\mathcal{L}(\mathcal{A})_{q_0})$, on déduit :

$$\begin{aligned}
\mathrm{env}(\rho(\mathcal{L}(\mathcal{A}))) &= \mathrm{env}(\bigcup_{q_0\in Q_0} \rho(\mathcal{L}(\mathcal{A}_{q_0}))) \\
&= \mathrm{env}(\bigcup_{q_0\in Q_0} \mathrm{env}(\rho(\mathcal{L}(\mathcal{A}_{q_0})))) \\
&= \mathrm{env}(\bigcup_{q_0\in Q_0} \mathrm{cov}(\mathcal{A})_{q_0})
\end{aligned}$$

□

#### 4.3.3.3 Cas non stable par résidu : étoile d'une partie

L'étoile d'une partie de $\mathbb{N}^m$ est un exemple d'enveloppe pour une classe d'approximation qui n'est pas stable par résidu pour la représentation $\rho_m$.

Rappelons que l'étoile d'une partie $X \subseteq \mathbb{N}^m$ est l'ensemble $X^*$ des vecteurs que l'on peut obtenir comme une somme finie de vecteurs de $X$. Ainsi, formellement, on a :

$$X^* = \left\{ \sum_{i=1}^{k} x_i;\ k \geqslant 0;\ x_i \in X \right\}$$

Montrons que l'étoile d'une partie correspond à une classe d'approximation qui n'est pas stable par résidu. Une partie étoilée est une partie $X \subseteq \mathbb{N}^m$ telle que $X^* = X$. Remarquons que la classe des parties étoilées est une classe d'approximation. L'enveloppe d'une partie correspond alors à l'étoile de cette partie. Le lemme suivant montre que la couverture minimale ne peut-être utilisée pour calculer l'enveloppe d'une partie représentée par un UBA.

**Lemme 4.60**
*La classe des parties étoilées n'est pas stable par résidu.*

*Démonstration :*
Considérons la partie $X = 3.\mathbb{N}$ qui est étoilée. Comme $1 = \gamma_1(0) \not\in X$, on a $0 \not\in \gamma_1^{-1}(X)$. Ainsi $\gamma_1^{-1}(X)$ ne peut-être étoilée car une partie étoilée contient le vecteur nul. □

On ne peut ainsi utiliser la couverture minimale d'un automate pour calculer l'étoile d'une partie représentée par un UBA. Ce résultat n'est pas étonnant car l'étoile d'une partie UBA-représentable n'est pas en général UBA-représentable comme le prouve la proposition suivante.

**Proposition 4.61**
*Il existe une partie UBA-représentable dont l'étoile n'est pas UBA-représentable.*

*Démonstration :*
Notons $P = \{2^n;\ n \geqslant 0\}$. Considérons la partie UBA-représentable $X = P \times \{1\}$ et supposons par l'absurde que $X^*$ est UBA-représentable. La partie $Y = (X^* + (1,0)) \cap (P \times \mathbb{N})$ est alors UBA-représentable. Considérons la partie UBA-représentable $Z$ définie par :

$$Z = \{(x,k) \in Y;\ \forall k' \in \mathbb{N};\ k' < k \Rightarrow (x,k') \not\in Y\}$$

Après avoir prouvé que $Z = \{(2^k,k);\ k \geqslant 0\}$, on montre qu'une telle partie n'est pas UBA-représentable.

Montrons l'inclusion $\{(2^k,k);\ k \geqslant 0\} \subseteq Y$. Pour tout $k \geqslant 0$, on a $(2^k,k) \in Y$. Puisque $2^k - 1 = \sum_{i=0}^{k-1} 2^i$, il vient $(2^k,k) = \sum_{i=0}^{k-1}(2^i,1) + (1,0)$, donc $(2^k,k) \in Y$.

Prouvons maintenant que $Y \subseteq \{(2^n,k);\ n \leqslant k\}$. Soit $(2^n,k) \in Y$. Il existe une suite de $k$ vecteurs $(2^{n_i},1)_{1 \leqslant i \leqslant k}$ de $X$ telle que $(x,k) = (1 + \sum_{i=1}^{k} 2^{n_i}, k)$. Comme $2^{n_i} + 2^{n_{i'}} = 2^{2.n_i}$ pour $n_i = n_{i'}$, en regroupant les mêmes puissances de 2 dans la somme $\sum_{i=1}^{k} 2^{n_i}$, il existe une partie $R \subseteq \mathbb{N}$ telle que $\mathrm{card}(R) \leqslant k$ et telle que $\sum_{i=1}^{k} 2^{n_i} = \sum_{r \in R} 2^r$. Comme $\sum_{i=0}^{n-1} 2^i = 2^n - 1 = \sum_{r \in R} 2^r$, par unicité de la décomposition binaire, $R = \{0, \dots, n-1\}$. De l'inégalité $\mathrm{card}(R) \leqslant k$, on déduit $n \leqslant k$.

Des inclusions $\{(2^k,k);\ k \geqslant 0\} \subseteq Y \subseteqq \{(2^n,k);\ n \leqslant k\}$, on déduit par définition de $Z$, l'égalité $Z = \{(2^k,k);\ k \geqslant 0\}$.

Pour montrer que $Z$ n'est pas UBA-représentable, on va montrer que l'ensemble des résidus de $Z$ est infini. Soit $k_0 \in \mathbb{N}$, et considérons le mot $\sigma_{k_0} = 0^{2.k_0}$. On a :

$$\begin{aligned}\gamma_{\sigma_{k_0}}^{-1}(Z) &= \mathbb{N} \cap \left(\frac{1}{2^{k_0}}(X)\right) \\ &= \{(2^{2^{k_0}.k-k_0}, k);\ k \geqslant \frac{k_0}{2^{k_0}}\}\end{aligned}$$

Ainsi, pour $k_0 \neq k_0'$, on a $\gamma_{\sigma_{k_0}}^{-1}(Z) \neq \gamma_{\sigma_{k_0'}}^{-1}(Z)$. L'ensemble des résidus de $Z$ est donc infini. La partie $Z$ n'est donc pas UBA-représentable. D'où une contradiction. □

**Remarque 4.62**
*Merci à Peter Habermelh pour avoir simplifié ma preuve de la proposition précédente.*

**Remarque 4.63**
*Rappelons que l'étoile d'un ensemble Presburger-définissable est Presburger-définissable en passant par les semi-linéaires [Reu89] et remarquons que dès qu'une partie $X \subseteq \mathbb{N}$ contient 1, on a $X^* = \mathbb{N}$ qui est donc UBA-représentable. Il semble difficile de caractériser les parties UBA-représentables dont l'étoile est UBA-représentable.*

**Problème ouvert 4.64**
*Caractériser les parties UBA-représentables dont l'étoile est UBA-représentable.*

## 4.4 Couverture minimale d'un automate binaire

Dans cette dernière section, on étudie la complexité du calcul de la couverture minimale d'un automate binaire pour deux classes d'approximation : les parties affines et les parties semi-affines de $\mathbb{N}^m$. On obtient ainsi deux résultats d'approximation :
- l'enveloppe affine d'une partie $X \subseteq \mathbb{N}^m$ représentée par un automate binaire est calculable en temps polynômial, et
- l'enveloppe semi-affine d'une partie $X \subseteq \mathbb{N}^m$ représentée par un automate binaire est calculable en temps exponentiel.

Pour cela, on commence par montrer dans la sous-section 4.4.1 que de nombreuse classes de parties de $\mathbb{N}^m$ sont des classes d'approximation stables par résidu. Dans la sous-section 4.4.2, on donne un algorithme de calcul de la couverture affine. Enfin, dans la sous-section 4.4.3, on montre comment utiliser cet algorithme pour calculer la couverture semi-affine.

Rappelons quelques notations données dans le chapitre 3 :
- l'enveloppe affine de $\mathbb{N}^m$ d'une partie $X \subseteq \mathbb{N}^m$ est notée $\mathrm{aff}_{\mathbb{N}^m}(X)$,
- l'enveloppe affine de $\mathbb{Q}^m$ d'une partie $X \subseteq \mathbb{Q}^m$ est notée $\mathrm{aff}(X)$,
- l'enveloppe semi-affine de $\mathbb{N}^m$ d'une partie $X \subseteq \mathbb{N}^m$ est notée $\mathrm{saff}_{\mathbb{N}^m}(X)$, et
- l'enveloppe semi-affine de $\mathbb{Q}^m$ d'une partie $X \subseteq \mathbb{Q}^m$ est notée $\mathrm{saff}(X)$.

Rappelons enfin que l'algorithmique des parties affines et semi-affines de $\mathbb{N}^m$ et $\mathbb{Q}^m$ est aussi donnée dans le chapitre 3.

### 4.4.1 Classe d'approximation stable par résidu

Dans cette sous-section, on montre la stabilité par résidu de différentes classes d'approximation.

**Proposition 4.65**
*Les classes de parties suivantes :*
- *les parties affines de* $\mathbb{N}^m$.
- *les parties semi-affines de* $\mathbb{N}^m$.
- *les clos par les haut.*
- *les clos par le bas.*
- *les parties convexes de* $\mathbb{N}^m$.

*sont des classes d'approximation stables par résidu pour la représentation* $\rho_m$.

*Démonstration :*
Rappelons que le résidu d'une partie $X \subseteq \mathbb{N}^m$ par un mot $\sigma$ est la partie $\gamma_\sigma^{-1}(X)$ (c.f. la proposition 4.35).

*Affines* : $\mathbb{N}^m$ est une partie affine de $\mathbb{N}^m$ et une intersection quelconque de parties affines est une partie affine. De plus, comme $\gamma_\sigma$ est affine, la classe des parties affines est stable par résidu.

*Semi-affine* : la proposition 3.6 prouve que la classe des semi-affines de $\mathbb{N}^m$ est stable par intersection quelconque. Comme $\gamma_\sigma$ est affine, cette classe est stable par résidu.

*Clos par le haut* : l'ensemble $\mathbb{N}^m$ est clos par le haut et une intersection quelconque de clos par le haut est clos par le haut. Montrons que la classe des clos par le haut est stable par résidu. Soit $\sigma \in \Sigma^*$ et un ensemble clos par le haut $X$ et montrons que $\gamma_\sigma^{-1}(X)$ est clos par le haut. On considère donc $x \in \gamma_\sigma^{-1}(X)$ et $y \geqslant x$. Comme la fonction $\gamma_\sigma$ est croissante, on a alors $\gamma_\sigma(y) \geqslant \gamma_\sigma(x) \in X$. Puisque $X$ est clos par le haut, on a $\gamma_\sigma(y) \in X$. Ainsi $y \in \gamma_\sigma^{-1}(X)$, on a donc montré que la classe des clos par le haut est stable par résidu.

*Clos par le bas* : une preuve symétrique au cas "clos par le haut" prouve que la classe des clos par le bas est stable par résidu.

*Convexe* : $\mathbb{N}^m$ est convexe et une intersection quelconque de convexes reste convexe. Or la classe des convexes est stable par résidu. En effet considérons un mot $\sigma$ et un convexe $C \subseteq \mathbb{N}^m$. Montrons que $\gamma_\sigma^{-1}(C)$ est convexe. Pour cela, on prend deux vecteurs $x, x' \in \gamma_\sigma^{-1}(C)$ et un vecteur $z \in \mathbb{N}^m$ tels qu'il existe $t, t' \in \mathbb{Q}^+$ vérifiant $t + t' = 1$ et $z = t.x + t'.x'$ et on montre que $z \in \gamma_\sigma^{-1}(C)$. Comme $\gamma_\sigma$ est une fonction affine, on a $\gamma_\sigma(z) = t.\gamma_\sigma(x) + t'.\gamma_\sigma(x')$. Par convexité de $C$, on obtient $\gamma_\sigma(z) \in C$. La classe des ensembles convexes est donc stable par résidu. □

Le théorème 4.59, montre alors que l'enveloppe d'une partie $X \subseteq \mathbb{N}^m$ représentée par un automate binaire $\mathcal{A}$ peut-être calculée à partir de la couverture minimale de l'automate $\mathcal{A}$.

Dans la suite, les cas affines et semi-affines sont détaillés.

**Remarque 4.66**
*Le cas clos par le haut est symétrique du cas affine alors que le cas convexe est symétrique du cas semi-affine. On peut déduire de ce dernier cas un résultat inattendu : l'enveloppe*

*convexe d'un UBA est un polyèdre. Ces résultats ne sont pas développés dans cette thèse mais seront prochainement soumis à publication.*

### 4.4.2 Couverture affine

Dans cette sous-section, on prouve que l'algorithme 1 calcule en temps polynomial la couverture affine minimale d'un automate binaire. On obtient comme corollaire que l'enveloppe affine d'une partie $X \subseteq \mathbb{N}^m$ représentée par un automate binaire est calculable en temps polynomial.

**Algorithme 1** Algorithme de calcul de la couverture affine minimale.

1: **entrée :** un automate binaire $\mathcal{A}$.
2: **sortie :** la couverture affine minimale de l'automate binaire $\mathcal{A}$.
3:
4: Soit $(A_q)_{q \in Q}$ la suite de parties affines de $\mathbb{N}^m$ définie par

$$A_q = \begin{cases} \{\overrightarrow{0}\} & \text{si } q \in F \\ \emptyset & \text{sinon} \end{cases}$$

5: **tant que** il existe une transition $q \xrightarrow{b} q'$ telle que $\gamma_b(A_{q'}) \not\subseteq A_q$ **faire**
6: $\quad A_q \Leftarrow \text{aff}_{\mathbb{N}^m}(A_q \cup \gamma_b(A_{q'}))$
7: **renvoyer** $(A_q)_{q \in Q}$

**Théorème 4.67**
*La couverture affine minimale d'un automate binaire est calculée en temps polynomial par l'algorithme 1.*

*Démonstration :*
On commence par montrer que la ligne 6 de l'algorithme est exécutée au plus $(m+1).|Q|$ fois. À chaque fois que la ligne 6 est exécutée, la dimension de la partie affine $A_q$ croît strictement. Comme la dimension d'une partie affine de $\mathbb{N}^m$ est un entier entre 0 et $m-1$, la ligne 6 ne peut être exécutée qu'au plus $(m+1).|Q|$ fois.

Montrons alors que les espaces affines calculés par l'algorithme ont une taille qui reste polynômialement petite tout au long de l'exécution. Notons $i$ le nombre de fois que la ligne 6 a été exécutée. Une récurrence immédiate prouve que pour tout état $q \in Q$, il existe une partie $X_q \subseteq \gamma_{\Sigma_r^{\leqslant i}}(\overrightarrow{0})$ telle que $A_q = \text{aff}_{\mathbb{N}^m}(X_q)$. Comme $\text{taille}(\gamma_\sigma(\overrightarrow{0})) \leqslant m.\log(|\sigma|)$ pour tout $\sigma \neq \varepsilon$, le théorème 3.23 montre que la taille des espaces affines calculés reste polynômialement petite.

On a donc prouvé que l'algorithme s'exécutait en temps polynomial. Il reste alors à montrer que cet algorithme calcule bien la couverture affine minimale.

Rappelons que $(A_q)_{q \in Q} \subseteq_Q (A'_q)_{q \in Q}$ si et seulement si $A_q \subseteq A'_q$ pour tout $q \in Q$. Montrons qu'à toute étape de l'algorithme, la suite $(A_q)_{q \in Q}$ est incluse dans $\text{cov}(\mathcal{A})$. Remarquons que $(A_q)_{q \in Q}$ est bien incluse dans $\text{cov}(\mathcal{A})$ après l'exécution de la ligne 4.

Comme la ligne 6 est la seule autre ligne qui modifie la suite $(A_q)_{q\in Q}$, il suffit de montrer que si $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$ avant l'exécution de la ligne 6 alors $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$ après son exécution. Considérons $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$ et une transition $q \xrightarrow{b} q'$. On a $\mathrm{aff}_{\mathbb{N}^m}(A_q \cup \gamma_b(A_{q'})) \subseteq \mathrm{cov}(\mathcal{A})_q$ et par définition d'une couverture, $\mathrm{cov}(\mathcal{A})_{q'} \subseteq \gamma_b^{-1}(\mathrm{cov}(\mathcal{A})_q)$. Comme de plus $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$, on a $\gamma_b(A_{q'}) \subseteq \gamma_b(\mathrm{cov}(\mathcal{A})_{q'}) \subseteq \mathrm{cov}(\mathcal{A})_q$. Ainsi, on a $A_q \cup \gamma_b(A_{q'}) \subseteq \mathrm{cov}(\mathcal{A}_q)$. Comme $\mathrm{cov}(\mathcal{A})_q$ est une partie affine de $\mathbb{N}^m$, on a donc prouvé l'inclusion recherchée $\mathrm{aff}_{\mathbb{N}^m}(A_q \cup \gamma_b(A_{q'})) \subseteq \mathrm{cov}(\mathcal{A})_q$.

Cela montre en particulier qu'à la ligne 7, l'inclusion $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$ reste valide.

Montrons alors qu'à la ligne 7, la suite $(A_q)_{q\in Q}$ est une couverture. À cette ligne, la condition de la boucle **tant que** n'est plus valide. On a donc $\gamma_b(A_{q'}) \subseteq A_q$ pour toute transition $q \xrightarrow{b} q'$. D'où $A_{q'} \subseteq \gamma_b^{-1}(A_q)$. De $\overrightarrow{0} \in A_{q_f}$ pour tout état $q_f \in F$, on déduit que $(A_q)_{q\in Q}$ est une couverture de l'automate $\mathcal{A}$. Par minimalité de la couverture $\mathrm{cov}(\mathcal{A})$, on obtient $\mathrm{cov}(\mathcal{A}) \subseteq_Q (A_q)_{q\in Q}$. Enfin, comme $(A_q)_{q\in Q} \subseteq_Q \mathrm{cov}(\mathcal{A})$, on a bien l'égalité $\mathrm{cov}(\mathcal{A}) = (A_q)_{q\in Q}$. □

En remarquant qu'un automate binaire est un cas particulier de “programmes affines”, on aurait pu déduire de [MOS04], un algorithme de calcul de la couverture affine en temps polynomial.

**Corollaire 4.68**
*L'enveloppe affine d'une partie $X \subseteq \mathbb{N}^m$ représentée par un automate binaire est calculable en temps polynomial.*

### 4.4.3 Couverture semi-affine

Dans cette sous-section, on prouve que la couverture semi-affine minimale d'un automate binaire est calculable en temps exponentiel. Pour calculer cette couverture, on montre qu'en “dépliant” un automate binaire, on obtient un nouvel automate binaire dont la couverture semi-affine minimale coïncide avec la couverture affine minimale. Il suffira alors d'utiliser l'algorithme de calcul de la couverture affine minimale sur ce nouvel automate pour en déduire la couverture semi-affine minimale de l'automate binaire de départ.

Pour cela, on commence par étudier des propriétés de stabilité des parties affines. Puis, on introduit la classe des automates binaires dépliés. Enfin, on prouve que la couverture semi-affine est calculable en temps exponentiel.

#### 4.4.3.1 Stabilité des parties affines

On montre deux résultats de stabilité des espaces affines, à savoir que, pour toute partie $X \subseteq \mathbb{N}^m$, telle que $\mathrm{saff}(X)$ est affine,

- l'enveloppe $\mathrm{saff}(\gamma_\sigma(X))$ est affine pour tout mot $\sigma \in \Sigma_r^*$, et
- l'enveloppe $\mathrm{saff}(\gamma_{\mathcal{L}^*}(X))$ est affine pour tout langage $\mathcal{L} \subseteq (\Sigma_r^m)^*$.

Le premier résultat de stabilité s'obtient comme corollaire du lemme suivant.

**Lemme 4.69**
*Pour toute partie $X \subseteq \mathbb{Q}^m$ et pour tout mot $\sigma$, on a :*

$$\mathrm{saff}(\lambda_\sigma(X)) = \lambda_\sigma(\mathrm{saff}(X))$$

*Démonstration :*

Comme la fonction $\lambda_\sigma$ est une fonction affine et bijective sur $\mathbb{Q}^m$, on peut appliquer la proposition 3.13 à la fonction $\lambda_\sigma^{-1}$. On obtient alors l'égalité énoncée. □

**Corollaire 4.70**
*Pour toute partie $X \subseteq \mathbb{N}^m$ telle que* $\mathrm{saff}(X)$ *est affine et pour tout mot $\sigma \in \Sigma_r^*$, l'enveloppe* $\mathrm{saff}(\gamma_\sigma(X))$ *est affine.*

Pour montrer le second résultat de stabilité, on commence par caractériser dans le lemme 4.71 l'enveloppe $\mathrm{saff}(\lambda_{\sigma^*}(X))$ puis on montre dans le lemme 4.72 un résultat de commutativité $\mathrm{saff}(\lambda_{\sigma_1^*\sigma_2^*}(X)) = \mathrm{saff}(\lambda_{\sigma_2^*\sigma_1^*}(X))$.

**Lemme 4.71**
*Pour toute partie $X \subseteq \mathbb{Q}^m$ et pour tout mot $\sigma$ tel que $m$ divise la longueur de $\sigma$, on a :*

$$\mathrm{saff}(\lambda_{\sigma^*}(X)) = \mathbb{Q}.\left(\mathrm{saff}(X) + \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)\right) - \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)$$

*Démonstration :*

On note $S$ le semi-affine de $\mathbb{Q}^m$ défini par $S = \mathrm{saff}(\bigcup_{k\geqslant 0} \lambda_{\sigma^k}(X))$ et on note $S_X$ l'espace semi-affine $S_X = \mathrm{saff}(X)$. Le lemme 4.69 prouve que pour tout entier $k \geqslant 0$, on a $\lambda_\sigma^k(S_X) = \mathrm{saff}(\lambda_{\sigma^k}(X)) \subseteq S$. Une récurrence immédiate sur $k$ montre que pour tout $a \in S_X$, on a :

$$\begin{aligned}
\lambda_\sigma^k(a) &= r^{\frac{|\sigma|}{m}.k}.a + \frac{r^{\frac{|\sigma|}{m}.k} - 1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma) \\
&= r^{\frac{|\sigma|}{m}.k}.\left(a + \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)\right) - \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)
\end{aligned}$$

En appliquant la proposition 3.13 qui permet “de faire sortir” une fonction affine d'une enveloppe semi-affine, on déduit de l'égalité précédente :

$$\mathrm{saff}(\lambda_{\sigma^*}(\{a\})) = \mathbb{Q}.\left(a + \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)\right) - \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)$$

En rappelant que $\mathrm{saff}(\lambda_{\sigma^*}(\{a\})) \subseteq S$ pour tout $a \in S_X$, on obtient :

$$S' = \mathbb{Q}.\left(S_X + \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma)\right) - \frac{1}{r^{\frac{|\sigma|}{m}} - 1}.\rho_m(\sigma) \subseteq S$$

En prenant l'enveloppe semi-affine de l'inclusion $\bigcup_{k\geqslant 0} \lambda_{\sigma^k}(X) \subseteq S'$, on déduit $S \subseteq S'$. On a donc prouvé $S = S'$. □

**Lemme 4.72**
*Pour toute partie $X \subseteq \mathbb{N}^m$ et pour tout couple de mots $(\sigma_1, \sigma_2)$ tel que $m$ divise la longueur de $\sigma_1$ et la longueur de $\sigma_2$, on a :*

$$\mathrm{saff}(\lambda_{\sigma_1^*\sigma_2^*}(X)) = \mathrm{saff}(\lambda_{\sigma_2^*\sigma_1^*}(X))$$

*Démonstration :*
Posons $x_1 = \frac{1}{r^{\frac{|\sigma_1|}{m}}-1}.\rho_m(\sigma_1)$ et $x_2 = \frac{1}{r^{\frac{|\sigma_2|}{m}}-1}.\rho_m(\sigma_2)$. Le lemme 4.71 montre que

$$\begin{aligned}
\mathrm{saff}(\lambda_{\sigma_1^*\sigma_2^*}(X)) &= \mathbb{Q}.\left(\mathrm{saff}(\lambda_{\sigma_2^*}(X)) + x_1\right) - x_1 \\
&= \mathbb{Q}.\left(\mathbb{Q}.\left(\mathrm{saff}(X) + x_2\right) - x_2 + x_1\right) - x_1 \\
&= \mathbb{Q}.\left(\mathrm{saff}(X) + x_2\right) + \mathbb{Q}.\left(x_1 - x_2\right) - x_1 \\
&= \mathbb{Q}.\left(\mathrm{saff}(X) + \frac{1}{2}(x_1 + x_2)\right) + \mathbb{Q}.\left(x_1 - x_2\right) - \frac{1}{2}(x_1 + x_2)
\end{aligned}$$

Par symétrie, on obtient donc $\mathrm{saff}(\lambda_{\sigma_1^*\sigma_2^*}(X)) = \mathrm{saff}(\lambda_{\sigma_2^*\sigma_1^*}(X))$. □

On peut alors démontrer le second résultat de stabilité.

**Proposition 4.73**
*Pour toute partie $X \subseteq \mathbb{N}^m$ telle que $\mathrm{saff}(X)$ est affine et pour tout langage $\mathcal{L} \subseteq (\Sigma_r^m)^*$, l'enveloppe $\mathrm{saff}(\gamma_{\mathcal{L}^*}(X))$ est affine.*

*Démonstration :*
Comme $\mathcal{L}$ est dénombrable, on peut considérer une suite de mots $\sigma_i \in \mathcal{L}$ telle que $\mathcal{L} = \{\sigma_i;\ i \geqslant 0\}$. Considérons la suite $(A_i)_{i\geqslant 0}$ de semi-affines de $\mathbb{Q}^m$ définie par la récurrence suivante : $A_0 = \mathrm{saff}(X)$ et $A_{i+1} = \mathrm{saff}(\gamma_{\sigma_i^*}(A_i))$. Le lemme 4.69 montre que pour tout $i \geqslant 0$, l'espace $A_i$ est affine. Ainsi, la suite $(A_i)_{i\geqslant 0}$ est une suite croissante d'espaces affines de $\mathbb{Q}^m$. Une telle suite est nécessairement stationnaire. Ainsi, il existe un indice $i_0 \geqslant 0$ tel que pour tout $i \geqslant i_0$, on a $A_i = A_{i_0}$. En particulier, cela prouve que pour tout $i \geqslant i_0$, on a $\lambda_{\sigma_i}(A) \subseteq A$. Puisque $A = \mathrm{saff}(\lambda_{\sigma_0^*\dots\sigma_{i_0}^*}(A_0))$, par le lemme 4.71, pour tout $i \leqslant i_0$, on a $A = \mathrm{saff}(\lambda_{\sigma_i^*.\sigma_0^*\dots\sigma_{i-1}^*.\sigma_{i+1}^*\dots\sigma_{i_0}^*}(A_0))$. Ainsi $\lambda_{\sigma_i}(A) \subseteq A$ pour tout $i \leqslant n_0$. On a donc montré $\lambda_\sigma(A) \subseteq A$ pour tout $\sigma \in \mathcal{L}$. En particulier $\mathrm{saff}(\lambda_{\mathcal{L}^*}(A)) \subseteq A$. Comme $X \subseteq A$, on a montré que $\mathrm{saff}(\lambda_{\mathcal{L}^*}(X)) \subseteq A$. Comme de plus $A = \mathrm{saff}(\lambda_{\sigma_0^*\dots\sigma_{i_0}^*}(X))$, on a aussi $A \subseteq \mathrm{saff}(\lambda_{\mathcal{L}^*}(X))$. □

#### 4.4.3.2 Dépliage d'un automate binaire

Pour pouvoir utiliser les deux résultats de stabilité des espaces affines, prouvés précédemment, on définit la classe des automates binaires dépliés et on montre comment déplier un automate.

**Définition 4.74**
*Un automate binaire déplié est un automate binaire $\mathcal{A}$ tel que :*

*(P1) l'ensemble des états finaux est un singleton $F = \{q_f\}$,*
*(P2) l'entier $m$ divise la longueur de toutes les boucles $q \xrightarrow{\sigma} q$, et*
*(P3) pour toute composante fortement connexe $C$, il existe au plus une transition $q \xrightarrow{b} q'$ telle que $q \in C$ et $q' \notin C$.*

On commence par montrer que la propriété (P2) peut-être facilement imposée à un automate binaire (elle est vérifiée par les NDD), puis on prouve que tout automate binaire possédant cette propriété peut-être déplié.

**Lemme 4.75**
*Pour tout automate binaire $\mathcal{A}$, on peut construire en temps polynomial un automate binaire $\mathcal{A}'$ acceptant le même langage et vérifiant (P2).*

*Démonstration :*
Il suffit de synchroniser l'automate $\mathcal{A} = (Q, \Sigma_r, \Delta, Q_0, F)$ avec l'automate acceptant le langage $(\Sigma_r^m)^*$. On note $k[m] \in \{0, \dots, m-1\}$ le reste de la division euclidienne de l'entier $k \in \mathbb{Z}$ par $m$. L'automate $\mathcal{A}'$ est défini par :
- $Q' = Q \times \{0, \dots, m-1\}$,
- $\Delta' = \{(q, i[m]) \xrightarrow{b} (q', i+1[m]);\ (q, b, q') \in \Delta;\ i \in \mathbb{N}\}$,
- $Q'_0 = Q_0 \times \{0\}$, et
- $F' = F \times \{0, \dots, m-1\}$.

Remarquons que par construction $\mathcal{A}'$ convient. □

**Lemme 4.76**
*Pour tout automate binaire $\mathcal{A}$ vérifiant (P2), on peut construire en temps exponentiel un automate binaire déplié $\mathcal{A}'$ acceptant le même langage.*

*Démonstration :*
Il suffit de "déplier" les composantes fortement connexes de l'automate binaire $\mathcal{A}$. □

On déduit des deux lemmes précédents que tout automate binaire peut être déplié.

**Proposition 4.77**
*De tout automate binaire $\mathcal{A}$, on construit en temps exponentiel un automate binaire déplié $\mathcal{A}'$ acceptant le même langage.*

#### 4.4.3.3 Calcul de la couverture semi-affine

On montre comment calculer la couverture semi-affine minimale d'un automate binaire en prouvant que la couverture semi-affine minimale d'un automate binaire déplié est égale à sa couverture affine minimale.

**Proposition 4.78**
*La couverture semi-affine minimale d'un automate binaire déplié est égale à sa couverture affine minimale.*

*Démonstration :*

Pour tout couple d'états $(q,q')$, on note $\mathcal{L}_{q\to q'}$ l'ensemble des étiquettes des chemins allant de $q$ à $q'$.

On commence par montrer que pour toute partie $X \subseteq \mathbb{N}^m$ telle que $\mathrm{cov}_{\mathbb{Q}^m}(X)$ est affine et pour tout couple d'états $(q,q')$ dans la même composante fortement connexe, l'enveloppe semi-affine $S = \mathrm{saff}(\gamma_{\mathcal{L}_{q\to q'}}(X))$ est affine. La proposition 4.73 prouve que $A = \mathrm{saff}(\gamma_{\mathcal{L}_{q'\to q'}}(X))$ est un espace affine. Considérons un mot $\sigma_0 \in \mathcal{L}_{q\to q'}$ et montrons que $S = \lambda_{\sigma_0}(A)$. Comme $S \supseteq \mathrm{saff}(\gamma_{\sigma_0.\mathcal{L}_{q\to q}}(X)) = \lambda_{\sigma_0}(A)$, il suffit de montrer l'inclusion inverse. Considérons donc un mot $\sigma \in \mathcal{L}_{q\to q'}$. Comme $q$ et $q'$ sont dans la même composante fortement connexe, il existe un mot $w \in \mathcal{L}_{q'\to q}$. On a $\mathrm{saff}(\gamma_{w\sigma\mathcal{L}_{q'\to q'}}(X)) = \lambda_{w\sigma}(\mathrm{saff}(\gamma_{\mathcal{L}_{q\to q}}(X)))$. Comme de plus $\gamma_{w\sigma\mathcal{L}_{q'\to q'}}(X) \subseteq \gamma_{\mathcal{L}_{q'\to q'}}(X)$, on a montré que $\lambda_{w\sigma}(A) \subseteq A$. Comme $\lambda_{w\sigma_0}$ est une fonction affine bijective et comme $A$ est un espace affine, cette inclusion est en fait une égalité $\lambda_{w\sigma}(A) = A$. En particulier pour $\sigma = \sigma_0$, on a aussi $\lambda_{w\sigma_0}(A) = A$. Ainsi, $\lambda_\sigma(A) = \lambda_w^{-1}(A) = \lambda_{\sigma_0}(A)$. On a donc en particulier prouvé que $\gamma_\sigma(X) \subseteq \lambda_\sigma(A) = \lambda_{\sigma_0}(A)$. On obtient alors $S = \mathrm{saff}(\gamma_{\mathcal{L}_{q\to q'}}(X)) \subseteq \lambda_{\sigma_0}(A)$. On a ainsi démontré que $\mathrm{saff}(\gamma_{\mathcal{L}_{q'\to q}}(X))$ est affine.

On note $q_f$ l'unique état final de l'automate binaire déplié $\mathcal{A}$ et on note $C_f$ la composante fortement connexe associée à $q_f$. Pour chaque composante fortement connexe $C \neq C_f$ de $\mathcal{A}$ telle qu'il existe un chemin allant d'un état de $C$ à $q_f$, on note $q_C \xrightarrow{b_C} q'_C$ l'unique transition telle que $q_C \in C$ et $q'_C \notin C$. La composante fortement connexe associée à $q'_C$ est notée $\alpha(C)$.

Considérons alors un état $q \in Q$ et notons $C$ sa composante fortement connexe associée. Remarquons que s'il n'existe pas de chemin allant de $q$ à $q_f$ alors $\mathcal{L}(\mathcal{A})_q = \emptyset$. Les lemmes 4.53 et 4.58 montrent alors que $\mathrm{cov}(\mathcal{A})_q = \emptyset$ et la proposition est donc vraie. On peut donc supposer qu'il existe un chemin allant de $q$ à $q_f$ et on note alors $C_n,\dots,C_0$ l'unique suite de composantes fortement connexes définie par $C_n = C$, $C_0 = C_f$ et $C_i = \alpha(C_{i+1})$. Remarquons que le langage $\mathcal{L}(\mathcal{A}_q)$ est par conséquence égal à $\mathcal{L}_{q\to q_f}$ si $n = 0$ et au langage suivant dans le cas $n \geqslant 1$ :

$$\mathcal{L}(\mathcal{A}_q) = \mathcal{L}_{q\to q_{C_0}} b_{C_0} \mathcal{L}_{q'_{C_0}\to q_{C_1}} \dots b_{C_{n-1}} \mathcal{L}_{q'_{C_{n-1}}\to q_{C_n}}$$

Or, d'après les lemmes 4.53 et 4.58, la couverture $\mathrm{cov}(\mathcal{A}_q)$ est égale à $\mathrm{saff}(\mathcal{L}(\mathcal{A}_q))$. Une récurrence immédiate sur $n$ montre dès lors que cette enveloppe est affine. □

On obtient par suite un algorithme de calcul en temps exponentiel de l'enveloppe semi-affine d'une partie $X$ représentée par un automate binaire.

**Théorème 4.79**
*Soit $X \subseteq \mathbb{N}^m$ une partie représentée par un automate binaire $\mathcal{A}$. L'ensemble des composantes affines de* $\mathrm{saff}(X)$ *est calculable en temps exponentiel. De plus, chaque composante a une taille polynomiale.*

*Démonstration :*

Considérons un automate binaire $\mathcal{A}$. On commence par déplier l'automate $\mathcal{A}$ en utilisant la proposition 4.77. On obtient alors un automate binaire déplié $\mathcal{A}'$ acceptant le même langage que $\mathcal{A}$. On calcule la couverture affine minimale de l'automate binaire $\mathcal{A}_q$ avec le corollaire 4.68. Montrons que les espaces affines obtenus ont une taille polynomiale en la taille de $\mathcal{A}$. Pour cela, il suffit de remarquer que l'on peut déplier à la volée les composantes de l'automate $\mathcal{A}$. La proposition 4.78 montre que cette couverture affine est en fait la couverture semi-affine minimale. En utilisant le théorème 4.59, on obtient à partir de cette couverture, les composantes affines de $\mathrm{saff}(X)$. □

**Corollaire 4.80**
*La couverture semi-affine minimale d'un automate binaire est calculable en temps exponentiel.*

*Démonstration :*
Considérons un automate binaire $\mathcal{A}$. En appliquant le théorème 4.79 aux automates binaire $\mathcal{A}_q$, on déduit des lemmes 4.53 et 4.58 la couverture semi-affine de $\mathcal{A}$. □

Cette complexité exponentielle en temps ne peut pas être évitée en général comme le montre le lemme 4.81. Ainsi, tout algorithme qui calcule la couverture semi-affine minimale d'un automate binaire en représentant les semi-affines de $\mathbb{N}^m$ par une union finie de parties affines de $\mathbb{N}^m$, demande au moins un temps exponentiel. Pour obtenir une meilleure complexité il est donc nécessaire de choisir une autre représentation des parties semi-affines de $\mathbb{N}^m$. Dans le chapitre 5 suivant, on étudiera la représentation des semi-affines par des automates binaires canoniques.

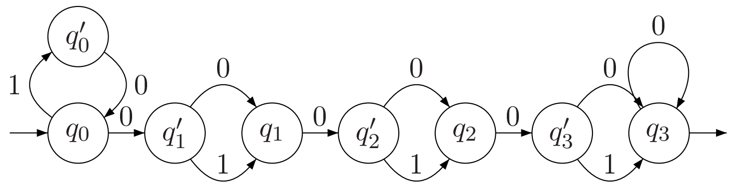
**Lemme 4.81**
*Il existe une suite d'UBA $(\mathcal{A}_n)_{n\geqslant 1}$ telle que le nombre d'états de $\mathcal{A}_n$ est égal à $2.n+3$ et telle que le nombre de composantes affines de $\mathrm{saff}(\rho_m(\mathcal{L}(\mathcal{A})))$ est égal à $2^n$.*

*Démonstration :*
On considère l'automate $\mathcal{A}_n = (Q_n, \Sigma_2, \Delta_n, \{q_0\}, \{q_n\})$ défini par

$$Q_n = \{q_0, q_0', q_1, q_1' \ldots, q_n, q_n'\}$$

et par $\Delta_n = \{q_0 \xrightarrow{1} q_0', q_0' \xrightarrow{0} q_0\} \bigcup_{1\leqslant i\leqslant n}\{q_{i-1} \xrightarrow{0} q_i', q_i' \xrightarrow{0,1} q_i\} \cup \{q_n \xrightarrow{0} q_n\}$. L'automate $\mathcal{A}_3$ est représenté par la figure 4.1. Remarquons qu'en complétant l'automate $\mathcal{A}_n$ (il suffit d'ajouter un état puit et des transitions allant vers cet état), on obtient un UBA à $2.(n+1)+1 = 2.n+3$ états reconnaissant la partie $X_n = \rho_m((1.0)^*.(0.(0+1))^n.0^*)$. De $\rho_m((0.(0+1))^n.0^*) = \{0\} \times \{0, \ldots, 2^n - 1\}$, on déduit $X_n = \{2^k.(0,i) + (2^k - 1).(1,0);\ k \geqslant 0;\ i \in \{0, \ldots, 2^n - 1\}\}$. Les propositions 3.13 et 3.12 montrent alors que $\mathrm{saff}(X_n) = \bigcup_{0\leqslant i<2^n} \mathbb{Q}.(1,i) - (1,0)$. L'ensemble des composantes de $\mathrm{saff}(X_n)$ est donc égal à $\{\mathbb{Q}.(1,i) - (1,0);\ i \in \{0, \ldots, 2^n - 1\}\}$. □

**Figure 4.1** L'automate $\mathcal{A}_3$



CHAPITRE 5

# Automate binaire et formule de Presburger

Dans ce chapitre, on étudie le lien entre les formules de Presburger et les automates binaires et on montre comment construire une formule de Presburger (sans quantificateur) à partir d'un automate binaire.

La logique de Presburger permet de décrire le lien entre les compteurs d'un système, avant et après l'exécution d'une transition ([BGP97] [BGP99] [CJ98] [FL02]), de définir et de calculer des ensembles d'états accessibles ([Boi98] [FO97b] [HP79] [Lam94] [BFLP03] [FS00a] [FS00b]).

Le problème de la validité d'une formule de Presburger est donc un problème central en vérification. Pour "dépasser" sa complexité élevée ([Ber77] [FR74]), différentes techniques de résolution ont été proposées ; l'outil Omega ([Ome]) élimine les quantificateurs et simplifie les formules ([FR74]) ; l'outil Brain ([Bra] [RV02]) décompose un ensemble Presburger-définissable sous forme d'un semi-linéaire ([GS66] [Huy85] [Reu89] [Hue78] [vzGS78]) ; les outils Csl-Alv, Fast, Lash et Mona considèrent une représentation par automate binaire (chapitre 4), aussi appelé NDD ([Boi98] [WB95] [WB00]) ou DFA ([BC96] [Kla97] [KMS02]) ; on trouvera dans [GBD02] une étude comparative de ces différentes techniques.

N'oublions pas qu'il *ne suffit pas* de savoir représenter des ensembles d'états, pour calculer effectivement l'ensemble des états accessibles d'un système. En effet, pour qu'un calcul itératif de point fixe, utilisant la logique de Presburger, converge, il est crucial de *simplifier* les structures obtenues à chaque itération. La représentation par automate est bien adaptée à ce problème. En effet, une simple minimisation d'automate ([Hop71]) permet de représenter *canoniquement* un ensemble défini par une formule de Presburger. Cela explique pourquoi les "model-checker symboliques" comme Csl-Alv, Fast ou Lash utilisant cette représentation en interne, arrivent à calculer efficacement des ensembles d'états accessibles ([BB02] [BB03] [FL02]).

Cependant, cette représentation par automate pose au moins *trois problèmes*. *Premièrement*, les automates peuvent être exponentiellement plus grands qu'une formule équivalente sans quantificateur ([BC96],[WB95]). *Deuxièmement*, on peut difficilement appliquer des méthodes d'abstraction comme celles développées dans [BPR02] consistant "à oublier une partie des formules". *Enfin*, alors que l'on peut avoir une "intuition" de l'ensemble représenté par une formule de Presburger, cela est difficile même pour un automate binaire d'une dizaine d'états.

Afin de contourner ces problèmes, nous nous proposons d'étudier la synthèse d'une formule de Presburger à partir d'un automate binaire. Rappelons que dans [Muc03] et [BHMV94], il est prouvé que l'on peut décider si un ensemble représenté par un automate binaire est Presburger-définissable (on déduit un algorithme décidant si un automate binaire représente un ensemble Presburger-définissable en temps 4-EXP). Malheureusement, aucune piste n'est donnée pour synthétiser une formule en temps élémentaire.

Dans ce chapitre, on s'intéresse à un sous-problème, celui de la synthèse d'une formule non-quantifiée. Ce problème est motivé par le fait que toute formule de Presburger peut être vue comme une succession de quantificateurs appliqués à une *formule non-quantifiée*, et qu'expérimentalement l'ensemble d'accessibilité de beaucoup de systèmes à compteurs est représentable par une formule de Presburger sans quantificateur (chapitre 10).

On a obtenu les résultats suivants :

- On peut décider en temps exponentiel si l'ensemble représenté par un automate binaire est non-quantifié (voir la fin du chapitre 2 pour la définition de non-quantifié).
- Pour un tel automate, on peut faire la synthèse d'une formule de Presburger non-quantifiée en temps exponentiel.

Dans la section 5.1, on rappelle comment construire en temps élémentaire l'automate binaire canonique (CBA) représentant les solutions d'une formule de Presburger. Puis, dans la section 5.2, on montre qu'en temps exponentiel, on peut décider si un automate binaire représente une partie non-quantifiée. Enfin, dans la dernière section 5.3 on prouve qu'en temps exponentiel, on peut synthétiser une formule de Presburger non-quantifiée à partir d'un automate.

## 5.1 De la formule à l'automate

Toute formule de Presburger est équivalente à une formule de la forme $Q_1 \dots Q_n \phi$ où $\phi$ est une formule non-quantifiée et où $Q_i$ est un quantificateur ($Q_i \in \{\exists x, \forall x\}$), simplement en déplaçant les quantificateurs d'une formule vers la gauche.

Dans les sous-sections 5.1.1 et 5.1.2, on étudie les algorithmes de construction des automates binaires canoniques représentant respectivement une partie non-quantifiée et une partie définissable dans la logique de Presburger.

### 5.1.1 Formule non-quantifiée

Comme une formule non-quantifiée est une conjonction, disjonction ou négation de formules de la forme $\langle \alpha, x \rangle = c$, il est naturel de chercher à construire pour une telle formule l'automate binaire canonique $\mathcal{A}_{\alpha,c}$ représentant l'ensemble des vecteurs $x \in \mathbb{N}^m$ solutions. On prouve qu'il n'existe pas d'algorithme construisant $\mathcal{A}_{\alpha,c}$ en temps polynomial en la taille de l'entrée et de la sortie du problème : taille($\alpha$) + taille($c$) + taille($\mathcal{A}_{\alpha,c}$). On déduit de ce résultat qu'un algorithme qui construit un automate binaire non ambigu (qui peut être ou non canonique) $\mathcal{A}'_{\alpha,c}$ équivalent à $\mathcal{A}_{\alpha,c}$ en temps polynomial en l'entrée et la sortie de l'algorithme $\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}'_{\alpha,c})$ produit des automates binaires qui ne peuvent pas être polynômialement petits devant $\mathcal{A}_{\alpha,c}$. Il faudra alors penser à utiliser systématiquement un algorithme de minimisation d'automates après l'utilisation d'un tel algorithme de construction.

Pour montrer que la construction de l'automate binaire canonique $\mathcal{A}_{\alpha,c}$ ne peut se faire en temps polynomial, on commence par énoncer le résultat de complexité suivant.

**Proposition 5.1 ([Sch87])**
*Soit $\alpha \in \mathbb{Z}^m$ et $c \in \mathbb{Z}$. Décider si le système $\langle \alpha, x\rangle = c$ admet une solution $x \in \mathbb{N}^m$ est NP-complet.*

**Remarque 5.2**
*Rappelons que l'on peut décider en temps polynomial si $\langle \alpha, x\rangle = c$ admet une solution dans $\mathbb{Z}^m$ ([Sch87]).*

On en déduit alors la proposition recherchée.

**Proposition 5.3**
*Il n'existe pas d'algorithme de construction de l'automate binaire canonique $\mathcal{A}_{\alpha,c}$ en temps polynomial en l'entrée et la sortie du problème* $\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}_{\alpha,c})$ *sous la conjecture P≠NP.*

*Démonstration :*
Supposons qu'il existe un algorithme construisant l'automate $\mathcal{A}_{\alpha,c}$ en temps polynomial en $\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}_{\alpha,c})$. Par hypothèse, il existe un polynôme $P(X) \in \mathbb{N}[X]$ que l'on peut supposer non constant tel que pour tout $\alpha \in \mathbb{Z}^m$ et pour tout $c \in \mathbb{Z}$, l'algorithme de construction de $\mathcal{A}_{\alpha,c}$ s'arrête après $P(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}_{\alpha,c}))$ étapes. On définit alors un nouvel algorithme qui prend en entré un couple $(\alpha, c)$ et décide si $\langle \alpha, x\rangle = c$ admet une solution $x \in \mathbb{N}^m$. L'algorithme simule l'algorithme de construction de $\mathcal{A}_{\alpha,c}$ pendant $P(\text{taille}(\alpha)+\text{taille}(c)+\text{taille}(\mathcal{A}(\emptyset)))$ étapes où $\mathcal{A}(\emptyset)$ est l'automate binaire canonique représentant l'ensemble vide. Si l'algorithme termine avant ce nombre d'étapes maximal, il suffit de décider que $\langle \alpha, x\rangle = c$ admet une solution $x \in \mathbb{N}^m$ si et seulement si le langage accepté par l'automate $\mathcal{A}_{\alpha,c}$ est non vide (ce test se fait en temps polynomial en $\text{taille}(\mathcal{A})_{\alpha,c} \leqslant P(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}(\emptyset)))$. Si l'algorithme n'a pas terminé avant, comme la fonction $i \to P(i)$ définie sur $\mathbb{N}$ est strictement croissante, et que $P(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}_{\alpha,c})) < P(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}(\emptyset))$, on a $\mathcal{A}(\emptyset) \neq \mathcal{A}_{\alpha,c}$. Dans ce cas $\mathcal{L}(\mathcal{A}_{\alpha,c})$ est non vide et il existe ainsi un vecteur $x \in \mathbb{N}^m$ solution de $\langle \alpha, x\rangle = c$. L'algorithme décide alors que $\langle \alpha, x\rangle = c$ admet une solution $x \in \mathbb{N}^m$. On a donc prouvé l'existence d'un algorithme en temps polynomial pour décider si $\langle \alpha, x\rangle = c$ admet une solution $x \in \mathbb{N}^m$. Comme ce problème est NP-complet, on a $P = NP$. □

Modulo la conjecture P≠NP, on a donc montré qu'un algorithme de construction polynomial en l'entrée et la sortie n'est pas possible. Dans la pratique, les algorithmes de construction utilisés produisent des automates binaires non ambigus $\mathcal{A}'_{\alpha,c}$ équivalents à

$\mathcal{A}_{\alpha,c}$ en temps polynomial en $O(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}'_{\alpha,c}))$ comme le montre le lemme suivant.

**Lemme 5.4 ([WB00],[BC96],[BB02])**
*Il existe un algorithme de construction qui pour tout couple $(\alpha, c)$ construit un automate binaire non ambigu $\mathcal{A}'_{\alpha,c}$ équivalent à $\mathcal{A}_{\alpha,c}$ en temps linéaire en la taille de l'entrée et de la sortie* $\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}'_{\alpha,c})$. *De plus, le nombre d'états de l'automate $\mathcal{A}'_{\alpha,c}$ est borné par*

$$3.m.(||\alpha||_1 + 1).\frac{\ln\left(r + \frac{||c||_1+1}{||\alpha||_1+1}\right)}{\ln(r)}$$

**Remarque 5.5**
*La majoration du nombre d'états prouvée dans le lemme 5.4 précédent peut paraître compliquée mais elle est donnée pour unifier les deux bornes proposées, l'une par Boigelot et Wolper en $\ln(|c|).\,||\alpha||_1$ et l'autre par Bartzis, Boudet, Bultan, et Comon en $O(|c| + ||\alpha||_1)$. Ces deux bornes sont en effet complémentaires car l'une montre que la taille est linéaire en $||\alpha||_1$ quand $c$ et $||\alpha||_1$ sont du même ordre de grandeur et l'autre montre que la taille est logarithmique en $|c|$ quand $|c|$ est grand devant $||\alpha||_1$.*

Montrons que les automates $\mathcal{A}'_{\alpha,c}$ produits par un tel algorithme ne peuvent être polynômialement petits devant $\mathcal{A}_{\alpha,c}$.

**Proposition 5.6**
*Considérons un algorithme construisant pour tout couple $(\alpha, c)$ un automate binaire non ambigu $\mathcal{A}'_{\alpha,c}$ équivalent à $\mathcal{A}_{\alpha,c}$ en temps polynomial en* $O(\text{taille}(\alpha)+\text{taille}(c)+\text{taille}(\mathcal{A}'_{\alpha,c}))$. *Sous la conjecture P≠NP, il n'existe pas de polynôme $P$ tel que pour tout couple $(\alpha, c)$ on a :*

$$\text{taille}(\mathcal{A}'_{\alpha,c}) \leqslant P(\text{taille}(\mathcal{A}_{\alpha,c}))$$

*Démonstration :*
Supposons l'existence d'un tel polynôme $P$. Comme on peut minimiser l'automate $\mathcal{A}'_{\alpha,c}$ en temps polynômial, on obtient ainsi un algorithme de construction de $\mathcal{A}_{\alpha,c}$ en temps polynomial en $O(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}_{\alpha,c}))$. D'après la proposition 5.3, on a une contradiction. □

La proposition 5.6 montre ainsi l'importante de minimiser les automates produits par de tels algorithmes. Néanmoins, même après minimisation, la taille de l'automate $\mathcal{A}_{\alpha,c}$ peut rester exponentielle en $\text{taille}(\alpha)$, comme le montre le lemme 5.7 suivant.

**Lemme 5.7**
*Pour tout $n \geqslant 0$, posons $\alpha_n = (r^n, -1)$. On a alors* $\text{taille}(\alpha_n) = n.\frac{\ln(r)}{\ln(2)}$ *et* $\text{taille}(\mathcal{A}_{\alpha_n,0}) \geqslant r^n$.

*Démonstration :*
On se place donc dans le cas $m = 2$. Notons $X_n = \{(x_1, x_2);\ \langle\alpha_n, (x_1, x_2)\rangle = 0\} = \mathbb{N}.(1, r^n)$. Pour obtenir la taille de l'automate binaire canonique représentant $X_n$, étudions

l'ensemble des résidus $Q(X_n)$ de $X_n = \mathbb{N}.(1, r^n)$. On va montrer que $\{\mathbb{N}.(1, r^n) + (0, j);\ j \in \{0, \ldots, r^n - 1\}\} \subseteq Q(X_n)$. Considérons $i \in \{0, \ldots, r^n - 1\}$. Il existe une suite $(b_i)_{1 \leqslant i \leqslant n}$ de $\Sigma_r$ telle que le mot $\sigma = 0b_1 0b_2 \ldots 0b_n$ vérifie $\rho_2(\sigma) = (i, 0)$. On a alors $\gamma_\sigma^{-1}(X_n) = (\frac{1}{r^n}(\mathbb{N}.(1, r^n) - (i, 0))) \cap \mathbb{N}^m = \mathbb{N}.(1, r^n) + (0, i)$. Comme de plus, pour tout $i \neq i' \in \{0, \ldots, r^{n-1}\}$, on a $\mathbb{N}.(1, r^n) + (0, i) \neq \mathbb{N}.(1, r^n) + (0, i')$. On a donc démontré que le cardinal de $Q(X_n)$ est supérieur à $r^n$. Ainsi, taille$(\mathcal{A}_{\alpha_n, 0}) \geqslant r^n$. □

Du lemme 5.4, on déduit de plus une majoration de la taille des automates binaires canoniques représentant les solutions d'une formule non-quantifiée (voir la fin du chapitre 2 pour la définition de non-quantifié).

**Théorème 5.8 ([BC96],[WB95])**
*Soit $X \subseteq \mathbb{N}^m$ une partie non-quantifiée. Il existe un automate binaire non ambigu représentant $X$ qui a une taille bornée exponentiellement par la taille de toute formule non-quantifiée représentant $X$. De plus, un tel automate est calculable en temps exponentiel.*

*Démonstration :*
On montre le théorème par récurrence sur la longueur des formules $\phi$. Remarquons que si $\phi$ est une formule de la forme $\phi := (t = c)$, alors le lemme 5.4 montre que l'on peut construire en temps exponentiel un automate binaire non ambigu $\mathcal{A}_\phi$ représentant $[\![\phi]\!]$. Il suffit alors de remarquer qu'en temps polynomial on construit à partir de deux automates binaires non ambigus représentant respectivement $[\![\phi]\!]$ et $[\![\phi']\!]$, des automates binaires non ambigus représentant respectivement $[\![\neg\phi]\!]$, $[\![\phi \vee \phi']\!]$ et $[\![\phi \wedge \phi']\!]$. □

Cette borne exponentielle ne peut malheureusement pas être évitée en général comme le montre le lemme 5.7.

### 5.1.2 Formule de Presburger

Dans cette sous-section on rappelle comment construire l'automate binaire canonique représentant les solutions d'une formule de Presburger. Dans la précédente sous-section, on a montré comment construire l'automate binaire canonique associé à une formule non-quantifiée. Ainsi, il suffit de montrer comment à partir d'un automate binaire $\mathcal{A}_\phi$ représentant les solutions d'une formule $\phi$, on peut construire un automate binaire $\mathcal{A}_{Q\ \phi}$ représentant les solutions de la formule $Q\ \phi$ où $Q \in \{\exists x, \forall x\}$ est un quantificateur. On commence par montrer que cette construction est possible en temps exponentiel. On peut ainsi construire à partir de toute formule de Presburger $\phi$ un automate binaire représentant les solutions de $\phi$. Pour montrer que cette construction peut se faire en temps élémentaire, on éliminera les quantificateurs d'une formule avant de construire l'automate binaire des solutions.

#### 5.1.2.1 Projection

On commence par établir le lien entre la partie $X \subseteq \mathbb{N}^m$ des solutions d'une formule de Presburger $\phi$ et les parties $X_{\exists x_i}$ et $X_{\forall x_i}$ de $\mathbb{N}^{m-1}$ solutions respectivement de $\exists x_i \phi$ et $\forall x_i \phi$. Pour cela, on introduit la fonction de projection $\Pi_i$ qui "élimine" la $i$ème variable.

**Définition 5.9**
*Pour tout $i \in \{1, \ldots, m\}$, on note $\Pi_i(X) : \mathbb{N}^m \to \mathbb{N}^{m-1}$ la fonction définie par $\Pi_i(x_1, \ldots, x_m) = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)$.*

Par définition de $[\![\exists x_i\ \phi]\!]$ et $[\![\forall x_i\ \phi]\!]$, on déduit $X_{\exists x_i} = \Pi_i(X)$ et $X_{\forall x_i} = \mathbb{N}^m \backslash \Pi_i(\mathbb{N}^m \backslash X)$. Ainsi, pour construire un automate binaire non ambigu représentant $X_{\exists x_i}$ où $X_{\forall x_i}$ à partir d'un automate binaire non ambigu représentant $X$, il suffit de montrer comment construire un automate binaire non ambigu représentant $\Pi_i(X)$.

Pour caractériser les états d'un tel automate, il est naturel d'étudier les résidus de $\Pi_i(X)$.

**Proposition 5.10**
*Pour toute partie $X \subseteq \mathbb{N}^m$ et pour tout $i \in \{0, \ldots, m-1\}$, on a*

$$\gamma_b^{-1}(\Pi_i(X)) = \begin{cases} \Pi_{i+1}(\gamma_b^{-1}(X)) & si\ i < m \\ \bigcup_{b' \in \Sigma_r} \Pi_1(\gamma_{bb'}^{-1}(X)) & si\ i = m \end{cases}$$

*Démonstration :*
Considérons le cas $i < m$. Soit $y \in \gamma_b^{-1}(\Pi_i(X))$. Il existe $x \in X$ tel que $\gamma_b(y) = \Pi_i(x)$. De cette égalité, on déduit $(y_2, \ldots, y_{m-1}, r.y_1 + b) = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)$. On a alors $(y_1, \ldots, y_{m-1}) = (\frac{x_m - b}{r}, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{m-1}) = \Pi_{i+1}(\frac{x_m - b}{r}, x_1, \ldots, x_{m-1}) = \Pi_{i+1}(\gamma_b^{-1}(x))$. Ainsi $y \in \Pi_{i+1}(\gamma_b^{-1}(X))$. Pour l'inclusion réciproque, considérons $y \in \Pi_{i+1}(\gamma_b^{-1}(X))$. Il existe alors $x \in \gamma_b^{-1}(X)$ tel que $y = \Pi_{i+1}(x) = (x_1, \ldots, x_i, x_{i+2}, \ldots, x_m)$. On en déduit $\gamma_b(y) = (x_2, \ldots, x_i, x_{i+2}, \ldots, x_m, r.x_1 + b) = \Pi_i(x_2, \ldots, x_m, r.x_1 + b) = \Pi_i(\gamma_b(x))$. Comme $\gamma_b(x) \in X$, on a donc prouvé que $\gamma_b(y) \in \Pi_i(X)$. Ainsi, on a $y \in \gamma_b^{-1}(\Pi_i(X))$.

Reste le cas $i = m$. Soit $y \in \gamma_b^{-1}(\Pi_m(X))$ et considérons $x \in X$ tel que $\gamma_b(y) = \Pi_m(x)$. De cette égalité, on déduit $(y_2, \ldots, y_{m-1}, r.y_1 + b) = (x_1, \ldots, x_{m-1})$. Notons $b'$ le reste de la division euclidienne de $x_m$ par $r$. Ainsi, $(y_1, \ldots, y_{m-1}) = (\frac{x_{m-1} - b}{r}, x_1, \ldots, x_{m-2}) = \Pi_1(\frac{x_m - b'}{r}, \frac{x_{m-1} - b}{r}, x_1, \ldots, x_{m-2}) = \Pi_1(\gamma_{bb'}^{-1}(x))$. On a donc $y \in \bigcup_{b' \in \Sigma_r} \Pi_1(\gamma_{bb'}^{-1}(X))$. Réciproquement, considérons $y \in \bigcup_{b' \in \Sigma_r} \Pi_1(\gamma_{bb'}^{-1}(X))$. Il existe alors $b' \in \Sigma_r$ tel que $y \in \Pi_1(\gamma_{bb'}^{-1}(X))$. Considérons $x \in \gamma_{bb'}^{-1}(X)$ tel que $y = \Pi_1(x) = (x_2, \ldots, x_m)$. On a $\gamma_b(y) = (x_3, \ldots, x_m, r.x_2 + b) = \Pi_m(x_3, \ldots, r.x_2 + b, r.x_1 + b') = \Pi_m(\gamma_{bb'}(x))$. De $\gamma_{bb'}(x) \in X$, on déduit $y \in \gamma_b^{-1}(X)$. □

On obtient alors le résultat cherché.

**Proposition 5.11 ([BC96],[WB00])**
*Pour tout automate binaire non ambigu $\mathcal{A}$ à $n$ états représentant une partie $X \subseteq \mathbb{N}^m$ et pour tout $i \in \{1, \ldots, m\}$, il existe un automate binaire non ambigu $\mathcal{A}'$ à $m.2^n$ états représentant $\Pi_i(X)$. De plus, un tel automate est calculable en temps exponentiel.*

*Démonstration :*
On redonne la preuve de cette proposition en utilisant les notions de cette thèse. Pour la borne $m.2^n$, notons $Q(X)$ l'ensemble des résidus de $X$. La proposition 5.10 montre que

les résidus de $\Pi_i(X)$ sont de la forme $\bigcup_{X' \in Q'} \Pi_{i'}(X')$ où $Q' \subseteq Q(X)$ et $i' \in \{1, \ldots, m\}$. Le cardinal de l'ensemble des résidus de $\Pi_i(X)$ est donc borné par $m.2^n$. Pour construire effectivement un tel automate, il suffit d'appliquer un des algorithmes d'élimination des quantificateurs [BC96],[WB00]. □

Pour construire l'automate binaire canonique représentant l'ensemble des vecteurs de $\mathbb{N}^m$ satisfaisant une formule de Presburger $\phi$, il suffit alors d'appliquer $k$ fois la proposition 5.11 où $k$ est le nombre de quantificateurs de $\phi$.

#### 5.1.2.2 Borne élémentaire

Pour montrer que la complexité d'un tel algorithme est élémentaire, on étudie la taille des automates binaires non ambigus représentants les solutions des formules de Presburger produites par un algorithme d'élimination des quantificateurs. Un tel algorithme produit en effet des formules non-quantifiées de la forme $\langle \alpha, x \rangle = c$ mais aussi des formules de la forme $\langle \alpha, x \rangle \leqslant c$ et de la forme $\langle \alpha, x \rangle = c[k]$.

Dans [BB02] il est montré qu'il existe un automate binaire non ambigu représentant $\langle \alpha, x \rangle = c[k]$ dont la taille est en $O(m.(||\alpha||_1 + |c|).k)$. En fait, on peut montrer une borne bien plus fine comme le montre le lemme suivant.

**Lemme 5.12**
*Pour tout vecteur $\alpha \in \mathbb{Z}^m$, pour tout $c \in \mathbb{Z}$ et pour tout $k \in \mathbb{N}^*$, la partie $\{x \in \mathbb{N}^m;\ \langle \alpha, x \rangle = c[k]\}$ de $\mathbb{N}^m$ est représentable par un automate binaire non ambigu dont le nombre d'états est borné par $(1 + 2.m.k)$. De plus, un tel automate est calculable en temps $O(r.m.k)$.*

*Démonstration :*
Définissons la suite $(k_j)_{j \geqslant 0}$ de $\mathbb{N}^*$ par la formule de récurrence $k_0 = k$ et $k_{j+1} = \frac{k_j}{\text{pgcd}(k_j, r)}$ pour $j \geqslant 0$ où $\text{pgcd}(k_j, r) \in \mathbb{N}^*$. On va montrer que l'ensemble des résidus de $\{x \in \mathbb{N}^m;\ \langle \alpha, x \rangle = c[k]\}$ est inclus dans la classe $\mathcal{C}\{\emptyset\} \bigcup_{j \geqslant 0} \mathcal{C}_j$ où $\mathcal{C}_j$ est la classe des parties de $\mathbb{N}^m$ définie par

$$\mathcal{C}_j = \{\{x \in \mathbb{N}^m;\ \left\langle \alpha, \gamma_0^i(x) \right\rangle = c_0[k_j]\};\ 0 \leqslant i < m;\ 0 \leqslant c_0 < k_j\}$$

Comme $\{x \in \mathbb{N}^m;\ \langle \alpha, x \rangle = c[k]\}$ est dans $\mathcal{C}_0$, il suffit de montrer que la classe $\mathcal{C}$ est stable par résidu. Considérons donc $X \in \mathcal{C}$ et $b \in \Sigma_r$ et montrons que $\gamma_b^{-1}(X) \in \mathcal{C}$. Remarquons que si $X = \emptyset$ alors $\gamma_b^{-1}(X) \in \mathcal{C}$. On peut donc supposer que $X \neq \emptyset$. Donc ce cas, il existe $i \in \{0, \ldots, m-1\}$, $j \geqslant 0$ et $c_0 \in \{0, \ldots, k_j - 1\}$ tels que $X = \{x \in \mathbb{N}^m;\ \left\langle \alpha, \gamma_0^i(x) \right\rangle = c_0[k_j]\}$. On a $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ \left\langle \alpha, \gamma_0^i(\gamma_b(x)) \right\rangle = c_0[k_j]\}$. De $\gamma_b(x) = \gamma_0(x) + b.e_m$, on déduit $\gamma_0^i(\gamma_b(x)) = \gamma_0^{i+1}(x) + b.\gamma_0^i(e_m)$. Notons $c'_0 = c_0 - \left\langle \alpha, \gamma_0^i(e_m) \right\rangle [k_j]$. On a alors $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ \left\langle \alpha, \gamma_0^{i+1}(x) \right\rangle = c'_0[k_j]\}$. Remarquons que si $i \neq m-1$ alors $\gamma_b^{-1}(X) \in \mathcal{C}_i$. On peut donc supposer que $i = m-1$. Or $\gamma_0^m(x) = r.x$, donc $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ r.\langle \alpha, x \rangle = c'_0[k_j]\}$. On peut supposer que $c'_0$ est divisible par $\text{pgcd}(k_j, r)$ car autrement $\gamma_b^{-1}(X) = \emptyset$. On note $r' = \frac{r}{\text{pgcd}(k_j, r)}$ et $c''_0 = \frac{c'_0}{\text{pgcd}(k_j, r)}$. On a alors $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ r'.\langle \alpha, x \rangle = c''_0[k_{j+1}]\}$. Comme $r'$ et $k_{j+1}$ sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $r'.u + k_{j+1}.v = 1$ (on obtient deux tels entiers en utilisant l'algorithme d'Euclide). Notons $c'''_0 = u.c''_0[k_{j+1}]$ et remarquons que $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ \langle \alpha, x \rangle = c'''_0[k_{j+1}]\}$. On a donc $\gamma_b^{-1}(X) \in \mathcal{C}$.

Il suffit alors de majorer le cardinal de $\mathcal{C}$. La suite $(k_j)_{j\geqslant 0}$ étant décroissante dans $\mathbb{N}^*$, elle est stationnaire. Notons $j_0 \geqslant 0$ le premier indice tel que $k_{j_0+1} = k_{j_0}$. On a alors $k_j = k_{j_0}$ pour tout $j \geqslant j_0$. Montrons que pour tout $j \in \{0, \dots, j_0-1\}$, on a $k_{j+1} \leqslant \frac{1}{2}k_j$. Par définition de $j_0$, on a $k_{j+1} \neq k_j$. Ainsi, $\text{pgcd}(k_j, r) \geqslant 2$ et on a donc l'inégalité $k_{j+1} \leqslant \frac{1}{2}k_j$. Cela montre en particulier que $\text{card}(\mathcal{C}) \leqslant 1 + m.(k_0 + \cdots + k_{j_0}) \leqslant 1 + m.k. \sum_{j=0}^{j_0} \frac{1}{2^j} \leqslant 1 + m.k. \sum_{j=0}^{\infty} \frac{1}{2^j} = 1 + 2.m.k$. On déduit $\text{card}(\mathcal{C}) \leqslant 1 + 2.m.k$. □

Une version légèrement modifiée de l'algorithme de construction de $\{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle = c\}$ proposé dans le lemme 5.4 nous permet de borner la taille de l'automate binaire canonique représentant $\{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle \leqslant c\}$.

**Lemme 5.13 ([WB00],[BC96],[BB02])**
*Il existe un algorithme de construction qui pour tout couple $(\alpha, c)$ construit un automate binaire non ambigu $\mathcal{A}$ représentant la partie $\{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle \leqslant c\}$ en temps linéaire en $O(\text{taille}(\alpha) + \text{taille}(c) + \text{taille}(\mathcal{A}))$ et dont le nombre d'états est borné par*

$$3.m.(||\alpha||_1 + 1).\frac{\ln\left(r + \frac{||c||_1+1}{||\alpha||_1+1}\right)}{\ln(r)}$$

On peut alors borner la taille de l'automate binaire canonique représentant l'ensemble des solutions d'une formule de Presburger.

**Théorème 5.14 ([WB00],[BB02])**
*Il existe une constante $c$ telle que pour toute formule de Presburger $\phi$, l'automate binaire canonique représentant $\phi$ a une taille bornée par*

$$2^{2^{2^{c.\text{taille}(\phi)}}}$$

Le théorème 5.14 montre en particulier que pour toute formule de Presburger $\phi$ et pour toute suite de quantificateurs $Q_1 \cdots Q_n$, l'automate binaire canonique $\mathcal{A}_{Q_1\cdots Q_m\ \phi}$ représentant $Q_1 \cdots Q_m\ \phi$ a une taille élémentaire en la taille de la formule $\phi$. Cependant, cela ne prouve pas que $\mathcal{A}_{Q_1\ \dots\ Q_m}\phi$ a une taille élémentaire en la taille de l'automate binaire canonique représentant $\phi$. Pour obtenir un tel résultat, il faudrait pouvoir "résoudre le problème ouvert 5.15" suivant.

**Problème ouvert 5.15**
*Soit $\mathcal{C}_P$ la classe des automates binaires canoniques représentant des parties définissables dans la logique de Presburger. Pour tout automate $\mathcal{A}$ dans $\mathcal{C}_P$, on note $l(\mathcal{A})$ la taille de la plus petite formule de Presburger dont l'ensemble des solutions est représenté par $\mathcal{A}$. La fonction $l(\mathcal{A})$ est-elle bornée de façon élémentaire en la taille de $\mathcal{A}$ ?*

Rappelons que dans [BHMV94] et [Muc03], il est prouvé que l'on peut décider si un automate binaire non ambigu $\mathcal{A}$ représente une partie définissable dans la logique de Presburger. La complexité de l'algorithme est 4-EXPTIME.

## 5.2 Les parties non-quantifiées de $\mathbb{N}^m$

Un point de départ pour résoudre le problèmes ouvert 5.15, est l'étude des automates binaires non ambigus représentant des parties non-quantifiées. Dans cette section, on montre que l'on peut décider en temps exponentiel si un automate binaire non ambigu représente une partie non-quantifiée. Ce résultat est nouveau, aussi bien d'un point de vue décidabilité que complexité.

Dans la sous-section 5.2.1 on introduit la classe des parties affines irréductibles permettant de décomposer une partie non-quantifiée en une union finie de parties non-quantifiées plus simples. Cette décomposition sera utilisée dans la sous-section 5.2.2 pour montrer que l'on peut calculer l'automate binaire représentant l'enveloppe semi-affine d'une partie $X$ en modifiant simplement les états finaux de tout automate binaire non ambigu représentant $X$. Enfin, dans la sous-section 5.2.3, on montre qu'en calculant la couverture semi-affine d'une partie $X$, on peut caractériser les parties non-quantifiées.

### 5.2.1 Les parties affines irréductibles de $\mathbb{N}^m$

On montre que l'on peut décomposer une partie non-quantifiée $X$ en une union finie de parties non-quantifiées de la forme $A\backslash S$ où $A$ est une partie affine et $S$ une partie semi-affine telles que $\mathrm{saff}_{\mathbb{N}^m}(A\backslash S) = A$. Remarquons que cette décomposition n'est pas triviale car il existe des parties affines $A$ et des parties semi-affines $S$ telles que $\mathrm{saff}(A\backslash S) \subsetneq A$ (prendre par exemple $A = \{(1,0),(0,1)\}$ et $S = \{(0,1)\}$).

Pour obtenir une telle décomposition, on caractérise dans la proposition suivante une classe de parties affines "irréductibles".

**Proposition 5.16**
*Considérons une partie affine $A$. Les deux propriétés suivantes sont équivalentes :*
- *Pour toute suite finie $(A_i)_{i\in I}$ de parties affines telle que $A \subseteq \bigcup_{i\in I} A_i$, il existe $i \in I$ tel que $A \subseteq A_i$.*
- *L'enveloppe semi-affine* $\mathrm{saff}(A)$ *est un espace affine.*

*Démonstration :*

Supposons que $\mathrm{saff}(A)$ soit un espace affine et considérons une suite finie $(A_i)_{i\in I}$ de parties affines de $\mathbb{N}^m$ telle que $A \subseteq \bigcup_{i\in I} A_i$. De $\mathrm{saff}(A) \subseteq \bigcup_{i\in I} \mathrm{saff}(A_i)$, on déduit en utilisant la proposition 3.16 qu'il existe $i \in I$ tel que $\mathrm{saff}(A) \subseteq \mathrm{saff}(A_i)$. En prenant l'intersection de cette inclusion avec $\mathbb{N}^m$, on déduit l'inclusion $A \subseteq A_i$. Réciproquement, supposons que pour toute suite finie $(A_i)_{i\in I}$ de parties affines de $\mathbb{N}^m$ telle que $A \subseteq \bigcup_{i\in I} A_i$, il existe $i \in I$ tel que $A \subseteq A_i$. Notons $S = \mathrm{saff}(A)$. De $S = \bigcup_{A'\in\mathrm{comp}(S)} A$, on déduit $A = S \cap \mathbb{N}^m = \bigcup_{A'\in\mathrm{comp}(S)} A' \cap \mathbb{N}^m$. Ainsi, par hypothèse, il existe $A' \in \mathrm{comp}(S)$ tel que $A \subseteq A' \cap \mathbb{N}^m$. On a alors $S = \mathrm{saff}(A) \subseteq A'$. De $A' \subseteq S$ on déduit alors $\mathrm{saff}(A) = A'$ qui est donc un espace affine. □

**Définition 5.17**
*Une partie affine $A$ est irréductible si* $\mathrm{saff}(A)$ *est un espace affine.*

Dans la proposition 5.18, on montre que toute partie affine se décompose en une union finie de parties affines irréductibles.

**Proposition 5.18**
*Toute partie affine peut se décomposer en une union finie de parties affines irréductibles.*

*Démonstration :*
Soient $X \subseteq \mathbb{N}^m$ une partie affine de $\mathbb{N}^m$ et $S$ le semi-affine de $\mathbb{Q}^m$ défini par $S = \mathrm{saff}(X)$. Considérons une composante affine $A$ de $S$. On va montrer que $A \cap \mathbb{N}^m$ est une partie affine irréductible de $\mathbb{N}^m$. La proposition 3.17 montre que $\bigcup_{A' \in \mathrm{comp}(S)} A' = S$. Ainsi de $S = \mathrm{saff}(S \cap \mathbb{N}^m)$, on déduit $S = \mathrm{saff}(\bigcup_{A' \in \mathrm{comp}(S)} A' \cap \mathbb{N}^m) = \bigcup_{A' \in \mathrm{comp}(S)} \mathrm{saff}(A' \cap \mathbb{N}^m)$. Comme $A$ est un espace affine inclus dans $S$, la proposition 3.16 montre qu'il existe un espace affine $A' \in \mathrm{comp}(S)$ tel que $A \subseteq \mathrm{saff}(A' \cap \mathbb{N}^m)$. De $A \subseteq A' \subseteq S$ et $A \in \mathrm{comp}(S)$, on déduit $A = A'$. On a donc $A \subseteq \mathrm{saff}(A \cap \mathbb{N}^m)$. Puisque $\mathrm{saff}(A \cap \mathbb{N}^m) \subseteq A$, $\mathrm{saff}(A \cap \mathbb{N}^m) = A$ est un espace affine. La partie $A \cap \mathbb{N}^m$ est donc une partie affine irréductible de $\mathbb{N}^m$. Pour prouver la proposition, il suffit alors de remarquer que $X = \bigcup_{A \in \mathrm{comp}(S)} (A \cap \mathbb{N}^m)$. □

Les parties affines irréductibles vérifient bien la propriété recherchée.

**Proposition 5.19**
*Pour toute partie affine irréductible $A$ et pour toute partie semi-affine $S$ telles que $A \not\subseteq S$, on a :*

$$\mathrm{saff}_{\mathbb{N}^m}(A \backslash S) = A$$

*Démonstration :*
De $A = (A \backslash S) \cup (A \cap S)$, on déduit $\mathrm{saff}(A) = \mathrm{saff}(A \backslash S) \cup \mathrm{saff}(A \cap S)$. Comme $\mathrm{saff}(A)$ est un espace affine de $\mathbb{Q}^m$, la proposition 3.16, montre que soit $\mathrm{saff}(A) \subseteq \mathrm{saff}(A \backslash S)$, soit $\mathrm{saff}(A) \subseteq \mathrm{saff}(A \cap S)$. Remarquons que si $\mathrm{saff}(A) \subseteq \mathrm{saff}(A \cap S)$, alors $\mathrm{saff}(A) \subseteq \mathrm{saff}(S)$. On a alors $A = \mathrm{saff}_{\mathbb{N}^m}(A) \subseteq \mathrm{saff}_{\mathbb{N}^m}(S) = S$ ce qui est absurde. Ainsi, on a montré que $\mathrm{saff}(A) \subseteq \mathrm{saff}(A \backslash S)$. On déduit de $\mathrm{saff}(A \backslash S) \subseteq \mathrm{saff}_{\mathbb{Q}_m}(A)$ que $\mathrm{saff}(A \backslash S) = \mathrm{saff}(A)$. D'où $\mathrm{saff}_{\mathbb{N}^m}(A \backslash S) = A$. □

On obtient alors la décomposition recherchée des parties non-quantifiées.

**Proposition 5.20**
*Toute partie non-quantifiée peut se décomposer en une union finie de parties non-quantifiées de la forme $A \backslash S$ où $A$ est une partie affine irréductible et $S$ une partie semi-affine vérifiant $A \not\subseteq S$.*

*Démonstration :*
Il existe une suite $(A_i)_{1 \leqslant i \leqslant n}$ de parties affines de $\mathbb{N}^m$ et une suite $(S_i)_{1 \leqslant i \leqslant n}$ de parties semi-affines de $\mathbb{N}^m$ telles que $X = \bigcup_{1 \leqslant i \leqslant n} A_i \backslash S_i$. La proposition 5.18 montre que chaque $A_i$ peut se décomposer en une union finie de parties affines irréductibles de $\mathbb{N}^m$. On peut donc supposer que les parties affines $A_i$ sont irréductibles. Remarquons enfin que si $A_i \subseteq S_i$ alors $A_i \backslash S_i = \emptyset$. On peut donc aussi supposer que $A_i \not\subseteq S_i$. □

### 5.2.2 Couverture d'un automate binaire non-quantifié

On montre dans cette sous-section qu'en modifiant simplement l'ensemble des états finaux d'un automate binaire non ambigu représentant une partie $X$ non-quantifiée, on obtient une représentation de $\mathrm{saff}_{\mathbb{N}^m}(X)$.

**Définition 5.21**
*Pour tout automate binaire non ambigu $\mathcal{A}$, on note $\mathcal{A}_0$ l'automate binaire obtenu à partie de $\mathcal{A}$ en remplaçant l'ensemble de ces états finaux par $F_0 = \{q \in Q;\ \overrightarrow{0} \in \mathrm{cov}(\mathcal{A})_q\}$ où $\mathrm{cov}(\mathcal{A})$ est la couverture semi-affine de $\mathcal{A}$.*

Dans le cas général où aucune hypothèse n'est faite sur la partie $X$ représenté par l'automate binaire non ambigu $\mathcal{A}$, la proposition 5.22 montre que la partie représentée par l'automate $\mathcal{A}_0$ est incluse dans $\mathrm{saff}_{\mathbb{N}^m}(X)$.

**Proposition 5.22**
*Pour toute partie $X$ représentée par un automate binaire non ambigu $\mathcal{A}$, on a :*

$$\mathcal{L}(\mathcal{A}_0)) \subseteq \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$$

*Démonstration :*
Considérons un mot $\sigma \in \mathcal{L}(\mathcal{A}_0)$ et montrons que $\sigma \in \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$. On note $q_0 \xrightarrow{\sigma} q$ un chemin acceptant $\sigma$ dans $\mathcal{A}_0$. Par définition de $\mathcal{A}_0$, on a $\overrightarrow{0} \in \mathrm{cov}(\mathcal{A})_q$. Comme $\mathrm{cov}(\mathcal{A})$ est une couverture, on a donc $\mathrm{cov}(\mathcal{A})_q \subseteq \gamma_\sigma^{-1}(\mathrm{cov}(\mathcal{A})_{q_0})$. Ainsi, $\rho_m(\sigma) \in \mathrm{cov}(\mathcal{A})_{q_0}$. Les lemmes 4.53 et 4.58 montrent que $\mathrm{cov}(\mathcal{A})_{q_0} = \mathrm{saff}_{\mathbb{N}^m}(\rho_m(\mathcal{L}(\mathcal{A}_{q_0}))) = \mathrm{saff}_{\mathbb{N}^m}(X)$. On a ainsi prouvé que $\sigma \in \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$. □

Comme le montre le lemme 5.23, on n'a pas l'égalité en général.

**Lemme 5.23**
*Il existe un automate binaire non ambigu $\mathcal{A}$ représentant une partie $X \subseteq \mathbb{N}^m$ tel que $\mathcal{L}(\mathcal{A}_0) \neq \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$.*

*Démonstration :*
On se place dans le cas $m = 1$ et $r = 2$ et considère la partie $X = \{2^i;\ i \geqslant 0\}$. Étudions les résidus de $X$. On a $\gamma_0^{-1}(X) = X$, $\gamma_1^{-1}(X) = \{0\}$. De plus $\gamma_0^{-1}(\{0\}) = 0$ et $\gamma_1^{-1}(\{0\}) = \emptyset$. Ainsi, l'ensemble $Q(X)$ des états de l'automate $\mathcal{A}(X)$ est égal à $Q(X) = \{X, \{0\}, \emptyset\}$. Les lemmes 4.53 et 4.58 montrent que pour tout $q \in Q(X)$, on a $\mathrm{cov}(\mathcal{A}(X))_q = \mathrm{saff}_{\mathbb{N}^m}(q)$. Ainsi, de $\mathrm{saff}_{\mathbb{N}^m}(X) = \mathbb{Q}$, $\mathrm{saff}_{\mathbb{N}^m}(\{0\}) = \{0\}$ et $\mathrm{saff}_{\mathbb{N}^m}(\emptyset) = \emptyset$, on déduit $\mathcal{L}(\mathcal{A}_0) = \{0\} \cup X \neq \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X)) = \mathbb{Q}$. □

Cependant, on va montrer que si l'automate binaire $\mathcal{A}$ représente une partie non-quantifiée $X$, alors $\mathcal{A}_0$ est un automate binaire non ambigu représentant $\mathrm{saff}_{\mathbb{N}^m}(X)$. Pour cela, on commence par montrer que la classe des parties non-quantifiées est stable par résidu et que les fonctions $\gamma_b^{-1}$ et $\mathrm{saff}_{\mathbb{N}^m}$ commutent pour toute partie non-quantifiée $X$.

**Proposition 5.24**
*La classe des parties non-quantifiées de $\mathbb{N}^m$ est stable par résidu.*

*Démonstration :*
D'après la proposition 5.20, il suffit de montrer que le résidu d'une partie $X = A \backslash S$ où $A$ est une partie affine de $\mathbb{N}^m$ et $S$ est une partie semi-affine de $\mathbb{N}^m$, est non-quantifié. Or le résidu de $X$ par un mot $\sigma$ est égal à $\gamma_\sigma^{-1}(X) = \gamma_\sigma^{-1}(A) \backslash \gamma_\sigma^{-1}(S)$. Comme la classe des parties semi-affines est stable par résidu, la partie $\gamma_\sigma^{-1}(X)$ est non-quantifiée. □

**Proposition 5.25**
*Pour toute partie non-quantifiée $X \subseteq \mathbb{N}^m$ et pour tout $b \in \Sigma_r$, on a :*

$$\gamma_b^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X)) = \mathrm{saff}_{\mathbb{N}^m}(\gamma_b^{-1}(X))$$

*Démonstration :*
La proposition 5.20 montre qu'il suffit de prouver la proposition pour $X = A \backslash S$ où $A$ est une partie affine irréductible de $\mathbb{N}^m$ et $S$ une partie semi-affine de $\mathbb{N}^m$ telles que $A \not\subseteq S$. Remarquons que $\gamma_b^{-1}(X) = \gamma_b^{-1}(A) \backslash \gamma_b^{-1}(S)$.

Montrons que $\gamma_b^{-1}(A)$ est irréductible et que $\gamma_b^{-1}(A) \not\subseteq \gamma_b^{-1}(S)$. Le lemme 3.13 appliqué à la fonction affine $\lambda_b^{-1}$, montre que $\mathrm{saff}(\gamma_b^{-1}(A)) = \lambda_b(\mathrm{saff}(A))$ et $\mathrm{saff}(\gamma_b^{-1}(S)) = \lambda_b^{-1}(\mathrm{saff}(S))$. En particulier, cela prouve que $\gamma_b^{-1}(A)$ est irréductible. Supposons par l'absurde que $\gamma_b^{-1}(A) \subseteq \gamma_b^{-1}(S)$. En prenant l'enveloppe semi-affine de cette inclusion, on obtient $\mathrm{saff}(\gamma_b^{-1}(A)) \subseteq \mathrm{saff}(\gamma_b^{-1}(S))$. Ainsi, on $\lambda_b^{-1}(\mathrm{saff}(A)) \subseteq \lambda_b^{-1}(\mathrm{saff}(S))$. Comme $\lambda_b$ est surjective, on a alors $\mathrm{saff}(A) \subseteq \mathrm{saff}(S)$. D'où $A \subseteq S$. On obtient alors une contradiction. Cela prouve que $\gamma_b^{-1}(A) \not\subseteq \gamma_b^{-1}(S)$.

Le lemme 5.19 montre alors que $\mathrm{saff}_{\mathbb{N}^m}(X) = A$ et $\mathrm{saff}_{\mathbb{N}^m}(\gamma_b^{-1}(X)) = \gamma_b^{-1}(A)$. De ces deux égalités, on déduit $\gamma_b^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X)) = \mathrm{saff}_{\mathbb{N}^m}(\gamma_b^{-1}(X))$. □

On peut alors démontrer l'inclusion manquante.

**Proposition 5.26**
*Pour toute partie non-quantifiée $X \subseteq \mathbb{N}^m$ représentée par un automate binaire non ambigu $\mathcal{A}$, on a :*

$$\mathcal{L}(\mathcal{A}_0)) \supseteq \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$$

*Démonstration :*
Considérons un mot $\sigma \in \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$ et montrons que $\sigma \in \mathcal{L}(\mathcal{A}_0)$. De $\gamma_\sigma(\overrightarrow{0}) \in \mathrm{saff}_{\mathbb{N}^m}(X)$ on déduit $\overrightarrow{0} \in \gamma_\sigma^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X))$. La proposition 5.25 prouve alors que $\overrightarrow{0} \in \mathrm{saff}_{\mathbb{N}^m}(\gamma_\sigma^{-1}(X))$. Comme l'automate $\mathcal{A}$ est complet, il existe un chemin $q_0 \xrightarrow{\sigma} q$ dans $\mathcal{A}$. Comme de plus l'automate $\mathcal{A}$ est déterministe, on a $\sigma^{-1}.\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}_q)$. La proposition 4.35 prouve que $\gamma_\sigma^{-1}(X) = \rho_m(\sigma^{-1}.\mathcal{L}(\mathcal{A}))$. Ainsi, on a $\overrightarrow{0} \in \mathrm{saff}_{\mathbb{N}^m}(\rho_m(\mathcal{L}(\mathcal{A})_q))$. Des lemmes 4.53 et 4.58, on déduit $\mathrm{saff}_{\mathbb{N}^m}(\rho_m(\mathcal{L}(\mathcal{A})_q)) = \mathrm{cov}(\mathcal{A})_q$. On a ainsi prouvé que $\sigma \in \mathcal{L}(\mathcal{A}')$. □

En appliquant les propositions 5.22 et 5.26, on montre alors que $\mathcal{A}_0$ est bien l'automate correspondant à l'enveloppe semi-affine.

**Théorème 5.27**
*Soit $\mathcal{A}$ un automate binaire non ambigu représentant une partie $X \subseteq \mathbb{N}^m$ non-quantifiée. L'automate $\mathcal{A}_0$ est un automate binaire non ambigu représentant* $\mathrm{saff}_{\mathbb{N}^m}(X)$.

Pour construire l'automate $\mathcal{A}_0$, il suffit de savoir décider l'appartenance $\overrightarrow{0} \in \mathrm{cov}(\mathcal{A})_q$. En modifiant l'algorithme de construction de la couverture semi-affine en algorithme de decison, on prouve que l'on peut décider ce problème en temps NP.

**Problème ouvert 5.28**
*Trouver la complexité du problème de decision $\overrightarrow{0} \in \mathrm{cov}(\mathcal{A})_q$ pour un état $q$ d'un automate binaire canonique $\mathcal{A}$.*

### 5.2.3 Caractérisation des parties non-quantifiées

Dans cette sous-section, on caractérise algorithmiquement les automates binaires non ambigus représentant des parties non-quantifiées. En remarquant que $X$ est une partie non-quantifiée si et seulement si la différence entre l'enveloppe semi-affine $\mathrm{saff}_{\mathbb{N}^m}(X)$ et $X$ est une partie non-quantifiée, on déduit une caractérisation des parties non-quantifiées par sur-approximation de plus en plus fine. En itérant cette technique à la limite, on introduit la notion de noyau d'une partie $X$ et on montre que ce noyau est vide si et seulement si $X$ est non-quantifiée.

**Définition 5.29**
*Pour toute partie $X \subseteq \mathbb{N}^m$, on note $\delta(X) = \mathrm{saff}_{\mathbb{N}^m}(X) \backslash X$.*

Comme la suite de parties semi-affines $(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X))_{i \geqslant 0})$ est décroissante, elle devient alors stationnaire. Le semi-affine que l'on obtient à la limite est appelé le noyau.

**Définition 5.30**
*Le noyau d'une partie $X$ de $\mathbb{N}^m$ est le semi-affine noté* $\ker(X)$ *et défini par :*

$$\ker(X) = \bigcap_{i \geqslant 0} \mathrm{saff}_{\mathbb{N}^m}(\delta^i(X))$$

#### 5.2.3.1 Critère algébrique

On montre que le noyau d'une partie $X$ est vide si et seulement si $X$ est non-quantifié.

**Lemme 5.31**
*Pour toute partie $X \subseteq \mathbb{N}^m$, il existe un entier $i_0 \geqslant 0$ tel que* $\ker(X) = \mathrm{saff}_{\mathbb{N}^m}(\delta^{i_0}(X))$.

*Démonstration :*
Remarquons que pour toute partie $X \subseteq \mathbb{N}^m$, la proposition 3.6 prouve l'existence d'un entier $i_0 \geqslant 0$ tel que $\ker(X) = \bigcap_{0 \leqslant i \leqslant i_0} \mathrm{saff}_{\mathbb{N}^m}(\delta^i(X))$. Comme la suite $(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X)))_{i \geqslant 0}$ est une suite décroissante, on a bien $\ker(X) = \mathrm{saff}_{\mathbb{N}^m}(\delta^{i_0}(X))$. □

**Proposition 5.32**
*Pour toute partie $X \subseteq \mathbb{N}^m$, on a :*

*$X$ est non ambigu si et seulement si $\delta(X)$ est non ambigu.*

*Démonstration :*
Remarquons que si $X$ est non ambigu alors $\delta(X) = \mathrm{saff}_{\mathbb{N}^m}(X) \backslash X$ est non ambigu. Réciproquement, supposons $\delta(X)$ non ambigu. Comme $X = \mathrm{saff}_{\mathbb{N}^m}(X) \backslash \delta(X)$, la partie $X$ est non ambigue. □

Pour montrer que les composantes affines de $\mathrm{saff}(\delta(X))$ sont strictement incluses dans les composantes affines de $\mathrm{saff}(X)$, on prouve le lemme 5.33 suivant.

**Lemme 5.33**
*Soit $X \subseteq \mathbb{N}^m$ une partie non-quantifiée. On a alors*

$$\mathrm{comp}(\mathrm{saff}(X)) \cap \mathrm{comp}(\mathrm{saff}(\delta(X))) = \emptyset$$

*Démonstration :*
La proposition 5.20 prouve qu'il existe une suite $(A_i)_{1 \leqslant i \leqslant n}$ de parties affines irréductibles de $\mathbb{N}^m$ et une suite $(S_i)_{1 \leqslant i \leqslant n}$ de parties semi-affines de $\mathbb{N}^m$ vérifiant $A_i \not\subseteq S_i$ et telles que $X = \bigcup_{1 \leqslant i \leqslant n} A_i \backslash S_i$. Le lemme 5.19 montre alors que $\mathrm{saff}_{\mathbb{N}^m}(X) = \bigcup_{1 \leqslant i \leqslant n} A_i$. On a donc :

$$\begin{aligned}
\delta(X) &= \left( \bigcup_{1 \leqslant i \leqslant n} A_i \right) \backslash \left( \bigcup_{1 \leqslant j \leqslant n} A_j \backslash S_j \right) \\
&= \bigcup_{1 \leqslant i \leqslant n} \bigcap_{1 \leqslant j \leqslant n} ((A_i \backslash A_j) \cup (A_i \cap S_j)) \\
&= \bigcup_{1 \leqslant i \leqslant n} \bigcup_{J \subseteq \{1, \dots, n\}} \left( \bigcap_{j \in J} (A_i \backslash A_j) \bigcap_{j \notin J} (A_i \cap S_j) \right)
\end{aligned}$$

Supposons par l'absurde l'existence d'un espace affine $A$ dans $\mathrm{comp}(\mathrm{saff}(X))$ et dans $\mathrm{comp}(\mathrm{saff}(\delta(X)))$. Comme $A \subseteq \mathrm{saff}(X)$, le lemme 3.16 montre qu'il existe un entier $i \in \{1, \dots, n\}$ tel que $A \subseteq \mathrm{saff}(A_i)$. Comme $A$ est une composante, on a alors l'égalité $A = \mathrm{saff}(A_i)$. De plus, comme $A \subseteq \mathrm{saff}(\delta(X))$, le lemme 3.16 montre qu'il existe un entier $i' \in \{1, \dots, m\}$ et une partie $J \subseteq \{1, \dots, n\}$ tels que $A \subseteq \mathrm{saff}_{\mathbb{N}^m}(\bigcap_{j \in J} (A_{i'} \backslash A_j) \bigcap_{j \notin J} (A_{i'} \cap S_j))$. On a alors $A \subseteq A_{i'}$. Comme $A$ est une composante, on a l'égalité $A = A_{i'}$. On sépare la preuve en deux cas : $i \in J$ et $i \notin J$. Considérons le cas $i \in J$. On a alors $A \subseteq \mathrm{saff}_{\mathbb{N}^m}(A_{i'} \backslash A_i) = \emptyset$. Comme $A$ est non vide on a donc une contradiction. Considérons enfin le cas $i \notin J$. On a alors $A_i = A \subseteq S_i$ et on a une contradiction. □

On prouve alors la caractérisation suivante des parties non-quantifiée.

**Théorème 5.34**
*Une partie est non-quantifiée si et seulement si son noyau est vide.*

*Démonstration :*

Considérons une partie $X \subseteq \mathbb{N}^m$. Supposons que $\ker(X) = \emptyset$ et montrons que $X$ est non-quantifié. Le lemme 5.31 prouve qu'il existe $i_0 \geqslant 0$ tel que $\ker(X) = \mathrm{saff}_{\mathbb{N}^m}(\delta^{i_0}(X))$. On a ainsi $\delta^{i_0}(X) = \emptyset$. Comme $\emptyset$ est non-quantifié, la proposition 5.32 montre alors que $X$ est non-quantifiée. Réciproquement, supposons $X$ non-quantifiée et montrons que $\ker(X) = \emptyset$. D'après le lemme 5.31, il existe un entier $i_0 \geqslant 0$ tel que $\ker(X) = \mathrm{saff}_{\mathbb{N}^m}(\delta^{i_0}(X))$. Considérons $Y = \delta^{i_0}(X)$. Le lemme 5.32 montre que $Y$ est non-quantifiée. De plus, on a $\mathrm{saff}_{\mathbb{N}^m}(Y) = \ker(X) \subseteq \mathrm{saff}_{\mathbb{N}^m}(\delta(Y)) \subseteq \mathrm{saff}_{\mathbb{N}^m}(Y)$. On a donc $\mathrm{saff}_{\mathbb{N}^m}(Y) = \mathrm{saff}_{\mathbb{N}^m}(\delta(Y))$. Le lemme 5.33 montre alors que $Y = \emptyset$. Ainsi, on a $\ker(X) = \emptyset$. □

#### 5.2.3.2 Critère algorithmique

Pour montrer que l'on peut décider un temps exponentiel si un automate binaire non ambigu représente une partie non-quantifiée, on commence par montrer que le noyau d'une partie $X$ est vide si et seulement si $\delta^{m+1}(X)$ est vide. Il suffit ainsi de calculer l'automate binaire non ambigu représentant $\delta^{m+1}(X)$ pour savoir si $X$ est non-quantifié.

**Proposition 5.35**
*Pour toute partie $X \subseteq \mathbb{N}^m$, on a $\ker(X) = \emptyset$ si et seulement si $\delta^{m+1}(X) = \emptyset$.*

*Démonstration :*

Remarquons que si $\delta^{m+1}(X) = \emptyset$ alors $\ker(X) = \emptyset$. Il suffit donc de montrer que si $\ker(X) = \emptyset$ alors $\delta^{m+1}(X) = \emptyset$. Le théorème 5.34 prouve que $X$ est non-quantifié. Montrons par récurrence que la dimension des composantes de $\mathrm{saff}(\delta^i(X))$ est bornée par $m-i$ pour $i \leqslant m+1$. Pour $i = 0$ la récurrence est immédiate. Supposons donc l'hypothèse de récurrence vraie pour $i \leqslant m$ et considérons une composante $A$ de $\mathrm{saff}(\delta^{i+1}(X))$. Comme $\mathrm{saff}(\delta^{i+1}(X)) \subseteq \mathrm{saff}(\delta^i(X))$, la proposition 3.16 prouve qu'il existe une composante $A'$ de $\mathrm{saff}(\delta^i(X))$ telle que $A \subseteq A'$. Le lemme 5.33 montre que $A \neq A'$. Ainsi, $\dim(A) < \dim(A')$. Or par hypothèse de récurrence, on a $\dim(A') \leqslant m - i$. On a donc prouvé la récurrence. En particulier, on a prouvé que $\delta^{m+1}(X) = \emptyset$. □

Pour construire un automate binaire non ambigu représentant $\delta(X)$ étant donné un automate binaire non ambigu $\mathcal{A}$ représentant $X$, l'idée est de considérer l'automate binaire non ambigu $\mathcal{A}_0$ défini dans la sous-section précédente et de montrer que cet automate représente bien une partie semi-affine. En effet, si ce n'est pas le cas, le théorème 5.27 prouve que $X$ n'est pas non-quantifié. Pour réaliser ce teste, on utilisera la proposition 5.36 suivante.

**Proposition 5.36**
*Pour toute partie affine de $X$ de $\mathbb{N}^m$ représentée par un espace affine $A$ de $\mathbb{Q}^m$, on peut construire en temps polynomial une formule non-quantifiée $\phi_X$ représentant $X$.*

*Démonstration :*

Notons $\rho(A) = (a, M)$ la représentation canonique de l'espace affine $A$. Rappelons que $\Pi_A(x) = M.x + a$ est la projection orthogonale sur $A$. Ainsi, $x \in A$ si et seulement si

**Algorithme 2** Décide si un UBA $\mathcal{A}$ représente une partie non-quantifiée.

**entrée :** Un automate binaire non ambigu $\mathcal{A} = (Q, \Sigma_r, \Delta, \{q_0\}, F)$.
**sortie :** "non-quantifié" si $\rho_m(\mathcal{L}(\mathcal{A}))$ est non-quantifiée et "quantifié" sinon.

$i \leftarrow 0$
**repéter**
  **si** $(i = m + 1)$ **alors**
    **si** $\mathcal{L}(\mathcal{A}) \neq \emptyset$ **alors**
      **renvoyer** "quantifié"
    **sinon**
      **renvoyer** "non-quantifié"
  Soit $\text{cov}(\mathcal{A})$ la couverture semi-affine de $\mathcal{A}$
  $F_0 \leftarrow \{q \in Q;\ \overrightarrow{0} \in \text{cov}(\mathcal{A})_q\}$
  $\mathcal{A}_0 \leftarrow (Q, \Sigma_r, \Delta, \{q_0\}, F_0)$
  Soit $\mathcal{C}$ l'ensemble des composantes de $\text{saff}(\rho_m(\mathcal{L}(\mathcal{A})))$.
  **pour** chaque espace affine $A \in \mathcal{C}$ **faire**
    Soit $\mathcal{A}_A$ l'automate binaire canonique représentant $A \cap \mathbb{N}^m$
    **si** $\mathcal{L}(\mathcal{A}_A) \not\subseteq \mathcal{L}(\mathcal{A}_0)$ **alors**
      **renvoyer** "quantifié"
  $F \leftarrow F_0 \backslash F$
  $\mathcal{A} \leftarrow (Q, \Sigma_r, \Delta, \{q_0\}, F)$
  $i \leftarrow i + 1$
**jusqu'à** vrai

$\Pi_A(x) = x$. De $X = A \cap \mathbb{N}^m$, on déduit $X = \{x \in \mathbb{N}^m;\ M.x = x + (Ma - a)\}$. Ainsi, la formule non-quantifiée $\phi_X$ suivante représente $X$.

$$\phi_X(x) := \bigwedge_{j=1}^{m} (\sum_{i=1}^{m} M_{ji}.x_i = x_j + (M.a - a)_j)$$

□

On peut alors caractériser les automates binaires non ambigus représentant des parties non-quantifiées.

**Théorème 5.37**
*On sait décider en temps exponentiel, si une partie $X \subseteq \mathbb{N}^m$, représentée par un automate binaire non ambigu, est non-quantifiée.*

*Démonstration :*
On note $X$ la partie représentée par l'automate binaire non ambigu $\mathcal{A}$ à la ligne 1. On note $\mathcal{A}^i$ l'automate binaire $\mathcal{A}$ à la ligne 6 en fonction de la variable $i \in \mathbb{N}$. De même, on note $\mathcal{A}_0^i$ l'automate binaire $\mathcal{A}_0$ à la ligne 14.

Commençons par montrer la complexité exponentielle de l'algorithme. Le corollaire 4.80 montre que la couverture semi-affine $\mathrm{cov}(\mathcal{A})$ est calculable en temps exponentiel. Remarquons de plus que l'ensemble $\mathcal{C}$ des composantes de $\mathrm{saff}(X)$ est calculable en temps exponentiel par le théorème 4.79 et que chaque composante $A \in \mathcal{C}$ a une taille polynomiale. Ainsi, en temps exponentiel on peut donc calculer par la proposition 5.36 et le théorème 5.8 pour chaque $A \in \mathcal{C}$, l'automate binaire canonique $\mathcal{A}_A$ représentant $A \cap \mathbb{N}^m$. On peut ainsi tester en temps quadratique l'inclusion $\mathcal{L}(\mathcal{A}_A) \subseteq \mathcal{L}(\mathcal{A}_0)$. On a donc prouvé que l'algorithme terminait en temps exponentiel.

Montrons par récurrence que pour tout $i \in \mathbb{N}$, on a $\mathcal{L}(\mathcal{A}^i) = \rho_m^{-1}(\delta^i(X))$. Pour $i = 0$, la propriété est vérifiée. Supposons donc la propriété vérifiée pour un $i \in\geqslant 0$ et montrons que si l'algorithme arrive à incrémenter la variable $i$ alors on a $\mathcal{L}(\mathcal{A}_0^i) = \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X)))$. La proposition 5.22 montre l'inclusion $\mathcal{L}(\mathcal{A}_0^i) \subseteq \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X)))$. Prouvons l'inclusion réciproque. Comme la condition de la ligne 17 n'est jamais vérifiée, on a pour toute composante $A$ de $\mathrm{saff}(\delta^i(X))$, $\rho_m^{-1}(A \cap \mathbb{N}^m) \subseteq \mathcal{L}(\mathcal{A}_0^i)$. Ainsi, on a bien $\rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X))) \subseteq \mathcal{L}(\mathcal{A}_0^i)$. On a donc prouvé que $\mathcal{L}(\mathcal{A}_0^i) = \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X)))$. Par définition de $\mathcal{A}^{i+1}$, on a $\mathcal{L}(\mathcal{A}^{i+1}) = \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i(X))) \backslash \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\delta^i)(X)) = \rho_m^{-1}(\delta^{i+1}(X))$. La récurrence est donc prouvée.

Supposons alors que $X$ est non-quantifiée et montrons que l'algorithme termine avec la réponse "non-quantifié". Comme $X$ est non-quantifié, la proposition 5.32 montre que pour tout $i \geqslant 0$, la partie $\delta^i(X)$ est non-quantifiée. Ainsi, d'après le théorème 5.27, l'automate $\mathcal{A}_0^i$ vérifie $\mathcal{L}(\mathcal{A}_0^i) = \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(\rho_m(\mathcal{L}(\mathcal{A}^i))))$. La condition de la ligne 17 n'est donc jamais vérifiée. De plus, à la ligne 6, quand $i = m+1$, on a $\mathcal{L}(\mathcal{A}^{m+1}) = \rho_m^{-1}(\delta^{m+1}(X)) = \emptyset$ d'après la proposition 5.35. L'algorithme termine donc en renvoyant "non-quantifié".

Réciproquement, supposons que l'algorithme termine avec la réponse "non-quantifié". Dans ce cas, quand $i = m+1$, on a $\mathcal{L}(\mathcal{A}^{m+1}) = \emptyset$. Ainsi, on a $\delta^{m+1}(X) = \emptyset$. La proposition 5.35 prouve que $\ker(X) = \emptyset$ et le théorème 5.27 montre que $X$ est non-quantifié. □

**Remarque 5.38**
*La complexité exponentielle en temps du problème de décision prouvée dans le théorème précédent n'est pas optimale. En effet, en modifiant l'algorithme 2, on peut montrer que ce problème peut être décidé par un algorithme déterministe en temps polynomial appelant un oracle NP un nombre logarithmique de fois [Got95]. Ainsi, ce problème de décision ne peut pas être EXPTIME-complet.*

**Problème ouvert 5.39**
*Trouver la complexité pour décider si un automate binaire non ambigu représente une partie non-quantifiée.*

## 5.3 De l'automate à la formule

On montre dans cette section comment calculer à partir d'un automate binaire non ambigu représentant une partie non-quantifiée $X$, une formule non-quantifiée $\phi$ dont $X$ est l'ensemble des solutions. On montre qu'en temps exponentiel, une telle formule est calculable. Cela montre en particulier une réciproque au théorème 5.8.

**Théorème 5.40**
*Soit $X \subseteq \mathbb{N}^m$ une partie non-quantifiée. Il existe une formule non-quantifiée représentant $X$ qui a une taille bornée exponentiellement par la taille de tout automate binaire non ambigu représentant $X$. De plus, une telle formule est calculable à partir d'un tel automate en temps exponentiel en la taille de celui ci.*

*Démonstration :*
On commence par montrer que pour toute partie non-quantifiée $X$ représentée par un automate binaire non ambigu $\mathcal{A} = (Q, \Sigma_r, \Delta, \{q_0\}, F)$, on peut calculer en temps exponentiel un automate binaire non ambigu $\mathcal{A}'$ de même taille représentant $\delta(X)$. D'après le corollaire 4.80, la couverture semi-affine $\mathrm{cov}(\mathcal{A})$ est calculable en temps exponentiel. Ainsi, l'automate binaire $\mathcal{A}_0 = (Q, \Sigma_r, \Delta, \{q_0\}, F_0)$ est calculable en temps exponentiel. Le théorème 5.27 prouve que l'automate $\mathcal{A}_0$ est un automate binaire non ambigu représentant $\mathrm{saff}_{\mathbb{N}^m}(X)$. Considérons alors l'automate $\mathcal{A}' = (Q, \Sigma_r, \Delta, \{q_0\}, F')$ avec $F' = F_0 \backslash F$. On a alors $\mathcal{L}(\mathcal{A}') = \mathcal{L}(\mathcal{A}_0) \backslash \mathcal{L}(\mathcal{A})$. Ainsi, $\mathcal{L}(\mathcal{A}') = \rho_m^{-1}(\mathrm{saff}_{\mathbb{N}^m}(X) \backslash X) = \rho_m^{-1}(\delta(X))$.

Construisons ainsi en temps exponentiel la suite d'automates binaires non ambigus $(\mathcal{A}^i)_{0 \leqslant i \leqslant m}$ tels que $\mathcal{L}(\mathcal{A}^i) = \rho_m^{-1}(\delta^i(X))$. Calculons en temps exponentiel l'ensemble $\mathcal{C}_i$ des composantes affine de $\mathrm{saff}(\delta^i(X))$ en utilisant le théorème 4.79 appliqué à l'automate binaire $\mathcal{A}^i$. Pour chaque espace affine $A$ dans $\mathcal{C}_0 \cup \dots \cup \mathcal{C}_m$, on construit une formule affine $\phi_A$ de taille polynomial en $A$ représentant $A \cap \mathbb{N}^m$ en utilisant la proposition 5.36. On note alors $\phi_i$ la formule semi-affine définie par :

$$\phi_i = \bigvee_{A \in \mathcal{C}_i} \phi_A$$

On considère alors la suite $(\psi_i)_{0 \leqslant i \leqslant m}$ de formules non-quantifiées définie par la récurrence $\psi_m = \phi_m$ et $\psi_{i-1} = \phi_i \wedge \neg(\psi_i)$. Montrons par récurrence que $[\![\psi_i]\!] = \delta^i(X)$. Pour $i = m$

la récurrence est vérifiée. Supposons donc que $[\![\psi_i]\!] = \delta^i(X)$ pour un $i \geqslant 1$ et montrons que $[\![\psi_{i-1}]\!] = \delta^{i-1}(X)$. On a $[\![\psi_{i-1}]\!] = [\![\phi_i]\!] \setminus [\![\psi_i]\!] = \text{saff}_{\mathbb{N}^m}(\delta^i(X)) \setminus \delta^i(X) = \delta^{i-1}(X)$. La récurrence est donc prouvée.

En particulier, on a $[\![\psi_0]\!] = X$ et comme la formule $\psi_0$ est non-quantifiée et bornée exponentiellement en la taille de $\mathcal{A}$, on a prouvé le théorème. □

Comme le montre le lemme 5.41, cette taille exponentielle de la formule non-quantifiée ne peut pas être évitée en général.

**Lemme 5.41**
*Il existe une suite d'automates binaires non ambigus $(\mathcal{A}_n)_{n\geqslant 0}$ représentant une suite de parties non-quantifiées $(X_n)_{n\geqslant 0}$ telle que le nombre d'états de $\mathcal{A}_n$ est égal à $n+2$ alors que la plus petite formule non-quantifiée représentant $X_n$ à une taille supérieure à $2^n$.*

*Démonstration :*
On se place dans le cas $m = 1$ et $r = 2$ et on note $\mathcal{A}_n$ l'automate binaire canonique représentant $X_n = \{0, \dots, 2^n - 1\}$. Pour montrer que le nombre d'états de $\mathcal{A}_n$ est égal à n+2, on commence par étudier les résidus par un bit $b$ de l'ensemble $X_n$. Pour $n \geqslant 1$, on a $\gamma_b^{-1}(X_n) = \{(x-b)/2;\ 0 \leqslant x \leqslant 2^n - 1\} \cap \mathbb{N} = X_{n-1}$. Pour $n = 0$, on a $\gamma_0^{-1}(X_0) = X_0$ et $\gamma_1^{-1}(X_0) = \emptyset$. L'ensemble des résidus de $X_n$ est donc égal à $\{X_i;\ 0 \leqslant i \leqslant n\} \cup \{\emptyset\}$. L'automate $\mathcal{A}_n$ à donc $n+2$ états. Remarquons que $X_n$ est non-quantifiée. Considérons alors une formule $\phi_n(x)$ non-quantifiée représentant $X_n$ et montrons que la taille de $\phi_n$ est supérieur à $2^n$. On note $C$ l'ensemble des constantes $c$ apparaissant dans des termes $x\#c$ de la formule $\phi_n$. Supposons qu'il existe $i \in X_n$ tel que $i \notin C$. Considérons alors un entier $i' \notin (C \cup X_n)$. Comme un terme $x\#c$ est vrai en $i$ si et seulement s'il est vrai en $i'$, cela montre que $i \in [\![\phi_n]\!] = X_n$ si et seulement si $i' \in [\![\phi_n]\!] = X_n$. Comme $i \in X_n$ et $i' \notin X_n$, on a donc une contradiction. Ainsi, la taille de $\phi_n$ est supérieur à $2^n$. □

Deuxième PARTIE

# Approximation et accélération des systèmes à compteurs

CHAPITRE 6

# Les systèmes à compteurs

Dans ce chapitre, on introduit différentes classes de systèmes à compteurs.

**Définition 6.1**
*Un système (de transitions étiquetées) $S$ est un tuple $S = (E, \Sigma, (\xrightarrow{a})_{a\in\Sigma})$ tel que $E$ est un ensemble non vide d'états, $\Sigma$ est un ensemble fini d'actions et $\xrightarrow{a}$ est une relation binaire sur $E$ pour chaque action $a \in \Sigma$.*

Pour un système $S$, nous aurons besoin des définitions suivantes :
- l'inverse de $S$ est le système $S^{-1} = (E, \Sigma, (\xrightarrow{a}^{-1})_{a\in\Sigma})$.
- la relation d'accessibilité en une étape est la relation binaire $\mathcal{R}_S = \bigcup_{a\in\Sigma} \xrightarrow{a}$.
- la relation d'accessibilité $\mathcal{R}_S^*$ est la fermeture réflexive et transitive de $\mathcal{R}_S$.
- l'ensemble des prédécesseurs en une étape d'une partie $X' \subseteq E$ est la partie notée $\mathrm{Pre}_S(X') = \{x \in E;\ \exists x' \in X';\ x\mathcal{R}_S x'\}$.
- l'ensemble des prédécesseurs d'une partie $X' \subseteq E$ est la partie notée $\mathrm{Pre}_S^*(X') = \{x \in E;\ \exists x' \in X';\ x\mathcal{R}_S^* x'\}$.
- l'ensemble des successeurs en une étape d'une partie $X \subseteq E$ est la partie notée $\mathrm{Post}_S(X) = \{x' \in E;\ \exists x \in X;\ x\mathcal{R}_S x'\}$.
- l'ensemble des successeurs d'une partie $X \subseteq E$ est la partie notée $\mathrm{Post}_S^*(X) = \{x' \in E;\ \exists x \in X;\ x\mathcal{R}_S^* x'\}$.

**Définition 6.2**
*Un système à $m \geqslant 0$ compteurs $S$ est un système tel que $E = \mathbb{N}^m$.*

Les systèmes à compteurs que l'on va manipuler seront tous déterministes, sauf ceux étudiés brièvement dans le chapitre 7.

**Définition 6.3**
*Un système $S$ est déterministe si pour tout $x \in E$ et pour tout $a \in \Sigma$, il existe au plus un $x' \in E$ tel que $x \xrightarrow{a} x'$.*

Pour avoir une description finie d'un système à compteurs, on va supposer que chaque relation de transition est représentable par un UBA ; la représentation par UBA d'une relation est étudiée dans la section 6.1. Cette représentation nous permet de définir la classe des systèmes à compteurs effectifs dans la section 6.2. En remarquant que les systèmes à compteurs effectifs et déterministes sont, en pratique, définis par des fonctions affines, on introduit naturellement dans la section 6.3 la classe des systèmes à compteurs affines et plus particulièrement la classe des systèmes à compteurs à monoïde fini. Enfin, dans la section 6.4 on montre que la classe des systèmes à compteurs à monoïde fini, contient les automates à compteurs, les réseaux de Petri, les systèmes broadcast généralisés et les VASS.

## 6.1 Représentation d'une relation par un UBA

En remarquant qu'une relation sur $\mathbb{N}^m$ n'est qu'une partie de $\mathbb{N}^{2m}$, on définit naturellement la notion de représentation d'une relation par un UBA.

**Définition 6.4**
*Un UBA $\mathcal{A}$ représente une relation $\mathcal{R}$ sur $\mathbb{N}^m$ si :*

$$\mathcal{L}(\mathcal{A}) = \rho_{2m}^{-1}(\{(x_1, x'_1, x_2, x'_2, \ldots, x_m, x'_m);\ (x, x') \in \mathcal{R}\})$$

Naturellement, l'UBA minimal représentant une relation $\mathcal{R}$ est noté $\mathcal{A}(\mathcal{R})$.

On a "entrelacé" les variables "primées et non primées" dans la précédente définition pour que :

- la relation d'identité soit représentable par un UBA avec seulement $r + 2$ états et plus généralement pour que les variables qui ne "sont pas modifiées" par une relation ne fassent pas exploser la taille de l'UBA.
- les tailles des UBA $\mathcal{A}(\mathcal{R})$ et $\mathcal{A}(\mathcal{R}^{-1})$ soient comparables à un facteur constant près.

**Proposition 6.5**
*Il existe un UBA $\mathcal{A}_r$ à $r + 2$ états tel que pour tout $m \geqslant 1$, la relation identité $I_m$ est représentée par l'UBA $\mathcal{A}_r$.*

*Démonstration :*

Il suffit de remarquer que $I_m$ est représentée par l'UBA $\mathcal{A}_r = (Q, \Sigma_r, \delta, \{q_0\}, F)$ défini pour tout $b, b' \in \Sigma_r$ par :

$$\begin{cases} Q = \{q_0, q_\perp, p_0, \ldots, p_{r-1}\} & \\ \delta(q_0, b) = p_b & \\ \delta(q_\perp, b) = q_\perp & \\ \delta(p_{b'}, b) = q_0 & b = b' \\ \delta(p_{b'}, b) = q_\perp & b \neq b' \\ F = \{q_0, p_0\} & \end{cases}$$

$\square$

Pour prouver que la taille des UBA $\mathcal{A}(\mathcal{R})$ et $\mathcal{A}(\mathcal{R}^{-1})$ sont comparables, on commence par établir le lemme suivant.

**Lemme 6.6**
*Soient $(b_i)_{1\leqslant i\leqslant n}$ et $(b'_i)_{1\leqslant i\leqslant n}$ deux suites de $\Sigma_r$. On note $x$ et $x'$ les vecteurs de $\mathbb{N}^m$ définis par $x = \rho_m(b_1 \dots b_n)$ et $x' = \rho_m(b'_1 \dots b'_n)$. On a :*

$$\rho_{2m}(b_1 b'_1 \dots b_n b'_n) = (x_1, x'_1, \dots x_m, x'_m)$$

*Démonstration :*
Par définition de $\rho_m$ et $\rho_{2m}$. □

**Proposition 6.7**
*Soit $\mathcal{R}$ une relation sur $\mathbb{N}^m$. La relation $\mathcal{R}$ est représentable par un UBA si et seulement si $\mathcal{R}^{-1}$ est représentable par un UBA. De plus, dans ce cas, on a :*

$$\text{taille}(\mathcal{A}(\mathcal{R}^{-1})) \leqslant (r+1).\text{taille}(\mathcal{A}(\mathcal{R}))$$

*Démonstration :*
On note $X_{\mathcal{R}} = \{(x_1, x'_1, \dots, x_m, x'_m);\ (x, x') \in \mathcal{R}\}$. On note de même $X_{\mathcal{R}^{-1}}$. Considérons l'UBA minimal $\mathcal{A} = \mathcal{A}(\mathcal{R}) = (Q, \Sigma_r, \delta, \{q_0\}, F)$ représentant $X_{\mathcal{R}}$. Notons $\mathcal{A}' = (Q \cup Q \times \Sigma_r, \Sigma_r, \delta', \{q_0\}, F')$ l'automate binaire défini par

$$\begin{cases} F' = F \cup F \times \{0\} & \\ \delta'(q, b) = (q, b) & \text{pour tout } (q, b) \in Q \times \Sigma_r \\ \delta'((q, b), b') = \delta(q, b'b) & \text{pour tout } ((q, b), b') \in (Q \times \Sigma_r) \times \Sigma_r \end{cases}$$

Par construction $\mathcal{A}'$ est un automate binaire déterministe et complet.

Montrons que $\mathcal{A}'$ représente $X_{\mathcal{R}^{-1}}$. Considérons $\sigma \in \mathcal{L}(\mathcal{A}')$. On commence par supposer que $\sigma$ est un mot de longueur paire. Il existe deux suites $(b_i)_{1\leqslant i\leqslant n}$ et $(b'_i)_{1\leqslant i\leqslant n}$ de $\Sigma_r$ telles que $\sigma = b_1 b'_1 \dots b_n b'_n$. On a alors $b'_1 b_1 \dots b'_n b_n \in \mathcal{L}(\mathcal{A})$. Ainsi d'après le lemme 6.6, on a $\rho_{2m}(\sigma) \in X_{\mathcal{R}^{-1}}$. On a donc prouvé l'inclusion $\rho_{2m}(\mathcal{L}(\mathcal{A}')) \subseteq X_{\mathcal{R}^{-1}}$. Considérons alors le cas où $\sigma$ est de longueur impaire. Comme $\delta'(q_0, \sigma) \in F \cup F \times \{0\}$ et que $\sigma$ est de longueur impaire, on a $\delta(q_0, \sigma) \in F \times \{0\}$. Ainsi, il existe un mot $\sigma' \in \Sigma_r^*$ tel que $\sigma = \sigma' 0$. D'après le cas précédent, comme $\sigma'$ est un mot de longueur paire, on a $\rho_{2m}(\sigma') \in X_{\mathcal{R}^{-1}}$. Comme $\rho_{2m}(\sigma) = \rho_{2m}(\sigma')$, on a prouvé que $\rho_{2m}(\sigma) \in X_{\mathcal{R}^{-1}}$. On a donc prouvé l'inclusion $\rho_{2m}(\mathcal{L}(\mathcal{A}')) \subseteq X_{\mathcal{R}^{-1}}$. Réciproquement, considérons $y \in X_{\mathcal{R}^{-1}}$. Il existe alors $\sigma \in \Sigma_r^*$ tel que $\rho_{2m}(\sigma) = y$. Comme $\rho_{2m}(\sigma 0) = \rho_{2m}(\sigma)$, on peut supposer que $\sigma$ est de longueur paire. Il existe ainsi deux suites $(b_i)_{1\leqslant i\leqslant n}$ et $(b'_i)_{1\leqslant i\leqslant n}$ de $\Sigma_r$ telles que $\sigma = b_1 b'_1 \dots b_n b'_n$. Comme $\rho_{2m}(\sigma) \in X_{\mathcal{R}^{-1}}$, le lemme 6.6 montre que $\rho_{2m}(b'_1 b_1 \dots b' n b_n) \in X_{\mathcal{R}}$. Comme $\mathcal{A}$ est un automate binaire non ambigu représentant $X_{\mathcal{R}}$, on a $b'_1 b_1 \dots b'_n b_n \in \mathcal{L}(\mathcal{A})$. Par construction de $\mathcal{A}'$, on a $\sigma \in \mathcal{L}(\mathcal{A}')$. On a donc prouvé l'inclusion $X_{\mathcal{R}^{-1}} \subseteq \rho_{2m}(\mathcal{L}(\mathcal{A}'))$. L'automate $\mathcal{A}'$ représente ainsi $X_{\mathcal{R}^{-1}}$.

D'après le lemme 4.39, en modifiant l'ensemble des états finaux de l'automate $\mathcal{A}'$, on obtient un automate binaire non ambigu $\mathcal{A}^{-1}$ représentant le même ensemble que $\mathcal{A}$.

□

## 6.2 Les systèmes à compteurs effectifs

Pour avoir une description finie des systèmes à compteurs adaptée à des calculs d'ensemble d'états accessibles représentables par des UBA, on considére la classe des systèmes à compteurs dont chaque relation de transition est UBA-représentable.

**Définition 6.8**
*Un système à compteurs effectif est un tuple $(S, (\mathcal{A}_a)_{a\in\Sigma})$ tel que que $S$ est un système à compteurs et $\mathcal{A}_a = \mathcal{A}(\xrightarrow{a})$.*

Comme l'UBA minimal $\mathcal{A}_a$ est uniquement déterminé par $\xrightarrow{a}$, on notera sans ambiguïté $S$ le système à compteurs effectif $(S, (\mathcal{A}_a)_{a\in\Sigma})$

**Définition 6.9**
*La taille d'un système à compteurs effectif $S$ est* $\text{taille}(S) = \sum_{a\in\Sigma} \text{taille}(\mathcal{A}(\xrightarrow{a}))$.

## 6.3 Les systèmes à compteurs affines

Dans la pratique, les transitions d'un système à compteurs effectif et déterministe sont des fonctions affines.

**Remarque 6.10**
*Il faudrait voir si une fonction UBA-représentable n'est pas une "union finie de fonctions affines".*

Comme une fonction affine peut s'écrire de plusieurs manières différentes, on va devoir "décorer" les fonctions affines.

Une fonction affine décorée est un tuple $(f, M, v)$ tel que $f$ est une fonction affine définie sur une partie $D$ vérifiant $f(x) = M.x + v$ pour tout $x \in D$.

La composée $(f_1, M_1, v_1) \circ (f_2, M_2, v_2)$ de deux fonctions affines décorées $(f_1, M_1, v_1)$ et $(f_2, M_2, v_2)$ est la fonction affine décorée $(f_1 \circ f_2, M_1.M_2, M_1.v_2 + v_1)$.

Un système à compteurs affine décoré est un tuple $(S, (M_a, v_a)_{a\in\Sigma})$ tel que $(f_a, M_a, v_a)$ est une fonction affine décorée pour tout $a \in \Sigma$.

Pour un tel système et suite d'actions $a_1$, ..., $a_n$ de $\Sigma$ on note $(f_{a_1\dots a_n}, M_{a_1\dots a_n}, v_{a_1\dots a_n})$ la fonction affine décorée définie par

$$(f_{a_1\dots a_n}, M_{a_1\dots a_n}, v_{a_1\dots a_n}) = (f_{a_n}, M_{a_n}, v_{a_n}) \circ \dots \circ (f_{a_1}, M_{a_1}, v_{a_1})$$

Le domaine de définition de $f_{a_1\dots a_n}$ est noté $D_{a_1\dots a_n}$.

**Définition 6.11**
*Le monoïde engendré multiplicativement par les matrices carrées $\{M_a;\ a \in \Sigma\}$ d'un système à compteurs affine décoré $S$ est noté $\mathcal{M}_S = \{M_\sigma;\ \sigma \in \Sigma^*\}$.*

Quand le contexte le permet, un système affine décoré $(S, (M_a, v_a)_{a\in\Sigma})$ est noté $S$ et appelé simplement système à compteurs.

**Définition 6.12**
*Un système à compteurs affine décoré $S$ est à monoïde fini si $\mathcal{M}_S$ est fini.*

Expliquons pourquoi la suite $(M_a)_{a\in\Sigma}$ est donnée explicitement. Rappelons que l'on peut décider la finitude du sous-monoïde engendré par une suite finie de matrices $(M_a)_{a\in\Sigma}$ dans $\mathcal{M}_m(\mathbb{Q})$ ([MS77], [Jac78]). De plus, dans le cas où les coefficients des matrices $M_a$ sont dans $\mathbb{N}$, ce problème est décidable en temps exponentiel. Cependant, décider si pour un système à compteurs affine $S$, il existe une suite de matrices $(M_a)_{a\in\Sigma}$ telle que $(S,(M_a)_{a\in\Sigma})$ est à monoïde fini est un problème difficile car la suite $(M_a)_{a\in\Sigma}$ n'est pas unique lorsqu'il existe $a\in\Sigma$ telle que l'enveloppe affine $\mathrm{aff}(D_a)$ n'est pas égale à tout $\mathbb{Q}^m$.

## 6.4 Réseaux de Petri et automates à compteurs

On montre dans cette section que la classe des systèmes à compteurs effectifs à monoïde fini est une classe de systèmes à compteurs contenant les réseaux de Petri Reset/Transfert ([Cia94] [DFS98]), les systèmes broadcasts généralisés ([EN98], [Del00a], [Del01], [Del00b]), les automates à compteurs, et les VASS ([FS00a], [BM99], [HP79] [HRHY86]).

### Les réseaux de Petri Reset/Transfert et les systèmes broadcasts

On rappelle quelques extensions des réseaux de Petri (on trouvera dans [Cia94] d'autres extensions).

**Définition 6.13**
*Un réseau de Petri $S$ est un système à compteurs affine tel que pour tout $a\in\Sigma$, il existe deux vecteurs $u_a, u'_a \in \mathbb{N}^m$ tels que $D_a = \{x\in\mathbb{N}^m;\ x \geqslant u_a\}$ et $f_a(x) = x - u_a + u'_a$ pour tout $x\in D_a$.*

Remarquons que le monoïde $\mathcal{M}_S$ d'un réseau de Petri $S$ est fini car il ne contient que la matrice identité : $\mathcal{M}_S = \{I\}$. Les matrices carrées utilisées pour étendre la classe des réseaux de Petri, sont des "reset/transfert".

**Définition 6.14 ([EN98])**
*Une matrice $M\in\mathcal{M}_m(\mathbb{Q})$ est dite reset/transfert si pour tout $i\in\{1,\dots,m\}$, soit $M.e_i = 0$ (ce qui correspond à mettre à zéro (reset) le compteur $i$), soit il existe $i'\in\{1,\dots,m\}$ tel que $M.e_i = e_{i'}$ (ce qui corresponds à transférer le contenu du compteur $i$ vers le compteur $i'$).*

Comme la classe des matrices reset/transfert est stable par multiplication, c'est un sous-monoïde fini de $\mathcal{M}_m(\mathbb{Q})$. Ainsi, en utilisant ces matrices pour définir les transitions affines d'un système à compteurs $S$, on est sûr que le monoïde $\mathcal{M}_S$ sera fini.

Les réseaux de Petri reset/transfert et les systèmes broadcasts généralisés définis ci-dessous sont ainsi des systèmes à compteurs à monoïde fini.

**Définition 6.15**
*Un réseau de Petri reset/transfert, est un système à compteurs affine tel que pour tout*

*$a \in \Sigma$, il existe une matrice reset/transfert $M_a$, deux vecteurs $u_a, u'_a \in \mathbb{N}^m$ tels que $D_a = \{x \in \mathbb{N}^m;\ x \geqslant u_a\}$ et $f_a(x) = M_a.(x - u_a) + u'_a$ pour tout $x \in D_a$.*

**Définition 6.16**
*Un système broadcast généralisé $S$, est un système à compteurs affine tel que pour tout $a \in \Sigma$, le domaine de définition $D_a$ est intervalle-définissable et il existe une matrice reset/transfert $M_a$ et un vecteur $v_a \in \mathbb{Z}^m$ tels que pour tout $x \in D_a$, on a $f_a(x) = M_a.x + v_a$.*

### Les automates à compteurs

On montre dans cette sous section que les systèmes à compteurs munis d'une "structure de contrôle", comme les automates à compteurs et les VASS, sont en fait des systèmes à compteurs dont un des compteurs est borné (ce compteur borné servant naturellement d'état de contrôle).

**Définition 6.17**
*Un automate à compteurs $S$ est un système tel qu'il existe :*
- *un ensemble fini $Q$ d'états de contrôle,*
- *un ensemble fini $\Sigma$ d'actions,*
- *une fonction de transition $\delta : Q \times \Sigma \to Q$,*
- *un domaine de définition $D_a$ intervalle-définissable pour chaque $a \in \Sigma$, et*
- *un vecteur $v_a \in \mathbb{Z}^m$ pour chaque $a \in \Sigma$.*

*tels que $E = Q \times \mathbb{N}^m$ et $(q, x) \xrightarrow{a} (q, x')$ si et seulement si $q' = \delta(q, a)$, $x \in D_a$ et $x' = x + v_a$.*

Un VASS est un cas particulier d'automate à compteurs.

**Définition 6.18**
*Un VASS (Vector Addition System with States) $S$ est un automate à compteurs tel que $D_a = \{x \in \mathbb{N}^m;\ x + v_a \geqslant 0\}$ pour tout $a \in \Sigma$.*

La définition suivante montre comment associer un système à compteurs à un automate à compteurs.

**Définition 6.19**
*Le système à compteurs associé à un automate à compteurs $S$, dont l'ensemble des états est $Q = \{0, \dots, \mathrm{card}(Q) - 1\}$ est ordoné, est défini par $S' = (Q \times \mathbb{N}^m, \Sigma, (\xrightarrow{a})_{a \in \Sigma})$.*

Remarquons le lien immédiat entre les relations d'accessibilité de $S$ et $S'$.

CHAPITRE 7

# Accessibilité symbolique

Dans ce chapitre on étudie la taille asymptotique de l'automate binaire non ambigu minimal représentant l'ensemble des prédécesseurs en $k$ étapes à partir d'un ensemble $X'$ lui-même représenté par un automate binaire.

La vérification d'un système infini, se réduit souvent à un calcul d'ensemble d'états accessibles [BFLP03]. Pour cela, on doit pouvoir calculer la *limite* d'une des deux suites croissantes $\mathrm{Pre}_S^{\leqslant k}(X')$ ou $\mathrm{Post}_S^{\leqslant k}(X)$. Rappelons que dans la pratique, la suite $\mathrm{Post}_S^{\leqslant k}(X)$ est strictement croissante. Ainsi, pour calculer la limite de cette suite, différentes techniques ont été développée, comme l'abstraction (introduction du chapitre 4), l'accélération (chapitres 9 et 10), ou les invariants (chapitre 8, [DRV01]).

Dans le cadre des systèmes bien structurés [FS01, FMP99, FPS00, FPS03], la suite $\mathrm{Pre}_S^{\leqslant k}(X')$ est stationnaire lorsque $X'$ est "clos par le haut" [AJ93] (les protocols broadcasts et les réseaux de Petri reset/transfert sont des cas particuliers de tels systèmes [EFM99, BM99]). Ainsi, en calculant symboliquement les ensembles $\mathrm{Pre}_S^{\leqslant k}(X')$ de proche en proche, on finira par obtenir la limite $\mathrm{Pre}_S^{*}(X') = \mathrm{Pre}_S^{\leqslant k_0}(X')$ pour un entier $k_0 \geqslant 0$. Comme la valeur de $k_0$ peut-être non-élémentaire (c'est le cas pour les "lossy chanel systems" [Sch02]), une classe simple de systèmes bien structurées) alors que pourtant dans la pratique, la suite est "rapidement" stationnaire [BB02, BB03, RV02, Del00a, Del00b, Del01], la complexité du calcul du plus petit entier $k_0$, ne *semble* pas être une mesure intéressante de la complexité du calcul de $\mathrm{Pre}_S^{\leqslant k}(X')$. Pour mieux mesurer la complexité de cet algorithme, on s'intéresse à :

- la complexité du calcul d'une représentation de $\mathrm{Pre}_S(X')$ en fonction d'une représentation de $X'$, et
- la taille asymptotique de la plus petite représentation de $\mathrm{Pre}_S^{\leqslant k}(X')$ en fonction de $k$.

Dans le cadre de la vérification des systèmes à compteurs effectifs, nous utilisons naturellement les automates binaires non ambigus comme représentation symbolique.

Dans ce chapitre, nous prouvons que :

- le calcul d'un automate binaire non ambigu représentant $\mathrm{Pre}_S(X')$ est calculable en *temps polynomial* en la taille de $\mathcal{A}(X')$ pour tout système à compteurs $S$ effectif et déterministe (la taille de l'automate binaire non ambigu représentant $\mathrm{Post}_S(X)$ est en général exponentielle en la taille de $\mathcal{A}(X)$).
- la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est *polynomiale en $k$* pour tout système à compteurs $S$ effectif et à monoïde fini et pour toute partie UBA-représentable $X'$. Pour obtenir ce résultat *inattendu*, on a caractérisé précisément la structure de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$.
- on a caractérisé les fonctions affines laissant stables par image inverse les logiques souvent utilisées en vérification : logique de Presburger, logique des intervalles et logique des clos par le haut. On montre que pour ces logiques, la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est respectivement exponentielle, polynômiale et constante.

Dans la section 7.1, on montre comment calculer en temps polynomial un automate binaire non ambigu représentant $\mathrm{Pre}_S(X')$ en fonction de $\mathcal{A}(X')$, pour tout système à compteurs $S$ effectif et déterministe. Dans le cas non-déterministe, on montre qu'une explosion exponentielle de la taille des automates est inévitable en général. La taille asymptotique en $k$ de l'automate $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$, est étudiée dans la section 7.2. Enfin, on explique dans la section 7.3, pourquoi l'étude de la taille asymptotique de $\mathcal{A}(\mathrm{Post}_S^{\leqslant k}(X'))$ n'est pas faite dans cette thèse.

## 7.1 Calcul de $\mathrm{Pre}_S(X')$ et $\mathrm{Post}_S(X)$

Dans cette section, on prouve que pour tout système à compteurs effectif et déterministe $S$, l'automate binaire non ambigu représentant les prédécesseurs de $X'$ est calculable en temps polynomial en la taille de $\mathcal{A}(X')$. Par contre, la taille de l'automate binaire non ambigu représentant les successeurs de $X'$ est en général exponentielle en la taille de $\mathcal{A}(X)$.

Rappelons que récemment, dans [BB02] et [BB03], il a été prouvé que sous les conditions du théorème 7.1 suivant, le calcul de $\mathcal{A}(\mathrm{Pre}_S(X'))$ et $\mathcal{A}(\mathrm{Post}_S(X))$ peut-être réalisé en temps polynomial en fonction respectivement de $\mathcal{A}(X')$ et $\mathcal{A}(X)$.

**Théorème 7.1 ([BB02],[BB03])**
*Soit $S$ un système à compteurs effectif et affine. On se place dans la base de décomposition $r = 2$. On peut alors calculer :*
- $\mathcal{A}(\mathrm{Pre}_S(X'))$ *en temps polynomial en fonction de* $\mathcal{A}(X')$ *si pour toute action* $a \in \Sigma$, *il existe un indice* $i_a \in \{1, \ldots, m\}$, *un vecteur* $\alpha \in (2.\mathbb{Z})^m$ *et une constante* $c \in \mathbb{Z}$ *tels que pour tout* $x \in D_a$, *on a* $(f_a(x))_i = x_i$ *pour* $i \neq i_a$ *et* $(f_a(x))_i = \langle \alpha, x \rangle + c$ *sinon.*
- $\mathcal{A}(\mathrm{Post}_S(X))$ *en temps polynomial en fonction de* $\mathcal{A}(X)$ *si pour toute action* $a \in \Sigma$, *il existe un indice* $i_a \in \{1, \ldots, m\}$, *un vecteur* $\alpha \in (2.\mathbb{Z}+1)^m$ *et une constante* $c \in \mathbb{Z}$ *tels que pour tout* $x \in D_a$, *on a* $(f_a(x))_i = x_i$ *pour* $i \neq i_a$ *et* $(f_a(x))_i = \langle \alpha, x \rangle + c$ *sinon.*

**Remarque 7.2**
*Remarquons que pour pouvoir appliquer le théorème précédent au calcul de* $\mathrm{Post}_S(X)$, *les*

*fonctions affines $f_a$ doivent être injectives. Ainsi le calcul de $\mathrm{Post}_S(X)$ correspond au calcul de $\mathrm{Pre}_{S^{-1}}(X)$ pour le système à compteurs affine $S^{-1}$. Le calcul des successeurs $\mathrm{Post}_S(X)$ est donc un calcul des prédécesseurs "caché".*

**Théorème 7.3**
*Soit $S$ un système à compteurs effectif. Pour tout $X' \subseteq \mathbb{N}^m$ représenté par un automate binaire non ambigu $\mathcal{A}'$, on peut calculer un automate binaire non ambigu $\mathcal{A}$ représentant $\mathrm{Pre}_S(X')$ en temps $O(\mathrm{taille}(\mathcal{A}))$ tel que :*

$$\mathrm{taille}(\mathcal{A}) \leqslant \begin{cases} (\mathrm{taille}(\mathcal{A}')+1)^{\mathrm{taille}(S)} & \text{si } S \text{ est déterministe} \\ 2^{\mathrm{taille}(\mathcal{A}').\mathrm{taille}(S)} & \text{sinon} \end{cases}$$

*Démonstration :*

Remarquons que le caractère déterministe des relations de $S$ est le point clef de ce résultat.

On considère un système à compteurs effectif $S$. Pour chaque $a \in \Sigma$, on note $\mathcal{A}^a = \mathcal{A}(\rightarrow_a) = (Q^a, \Sigma_r, \delta^a, \{q_0^a\}, F^a)$. On considère un automate binaire non ambigu $\mathcal{A}' = (Q', \Sigma_r, \delta', \{q'_0\}, F')$ représentant une partie $X' \subseteq \mathbb{N}^m$. Pour chaque $a \in \Sigma$, on pose $X_a = \{x \in \mathbb{N}^m;\ \exists x' \in X';\ x \rightarrow_a x'\}$. On va montrer que l'on peut calculer un automate binaire non ambigu $\mathcal{A}$ représentant $X_a$ en temps $O(\mathcal{A})$ et tel que :

$$\mathrm{taille}(\mathcal{A}) \leqslant \begin{cases} (\mathrm{taille}(\mathcal{A}')+1)^{\mathrm{taille}(\mathcal{A}^a)} & \text{si } S \text{ est déterministe} \\ 2^{\mathrm{taille}(\mathcal{A}').\mathrm{taille}(\mathcal{A}^a)} & \text{sinon} \end{cases}$$

En effet, il suffira alors de remarquer que $\rho_m^{-1}(\mathrm{Pre}_S(X')) = \bigcup_{a\in\Sigma} \rho_m^{-1}(X_a)$ pour prouver le théorème.

En temps $O(\mathrm{taille}(\mathcal{A}^a))$, on calcule l'ensemble des états $Q_\perp^a \subseteq Q^a$ de l'automate $\mathcal{A}^a$ co-accessibles à partir d'un état final de $F^a$. Remarquons que si $q_0^a \notin Q_\perp^a$ alors $\mathcal{L}(\mathcal{A}^a) = \emptyset$ et dans ce cas $X_a = \emptyset$. Comme $\mathcal{A}^a$ est l'UBA minimal représentant $\emptyset$, on a $\mathrm{taille}(\mathcal{A}^a) = 1$. L'ensemble $X_a$ est alors représenté par l'UBA à un état représentant $\emptyset$. On peut donc supposer que $q_0^a \in Q_\perp^a$. On note $\delta_\perp^a$ la restriction de $\delta^a$ à l'ensemble des couples $(q_\perp^a, b) \in Q_\perp^a \times \Sigma_r$ tels que $\delta^a(q_\perp^a, b) \in Q_\perp^a$.

Considérons l'automate binaire $\mathcal{A} = (Q, \Sigma_r, \delta, \{q_0\}, F)$ défini par :

$$\begin{cases} Q = \mathcal{P}(Q' \times Q_\perp^a) \\ \delta(q,b) = \{(\delta'(q',b'), \delta_\perp^a(q^a, bb'));\ (q', q^a) \in q;\ b' \in \Sigma_r\} \\ q_0 = \{(q'_0, q_0^a)\} \\ F = \{q \in Q;\ q \cap F' \times F^a \neq \emptyset\} \end{cases}$$

Un algorithme construisant l'automate $\mathcal{A}$ de proche en proche en partant de l'état initial $q_0$, ne va construire que l'ensemble des états accessibles de $\mathcal{A}$. On peut donc supposer, quitte à remplacer $\mathcal{A}$ par un sous-automate, que tous les états de $\mathcal{A}$ sont accessibles.

Remarquons que $\mathrm{taille}(\mathcal{A}) \leqslant 2^{\mathrm{taille}(\mathcal{A}').\mathrm{taille}(\mathcal{A}^a)}$. Montrons que si $S$ est déterministe alors l'ensemble des états accessibles de $\mathcal{A}$ est borné par $(\mathrm{taille}(\mathcal{A})+1)^{\mathrm{taille}(\mathcal{A}_a)}$. Pour prouver cette majoration, on commence par montrer que pour tout état accessible $q$ de $\mathcal{A}$ et pour tout $q_{\perp}^{a} \in Q_{\perp}^{a}$, il existe au plus un état $q' \in Q'$ tel que $(q', q_{\perp}^{a}) \in q$. Considérons donc un état accessible $q \in Q$, un état $q_{\perp}^{a} \in Q_{\perp}^{a}$ et deux états $q_1', q_2' \in Q'$ tels que $(q_1', q_{\perp}^{a})$ et $(q_2', q_{\perp}^{a})$ sont dans $q$. Comme $q$ est accessible, il existe une suite $b_1, \ldots, b_n$ dans $\Sigma_r$ telle que $q = \delta(q_0, b_1 \ldots b_n)$. Par construction de $\mathcal{A}$, comme $(q_1', q_{\perp}^{a})$ et $(q_2', q_{\perp}^{a})$ sont dans $q$, il existe deux suites $b_{1,1}', \ldots b_{n,1}'$ et $b_{1,2}', \ldots, b_{n,2}'$ de $\Sigma_r$ telles que :

$$\begin{cases} q_{\perp}^{a} = \delta^{a}(q_0^{a}, b_1 b_{1,1}' \ldots b_n b_{n,1}') \\ q_{\perp}^{a} = \delta^{a}(q_0^{a}, b_1 b_{1,2}' \ldots b_n b_{n,2}') \\ q_1' = \delta'(q_0', b_{1,1}' \ldots b_{n,1}') \\ q_2' = \delta'(q_0', b_{1,2}' \ldots b_{n,2}') \end{cases}$$

Comme $q_{\perp}^{a} \in Q_{\perp}^{a}$, il existe un mot $\sigma \in \Sigma_r^*$ tel que $\delta^{a}(q_{\perp}^{a}, \sigma) \in F^{a}$. Comme $\mathcal{A}^{a}$ est un automate binaire non ambigu, quitte à remplacer $\sigma$ par $\sigma 0$, on peut supposer que $\sigma$ est un mot de longueur paire. Considérons une suite $b_{n+1}$, $b_{n+1}'$, ..., $b_k, b_k'$ dans $\Sigma_r$ telle que $\sigma = b_{n+1} b_{n+1}' \ldots b_k b_k'$. On note $x_1'$, $x_2'$ et $x$ les vecteurs de $\mathbb{N}^m$ définis par :

$$\begin{cases} x_1' = \rho_m(b_{1,1}' \ldots b_{n,1}' b_{n+1}' \ldots b_k') \\ x_2' = \rho_m(b_{1,2}' \ldots b_{n,2}' b_{n+1}' \ldots b_k') \\ x = \rho_m(b_1 \ldots b_k) \end{cases}$$

Comme $b_1 b_{1,1}' \ldots b_n b_{n,1}' b_{n+1} b_{n+1}' \ldots b_k b_k'$ et $b_1 b_{1,2}' \ldots b_n b_{n,2}' b_{n+1} b_{n+1}' \ldots b_k b_k'$ sont des mots de $\mathcal{L}(\mathcal{A}^{a})$, le lemme 6.6 montre que $x \rightarrow_a x_1'$ et $x \rightarrow_a x_2'$. Comme $S$ est déterministe, on a donc $x_1' = x_2'$. Les mots $b_{1,1}' \ldots b_{n,1}' b_{n+1}' \ldots b_k'$ et $b_{1,2}' \ldots b_{n,2}' b_{n+1}' \ldots b_k'$ sont donc de la même longueur et représentent le même vecteur de $\mathbb{N}^m$. Le lemme 4.32 montre que dans ce cas $b_{1,1}' \ldots b_{n,1}' b_{n+1}' \ldots b_k' = b_{1,2}' \ldots b_{n,2}' b_{n+1}' \ldots b_k'$. En particulier, on a prouvé que $q_1' = \delta'(q_0', b_{1,1}' \ldots b_{n,1}') = \delta'(q_0', b_{1,2}' \ldots b_{n,2}') = q_2'$.

On a donc prouvé que si $S$ est déterministe, le nombre d'états accessibles de $\mathcal{A}$ est borné par $(\text{taille}(\mathcal{A}') + 1)^{\text{taille}(\mathcal{A}^{a})}$.

Pour finir la preuve du théorème, on se replace dans le cas général où $S$ est un système à compteurs effectif non nécessairement déterministe.

On commence par montrer que $\mathcal{A}$ représente $X_a$. Considérons un mot $b_1 \ldots b_n \in \mathcal{L}(\mathcal{A})$. Par construction de $\mathcal{A}$, il existe un mot $b_1' \ldots b_n'$ tel que $b_1 b_1' \ldots b_n b_n' \in \mathcal{L}(\mathcal{A}^{a})$ et $b_1' \ldots b_n' \in \mathcal{L}(\mathcal{A}')$. Soient $x = \rho_m(b_1 \ldots b_n)$ et $x' = \rho_m(b_1' \ldots b_n')$. D'après le lemme 6.6, on a $x \rightarrow_a x'$. De plus, comme $x' \in X'$, on déduit $x \in X_a$. On a donc prouvé l'inclusion $\rho_m(\mathcal{L}(\mathcal{A})) \subseteq X_a$. Prouvons l'inclusion inverse. Considérons $x \in X_a$. Il existe $x' \in X'$ tel que $x \rightarrow_a x'$. Comme $\mathcal{A}^{a}$ est un automate binaire représentant la relation $\rightarrow_a$, il existe un mot $\sigma \in \mathcal{L}(\mathcal{A}^{a})$ tel que $\rho_{2.m}(\sigma) = (x_1, x_1', \ldots, x_m, x_m')$. Comme $\mathcal{A}^{a}$ est de plus non ambigu, on peut supposer, quitte à remplacer $\sigma$ par $\sigma.0$, que le mot $\sigma$ est divisible par 2. On considère deux suites $(b_i)_{1 \leqslant i \leqslant n}$ et $(b_i)_{1 \leqslant i \leqslant n}$ de $\Sigma_r$ telles que $\sigma = b_1 b_1' \ldots b_n b_n'$. Notons $x$ et $x'$ les vecteurs de $\mathbb{N}^m$ définis par $x = \rho_m(b_1 \ldots b_n)$ et $x' = \rho_m(b_1' \ldots b_n')$. Par construction de l'automate $\mathcal{A}$, on a $b_1 \ldots b_n \in \mathcal{L}(\mathcal{A})$. Ainsi, $x \in \rho_m(\mathcal{L}(\mathcal{A}))$. On a donc prouvé l'inclusion $X_a \subseteq \rho_m(\mathcal{L}(\mathcal{A}))$. L'automate $\mathcal{A}$ représente donc $X_a$. En modifiant l'ensemble des états finaux de $\mathcal{A}$, on déduit du lemme 4.39 un automate binaire non ambigu représentant $X_a$. $\square$

**Remarque 7.4**
*L'algorithme de construction de* $\mathrm{Pre}_S(X')$ *utilisé dans la preuve du théorème précédent n'est autre que celui utilisé dans les outils* LASH *et* FAST *[WB00], [Las], [Fas], [BFLP03]. Il est générique car les cas* $S$ *déterministe et* $S$ *non déterministe sont traités de la même façon. Il consiste en effet à construire l'automate binaire non ambigu représentant* $\{(x, x') \in \mathcal{R}_S;\ x' \in X'\}$*, puis à éliminer les variables* $x'_1, \dots, x'_m$*. Rappelons que le coût de l'élimination est exponentiel en général (voir par exemple la proposition 5.11). La complexité polynomiale en la taille de* $\mathcal{A}(X')$ *est donc plutôt surprenante.*

Du théorème 7.3 précédent, on déduit qu'un automate binaire non ambigu représentant $\mathrm{Post}_S(X)$ est calculable en temps exponentiel en fonction de la taille d'un automate binaire représentant $X$ pour tout système à compteurs effectif.

**Corollaire 7.5**
*Soit* $S$ *un système à compteurs effectif. Pour tout* $X' \subseteq \mathbb{N}^m$ *représenté par un automate binaire non ambigu* $\mathcal{A}'$*, on peut calculer un automate binaire non ambigu* $\mathcal{A}$ *représentant* $\mathrm{Post}_S(X')$ *en temps* $O(\mathrm{taille}(\mathcal{A}))$ *tel que :*

$$\mathrm{taille}(\mathcal{A}) \leqslant 2^{(r+1).\mathrm{taille}(\mathcal{A}').\mathrm{taille}(S)}$$

*Démonstration :*
Il suffit en effet de considérer le système à compteurs $S^{-1} = (\mathbb{N}^m, \Sigma, (\xrightarrow[a]{-1})_{a\in\Sigma})$ et de remarquer que $\mathrm{Post}_S(X) = \mathrm{Pre}_{S^{-1}}(X)$. La proposition 6.7 montre que $\mathrm{taille}(S^{-1}) \leqslant (r+1).\mathrm{taille}(S)$ et le théorème 7.3 prouve alors le corollaire. □

Pour montrer que sans l'hypothèse "$S$ déterministe" on obtient une complexité exponentielle de $\mathcal{A}(\mathrm{Pre}_S(X'))$, on considère l'exemple suivant.

**Exemple 7.6**
*Soit* $S_1 = (\mathbb{N}^2, \{a\}, (\rightarrow_a))$ *le système à compteurs effectif et non déterministe défini par* $(x_1, x_2) \rightarrow_a (x'_1, x'_2)$ *si et seulement si* $x_1 = 0$ *et* $x'_2 = x_2$*.*

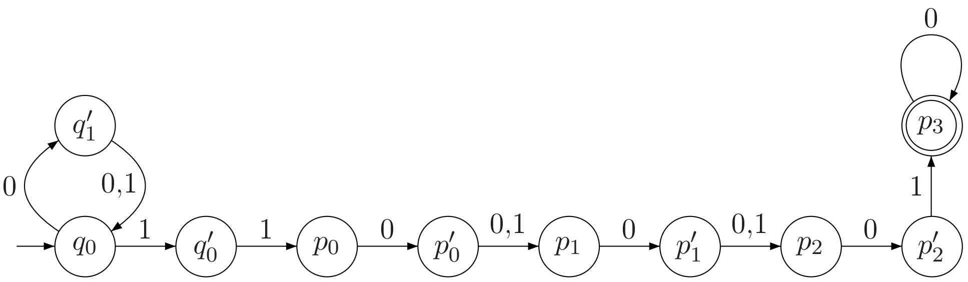
On va montrer qu'il existe une suite $(X'_n)_{n\geqslant 0}$ de parties de $\mathbb{N}^2$ représentables par des UBA, telle que $\mathcal{A}(\mathrm{Pre}_{S_1}(X'_n))$ a une taille exponentielle en la taille de $\mathcal{A}(X'_n)$. Pour cela, on considère les deux langages réguliers non ambigus $\mathcal{L}_n$ et $\mathcal{L}'_n$ définis par :

$$\mathcal{L}_n = (00+01)^*01(00+01)^n010^*$$
$$\mathcal{L}'_n = (00+01)^*11(00+01)^n010^*$$

**Lemme 7.7**
*La partie* $X'_n = \rho_2(\mathcal{L}'_n)$ *vérifie :*

$$\begin{cases} \lim_{n\to\infty} \mathrm{taille}(\mathcal{A}(X'_n)) = \infty \\ \mathrm{taille}(\mathcal{A}(X'_n)) \leqslant 7 + 2.n \end{cases}$$

**Figure 7.1** L'automate $\mathcal{A}_3$ sans l'état $q_\perp$




*Démonstration :*

Comme $\mathcal{L}'_n$ est un langage non ambigu, on a $\mathcal{L}(\mathcal{A}(X'_n)) = \mathcal{L}'_n$. Comme les langages $(\mathcal{L}_n)_{n\geqslant 0}$ sont deux à deux distincts, on a $\lim_{n\to\infty} \text{taille}(\mathcal{A}(X'_n)) = \infty$. Il suffit donc de construire un automate binaire déterministe et complet avec $(7 + 2.n)$ états reconnaissant le langage $\mathcal{L}'_n$. Considérons l'automate binaire $\mathcal{A}_n = (Q_n, \Sigma_r, \Delta_n, \{q_0\}, F_n)$ défini par (l'automate $\mathcal{A}_3$ est représenté à la figure 7.1) :

$$\left\{ \begin{array}{ll} Q_n = & \{q_0, q'_0, q_1, q_\perp, p_0\} \bigcup_{k=1}^{n+1}\{p'_{k-1}, p_k\} \\ \Delta_n = & \{q_0 \xrightarrow{0} q'_1 \xrightarrow{0,1} q_0, q_0 \xrightarrow{1} q'_0 \xrightarrow{1} p_0, q'_0 \xrightarrow{0} q_\perp\} \\ & \bigcup_{k=0}^{n-1}\{q_\perp \xleftarrow{1} p_k \xrightarrow{0} p'_k \xrightarrow{0,1} p_{k+1}\} \\ & \cup\{q_\perp \xleftarrow{1} p_n \xrightarrow{0} p'_n \xrightarrow{1} p_{n+1} \xrightarrow{0} p_{n+1} \xrightarrow{1} q_\perp, p'_n \xrightarrow{0} q_\perp\} \\ F_n = & \{q_n\} \end{array} \right.$$

Par construction $\mathcal{L}(\mathcal{A}_n) = \mathcal{L}'_n$ et $\text{taille}(\mathcal{A}_n) = \text{card}(Q_n) = 7 + 2.n$. □

**Lemme 7.8**
*La partie $X_n = \rho_2(\mathcal{L}_n)$ vérifie :*

$$\text{taille}(\mathcal{A}(X_n)) \geqslant 2^{n+1}$$

*Démonstration :*

Comme $\mathcal{L}_n$ est un langage non ambigu, on a $\mathcal{L}(\mathcal{A}(X'_n)) = \mathcal{L}_n$. Pour prouver le lemme, on va montrer que l'ensemble des résidus de $\mathcal{L}_n$ contient au moins $2^{n+1}$ éléments.

Considérons une suite $b_0$, ..., $b_n$ dans $\{0, 1\}$. On note $I = \{i \in \{0, \dots, n\};\ b_i = 1\}$ et $\sigma_I = 0b_0 \dots 0b_n$. Il suffit de prouver l'égalité suivante :

$$\sigma_I^{-1}.\mathcal{L}_n = (00 + 01)^*01(00 + 01)^n010^* \bigcup_{i\in I}(00 + 01)^i010^*$$

Pour tout $i \in I$, on a $\sigma_I(00+01)^i010^* = 0b_0 \dots 0b_{i-1}010b_{i+1} \dots 0b_n(00+01)^i010^* \subseteq (00+01)^*01(00+01)^n010^*$. Ainsi, $(00+01)^i010^* \subseteq \sigma_I^{-1}\mathcal{L}_n$. De plus, comme $\sigma_I(00+01)^*01(00+$

$01)^n010^* \subseteq (00+01)^*01(00+01)^n010^* = \mathcal{L}_n$, on a aussi prouver que $(00+01)^*01(00+01)^n010^* \subseteq \sigma_I^{-1}\mathcal{L}_n$. On a donc l'inclusion $(00+01)^*01(00+01)^n010^* \bigcup_{i\in I}(00+01)^i010^* \subseteq \sigma_I^{-1}\mathcal{L}_n$. Prouvons l'inclusion inverse. Soit $\sigma \in \sigma_I^{-1}.\mathcal{L}_n$. On a $\sigma_I\sigma \in \mathcal{L}_n$. Il existe un mot $w \in (00+01)^*$, un mot $w' \in (00+01)^n$ un entier $k \geqslant 0$ tel que $\sigma_I\sigma = w01w'010^k$. Commençons par le cas $|w| \geqslant |\sigma_I|$. Il existe $w'' \in (00+01)^*$ tel que $w = \sigma_I w''$. Ainsi, on a $\sigma = w''01w'010^k \in (00+01)^*01(00+01)^n010^*$. Considérons maintenant le cas $|w| < |\sigma_I|$. Comme $|w01w'| = |w|+2+2.n \geqslant 2(n+1) = |\sigma_I|$, il existe $u, v \in (00+01)^*$ tels que $w' = uv$ et $\sigma_I = w01u$. De $\sigma_I.\sigma = \sigma_I v010^k$, on déduit $\sigma = v010^k$. Comme $\sigma_I = w01u$, on a $\frac{|w|}{2} \in I$. De plus, de $|v| = |w'| - |u| = 2n - |u|$ et $\sigma_I = w01u$, on déduit $2(n+1) = |w| + |u| + 2$. Donc $|v| = |w|$. On a prouvé que $\sigma = v010^k \in (00+01)^{\frac{|w|}{2}}010^* \in \bigcup_{i\in I}(00+01)^i010^*$.
□

**Proposition 7.9**
*Il existe une suite $(X'_n)_{n\geqslant 0}$ de parties de $\mathbb{N}^2$ représentables par des automates binaires telle que :*

$$\begin{cases} \lim_{n\to\infty} \mathrm{taille}(\mathcal{A}(X'_n)) = \infty \\ \mathrm{taille}(\mathcal{A}(\mathrm{Pre}_{S_1}(X'_n))) \geqslant \left(\sqrt{2}\right)^{\mathrm{taille}(\mathcal{A}(X'_n))-3} \end{cases}$$

*Démonstration :*

Considérons les suites $(X'_n)_{n\geqslant 0}$ et $(X_n)_{n\geqslant 0}$ définies par $X_n = \rho_2((00+01)^*11(00+01)^n010^*)$ et $X'_n = \rho_2((00+01)^*01(00+01)^n010^*)$. Comme $X_n = \mathrm{Pre}_{S_1}(X'_n)$, on déduit des lemmes 7.7 et 7.8 la proposition. □

De la précédente proposition 7.9, on déduit un exemple de réseau de Petri reset/transfert $S_2$ pour lequel la taille de $\mathcal{A}(\mathrm{Post}_{S_2}(X))$ est exponentielle en taille$(\mathcal{A}(X))$.

**Exemple 7.10**
*Soit $S_2 = (\mathbb{N}^2, \{a\}, (\rightarrow_a))$ le réseau de Petri Reset/Transfert défini par $(x_1, x_2) \rightarrow_a (x'_1, x'_2)$ si et seulement si $x'_1 = 0$ et $x'_2 = x_2$.*

**Corollaire 7.11**
*Il existe une suite $(X_n)_{n\geqslant 0}$ de parties de $\mathbb{N}^2$ représentables par des automates binaires telle que :*

$$\begin{cases} \lim_{n\to\infty} \mathrm{taille}(\mathcal{A}(X_n)) = \infty \\ \mathrm{taille}(\mathcal{A}(\mathrm{Post}_{S_2}(X_n))) \geqslant \left(\sqrt{2}\right)^{\mathrm{taille}(\mathcal{A}(X_n))-3} \end{cases}$$

*Démonstration :*

Il suffit de remarquer que $S_2 = S_1^{-1}$ et d'appliquer la proposition 7.9. □

Dans cette section, on a donc montré que dans le cas des systèmes à compteurs effectifs et déterministes, le calcul de $\mathrm{Pre}_S(X')$ est en général plus facile que le calcul de $\mathrm{Post}_S(X)$. C'est une propriété intéressante car pour les systèmes à compteurs $S$ utilisés dans la pratique, la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k\geqslant 0}$ converge alors que la suite $(\mathrm{Post}_S^{\leqslant k}(X))_{k\geqslant 0}$ diverge ([EFM99],[FMP99],[FS01], [BM99] [BGP99] ,[BB03], [BB02]).

## 7.2 Taille asymptotique de $\mathrm{Pre}_S^{\leqslant k}(X')$

Le calcul en temps polynômial de $\mathcal{A}(\mathrm{Pre}_S(X'))$ en fonction de $\mathcal{A}(X')$ est une première étape vers un calcul effectif de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$. Cependant si à chaque itération, la taille de l'automate $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k+1}(X'))$ est doublée par rapport à la taille de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k})$, on obtient une taille en $k$ qui se trouve être exponentielle. Dans cette section, on va étudier la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))_{k\geqslant 0}$ en fonction de $k$ suivant deux approches :

- par une restriction globale au système : cas où le monoïde $\mathcal{M}_S$ est fini.
- par des restrictions locales au système : cas où chaque fonction affine laisse stables par image inverse les parties définissables dans une logique donnée.

Dans la pratique, on remarque que les trois logiques suivantes sont souvent utilisées pour décrire les relations $\rightarrow_a$ d'un système à compteurs $S$ et la partie $X'$ de $\mathbb{N}^m$ :

- Presburger,
- clos par le haut, et
- intervalle.

Dans la sous-section 7.2.1, on prouve que pour un système à compteurs effectif à monoïde fini et pour une partie $X'$ UBA-représentable, la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est polynomiale en $k$. Dans les sous-sections suivantes on prouve que cette la taille asymptotique en $k$ est respectivement exponentielle, constante et polynomiale pour la logique de Presburger (sous-section 7.2.2), pour les clos par le haut (sous-section 7.2.3) et pour la logique des intervalles (sous-section 7.2.4). Enfin, pour être exhaustifs, on étudie dans la sous-section 7.2.5 d'autres logiques pour lesquels $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ reste asymptotiquement exponentielle en $k$ comme dans le cas plus général de la logique de Presburger.

### 7.2.1 Cas des systèmes à compteurs à monoïde fini

On montre dans cette sous-section un résultat *inattendu* : la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est en $O(k^m)$ quelque soit le système à compteurs effectif à monoïde fini $S$ et quelque soit la partie $X'$ UBA-représentable.

**Lemme 7.12**
*Soit $X \subseteq \mathbb{N}^m$ une partie UBA-représentable, $M \in \mathcal{M}_m(\mathbb{Z})$, et $\alpha > 0$ un réel. Il existe une classe finie $\mathcal{C}_{X,M,\alpha}$ de parties de $\mathbb{N}^m$ telle que pour tout $v \in \mathbb{Z}^m$ et pour tout $w \in \Sigma_r^*$, on a :*

$$|w| \geqslant m.\frac{\ln(1+\alpha.\,||v||_\infty)}{\ln(r)} \implies \gamma_w^{-1}\left(M^{-1}(X-v)\right) \in \mathcal{C}_{X,M,\alpha}$$

*Démonstration :*

Soit $v \in \mathbb{Z}^m \backslash \{0\}$. Considérons le plus petit entier $k \geqslant \frac{\ln(1+\alpha.||v||_\infty)}{\ln(r)} - 1$. Comme $v \neq 0$, on a $k \geqslant 0$. Soit $w \in \Sigma_r^{m.k}$

$$\begin{aligned}\gamma_w^{-1}(M^{-1}(X-v)) &= \mathbb{N}^m \cap \left[\frac{1}{r^k}(M^{-1}(X-v)-\rho(w))\right]\\ &= \mathbb{N}^m \cap \left[M^{-1}(\frac{1}{r^k}(X-v-M.\rho(w)))\right]\end{aligned}$$

Comme de plus $X = \bigcup_{w' \in \Sigma^{m.k}} \gamma_{w'}(\gamma_{w'}^{-1}(X))$, on a :

$$\gamma_w^{-1}(M^{-1}(X-v)) = \bigcup_{w' \in \Sigma_r^{k.m}} \left( \mathbb{N}^m \cap M^{-1} \left( \gamma_{w'}^{-1}(X) + \frac{\rho(w') - v - M.\rho(w)}{r^k} \right) \right)$$

Considérons la partie $B = \{z \in \mathbb{Z}^m;\ ||z||_\infty \leqslant \frac{r}{\alpha} + m\}$ et montrons que pour tout $w' \in \Sigma_r^{m.k}$, si $\frac{\rho(w')-v-M.\rho(w)}{r^k} \notin B$, alors $\mathbb{N}^m \cap M^{-1}\left(\gamma_{w'}^{-1}(X) + \frac{\rho(w')-v+M.\rho(w)}{r^k}\right)$ est vide. Par contraposition, supposons ce dernier ensemble non vide. Il existe alors $y \in \gamma_{w'}^{-1}(X)$ et $z \in \mathbb{N}^m$ tels que $y + \frac{\rho(w')-v-M.\rho(w)}{r^k} = M.z$. En particulier $\frac{\rho(w')-v-M.\rho(w)}{r^k} \in \mathbb{Z}^m$. Pour montrer que $z \in B$, il suffit de donner la majoration suivante :

$$\begin{aligned} \left|\left|\frac{\rho(w') - v - M.\rho(w)}{r^k}\right|\right|_\infty &\leqslant \frac{(r^k-1) + \frac{1}{\alpha}.(r^{k+1}-1) + m.\,||M||_\infty.(r^k-1)}{r^k} \\ &< 1 + \frac{r}{\alpha} + m.\,||M||_\infty \end{aligned}$$

Considérons la partie $U_{w,v}^k \subseteq Q(X) \times B$ définie par :

$$U_{w,v}^k = \left\{ (q,b) \in Q(X) \times B;\ \exists w' \in \Sigma_r^{k.m};\ q = \gamma_{w'}^{-1}(X) \text{ et } \frac{\rho(w') - v - M.\rho(w)}{r^k} = b \right\}$$

On a alors :

$$\gamma_w^{-1}(M^{-1}(X-v)) = \bigcup_{(q,b) \in U_{w,v}^k} \mathbb{N}^m \cap M^{-1}(q+b)$$

On considère la classe $\mathcal{C}_{X,M,\alpha}$ de $\mathbb{N}^m$ définie par :

$$\mathcal{C}_{X,M,\alpha} = \left\{ \bigcup_{(q,b) \in F} \gamma_{w''}^{-1}(M^{-1}(q+b));\ w'' \in \Sigma_r^{<m};\ F \subseteq Q(X) \times B \right\}$$

Par construction $\mathcal{C}_{X,M,\alpha}$ convient. □

**Proposition 7.13**
*Pour tout système à compteurs $S$ à monoïde fini, il existe deux entiers $c_S, d_S \in \mathbb{N}^*$ tels que pour tout mot $\sigma \in \Sigma^*$, on a*

$$\begin{cases} d_S.v_\sigma \in \mathbb{Z}^m \\ d_S.M_\sigma \in \mathcal{M}_m(\mathbb{Z}) \\ ||d_S.v_\sigma||_\infty \leqslant c_S.|\sigma| \end{cases}$$

*Démonstration :*

Remarquons qu'il existe un entier $d_S \in \mathbb{N}^*$ tel que pour tout $M \in \mathcal{M}_S$ et pour tout $a \in \Sigma$, on a $d_S.M.v_a \in \mathbb{Z}^m$ et $d_S.M \in \mathcal{M}_m(\mathbb{Z})$. Pour montrer que $d_S$ convient, considérons un mot $\sigma \in \Sigma^*$. Une récurrence sur la longueur de $\sigma$ montre qu'il existe une suite $(M_i, v_{a_i})_{1 \leqslant i \leqslant |\sigma|}$ de $\mathcal{M}_S \times \Sigma$ telle que $v_\sigma = \sum_{i=1}^{|\sigma|} M_i.v_{a_i}$. Ainsi $d_S.v_\sigma \in \mathbb{Z}^m$ et $||d_S.v_\sigma||_\infty \leqslant c_S.|\sigma|$ où $c_S = \max\{||M.v_a||_\infty;\ (M,a) \in \mathcal{M}_S \times \Sigma\}$. Enfin, comme $M_\sigma \in \mathcal{M}_S$, on a bien $d_S.M_\sigma \in \mathcal{M}_m(\mathbb{Z})$. □

**Proposition 7.14**
*Soit $S$ un système à compteurs à monoïde fini. Il existe une classe finie $\mathcal{C}_S$ de parties de $\mathbb{N}^m$ telle que pour tout $w \in \Sigma_r^*$ et pour tout $\sigma \in \Sigma^*$, on a :*

$$|w| \geqslant m.\frac{\ln(1+|\sigma|)}{\ln(r)} \implies \gamma_w^{-1}(D_\sigma) \in \mathcal{C}_S$$

*Démonstration :*

Considérons un système à compteurs à monoïde fini $(S, (M_a, v_a)_{a\in\Sigma})$ définis sur des domaines UBA-réprésentables $D_a$ et une partie $X'$ UBA-représentable. On note $g_\sigma : \mathbb{Q}^m \to \mathbb{Q}^m$ la fonction affine définie par $g_\sigma(x) = M_\sigma.x + v_\sigma$ pour tout $x \in \mathbb{Q}^m$. On considère des entiers $c_S, d_S \in \mathbb{N}^*$ vérifiant la proposition 7.13.

Considérons une suite $(a_i)_{1\leqslant i\leqslant n}$ avec $n \geqslant 1$ de $\Sigma$ et posons $\sigma = a_1 \dots a_n$. On pose $\sigma_0 = \varepsilon$ et $\sigma_i = a_1 \dots a_i$ pour $i \in \{1, \dots, n\}$. La partie $I_{(M,a)}(\sigma) = \{i \in \{1, \dots, |\sigma|\};\ M_{\sigma_{i-1}} = M;\ a_i = a\}$ permet de décrire facilement le domaine de définition $D_\sigma$ de la fonction $f_\sigma$ :

$$\begin{aligned} D_\sigma &= g_0^{-1}(D_{a_1}) \cap g_1^{-1}(D_{a_2}) \cap \dots \cap g_{k'-1}^{-1}(D_{a_{k'}}) \\ &= \bigcap_{\substack{(M,a) \\ i\in I_{(M,a)(\sigma)}}} (d_S.M)^{-1}(d_S.D_a - d_S.v_{\sigma_{i-1}}) \end{aligned}$$

Pour chaque couple $(M, a) \in \mathcal{M}_S \times \Sigma$, on considère une classe finie $\mathcal{C}_{d_S.D_a, d_S.M, c_S^{-1}}$ de parties de $\mathbb{N}^m$ vérifiant le lemme 7.12. Considérons $w \in \Sigma_r^*$ tel que $|w| \geqslant m.\frac{\ln(1+|\sigma|)}{\ln(r)}$. Comme pour tout $(M, a) \in \mathcal{M}_S \times \Sigma$ et pour tout $i \in I_{(M,a)}(\sigma)$, on a $c_S^{-1}.\,||d_S.v_i||_\infty \leqslant |\sigma|$, on déduit $\gamma_w^{-1}((d_S.M)^{-1}(d_S.D_a - d_S.v_{\sigma_{i-1}})) \in \mathcal{C}_{d_S.D_a, d_S.M, c_S^{-1}}$. Ainsi, on a prouvé que $\gamma_w^{-1}(D_\sigma)$ est dans la classe finie $\mathcal{C}_S$ de parties de $\mathbb{N}^m$ définie par :

$$\mathcal{C}_S = \left\{ \bigcap_{Y\in F} Y;\ F \subseteq \bigcup_{M,a} \mathcal{C}_{d_S.D_a, d_S.M, c_S^{-1}} \right\}$$

On a ainsi prouvé la proposition. □

**Proposition 7.15**
*Soit $S$ un système à compteurs effectif à monoïde fini et $X'$ une partie UBA-représentable. Il existe une classe finie $\mathcal{C}_{S,X'}$ de parties de $\mathbb{N}^m$, telle que pour tout $k \geqslant 0$ et pour tout $w \in \Sigma_r^*$, on a :*

$$|w| \geqslant m.\frac{\ln(1+k)}{\ln(r)} \implies \gamma_w^{-1}(\mathrm{Pre}_S^{\leqslant k}(X')) \in \mathcal{C}_{S,X'}$$

*Démonstration :*

On considère des entiers $c_S, d_S \in \mathbb{N}^*$ vérifiant la proposition 7.13 et on considère une classe finie $\mathcal{C}_S$ de parties de $\mathbb{N}^m$ vérifiant la proposition 7.14. Comme $\mathrm{Pre}_S^{\leqslant k}(X') =$

$\bigcup_{\sigma\in\Sigma^{\leqslant k}} g_\sigma^{-1}(X')\cap D_\sigma$, on obtient l'égalité suivante :

$$\begin{aligned}\mathrm{Pre}_S^{\leqslant k}(X') &= \bigcup_{\sigma\in\Sigma^{\leqslant k}} g_\sigma^{-1}(X')\cap D_\sigma\\ &= \bigcup_{\sigma\in\Sigma^{\leqslant k}} \big([(d_S.M_\sigma)^{-1}(d_S.X'-d_S.v_\sigma)]\cap D_\sigma\big)\end{aligned}$$

Pour chaque $M'\in\mathcal{M}_S$, on considère une classe finie $\mathcal{C}_{d_S.X',d_S.M',c_S^{-1}}$ de parties de $\mathbb{N}^m$ vérifiant le lemme 7.12. Considérons $w\in\Sigma_r^*$ tel que $|w|\geqslant m.\frac{\ln(1+|\sigma|)}{\ln(r)}$. On a alors $\gamma_w^{-1}(D_\sigma)\in\mathcal{C}_S$ et comme $||d_S.v_\sigma||_\infty\leqslant c_S.|\sigma|$, on a $\gamma_w^{-1}((d_S.M_\sigma)^{-1}(d_S.X'-d_S.v_\sigma))\in\mathcal{C}_{d_S.X',d_S.M_\sigma,c_S^{-1}}$. Considérons les classes finies $\mathcal{C}_0$ et $\mathcal{C}_{S,X'}$ de parties de $\mathbb{N}^m$ définies par :

$$\begin{cases}\mathcal{C}_0=\{X\cap Y;\ X\in\bigcup_{M'\in\mathcal{M}_S}\mathcal{C}_{d_S.X',d_S.M',c_S^{-1}};\ Y\in\mathcal{C}_S\}\\ \mathcal{C}_{S,X'}=\{\bigcup_{Z\in F}Z;\ F\subseteq\mathcal{C}_0\}\end{cases}$$

On a prouvé que $\gamma_w^{-1}(\mathrm{Pre}_S^{\leqslant k}(X'))\in\mathcal{C}_{S,X'}$. □

**Remarque 7.16**
*La proposition précédente nous donne la structure de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$. En effet, on déduit de cette proposition, l'existence d'un ensemble fini d'UBA $\mathcal{C}_{S,X'}$ tel que pour tout $k\geqslant 0$, l'UBA $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est un BDD dont chaque feuille est un UBA de $\mathcal{C}_{S,X'}$. Cela explique pourquoi l'implémentation récente des UBA par Jean-Michel Couvreur (article soumis à TACAS'03), utilisant des méthodes "à la BDD" (permettant la mise en place de cache de calculs), obtient de si bon résultats comparés à une implémentation classique comme celle de* FAST, LASH *ou* MONA *(cette bibliothèque d'automates sera très prochainement implémentée dans l'outil* FAST*).*

On peut alors prouver le théorème *inattendu* suivant :

**Théorème 7.17**
*Soit $S$ un système à compteurs effectif à monoïde fini et $X'$ une partie UBA-représentable. La taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est en $O(k^m)$.*

*Démonstration :*
On considère une classe finie $\mathcal{C}_{S,X'}$ de parties de $\mathbb{N}^m$ vérifiant la proposition 7.15. On a alors taille$(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X')))\leqslant\frac{1}{r-1}(1+k)^m+\mathrm{card}(\mathcal{C}_{S,X'})$. Ainsi, taille$(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X')))$ est en $O(k^m)$. □

**Remarque 7.18**
*En utilisant dans la preuve du théorème précédent, le résultat prouvé dans [CP89], nous pensons qu'une majoration plus fine en $O(\frac{k^m}{\ln(k)})$ peut être obtenue.*

### 7.2.2 Calcul exponentiel dans la logique de Presburger

On s'intéresse à la classe des systèmes à compteurs affine utilisant des fonctions affines laissant stables par image inverse les parties Presburger-définissables. Pour cette classe de systèmes à compteurs, on montre que la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est en général exponentielle en $k$.

**Proposition 7.19**
*Soit $f : D \rightarrow \mathbb{N}^m$ une fonction affine définie sur une partie $D$ de $\mathbb{N}^m$. Les deux assertions suivantes sont équivalentes :*
- *Le domaine de définition $D$ est Presburger-définissable.*
- *Pour tout $X' \subseteq \mathbb{N}^m$ Presburger-définissable, $f^{-1}(X')$ est Presburger-définissable.*

*Démonstration :*
Une des implications est évidente. En effet, si pour tout $X'$ Presburger-définissable, $f^{-1}(X')$ est Presburger-définissable alors en particulier, comme $X' = \mathbb{N}^m$ est Presburger-définissable, la partie $D = f^{-1}(\mathbb{N}^m)$ est Presburger-définissable. Montrons l'autre implication. Pour cela, on considère une fonction affine $f$ telle que $D$ est Presburger-définissable et une partie $X'$ Presburger-définissable. Montrons que $f^{-1}(X')$ est Presburger-définissable. Comme $f$ est affine, il existe une matrice carrée $M \in \mathcal{M}_m(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^m$ tels que $f(x) = M.x+v$ pour tout $x \in D$. De plus, comme $D$ et $X'$ sont Presburger-définissables, il existe une formule $\phi_D(x)$ et une formule $\phi'(x')$ représentant respectivement $D$ et $X'$. Remarquons que la formule de Presburger $\exists x' \, [\phi_D(x) \wedge (M.x+v = x') \wedge \phi'(x')]$ représente $f^{-1}(X')$. □

Du théorème 7.3, on déduit le corollaire suivant.

**Corollaire 7.20**
*Soit $S$ un système à compteurs affine dont les domaines de définition sont Presburger-définissables et soit $X'$ une partie Presburger-définissable. Il existe un entier $c \geqslant 1$ tel que pour tout $k \geqslant 0$ :*

$$\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X')) \leqslant c^k$$

*Démonstration :*
Le théorème 7.3 montre que pour tout automate binaire non ambigu $\mathcal{A}'$, il existe un automate binaire non ambigu $\mathcal{A}$ représentant $\mathrm{Pre}_S^{\leqslant 1}(\rho_m(\mathcal{L}(\mathcal{A}')))$ tel que $\mathrm{taille}(\mathcal{A}) \leqslant (\mathrm{taille}(\mathcal{A}')+1)^{\mathrm{taille}(S)+1}$. Posons $c' = (\mathrm{taille}(S)+1).\frac{\ln(3)}{\ln(2)}$ et remarquons que pour tout $x \geqslant 2$, on a $(x+1)^{\mathrm{taille}(S)+1} \leqslant x^{c'}$. Une récurrence montre que pour tout $k \geqslant 0$, on a $\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))) \leqslant (\mathrm{taille}(\mathcal{A}(X'))+2)^{k.c'}$. En posant $c = (\mathrm{taille}(\mathcal{A}(X'))+2)^{c'}$, on obtient la preuve du corollaire. □

On peut montrer que cette borne exponentielle est optimale dans le cas général en considérant l'exemple suivant.

**Exemple 7.21**
*Soit $S_3 = (\mathbb{N}^2, \{a\}, (\rightarrow_a))$ le système à compteurs affine défini par $f_a(x_1, x_2) = (r.x_1, x_2)$ sur $D_a = \mathbb{N}^2$.*

**Proposition 7.22**
*Soit $X' = \{(x'_1, x'_2) \in \mathbb{N}^2;\ x'_1 = x'_2\}$. Pour tout entier $k \geqslant 0$, on a*

$$\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_{S_3}^{\leqslant k}(X'))) \geqslant r^{k-1}$$

*Démonstration :*

Considérons la partie $X_i$ de $\mathbb{N}^2$ définie par $X_i = \{(x, r^i.x);\ x \in \mathbb{N}\}$. Une récurrence immédiate montre que $\mathrm{Pre}_{S_3}^{\leqslant k}(X') = \bigcup_{i=0}^{k} X_i$. Supposons par l'absurde qu'il existe un automate binaire non ambigu $\mathcal{A} = (Q, \Sigma_r, \delta, \{q_0\}, F)$ représentant $\mathrm{Pre}_{S_3}^{\leqslant k}(X')$ et tel que $\mathrm{taille}(Q) < r^{k-1}$. Soit $\mathcal{L} = (00 + \cdots + (r-1)0)^{k-1}10$. Comme $\mathrm{card}(Q) < r^{k-1} = \mathrm{card}(\mathcal{L})$, il existe deux mots $\sigma \neq \sigma'$ dans $\mathcal{L}$ tels que $\delta(q_0, \sigma) = \delta(q_0, \sigma')$. Soient $y, y'$ les deux entiers de $\mathbb{N}$ tels que $\rho_2(\sigma) = (y, 0)$ et $\rho_2(\sigma') = (y', 0)$. On a $y, y' \in \{r^{k-1}, \ldots, r^k - 1\}$. Considérons le mot $w \in \Sigma_r^*$ tel que $\rho_2(w) = (0, y)$. De $\rho_2(\sigma w) = \rho_2(\sigma) + r^k.\rho_2(w) = (y, r^k.y)$, on déduit $\rho_2(\sigma w) \in X_k$. Comme $\mathcal{A}$ est un automate binaire non ambigu représentant $\bigcup_{i=0}^{k} X_i$, on a $\sigma w \in \mathcal{L}(\mathcal{A})$. De $\delta(q_0, \sigma) = \delta(q_0, \sigma')$, on déduit $\sigma' w \in \mathcal{L}(\mathcal{A})$. Donc $(y', r^k.y) = \rho_2(\sigma' w) \in \bigcup_{i=0}^{k} X_i$. Il existe donc $i \in \{0, \ldots, k\}$ tel que $(y', r^k.y) \in X_i$. On a donc $r^k.y = r^i.y'$. De $y \geqslant r^{k-1}$ et $y' < r^k$, on déduit $i > k-1$. Donc $i = k$. On a prouvé que $y = y'$ Comme $\sigma$ et $\sigma'$ sont deux mots de même longueur représentant le même vecteur, le lemme 4.32 montre que $\sigma = \sigma'$. On a donc une contradiction. $\square$

### 7.2.3 Cas clos par le haut

Les systèmes à compteurs affines dont les domaines de définition sont clos par le haut font partis de la classe des "systèmes dits bien structurés" [FMP99], [FS01], [FPS00] [AJ93]. Pour ces systèmes à compteurs $S$ et pour tout $X'$ clos par le haut, la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k \geqslant 0}$ est stationnaire et il existe ainsi un entier $k \geqslant 0$ tel que $\mathrm{Pre}_S^*(X') = \mathrm{Pre}_S^{\leqslant k}(X')$.

**Remarque 7.23**
*Les clos par le haut de $\mathbb{N}^m$ peuvent être représentés de façon concise par des "Covering Sharing Trees" CST ([DRB02] [Bab] [DRV01]). On va montrer que la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k \geqslant 0}$ est stationnaire. Ainsi, la taille asymptotique en $k$ des CST est stationnaire.*

Après avoir caractérisé les fonctions affines laissant stables par image inverse les clos par le haut, on montrera que la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est constante.

**Proposition 7.24**
*Soit $f : D \to \mathbb{N}^m$ une fonction affine définie sur une partie $D$ de $\mathbb{N}^m$. Les deux assertions suivantes sont équivalentes :*
- *Le domaine de définition $D$ est clos par le haut.*
- *Pour tout $X' \subseteq \mathbb{N}^m$ clos par le haut, $f^{-1}(X')$ est clos par le haut.*

*Démonstration :*

Une des implications est évidente. En effet, si pour tout $X'$ clos par le haut, $f^{-1}(X')$ est clos par le haut, alors en particulier, comme $X' = \mathbb{N}^m$ est clos par le haut, $D = f^{-1}(\mathbb{N}^m)$ est clos par le haut. Montrons l'autre implication. Pour cela, on considère une fonction affine $f$ telle que $D$ est clos par le haut et un clos par le haut $X'$. Montrons que $f^{-1}(X')$ est clos par le haut. On peut supposer que $f^{-1}(X') \neq \emptyset$. Il existe une matrice carrée $M \in \mathcal{M}_m(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^m$ tels que $f(x) = M.x + v$ pour tout $x \in D$. On commence par prouver que $M \in \mathcal{M}_m(\mathbb{N})$. Comme $f^{-1}(X') \neq \emptyset$, en particulier $D \neq \emptyset$ et il existe un vecteur $d_0 \in D$. Pour tout $i \in \{1, \ldots, m\}$, comme $d_0$ est dans le clos par le haut $D$, on a $d_0 + \mathbb{N}.e_i \subseteq D$. Ainsi $M.d_0 + v + \mathbb{N}.M.e_i \subseteq \mathbb{N}^m$. En particulier, on a $M.e_i \in \mathbb{N}^m$. On a donc bien prouvé que $M \in \mathcal{M}_m(\mathbb{N})$. Considérons alors $x \in f^{-1}(X')$, $z \in \mathbb{N}^m$ et montrons que $x + z \in f^{-1}(X')$. Comme $x \in f^{-1}(X')$, on a $x \in D$. Comme de plus $D$ est clos par le haut, on a $x + z \in D$. La fonction affine $f$ est donc définie au point $x + z$. On a de plus $f(x + z) = f(x) + M.z$. Comme $M.z \in \mathbb{N}^m$ et que $f(x)$ est un élément du clos par le haut $X'$, on a $f(x) + M.z \in X'$. Ainsi, $f(x + z) \in X'$ et on a prouvé que $x + z \in f^{-1}(X')$. La partie $f^{-1}(X')$ est donc close par le haut. □

**Théorème 7.25**
*Soit $S$ un système à compteurs affine dont les domaines de définition sont clos par le haut et soit $X'$ un clos par le haut. Il existe un entier $c \geqslant 1$ tel que pour tout $k \geqslant 0$ :*

$$\text{taille}(\mathcal{A}(\text{Pre}_S^{\leqslant k}(X'))) \leqslant c$$

*Démonstration :*

Il suffit de montrer que la suite $(\text{Pre}_S^{\leqslant k}(X'))_{k \geqslant 0}$ est stationnaire. D'après la proposition 7.24, c'est une suite de clos par le haut. Or, d'après [FS01], une suite croissante de clos par le haut est stationnaire. □

**Remarque 7.26**
*Trouver une borne élémentaire en* taille($S$) *et en* taille($\mathcal{A}(X')$) *du plus petit entier $k \geqslant 0$ tel que $\text{Pre}_S^{\leqslant k}(X') = \text{Pre}_S^*(X')$ est un problème ouvert. Rappelons que dans le cas des "lossy channel systems" (une classe de systèmes bien structurés), le plus petit entier $k \geqslant 0$ tel que $\text{Pre}_S^{\leqslant k}(X') = \text{Pre}_S^*(X')$ est non primitif récursif ([Sch02]).*

**Problème ouvert 7.27**
*Soit $S$ un système à compteurs affine dont les domaines de définition sont clos par le haut et soit $X'$ un clos par le haut. Montrer que l'on ne peut pas borner le plus petit $k \geqslant 0$ tel que $\text{Pre}_S^{\leqslant k}(X') = \text{Pre}_S^*(X')$ par une fonction élémentaire en* taille($S$) *et en* taille($\mathcal{A}(X')$).

### 7.2.4 Calcul polynomial dans la logique des intervalles

On s'intéresse à la classe des systèmes à compteurs affine utilisant des fonctions affines laissant stables par image inverse les parties intervalle-définissables. Pour cette classe de systèmes à compteurs, et pour une partie $X'$ intervalle-définissable, on montre que la taille asymptotique de $\mathcal{A}(\text{Pre}_S^{\leqslant k}(X'))$ est polynomiale en $k$.

**Remarque 7.28**
*Rappelons que la logique des intervalles est suffisamment expressive pour définir la plupart*

*des domaines de définition de la grande majorité des systèmes à compteurs utilisés dans la pratique (33 des 40 exemples analysés avec* FAST *sont ainsi défini).*

**Remarque 7.29**
*Les parties de $\mathbb{N}^m$ intervalle-définissables peuvent être représentées canoniquement par des "Interval Decision Diagrams" (IDD), une représentation canonique utilisant les mêmes techniques que les BDD ([ST98]). Cette représentation semble avoir une bonne complexité en pratique ([Str98]). Cependant, comme notre objectif est d'estimer la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ pour différentes logiques, on n'étudiera pas dans cette thèse les IDD.*

#### 7.2.4.1 Granularité et automate binaire

On montre dans cette sous-section que pour toute formule $\phi$, dans la logique des intervalles, représentant une partie $X \subseteq \mathbb{N}^m$, on peut majorer la taille de l'automate $\mathcal{A}(X)$ en fonction du plus grand entier utilisé dans $\phi$.

**Définition 7.30**
*La granularité d'une partie $X$ intervalle-définissable est le plus petit entier noté $\mathrm{gran}(X) \geqslant 0$ tel qu'il existe une formule $\phi$ dans la logique des intervalles où $c < \mathrm{gran}(X)$, définissant $X$ :*

$$\phi := v_i = c|\phi \vee \phi|\phi \wedge \phi|\neg\phi|true|false$$

Pour faire des raisonnements sur des parties $X$ intervalle-définissables, on introduit la notion de bloc et on montre que toute partie intervalle-définissable peut se décomposer comme une union finie de blocs.

**Définition 7.31**
*Un bloc $X$ est une partie définie par une formule de la forme $\bigwedge_{j \in J_=}(v_j = c_j) \bigwedge_{j \in J_{\neq}}(v_j \neq c_j)$ où $J_=$ et $J_{\neq}$ sont deux sous-ensembles disjoints de $\{1, \ldots, m\}$.*

**Lemme 7.32**
*Toute partie $X$ intervalle-définissable peut se décomposer en une union finie de blocs de granularités bornées par $\mathrm{gran}(X)$.*

*Démonstration :*
Considérons une partie $X$ intervalle-définissable. Il existe alors une formule $\phi$ dans la logique des intervalles où $c < \mathrm{gran}(X)$ représentant $X$ :

$$\phi := v_i = c|\phi \vee \phi|\phi \wedge \phi|\neg\phi|true|false$$

En développant une telle formule, on fait apparaître une disjonction de formules de la forme $\bigwedge_{j \in J_=}(v_j = c_j) \bigwedge_{j \in J_{\neq}}(v_j \neq c_j)$ où $J_= \cap J_{\neq} = \emptyset$. □

De cette décomposition, on va déduire facilement que les opérations ensemblistes sur les parties intervalle-définissables ne font que décroître la granularité.

**Proposition 7.33**
*Soient $X, X' \subseteq \mathbb{N}^m$ des parties intervalle-définissables, $i \in \{1, \ldots, m\}$, $\sigma \in \Sigma_r^m$ et $b \in \Sigma_r$. On a :*

$$\begin{cases} \mathrm{gran}(X \cup X') \leqslant \max(\mathrm{gran}(X), \mathrm{gran}(X')) \\ \mathrm{gran}(X \cap X') \leqslant \max(\mathrm{gran}(X), \mathrm{gran}(X')) \\ \mathrm{gran}(\mathbb{N}^m \backslash X) = \mathrm{gran}(X) \\ \mathrm{gran}(\Pi_i(X)) \leqslant \mathrm{gran}(X) \\ \mathrm{gran}(\gamma_\sigma^{-1}(X)) \leqslant \frac{\mathrm{gran}(X)-1}{r} + 1 \\ \mathrm{gran}(\gamma_b^{-1}(X)) \leqslant \mathrm{gran}(X) \end{cases}$$

*Démonstration :*

Remarquons que si $X$ et $X'$ sont représentées respectivement par les formules $\phi$ et $\phi'$, les parties $X \cup X'$, $X \cap X'$ et $\mathbb{N}^m \backslash X$ sont respectivement représentées par les formules $\phi \vee \phi'$, $\phi \wedge \phi'$ et $\neg \phi$. Ainsi, on a bien $\mathrm{gran}(X \cup X') \leqslant \max(\mathrm{gran}(X), \mathrm{gran}(X'))$, $\mathrm{gran}(X \cap X') \leqslant \max(\mathrm{gran}(X), \mathrm{gran}(X'))$ et $\mathrm{gran}(\mathbb{N}^m \backslash X) \leqslant \mathrm{gran}(X)$. Par symétrie, on déduit de $\mathrm{gran}(\mathbb{N}^m \backslash X) \leqslant \mathrm{gran}(X)$, l'égalité $\mathrm{gran}(\mathbb{N}^m \backslash X) = \mathrm{gran}(X)$.

Montrons que $\mathrm{gran}(\Pi_i(X)) \leqslant \mathrm{gran}(X)$. D'après le lemme 7.32, on peut supposer que $X$ est un bloc représenté par une formule de la forme $\bigwedge_{j \in J_=} (v_j = c_j) \bigwedge_{j \in J_{\neq}} (v_j \neq c_j)$ où $J_= \cap J_{\neq} = \emptyset$ et $c_j < \mathrm{gran}(X)$ pour tout $j \in J_= \cup J_{\neq}$. Il suffit alors de remarquer que $\Pi_i(X)$ est représenté par la formule $\bigwedge_{j \in J_= \backslash \{i\}} (v_j = c_j) \bigwedge_{j \in J_{\neq} \backslash \{i\}} (v_j \neq c_j)$.

Montrons que $\mathrm{gran}(\gamma_\sigma^{-1}(X)) \leqslant \frac{\mathrm{gran}(X)-1}{r} + 1$. Comme pour toute partie $X$ et $X'$ de $\mathbb{N}^m$, on a $\gamma_\sigma^{-1}(X \cup X') = \gamma_\sigma^{-1}(X) \cup \gamma_\sigma^{-1}(X')$, $\gamma_\sigma^{-1}(X \cap X') = \gamma_\sigma^{-1}(X) \cap \gamma_\sigma^{-1}(X')$, et $\gamma_\sigma^{-1}(\mathbb{N}^m \backslash X) = \mathbb{N}^m \backslash \gamma_\sigma^{-1}(X)$, on peut supposer que $X$ est de la forme $X = \{x \in \mathbb{N}^m;\ x_i = c\}$ où $c \geqslant 0$ et $i \in \{1, \ldots, m\}$. On a a $\mathrm{gran}(X) = c + 1$. Soit $(b_i)_{1 \leqslant i \leqslant m}$ une suite de $\Sigma_r$ telle que $\sigma = b_1 \ldots b_m$. On a alors $\gamma_\sigma^{-1}(X) = \{x \in \mathbb{N}^m; x_i = \frac{c - b_i}{r}\}$. Ainsi, si $c - b_i$ n'est pas divisible par $r$, on a $\gamma_\sigma^{-1}(X) = \emptyset$ et donc $\mathrm{gran}(\gamma_\sigma^{-1}(X)) = 0$. Si $c - b_i$ est divisible par $r$, on a $\mathrm{gran}(\gamma_\sigma^{-1}(X)) = \frac{c - b_i}{r} + 1 \leqslant \frac{\mathrm{gran}(X)-1}{r} + 1$.

Montrons enfin que $\mathrm{gran}(\gamma_b^{-1}(X)) \leqslant \mathrm{gran}(X)$. Comme dans le cas précédent, on peut supposer que $X = \{x \in \mathbb{N}^m;\ x_i = c\}$. On divise la preuve en deux cas $i = m$ et $i < m$. Remarquons que si $i < m$ alors $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ x_{i+1} = c\}$ et on a bien $\mathrm{gran}(\gamma_b^{-1}(X) \leqslant \mathrm{gran}(X)$. Considérons donc le cas $i = m$. On a $\gamma_b^{-1}(X) = \{x \in \mathbb{N}^m;\ x_1 = \frac{c-b}{r}\}$. Ainsi, si $c - b$ n'est pas divisible par $r$, on a a $\gamma_b^{-1}(X) = \emptyset$ et dans ce cas $\mathrm{gran}(\gamma_b^{-1}(X)) = 0 \leqslant \mathrm{gran}(X)$, et si $c - b$ est divisible par $r$, on a $\mathrm{gran}(\gamma_b^{-1}(X)) = \frac{c-b}{r} \leqslant \mathrm{gran}(X)$. □

La proposition précédente montre en particulier que la granularité des résidus de $X$ est bornée par la granularité de $X$. On va montrer que la taille de $\mathcal{A}(X)$ est majorée par $(r.(\mathrm{gran}(X) + 1))^m$.

**Définition 7.34**
*Pour toute partie $X$ de $\mathbb{N}^m$, pour toute partie $I \subseteq \{1, \ldots, m\}$ et pour tout $n \geqslant 0$, on définie la partie $X_{I,n} \subseteq X$ par :*

$$X_{I,n} = \{x \in \mathbb{N}^m;\ \forall i \in I\ x_i = n;\ \forall i \notin I\ x_i < n\}$$

**Proposition 7.35**
*Pour toute partie $X$ intervalle-définissable et pour tout entier $n \geqslant \mathrm{gran}(X)$, on a :*

$$X = \bigcup_{I \subseteq \{1,\dots,m\}} X_{I,n} + \sum_{i \in I} \mathbb{N}.e_i$$

*Démonstration :*

On commence par prouver la proposition dans le cas d'un bloc $X$ représentée par une formule de la forme $\phi = \bigwedge_{j \in J_=} (v_j = c_j) \bigwedge_{j \in J_{\neq}} (v_j \neq c_j)$ où $J_= \cap J_{\neq} = \emptyset$ et où $c_j < \mathrm{gran}(X)$ pour tout $j \in J_= \cup J_{\neq}$. Considérons $x \in X$ et montrons que $x \in \bigcup_{I \subseteq \{1,\dots,m\}} X_{I,n} + \sum_{i \in I} \mathbb{N}.e_i$. Considérons $I = \{i \in \{1,\dots,m\};\ x_i \geqslant n\}$. Comme pour tout $j \in J_=$, on a $x_j = c_j < \mathrm{gran}(X) \leqslant n$, on déduit $I \subseteq \{1,\dots,m\} \backslash J_=$. Considérons le vecteur $y$ défini par $y_i = n$ si $i \in I$ et par $y_i = x_i$ sinon. Comme $x$ vérifie la formule $\phi$, le vecteur $y$ vérifie aussi la formule $\phi$. On a donc $y \in X_{I,n}$. De $x \in y + \sum_{i \in I} \mathbb{N}.e_i$, on déduit $x \in \bigcup_{I \subseteq \{1,\dots,m\}} X_{I,n} + \sum_{i \in I} \mathbb{N}.e_i$. Réciproquement, considérons $x \in \bigcup_{I \subseteq \{1,\dots,m\}} X_{I,n} + \sum_{i \in I} \mathbb{N}.e_i$ et montrons que $x \in X$. Il existe $I \subseteq \{1,\dots,m\}$ et $y \in X_{I,n}$ tels que $x \in y + \sum_{i \in I} \mathbb{N}.e_i$. Comme $y \in X_{I,n} \subseteq X$, le vecteur $y$ vérifie la formule $\phi$. Ainsi, pour tout $i \in I$, comme $y_i = n \geqslant \mathrm{gran}(X)$, on a $I \subseteq \{1,\dots,m\} \backslash J_=$. De $x \in y + \sum_{i \in I} \mathbb{N}.e_i$, on déduit que $x$ vérifie la formule $\phi$. On a donc $x \in X$.

Considérons alors le cas général d'une partie $X$ intervalle-définissable. D'après le lemme 7.32, la partie $X$ est une union finie de blocs $X = \bigcup_{k \in K} X_k$ tels que $\mathrm{gran}(X_k) \leqslant \mathrm{gran}(X)$. De $X_{I,n} = \bigcup_{k \in K} (X_k)_{I,n}$ et du cas précédent, on déduit la proposition. □

**Remarque 7.36**
*La proposition 7.35 précédente donne une représentation d'une partie intervalle-définissable sous la forme d'un semi-linéaire (base et périodes) [GS66] [Huy85] [Reu89].*

**Lemme 7.37**
*Le cardinal de l'ensemble des intervalle-définissables de granularité bornée par 1 est bornée par $2^{3^m}$.*

*Démonstration :*

Remarquons qu'un bloc de granularité bornée par 1 est définie par une formule de la forme $\bigwedge_{j \in J_=} (v_j = 0) \bigwedge_{j \in J_{\neq}} (v_j \neq 0)$. Ainsi, le nombre de blocs de granularité bornée par 1 est majoré par $3^m$. Enfin, comme une partie intervalle-définissable de granularité bornée par 1 est une union finie de blocs de granularité aussi bornée par 1, le nombre de telles parties est majoré par $2^{3^m}$. □

On peut alors majorer $\mathrm{taille}(\mathcal{A}(X))$ en fonction de $\mathrm{gran}(X)$.

**Proposition 7.38**
*Pour toute partie $X \subseteq \mathbb{N}^m$ intervalle-définissable, on a* $\mathrm{taille}(\mathcal{A}(X)) \leqslant (r.\mathrm{gran}(X))^m + 2^{3^m}$.

*Démonstration :*

D'après le théorème 4.37, l'ensemble des états de $\mathcal{A}(X)$ est égal à $Q(X) = \{\gamma_\sigma^{-1}(X);\ \sigma \in$

$\Sigma_r^*\}$. Remarquons que si $\mathrm{gran}(X) = 0$ alors $X = \mathbb{N}^m$ ou $X = \emptyset$ et dans ce cas $\mathrm{taille}(\mathcal{A}(X)) = 1$. On peut donc supposer que $\mathrm{gran}(X) \geqslant 1$. Considérons le plus petit entier $k \geqslant 0$ tel que $k \geqslant \frac{\ln(\mathrm{gran}(X))}{\ln(r)} > k - 1$. D'après la proposition 7.33, pour tout mot $\sigma \in \Sigma_r^{km}$, on a $\mathrm{gran}(\gamma_\sigma^{-1}(X)) \leqslant \frac{\mathrm{gran}(X)-1}{r^k} + 1 \leqslant \frac{r^k-1}{r^k} + 1 < 2$. Ainsi $\mathrm{gran}(\gamma_\sigma^{-1}(X)) \in \{0, 1\}$. Notons $Q_1$ l'ensemble des parties intervalle-définissables $X$ dont la granularité est bornée par 1. D'après la proposition 7.33, on a $Q(X) \subseteq Q_1 \cup \{\gamma_\sigma^{-1}(X);\ |\sigma| < m.k\}$. Ainsi $\mathrm{card}(Q(X)) \leqslant \mathrm{card}(Q_1) + \mathrm{card}(\Sigma_r^{<m.k})$. D'après le lemme 7.37, on a $\mathrm{card}(Q_1) \leqslant 2^{3^m}$. De plus, comme $\mathrm{card}(\Sigma_r^{<m.k}) = \frac{r^{m.k}-1}{r-1} < \frac{(r.\mathrm{gran}(X))^m-1}{r-1} \leqslant (r.\mathrm{gran}(X))^m$, on a donc la majoration recherchée. □

#### 7.2.4.2 Taille asymptotique

Après avoir caractérisé les fonctions affines laissant stables par image inverse les parties intervalle-définissables, on prouve que la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X))$ est polynomiale.

Le lemme suivant sera utilisé pour borner la granularité de $f^{-1}(X')$ en fonction de la granularité de $X$.

**Lemme 7.39**
*Soient $d, \alpha \in \mathbb{N}^m$ et $c \geqslant 0$. La partie $X = d + \{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle = c\}$ est intervalle-définissable et $\mathrm{gran}(X) \leqslant ||d||_\infty + c + 1$ :*

*Démonstration :*
Notons $I = \{i \in \{1, \ldots, m\};\ \alpha_i \neq 0\}$ et considérons $X' = \{x \in \mathbb{N}^m;\ \forall i \notin I\ x_i = 0;\ \sum_{i \in I} \alpha_i.x_i = c\}$. Montrons que pour tout $x' \in X'$, on a $||x'||_\infty \leqslant c$. Pour $i \notin I$, on a $x'_i = 0 \leqslant c$ et pour $i \in I$, on a $x'_i \leqslant \frac{c}{\alpha_i} \leqslant c$. On a donc en particulier prouvé que $X'$ est fini. Il suffit alors de remarquer que la formule suivante représente $X$ :

$$\bigvee_{x' \in X'} \left[ \bigwedge_{i \in I} (v_i = x'_i + d_i) \bigwedge_{i \notin I} \bigwedge_{c_i \in \{0, \ldots, d_i - 1\}} (v_i \neq c_i) \right]$$

□

On peut alors caractériser les fonctions affines laissant stables par image inverse les parties intervalle-définissables.

**Proposition 7.40**
*Soit $f : D \to \mathbb{N}^m$ une fonction affine définie sur une partie $D$ de $\mathbb{N}^m$. Les deux assertions suivantes sont équivalentes :*

- *Le domaine de définition $D$ est intervalle-définissable.*
- *Pour tout $X' \subseteq \mathbb{N}^m$ intervalle-définissable, $f^{-1}(X')$ est intervalle-définissable.*

*De plus, dans ce cas, $\mathrm{gran}(f^{-1}(X')) \leqslant \mathrm{gran}(X') + \mathrm{gran}(D)$ pour tout $X$' intervalle-définissable.*

*Démonstration :*

Une des implications est évidente. En effet, si pour tout $X'$ intervalle-définissable, $f^{-1}(X')$ est intervalle-définissable, alors en particulier, comme $X' = \mathbb{N}^m$ est intervalle-définissable, la partie $D = f^{-1}(\mathbb{N}^m)$ est intervalle-définissable. Montrons l'autre implication. Pour cela, on considère une fonction affine $f : D \to \mathbb{N}^m$ et une partie $X'$ telle que $D$ et $X'$ sont intervalle-définissables.

On commence par montrer que l'on peut supposer que $D$ est un bloc. D'après le lemme 7.32, le domaine de définition $D$ est une union finie de blocs $D = \bigcup_{k\in K} D_k$ tels que $\mathrm{gran}(D_k) \leqslant \mathrm{gran}(D)$. Considérons les restrictions $f_k : D_k \to \mathbb{N}^m$ de $f$. Comme $f^{-1}(X') = \bigcup_{k\in K} f_k^{-1}(X')$, la proposition 7.33 montre que l'on peut supposer $D = D_k$.

On montre alors que l'on peut supposer que $X' = \{x \in \mathbb{N}^m;\ x_i = c\}$ où $c \geqslant 0$ et où $i \in \{1, \ldots, m\}$. En effet, comme pour toute partie $X$ et $X'$ de $\mathbb{N}^m$, on a $f^{-1}(X \cup X') = f^{-1}(X) \cup f^{-1}(X')$, $f^{-1}(X \cap X') = f^{-1}(X) \cap f^{-1}(X')$ et $f^{-1}(\mathbb{N}^m \backslash X) = D \cap (\mathbb{N}^m \backslash f^{-1}(X))$, on peut supposer que $X' = \{x \in \mathbb{N}^m;\ x_i = c\}$.

Comme $D$ est un bloc, il est définissable par une formule de la forme $\bigwedge_{j\in J_=}(v_j = c_j) \bigwedge_{j\in J_{\neq}}(v_j \neq c_j)$ où $J_= \cap J_{\neq} = \emptyset$ et $c_j < \mathrm{gran}(D)$. Comme $f : D \to \mathbb{N}^m$ est une fonction affine, il existe une matrice $M \in \mathcal{M}_m(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^m$ tels que $f(x) = M.x + v$ pour tout $x \in D$. Considérons le vecteur $d \in \mathbb{N}^m$ défini par :

$$d_j = \begin{cases} c_j & \text{si } j \in J_= \\ 0 & \text{si } j \in J_{\neq} \text{ et } c_j \neq 0 \\ 1 & \text{si } j \in J_{\neq} \text{ et } c_j = 0 \\ 0 & \text{sinon} \end{cases}$$

Comme $d \in D$, on a $f(d) \in \mathbb{N}^m$. De plus, par construction, on a $D - d \subseteq \mathbb{N}^m$. Montrons que pour tout $j \notin J_=$, on a $M.e_j \in \mathbb{N}^m$. Considérons $n \geqslant \mathrm{gran}(D)$ et remarquons que $d + n.e_j \in D$. Ainsi $M.d + v + n.M.e_j \in \mathbb{N}^m$ pour tout $n \geqslant \mathrm{gran}(D)$. En particulier $M.e_j \in \mathbb{N}^m$.

On a :

$$\begin{aligned} f^{-1}(X') &= \{x \in D;\ f(x) \in X'\} \\ &= \{x \in D;\ (f(d) + M.(x-d))_i = c\} \\ &= \{x \in D;\ \sum_{j\notin J_=} M_{ij}.(x_j - d_j) = c - f(d)_i\} \\ &= D \cap \left( d + \{x \in \mathbb{N}^m;\ \sum_{j\notin J_=} M_{ij}x_j = c - f(d)_i\} \right) \end{aligned}$$

Remarquons que si $c - f(d)_i < 0$ alors $f^{-1}(X') = \emptyset$. Comme $f(d)_i \geqslant 0$, on peut donc supposer que $c - f(d)_i \in \{0, \ldots, c\}$. Montrons que $\max_i(d_i) \leqslant \mathrm{gran}(D)$. Remarquons que si $\mathrm{gran}(D) = 0$ alors $D = \mathbb{N}^m$ (car $D \neq \emptyset$). On a donc $J_= \cup J_{\neq} = \emptyset$. Dans ce cas, $d = 0$ et on a bien $\max_i(d_i) \leqslant \mathrm{gran}(D)$. De plus, si $\mathrm{gran}(D) \geqslant 1$, alors $\max_i(d_i) \leqslant \mathrm{gran}(D)$. Le lemme 7.39 montre que $\mathrm{gran}(f^{-1}(X')) \leqslant \max(\mathrm{gran}(D), c + 1 + \mathrm{gran}(D)) \leqslant \mathrm{gran}(X') + \mathrm{gran}(D)$.

□

**Remarque 7.41**
*La majoration* $\mathrm{gran}(\gamma_b^{-1}(X)) \leqslant \mathrm{gran}(X)$ *prouvée à la proposition 7.33 est un cas particulier de la proposition précédente. En effet, la fonction* $\gamma_b$ *étant affine et définie sur* $\mathbb{N}^m$, *on a* $\mathrm{gran}(\gamma_b^{-1}(X)) \leqslant \mathrm{gran}(\mathbb{N}^m)+\mathrm{gran}(X)$. *Or par définition de la granularité, on a* $\mathrm{gran}(\mathbb{N}^m) = 0$.

**Remarque 7.42**
*De la proposition précédente, on déduit que la composée de deux fonctions affines* $f$ *et* $g$ *dont les domaines de définition respectifs* $D_f$ *et* $D_g$ *sont intervalle-définissables est une fonction affine* $f \circ g$ *dont le domaine de définition* $D_{f\circ g}$ *est intervalle-définissable et vérifie* $\mathrm{gran}(D_{f\circ g}) \leqslant \mathrm{gran}(D_f) + \mathrm{gran}(D_g)$.

On peut alors prouver que la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est polynomiale.

**Théorème 7.43**
*Soit* $S$ *un système à compteurs affine dont les domaines de définition sont intervalle-définissables, et soit* $X'$ *une partie intervalle-définissable. Il existe deux entiers* $c', c_S \geqslant 0$ *tels que pour tout* $k \geqslant 0$ :

$$\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X')) \leqslant (r.(c' + c_S.k))^m + 2^{3^m}$$

*Démonstration :*
Soient $c_S = \max_{a\in\Sigma} \mathrm{gran}(D_a)$ et $c' = \mathrm{gran}(X')$. La proposition 7.40 montre que $\mathrm{Pre}_S^{\leqslant k}(X')$ est intervalle-définissable et que $\mathrm{gran}(\mathrm{Pre}_S^{\leqslant k}(X')) \leqslant c' + c_S.k$. La proposition 7.38 prouve que $\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))) \leqslant (r.(c' + c_S.k))^m + 2^{3^m}$. □

Comme corollaire, on déduit que l'automate $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est calculable en temps polynômial en $k$.

**Corollaire 7.44**
*Soit* $S$ *un système à compteurs affine dont les domaines de définition sont intervalle-définissables, et soit* $X'$ *une partie intervalle-définissable. La complexité de l'algorithme qui calcule de proche en proche* $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ *en utilisant l'algorithme donné au théorème 7.3 a une complexité polynomial en* $k$.

*Démonstration :*
D'après le théorème 7.3, on peut calculer en temps polynomial en $\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X')))$ un UBA représentant $\mathrm{Pre}_S^{\leqslant k+1}(X')$. En utilisant l'algorithme de minimisation des automates de Hopcroft [Hop71], on prouve ainsi que $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k+1}(X'))$ est calculable en temps polynomial en fonction de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$. Enfin, d'après le théorème 7.43, la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est polynomial en $k$. On a donc prouver que $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est calculable en temps polynomial en $k$. □

**Remarque 7.45**
*On aurait pu obtenir une complexité en* $O(k^m)$ *dans le corollaire précédent pour la construction de* $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ *en représentant les parties intervalle-définissables par des semi-*

*linéaires base et période (c.f. proposition 7.35 et remarque 7.36). L'outil* Brain *[Bra] utilise cette base. Cela peut expliquer ses bonnes performances pour ce type de systèmes à compteurs ([BB02],[BB03]). Cependant, on n'a pas souhaité utiliser les semi-linéaires, quitte à obtenir une complexité plus élevée dans le cas le pire, car en calculant* $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ *de proche en proche en n'utilisant que des UBA minimaux, on peut raisonnablement espérer que dans la pratique, la taille des automates calculés sera logarithmique en* $(r.(c' + 1 + c_S.k))^m$*, comme dans le cas des BDD ([Bry92]).*

### 7.2.5 Autres logiques

Dans cette dernière sous-section, on étudie la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ pour les logiques suivantes :
- clos par le bas,
- semi-affine,
- non-quantifié,
- polyèdre.

Mis à part pour la logique des non-quantifiés, justifiée par le fait que l'on sait extraire d'un automate binaire non ambigu représentant un tel ensemble une formule de Presburger le représentant, ces logiques n'apportent malheureusement pas de résultats nouveaux intéressants.

En effet, alors que les fonctions affines laissant stables par image inverse les clos par le bas, forment une classe trop restreinte pour pouvoir être utilisée dans le cadre de la vérification, les fonctions affines laissant stables les semi-affines et les polyèdres donne une taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ exponentielle.

Cette étude est néanmoins intéressante car elle permet de caractériser les fonctions affines laissant stables par image inverse les parties définissables dans une logique donnée.

#### 7.2.5.1 Cas clos par le bas

On va montrer que pour la logique des clos par le bas, la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k\geqslant 0}$ est stationnaire. La preuve n'est pas aussi simple que dans le cas des clos par le haut car une suite croissante, pour la relation d'inclusion, de clos par le bas, n'est pas nécessairement stationnaire, comme le montre l'exemple $X_n = \{0, \dots, n\}$.

**Proposition 7.46**
*Soit* $f : D \to \mathbb{N}^m$ *une fonction affine définie sur une partie* $D$ *de* $\mathbb{N}^m$*. Les deux assertions suivantes sont équivalentes :*
- *$D$ et clos par par le bas et il existe une matrice $M \in \mathcal{M}_m(\mathbb{N}^m)$ et un vecteur $v \in \mathbb{N}^m$ tels que $f(x) = M.x + v$ pour tout $x \in D$,*
- *$f^{-1}(X')$ est clos par le bas pour tout $X'$ clos par le bas.*

*Démonstration :*
Supposons que $f^{-1}(X')$ soit clos par le bas pour tout clos par le bas $X'$. En particulier, comme $\mathbb{N}^m$ est clos par le bas, $D = f^{-1}(\mathbb{N}^m)$ est clos par le bas. Remarquons que si $D = \emptyset$ alors $M = I$ et $v = 0$ vérifient $f(x) = M.x+v$ pour tout $x \in D$. On peut donc supposer que

$D \neq \emptyset$. Considérons alors $d \in D$. On considère le clos par le bas $X' = \{x' \in \mathbb{N}^m;\ x' \leqslant f(d)\}$. Comme $d \in f^{-1}(X')$ et que $0 \leqslant d$, on a $0 \in f^{-1}(X')$. On a donc prouvé que $f(0) = v \in \mathbb{N}^m$ et que $v = f(0) \in X'$. Par définition de $X'$, on a $v \leqslant M.d + v$. Ainsi, pour tout $d \in D$, on a $M.d \in \mathbb{N}^m$. Considérons $I = \{i \in \{1, \dots, m\};\ \exists d \in D\ d_i \neq 0\}$. Montrons que pour tout $i \in I$, on a $M.e_i \in \mathbb{N}^m$. Par définition de $I$. Il existe $d \in D$ tel que $d_i \neq 0$. Comme $e_i \leqslant d$, on a donc $e_i \in D$. D'où $M.e_i \in \mathbb{N}^m$. Considérons alors la matrice $M'$ définie par $M'.e_i = M.e_i$ si $i \in I$ et par $M'.e_i = 0$ sinon. Pour tout $x \in D$, on a alors $f(x) = M.x + v = M'.x + v$. Comme $M' \in \mathbb{N}^m$ et $v \in \mathbb{N}^m$, on a prouvé une implication. Réciproquement, considérons une fonction affine $f : D \rightarrow \mathbb{N}^m$ telle que $D$ est un clos par le bas et telle qu'il existe une matrice carrée $M \in \mathcal{M}_m(\mathbb{N})$ et un vecteur $v \in \mathbb{N}^m$ tels que pour tout $x \in D$, on a $f(x) = M.x + v$. Montrons que $f^{-1}(X')$ est clos par le bas pour tout clos par le bas $X'$. Pour cela, considérons $x \in f^{-1}(X')$ et $z \in \mathbb{N}^m$ tels que $x - z \in \mathbb{N}^m$. Comme $x \in f^{-1}(X')$, on a $x \in D$. Comme $D$ est clos par le bas, on a donc $x - z \in D$. Remarquons que $f(x - z) = f(x) - M.z$. Comme $f(x) \in X'$, $M.z \in \mathbb{N}^m$ et que $X'$ est clos par le bas, on a $f(x) - M.z \in X'$. Ainsi, $x - z \in f^{-1}(X')$. On a donc bien prouvé que $f^{-1}(X')$ est clos par le bas. □

Comme le montre le lemme suivant, l'hypothèse $D$ clos par le bas n'est pas suffisante pour caractériser les fonctions affines laissant stables par image inverse les clos par le bas.

**Lemme 7.47**
*Il existe une fonction affine $f : D \rightarrow \mathbb{N}^m$ définie sur un clos par le bas et un clos par le bas $X'$ tels que $f^{-1}(X')$ n'est pas clos par le bas.*

*Démonstration :*
On considère $f(x) = 1 - x$ définie sur le clos par le bas $D = \{0, 1\}$. Remarquons que $X' = \{0\}$ est un clos par le bas et que $f^{-1}(X') = \{1\}$ n'est pas clos par le bas. □

Pour montrer que la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k \geqslant 0}$ est stationnaire, on prouve que la granularité de cette suite est bornée.

**Lemme 7.48**
*Soit $f : D \rightarrow \mathbb{N}^m$ une fonction affine définie sur une partie intervalle-définissable telle qu'il existe $M \in \mathcal{M}_m(\mathbb{N})$ et $v \in \mathbb{N}^m$ vérifiant $f(x) = M.x + v$ pour tout $x \in D$.*
*Pour toute partie intervalle-définissable $X'$, on a $\mathrm{gran}(f^{-1}(X')) \leqslant \max(\mathrm{gran}(D), \mathrm{gran}(X'))$.*

*Démonstration :*
Considérons la fonction $g : \mathbb{N}^m \rightarrow \mathbb{N}^m$ définie par $g(x) = M.x + v$. D'après la proposition 7.40, on a $\mathrm{gran}(g^{-1}(X')) \leqslant \mathrm{gran}(X')$ pour tout $X'$ intervalle-définissable. Comme $f^{-1}(X') = D \cap g^{-1}(X')$, on obtient le lemme. □

On peut alors prouver que la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est constante.

**Théorème 7.49**
*Soit $S$ un système à compteurs affine dont les fonctions affines laissent stables les clos par le bas, et soit $X'$ un clos par le bas. Il existe une constante $c \geqslant 1$ telle que pour tout entier*

*$k \geqslant 0$ on a :*

$$\mathrm{taille}(\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))) \leqslant c$$

*Démonstration :*

Posons $c = \max(\max_{a\in\Sigma} \mathrm{gran}(D_a), \mathrm{gran}(X'))$. D'après le lemme 7.48, pour tout $k \geqslant 0$, on a $\mathrm{gran}(\mathrm{Pre}_S^{\leqslant k}(X')) \leqslant c$. Comme il existe au plus $(c+1)^m$ parties intervalle-définissables dont la granularité est bornée par $c$, la suite $(\mathrm{Pre}_S^{\leqslant k}(X'))_{k\geqslant 0}$ est stationnaire. Ainsi la taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est constante. □

**Remarque 7.50**
*Contrairement au cas clos par le haut, on peut donner une borne élémentaire en* $\mathrm{taille}(S)$ *et* $\mathrm{taille}(\mathcal{A}(X'))$ *du plus petit entier $k \geqslant 0$ tel que $\mathrm{Pre}_S^{\leqslant k}(X') = \mathrm{Pre}_S^{*}(X')$. Pour obtenir une telle borne, la preuve du théorème précédent montre qu'il suffit de majorer la granularité d'un automate binaire représentant un clos par le bas. En montrant que l'enveloppe semi-affine dans $\mathbb{N}^m$ d'un non quantifié $X$ représenté par $\mathcal{A}(X)$ est une union finie de blocs de granularité bornée par $r^{\mathrm{taille}(\mathcal{A}(X))}$, on déduit du théorème 5.40 (et de sa preuve) que* $\mathrm{gran}(X) \leqslant r^{\mathrm{taille}(\mathcal{A}(X))}$ *(cette preuve n'est pas développée dans cette thèse).*

#### 7.2.5.2 Calcul exponentiel dans les autres logiques

On montre que la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ reste exponentielle pour les logiques suivantes : semi-affine, non-quantifié, polyèdre.

**Remarque 7.51**
*La classe des parties non-quantifiées est utilisée pour décrire les domaines de définition de quelques systèmes à compteurs analysés par* CSL-ALV *([Alv]). En effet, certains de ces systèmes utilisent des domaines de définition de la forme $x_i = x_j$ comparant ainsi le contenu des compteurs $x_i$ et $x_j$.*

**Proposition 7.52**
*Soit $f : D \rightarrow \mathbb{N}^m$ une fonction affine définie sur une partie $D$ de $\mathbb{N}^m$. On a les caractérisations suivantes :*

- *$f^{-1}(X')$ est semi-affine pour tout $X'$ semi-affine si et seulement si $D$ est semi-affine.*
- *$f^{-1}(X')$ est non-quantifiée pour tout $X'$ non quantifié si et seulement si $D$ est non quantifié.*
- *$f^{-1}(X')$ est polyèdre-définissable pour tout $X'$ polyèdre-définissable si et seulement si $D$ est polyèdre-définissable.*

*Démonstration :*

On considère le cas semi-affine. Une des implications est évidente. En effet, si $f^{-1}(X')$ est semi-affine pour tout $X'$ semi-affine, alors en particulier, comme $\mathbb{N}^m$ est semi-affine, $D = f^{-1}(\mathbb{N}^m)$ est semi-affine. Prouvons l'autre implication en considérant une fonction affine $f$ définie sur une partie semi-affine $D$. Soit $X'$ une partie semi-affine. Montrons que $f^{-1}(X')$ est semi-affine. Comme pour toute partie $X_1'$, $X_2'$, on a $f^{-1}(X_1' \cup X_2') =$

$f^{-1}(X'_1) \cup f^{-1}(X'_2)$, on peut supposer que $X'$ est une partie affine. Il existe une formule $\phi'(x') = \bigwedge_{k \in K}(\langle \alpha_k, x' \rangle = c_k)$ où $\alpha_k \in \mathbb{Q}^m$ et $c_k \in \mathbb{Q}$ représentant $X'$. Considérons une formule $\phi_D$ dans la logique des semi-affines représentant $D$ et remarquons que $f^{-1}(X')$ est représentée par la formule semi-affine suivante :

$$\phi_D \bigwedge_{k \in K} (\langle \alpha_k, M.x + v \rangle = c_k)$$

On considère le cas non-quantifié. Une des implications est évidente. En effet, si $f^{-1}(X')$ est non-quantifiée pour tout $X'$ non-quantifiée, alors en particulier, comme $\mathbb{N}^m$ est non quantifié, $D = f^{-1}(\mathbb{N}^m)$ est non quantifies. Prouvons l'autre implication en considérons une fonction affine $f$ définie sur une partie non-quantifiée $D$. Montrons que $f^{-1}(X')$ est non-quantifiée pour tout $X'$ non-quantifiée. Comme $f^{-1}(X \cup X') = f^{-1}(X) \cup f^{-1}(X')$ et que $f^{-1}(\mathbb{N}^m \backslash X) = D \cap (\mathbb{N}^m \backslash f^{-1}(X))$ pour toute partie $X$ et $X'$, on peut supposer que $X'$ est une partie affine. Il existe une formule $\phi'(x') = \bigwedge_{k \in K}(\langle \alpha_k, x' \rangle = c_k)$ où $\alpha_k \in \mathbb{Q}^m$ et $c_k \in \mathbb{Q}$ représentant $X'$. Considérons une formule non quantifiée $\phi_D$ représentant $D$ et remarquons que $f^{-1}(X')$ est représentée par la formule non-quantifiée suivante :

$$\phi_D \bigwedge_{k \in K} (\langle \alpha_k, M.x + v \rangle = c_k)$$

On considère enfin le cas polyèdre-définissable. Une des implications est évidente. En effet, si $f^{-1}(X')$ est polyèdre-définissable pour tout $X'$ polyèdre-définissable, alors en particulier, comme $\mathbb{N}^m$ est polyèdre-définissable, $D = f^{-1}(\mathbb{N}^m)$ est polyèdre-définissable. Prouvons l'autre implication en considérons une fonction affine $f$ définie sur une partie polyèdre-définissable $D$. Montrons que $f^{-1}(X')$ est polyèdre-définissable pour tout $X'$ polyèdre-définissable. Comme $f^{-1}(X \cup X') = f^{-1}(X) \cup f^{-1}(X')$ pour toute partie $X$ et $X'$, on peut supposer que $X'$ est représenté par une formule $\phi'(x') = \bigwedge_{k \in K}(\langle \alpha_k, x' \rangle \leqslant c_k)$ où $\alpha_k \in \mathbb{Q}^m$ et $c_k \in \mathbb{Q}$. Considérons une formule $\phi_D$ dans la logique des polyèdres représentant $D$ et remarquons que $f^{-1}(X')$ est représentée par la formule suivante :

$$\phi_D \bigwedge_{k \in K} (\langle \alpha_k, M.x + v \rangle \leqslant c_k)$$

□

**Remarque 7.53**
*Comme les domaines de définition du système à compteurs de la proposition 7.22 sont semi-affines, non quantifiés et polyèdre-définissables, on déduit que la taille asymptotique de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$ est en général exponentielle en $k$.*

## 7.3 A propos de $\mathrm{Post}_S^{\leqslant k}(X)$

L'étude de la taille asymptotique de $\mathcal{A}(\mathrm{Post}_S^{\leqslant k}(X))$ est plus difficile et moins intéressante que celle de $\mathcal{A}(\mathrm{Pre}_S^{\leqslant k}(X'))$. En effet, on montre que pour les logiques étudiées dans le cas des prédécesseurs, mis à part les clos par le haut, la caractérisation effective des fonctions affines laissant stable cette logique par image directe est difficile car il existe de telles fonctions définie sur des ensembles non récursifs. De plus, pour la logique des clos par le haut, la caractérisation des fonctions affines laissant stables par image directe les clos par le haut, n'est pas utile en vérification car dans la pratique l'ensemble des états initiaux $X$ d'un système à compteurs, est rarement clos par le haut.

### 7.3.1 Cas clos par le haut

On caractérise les fonctions affines laissant stables par image directe les clos par le haut. On montre en particulier que l'inverse d'un système à compteurs utilisant de tels fonctions n'est autre qu'un système affine dont les domaines de définition sont clos par le haut. Ainsi, on a $\mathrm{Post}_S^{\leqslant k}(X) = \mathrm{Pre}_{S^{-1}}^{\leqslant k}(X)$ et ce calcul des successeur n'est autre qu'un calcul caché des prédécesseurs. On obtient ainsi une taille asymptotique en $k$ de $\mathcal{A}(\mathrm{Post}_S^{\leqslant k}(X))$ constante.

**Proposition 7.54**
*Soit $f : D \rightarrow \mathbb{N}^m$ une fonction affine définie sur une partie $D$ de $\mathbb{N}^m$. Les deux assertions suivantes sont équivalentes :*
- *L'image $f(D)$ est close par le haut,*
- *Pour tout $X \subseteq \mathbb{N}^m$ clos par le haut, $f(X)$ est clos par le haut.*

*De plus, dans ce cas $f : D \rightarrow f(D)$ est une fonction bijective.*

*Démonstration :*
Une des implications est évidente. En effet, si pour tout $X$ clos par le haut, $f(X)$ est clos par le haut alors en particulier comme $\mathbb{N}^m$ est clos par le haut, $f(D) = f(\mathbb{N}^m)$ est clos par le haut. Réciproquement, considérons une fonction affine $f : D \rightarrow \mathbb{N}^m$ telle que $f(D)$ est clos par le haut. Remarquons que si $f(D) = \emptyset$ alors l'image par $f$ d'un clos par le haut est bien un clos par le haut (c'est même l'ensemble vide). On peut donc supposer que $f(D) \neq \emptyset$. Comme $f$ est une fonction affine, il existe une matrice carrée $M \in \mathcal{M}_m(\mathbb{Q})$ et un vecteur $v \in \mathbb{Q}^m$ tel que $f(x) = M.x + v$ pour tout $x \in D$. Considérons $d \in D$. Comme $f(D)$ est clos par le haut, pour tout $i \in \{1, \dots, m\}$, on a $f(d) + e_i \in f(D)$. Il existe donc $d_i \in D$ tel que $f(d_i) = f(d) + e_i$. Ainsi $M.(d_i - d) = e_i$. La matrice $M$ est donc inversible. La fonction $f^{-1} : f(D) \rightarrow \mathbb{N}^m$ est une fonction affine telle que $f(D)$ est clos par le haut. La proposition 7.24 prouve que pour tout $X$ clos par le haut, la partie $(f^{-1})^{-1}(X)$ est close par le haut. On a donc prouvé que pour tout $X$ clos par le haut, $f(X)$ est clos par le haut.
□

**Remarque 7.55**
*Une étude plus précise des fonctions affines telles que $f(D)$ est clos par le haut montre qu'il existe une matrice de permutation $M$ et un vecteur $v \in \mathbb{Z}^m$ tels que $f(x) = M.x + v$ pour tout $x \in \mathbb{N}^m$. Ainsi, à permutation près, on peut montrer qu'un système à compteurs affine dont chaque fonction affine laisse stables les clos par le haut n'est autre qu'un réseau de Petri.*

On déduit immédiatement de la proposition 7.54 les corollaires suivants.

**Corollaire 7.56**
*Soit $S$ un système à compteurs affine tel que pour tout $a \in \Sigma$, $f_a(D_a)$ est clos par le haut. Le système à compteurs $S^{-1}$ est affine et ses domaines de définition sont clos par le haut.*

**Corollaire 7.57**
*Soit $S$ un système à compteurs affine tel que pour tout $a \in \Sigma$, $f_a(D_a)$ est clos par le haut et soit $X$ un clos par le haut. Il existe un entier $c \geqslant 1$ tel que pour tout $k \geqslant 0$ :*

$$\text{taille}(\mathcal{A}(\text{Pre}_S^{\leqslant k}(X'))) \leqslant c$$

*Démonstration :*
D'après la proposition 7.54, le système à compteurs $S^{-1}$ est affine et ses domaines de définition sont clos par le haut. De $\text{Post}_S^{\leqslant k}(X) = \text{Pre}_{S^{-1}}^{\leqslant k}(X)$ et du théorème 7.25, on déduit le corollaire. □

**Remarque 7.58**
*Le précèdent résultat n'a pas d'intérêt en vérification car l'ensemble des états initiaux d'un système à compteurs est rarement clos par le haut.*

### 7.3.2 Autres logiques

On montre que pour les logiques Presburger, intervalle, semi-affine, non-quantifiée et polyèdre, la caractérisation des fonctions affines laissant stables par image directe ces logiques a peu de signification car il existe de telles fonctions définies sur des parties non récursives.

Comme le montre le lemme suivant, il ne suffit pas d'imposer à $f(D)$ d'être dans la logique en question (remarquons que $\mathbb{N}\times\{0\}$ est à la fois Presburger, intervalle, semi-affine, non-quantifiée et polyèdre).

**Lemme 7.59**
*Il existe une fonction affine $f : D \rightarrow \mathbb{N}^2$ définie sur une partie $D \subseteq \mathbb{N}^2$ telle que $f(D) = \mathbb{N} \times \{0\}$ et telle que $f(\mathbb{N} \times \{0\})$ ne soit pas Presburger-définissable.*

*Démonstration :*
Soit $X \subseteq \mathbb{N}$. Pour tout $x \in X$, on note $i_x \geqslant 0$ le cardinal de l'ensemble des $x' \in X$ strictement plus petit que $x$. On a donc $i_x \leqslant x$ pour tout $x \in X$. On pose $h(X) = \{x^2, x^2 + i_x;\ x \in X\}$. Remarquons que l'application qui à $X$ associe $h(X)$ est injective. Comme l'ensemble des parties Presburger-définissables est dénombrable (car chaque partie est représentée par une formule de longueur finie) alors que l'ensemble des parties de $\mathbb{N}$ est indénombrable, il existe une partie $X$ de $\mathbb{N}$ telle que $h(X)$ n'est pas Presburger-définissable. Posons $Y = h(X) \cup \{0\}$. Considérons $D = \{(x_1, x_2);\ x_1 \geqslant x_2;\ x_1, x_2 \in Y\}$ et la fonction affine $f : D \rightarrow \mathbb{N}^2$ définie par $f(x_1, x_2) = (x_1 - x_2, 0)$. Comme $h(X)$ n'est pas Presburger-définissable, $X$ est infini. Ainsi, pour tout entier $i \geqslant 0$, il existe un élément $x \in X$ tel que $i_x = i$. On a donc $(x^2 + i_x, x^2) \in D$. Comme $f(x^2 + i_x, x^2) = (i_x, 0)$ et que $f(D) \subseteq \mathbb{N}\times\{0\}$,

on a prouvé que $f(D) = \mathbb{N} \times \{0\}$. Remarquons enfin que $f(\mathbb{N} \times \{0\}) = Y \times \{0\}$ qui n'est pas Presburger-définissable. $\square$

De plus, comme le montre le lemme suivant, une fonction affine peut laisser stables par image directe les éléments des logiques Presburger, intervalle, semi-affine, non-quantifiée et polyèdre, sans pour autant avoir un domaine de définition récursif.

**Lemme 7.60**
*Il existe une fonction affine $f : D \to \mathbb{N}^m$ définie sur une partie $D$ non récursive telle que pour toute partie $X \subseteq \mathbb{N}^m$, on a $f(X) = \{0\}$.*

*Démonstration :*
Il suffit de considérer une partie $D$ non récursive et la fonction affine $f : D \to \mathbb{N}^m$ définie par $f(x) = 0$ pour tout $x \in D$. $\square$

Pour ces deux raisons, on n'étudie pas dans cette thèse la taille asymptotique de $\mathcal{A}(\mathrm{Post}_S^{\leqslant k}(X))$ pour ces différentes logiques.

**Remarque 7.61**
*On peut caractériser les fonctions affines laissant stables les logiques à la fois par image directe et par image inverse. On montre en particulier que les systèmes à compteurs affines $S$ laissant stables les parties intervalle-définissables par prédécesseur et successeur sont exactement les systèmes à compteurs broadcasts généralisés. Malgré une explosion exponentielle possible à chaque application de $\mathrm{Post}_S$, on montre qu'asymptotiquement la taille de $\mathcal{A}(\mathrm{Post}_S^{\leqslant k}(X))$ est polynomiale en $k$ (Cette étude n'est pas présentée dans cette thèse).*

CHAPITRE 8

# Enveloppe étoile d'une relation binaire

Dans ce chapitre, on étend les invariants de places aux systèmes à compteurs.

L'analyse statique d'un système cherche à obtenir une approximation de sa relation d'accessibilité sans avoir à la construire explicitement. Rappelons que pour les réseaux de Petri, une telle approximation peut-être obtenue en calculant ses invariants de places [KJ87, Cia94, DRV01, Ler03]. En plus d'être calculable en temps polynomial, les invariants permettent :

- de faire converger, dans certains cas, le calcul itératif des états accessibles d'un système en ne considérant que les états qui peuvent potentiellement atteindre un état dangereux[DRV01].
- de détecter des compteurs bornés. En remarquant qu'une fonction qui fait croître strictement un compteur borné ne peut-être itérée qu'un nombre fini de fois, on peut ainsi *"éliminer" des compositions* de fonctions qui "ne sont pas accélérables" (chapitre 9).
- de détecter des relations linéaires entre les compteurs [MOS04, GN03]. On peut ainsi *réduire* le nombre de variables nécessaires pour représenter des états. Par exemple, si l'on a l'égalité $5.x = 7.y$, on peut "éliminer" le compteur $y$ et ne garder que $x$. On réduit ainsi le nombre de compteurs qui, rappelons le, est un facteur limitant de la vérification symbolique.

Nous généralisons la définition des invariants de place. Dans [Cia94], une telle extension est proposée pour la classe des "self modifying Petri Nets". Pour construire ses invariants de places, Ciardo montre qu'ils coïncident avec ceux d'un réseau de Petri effectivement calculable. Cette technique est ainsi limitée à des systèmes à compteurs "proches" des réseaux de Petri. Dans ce chapitre, on montre que le calcul des invariants de places d'un système $S$ est équivalent [Ler03] à celui de *la plus petite relation affine* réflexive et transitive contenant $\mathcal{R}_S$ (la relation d'accessibilité en une étape du système $S$), appelé *l'enveloppe affine étoile* de $\mathcal{R}_S$.

Cependant, dans le cas des réseaux de Petri reset/transfert, l'enveloppe affine étoile est une sur-approximation trop large pour être utilisée. Pour ces systèmes, la plus petite relation *semi-affine* réflexive et transitive contenant $\mathcal{R}_S$, appelée l'enveloppe semi-affine étoile de $\mathcal{R}_S$ permet de résoudre ce problème.

Dans ce chapitre, on a :
- défini la notion d'enveloppe étoile d'une relation pour une classe d'approximation. L'enveloppe affine (respectivement semi-affine) étoile correspond à l'enveloppe étoile pour la classe des parties affines (respectivement semi-affines).
- prouvé que l'enveloppe affine étoile d'un système à compteurs est calculable en temps polynomial. Ainsi, les invariants de place sont calculables en temps polynomial comme dans le cas des réseaux de Petri.
- donné un algorithme (respectivement un semi-algorithme) pour calculer l'enveloppe semi-affine étoile d'une relation affine (respectivement semi-affine).
- prouvé que *l'enveloppe semi-affine étoile de la relation d'accessibilité* d'un réseau de Petri reset/transfert ou d'un système broadcast est calculable en temps *double exponentiel*.

Dans la section 8.1, on définit la notion d'enveloppe étoile d'une relation pour une classe d'approximation et on établit le lien avec l'abstraction. Les enveloppes affines et semi-affines étoiles sont introduites dans la section 8.2. Un algorithme pour calculer l'enveloppe affine étoile d'une relation affine est donné dans la section 8.3 et un semi-algorithme de calcul de l'enveloppe semi-affine étoile d'une relation semi-affine est présenté dans la section 8.4.

Sans ambiguïté, on note pour une relation binaire $\mathcal{R}$ sur $\mathbb{Q}^m$, $\text{aff}(\mathcal{R})$ l'enveloppe affine dans $\mathbb{Q}^{2.m}$ de $\mathcal{R}$, et on note $\text{saff}(\mathcal{R})$ l'enveloppe semi-affine dans $\mathbb{Q}^{2.m}$ de $\mathcal{R}$.

## 8.1 Enveloppe étoile d'une relation

En utilisant une classe d'approximation $\mathcal{C}$ de $E \times E$ pour un ensemble $E$ non vide, on montre que toute relation binaire $\mathcal{R}$ sur $E$ est incluse dans une plus petite relation de $\mathcal{C}$ réflexive et transitive, appelée l'enveloppe étoile de $\mathcal{R}$ et notée $\text{env}^*_{\mathcal{C}}(\mathcal{R})$. On obtient ainsi une fonction $\mathcal{P}(E \times E) \to \mathcal{C}$ qui, à une relation binaire $\mathcal{R}$ sur $E$, associe l'enveloppe étoile $\text{env}^*_{\mathcal{C}}(\mathcal{R})$. On montre enfin l'intérêt d'étudier la restriction de cette fonction à $\mathcal{C}$.

On se donne donc une classe d'approximation $\mathcal{C}$ de $E \times E$ où $E$ est un ensemble non vide. La proposition suivante montre que toute relation binaire sur $E$ peut être sur-approximée par une relation de $\mathcal{C}$.

**Proposition 8.1**
*Pour toute relation binaire $\mathcal{R}$ sur $E$, il existe une plus petite relation binaire (pour l'inclusion) réflexive et transitive appartenant à $\mathcal{C}$ et contenant $\mathcal{R}$.*

*Démonstration :*
On note $\mathcal{R}'$ l'intersection de toutes les relations binaires réflexives et transitives de $\mathcal{C}$ contenant $\mathcal{R}$. Comme $E \times E \in \mathcal{C}$, cette intersection est bien définie. Par construction $\mathcal{R}'$

est la plus petite relation binaire (pour l'inclusion) réflexive et transitive appartenant à $\mathcal{C}$ et contenant $\mathcal{R}$. □

**Définition 8.2**
*L'enveloppe étoile d'une relation binaire $\mathcal{R}$ sur $E$ est la plus petite relation binaire réflexive et transitive de $\mathcal{C}$ contenant $\mathcal{R}$, notée* $\mathrm{env}^*_{\mathcal{C}}(\mathcal{R})$ *ou simplement* $\mathrm{env}^*(\mathcal{R})$.

L'enveloppe étoile d'une relation binaire $\mathcal{R}$ sur-approxime naturellement la fermeture réflexive et transitive de la relation $\mathcal{R}$. La proposition suivante montre en effet que $\mathrm{env}^*(\mathcal{R})$ contient la relation $\mathcal{R}^*$.

**Proposition 8.3**
*Pour toute relation binaire $\mathcal{R}$ sur $E$, on a* $\mathcal{R}^* \subseteq \mathrm{env}^*(\mathcal{R})$.

*Démonstration :*
Comme $\mathrm{env}^*(\mathcal{R})$ est réflexive et transitive, on déduit de $\mathcal{R} \subseteq \mathrm{env}^*(\mathcal{R})$ que $\mathcal{R}^* \subseteq \mathrm{env}^*(\mathcal{R})$. □

La proposition suivante explique pourquoi dans la suite on ne cherche à calculer que l'enveloppe étoile d'une relation de $\mathcal{C}$ et non l'enveloppe étoile d'une relation quelconque sur $E$. En effet, dans une phase préliminaire, on calcule l'enveloppe $\mathcal{R}' = \mathrm{env}(\mathcal{R})$ de $\mathcal{R}$, puis on calcule $\mathrm{env}^*(\mathcal{R}')$. Ainsi, dans le cas affine (respectivement semi-affine), il suffira simplement de montrer comment calculer l'enveloppe affine étoile d'une relation affine (respectivement l'enveloppe semi-affine étoile d'une relation semi-affine).

**Proposition 8.4**
*Pour toute relation binaire $\mathcal{R}$ sur $E$, on a* $\mathrm{env}^*(\mathcal{R}) = \mathrm{env}^*(\mathrm{env}(\mathcal{R}))$.

*Démonstration :*
De $\mathcal{R} \subseteq \mathrm{env}(\mathcal{R}) \subseteq \mathrm{env}^*(\mathrm{env}(\mathcal{R}))$, on déduit par minimalité de $\mathrm{env}^*(\mathcal{R})$ que $\mathrm{env}^*(\mathcal{R}) \subseteq \mathrm{env}^*(\mathrm{env}(\mathcal{R}))$. De $\mathcal{R} \subseteq \mathrm{env}^*(\mathcal{R})$ et de $\mathrm{env}^*(\mathcal{R}) \in \mathcal{C}$, on déduit $\mathrm{env}(\mathcal{R}) \subseteq \mathrm{env}^*(\mathcal{R})$. Ainsi, par minimalité de $\mathrm{env}^*(\mathrm{env}(\mathcal{R}))$, on a $\mathrm{env}^*(\mathrm{env}(\mathcal{R})) \subseteq \mathrm{env}^*(\mathcal{R})$. □

Pour calculer l'enveloppe étoile d'une relation, on doit donc étudier la fonction $\mathcal{C} \to \mathcal{C}$ qui à une relation $\mathcal{R}$ de $\mathcal{C}$ associe la relation $\mathrm{env}^*(\mathcal{R})$.

**Exemple 8.5**
*Cette exemple montre le lien entre les techniques d'abstraction (voir [BPR02] et [BPR01] pour des exemples d'applications) et l'enveloppe étoile. Dans les techniques d'abstraction, on utilise un ensemble fini $P_0$ de parties de $E$ appelé ensemble de "prédicats". Considérons la classe $P$ correspondant à la fermeture par union, intersection et complémentaire de $P_0$, et la classe d'approximation $\mathcal{C} = P \times P$. Soit $S = (E, \Sigma, (\xrightarrow{a})_{a\in\Sigma})$ un système. Rappelons que l'abstraction du système $S$ correspond au système $S' = (E, \Sigma, (\mathrm{env}(\xrightarrow{a}))_{a\in\Sigma})$. On va montrer que l'enveloppe étoile $\mathrm{env}^*(\mathcal{R}_S)$ de la relation d'accessibilité en une étape $\mathcal{R}_S$ de $S$ est égale à la relation d'accessibilité $\mathcal{R}^*_{S'}$ du système abstrait $S'$. On commence par établir l'égalité $\mathcal{R}_{S'} = \mathrm{env}(\mathcal{R}_S)$. On a en effet $\mathcal{R}_{S'} = \bigcup_{a\in\Sigma} \mathrm{env}(\xrightarrow{a}) = \mathrm{env}(\bigcup_{a\in\Sigma} \xrightarrow{a}) = \mathrm{env}(\mathcal{R}_S)$.*

*En particulier, on a* $\mathcal{R}_{S'} \subseteq \mathrm{env}^*(\mathcal{R}_S)$*. comme* $\mathrm{env}^*(\mathcal{R}_S)$ *est réflexive et transitive, on a donc prouvé l'inclusion* $\mathcal{R}^*_{S'} \subseteq \mathrm{env}^*(\mathcal{R}_S)$*. Montrons l'inclusion réciproque. Comme* $\mathcal{R}^*_{S'}$ *est une relation de* $\mathcal{C}$*, réflexive, transitive et contenant* $\mathcal{R}_S \subseteq \mathrm{env}(\mathcal{R}_S) = \mathcal{R}_{S'}$*, par minimalité de l'enveloppe étoile, on a* $\mathrm{env}^*(\mathcal{R}_S) \subseteq \mathcal{R}^*_{S'}$*. On a donc bien établi l'égalité* $\mathrm{env}^*(\mathcal{R}_S) = \mathcal{R}^*_{S'}$*.*

## 8.2 Comparaison enveloppe affine/semi-affine étoile

Dans la section précédente, on a défini l'enveloppe étoile d'une relation pour une classe d'approximation. Comme dans le reste de ce chapitre, seules les classes d'approximation par espaces affines et semi-affines sont étudiées, correspondant respectivement à la classe d'approximation par parties affines et par parties semi-affines, on compare dans cette section introductive ces deux enveloppes étoiles.

**Définition 8.6**
L'enveloppe affine étoile *(resp.* l'enveloppe semi-affine étoile*) d'une relation* $\mathcal{R}$ *de* $\mathbb{Q}^m$ *est l'enveloppe étoile* $\mathrm{aff}^*(\mathcal{R})$ *(resp.* $\mathrm{saff}^*(\mathcal{R})$*) de* $\mathcal{R}$ *pour la classe d'approximation des espace affine de* $\mathbb{Q}^m \times \mathbb{Q}^m$ *(resp. des espaces semi-affines de* $\mathbb{Q}^m \times \mathbb{Q}^m$*).*

Dans la sous-section 8.2.1, on établit le lien entre $\mathrm{aff}^*(\mathcal{R})$ et $\mathrm{saff}^*(\mathcal{R})$ pour une relation binaire $\mathcal{R}$. Dans la sous-section 8.2.2 on calcule sur un exemple de système à compteurs $S$, la relation $\mathrm{saff}^*(\mathcal{R}_S)$ que l'on compare à $\mathrm{aff}^*(\mathcal{R}_S)$. Enfin, dans la sous-section 8.2.3, on montre que $\mathrm{aff}^*(\mathcal{R}_S)$ et $\mathrm{saff}^*(\mathcal{R}_S)$ coïncident pour tout réseau de Petri $S$.

### 8.2.1 Lien entre $\mathrm{aff}^*(\mathcal{R})$ et $\mathrm{saff}^*(\mathcal{R})$

Dans cette sous-section, on prouve l'égalité $\mathrm{aff}(\mathrm{saff}^*(\mathcal{R})) = \mathrm{aff}^*(\mathcal{R})$.

La proposition suivante sera principalement utilisée dans la section 8.3 pour prouver que l'enveloppe affine étoile d'une relation affine est calculable en temps polynomial. Cette proposition est prouvée dans cette section pour établir le lien entre les enveloppes affine étoile et semi-affine étoile.

**Proposition 8.7**
*Pour toute relation affine* $\mathcal{R}$*, on a :*

$$\mathrm{aff}^*(\mathcal{R}) = \mathrm{aff}(\mathcal{I} \cup \mathcal{R})$$

*Démonstration :*
Remarquons que $\mathcal{I} \cup \mathcal{R} \subseteq \mathrm{aff}^*(\mathcal{R})$. Comme de plus $\mathrm{aff}^*(\mathcal{R})$ est un espace affine, on a $\mathrm{aff}(\mathcal{I} \cup \mathcal{R}) \subseteq \mathrm{aff}^*(\mathcal{R})$. Pour montrer l'inclusion réciproque, comme $\mathrm{aff}(\mathcal{I} \cup \mathcal{R})$ est une relation reflexive contenant $\mathcal{R}$, il suffit de prouver qu'elle est transitive. Pour cela, considérons $(x, x')$ et $(x', x'')$ dans $\mathrm{aff}(\mathcal{I} \cup \mathcal{R})$. Comme $(x, x'') = (x, x') + (x', x'') - (x', x')$, et que $(x, x')$, $(x', x'')$ et $(x', x')$ sont dans l'espace affine $\mathrm{aff}(\mathcal{I} \cup \mathcal{R})$, le couple $(x, x'')$ est aussi dans cet espace affine. On a ainsi prouvé que $\mathrm{aff}(\mathcal{I} \cup \mathcal{R})$ est une relation reflexive et

transitive contenant $\mathcal{R}$. Par minimalité de l'enveloppe affine étoile, on obtient l'inclusion $\mathrm{aff}^*(\mathcal{R}) \subseteq \mathrm{aff}(\mathcal{I} \cup \mathcal{R})$. □

On peut alors établir le lien entre l'enveloppe affine étoile et l'enveloppe semi-affine étoile.

**Proposition 8.8**
*Pour toute relation binaire $\mathcal{R}$, on a :*

$$\mathrm{aff}^*(\mathcal{R}) = \mathrm{aff}(\mathrm{saff}^*(\mathcal{R}))$$

*Démonstration :*
Comme $\mathrm{aff}^*(\mathcal{R})$ est une relation affine réflexive et transitive, et en particulier une relation semi-affine réflexive et transitive, qui contient $\mathcal{R}$, par minimalité de l'enveloppe semi-affine étoile, on a $\mathrm{saff}^*(\mathcal{R}) \subseteq \mathrm{aff}^*(\mathcal{R})$. Comme de plus $\mathrm{aff}^*(\mathcal{R})$ est une relation affine, par minimalité de l'enveloppe affine, on a $\mathrm{aff}(\mathrm{saff}^*(\mathcal{R})) \subseteq \mathrm{aff}^*(\mathcal{R})$. Montrons l'inclusion réciproque. La proposition 8.7 montre que $\mathrm{aff}^*(\mathcal{R}) = \mathrm{aff}(\mathcal{I} \cup \mathcal{R})$. De l'inclusion $\mathcal{I} \cup \mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R})$, on déduit alors par minimalité de l'enveloppe affine, $\mathrm{aff}(\mathcal{I} \cup \mathcal{R}) \subseteq \mathrm{aff}(\mathrm{saff}^*(\mathcal{R}))$. Ainsi $\mathrm{aff}^*(\mathcal{R}) \subseteq \mathrm{aff}(\mathrm{saff}^*(\mathcal{R}))$. □

### 8.2.2 Calcul de l'enveloppe semi-affine étoile d'un réseau de Petri transfert

Dans cette section, on montre sur un exemple de réseau de Petri transfert $S$, que l'enveloppe semi-affine étoile $\mathrm{saff}^*(\mathcal{R}_S)$ de la relation d'accessibilité en une étape $\mathcal{R}_S$ de $S$ peut ne pas coïncider avec l'enveloppe affine étoile $\mathrm{aff}^*(\mathcal{R}_S)$.

On considère le réseau de Petri transfert $S = (\Sigma, \xrightarrow{a})_{a \in \Sigma})$ donné dans [Cia94]. On a $\Sigma = \{a, b\}$, $m = 2$ et les relations $\xrightarrow{a}$ et $\xrightarrow{b}$ sont définies par :

$$\begin{cases} (x_1, x_2) \xrightarrow{a} (x'_1, x'_2) & \text{ssi } x_1 \geqslant 1 \text{ et } (x'_1, x'_2) = (0, x_2 + x_1) \\ (x_1, x_2) \xrightarrow{b} (x'_1, x'_2) & \text{ssi } x_2 \geqslant 1 \text{ et } (x'_1, x'_2) = (x_1 + x_2, 0) \end{cases}$$

La relation d'accessibilité en une étape de $S$ est alors définie par $\mathcal{R}_S = \xrightarrow{a} \cup \xrightarrow{b}$. Considérons les fonctions affines $g_a, g_b : \mathbb{Q}^2 \to \mathbb{Q}^4$ définies par $g_a(x_1, x_2) = (x_1, x_2, 0, x_2 + x_1)$ et $g_b(x_1, x_2) = (x_1, x_2, x_1 + x_2, 0)$. Considérons aussi les domaines de définition $D_a$ et $D_b$ définies par $D_a = \{x \in \mathbb{N}^2;\ x_1 \geqslant 1\}$ et $D_b = \{x \in \mathbb{N}^2;\ x_2 \geqslant 1\}$. On a alors $\xrightarrow{a} = g_a(D_a)$ et $\xrightarrow{b} = g_b(D_b)$. La proposition 3.13 qui permet de "sortir" une fonction affine d'une enveloppe, prouve alors les égalités suivantes :

$$\begin{cases} \mathrm{aff}(\xrightarrow{a}) = g_a(\mathrm{aff}(D_a)) \\ \mathrm{aff}(\xrightarrow{b}) = g_b(\mathrm{aff}(D_b)) \\ \mathrm{saff}(\xrightarrow{a}) = g_a(\mathrm{saff}(D_a)) \\ \mathrm{saff}(\xrightarrow{b}) = g_b(\mathrm{saff}(D_b)) \end{cases}$$

**Lemme 8.9**
*Pour toute partie $X \subseteq \mathbb{Q}$ infini, nous avons* $\text{saff}(X) = \mathbb{Q}$.

*Démonstration :*
Comme $\text{saff}(X)$ est un espace semi-affine, il existe une classe finie $\mathcal{C}$ d'espaces affines non vides de $\mathbb{Q}$ tels que $\text{saff}(X) = \bigcup_{A \in \mathcal{C}} A$. Rappelons qu'un espace affine non vide $A$ de $\mathbb{Q}$ est soit égal à un singleton $A = \{x\}$ pour $x \in \mathbb{Q}$, soit égal à $\mathbb{Q}$. Suppsons par l'absurde que tous les espaces affines de $\mathcal{C}$ soit des singletons. Dans ce cas $\text{saff}(X)$ est un ensemble fini ce qui contredit l'inclusion $X \subseteq \text{saff}(X)$. Ainsi, $\mathbb{Q} \in \mathcal{C}$ et on a prouvé que $\text{saff}(X) = Q$. □

Comme $D_a$ et $D_b$ sont des parties closes par le haut, on peut montrer la proposition suivante :

**Proposition 8.10**
*Pour toute partie non vide $X \subseteq \mathbb{N}^m$ close par le haut, on a* $\text{aff}(X) = \mathbb{Q}^m = \text{saff}(X)$.

*Démonstration :*
Comme $\text{saff}(X) \subseteq \text{aff}(X) \subseteq \mathbb{Q}^m$, il suffit de prouver que $\text{saff}(X) = \mathbb{Q}^m$. Considérons $x_0 \in \mathbb{N}^m$. Comme $X$ est clos par le haut, on a $x_0 + \sum_{i=1}^{m} \mathbb{N}.e_i \subseteq X$. D'après la proposition 3.12, on a $\text{saff}(x_0 + \sum_{i=1}^{m} \mathbb{N}.e_i) = x_0 + \sum_{i=1}^{m} \text{saff}(\mathbb{N}.e_i)$. Considérons la fonction affine $g_i : \mathbb{Q} \rightarrow \mathbb{Q}^m$ définie par $g_i(x) = x.e_i$. D'après la proposition 3.13, on a $\text{saff}(g_i(\mathbb{N})) = g_i(\text{saff}(\mathbb{N}))$. Or d'après le lemme 8.9, on a $\text{saff}(\mathbb{N}) = \mathbb{Q}$. Comme $\mathbb{N}.e_i = g_i(\mathbb{N})$, on a ainsi prouvé $\text{saff}(\mathbb{N}.e_i) = \mathbb{Q}.e_i$. De l'inclusion $x_0 + \sum_{i=1}^{m} \text{saff}(\mathbb{N}.e_i) \subseteq \text{saff}(X)$, on déduit enfin $\mathbb{Q}^m \subseteq \text{saff}(X)$. □

La proposition précédente montre donc que $\text{aff}(D_a) = \mathbb{Q}^m = \text{saff}(D_a)$ et $\text{aff}(D_b) = \mathbb{Q}^m = \text{saff}(D_b)$. Considérons les relations $\mathcal{R}_a$ et $\mathcal{R}_b$ définies par $\mathcal{R}_a = g_a(\mathbb{Q}^m)$ et $\mathcal{R}_b = g_b(\mathbb{Q}^m)$. De $\xrightarrow{a} \subseteq \text{aff}^*(\mathcal{R}_S)$, on déduit $\mathcal{R}_a = \text{aff}(\xrightarrow{a}) \subseteq \text{aff}^*(\mathcal{R}_S)$. Symétriquement, en posant $\mathcal{R}' = \mathcal{R}_a \cup \mathcal{R}_b \cup \mathcal{I}$, on déduit $\mathcal{R}' \subseteq \text{aff}^*(\mathcal{R}_S)$ et $\mathcal{R}' \subseteq \text{saff}^*(\mathcal{R}_S)$.

De $\mathcal{R}' \subseteq \text{aff}^*(\mathcal{R}_S)$, on déduit $\text{aff}(\mathcal{R}') \subseteq \text{aff}^*(\mathcal{R}_S)$. Comme $\text{aff}(\mathcal{R}') = \{(x_1, x_2, x_1', x_2');\ x_1 + x_2 = x_1' + x_2'\}$ et que cette relation est réflexive et transitive, par minimalité de l'enveloppe affine étoile, on a prouvé l'égalité suivante :

$$\text{aff}^*(\mathcal{R}_S) = \{(x_1, x_2, x_1', x_2');\ x_1 + x_2 = x_1' + x_2'\}$$

De $\mathcal{R}_a.\mathcal{R}_b = \mathcal{R}_b$ et $\mathcal{R}_b.\mathcal{R}_a = \mathcal{R}_a$, on déduit que $\mathcal{R}'$ est réflexive et transitive. Par minimalité de l'enveloppe semi-affine étoile, on a $\text{saff}^*(\mathcal{R}_S) \subseteq \mathcal{R}'$. On a donc prouvé l'égalité suivante :

$$\text{saff}^*(\mathcal{R}_S) = \mathcal{R}_a \cup \mathcal{R}_b \cup \mathcal{I}$$

$S$ est donc un réseau de Petri transfert $S$ pour lequel $\text{saff}^*(\mathcal{R}_S)$ et $\text{aff}^*(\mathcal{R}_S)$ ne coïncident pas. Remarquons que l'inclusion $\mathcal{R}_S^* \subseteq \text{aff}^*(\mathcal{R}_S)$ n'apporte que l'invariant $x_1 + x_2 = x_1' + x_2'$ alors que l'inclusion $\mathcal{R}_S^* \subseteq \text{saff}^*(\mathcal{R})$ produit un invariant "disjonctif" :

$$((x_1' = 0) \wedge (x_2' = x_2 + x_1)) \vee ((x_1' = x_1 + x_2) \wedge (x_2' = 0)) \vee ((x_1' = x_1) \wedge (x_2' = x_2))$$

### 8.2.3 Enveloppe affine et semi-affine étoile d'un réseau de Petri

Dans la sous-section précédente, on a présenté un exemple de réseau de Petri transfert pour lequel l'enveloppe affine étoile et l'enveloppe semi-affine étoile de la relation d'accessibilité en une étape ne coïncident pas. Dans cette sous-section on montre que pour les réseaux de Petri, ces deux enveloppes coïncident toujours.

**Proposition 8.11**
*Pour tout réseau de Petri $S$, on a :*

$$\mathrm{saff}^*(\mathcal{R}_S) = \mathrm{aff}^*(\mathcal{R}_S)$$

*Démonstration :*
Considérons un réseau de Petri $S = (\Sigma, (\xrightarrow{a})_{a\in\Sigma})$. Les relations $\xrightarrow{a}$ peuvent alors s'écrire $x \xrightarrow{a} x'$ si et seulement si $x \geqslant v_a$ et $x' = x - v_a + v'_a$, pour des vecteurs $v_a, v'_a \in \mathbb{N}^m$.

Montrons que $\mathrm{saff}(\mathcal{R}_a) = \mathcal{I} + (\overrightarrow{0}, v'_a - v_a)$. Considérons la fonction affine $g_a : \mathbb{Q}^m \rightarrow \mathbb{Q}^m \times \mathbb{Q}^m$ définie par $g_a(x) = (x, x - v_a + v'_a)$. De la proposition 3.13 et de l'égalité $\xrightarrow{a}= g_a(\{x \in \mathbb{N}^m;\ x \geqslant v_a\})$, on déduit $\mathrm{saff}(\xrightarrow{a}) = g_a(\mathrm{saff}(\{x \in \mathbb{N}^m;\ x \geqslant v_a\}))$. La proposition 8.10 prouve que $\mathrm{saff}(\{x \in \mathbb{N}^m;\ x \geqslant v_a\}) = \mathbb{Q}^m$. On a donc $\mathrm{saff}(\xrightarrow{a}) = \mathcal{I} + (\overrightarrow{0}, v'_a - v_a)$.

On numérote les éléments de $\Sigma = \{a_1, \ldots, a_n\}$. Considérons alors une suite $(\alpha_i)_{1\leqslant i\leqslant n}$ de $\mathbb{N}$. Comme $\mathrm{saff}(\xrightarrow{a}) \subseteq \mathrm{saff}^*(\mathcal{R}_S)$ pour tout $a \in \Sigma$ et que la relation $\mathrm{saff}^*(\mathcal{R})$ est réflexive et transitive, on a prouvé :

$$\mathcal{I} + \sum_{i=1}^{n} \alpha_i.(\overrightarrow{0}, v'_{a_i} - v_{a_i}) = \mathrm{saff}(\xrightarrow{a_1})^{\alpha_1} \ldots \mathrm{saff}(\xrightarrow{a_n})^{\alpha_n} \subseteq \mathrm{saff}^*(\mathcal{R}_S)$$

On a donc prouvé l'inclusion $\mathcal{I} + \sum_{a\in\Sigma} \mathbb{N}.(\overrightarrow{0}, v'_a - v_a) \subseteq \mathrm{saff}^*(\mathcal{R}_S)$. Par minimalité de l'enveloppe semi-affine, on a $\mathrm{saff}(\sum_{a\in\Sigma} \mathbb{N}.(\overrightarrow{0}, v'_a - v_a)) \subseteq \mathrm{saff}^*(\mathcal{R}_S)$. Posons $\mathcal{R}' = \sum_{a\in\Sigma} \mathbb{Q}.(\overrightarrow{0}, v'_a - v_a)$. La proposition 3.12 montre l'égalité suivante $\mathrm{saff}(\sum_{a\in\Sigma} \mathbb{N}.(\overrightarrow{0}, v'_a - v_a)) = \mathcal{R}'$. On donc $\mathcal{R}' \subseteq \mathrm{saff}^*(\mathcal{R}_S)$. Montrons l'inclusion réciproque. Comme $\mathcal{R}_S \subseteq \mathcal{R}'$ et que $\mathcal{R}'$ est réflexive et transitive, par minimalité de l'enveloppe semi-affine étoile, on a $\mathrm{saff}^*(\mathcal{R}_S) \subseteq \mathcal{R}'$. On a donc prouvé que $\mathrm{saff}^*(\mathcal{R}) = \mathcal{R}'$. En particulier $\mathrm{saff}^*(\mathcal{R})$ est un espace affine. La proposition 8.8 permet alors de conclure que $\mathrm{saff}^*(\mathcal{R}_S) = \mathrm{aff}^*(\mathcal{R}_S)$. □

## 8.3 Enveloppe affine étoile

L'enveloppe affine étoile d'une relation affine est étudiée dans cette section. On prouve dans la sous-section 8.3.1 que cette enveloppe est calculable en temps polynômial. On déduit alors que l'enveloppe affine de la relation d'accessibilité d'un système à compteurs est calculable en temps polynômial. Enfin, dans la sous-section 8.3.2 on établie le lien entre l'enveloppe affine étoile et les invariants dits de place d'un système à compteurs.

### 8.3.1 Calcul de l'enveloppe affine étoile

On prouve dans cette sous-section que l'enveloppe affine étoile d'une relation affine $\mathcal{R}$ se calcule en temps polynômial en fonction de la taille de $\mathcal{R}$. Comme l'enveloppe affine d'un ensemble représenté par un automate binaire est calculable en temps polynômial, on déduit que l'enveloppe affine de la relation d'accessibilité d'une large classe de systèmes à compteurs est calculable en temps polynômial.

De la proposition 8.7, on déduit les deux corollaires suivants.

**Corollaire 8.12**
*L'enveloppe affine étoile d'une relation affine $\mathcal{R}$ est calculable en temps polynômial en fonction de la taille de $\mathcal{R}$.*

*Démonstration :*
La proposition 8.7 montre que $\text{aff}^*(\mathcal{R}) = \text{aff}(\mathcal{I} \cup \mathcal{R})$. L'enveloppe étoile $\text{aff}^*(\mathcal{R})$ est donc calculable en temps polynomial. □

**Corollaire 8.13**
*Pour toute relation binaire $\mathcal{R}$, on a $\text{aff}(\mathcal{R}^*) = \text{aff}^*(\mathcal{R})$.*

*Démonstration :*
Considérons une relation binaire $\mathcal{R}$. Par minimalité de l'enveloppe affine, on déduit de $\mathcal{R}^* \subseteq \text{aff}^*(\mathcal{R})$, l'inclusion $\text{aff}(\mathcal{R}^*) \subseteq \text{aff}^*(\mathcal{R})$. Montrons l'inclusion réciproque. Comme $\mathcal{I} \cup \mathcal{R} \subseteq \mathcal{R}^*$, on a $\text{aff}(\mathcal{I} \cup \mathcal{R}) \subseteq \text{aff}(\mathcal{R}^*)$. Or d'après la proposition 8.7, on a $\text{aff}^*(\mathcal{R}) = \text{aff}(\mathcal{I} \cup \mathcal{R})$. On a donc prouvé $\text{aff}^*(\mathcal{R}) \subseteq \text{aff}(\mathcal{R}^*)$. □

Les outils de vérification symbolique [Fas] et [Las] prennent en entrée des systèmes à compteurs $S = (\mathbb{N}^m, \Sigma, (\xrightarrow{a})_{a \in \Sigma})$ tels que $\xrightarrow{a}$ est représentée par une formule de Presburger $\phi_a$ et par une fonction affine $f_a$ telles que $x \xrightarrow{a} x'$ si et seulement si $x \in [\![\phi_a]\!]$ et $x' = f_a(x)$. Dans une étape préliminaire, ces outils construisent pour chaque action $a \in \Sigma$, l'automate binaire canonique $\mathcal{A}_a$ représentant la partie $[\![\phi_a]\!]$. Dans le théorème suivant, on montre que l'on peut calculer l'enveloppe affine de la relation d'accessibilité de $S$ en temps polynômial en fonction de la taille des automates $(\mathcal{A}_a)_{a \in \Sigma}$ et de la taille des fonctions affines $f_a$.

**Définition 8.14**
*Une représentation d'un système à compteurs $S = (\Sigma, (\xrightarrow{a})_{a \in \Sigma})$ par automate binaire et fonction affine est un couple $(\mathbb{Q}^m, \Sigma, (\mathcal{A}_a)_{a \in \sigma}, (f_a)_{a \in \Sigma})$ tel que :*
- *$(\mathcal{A}_a)_{a \in \Sigma}$ est une suite d'automates binaires,*
- *$(f_a)_{a \in \Sigma}$ est une suite de fonctions affines de $\mathbb{Q}^m$ dans $\mathbb{Q}^m$, et*
- *pour tout $a \in \Sigma$, on a $x \xrightarrow{a} x'$ si et seulement si $x \in \rho_m(\mathcal{L}(\mathcal{A}_a))$ et $x' = f_a(x)$.*

**Théorème 8.15**
*Pour tout système à compteurs $S$ représenté par automate binaire et fonction affine, l'enveloppe affine de la relation d'accessibilité de $S$ est calculable en temps polynômial.*

*Démonstration :*

Considérons donc un système à compteurs $S$ représenté par $(\mathbb{Q}^m, \Sigma, (\mathcal{A}_a)_{a\in\sigma}, (f_a)_{a\in\Sigma})$.

On commence par montrer l'égalité $\mathrm{aff}(\mathcal{R}_S^*) = \mathrm{aff}(\mathcal{I}\bigcup_{a\in\Sigma}\mathrm{aff}(\xrightarrow{a}))$. D'après la proposition 8.13, on a $\mathrm{aff}(\mathcal{R}_S^*) = \mathrm{aff}^*(\mathcal{R}_S)$. D'après la proposition 8.4, on a $\mathrm{aff}^*(\mathcal{R}_S) = \mathrm{aff}^*(\mathrm{aff}(\mathcal{R}_S))$. Enfin, la proposition 8.7 montre que $\mathrm{aff}^*(\mathrm{aff}(\mathcal{R}_S)) = \mathrm{aff}(\mathcal{I}\cup\mathrm{aff}(\mathcal{R}_S))$. On a donc bien prouvé l'égalité $\mathrm{aff}(\mathcal{R}_S^*) = \mathrm{aff}(\mathcal{I}\bigcup_{a\in\Sigma}\mathrm{aff}(\xrightarrow{a}))$.

Pour prouver le théorème, il suffit donc de prouver que les espace affines $\mathrm{aff}(\xrightarrow{a})$ sont calculables en temps polynômial.

Montrons que $\mathrm{aff}(\mathcal{R}_a)$ est calculable en temps polynômial. Considérons la fonction affine $g_a : \mathbb{Q}^m \to \mathbb{Q}^m \times \mathbb{Q}^m$ définie par $g_a(x) = (x, f_a(x))$. Comme $\xrightarrow{a} = g_a(\rho_L(\mathcal{L}(\mathcal{A}_a)))$, la proposition 3.13 prouve l'égalité $\mathrm{aff}(\xrightarrow{a}) = f_a(\mathrm{aff}(\rho_L(\mathcal{L}(\mathcal{A}_a))))$. Or, d'après le corollaire 4.68, l'enveloppe affine de $\mathrm{aff}(\rho_L(\mathcal{A}_a))$ est calculable en temps polynomial en la taille de l'automate $\mathcal{A}_a$. Ainsi $\mathrm{aff}(\xrightarrow{a})$ est calculable en temps polynômial. □

**Remarque 8.16**
*On peut étendre le théorème précédent en représentant des actions $a$ du système à compteurs $S$ par des transducteurs $\mathcal{A}_a$ tels que $\rho_{2.m}(\mathcal{L}(\mathcal{A}_a)) = \xrightarrow{a}$. Le calcul de l'enveloppe affine de la relation d'accessibilité reste en effet polynômial.*

### 8.3.2 Les invariants de place

L'enveloppe affine étoile de la relation d'accessibilité en une étape du réseau de Petri transfert de la sous-section 8.2.2 a fait apparaître un invariant de la forme $x_1+x_2 = x_1'+x_2'$. On établit dans cette sous-section le lien entre l'enveloppe affine étoile $\mathrm{aff}^*(\mathcal{R}_S)$ de la relation d'accessibilité en une étape d'un système à compteurs $S$ et l'ensemble des invariants de ce type, appelé invariants de place de $S$.

**Définition 8.17 ([Cia94])**
*Un invariant de place d'un système à compteurs $S = (\Sigma, (\xrightarrow{a})_{a\in\Sigma})$ est une forme linéaire $l : \mathbb{Q}^m \to \mathbb{Q}$ telle que pour toute action $a \in \Sigma$ et pour tout $x \xrightarrow{a} x'$ on a $l(x) = l(x')$. L'ensemble des invariants de place d'un système à compteurs $S$ est noté* $\mathrm{Inv}(S)$

La proposition suivante montre que $\mathrm{Inv}(S)$ est calculable en temps polynômial en fonction de $\mathrm{aff}^*(\mathcal{R}_S)$ et que réciproquement $\mathrm{aff}^*(\mathcal{R}_S)$ est calculable en temps polynômial en fonction de $\mathrm{Inv}(S)$.

**Proposition 8.18**
*Pour tout système à compteurs $S = (\Sigma, (\xrightarrow{a})_{a\in\Sigma})$, on a :*

$$\mathrm{aff}^*(\mathcal{R}_S) = \{(x,x');\ l(x) = l(x')\ \forall l \in \mathrm{Inv}(S)\}$$
$$\mathrm{Inv}(S) = \{l : \mathbb{Q}^m \to \mathbb{Q};\ l \textit{ forme linéaire telle que } l(x) = l(x') \textit{ pour tout } (x,x') \in \mathrm{aff}^*(\mathcal{R}_S)\}$$

*Démonstration :*

On note $\mathcal{R} = \{(x,x');\ l(x) = l(x')\ \forall l \in \mathrm{Inv}(S)\}$.

On commence par établir la première égalité. Montrons que $\mathcal{R}$ est un espace affine. Considérons $(x, x'), (y, y') \in \mathcal{R}$ et $t_1, t_2 \in \mathbb{Q}$ tels que $t_1 = t_2$ et prouvons que $t_1.(x, x') + t_2.(y, y') \in \mathcal{R}$. Pour tout $l \in \mathrm{Inv}(S)$, on a $l(t_1.x + t_2.y) = t_1.l(x) + t_2.l(y) = t_1.l(x') + t_2.l(y') = l(t_1.x' + t_2.y')$. Ainsi $t_1.(x, x') + t_2.(y, y') \in \mathcal{R}$ et on a bien montré que $\mathcal{R}$ est un espace affine. Montrons que $\mathcal{R}_S \subseteq \mathcal{R}$. Pour tout $(x, x') \in \mathcal{R}_S$, il existe $a \in \Sigma$ tel que $x \xrightarrow{a} x'$. Ainsi, pour tout $l \in \mathrm{Inv}(S)$, on a $l(x) = l(x')$. On a donc prouvé que $\mathcal{R}_S \subseteq \mathcal{R}$. Comme $\mathcal{R}$ est réflexive et transitive et contient $\mathcal{R}_S$, par minimalité de l'enveloppe affine étoile, on a $\mathrm{aff}^*(\mathcal{R}_S) \subseteq \mathcal{R}$. Montrons l'inclusion réciproque. Considérons $(x_0, x'_0) \in \mathcal{R}$ et supposons par l'absurde que $(x_0, x'_0) \in \mathrm{aff}^*(\mathcal{R}_S)$. Il existe une fonction affine $f : \mathbb{Q}^m \times \mathbb{Q}^m \to \mathbb{Q}$ telle que $f(x_0, x'_0) \neq 0$ et pour tout $(x, x') \in \mathrm{aff}^*(\mathcal{R}_S)$, on a $f(x, x') = 0$. Considérons deux formes linéaires $l$ et $l'$ et un rationnel $c \in \mathbb{Q}$ tel que $f(x, x') = l(x) - l'(x') + c$ pour tout $(x, x') \in \mathbb{Q}^m \times \mathbb{Q}^m$. Soit $x \in \mathbb{Q}^m$. De $(x, x) \in \mathcal{I} \subseteq \mathrm{aff}^*(\mathcal{R}_S)$, on déduit $0 = f(x, x) = l(x) - l'(x) + c = 0$. On a donc $c = 0$ et $l = l'$. Ainsi, pour tout $(x, x') \in \mathrm{aff}^*(\mathcal{R}_S)$, on a $l(x) = l(x')$. En particulier, pour toute action $a \in \Sigma$ et pour tout $x \xrightarrow{a} x'$, on déduit $l(x) = l(x')$ de $(x, x') \in \mathcal{R}_S \subseteq \mathrm{aff}^*(\mathcal{R}_S)$. On a donc $l \in \mathrm{Inv}(S)$. Enfin, comme $(x_0, x'_0) \in \mathcal{R}$, on a $f(x_0, x'_0) = l(x_0) - l(x'_0) = 0$. On a donc une contradiction. On a donc prouvé la première égalité.

Montrons la deuxième égalité. Considérons $l \in \mathrm{Inv}(S)$ et un couple $(x, x') \in \mathrm{aff}^*(\mathcal{R}_S)$. D'après la première égalité, on a $(x, x') \in \mathcal{R}$. Ainsi $l(x) = l(x')$ et on a montré l'inclusion $\mathrm{Inv}(S) \subseteq \{\text{formes linéaires } l : \mathbb{Q}^m \to \mathbb{Q};\ l(x) = l(x')\ \forall (x, x') \in \mathrm{aff}^*(\mathcal{R}_S)\}$. Pour l'inclusion réciproque, considérons une forme linéaire $l$ telle que $l(x) = l(x')$ pour tout $(x, x') \in \mathrm{aff}^*(\mathcal{R}_S)$. En particulier, pour tout $(x, x') \in \mathcal{R}_S$, on a $l(x) = l(x')$. On a donc $l \in \mathrm{Inv}(S)$.

□

On a donc établie que le calcul de l'enveloppe affine étoile de $\mathcal{R}_S$ revient ni plus ni moins à calculer l'ensemble des invariants de place $\mathrm{Inv}(S)$.

## 8.4 Enveloppe semi-affine étoile d'une relation affine

On montre dans cette section que l'enveloppe semi-affine étoile $\mathrm{saff}^*(\mathcal{R})$ d'une relation affine est calculable en temps polynômial en sa taille et la taille de $\mathcal{R}$. On montre de plus que la relation semi-affine $\mathrm{saff}^*(\mathcal{R})$ est une union finie d'au plus $(4m + 1)^{2.m}$ relations affines de taille polynomiale en la taille de $\mathcal{R}$.

Dans la sous-section 8.4.1, on montre que les itérées d'une relation affine correspondent aux itérées d'une fonction affine calculables en temps polynômial. Enfin, dans la sous-section 8.4.2, on montre comment calculer $\mathrm{saff}^*(\mathcal{R})$ pour une relation affine $\mathcal{R}$.

### 8.4.1 Itérée d'une relation affine

On montre que l'on peut associer à toute relation affine $\mathcal{R}$, une fonction affine $f$ telle que les itérées de $\mathcal{R}$ correspondent aux itérées de $f$. Pour cela, on prouve que l'on peut calculer en temps polynômial un espace affine $D(\mathcal{R}^\infty)$ appelé *domaine de définition limite*, un espace vectoriel $V(\mathcal{R}^\infty)$ appelé *direction limite* et une fonction affine $f : D(\mathcal{R}^\infty) \to D(\mathcal{R}^\infty)$ telle que pour tout $i \geqslant m+1$, on a :

$$\mathcal{R}^i = \{(x, x') \in D(\mathcal{R}^\infty) \times \mathbb{Q}^m;\ x' \in f^i(x) + V(\mathcal{R}^\infty)\}$$

#### 8.4.1.1 Domaine de définition limite

On montre que l'on peut associer à une relation affine $\mathcal{R}$ un espace affine $D(\mathcal{R})$ appelé domaine de définition de $\mathcal{R}$. En remarquant que la suite des domaines de définition $(D(\mathcal{R}^i))_{i\geqslant 0}$ des itérées d'une relation affine $\mathcal{R}$ est une suite décroissante stationnaire, on introduit la notion de domaine de définition limite $D(\mathcal{R}^\infty)$. On prouve que cet espace affine est calculable en temps polynômial.

**Définition 8.19**
*Le domaine de définition d'une relation affine $\mathcal{R}$ est l'espace affine noté $D(\mathcal{R}) = \{x \in \mathbb{Q}^m;\ \exists y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}\}$.*

Naturellement la suite $(D(\mathcal{R}^i))_{i\geqslant 0}$ est une suite décroissante d'espaces affines et, comme toute suite décroissante d'espaces affines, elle est donc stationnaire. Dans le lemme suivant on montre que l'on peut detecter le moment où elle devient stationnaire car elle est strictement décroissante avant.

**Lemme 8.20**
*Soit $\mathcal{R}$ une relation binaire affine. La suite $(D(\mathcal{R}^i))_{i\geqslant 0}$ est décroissante et stationnaire. De plus pour tout indice $i_0 \geqslant 0$ tel que $D(\mathcal{R}^{i_0+1}) = D(\mathcal{R}^{i_0})$, on a $D(\mathcal{R}^i) = D(\mathcal{R}^{i_0})$ pour tout $i \geqslant i_0$.*

*Démonstration :*
De $D(\mathcal{R}^{i+1}) \subseteq D(\mathcal{R}^i)$, on déduit que $(D(\mathcal{R}^i))_{i\geqslant 0}$ est une suite décroissante d'espaces affines. Ainsi, il existe un indice $i_0$ tel que $D(\mathcal{R}^{i_0+1}) = D(\mathcal{R}^{i_0})$. Pour montrer la proposition il suffit de prouver que l'on a alors $D(\mathcal{R}^{i_0+2}) = D(\mathcal{R}^{i_0+1})$. Comme $D(\mathcal{R}^{i_0+2}) \subseteq D(\mathcal{R}^{i_0+1})$, il suffit de prouver l'inclusion réciproque. Pour cela, considérons $x \in D(\mathcal{R}^{i_0+1})$. Il existe alors $y \in \mathbb{Q}^m$ tel que $(x, y) \in \mathcal{R}^{i_0+1}$. Soit $x' \in \mathbb{Q}^m$ tel que $(x, x') \in \mathcal{R}$ et $(x', y) \in \mathcal{R}^{i_0}$. Le vecteur $x'$ est donc dans $D(\mathcal{R}^{i_0}) = D(\mathcal{R}^{i_0+1})$. Il existe $y' \in \mathbb{Q}^m$ tel que $(x', y') \in \mathcal{R}^{i_0+1}$. On a prouvé que $(x, y') \in \mathcal{R}^{i_0+2}$. De $x \in D(\mathcal{R}^{i_0+2})$, on déduit l'inclusion $D(\mathcal{R}^{i_0+1}) \subseteq D(\mathcal{R}^{i_0+2})$.
□

**Définition 8.21**
*Le domaine de définition limite d'une relation affine $\mathcal{R}$ est l'espace affine noté $D(\mathcal{R}^\infty)$ et défini par $D(\mathcal{R}^\infty) = \bigcap_{i\geqslant 0} D(\mathcal{R}^i)$.*

La proposition suivante montre que la suite $(D(\mathcal{R}^i))_{i\geqslant 0}$ est stationnaire à partir de $i = m+1$.

**Proposition 8.22**
*Pour toute relation affine $\mathcal{R}$, on a $D(\mathcal{R}^\infty) = D(\mathcal{R}^{m+1})$.*

*Démonstration :*

Notons $i_0 \geqslant 0$ le premier indice tel que $D(\mathcal{R}^{i_0+1}) = D(\mathcal{R}^{i_0})$. On a alors $D(\mathcal{R}^\infty) = D(\mathcal{R}^i)$ pour tout $i \geqslant i_0$. Il suffit donc de montrer que $i_0 \leqslant m+1$. Pour tout $i \in \{0, \ldots, i_0 - 1\}$, on a $D(\mathcal{R}^{i+1}) \subsetneq D(\mathcal{R}^i)$. Ainsi $\dim(D(\mathcal{R}^{i+1})) < \dim(D(\mathcal{R}^i))$. On obtient alors $\dim(D(\mathcal{R}^{i_0})) \leqslant m - i_0$. Comme $\dim(D(\mathcal{R}^{i_0})) \geqslant -1$, on a bien $i_0 \leqslant m+1$. □

Ainsi, il suffit de calculer $D(\mathcal{R}^{m+1})$ pour obtenir $D(\mathcal{R}^\infty)$.

**Corollaire 8.23**
*Le domaine de définition limite d'une relation affine est calculable en temps polynomial.*

*Démonstration :*

Considérons une relation $\mathcal{R}$ donnée par sa représentation canonique $\rho(\mathcal{R})$. On peut calculer en temps polynomial la représentation canonique $\rho(\mathcal{R}^{m+1})$. Considérons la fonction affine $f : \mathbb{Q}^m \times \mathbb{Q}^m \to \mathbb{Q}^m$ définie par $f(x, x') = x$. On a alors $D(\mathcal{R}^{m+1}) = f(\mathcal{R}^{m+1})$ qui est donc calculable en temps polynomial. □

#### 8.4.1.2 Direction limite

On remarque qu'une relation affine $\mathcal{R}$ associe à chaque vecteur $x \in D(\mathcal{R})$ un espace affine non vide $\{y;\ (x,y) \in \mathcal{R}\}$. On montre que le vectorialisé de cet espace est un espace vectoriel qui ne dépend pas du point $x$ de $D(\mathcal{R})$. Cette espace vectoriel noté $V(\mathcal{R})$ est appelé la direction de $\mathcal{R}$. En remarquant que la suite des directions $(V(\mathcal{R}^i))_{i \geqslant 0}$ est une suite croissante stationnaire d'espaces vectoriels, on introduit la notion de direction limite $V(\mathcal{R}^\infty)$. On prouve enfin que cet espace vectoriel est calculable en temps polynômial.

Pour définir la direction d'une relation affine, on commence par prouver le lemme suivant.

**Lemme 8.24**
*Soit $\mathcal{R}$ une relation affine non vide. Il existe un unique espace vectoriel $V$ tel que pour tout $x \in D(\mathcal{R})$, le vectorialisé de $\{y \in \mathbb{Q}^m;\ (x,y) \in \mathcal{R}\}$ est égal à $V$.*

*Démonstration :*

Considérons $x_1, x_2 \in D(\mathcal{R})$ et notons $A_1 = \{y \in \mathbb{Q}^m;\ (x_1, y) \in \mathcal{R}\}$ et $A_2 = \{y \in \mathbb{Q}^m;\ (x_2, y) \in \mathcal{R}\}$. Il suffit de montrer que $A_1$ et $A_2$ sont deux espaces affines non vide de même direction. Comme $\mathcal{R}$ est une relation affine, $A_1$ et $A_2$ sont des espaces affines. De plus, comme $x_1, x_2 \in D(\mathcal{R})$, les espaces affines $A_1$ et $A_2$ sont non vides. Pour prouver la proposition, par symétrie, il suffit de montrer que $\overrightarrow{A_1} \subseteq \overrightarrow{A_2}$. Considérons $\overrightarrow{a} \in \overrightarrow{A_1}$. Il existe $y^+, y^- \in A_1$ tels que $\overrightarrow{a} = y^+ - y^-$. Notons $y_2$ un vecteur de $A_2$. Comme $1 + 1 - 1 = 1$ et que $(x_2, y_2)$, $(x_1, y^+)$, $(x_1, y^-)$ sont des couples de la relation affine $\mathcal{R}$, on a $(x_2, y_2 + \overrightarrow{a}) = (x_2, y_2) + (x_1, y^+) - (x_1, y^{-1}) \in \mathcal{R}$. Ainsi, $y_2 + \overrightarrow{a} \in A_2$. On a montré que $\overrightarrow{a} = (y_2 + \overrightarrow{a}) - y_2 \in \overrightarrow{A_2}$. On a donc bien prouvé l'inclusion $\overrightarrow{A_1} \subseteq \overrightarrow{A_2}$. □

**Définition 8.25**
*La direction d'une relation affine non vide $\mathcal{R}$ est l'unique espace vectoriel noté $V(\mathcal{R})$ égal au vectorialisé de $\{y \in \mathbb{Q}^m;\ (x,y) \in \mathcal{R}\}$ pour tout $x \in D(\mathcal{R})$. On note $V(\emptyset) = \mathbb{Q}^m$.*

Pour montrer que $(V(\mathcal{R}^i))_{i\geqslant 0}$ est une suite croissante, on commence par prouver le lemme suivant.

**Lemme 8.26**
*Soit $\mathcal{R}$ une relation affine. Pour tout $i \geqslant 0$ et pour tout $x \in D(\mathcal{R}^{i+1})$, il existe $x' \in D(\mathcal{R}^i)$ tel que $(x,x') \in \mathcal{R}$.*

*Démonstration :*
Considérons $x \in D(\mathcal{R}^{i+1})$. Il existe alors $y \in \mathbb{Q}^m$ tel que $(x,y) \in \mathcal{R}^{i+1}$. Soit $x' \in \mathbb{Q}^m$ tel que $(x,x') \in \mathcal{R}$ et $(x',y) \in \mathcal{R}^i$. On déduit de $(x',y) \in \mathcal{R}^i$ que $x' \in D(\mathcal{R}^i)$. □

On peut alors montrer que la suite $(V(\mathcal{R}^i))_{i\geqslant 0}$ est croissante.

**Lemme 8.27**
*Soit $\mathcal{R}$ une relation binaire affine. La suite $(V(\mathcal{R}^i))_{i\geqslant 0}$ est croissante et stationnaire.*

*Démonstration :*
Montrons que pour tout $i \geqslant 0$, on a $V(\mathcal{R}^i) \subseteq V(\mathcal{R}^{i+1})$. On peut supposer que $\mathcal{R}^{i+1}$ est non vide car sinon $V(\mathcal{R}^{i+1}) = \mathbb{Q}^m$ et l'inclusion est vérifiée. Considérons alors $x \in D(\mathcal{R}^{i+1})$. D'après le lemme 8.26, il existe $x' \in D(\mathcal{R}^i)$ tel que $(x,x') \in \mathcal{R}$. De l'inclusion $\{y \in \mathbb{Q}^m;\ (x',y) \in \mathcal{R}^i\} \subseteq \{y \in \mathbb{Q}^m;\ (x,y) \in \mathcal{R}^{i+1}\}$, on déduit $V(\mathcal{R}^i) \subseteq V(\mathcal{R}^{i+1})$. On a donc prouvé que $(V(\mathcal{R}^i))_{i\geqslant 0}$ est une suite croissante d'espaces vectoriels. Cette suite est donc stationnaire. □

**Définition 8.28**
*La direction limite d'une relation affine $\mathcal{R}$ est l'espace vectoriel noté $V(\mathcal{R}^\infty)$ et défini par $V(\mathcal{R}^\infty) = \bigcup_{i\geqslant 0} V(\mathcal{R}^i)$.*

Le calcul de $V(\mathcal{R}^\infty)$ peut sembler plus compliqué que celui de $D(\mathcal{R}^\infty)$ car la suite $V(\mathcal{R}^\infty)$ n'est pas nécessairement strictement croissante avant de devenir stationnaire comme le montre l'exemple 8.29.

**Exemple 8.29**
*La relation affine $\mathcal{R}$ sur $\mathbb{Q}$ définie par $\mathcal{R} = \{(0,1)\}$ vérifie $V(\mathcal{R}^0) = V(\mathcal{R}^1) = \{0\}$ et pourtant $V(\mathcal{R}^2) = \mathbb{Q} \neq \{0\}$.*

Cependant, on va montrer que si le domaine de définition limite de $\mathcal{R}$ est non vide alors, la suite $(V(\mathcal{R}^i))_{i\geqslant 0}$ est bien strictement croissante avant de devenir stationnaire. On commence par montrer le lemme suivant.

**Lemme 8.30**
*Soit $\mathcal{R}$ une relation affine. Pour tout $x \in D(\mathcal{R}^\infty)$, il existe $x' \in D(\mathcal{R}^\infty)$ tel que $(x,x') \in \mathcal{R}$.*

*Démonstration :*

D'après le lemme 8.20, il existe $i_0 \geqslant 0$ tel que $D(\mathcal{R}^{i_0}) = D(\mathcal{R}^\infty)$. Considérons $x \in D(\mathcal{R}^\infty)$. De $D(\mathcal{R}^{i_0+1}) = D(\mathcal{R}^\infty)$, on déduit $x \in D(\mathcal{R}^{i_0+1})$. D'après le lemme 8.26, il existe $x' \in D(\mathcal{R}^{i_0}) = D(\mathcal{R}^\infty)$ tel que $(x, x') \in \mathcal{R}$. □

**Lemme 8.31**

*Soit $\mathcal{R}$ une relation affine dont le domaine de définition limite $D(\mathcal{R}^\infty) \neq \emptyset$ est non-vide. Pour tout indice $i_0 \geqslant 0$ tel que $V(\mathcal{R}^{i_0+1}) = V(\mathcal{R}^{i_0})$, on a $V(\mathcal{R}^i) = V(\mathcal{R}^{i_0})$ pour tout $i \geqslant i_0$.*

*Démonstration :*

Considérons un indice $i_0 \geqslant 0$ tel que $V(\mathcal{R}^{i_0+1}) = V(\mathcal{R}^{i_0})$. Il suffit de montrer que l'on a alors $V(\mathcal{R}^{i_0+2}) = V(\mathcal{R}^{i_0+1})$. Or, d'après le lemme 8.27, on a $V(\mathcal{R}^{i_0+1}) \subseteq V(\mathcal{R}^{i_0+2})$. Il suffit donc de montrer l'inclusion réciproque. Considérons alors $x \in D(\mathcal{R}^\infty)$. D'après le lemme 8.30, il existe $x' \in D(\mathcal{R}^\infty)$ tel que $(x, x') \in \mathcal{R}$. De l'inclusion $\{y \in \mathbb{Q}^m;\ (x', y) \in \mathcal{R}^{i_0}\} \subseteq \{y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}^{i_0+1}\}$ et de l'égalité $V(\mathcal{R}^{i_0+1}) = V(\mathcal{R}^{i_0})$, on déduit l'égalité $\{y \in \mathbb{Q}^m;\ (x', y) \in \mathcal{R}^{i_0}\} = \{y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}^{i_0+1}\}$. Considérons alors $y \in \mathbb{Q}^m$ tel que $(x, y) \in \mathcal{R}^{i_0+2}$. Soit $y' \in \mathbb{Q}^m$ tel que $(x, y') \in \mathcal{R}^{i_0+1}$ et $(y', y) \in \mathcal{R}$. De l'égalité $\{y \in \mathbb{Q}^m;\ (x', y) \in \mathcal{R}^{i_0}\} = \{y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}^{i_0+1}\}$, on déduit $(x', y') \in \mathcal{R}^{i_0}$. D'où $(x', y) \in \mathcal{R}^{i_0+1}$. On a donc prouvé l'inclusion $\{y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}^{i_0+2}\} \subseteq \{y \in \mathbb{Q}^m;\ (x', y) \in \mathcal{R}^{i_0+1}\}$. En prenant le vectorialisé de cette inclusion, on déduit $V(\mathcal{R}^{i_0+2}) \subseteq V(\mathcal{R}^{i_0+1})$. □

La proposition suivante montre que $(V(\mathcal{R}^i))_{i \geqslant 0}$ est stationnaire à partir de $i = m + 1$.

**Proposition 8.32**

*Pour toute relation affine $\mathcal{R}$, on a $V(\mathcal{R}^\infty) = V(\mathcal{R}^{m+1})$.*

*Démonstration :*

Remarquons que si $D(\mathcal{R}^\infty) = \emptyset$, la proposition montre que $D(\mathcal{R}^{m+1}) = \emptyset$. De $\mathcal{R}^{m+1} = \emptyset$, on déduit $V(\mathcal{R}^\infty) = \mathbb{Q}^m = V(\mathcal{R}^{m+1})$. On peut donc supposer que $D(\mathcal{R}^\infty) \neq \emptyset$. Considérons le premier indice $i_0 \geqslant 0$ tel que $V(\mathcal{R}^{i_0+1}) = V(\mathcal{R}^{i_0})$. D'après le lemme 8.31, on a $V(\mathcal{R}^\infty) = V(\mathcal{R}^i)$ pour tout $i \geqslant i_0$. Il suffit donc de prouver que $i_0 \leqslant m + 1$. Comme pour tout $i \in \{0, \dots, i_0 - 1\}$, on a $V(\mathcal{R}^i) \subsetneq V(\mathcal{R}^{i+1})$, on déduit $\dim(V(\mathcal{R}^i)) > \dim(V(\mathcal{R}^{i+1}))$. Ainsi, $\dim(V(\mathcal{R}^{i_0})) \geqslant i_0$. Comme $\dim(V(\mathcal{R}^{i_0})) \leqslant m$, on déduit $i_0 \leqslant m$. □

Ainsi, il suffit de calculer $V(\mathcal{R}^{m+1})$ pour obtenir $V(\mathcal{R}^\infty)$.

**Corollaire 8.33**

*La direction limite d'une relation affine est calculable en temps polynomial.*

*Démonstration :*

Considérons une relation affine $\mathcal{R}$ donnée par sa représentation canonique $\rho(\mathcal{R})$. On peut calculer en temps polynomial la représentation canonique $\rho(\mathcal{R}^{m+1})$. Si $\mathcal{R}^{m+1} = \emptyset$, alors $V(\mathcal{R}^{m+1}) = \mathbb{Q}^m$ est calculable en temps polynômial. Dans le cas où $\mathcal{R}^{m+1} \neq \emptyset$, on a $\rho(\mathcal{R}^{m+1}) = (a, M)$. Comme $a = (x_0, x_0') \in \mathcal{R}^{m+1}$, on déduit $x_0 \in D(\mathcal{R}^{m+1})$. L'espace affine

$\mathcal{R}^{m+1}\cap(\{x_0\}\times\mathbb{Q}^m)$ est alors calculable en temps polynômial. Considérons la fonction affine $f:\mathbb{Q}^m\times\mathbb{Q}^m\rightarrow\mathbb{Q}^m$ définie par $f(x,x')=x'$. Comme $V(\mathcal{R}^{m+1})=f(\mathcal{R}^{m+1}\cap(\{x_0\}\times\mathbb{Q}^m))$, on a prouvé que $V(\mathcal{R}^{\infty})=V(\mathcal{R}^{m+1})$ est calculable en temps polynômial. □

#### 8.4.1.3 Fonction affine associée

On peut alors montrer que les itérées d'une relation affine correspondent en fait aux itérées d'une fonction affine calculable en temps polynômial.

**Proposition 8.34**
*Pour toute relation affine $\mathcal{R}$, il existe une fonction affine $f:\mathbb{Q}^m\rightarrow\mathbb{Q}^m$ calculable en temps polynômial telle que pour tout $i\geqslant 0$, on a $f(D(\mathcal{R}^{i+1}))\subseteq D(\mathcal{R}^i)$ et on a aussi :*

$$\mathcal{R}^i=\{(x,x');\ x\in D(\mathcal{R}^i);\ x'\in f^i(x)+V(\mathcal{R}^i)\}$$

*Démonstration :*
On commence par montrer l'existence d'une fonction affine $f:\mathbb{Q}^m\rightarrow\mathbb{Q}^m$ telle que $f(D(\mathcal{R}^{i+1}))\subseteq D(\mathcal{R}^i)$ et telle que $(x,f(x))\in\mathcal{R}$ pour tout $x\in D(\mathcal{R})$. Comme la suite $D(\mathcal{R}^{\infty})=D(\mathcal{R}^{m+1})\subseteq D(\mathcal{R}^m)\subseteq\cdots\subseteq D(\mathcal{R}^0)=\mathbb{Q}^m$ est décroissante, on peut construire en temps polynomial une suite $(\mathcal{B}_i)_{0\leqslant i\leqslant m+1}$ de parties de $D(\mathcal{R}^i)$ telle que pour tout $i\in\{0,\ldots,m+1\}$, la partie $\mathcal{B}_{m+1}\cup\cdots\cup\mathcal{B}_i$ est une base de l'espace affine $D(\mathcal{R}^i)$. Pour tout $x\in\mathcal{B}_{i+1}$, d'après le lemme 8.26, il existe $g(x)\in D(\mathcal{R}^i)$ tel que $(x,g(x))\in\mathcal{R}$. Pour tout $x\in\mathcal{B}_0$, on pose $g(x)=x$. Comme $\bigcup_{i=0}^{m+1}\mathcal{B}_i$ est une base de l'espace affine $D(\mathcal{R}^0)=\mathbb{Q}^m$, il existe une unique fonction affine $f:Q^m\rightarrow\mathbb{Q}^m$ telle que pour tout $x\in\bigcup_{i=0}^{m+1}D(\mathcal{R}^i)$, on a $f(x)=g(x)$. Remarquons que par construction, pour tout $i\geqslant 0$, on a $f(D(\mathcal{R}^{i+1}))\subseteq D(\mathcal{R}^i)$. Montrons que pour tout $x\in D(\mathcal{R})$, on a $(x,f(x))\in\mathcal{R}$. Considérons $x\in D(\mathcal{R})$. comme $\mathcal{B}=\bigcup_{j=1}^{m+1}\mathcal{B}_j$ est une base de $D(\mathcal{R})$ et que $x\in D(\mathcal{R})$, il existe une suite $(q_y)_{y\in\mathcal{B}}$ de rationnels telle que $\sum_{y\in\mathcal{B}}q_y=1$ et $x=\sum_{y\in\mathcal{B}}q_y.y$. Comme $\mathcal{R}$ est un espace affine et que pour tout $y\in\mathcal{B}$, on a $(y,f(y))\in\mathcal{R}$, on déduit $(x,f(x))=\sum_{y\in\mathcal{B}}q_y.(y,f(y))\in\mathcal{R}$.Une récurrence sur $i\geqslant 0$ montre alors que pour tout $x\in D(\mathcal{R}^i)$, on a $(x,f^i(x))\in\mathcal{R}^i$. On déduit de $f^i(x)\in\{y\in\mathbb{Q}^m;\ (x,y)\in\mathcal{R}^i\}$ que $\{y\in\mathbb{Q}^m;\ (x,y)\in\mathcal{R}^i\}=f^i(x)+V(\mathcal{R}^i)$. On a donc prouvé le lemme. □

### 8.4.2 Un algorithme polynômial pour calculer l'enveloppe semi-affine étoile d'une relation affine

On commence par étudier la relation $\mathrm{saff}(\mathcal{R}^*)$ quand $\mathcal{R}$ correspond à une fonction. De ce cas particulier et de la proposition 8.34, on caractérise $\mathrm{saff}(\mathcal{R}^*)$ dans le cas général et on prouve en particulier l'égalité $\mathrm{saff}^*(\mathcal{R})=\mathrm{saff}(\mathcal{R}^*)$. On obtient ainsi un algorithme de calcul de $\mathrm{saff}^*(\mathcal{R})$ pour une relation affine $\mathcal{R}$ en temps polynômial en la taille de $\mathcal{R}$ et la taille de $\mathrm{saff}^*(\mathcal{R})$.

On commence par prouver deux lemmes techniques qui nous servirons à prouver la proposition 8.37. On note $C_n^p=\frac{n!p!}{(n-p)!}$.

**Lemme 8.35**
*Soient $m \geqslant 1$ et $I \subseteq \{m, \ldots, \infty\}$ une partie infinie. Il existe une partie finie $P \subseteq I \times I$ et une suite $(q_p)_{p \in P}$ de $\mathbb{Q}$ telles que :*

$$\sum_{(i,i') \in P} q_{(i,i')}.(C_i^k - C_i^{k'}) = \begin{cases} 1 & \textit{pour } k = 1 \\ 0 & \textit{pour tout } k \in \{2, \ldots, m\} \end{cases}$$

*Démonstration :*

On va montrer que l'espace vectoriel $V$ engendré par la partie $\{(C_i^k - C_{i'}^k)_{1 \leqslant k \leqslant m};\ i, i' \in I\}$ est égal à $\mathbb{Q}^m$. Supposons par l'absurde que $V \neq \mathbb{Q}^m$. Dans ce cas, il existe une suite $(c_k)_{1 \leqslant k \leqslant \alpha - 1}$ de rationnels non tous nuls telle que pour tout $i, i' \in I$, on a $\sum_{k=1}^m c_k.(C_i^k - C_{i'}^k) = 0$ Considérons les polynômes $P_k(X) = \frac{1}{k!}.X.(X-1)\ldots(X-k+1)$ pour $k \geqslant 0$ et le polynôme $P$ défini par $P(X) = \sum_{k=1}^m c_k.P_k(X)$. Pour tout $i, i' \in I$, on a $P(i) - P(i') = \sum_{k=1}^m c_k.(C_i^k - C_{i'}^k) = 0$. Ainsi, le polynôme $P(X) - P(i).P_0(X)$ admet une infinité de racines $i'$ distinctes. Ce polynôme est donc nul. Comme la famille $(P_k)_{k \geqslant 0}$ est libre dans l'espace vectoriel $\mathbb{Q}[X]$, on a $c_k = 0$ pour tout $k$, ce qui est absurde. On a donc montré que $V = \mathbb{Q}^m$. En particulier, on a $(1, 0, \ldots, 0) \in V$ et par définition de $V$, il existe une partie finie $P \subseteq I \times I$ et une suite $(q_p)_{p \in P}$ vérifiant le lemme. □

**Lemme 8.36 ([AF88])**
*Soient $P_1$, ..., $P_n$ une suite finie de polynômes de $\mathbb{Q}[X]$ deux à deux premiers entre eux et $l : V \to V$ une fonction linéaire. Les espaces vectoriels $\ker(P_1(l))$, ..., $\ker(P_n(l))$ sont en somme directe et on a :*

$$\ker((P_1.\ldots.P_n)(l)) = \ker(P_1(l)) \oplus \cdots \oplus \ker(P_n(l))$$

*De plus, pour tout $v \in V$, on peut calculer en temps polynômial une suite $(v_i)_{1 \leqslant i \leqslant n}$ de $\ker(P_i(l))$ telle que $v = \sum_{i=1}^n v_i$.*

*Démonstration :*

On donne la preuve de ce lemme pour éviter au lecteur la lecture de différentes parties de [AF88].

Pour montrer que les espaces vectoriels $\ker(P_1(l))$, ..., $\ker(P_n(l))$ sont en somme directe, il suffit de montrer que pour toute somme nulle $\sum_{i=1}^n v_i = \overrightarrow{0}$ avec $v_i \in \ker(P_i(l))$, on a $v_i = \overrightarrow{0}$ pour tout $i$. Comme $P_i$ est premier avec $P_1 \ldots P_{i-1}.P_{i+1} \ldots P_n$, il existe deux polynômes $Q_i$ et $Q'_i$ tels que $Q_i.P_i + Q'_i.P_1 \ldots P_{i-1}.P_{i+1} \ldots P_n = 1$. De $v_i = -(v_1 + \cdots + v_{i-1} + v_{i+1} + \cdots + v_n)$, on déduit $v_i = Q_i(l) \circ P_i(l)(v_i) + (Q'_i.P_1 \ldots P_{i-1}.P_{i+1} \ldots P_n)(l)(-(v_1 + \cdots + v_{i-1} + v_{i+1} + \cdots + v_n)) = \overrightarrow{0} + \overrightarrow{0} = \overrightarrow{0}$. On a donc bien prouvé que les espaces vectoriels $\ker(P_1(l))$, ..., $\ker(P_n(l))$ sont en somme directe. Montrons alors l'égalité $\ker((P_1.\ldots.P_n)(l)) = \ker(P_1(l)) \oplus \cdots \oplus \ker(P_n(l))$ Comme $\ker(P_i(l)) \subseteq \ker((P_1.\ldots.P_n)(l))$, on a l'inclusion $\ker(P_1(l)) \oplus \cdots \oplus \ker(P_n(l)) \subseteq \ker((P_1.\ldots.P_n)(l))$. Il suffit donc de prouver l'inclusion réciproque. Considérons $v \in \ker((P_1.\ldots.P_n)(l))$. Comme les polynômes $P_1 \ldots P_{i-1}.P_{i+1} \ldots P_n$ sont premiers entre eux, il existe une suite de polynômes $(Q''_i)_{1 \leqslant i \leqslant n}$

de $\mathbb{Q}[X]$ (calculable en temps polynômial par l'algorithme d'Euclide) telle que

$$1 = \sum_{i=1}^{n} Q''_i.P_1 \dots P_{i-1}.P_{i+1} \dots P_n$$

Notons alors $v_i = (Q''_i.P_1 \dots P_{i-1}.P_{i+1} \dots P_n)(l)(v)$. Comme $v \in \ker(P_1 \dots P_n(l))$, on a $P_i(l)(v_i) = \overrightarrow{0}$ et donc $v_i \in \ker(P_i(l))$. De plus $v = \sum_{i=1}^{n} v_i$. □

De la proposition suivante, on peut déduire un algorithme de calcul de l'enveloppe semi-affine de l'itérée d'une fonction affine.

**Proposition 8.37**
*Soient $f : D \to D$ une fonction affine définie sur un espace affine non vide $D$ et $\mathcal{R} = \{(x, f(x);\ x \in D\}$ la relation affine associée à $f$. Il existe un espace vectoriel $W$ calculable en temps polynômial tel que :*
– $\overrightarrow{f}(W) = W$,
– $\{\mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W; r \geqslant 0\}$ *est un ensemble fini d'au plus* $(4.m)^{2.m}$ *relations affines de taille polynomiale en la taille de* $\mathcal{R}$, *et*
– saff $\left(\bigcup_{i \geqslant m+1}^{\infty} \mathcal{R}^i\right) = \bigcup_{r \geqslant 0} \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$.

*Démonstration :*
On note $l : \overrightarrow{D} \to \overrightarrow{D}$, le linéarisé de la fonction affine $f : D \to D$. Rappelons que la suite des polynômes cyclotomiques $(\phi_i)_{i \geqslant 1}$ est caractérisée par l'égalité suivante, vraie pour tout $n \geqslant 1$ :

$$X^n - 1 = \prod_{i|n} \phi_i(X)$$

Rappelons aussi qu'en temps polynômial, on peut calculer le polynôme caractéristique de $l$ noté $P_l(X) \in \mathbb{Q}[X]$. On a alors $P_l(l) = 0$ ([AF88]). Rappelons enfin ([Boi98], [Knu69]) qu'en temps polynomial on peut calculer une partie finie $J_0 \subseteq \mathbb{N}^*$, une suite $(\alpha_j)_{j \in J_0}$ de $\mathbb{N}^*$, un entier $r_0 \geqslant 0$ et un polynôme $P_\infty$ tels que :
– $P_l = X^{r_0}.P_\infty.\prod_{j \in J_0} \phi_j^{\alpha_j}$, et
– les polynômes $X$, $P_\infty$ et $\phi_i$ pour tout $i \geqslant 1$ sont premiers entre eux.
Posons $J = J_0 \cup \{1\}$ et considérons le polynôme $P = X^m.P_\infty.\prod_{j \in J} \phi_j^m$. Montrons que le polynôme $P_l$ divise le polynôme $P$. Comme $P_l$ est de degré $\dim(\overrightarrow{D}) \leqslant m$, on a $r_0 \leqslant m$ et pour tout $j \in J_0$, on a $\alpha_j \leqslant m$. Ainsi, les polynômes $X^m$, $P_\infty$ et $(\phi_j^m)_{j \in J_0}$ divisent $P$. Comme ces polynômes sont deux à deux premiers entre eux, on a prouvé que $P_l$ divise $P$.

En particulier, on a $P(l) = 0$ et le lemme 8.36 prouve alors que $\overrightarrow{D} = \ker(l^m) \oplus \ker(P_\infty(l)) \oplus_{j \in J} \ker(\phi_j^m(l))$. On note $V_0 = \ker(l^m)$, $V_\infty = \ker(P_\infty(l))$ et pour tout $j \in J$, on note $V_j = \ker(\phi_j^m(l))$. Remarquons que ces espaces vectoriels sont calculables en temps polynomial. De plus, comme $l$ laisse stable ces espaces, on peut considérer les restrictions $l_0 : V_0 \to V_0$, $l_\infty : V_\infty \to V_\infty$ et $l_j : V_j \to V_j$ de $l$ à ces espaces.

On note $[k]_i$ le reste de la division euclidienne de $k$ par $i$ pour $i \geqslant 1$.

On pose $\Delta = \mathrm{ppcm}(J)$ le plus petit commun diviseur des entiers de $J$. Remarquons que $\Delta$ est calculable en temps polynômial par un algorithme d'Euclide. Montrons que

$\Delta \leqslant (4.m)^{2.m}$. D'après [Boi98], on a $\max(J) \leqslant 210.(\frac{m}{48})^{\frac{\ln(11)}{\ln(10)}} \leqslant (4.m)^2$. Ainsi, comme $\mathrm{card}(J) \leqslant m+1$ et que $1 \in J$, on a $\Delta = \mathrm{ppcm}(J) \leqslant \prod_{j\in J} j \leqslant (4.m)^{2.m}$.

On a décomposé le reste de la preuve en plusieurs étapes correspondant à des lemmes qui ne peuvent être sortis de la preuve car ils utilisent des notations introduites précédemment.

**1ère étape :** on montre qu'il existe $d_1 \in D$ et $x_1 \in V_1$ calculable en temps polynômial tels que $x_1 = f(d_1) - d_1$. On commence par montrer que l'on peut construire en temps polynômial un vecteur $d \in D$. Comme la représentation de $D$ est $\rho(D) = (d, M_D)$ alors $d \in D$ et $d$ a une taille polynomial. On note $J' = J\backslash\{1\}$. On considère alors $V = V_0 \oplus V_\infty \oplus_{j'\in J'} V_{j'}$. D'après le lemme 8.36, on a $\overrightarrow{D} = V \oplus V_1$. Ainsi, on peut calculer en temps polynomial $v \in V$ et $x_1 \in V_1$ tels que $f(d) - d = v + x_1$. Comme $l$ laisse stable $V$, on peut considérer la restriction de $l$ à $V$ notée $l_V : V \to V$. Comme les polynômes $(X-1)$ et $X^m.P_\infty.\sum_{j'\in J'} \phi_{j'}^{\alpha_{j'}}$ sont premiers entre eux, la fonction $(X-1)(l_V)$ est injective et donc bijective. Ainsi, on peut calculer en temps polynomial un vecteur $v' \in V$ tel que $l(v') - v' = v$. Le vecteur $d_1 = d - v'$ vérifie alors $f(d_1) - d_1 = f(d) - d + v' - l(v') = x_1$. Comme $x_1 \in V_1$, on a prouvé l'étape.

**Notation :** notons $W$ l'espace vectoriel défini par :

$$W = V_\infty + \sum_{j\in J} \phi_j(l)(V_j) + \mathbb{Q}.x_1$$

Remarquons que cet espace vectoriel est calculable en temps polynomial.

**2ème étape :** montrons que $l(W) = W$.
Considérons $w \in W$. Il existe alors $v_\infty \in V_\infty$, $(v_j)_{j\in J}$ dans $V_j$ et $t \in \mathbb{Q}$ tels que $w = v_\infty + \sum_{j\in J} \phi_j(l)(v_j) + t.x_1$. On a alors $l(w) = l_\infty(v_\infty) + \sum_{j\in J} \phi_j(l)(l_j(v_j)) + t.(l_1(x_1) - x_1) + t.x_1$. Comme $l_1(x_1) - x_1 = \phi_1(l_1)(x_1) \in W$, on a prouvé que $l(W) \subseteq W$. Enfin, comme les polynômes $X^r$ et $P_\infty.\prod_{j\in J} \phi_j^m$ sont premiers entre eux, la restriction de $l$ à $W$ est injective et donc bijective. On a donc $l(W) = W$.

**3ème étape :** pour tout $r \geqslant 0$, pour tout $v_0 \in V_0$, pour tout $v_\infty \in V_\infty$ et pour tout $(v_j)_{j\in J}$ dans $V_j$, on a :

$$f^{m+1+r}(d_1 + v_0 + v_\infty + \sum_{j\in J} v_v) = d_1 + l_\infty^{m+1+r}(v_\infty) + \sum_{j\in J} l_j^{m+1+r}(v_j) + \sum_{k=0}^{m+1+r} l_1^k(x_1)$$

Cette égalité provient simplement de $l_0^m(v_0) = 0$.

**4ème étape :** on montre que pour tout $i \geqslant 0$, pour tout $j \in J$ et pour tout $v_j \in V_j$, on a :

$$l_j^i(v_j) \in l_j^{[i]_j}(v_j) + \phi_j(l_j)(V_j) \tag{8.1}$$

Notons $q$ le quotient de la division euclidienne de $i$ par $j$. On a alors $i = q.j + [i]_j$. De l'égalité $l_j^i(v_j) = l_j^{[i]_j}(v_j) + (X^j - 1)(l_j)(\sum_{k=0}^{q-1} l_j^{k.j+[i]_j}(v_j))$, on déduit $l_j^i(v_j) \in l_j^{[i]_j} + (X^j - 1)(l_j)(V_j)$.

Comme $\phi_j$ divise $X^j - 1$, il existe un polynôme $Q$ tel que $X^j - 1 = \phi_j.Q$. On a donc prouvé que $l_j^i(v_j) \in l_j^{[i]_j} + (X^j - 1)(l_j)(V_j) \subseteq l_j^{[i]_j} + \phi_j(l_j)(V_j)$. On a donc prouvé l'inclusion (8.1).

**5ème étape :** on montre que pour tout $r \geqslant 0$, pour tout $v_0 \in V_0$, pour tout $v_1 \in V_\infty$, pour tout $(v_j)_{j \in J}$ dans $V_j$, on a :

$$f^{m+1+r}(d_1 + v_0 + v_\infty + \sum_{j \in J} v_j) + W = d_1 + \sum_{j \in J} l^{[m+1+r]_j}(v_j) + W \tag{8.2}$$

Il suffit d'appliquer l'inclusion (8.1) à chaque terme $l^{m+1+r}(v_j)$ en remarquant que $\phi_j(l_j)(V_j) \subseteq W$.

**6ème étape :** pour tout $i \geqslant 0$ et pour tout $r \geqslant 0$, on a

$$\mathcal{R}^{m+1+r+\Delta} + \{\overrightarrow{0}\} \times W = \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W \tag{8.3}$$

C'est une conséquence immédiate de l'égalité (8.2).

**7ème étape :** pour tout $r \geqslant 0$, la relation $\mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$ a une taille polynomiale en la taille de $\mathcal{R}$. C'est aussi une conséquence immédiate de l'égalité (8.2).

**8ème étape :** pour tout $r \geqslant 0$, on a l'inclusion suivante :

$$\mathrm{saff}\left(\bigcup_{i=m+1}^{\infty} \mathcal{R}^i\right) \subseteq \bigcup_{r=0}^{\Delta-1} \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W \tag{8.4}$$

Pour tout $r \geqslant 0$ et pour tout $i \geqslant 0$, on a $\mathcal{R}^{m+1+r+i.\Delta} \subseteq \mathcal{R}^{m+1+r+i.\Delta} + \{\overrightarrow{0}\} \times W = \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$. Ainsi, $\bigcup_{i \geqslant 0}^{\infty} \mathcal{R}^{m+1+r+i.\Delta} \subseteq \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$. Par minimalité de l'enveloppe semi-affine, on déduit l'inclusion $\mathrm{saff}(\bigcup_{i \geqslant 0}^{\infty} \mathcal{R}^{m+1+r+i.\Delta}) \subseteq \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$. On obtient ainsi l'inclusion (8.4).

**9 ème étape :** on montre l'inclusion réciproque de (8.4) :

$$\bigcup_{r=0}^{\Delta-1} \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W \subseteq \mathrm{saff}\left(\bigcup_{i=m+1}^{\infty} \mathcal{R}^i\right) \tag{8.5}$$

Considérons $r \geqslant 0$, notons $S$ le semi-affine $S = \mathrm{saff}(\bigcup_{i \geqslant 0}^{\infty} \mathcal{R}^{m+1+r+i.\Delta})$ et $r'$ l'entier $r' = m + 1 + r$. Pour tout $i \geqslant 0$, on a $\mathcal{R}^{r'+i.\Delta} \subseteq S$. La proposition 3.16 montre qu'il existe une composante affine $\mathcal{R}_r \in \mathrm{comp}(S)$ telle que $\mathcal{R}^{r'+i.\Delta} \subseteq \mathcal{R}_r$. Comme l'ensemble des composantes de $S$ est fini, il existe une composante $\mathcal{R}_r$ telle que l'ensemble $I = \{i \geqslant 0;\ \mathcal{R}^{r'+i.\Delta} \subseteq \mathcal{R}_r\}$ soit infini. On va prouver que la direction $V(\mathcal{R}_r)$ contient $W$ en prouvant que les espaces vectoriels $\phi_j(l)(V_j)$ pour $j \in J$, $V_\infty$ et $\mathbb{Q}.x_1$ sont inclus dans $V(\mathcal{R}_r)$.

Montrons que $\phi_j(l)(V_j) \subseteq V(\mathcal{R}_r)$. Remarquons que si $m < 2$ alors $\phi_j(l)(V_j) = \{\overrightarrow{0}\}$ et l'inclusion est évidente. On peut donc supposer que $m \geqslant 2$. Pour tout $i, i' \in I$, pour tout

$j \in J$ et pour tout $v_j \in V_j$, on a :

$$\begin{aligned} V(\mathcal{R}_r) &\ni (f^{r'+i.\Delta}(d_1 + v_j) - f^{r'+i'.\Delta}(d_1 + v_j)) - (f^{r'+i.\Delta}(d_1) - f^{r'+i'.\Delta}(d_1)) \\ &= l_j^{r'+i.\Delta}(v_j) - l_1^{r'+i'.\Delta}(v_j) \in V(\mathcal{R}_r) \end{aligned}$$

Remarquons que pour $k \geqslant m$, le polynôme $\phi_j^m$ divise $(X^\Delta - 1)^k$, ainsi pour tout $k \geqslant m$, on a $(X^\Delta - 1)^k(l_j) = 0$. On a donc pour $i \geqslant m - 1$ :

$$\begin{aligned} l_j^{r'+i.\Delta}(v_j) &= ((1 + (X^\Delta - 1))^i.X^{r'})(l_j)(v_j) \\ &= \sum_{k=0}^{m-1} C_i^k (X^\Delta - 1)^k (l_j)(l_1^{r'}(v_j)) \end{aligned}$$

Pour tout $i, i' \in I$ tels que $i, i' \geqslant m - 1$ et pour tout $v_j \in V_j$, on a donc :

$$\sum_{k=1}^{m-1} (C_i^k - C_{i'}^k).(X^\Delta - 1)^k (l_j)(l_j^{r'}(v_j)) \in V(\mathcal{R}_r)$$

En appliquant le lemme 8.35, on obtient alors $(X^\Delta - 1)(l_j)(l_j^{r'}(V_j)) \subseteq V(\mathcal{R}_r)$. Comme les polynômes $X^{r'}$ et $\phi_j^m$ sont premiers entre eux, le lemme 8.36 montre que la fonction linéaire $l_j^{r'}$ est injective et donc bijective. En particulier, on a $l_j^{r'}(V_j) = V_j$. On a donc prouvé l'inclusion $(X^\Delta - 1)(l_j)(V_j) \subseteq V(\mathcal{R}_r)$. Posons $J' = J \backslash \{j\}$. Comme $X^\Delta - 1 = \phi_j Q$ où $Q = \prod_{j' \in J'} \phi_{j'}$, les polynômes $Q$ et $\phi_j$ sont premiers entre eux. Le lemme 8.36 montre que la fonction $Q(l_j)$ est injective et donc bijective. Ainsi $(X^\Delta - 1)(l_j)(V_j) = \phi_j(l_j) \circ Q(l_j)(V_j) = \phi_j(l_j)(V_j)$. On donc bien prouvé que $\phi_j(l)(V_j) = \phi_j(l_j)(V_j) \subseteq V(\mathcal{R}_r)$.

Montrons que $V_\infty \subseteq V(\mathcal{R}_r)$. Pour tout couple $i, i' \in I$ et pour tout $v_\infty \in V_\infty$, on a :

$$\begin{gathered} f^{r'+i.\Delta}(d_1 + v_\infty) - f^{r'+i'.\Delta}(d_1 + v_\infty) \in V(\mathcal{R}_r) \\ f^{r'+i.\Delta}(d_1) - f^{r'+i'.\Delta}(d_1) \in V(\mathcal{R}_r) \end{gathered}$$

En prenant la différence de ces deux éléments de $V(\mathcal{R}_r)$, on déduit :

$$l_\infty^{r'+i.\Delta}(v_\infty) - l_\infty^{r'+i'.\Delta}(v_\infty) \in V(\mathcal{R}_r)$$

Comme $I$ est infini, il contient au moins deux éléments distincts notés $i > i'$. Comme les polynômes $P_\infty$ et $X^{r'+i.\Delta} - X^{r'+i'.\Delta} = X^{r'+i'.\Delta}.(X^{(i-i').\Delta} - 1) = X^{r'+i'.\Delta}.\prod_{k|((i-i').\Delta)} \phi_k$ sont premiers entre eux, le lemme 8.36 montre que la fonction linéaire $l_\infty^{r'+i.\Delta} - l_\infty^{r'+i'.\Delta}$ est injective et donc bijective. On a donc $V_\infty = (l_\infty^{r'+i.\Delta} - l_\infty^{r'+i'.\Delta})(V_\infty) \subseteq V(\mathcal{R}_r)$.

Montrons maintenant que $\mathbb{Q}.x_1 \subseteq V(\mathcal{R}_r)$. Soit $i > i'$ dans $I$. On a :

$$f^{r'+i.\Delta}(d_1) - f^{r'+i'.\Delta}(d_1) \in V(\mathcal{R}_r)$$

Ainsi, $\sum_{k=r'+i'.\Delta}^{r'+i.\Delta-1} l_1^k(x_1) \in V(\mathcal{R}_r)$. De $\phi_1(l_1)(V_1) \subseteq V(\mathcal{R}_r)$, on déduit en utilisant l'égalité (8.1) que $(i - i').\Delta.x_1 \in V(\mathcal{R}_r)$. D'où $\mathbb{Q}.x_1 \subseteq V(\mathcal{R}_r)$.

On a donc bien prouvé que $W \subseteq V(\mathcal{R}_r)$. Considérons alors un indice $i \in I$. De $\mathcal{R}^{r'+i.\Delta} \subseteq \mathcal{R}_r$ et $W \subseteq V(\mathcal{R}_r)$, on déduit $\mathcal{R}^{r'+i.\Delta} + \{\overrightarrow{0}\} \times W \subseteq \mathcal{R}_r$. L'égalité (8.3) montre que $\mathcal{R}^{r'+i.\Delta} + \{\overrightarrow{0}\} \times W = \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$. On a donc prouvé que pour tout $r \geqslant 0$, on a $\mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W \subseteq \mathrm{saff}(\bigcup_{i\geqslant 0}^{\infty} \mathcal{R}^{m+1+r+i.\Delta})$. On a donc prouvé l'inclusion (8.5).

**10 ètape (finale) :** en utilisant les inclusions (8.4) et (8.5), on déduit l'égalité suivante :

$$\mathrm{saff}(\bigcup_{i=m+1}^{\infty} \mathcal{R}^i) = \bigcup_{r=0}^{\Delta-1} \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$$

□

Rappelons que l'objectif de cette sous-section est de donner un algorithme pour calculer l'enveloppe semi-affine d'une relation affine. On doit donc généraliser le lemme précédent à des relations affines $\mathcal{R}$ qui ne sont pas nécessairement des fonctions affines. On commence par prouver les deux lemmes suivants.

**Lemme 8.38**
*Soient $\mathcal{R} \subseteq \mathcal{R}'$ deux relations affines telles que $D(\mathcal{R}') \subseteq D(\mathcal{R})$ et $V(\mathcal{R}') \subseteq V(\mathcal{R}')$. Alors $\mathcal{R} = \mathcal{R}'$.*

*Démonstration :*
Considérons $(x, y) \in \mathcal{R}'$. On a alors $x \in D(\mathcal{R}') \subseteq D(\mathcal{R})$. Ainsi, il existe $y' \in \mathbb{Q}^m$ tel que $(x, y') \in \mathcal{R}$. Comme $\mathcal{R} \subseteq \mathcal{R}'$, on a $(x, y') \in \mathcal{R}'$. Comme $(x, y)$ et $(x, y')$ sont dans $\mathcal{R}'$, on a $y - y' \in V(\mathcal{R}')$. De $V(\mathcal{R}') \subseteq V(\mathcal{R})$, on déduit $y - y' \in V(\mathcal{R})$. Comme $(x, y') \in \mathcal{R}$ et $y - y' \in V(\mathcal{R})$, on a $(x, y) = (x, y') + (\overrightarrow{0}, y' - y) \in \mathcal{R}$. On a donc prouvé que $\mathcal{R}' \subseteq \mathcal{R}$. □

**Lemme 8.39**
*Soient $\mathcal{R}$ et $\mathcal{R}'$ deux relations binaires sur $\mathbb{Q}^m$ et $W$ une partie de $\mathbb{Q}^m$. On a les deux égalités suivantes :*

$$\mathcal{R}.(\mathcal{R}' + (\{\overrightarrow{0}\} \times W)) = (\mathcal{R}.\mathcal{R}') + (\{\overrightarrow{0}\} \times W)$$
$$(\mathcal{R} + (W \times \{\overrightarrow{0}\})).\mathcal{R}' = (\mathcal{R}.\mathcal{R}') + (W \times \{\overrightarrow{0}\})$$

*Démonstration :*
Considérons $(x, y') \in \mathcal{R}.(\mathcal{R}' + (\{\overrightarrow{0}\} \times W))$. Il existe alors $y \in \mathbb{Q}^m$ telle que $(x, y) \in \mathcal{R}$ et $(y, y') \in \mathcal{R}' + (\{\overrightarrow{0}\} \times W)$. Ainsi, il existe $y'_0 \in \mathbb{Q}^m$ et $w \in W$ tels que $(y, y'_0) \in \mathcal{R}'$ et $y' = y'_0 + w$. On a donc $(x, y'_0) \in \mathcal{R}.\mathcal{R}'$. De $(x, y') = (x, y'_0) + (\overrightarrow{0}, w)$, on déduit $(x, y') \in (\mathcal{R}.\mathcal{R}') + (\{\overrightarrow{0}\} \times W)$. Réciproquement, considérons $(x, y') \in (\mathcal{R}.\mathcal{R}') + (\{\overrightarrow{0}\} \times W)$. Il existe alors $y'_0 \in \mathbb{Q}^m$ et $w \in W$ tels que $(x, y'_0) \in \mathcal{R}.\mathcal{R}'$ et $y' = y'_0 + w$. Soit $y \in \mathbb{Q}^m$ tel que $(x, y) \in \mathcal{R}$ et $(y, y'_0) \in \mathcal{R}'$. De $(y, y') = (y, y'_0) + (\overrightarrow{0}, w)$, on déduit $(x, y') \in \mathcal{R}.(\mathcal{R}' + (\{\overrightarrow{0}\} \times W))$. On a donc prouvé l'égalité $\mathcal{R}.(\mathcal{R}' + (\{\overrightarrow{0}\} \times W)) = (\mathcal{R}.\mathcal{R}') + (\{\overrightarrow{0}\} \times W)$. En prenant l'inverse de cette égalité, on déduit alors la deuxième égalité du lemme. □

On peut alors prouver la proposition suivante qui aura comme corollaire le calcul en temps polynômial de la relation $\mathrm{saff}^*(\mathcal{R})$.

**Proposition 8.40**
*On a* $\mathrm{saff}^*(\mathcal{R}) = \mathrm{saff}(\mathcal{R}^*)$ *pour toute relation affine* $\mathcal{R}$*. De plus, on peut calculer en temps polynômial une relation affine* $\mathcal{R}_0$ *qui commute avec* $\mathcal{R}$ *et telle que l'ensemble* $\mathcal{C} = \{\mathcal{R}^r.\mathcal{R}_0;\ r \geqslant 0\}$ *vérifie :*

- *le cardinal de* $\mathcal{C}$ *est borné par* $(4.m)^{2.m}$,
- *les relations affines de* $\mathcal{C}$ *ont une taille bornée polynomialement en la taille de* $\mathcal{R}$,
- *les relations affines de* $\mathcal{C}$ *sont deux à deux incomparables (pour* $\subseteq$*),*
- *la relation* $\mathcal{R}_0.\mathcal{R}_0$ *est dans* $\mathcal{C}$*, et*
- $\mathrm{saff}(\mathcal{R}^*) = \left(\bigcup_{i=0}^m \mathcal{R}^i\right) \cup \left(\bigcup_{\mathcal{R}' \in \mathcal{C}} \mathcal{R}'\right)$.

*Démonstration :*

Remarquons que si $D(\mathcal{R}^\infty) = \emptyset$ alors $\mathcal{R}^{m+1} = \emptyset$ et on a dans ce cas $\mathrm{saff}^*(\mathcal{R}) = \bigcup_{i=0}^m \mathcal{R}^i$. L'espace affine $\mathcal{R}_0 = \emptyset$ convient. On peut donc supposer que $D(\mathcal{R}^\infty) \neq \emptyset$. La proposition 8.34 montre l'existence d'une fonction affine $f : \mathbb{Q}^m \to \mathbb{Q}^m$ calculable en temps polynômial telle que pour tout $i \geqslant 0$, on a $f(D(\mathcal{R}^{i+1})) \subseteq D(\mathcal{R}^i)$ et on a :

$$\mathcal{R}^i = \{(x, x');\ x \in D(\mathcal{R}^i);\ x' \in f^i(x) + V(\mathcal{R}^i)\}$$

En particulier, on a $f(D(\mathcal{R}^\infty)) \subseteq D(\mathcal{R}^\infty)$ et on a pour tout $i \geqslant m+1$,

$$\mathcal{R}^i = \{(x, x');\ x \in D(\mathcal{R}^\infty);\ x' \in f^i(x) + V(\mathcal{R}^\infty)\}$$

Notons $\mathcal{R}_f$ la relation affine définie par $\mathcal{R}_f = \{(x, f(x));\ x \in D(\mathcal{R}^\infty)\}$. La proposition 8.37 montre l'existence d'un espace vectoriel $W \subseteq \overrightarrow{D(\mathcal{R}^\infty)}$ calculable en temps polynomial tel que $\overrightarrow{f}(W) = W$ et tel que $\{\mathcal{R}_f^{m+1+r} + \{\overrightarrow{0}\} \times W;\ r \geqslant 0\}$ contient au plus $(4.m)^{2.m}$ espaces affines de taille polynomiale en la taille de $\mathcal{R}_f$ et tel que :

$$\mathrm{saff}\left(\bigcup_{j \geqslant m+1}^{\infty} \mathcal{R}_f^j\right) = \bigcup_{r \geqslant 0} \mathcal{R}_f^{m+1+r} + \{\overrightarrow{0}\} \times W$$

On a alors :

$$\begin{aligned}
\mathrm{saff}(\mathcal{R}^*) &= \left(\bigcup_{i=0}^m \mathcal{R}^i\right) \cup \mathrm{saff}\left(\bigcup_{i=m+1}^{\infty} \{(x, x');\ x \in D(\mathcal{R}^\infty);\ x' \in f^i(x) + V(\mathcal{R}^\infty)\}\right) \\
&= \left(\bigcup_{i=0}^m \mathcal{R}^i\right) \cup \left(\mathrm{saff}\left(\bigcup_{i=m+1}^{\infty} \mathcal{R}_f^i\right) + \{\overrightarrow{0}\} \times V(\mathcal{R}^\infty)\right) \\
&= \left(\bigcup_{i=0}^m \mathcal{R}^i\right) \cup \left(\left(\bigcup_{r \geqslant 0} \mathcal{R}_f^{m+1+r} + \{0\} \times W\right) + \{\overrightarrow{0}\} \times V(\mathcal{R}^\infty)\right) \\
&= \left(\bigcup_{i=0}^m \mathcal{R}^i\right) \cup \left(\bigcup_{r \geqslant 0} \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W\right)
\end{aligned}$$

Montrons que pour tout $i \geqslant 0$ on a :

$$\mathcal{R}^i + \{\overrightarrow{0}\} \times W = \mathcal{R}^i + W \times W = \mathcal{R}^i + W \times \{\overrightarrow{0}\} \tag{8.6}$$

Comme $\mathcal{R}^i + \{\overrightarrow{0}\} \times W$ et $\mathcal{R}^i + W \times \{\overrightarrow{0}\}$ sont deux relations affines incluses dans $\mathcal{R}^i + W \times W$, il suffit de prouver les deux inclusions réciproques. Considérons alors $(x, y) \in \mathcal{R}^i + W \times W$. Soient $(w, w') \in W \times W$ et $(x', y') \in \mathcal{R}^i$ tels que $(x, y) = (x', y') + (w, w')$. Comme $(x', y') \in \mathcal{R}^i$, il existe $v \in V(\mathcal{R}^i)$ tel que $y' = f^i(x') + v$. On a alors $(x, y) = (x' + w, f^i(x') + v + w')$. Commençons par montrer que $(x, y) \in \mathcal{R}^i + \{\overrightarrow{0}\} \times W$. Comme $\overrightarrow{f^i}(W) \subseteq W$, on a $\overrightarrow{f^i}(w) \in W$. De $(x, y) = (x' + w, f^i(x' + w)) + (\overrightarrow{0}, v + (w' - \overrightarrow{f^i}(w)))$, on déduit $(x, y) \in \mathcal{R}^i_f + \{\overrightarrow{0}\} \times (V(\mathcal{R}^i) + W) = \mathcal{R}^i + \{\overrightarrow{0}\} \times W$. Montrons alors que $(x, y) \in \mathcal{R}^i + W \times \{\overrightarrow{0}\}$. Comme $\overrightarrow{f^i}(W) = W$, il existe $w'' \in W$ tel que $\overrightarrow{f^i}(w'') = w'$. De $(x, y) = (x' + w'', f^i(x' + w'')) + (w' - w'', v)$, on déduit $(x, y) \in \mathcal{R}^i_f + W \times V(\mathcal{R}^i) = \mathcal{R}^i + W \times \{\overrightarrow{0}\}$. On donc bien prouvé l'égalité (8.6).

Posons $\mathcal{R}_0 = \mathcal{R}^{m+1} + W \times W$. Cette relation affine est donc calculable en temps polynomial. Le lemme 8.39 montre que $\mathcal{R}^r.\mathcal{R}_0 = \mathcal{R}^r.(\mathcal{R}^{m+1} + \{\overrightarrow{0}\} \times W) = \mathcal{R}^{m+1+r} + \{\overrightarrow{0}\} \times W$. En particulier, on a prouvé que $\mathcal{C} = \{\mathcal{R}^r.\mathcal{R}_0;\ r \geqslant 0\}$ contient au plus $(4.m)^{2.m}$ relations affines de taille polynomiale en la taille de $\mathcal{R}$. On a de plus l'égalité suivante :

$$\text{saff}(\mathcal{R}^*) = \left(\bigcup_{i=0}^{m} \mathcal{R}^i\right) \cup \left(\bigcup_{\mathcal{R}' \in \mathcal{C}} \mathcal{R}'\right)$$

Montrons que $\mathcal{R}_0$ et $\mathcal{R}$ commutent en appliquant plusieurs fois l'égalité (8.6) et le lemme 8.39. On a $\mathcal{R}_0.\mathcal{R} = (\mathcal{R}^{m+1} + W \times \{\overrightarrow{0}\}).\mathcal{R} = \mathcal{R}^{m+1+1} + W \times \{\overrightarrow{0}\} = \mathcal{R}^{m+1+1} + \{\overrightarrow{0}\} \times W = \mathcal{R}.(\mathcal{R}^{m+1} + \{\overrightarrow{0}\} \times W) = \mathcal{R}.\mathcal{R}_0$.

Montrons que $\mathcal{R}_0.\mathcal{R}_0 = \mathcal{R}^{m+1}.\mathcal{R}_0$ en appliquant plusieurs fois l'égalité (8.6) et le lemme 8.39. On a $\mathcal{R}_0.\mathcal{R}_0 = (\mathcal{R}^{m+1} + W \times \{\overrightarrow{0}\}).(\mathcal{R}^{m+1} + \{\overrightarrow{0}\} \times W) = \mathcal{R}^{2.m+2} + W \times W = \mathcal{R}^{2m+2} + \{\overrightarrow{0}\} \times W = \mathcal{R}^{m+1}.(\mathcal{R}^{m+1} + \{\overrightarrow{0}\} \times W) = \mathcal{R}_{m+1}.\mathcal{R}_0$.

En particulier, on a prouvé que $\text{saff}(\mathcal{R}^*).\text{saff}(\mathcal{R}^*) \subseteq \text{saff}(\mathcal{R}^*)$. Par minimalité de la relation semi-affine étoile, et comme $\text{saff}(\mathcal{R}^*) \subseteq \text{saff}^*(\mathcal{R})$, on a prouvé l'égalité $\text{saff}(\mathcal{R}^*) = \text{saff}^*(\mathcal{R})$.

Il reste donc juste à prouver que les relations affines de $\mathcal{C}$ sont incomparables. Supposons que $\mathcal{R}^r.\mathcal{R}_0 \subseteq \mathcal{R}^{r'}.\mathcal{R}_0$. Comme $D(\mathcal{R}^r.\mathcal{R}_0) = D(\mathcal{R}^\infty) = D(\mathcal{R}^{r'}.\mathcal{R}_0)$ et que $V(\mathcal{R}^r.\mathcal{R}_0) = V(\mathcal{R}^\infty) + W = V(\mathcal{R}^{r'}.\mathcal{R}_0)$, le lemme 8.38 montre que $\mathcal{R}^r.\mathcal{R}_0 = \mathcal{R}^{r'}.\mathcal{R}_0$. On a donc bien prouvé que les éléments de $\mathcal{C}$ sont incomparables. □

De la précédente proposition, on déduit le théorème suivant.

**Théorème 8.41**
*L'enveloppe semi-affine étoile* $\text{saff}^*(\mathcal{R})$ *d'une relation affine* $\mathcal{R}$ *est calculable en temps polynômial en la taille de* $\mathcal{R}$ *et la taille de* $\text{saff}^*(\mathcal{R})$*. De plus,* $\text{saff}^*(\mathcal{R})$ *est une union finie d'au plus* $(4.m+1)^{2.m}$ *relations affines de taille polynômiale en la taille de* $\mathcal{R}$*.*

*Démonstration :*
Considérons une relation affine $\mathcal{R}_0$ calculable en temps polynômial vérifiant les hypothèses de la proposition 8.40. On considère alors la suite $(\mathcal{R}_i)_{i \geqslant 0}$ définie par

$$\mathcal{R}_i = \left(\bigcup_{j=0}^{m} \mathcal{R}^j\right) \cup \left(\bigcup_{r=0}^{i-1} \mathcal{R}^r.\mathcal{R}_0\right)$$

La proposition 8.40 montre que la relation semi-affine $\mathcal{R}_i$ est calculable en temps polynomial en $\mathcal{R}$ et en $i$. Considérons le premier indice $i_0$ tel que $\mathcal{R}_{i_0+1} = \mathcal{R}_{i_0}$. D'après la proposition 8.40, un tel indice existe et on a alors $\text{saff}^*(\mathcal{R}) = \mathcal{R}_{i_0}$. Remarquons que si $i_0 = 0$ alors l'algorithme termine bien en temps polynômial. On peut donc supposer que $i_0 \geqslant 1$.

Montrons que les relations $\mathcal{R}^r.\mathcal{R}_0$ pour $r \in \{0, \dots, i_0 - 1\}$ sont deux à deux incomparables. S'il existe $r, r'$ tels que $\mathcal{R}^r.\mathcal{R}_0 \subseteq \mathcal{R}^{r'}.\mathcal{R}_0$, la proposition 8.40 montre que l'on a alors $\mathcal{R}^r.\mathcal{R}_0 = \mathcal{R}^{r'}.\mathcal{R}_0$. Ainsi, par minimalité de $i_0$, on a $r = r'$. On a donc bien prouvé que les relations $\mathcal{R}^r.\mathcal{R}_0$ pour $r \in \{0, \dots, i_0 - 1\}$ sont deux à deux incomparables.

Considérons $\mathcal{C} = \{\mathcal{R}^r.\mathcal{R}_0;\ r \in \{0, \dots, i_0 - 1\}\}$.

Montrons que l'ensemble des composantes affines de $\text{saff}^*(\mathcal{R})$ contient $\mathcal{C}$. Comme $\text{saff}^*(\mathcal{R}) = \mathcal{R}_{i_0}$, l'ensemble des composantes de $\text{saff}^*(\mathcal{R})$ est inclus dans $\mathcal{C}' = \{\mathcal{R}^i;\ 0 \leqslant i \leqslant m\} \cup \mathcal{C}$. Pour montrer que $\mathcal{C}$ est inclus dans l'ensemble des composantes affines de $\text{saff}^*(\mathcal{R})$, on doit donc prouver que les éléments de $\mathcal{C}$ sont des relations affines maximales pour la relation d'inclusion dans $\mathcal{C}'$. Comme les éléments de $\mathcal{C}$ sont deux à deux incomparables, il suffit de remarquer que l'on ne peut pas avoir $\mathcal{R}^r.\mathcal{R}_0 \subseteq \mathcal{R}^i$ pour $i \in \{0, \dots, m\}$. En effet, dans ce cas, $\mathcal{R}_{r-1} = \mathcal{R}_r$ et par minimalité de $i_0$, on a $i_0 \leqslant \max(0, r - 1)$ ce qui contredit $r < i_0$.

Comme $\mathcal{C}$ est inclus dans l'ensemble des composantes affines de $\text{saff}^*(\mathcal{R})$ et contient $i_0$ relations affines, on déduit la majoration $i_0 \leqslant \text{card}(\text{comp}(\text{saff}^*(\mathcal{R})))$. On a donc prouvé que la relation semi-affine étoile $\text{saff}^*(\mathcal{R}) = \mathcal{R}_{i_0}$ est calculable en temps polynômial en la taille de $\mathcal{R}$ et en la taille de $\text{saff}^*(\mathcal{R})$. □

L'algorithme qu'on déduit du théorème 8.41 à été implémenté dans l'outil FAST. Le calcul de l'enveloppe semi-affine étoile a terminé sur les 40 exemples testés. Même si en théorie la taille de $\text{saff}^*(\mathcal{R})$ peut-être exponentielle en $m$, dans la pratique, pour des relations affines issues de systèmes à compteurs, on n'a jamais rencontré cette explosion.

## 8.5 Enveloppe semi-affine étoile d'une relation semi-affine

On présente un semi-algorithme qui calcule l'enveloppe semi-affine étoile d'une relation semi-affine quand il termine. Toutes les relations semi-affines testées dans la pratique ont fait terminer l'algorithme. Cependant, prouver sa terminaison est un problème difficile de type théorème de Burnside ([MS77], [MZ75] [Jac78]).

Dans la sous-section 8.5.1, on présente ce semi-algorithme et on prouve sa correction. Puis, dans la sous-section 8.5.2, on montre sa terminaison pour une large classe de systèmes à compteurs comprenant les réseaux de Petri/transfert ([Cia94], [DFS98]) et les systèmes broadcasts ([EN98], [Del00a], [Del01], [Del00b]).

### 8.5.1 Un semi-algorithme

On montre dans cette sous-section que le semi-algorithme 3 est correct et calcule donc l'enveloppe semi-affine étoile d'une relation semi-affine lorsqu'il termine.

La proposition suivante prouve la correction du semi-algorithme.

**Algorithme 3** Semi-algorithme de calcul de l'enveloppe semi-affine étoile d'une relation semi-affine.

1: **entrée :** une relation semi-affine $\mathcal{R}_0$.
2: **sortie :** l'enveloppe semi-affine étoile de $\mathcal{R}_0$.
3:
4: $\mathcal{R} \leftarrow \bigcup_{\mathcal{R}_a \in \mathrm{comp}(\mathcal{R}_0)} \mathrm{saff}^*(\mathcal{R}_a)$
5: **tant que** $\mathcal{R}.\mathcal{R} \nsubseteq \mathcal{R}$ **faire**
6: $\quad \mathcal{R} \leftarrow \bigcup_{\mathcal{R}_a, \mathcal{R}_b \in \mathrm{comp}(\mathcal{R})} \mathrm{saff}^*(\mathcal{R}_a.\mathcal{R}_b)$
7: **renvoyer** $\mathcal{R}$

**Proposition 8.42**
*L'assertion $\mathcal{I} \cup \mathcal{R}_0 \subseteq \mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$ est un invariant du semi-algorithme 3. En particulier, lorsqu'il termine, il renvoie bien l'enveloppe semi-affine étoile $\mathrm{saff}^*(\mathcal{R}_0)$.*

*Démonstration :*
Pour montrer l'invariant $\mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$, il suffit de prouver que pour toute relation semi-affine $\mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$, les deux relations semi-affines suivantes restent incluses dans $\mathrm{saff}^*(\mathcal{R}_0)$ :

$$\begin{cases} \bigcup_{\mathcal{R}_a \in \mathrm{comp}(\mathcal{R})} \mathrm{saff}^*(\mathcal{R}_a) \\ \bigcup_{\mathcal{R}_a, \mathcal{R}_b \in \mathrm{comp}(\mathcal{R})} \mathrm{saff}^*(\mathcal{R}_a.\mathcal{R}_b) \end{cases}$$

Montrons la première inclusion. Pour toute composante affine $\mathcal{R}_a \in \mathrm{comp}(\mathcal{R})$, on a $\mathcal{R}_a \subseteq \mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$. Par minimalité de la couverture semi-affine étoile, on a $\mathrm{saff}^*(\mathcal{R}_a) \subseteq \mathrm{saff}^*(\mathcal{R}_0^*)$. L'inclusion $\bigcup_{\mathcal{R}_a \in \mathrm{comp}(\mathcal{R}_0)} \mathrm{saff}^*(\mathcal{R}_a) \subseteq \mathrm{saff}^*(\mathcal{R}_0)$ est donc prouvée. Montrons la deuxième inclusion. Considérons deux composantes affine $\mathcal{R}_a, \mathcal{R}_b \in \mathrm{comp}(\mathcal{R})$. Comme $\mathcal{R}_a, \mathcal{R}_b \subseteq \mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$, on déduit $\mathcal{R}_a.\mathcal{R}_b \subseteq \mathrm{saff}^*(\mathcal{R}_0).\mathrm{saff}^*(\mathcal{R}_0) \subseteq \mathrm{saff}^*(\mathcal{R}_0)$. Par minimalité de l'enveloppe semi-affine, on a alors prouvé la deuxième inclusion $\mathrm{saff}^*(\mathcal{R}_a.\mathcal{R}_b) \subseteq \mathrm{saff}^*(\mathcal{R}_0)$. Ainsi, l'invariant $\mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R})$ a été prouvé.

Pour montrer l'invariant $\mathcal{I} \cup \mathcal{R}_0 \subseteq \mathcal{R}$, il suffit de remarquer que la suite des relations semi-affines $\mathcal{R}$, construite par l'algorithme, est croissante.

Comme à la ligne 7, on a $\mathcal{R}.\mathcal{R} \subseteq \mathcal{R}$, la relation $\mathcal{R}$ est transitive. Comme de plus, $\mathcal{R}_0 \subseteq \mathcal{R}$, par minimalité de l'enveloppe semi-affine étoile, on a $\mathrm{saff}^*(\mathcal{R}_0) \subseteq \mathcal{R}$. L'invariant $\mathcal{R} \subseteq \mathrm{saff}^*(\mathcal{R}_0)$ prouve donc qu'à la ligne 7, on a $\mathcal{R} = \mathrm{saff}^*(\mathcal{R}_0)$. □

Prouver que le semi-algorithme 3 termine est un problème ouvert que l'on peut classer parmi les problèmes de type théorème de Burnside. En effet, le lemme 8.43 montre que l'on peut décider la finitude d'un monoïde engendré par un ensemble fini de matrices de $\mathcal{M}_m(\mathbb{Q})$ en fonction de la structure de l'enveloppe semi-affine étoile d'une relation semi-affine (rappelons que la finitude du monoïde engendré par un ensemble fini de matrices carrées de $\mathcal{M}_m(\mathbb{Q})$ est décidable ([MS77], [MZ75], [Jac78]).

**Lemme 8.43**
*Soit $F$ un ensemble fini de matrices carrées de $\mathcal{M}_m(\mathbb{Q})$. Considérons la relation semi-affine $\mathcal{R}_0 = \bigcup_{M \in F}\{(x, M.x);\ x \in \mathbb{Q}^m\}$. Les composantes affines de $\mathrm{saff}^*(\mathcal{R}_0)$ correspondent à des fonctions affines si et seulement si le monoïde engendré par $F$ est fini.*

*Démonstration :*

On note $\mathcal{M}_F$ le monoïde engendré par $F$. Pour toute matrice $M \in \mathcal{M}_m(\mathbb{Q})$, on note $\mathcal{R}_M$ la relation affine sur $\mathbb{Q}^m$ définie par $\mathcal{R}_M = \{(x, M.x);\ x \in \mathbb{Q}^m\}$.

Supposons que les composantes affines de $\mathrm{saff}^*(\mathcal{R}_0)$ soient des fonctions affines. Ainsi, pour chaque composante affine $\mathcal{R}$ de $\mathrm{saff}^*(\mathcal{R}_0)$, il existe une matrice $M_\mathcal{R}$ et un vecteur $v_\mathcal{R}$ tels que $\mathcal{R} = \{(x, M_\mathcal{R}.x + v_\mathcal{R});\ x \in D(\mathcal{R})\}$. On va montrer que $\mathcal{M}_F \subseteq \{M_\mathcal{R};\ \mathcal{R} \in \mathrm{comp}(\mathrm{saff}^*(\mathcal{R}_0))\}$. Considérons une matrice $M \in \mathcal{M}_F$. Il existe une suite finie $(M_i)_{1 \leqslant i \leqslant n}$ de $F$ telle que $M = M_1 \dots M_n$. Comme $\mathcal{R}_{M_i} \subseteq \mathcal{R}_0 \subseteq \mathrm{saff}^*(\mathcal{R}_0)$, par transitivité de $\mathrm{saff}^*(\mathcal{R}_0)$, on a aussi $\mathcal{R}_M = \mathcal{R}_{M_n} \dots \mathcal{R}_{M_1} \in \mathrm{saff}^*(\mathcal{R}_0)$. La proposition 3.16, montre l'existence d'une composante affine $\mathcal{R}$ de $\mathrm{saff}^*(\mathcal{R}_0)$ telle que $\mathcal{R}_M \subseteq \mathcal{R}$. On a alors $M = M_\mathcal{R}$. Comme $\mathcal{M}_F \subseteq \{M_\mathcal{R};\ \mathcal{R} \in \mathrm{comp}(\mathrm{saff}^*(\mathcal{R}_0))\}$, on a prouvé que le monoïde $\mathcal{M}_F$ est fini.

Réciproquement, supposons que le monoïde $\mathcal{M}_F$ soit fini. Comme pour tout $M \in \mathcal{M}_F$, on a $\mathcal{R}_M \subseteq \mathrm{saff}^*(\mathcal{R}_0)$, alors $\bigcup_{M \in \mathcal{M}_F} \mathcal{R}_M \subseteq \mathrm{saff}^*(\mathcal{R}_0)$. Prouvons l'inclusion réciproque. Comme $\bigcup_{M \in \mathcal{M}_F} \mathcal{R}_M$ est une relation réflexive et transitive contenant $\mathcal{R}_0$, par minimalité de l'enveloppe semi-affine étoile, $\mathrm{saff}^*(\mathcal{R}_0) = \bigcup_{M \in \mathcal{M}_F} \mathcal{R}_M$. On a donc prouvé l'égalité $\mathrm{saff}^*(\mathcal{R}_0) = \bigcup_{M \in \mathcal{M}_F} \mathcal{R}_M$. En particulier, cela montre que les relations affines de $\mathrm{saff}^*(\mathcal{R}_0)$ sont des fonctions. $\square$

**Problème ouvert 8.44**
*Prouver la terminaison du semi-algorithme 3.*

### 8.5.2 Cas des systèmes à compteurs à monoïde fini

Dans cette sous-section, on montre que l'algorithme 3 termine pour $\mathcal{R}_0 = \mathrm{saff}(\mathcal{R}_S)$ où $\mathcal{R}_S$ est la relation d'accessibilité en une étape d'un système à compteurs $S$ à monoïde fini tel que $\mathrm{saff}(D_a) = \mathbb{Q}^m$. On prouve ainsi que l'enveloppe semi-affine étoile de la relation d'accessibilité d'un réseau de Petri reset/transfert ([Cia94], [DFS98]) ou d'un système broadcast ([EN98], [Del00a], [Del01], [Del00b]) est calculable.

*On considère un système à compteurs $S$ à monoïde fini tel que l'enveloppe semi-affine de chaque $D_a$ est égale à $\mathbb{Q}^m$.*

**Remarque 8.45**
*Comme le montre la proposition 8.10, cette condition est vérifiée par les clos par le haut. Cependant, elle n'est pas vérifiée pour les "tests-à-zéro".*

La couverture semi-affine $\mathrm{saff}(\mathcal{R}_S)$ de la relation d'accessibilité en une étape $\mathcal{R}_S$ est notée $\mathcal{R}$. On note $\mathcal{R}_a = \{(x, M_a.x + v_a);\ x \in \mathbb{Q}^m\}$ pour tout $a \in \Sigma$. Pour un mot $\sigma = a_1 \dots a_n$ de $\Sigma^*$, on note $\mathcal{R}_\sigma = \mathcal{R}_{a_1} \dots \mathcal{R}_{a_n}$.

On commence par caractériser la relation semi-affine $\mathcal{R}$ dans le lemme suivant.

**Lemme 8.46**
*On a $\mathcal{R} = \bigcup_{a \in \Sigma} \mathcal{R}_a$.*

*Démonstration :*

Considérons la fonction affine $g_a : \mathbb{Q}^m \to \mathbb{Q}^m \times \mathbb{Q}^m$ définie par $g_a(x) = (x.M_a.x + v_a)$.

Comme $\mathcal{R}_S = \bigcup_{a\in\Sigma} g_a(D_a)$, on déduit du lemme 3.13 que $\text{saff}(g_a(D_a)) = g_a(\text{saff}(D_a))$. Comme $\text{saff}(D_a) = \mathbb{Q}^m$, on a prouvé le lemme. □

On peut alors prouver qu'il suffit de calculer la couverture semi-affine de $\mathcal{R}^*$ pour obtenir l'enveloppe semi-affine étoile de $\mathcal{R}$.

**Proposition 8.47**
*On a* $\text{saff}^*(\mathcal{R}) = \text{saff}(\mathcal{R}^*)$.

*Démonstration :*
Pour tout $M \in \mathcal{M}_S$, on définit $\mathcal{L}_M \subseteq \Sigma^*$ et $V_M \subseteq \mathbb{Q}^m$ par :

$$\mathcal{L}_M = \{a_1 \dots a_n;\ n \geqslant 0;\ M_{a_1} \dots M_{a_n} = M\}$$
$$V_M = \{\sum_{i=1}^{n} M_{a_1} \dots M_{a_{i-1}}.v_{a_i};\ a_1 \dots a_n \in \mathcal{L}_M\}$$

Remarquons que $\mathcal{R}^* = \bigcup_{M\in\mathcal{M}_S} \{(x, M.x);\ x \in \mathbb{Q}^m\} + \{\overrightarrow{0}\} \times V_M$. Ainsi, on a $\text{saff}(\mathcal{R}^*) = \bigcup_{M\in\mathcal{M}_S} \{(x, M.x);\ x \in \mathbb{Q}^m\} + \{\overrightarrow{0}\} \times \text{saff}(V_M)$. Pour montrer que $\text{saff}(\mathcal{R}^*) = \text{saff}^*(\mathcal{R})$, il suffit de prouver que $\text{saff}(\mathcal{R}^*)$ est réflexive et transitive. Comme $\mathcal{I} \subseteq \text{saff}(\mathcal{R}^*)$, il reste donc a montrer la transitivité. On a :

$$\begin{aligned}
&\text{saff}(\mathcal{R}^*).\text{saff}(\mathcal{R}^*)\\
&= \bigcup_{M,M'\in\mathcal{M}_S} \begin{pmatrix} \{(x, M.x);\ x \in \mathbb{Q}^m\} \\ +\{\overrightarrow{0}\} \times \text{saff}(V_M) \end{pmatrix} . \begin{pmatrix} \{(x, M'.x);\ x \in \mathbb{Q}^m\} \\ +\{\overrightarrow{0}\} \times \text{saff}(V_{M'}) \end{pmatrix}\\
&= \bigcup_{M_0\in\mathcal{M}_S} \bigcup_{\substack{M, M' \in \mathcal{M}_S \\ M'.M = M_0}} \begin{pmatrix} \{(x, M_0.x);\ x \in \mathbb{Q}^m\} \\ +\{\overrightarrow{0}\} \times (M'.\text{saff}(V_M) + \text{saff}(V_{M'})) \end{pmatrix}\\
&= \bigcup_{M_0\in\mathcal{M}_S} \begin{pmatrix} \{(x, M_0.x);\ x \in \mathbb{Q}^m\} \\ +\{\overrightarrow{0}\} \times \left( \bigcup_{\substack{M, M' \in \mathcal{M}_S \\ M'.M = M_0}} \big(M'.\text{saff}(V_M) + \text{saff}(V_{M'})\big) \right) \end{pmatrix}
\end{aligned}$$

D'après les propositions 3.13 et 3.12, on a

$$\bigcup_{\substack{M, M' \in \mathcal{M}_S \\ M'.M = M_0}} \big(M'.\text{saff}(V_M) + \text{saff}(V_{M'})\big) = \text{saff}( \bigcup_{\substack{M, M' \in \mathcal{M}_S \\ M'.M = M_0}} \text{saff}(M'.V_M + V_{M'})$$

Pour montrer l'inclusion $\text{saff}(\mathcal{R}^*).\text{saff}(\mathcal{R}^*) \subseteq \text{saff}(\mathcal{R}^*)$, il suffit alors de prouver que $M'.V_M + V_{M'} \subseteq V_{M_0}$. Pour cela, on considère $v \in V_M$ et $v' \in V_{M'}$. Par définition de $V_M$ et $V_{M'}$, il existe un mot $a_1 \dots a_n$ dans $\mathcal{L}_M$ et un mot $a'_1 \dots a'_{n'}$ dans $\mathcal{L}_{M'}$ tels que $v =$

$\sum_{i=1}^{n} M_{a_1} \dots M_{a_{i-1}}.v_{a_i}$ et $v' = \sum_{i=1}^{n'} M_{a'_1} \dots M_{a'_{i-1}}.v_{a'_i}$. Comme $M_{a'_1} \dots M_{a'_{n'}}.M_{a_1} \dots M_{a_n} = M'.M = M_0$, on a prouvé que $a'_1 \dots a'_{n'}.a_1 \dots a_n \in \mathcal{L}_{M_0}$. On a alors $V_{M_0} \ni (\sum_{i=1}^{n'} M_{a'_i}.v_{a'_i})+ M'.\sum_{i=0}^{m} M_{a_i}.v_{a_i} = v' + M'.v$. On a donc bien prouvé l'inclusion $M'.V_M + V_{M'} \subseteq V_{M_0}$. Ainsi, on a prouvé la transitivité de saff$(\mathcal{R}^*)$. La proposition est donc prouvée. □

Pour montrer que l'algorithme 3 termine, on va utiliser un automate dont les états seront étiquetés par des matrices du monoïde $\mathcal{M}_S$.

**Lemme 8.48**
*Soit $\mathcal{A}$ un automate fini. Pour tout mot $\sigma \in \mathcal{L}(\mathcal{A})$, il existe une suite finie $(\sigma_i)_{1\leqslant i\leqslant n}$ de $\Sigma^*$ et une suite finie $(\alpha_i)_{1\leqslant i\leqslant n}$ de $\mathbb{N}$ telles que :*
- $\sigma_1^{\alpha_1} \dots \sigma_n^{\alpha_n} \in \mathcal{L}(\mathcal{A})$,
- *$\sigma$ et $\sigma_1^{\alpha_1} \dots \sigma_n^{\alpha_n}$ ont la même image de Parikh,*
- $\max(|\sigma_i|) \leqslant \operatorname{card}(Q)$, *et*
- $n \leqslant 1 + 2.\operatorname{card}(\Sigma)^{1+\operatorname{card}(Q)}$

*Démonstration :*
Considérons un mot $\sigma \in \mathcal{L}(\mathcal{A})$. Il existe alors un chemin acceptant $\sigma$ noté $P$. On note $E$ l'ensemble des cycles élémentaires de l'automate $\mathcal{A}$. A tout triplet $(p, c, s)$ où $p = (P_i)_{0\leqslant i\leqslant k}$ est une suite finie de chemins, $c = (C_i)_{1\leqslant i\leqslant k}$ est une suite finie de cycles élémentaires, et à $s = (\alpha)_{1\leqslant i\leqslant k}$ est une suite finie de $\mathbb{N}^*$ telles que $P_0.C_1^{\alpha_1}.P_1 \dots C^{\alpha_k}.P_k$ est un chemin de $\mathcal{A}$ dont l'image de Parikh de l'étiquette est égale à l'image de Parikh de $\sigma$, on associe le couple $(\sum_{i=0}^{k} |P_i|, k)$ de $\mathbb{N}\times\mathbb{N}$. Considérons alors la relation d'ordre lexicographique sur $\mathbb{N}\times\mathbb{N}$ notée $\leqslant_{lex}$ et définie par $(x, k) \leqslant_{lex} (x', k')$ si et seulement si $(x < x') \vee ((x = x') \wedge (k \leqslant k'))$. On considère alors le triplet $(p, c, s)$ dont le couple associé $(x, k)$ est minimal pour la relation d'ordre $\leqslant_{lex}$ (un tel triplet existe car $\mathbb{N} \times \mathbb{N}$ est totalement ordonné par la relation d'ordre lexicographique).

Montrons par l'absurde que $k \leqslant \operatorname{card}(\Sigma)^{\operatorname{card}(Q)+1}$. Comme l'ensemble $E$ des cycles élémentaires de $\mathcal{A}$ a un cardinal borné par $\operatorname{card}(\Sigma)^{\operatorname{card}(Q)+1}$, il existe dans ce cas $i < i'$ tel que $C_i = C_{i'}$. Le chemin suivant contredit la minimalité de $(x, k)$ en générant un couple $(x, k - 1)$ :

$$P_0.C_1^{\alpha_1}.P_1 \dots P_{i-1}.C_i^{\alpha_i+\alpha_{i'}}.P_i \dots P_{i'-1}.P_{i'} \dots C^{\alpha_k}.P_k$$

Montrons aussi par l'absurde que les chemins $P_i$ ont une longueur bornée par $\operatorname{card}(Q)$. En effet, dans le cas contraire, il existerait un entier $i_0$ tel que la longueur du chemin $P_{i_0}$ est strictement plus grande que le nombre d'états de l'automate $\mathcal{A}$. On peut alors décomposer le chemin $P_{i_0}$ en $P'.C.P''$ où $C$ est un cycle élémentaire. Le chemin suivant contredit la minimalité de $(x, k)$ en générant un couple $(x - |C|, k + 1)$ :

$$P_0.C_1^{\alpha_1}.P_1 \dots C_i^{\alpha_i}.P'.C.P''.C_{i+1} \dots C^{\alpha_k}.P_k$$

Comme $\max(|P_i|) \leqslant \operatorname{card}(Q)$ et $\max(|C_i|) \leqslant \operatorname{card}(Q)$, et $k \leqslant \operatorname{card}(\Sigma)^{\operatorname{card}(Q)+1}$, on a prouvé le lemme. □

**Proposition 8.49**
*Pour tout mot $\sigma \in \Sigma^*$, il existe une suite finie $(\sigma_i)_{1\leqslant i\leqslant n}$ de $\Sigma^*$ telle que :*

$$\begin{cases} \mathcal{R}_\sigma \subseteq \mathcal{R}^*_{\sigma_1}\dots\mathcal{R}^*_{\sigma_n} \\ \max(|\sigma_i|) \leqslant \mathrm{card}(\mathcal{M}_S) \\ n \leqslant 1+2.(\mathrm{card}(\mathcal{M}_S).\mathrm{card}(\Sigma))^{1+\mathrm{card}(\mathcal{M}_S)} \end{cases}$$

*Démonstration :*

On considère l'automate déterministe $\mathcal{A}$ dont l'ensemble des états est le monoïde fini $\mathcal{M}_S$ et défini par $\mathcal{A} = (\mathcal{M}_S, \mathcal{M}_S \times \Sigma, \delta, \{I\}, \mathcal{M}_S)$ où la fonction de transition $\delta$ est définie sur l'ensemble des couples $(M, (M', a))$ tels que $M = M'$ par $\delta(M, (M, a)) = M.M_a$. Pour tout chemin $P = I \xrightarrow{(M_1,a_1)\dots(M_n,a_n)} M$ de l'automate $\mathcal{A}$, on note $\sigma_P$ le mot $\sigma_P = a_1\dots a_n$ de $\Sigma^*$ et on note $\mathcal{R}_P$ la relation affine définie par :

$$\mathcal{R}_P = \{(x, M.x);\ x \in \mathbb{Q}^m\} + \{(\overrightarrow{0}, \sum_{i=1}^{n} M_i.v_{a_i}\}$$

On montre par récurrence sur $n \geqslant 0$ que pour tout chemin $P = I \to M$ de longueur $|P| = n$ de l'automate $\mathcal{A}$, on a $\mathcal{R}_{\sigma_P} = \mathcal{R}_P$. Pour $n = 0$, le seul chemin possible est $I \xrightarrow{\varepsilon} I$ et on a alors $\mathcal{R}_\varepsilon = \mathcal{I}$. Ainsi, l'hypothèse de récurrence est vraie pour $n = 0$. Supposons donc cette hypothèse vraie pour un entier $n \geqslant 0$ et considérons un chemin $I \xrightarrow{(M_1,a_1)\dots(M_{n+1},a_{n+1})} M'$. Considérons une matrice $M \in \mathcal{M}_S$ telle que $I \xrightarrow{(M_1,a_1)\dots(M_n,a_n)} M$ et $M \xrightarrow{(M_{n+1},a_{n+1})} M'$ soient deux chemins de l'automate $\mathcal{A}$. Par définition de la fonction de transition $\delta$, on a $M' = M.M_{a_n}$ et $M = M_{n+1}$. De plus, par hypothèse de récurrence, on a $\mathcal{R}_{a_1\dots a_n} = \{(x, M.x);\ x \in \mathbb{Q}^m\} + \{(\overrightarrow{0}, \sum_{i=1}^{n} M_i.v_{a_i}\}$. De $\mathcal{R}_{a_1\dots a_{n+1}} = \mathcal{R}_{a_1\dots a_n}.\mathcal{R}_{a_{n+1}}$, on déduit $\mathcal{R}_{a_1\dots a_{n+1}} = \{(x, M.M_{a_n}.x;\ x \in \mathbb{Q}^m\} + \{\overrightarrow{0}, \sum_{i=1}^{n} M_i.v_{a_i} + M.v_{a_{n+1}}\}$. Cela démontre l'hypothèse de récurrence au rang $n+1$. On a donc prouvé que pour tout chemin $P = I \to M$, on a $\mathcal{R}_P = \mathcal{R}_{\sigma_P}$.

Considérons alors $\sigma \in \Sigma^*$. Par définition de l'automate $\mathcal{A}$, il existe un chemin $P = I \to M$ tel que $\sigma_P = \sigma$. Considérons l'automate $\mathcal{A}_M$ déduit de $\mathcal{A}$ en remplaçant l'ensemble des états finaux de $\mathcal{A}$ par le singleton $\{M\}$. D'après le lemme 8.48, il existe une suite finie $(\sigma_i)_{1\leqslant i\leqslant n}$ de mots de $\Sigma^*$ et une suite finie $(\alpha_i)_{1\leqslant i\leqslant n}$ de $\mathbb{N}$ telles que $\sigma_1^{\alpha_1}\dots\sigma_n^{\alpha_n}$ soit l'étiquette d'un chemin $P'$ de $\mathcal{A}_M$ de même image de Parikh que l'étiquette de $P$ et telles :

$$\begin{cases} \max(|\sigma_i|) \leqslant \mathrm{card}(\mathcal{M}_S) \\ n \leqslant 1+2.(\mathrm{card}(\mathcal{M}_S).\mathrm{card}(\Sigma))^{1+\mathrm{card}(\mathcal{M}_S)} \end{cases}$$

On a alors $\mathcal{R}_P = \mathcal{R}_{P'}$. On déduit de cette égalité $\mathcal{R}_\sigma = \mathcal{R}_P = \mathcal{R}_{P'} = \mathcal{R}_{\sigma_{P'}} \subseteq \mathcal{R}^*_{\sigma_1}\dots\mathcal{R}^*_{\sigma_n}$.
□

On peut alors prouver que le semi-algorithme 3 termine sur l'entrée $\mathcal{R}$.

**Proposition 8.50**
*Le semi-algorithme 3 termine sur l'entrée $\mathcal{R}$ en temps double exponentiel en la taille du monoïde $\mathcal{M}_S$.*

*Démonstration :*

On note $\mathcal{R}_i$ la relation $\mathcal{R}$ avant l'exécution de la ligne 6 en fonction du nombre $i \geqslant 1$ de fois que la boucle "tant que" a été exécutée. Pour $i \geqslant \ln(\mathrm{card}(\mathcal{M}_S))/\ln(2)$ et pour $\sigma \in \Sigma^*$ tel que $|\sigma| \leqslant \mathrm{card}(\mathcal{M}_S)$, on a $\mathrm{saff}(\mathcal{R}_\sigma^*) \subseteq \mathcal{R}_i$. Posons $n = 1+2.(\mathrm{card}(\mathcal{M}_S).\mathrm{card}(\Sigma))^{1+\mathrm{card}(\mathcal{M}_S)}$ et $i_0 = \ln(n.\mathrm{card}(\mathcal{M}_S))/\ln(2)$. Pour tout $i \geqslant i_0$, et pour toute suite $\sigma_i$, ..., $\sigma_n$ de $\Sigma^{\leqslant \mathrm{card}(\mathcal{M}_S)}$, on a alors l'inclusion suivante :

$$\mathrm{saff}(\mathcal{R}_{\sigma_1}^*)\ldots\mathrm{saff}(\mathcal{R}_{\sigma_n}^*) \subseteq \mathcal{R}_i$$

D'après la proposition 8.49, on a alors $\mathcal{R}_\sigma \subseteq \mathcal{R}_i$ pour tout $i \geqslant i_0$. Ainsi, pour tout $i > i_0$, on a $\mathrm{saff}(\mathcal{R}^*) = \mathrm{saff}(\bigcup_{\sigma\in\Sigma^*}\mathcal{R}_\sigma) \subseteq \mathcal{R}_i$. Or d'après la proposition 8.47, on a $\mathrm{saff}^*(\mathcal{R}) = \mathrm{saff}(\mathcal{R}^*)$. Ainsi, pour $i > i_0$ on a $\mathrm{saff}^*(\mathcal{R}) \subseteq \mathcal{R}_i$. Or d'après la proposition 8.42, on a $\mathcal{R}_i \subseteq \mathrm{saff}^*(\mathcal{R})$. On a donc prouvé que pour $i > i_0$, on a $\mathcal{R}_i = \mathrm{saff}^*(\mathcal{R})$. Comme $\mathrm{saff}^*(\mathcal{R}).\mathrm{saff}^*(\mathcal{R}) \subseteq \mathrm{saff}^*(\mathcal{R})$, la condition de la boucle "tant que" n'est alors plus valide pour $i > i_0$. Le semi-algorithme 3 termine donc après $i_0$ itération de la boucle "tant que". Bornons alors la taille des relations semi-affines $\mathcal{R}_i$ que l'on produit pendant l'exécution de l'algorithme. Posons $c = 1 + (4.m+1)^{2.m}$. En utilisant le théorème 8.41, on obtient la majoration suivante pour $i \geqslant 1$ :

$$\mathrm{card}(\mathrm{comp}(\mathcal{R}_{i+1})) \leqslant c.\mathrm{card}(\mathrm{comp}(\mathcal{R}_i))^2$$

Le théorème 8.40 et la proposition 3.23 montrent de plus que les composantes affines de $\mathcal{R}_{i+1}$ ont une taille polynômiale en la taille des composantes affines de $\mathcal{R}_i$. Il existe donc une constante $c'$ et un entier $m \geqslant 0$ tel que pour tout $i \geqslant 0$, on a :

$$\mathrm{taille}(\mathcal{R}_{i+1}) \leqslant c.\mathrm{taille}(\mathcal{R}_i)^m$$

On a donc $\mathrm{taille}(\mathcal{R}_i) = O(\mathrm{card}(\mathcal{R}_0)^{m^{i_0}})$. Comme $m^{i_0} \leqslant n.\mathrm{card}(\mathcal{M}_S).\ln(m)/\ln(2)$, on a prouvé que la taille des relations semi-affines calculées par l'algorithme ont une taille double exponentielle en la taille du monoïde. □

**Théorème 8.51**

*L'enveloppe semi-affine étoile de la relation d'accessibilité des système à compteurs suivant est calculable en temps élémentaire (au plus triple exponentiel) :*

- *Les réseaux de Petri reset/transfert ([Cia94], [DFS98])*
- *Les systèmes broadcasts ([EN98], [Del00a], [Del01], [Del00b]).*

*Démonstration :*

En effet, pour ces systèmes à compteurs, le monoïde $\mathcal{M}_S$ est un sous-monoïde des matrices reset/transfert. Ainsi, $\mathrm{card}(\mathcal{M}_S) \leqslant (m+1)^m$. Comme les domaines de définitions $D_a$ sont des parties closes par le haut, la proposition 8.10 prouve que l'on a bien $\mathrm{saff}(D_a) = \mathbb{Q}^m$. La proposition 8.50 prouve que le semi-algorithme 3 termine sur l'entrée $\mathcal{R}_0 = \mathrm{saff}(\mathcal{R}_S)$. De la proposition 8.42, on déduit que $\mathrm{saff}^*(\mathcal{R}_0)$ est calculable en temps triple exponentiel. Enfin, comme $\mathrm{saff}^*(\mathcal{R}_0) = \mathrm{saff}^*(\mathcal{R}_S) = \mathrm{saff}^*(\mathcal{R}_S^*)$, on a prouvé le théorème. □

**Remarque 8.52**
*Le semi-algorithme 3 a été implémenté. La complexité triple exponentielle n'a jamais été rencontrée dans les études de cas que l'on a fait. On a même obtenu des résultats en quelques minutes de calcul. On peut donc raisonnablement penser que cette complexité théorique n'est pas optimale.*

CHAPITRE 9

# Accessibilité par accélération

On étudie dans ce chapitre le problème du choix des accélérations pour calculer l'ensemble des états accessibles d'un système.

Les classes de systèmes pour lesquelles l'accessibilité est un problème décidable, sont souvent trop restreintes pour pouvoir être utilisées directement sur un système réel. En effet, même pour des systèmes simples comme les réseaux de Petri reset/transfert, l'accessibilité est indécidable [DFS98]. L'accélération est une technique pour *aider à décider* l'accessibilité pour ces classes de systèmes indécidables, en cherchant à calculer l'ensemble des états accessibles en *itérant à la limite* des composées d'actions [BW94].

L'accélération a fait l'objet de nombreuses études et implémentations [Tre, ABS01, APSY02, ASY01, Fas, BFLP03, Las] ; l'accélération des "lossy chanel systems" utilise les SRE [ABJ98] ; pour les "FIFO chanel systems ", on utilise des QDD [BGWW97, WB98] ou des CQDD [Bou01] ; pour les systèmes répartis en anneau, des automates finis permettent d'accélérer des transitions [BF] ; pour les systèmes à compteurs affines, l'accélération peut se faire en utilisant des UBA (chapitre 4) [BW94, Boi, FL02].

Cependant, pour pouvoir *effectivement utiliser les accélérations*, il est important de savoir les *choisir* pour faire converger le calcul itératif de l'ensemble des états accessibles par accélération.

Dans ce chapitre, on étudie ce problème pour les systèmes à compteurs affines. On montre que l'on peut raisonnablement appliquer un algorithme de type "*brute force*" sur l'ensemble des composées d'au plus $k$ actions par une méthode de *réduction exponentielle*.

On trouve dans ce chapitre :
- une *extension* du résultat d'accélération de Boigelot des fonctions affines à des domaines de définition non-convexes, permettant la mise en place de technique de réduction.
- une classe de systèmes à compteurs (contenant les réseaux de Petri reset/transfert) pour laquelle le nombre de composées d'au plus $k$ actions est *polynomial* en $k$.

- un exemple de système à compteurs effectif à monoïde fini dont le nombre de composées d'au plus $k$ actions est *exponentiel* en $k$.
- une technique de réduction permettant de réduire les composées d'au plus $k$ actions d'un systèmes à compteurs effectif à monoïde fini, à un ensemble calculable en temps polynomial en fonction de $k$.
- une classe de systèmes à compteurs pour laquelle l'accélération suffit pour calculer l'ensemble des états accessibles.

Dans la section 9.1, on définit l'accélération d'une composée d'action et on montre sur un exemple comment calculer l'ensemble des états accessibles d'un système avec cette technique. Comme nous utiliserons des parties de $\mathbb{Z}^m$ définissables par des UBA, pour rappeler des résultats d'accélération valables pour des fonctions affine définie sur tout $\mathbb{Z}^m$, on étendra à $\mathbb{Z}^m$, dans la section 9.2, quelques définitions données dans le cadre de $\mathbb{N}^m$ dans les chapitres précédents. L'accélération d'une fonction affine est étudiée dans la section 9.3. Enfin, dans la section 9.4, on étudie le problème du choix des accélérations.

## 9.1 Définition de l'accélération

L'ensemble des états accessibles d'un système à compteurs n'est pas en général calculable comme un point fixe de la suite croissante $\mathrm{Post}_S^{\leqslant k}(X)$ car elle peut ne pas être stationnaire (chapitre 7). Pour vérifier un tel système infini, on doit donc trouver une méthode pour calculer, en un nombre fini d'étapes, un ensemble infini d'états accessibles. Pour cela, on va accélérer des compositions d'actions (aussi appelées "meta-transitions" [BW94] ou encore "exact widening" dans le cadre de l'interprétation abstraite).

**Définition 9.1**
*L'accélération d'une composée d'actions $\sigma \in \Sigma^*$ d'un système $S$ est la relation notée $\xrightarrow{\sigma^*}$ définie par*

$$\xrightarrow{\sigma^*} = (\xrightarrow{\sigma})^*$$

Dans cette section, on va montrer sur l'exemple 9.2, comment l'accélération peut-être utilisée pour calculer l'ensemble des états accessibles.

**Exemple 9.2**
*On considère un réseaux de Petri $S_{pc} = (\mathbb{N}^5, \Sigma, (\rightarrow_a)_{a\in\Sigma})$ où $\Sigma = \{e_W, e_{R_1}, e_{R_2}\}$ et :*

$$\begin{cases} (c,i,b,o_1,o_2) \xrightarrow{e_W} (c,i-1,b+1,o_1,o_2) & \text{si } i \geqslant 1 \\ (c,i,b,o_1,o_2) \xrightarrow{e_{R_1}} (c,i,b-1,o_1+1,o_2) & \text{si } b \geqslant 1 \\ (c,i,b,o_1,o_2) \xrightarrow{e_{R_2}} (c,i,b-1,o_1,o_2+1) & \text{si } b \geqslant 1 \end{cases}$$

*On considère l'ensemble des états initiaux $X_0 = \{(c,i,b,o_1,o_2);\ (c = i) \wedge (b = o_1 = o_2 = 0)\} \subseteq \mathbb{N}^5$.*

*Cet exemple modélise un "producteur consommateur" contenant un buffer $b$ et deux sorties $o_1$ et $o_2$. La transition $e_W$ ("Write") permet d'écrire une lettre dans le buffer $b$ alors* *que les transitions $e_{R_1}$ et $e_{R_2}$ ("Read") retire une lettre de $b$ pour la sortir respectivement dans $o_1$ ou dans $o_2$.*

Comme le montre le lemme 9.3, il est inutile de cherche à calculer $\mathrm{Post}^*_{S_{pc}}(X_0)$ comme un point fixe de la suite $\mathrm{Post}^{\leqslant k}_{S_{pc}}(X_0)$ car elle n'est pas stationnaire.

**Lemme 9.3**
*Pour tout entier $k \geqslant 0$, on a $\mathrm{Post}^{\leqslant k}_{S_{pc}}(X_0) \neq \mathrm{Post}^*_{S_{pc}}(X_0)$.*

*Démonstration :*
Soit $k \geqslant 0$. De $(k+1, k+1, 0, 0, 0) \xrightarrow{e_W^{k+1}.e_{R_1}^{k+1}} (k+1, 0, 0, k+1, 0)$ et $(k+1, k+1, 0, 0, 0) \in X_0$, on déduit $(k+1, 0, 0, k+1, 0) \in \mathrm{Post}^*_{S_{pc}}(X_0)$. Considérons alors un entier $k'$ tel que $(k+1, 0, 0, k+1, 0) \in \mathrm{Post}^{\leqslant k'}_{S_{pc}}(X_0)$. Il existe $\sigma \in \Sigma^{\leqslant k'}$ et $(c, c, 0, 0, 0) \in X_0$ tels que $(c, c, 0, 0, 0) \xrightarrow{\sigma} (k+1, k+1, 0, 0, 0)$. Par définition de $S_{pc}$, la première composante étant constante, on a $c = k+1$. De plus, comme la variable $i$ ne décroît de 1 qu'a chaque fois que l'on utilise la transition $e_W$, le nombre de $e_W$ dans $\sigma$ est égale à $k+1$. En particulier $k' \geqslant |\sigma| \geqslant k+1$ et on a prouvé que $(k+1, k+1, 0, 0, 0) \notin \mathrm{Post}^{\leqslant k}_{S}(X_0)$. $\square$

Cependant l'accélération des actions $e_W$, $e_{R_1}$ et $e_{R_2}$ permet d'atteindre tous les états accessibles de $\mathrm{Post}^*_S(X_0)$.

**Lemme 9.4**
*Pour tout $x \in \mathrm{Post}^*_{S_{pc}}(X_0)$, il existe $x_0 \in X_0$ tel que :*

$$x_0 \xrightarrow{e_W^*} \xrightarrow{e_{R_1}^*} \xrightarrow{e_{R_2}^*} x$$

*Démonstration :*
On commence par montrer que $\mathrm{Post}^*_{S_{pc}}(X_0) = X'$ où $X' = \{(c, i, b, o_1, o_2);\ c = i + b + o_1 + o_2\}$. Considérons donc $(c, i, b, o_1, o_2) \in X'$. Comme $(c, c, 0, 0, 0) \in X_0$ et $(c, c, 0, 0, 0) \xrightarrow{e_W^{b+o_1+o_2}} (c, i, b + o_1 + o_2, 0, 0) \xrightarrow{e_{R_1}^{o_1}} (c, i, b + o_2, o_1, 0) \xrightarrow{e_{R_2}^{o_2}} (c, i, b, o_1, o_2)$, on a $X' \subseteq \mathrm{Post}^*_{S_{pc}}$. Montrons l'inclusion réciproque. Il suffit de prouver que pour tout $(c, i, b, o_1, o_2) \xrightarrow{a} (c', i', b', o_1', o_2')$ tel que $a \in \Sigma$ et $(c, i, b, o_1, o_2) \in X'$, on a $(c', i', b', o_1', o_2') \in X'$. Dans les trois cas $a = e_W$, $a = e_{R_1}$ et $a = e_{R_2}$, on a bien $(c', i', b', o_1', o_2') \in X'$. Ainsi on a prouvé que $\mathrm{Post}_{S_{pc}}(X_0) = X'$ et en particulier, on a prouvé le lemme. $\square$

Pour pouvoir utiliser automatiquement cette technique d'accélération, il va falloir prouver que :
- on peut effectivement représenter l'accélération de toute composée d'actions.
- on peut trouver les "bonnes composées d'action" à accélérer pour calculer l'ensemble des états accessibles.

## 9.2 Remarque sur les parties de $\mathbb{Z}^m$

Dans ce chapitre, nous utiliserons des parties de $\mathbb{Z}^m$. Pour étendre les résultats des précédents chapitres sur les parties de $\mathbb{N}^m$ aux parties de $\mathbb{Z}^m$, on va établir le lien simple entre les parties de $\mathbb{Z}^m$ et les parties de $\mathbb{N}^{2.m}$, qui consiste à remarquer qu'un entier relatif $x \in \mathbb{Z}$ est la différence de deux entiers positifs $x = x^+ - x^-$ avec $x^+, x^- \in \mathbb{N}$.

**Définition 9.5**
*On considère la fonction affine* $f_{\mathbb{N}\to\mathbb{Z}} : \mathbb{N}^{2m} \to \mathbb{Z}^m$ *définie par* $f_{\mathbb{N}\to\mathbb{Z}}(x_1^+, x_1^-, \ldots, x_m^+, x_m^-) = (x_1^+ - x_1^-, \ldots, x_m^+ - x_m^-)$.

Même si les automates que nous obtenons par cette méthode ne sont pas aussi concis que ceux que l'on pourrait obtenir, par exemple avec le complément à 2 ([Boi98]), nous avons choisi cette méthode pour comparer simplement les résultats d'accélérations. Notre objectif n'étant plus la concision mais l'expressivité.

### 9.2.1 Presburger-définissable

On s'intéresse aux parties de $\mathbb{Z}^m$ Presburger-définissables.

**Définition 9.6**
*Une partie $X \subseteq \mathbb{Z}^m$ est Presburger-définissable en tant que partie de $\mathbb{Z}^m$, s'il existe une formule de Presburger dont l'interprétation sur $\mathbb{Z}$ définit $X$.*

La proposition 9.7 est importante car elle montre la cohérence de la définition précédente avec la définition des parties Presburger-définissables de $\mathbb{N}^m$.

**Proposition 9.7**
*Une partie $X \subseteq \mathbb{N}^m$ est Presburger-définissable en tant que partie de $\mathbb{N}^m$ si et seulement si $X$ est Presburger-définissable en tant que partie de $\mathbb{Z}^m$.*

*Démonstration :*
Considérons une partie $X \subseteq \mathbb{N}^m$. Supposons qu'il existe une formule $\phi$ dont l'interprétation sur $\mathbb{N}$ est égale à $X$. En remplaçant dans $\phi$ chaque quantificateur $\exists x\ \phi_0$ par $\exists x\ (x \geqslant 0 \wedge \phi_0)$ et chaque quantificateur $\forall x\ \phi_0$ par $\forall x\ (x < 0 \vee \phi_0)$, on obtient une formule $\phi'$ telle que $x \geqslant 0 \wedge \phi'$ définie sur $\mathbb{Z}$ la partie $X$. Réciproquement, supposons qu'il existe une formule $\phi$ dont l'interprétation sur $\mathbb{Z}$ est égale à $X$. En remplaçant chaque quantificateur $\exists x$ par $\exists x^+ \exists x^-$, chaque quantificateur $\forall x$ par $\forall x^+ \forall x^-$, et chaque variable $x$ apparaissant dans un terme $t$ par $x^+ - x^-$, on obtient une formule $\phi'$ telle que $\exists x^+ \exists x^-\ ((x = x^+ - x^-) \wedge \phi')$ définie sur $\mathbb{N}$ la partie $X$. □

Enfin, on montre que la notion de parties de $\mathbb{Z}^m$ Presburger-définissables, correspond à remonter par la fonction $f_{\mathbb{N}\to\mathbb{Z}}$ la notion de Presburger-définissable des parties de $\mathbb{N}^{2.m}$.

**Proposition 9.8**
*Une partie $X \subseteq \mathbb{Z}^m$ est Presburger-définissable si et seulement si $f_{\mathbb{N}\to\mathbb{Z}}^{-1}(X) \subseteq \mathbb{N}^{2m}$ est Presburger-définissable.*

*Démonstration :*

Considérons une partie $X \subseteq \mathbb{Z}^m$. Supposons $X$ Presburger-définissable. Il existe une formule $\phi$ dont l'interprétation sur $\mathbb{Z}$ est $X$. La formule $\exists x\ (x = x^+ - x^-) \wedge (x^+ \geqslant 0) \wedge (x^- \geqslant 0) \wedge \phi)$ définie sur $\mathbb{Z}$ la partie $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X)$ qui est donc Presburger-définissable. Réciproquement, supposons que $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X)$ est Presburger-définissable. Il existe alors une formule $\phi$ dont l'interprétation sur $\mathbb{Z}$ est $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X)$. La formule $\exists x^+ \exists x^-((x = x^+ - x^-) \wedge (x^+ \geqslant 0) \wedge (x^- \geqslant 0) \wedge \phi)$ définie sur $\mathbb{Z}$ la partie $X$. □

### 9.2.2 BA-définissable

On définit la notion de représentation par un automate binaire d'une partie de $\mathbb{Z}^m$ en remontant cette notion par la fonction $f_{\mathbb{N}\to\mathbb{Z}}$.

**Définition 9.9**
*Une partie $X \subseteq \mathbb{Z}^m$ est représentée par un automate binaire $\mathcal{A}$ si $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X)$ est représentée par $\mathcal{A}$.*

Il faut alors prouver la cohérence de la précédente définition pour les parties de $\mathbb{N}^m$.

**Proposition 9.10**
*Une partie $X \subseteq \mathbb{N}^m$ est représentable par un automate binaire $\mathcal{A}$ en tant que partie de $\mathbb{N}^m$ si et seulement si $X$ est représentable par un automate binaire $\mathcal{A}$ en tant que partie de $\mathbb{Z}^m$.*

*Démonstration :*

La preuve est la même que celle donnée pour le cas Presburger (cf proposition 9.7). □

### 9.2.3 Polyèdre

On rappelle la définition d'un polyèdre de $\mathbb{Z}^m$.

**Définition 9.11**
*Un demi-espace de $\mathbb{Z}^m$ est une partie $X \subseteq \mathbb{Z}^m$ telle qu'il existe un vecteur $\alpha \in \mathbb{Q}^m \backslash \{0\}$ et un rationnel $c \in \mathbb{Q}$ vérifiant $X = \{x \in \mathbb{Z}^m;\ \langle x, \alpha\rangle \leqslant c\}$.*

**Définition 9.12**
*Un polyèdre $X$ de $\mathbb{Z}^m$ est une intersection finie de demi-espaces de $\mathbb{Z}^m$.*

La cohérence de la précédente définition est prouvée par la proposition suivante.

**Proposition 9.13**
*Une partie $X \subseteq \mathbb{N}^m$ est un polyèdre de $\mathbb{N}^m$ si et seulement si $X$ est un polyèdre de $\mathbb{Z}^m$.*

*Démonstration :*

Supposons que $X$ soit un polyèdre de $\mathbb{N}^m$. Il existe une partie finie $F \subseteq \mathbb{Q}^m \times \mathbb{Q}$

telle que $X = \bigcap_{(\alpha,c)\in F}\{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle \leqslant c\}$. Comme $X = \bigcap_{i=1}^{m}\{x \in \mathbb{Z}^m;\ \langle -e_i, x_i\rangle \leqslant 0\}\bigcap_{(\alpha,c)\in F}\{x \in \mathbb{Z}^m;\ \langle \alpha, x\rangle \leqslant c\}$, la partie $X$ est donc un polyèdre de $\mathbb{Z}^m$. Réciproquement, supposons que $X$ soit un polyèdre de $\mathbb{Z}^m$. Il existe une partie finie $F \subseteq \mathbb{Q}^m \times \mathbb{Q}$ telle que $X = \bigcap_{(\alpha,c)\in F}\{x \in \mathbb{Z}^m;\ \langle \alpha, x\rangle \leqslant c\}$. Comme $X \subseteq \mathbb{N}^m$, on a alors $X = \bigcap_{(\alpha,c)\in F}\{x \in \mathbb{N}^m;\ \langle \alpha, x\rangle \leqslant c\}$. Ainsi, $X$ est un polyèdre de $\mathbb{N}^m$. □

Comme le montre la proposition suivante, la fonction $f_{\mathbb{N}\to\mathbb{Z}}$ permet de remonter la notion de polyèdre de $\mathbb{N}^{2m}$ en polyèdre de $\mathbb{Z}^m$.

**Proposition 9.14**
*Une partie $X \subseteq \mathbb{Z}^m$ est un polyèdre si et seulement si $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X)$ est un polyèdre.*

*Démonstration :*
Supposons que $X$ soit un polyèdre. Il existe une partie finie $F \subseteq \mathbb{Q}^m \times \mathbb{Q}$ telle que $X = \bigcap_{(\alpha,c)\in F}\{x \in \mathbb{Z}^m;\ \langle \alpha, x\rangle \leqslant c\}$. Comme $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X) = \bigcap_{(\alpha,c)\in F} f^{-1}_{\mathbb{N}\to\mathbb{Z}}(\{x \in \mathbb{Z}^m;\ \langle \alpha, x\rangle \leqslant c\})$, on peut supposer que $X = \{x \in \mathbb{Z}^m;\ \langle \alpha, x\rangle \leqslant c\}$. Dans ce cas $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X) = \{x' = (x_1^+, x_1^-, \dots, x_m^+, x_m^-) \in \mathbb{N}^{2m};\ \langle \alpha, f_{\mathbb{N}\to\mathbb{Z}}(x')\rangle \leqslant c\}$. Considérons $\alpha' = (\alpha_1, -\alpha_1, \dots, \alpha_m, -\alpha_m) \in \mathbb{Q}^{2m}$ et remarquons que $f^{-1}_{\mathbb{N}\to\mathbb{Z}}(X) = \{x' \in \mathbb{N}^{2m};\ \langle \alpha', x'\rangle \leqslant c\}$. □

## 9.3 Calcul d'une accélération

Dans cette section, on s'intéresse au problème du calcul de l'accélération d'une composée d'actions d'un système à compteurs affine. Comme une telle composée est une fonction affine, on commence par étudier dans la sous-section 9.3.1 l'accélération des fonctions affines. Enfin, dans la sous-section 9.3.2, on montre que l'accélération de toute composée d'actions d'un système à compteurs à monoïde fini est effectivement représentable par un UBA.

### 9.3.1 Accélération d'une fonction affine

Comme l'on souhaite accélérer des composées d'actions d'un système à compteurs effectif affine, il est naturel de chercher à caractériser les fonctions affines dont l'accélération est effectivement représentable par un UBA.

**Définition 9.15**
*Pour une fonction affine $f : D \to \mathbb{Z}^m$ où $D \subseteq \mathbb{Z}^m$ et une partie $X \subseteq \mathbb{Z}^m$, on pose $f^*(X) = \bigcup_{i\geqslant 0} f^i(X)$.*

B. Boigelot [Boi98] à donné une condition suffisante pour pouvoir accélérer une fonction affine définie sur un polyèdre (cette condition est de plus prouvée nécessaire dans le cas où le polyèdre est égal à tout $\mathbb{Z}^m$).

**Théorème 9.16 ([Boi98])**
*Soit $(f, M, v)$ une fonction affine décorée, définie sur un polyèdre $D \subseteq \mathbb{Z}^m$, et à valeur dans $\mathbb{Z}^m$, telle que $M$ et $v$ sont à coefficients dans $\mathbb{Z}$.*

*Supposons qu'il existe $p \in \mathbb{N}^*$ tel que les deux conditions [B1] et [B2] suivantes soient vérifiées :*

– *[B1] les valeurs propres de la matrice $M^p$ sont dans $\{0,1\}$, et*
– *[B2] la matrice $M^p$ est diagonalisable.*

*Alors, pour toute partie $X \subseteq \mathbb{Z}^m$ Presburger-définissable, $f^*(X)$ est effectivement Presburger définissable. De plus, si $D = \mathbb{Z}^m$, les conditions [B1] et [B2] deviennent nécessaires et suffisantes.*

On a alors cherché à étendre le théorème précédent à des domaines de définitions UBA-définissables. Cette extension ( justifiée dans la section 9.4), est vraiment utile (c'est le coeur de l'outil Fast) pour pouvoir accélérer efficacement des composées d'actions. En effet, on montrera que cette extension permet de réduire *exponentiellement* le nombre de composées de fonctions affines à accélérer.

On commence par montrer que les deux conditions (*[B1]* and *[B2]*) données par Boigelot sont équivalentes à la finitude du monoïde $\langle M \rangle$.

**Lemme 9.17**
*Soit $M \in \mathcal{M}_m(\mathbb{Z})$. Les deux conditions ([B1] et [B2]) sont équivalentes à la finitude du monoïde $\langle M \rangle$.*

*Démonstration :*

Supposons qu'il existe un entier $p \in \mathbb{N}^*$ tel que les valeurs propres de $M^p$ sont dans $\{0,1\}$ et que la matrice $M^p$ est diagonalisable. Il existe alors une matrice $P$ inversible et une matrice diagonale $\Delta$ telle que $M = P^{-1}.\Delta.P$ et $\Delta_{ii} \in \{0,1\}$ pour tout $i \in \{1,\ldots,m\}$. Ainsi, $M^{2p} = M^p.M^p = P^{-1}.\Delta.P.P^{-1}\Delta.P = P^{-1}.\Delta^2.P = P^{-1}.\Delta.P = M^p$. Le monoïde $\langle M \rangle$ est donc fini.

Réciproquement, supposons que le monoïde $\langle M \rangle$ est fini. Il existe $(a,b) \in \mathbb{N}\times\mathbb{N}^*$ tel que $M^{a+b} = M^a$. Considérons le plus petit entier $d$ tel que $d \geqslant \frac{a}{b}$. De l'égalité $M^{a+b} = M^a$, on déduit $M^{a+d.b} = M^a$. En multipliant cette dernière égalité par $M^{d.b-a}$, on obtient $(M^{d.b})^2 = M^{d.b}$. Ainsi, en posant $p = d.b \leqslant (\frac{a}{b}+1).b \leqslant a+b$, on a prouvé que le polynôme $X(X-1)$ annule $M^p$. D'après [AF88], la matrice $M^p$ est diagonalisable et ses valeurs propres sont dans $\{0,1\}$. □

On peut alors démontrer l'extension du théorème 9.16 à des domaines de définition UBA-représentables.

**Théorème 9.18**
*Soit $(f, M, v)$ une fonction affine décorée, définie sur un domaine $D \subseteq \mathbb{Z}^m$ représenté par un UBA $\mathcal{A}$, et à valeur dans $\mathbb{Z}^m$.*

*Si le monoïde $\langle M \rangle$ est fini, la relation $x' \in f^*(\{x\})$ est effectivement représentable par un UBA. De plus, si $D$ est Presburger-définissable, cette relation est Presburger-définissable.*

*Démonstration :*

Rappelons que la notion de représentation d'une partie de $\mathbb{Z}^m$ par un automate binaire est donnée par la définition 9.9.

On considère la fonction $g : \mathbb{Q}^m \to \mathbb{Q}^m$ définie par $g(x) = M.x + v$ pour tout $x \in \mathbb{Q}^m$. Comme le monoïde $\{M^i;\ i \geqslant 0\}$ est fini, il existe $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ tel que $M^{a+b} = M^a$.

Montrons par récurrence sur $n \geqslant 0$ que pour tout $n \in \mathbb{N}$ et pour tout $x \in \mathbb{Q}^m$, on a $g^{a+n.b}(x) = g^a(x) + n.M^a.g^b(0)$. Pour $n = 0$, la récurrence est prouvée. Montrons la récurrence pour $n = 1$ car pour établir la récurrence, ce cas sera utilisé. De $g^b(x) = M^b.x + g^b(0)$ et $g^a(x) = M^a.x + g^a(0)$, on déduit $g^{a+b}(x) = g^a(g^b(x)) = M^a(M^b.x + g^b(0)) + g^a(0) = M^{a+b}.x + g^a(0) + M^a.g^b(0)$. De $M^{a+b} = M^a$, on déduit l'égalité $g^{a+b}(x) = g^a(x) + M^a.g^b(0)$. Considérons donc un entier $n \geqslant 1$ tel que $g^{a+n.b}(x) = g^a(x) + n.M^a.g^b(0)$ pour tout $x \in \mathbb{Q}^m$. On a alors $g^{a+(n+1).b}(x) = g^{a+n.b}(g^b(x)) = g^a(g^b(x)) + n.M^a.g^b(0) = g^a(x) + (n+1).M^a.g^b(0)$.

Ainsi, la partie $G = \{(i, x, x') \in \mathbb{N} \times \mathbb{Z}^m \times \mathbb{Z}^m;\ x' = g^i(x)\}$ est définie par la formule de Presburger suivante :

$$
\begin{aligned}
\begin{bmatrix} x' = g^i(x) \\ \wedge i \geqslant 0 \end{bmatrix} &\Longleftrightarrow \begin{cases} \displaystyle\bigvee_{r=0}^{a-1} \left[(x' = g^r(x)) \wedge (i = r)\right] \\ \displaystyle\bigvee_{r=0}^{b-1} \left[\exists n;\ \left[(n \geqslant 0) \wedge \Big((x' = g^{a+r+n.b}(x)) \wedge (i = a + r + n.b)\Big)\right]\right] \end{cases} \\
&\Longleftrightarrow \begin{cases} \displaystyle\bigvee_{r=0}^{a-1} \left[(x' = g^r(x)) \wedge (i = r)\right] \\ \displaystyle\bigvee_{r=0}^{b-1} \exists n \begin{bmatrix} (n \geqslant 0) \\ \wedge (x' = g^{a+r}(x) + n.M^{a+r}.g^b(0)) \\ \wedge (i = a + r + n.b) \end{bmatrix} \end{cases}
\end{aligned}
$$

Ainsi, on peut construire effectivement l'UBA $\mathcal{A}(G)$. Remarquons que l'on a $x' = f^i(x)$ si et seulement si $x' = g^i(x)$ et pour tout $0 \leqslant k < i$ on a $g^k(x) \in D$. On considère la partie $H = \{(k, x) \in \mathbb{N} \times \mathbb{Z};\ g^k(x) \in D\}$. Comme $(k, x) \in H$ si et seulement si $(k \geqslant 0) \wedge (\exists x';\ ((k, x, x') \in G) \wedge (x' \in D))$, on peut effectivement construire l'UBA $\mathcal{A}(H)$. Considérons enfin la relation $\mathcal{R}$ sur $\mathbb{Z}^m$ définie par $x\mathcal{R}x'$ si et seulement si $x' \in f^*(x)$. Comme $x\mathcal{R}x'$ si et seulement si $\exists i\ [(i \geqslant 0) \wedge ((i, x, x') \in G) \wedge (\forall k\ (0 \leqslant k < i) \Longrightarrow (k, x) \in H)]$, on peut construire effectivement l'UBA $\mathcal{A}(\mathcal{R})$. Remarquons enfin que si $D$ est Presburger-définissable alors $\mathcal{R}$ est aussi Presburger-définissable. □

**Remarque 9.19**
*On a ainsi étendu le théorème 9.16 en considérant des domaines de définition non-convexes.*

**Remarque 9.20**
*Comme les domaines de définition des systèmes à compteurs que l'on considère dans la pratique sont Presburger-définissables, le théorème précédent montre que si l'ensemble des états accessibles* $\mathrm{Post}_S^*(X_0)$ *n'est pas Presburger-définissable (par exemple dans [HP79]) alors un algorithme n'utilisant que des accélérations ne pourra jamais calculer cet ensemble.*

**Remarque 9.21**
*Il existe des fonctions affines dont le monoïde n'est pas fini et dont l'accélération est Presburger-définissable. Par exemple, l'accélération de la fonction affine* $f : \{0, 1\} \to \mathbb{N}$

*définie par $f(x) = 2.x$ est un ensemble fini qui est donc Presburger-définissable mais le monoïde $\{2^n;\ n \geqslant 0\}$ n'est pas fini.*

**Problème ouvert 9.22**
*Peut-on effectivement et efficacement caractériser les fonctions affines $f$ dont l'accélération est Presburger-définissable ?*

### 9.3.2 Accélération d'une composée d'actions

On montre que pour un système à compteurs effectif à monoïde fini, l'accélération de toute composée d'actions est effectivement représentable par un UBA.

Commençons par prouver que la finitude du monoïde $\mathcal{M}_S$ est nécessaire dont le cas d'un système affine dont les domaines de définition sont égaux à tout $\mathbb{Z}^m$.

**Proposition 9.23**
*Soit $S$ un système à compteurs affine dont les domaines de définition sont égaux à tout $\mathbb{Z}^m$. Le système $S$ est à monoïde fini si et seulement si l'accélération de toute composée d'actions est Presburger-définissable.*

*Démonstration :*
Considérons un système à compteurs affine $S$ dont les domaines de définition sont égaux à tout $\mathbb{Z}^m$. Montrons que pour tout $a \in \Sigma$, il existe une unique matrice $M_a \in \mathcal{M}_m(\mathbb{Q})$ et un unique vecteur $v_a \in \mathbb{Q}^m$ tel que $f_a(x) = M_a.x + v_a$. Comme $0 \in D_a$, on a $v_a = f_a(0)$ ce qui montre que $v_a$ est unique. De plus, comme pour tout $i \in \{1, \ldots, m\}$, le vecteur unitaire $e_i$ est dans $D_a$, on a $f_a(e_i) - f_a(0) = M_a.e_i$. La matrice $M_a$ est donc unique. On a de plus prouvé que les coefficients de $M_a$ et $v_a$ sont dans $\mathbb{Z}$.

Supposons que le système à compteurs $S$ soit à monoïde fini. L'accélération de $\sigma \in \Sigma^*$ est la relation $x' \in f_\sigma^*(\{x\})$ où $f_\sigma(x) = M_\sigma.x + v_\sigma$ pour tout $x \in D_\sigma$, où $M_\sigma \in \mathcal{M}_S$. Le monoïde engendré par $M_\sigma$ est donc fini. D'après le théorème 9.18, comme $D_\sigma = \mathbb{Z}^m$ est Presburger-définissable, la relation $x' \in f_\sigma^*(\{x\})$ est Presburger-définissable. Ainsi, l'accélération de toute composée d'actions est Presburger-définissable.

Réciproquement, supposons que l'accélération de toute composée d'actions est Presburger définissable. Considérons $M \in \mathcal{M}_S$ et montrons que le monoïde engendré par $M$ est fini. Par définition de $\mathcal{M}_S$, il existe une composée d'actions $\sigma \in \Sigma^*$ telle que $M_\sigma = M$. Par hypothèse l'accélération de $\sigma$ est Presburger-définissable. Ainsi, pour toute partie $X \subseteq \mathbb{Z}^m$ Presburger-définissable, la partie $f_\sigma^{-1}(X)$ est Presburger-définissable. D'après le théorème 9.16 et le lemme 9.17, le monoïde $\{M^i;\ i \geqslant 0\}$ est fini. D'après le théorème de Burnside ([MZ75], [Jac78], [MS77]), le monoïde $\mathcal{M}_S$ est fini. Ainsi, le système à compteurs $S$ est à monoïde fini. □

La proposition précédente montre qu'il est naturel de s'intéresser à la classe des systèmes à compteurs effectifs à monoïde fini.

**Théorème 9.24**
*L'accélération de toute composée d'actions d'un système à compteurs effectif à monoïde fini est effectivement représentable par un UBA. Si de plus les domaines de définition du système sont Presburger-définissables, alors l'accélération est aussi Presburger-définissable.*

*Démonstration :*

L'accélération de $\sigma \in \Sigma^*$ est la relation $x' \in f_\sigma^*(\{x\})$ où $f_\sigma(x) = M_\sigma.x + v_\sigma$ pour tout $x \in D_\sigma$. Rappelons que $M_\sigma = M_{a_n} \dots M_{a_1}$ où $(a_i)_i$ est une suite de $\Sigma$ telle que $\sigma = a_1 \dots a_n$. Comme le monoïde $\mathcal{M}_S$ est fini, le monoïde engendré par $M_\sigma$ est alors fini. D'après le théorème 9.18, la relation $x' \in f_\sigma^*(\{x\})$ est effectivement représentable par un UBA. De plus, si pour tout $a \in \Sigma$, $D_a$ est Presburger-définissable alors d'après la proposition 7.19, le domaine de définition $D_\sigma$ est Presburger-définissable. Dans ce cas la relation $x' \in f_\sigma^*(\{x\})$ est donc Presburger-définissable. □

On a donc prouvé que pour la classe des systèmes à compteurs effectif à monoïde fini, l'accélération de toute composée d'actions est effectivement représentable par un UBA. Il reste donc à expliquer comment choisir les composées d'actions à accélérer pour pouvoir effectivement construire l'ensemble des états accessibles d'un système à compteurs.

## 9.4 Choix des accélérations

On a montré dans la section précédente que l'accélération de toute composée d'actions est effectivement représentable par un UBA. Seulement, comme l'ensemble des composées d'actions est infini, le choix des accélérations à considérer dans un calcul d'ensemble d'accessibilité, devient délicat. La stratégie que l'on va étudier dans cette section, est celle qui consiste à se fixer à l'avance en entier $k \geqslant 0$, correspondant à la plus grande longueur de compositions d'actions que l'on va s'autoriser à accélérer. Il est en effet simple de modifier un algorithme dont le $k$ est fixé par un algorithme qui fait croître de 1 l'entier $k$ à chaque fois que le calcul semble diverger (dépassement de la mémoire autorisée, dépassement du temps alloué, etc).

**Définition 9.25**
*L'ensemble des composées d'au plus $k \geqslant 0$ actions d'un système à compteurs affine $S$ est l'ensemble des fonctions affines $F_k(S) = \{f_\sigma;\ |\sigma| \leqslant k\}$.*

On étudie le cardinal de $F_k(S)$ en fonction de $k$ dans la sous-section 9.4.1, en montrant des cas polynomiaux et d'autres exponentiels. Enfin, dans la sous-section 9.4.2, on montre comment réduire l'ensemble $F_k(S)$ en un nouvel ensemble $[F_k(S)]$ dont le cardinal est toujours polynomial en $k$.

### 9.4.1 Cardinal asymptotique de $F_k(S)$

On étudie le cardinal asymptotique de $F_k(S)$ en fonction de $k$. Remarquons qu'il est majoré par $\frac{\mathrm{card}(\Sigma)^{k+1}-1}{\mathrm{card}(\Sigma)-1}$. Cependant, les expérimentations que l'on a réalisées avec l'outil FAST, nous ont montrées que cette borne exponentielle dans le cas le pire n'est jamais atteinte en pratique. En effet, on observe plutôt une taille de $F_k(S)$ polynomiale en $k$. Pour expliquer ce décalage entre la borne exponentielle théorique et la borne polynomiale en pratique, on caractérise les classes de parties de $\mathbb{Z}^m$ à intersection exponentielle, polynomiale, ou constante.

**Définition 9.26**
*Pour une partie $X \subseteq \mathbb{Z}^m$, la classe $\Gamma_n(X)$ de parties de $\mathbb{Z}^m$ est définie par :*

$$\Gamma_n(X) = \{\bigcap_{v \in V}(X - v);\ V \subseteq \{-n, \dots, n\}^m\}$$

**Définition 9.27**
*Une partie $X \subseteq \mathbb{Z}^m$ est à intersection exponentielle (resp. polynomiale, constante) si le cardinal asymptotique de $\Gamma_n(X)$ est exponentiel (resp. polynomial, constant) en $n$.*

**Remarque 9.28**
*La partie $\mathbb{Z}^m$ est à intersection constante car pour tout $n \geqslant 0$, on a $\Gamma_n(X) = \{\mathbb{Z}^m\}$. La partie $X = \{0\} \subseteq \mathbb{Z}^m$ est à intersection polynomiale car $\Gamma_n(X) = \{\mathbb{Z}^m, \emptyset\} \cup \{\{b\};\ b \in \mathbb{Z}^m;\ ||b||_\infty \leqslant n\}$. La partie $X = \mathbb{Z}^m \backslash \{0\}$ n'est pas à intersection polynomiale car $\Gamma_n(X) = \{\mathbb{Z}^m \backslash V;\ V \subseteq \{-n, \dots, n\}^m\}$.*

Dans la sous-section 9.4.1.1, on caractérise les parties de $\mathbb{Z}^m$ à intersection constante. Puis, dans la sous-section 9.4.1.2, on montre qu'un polyèdre est à intersection polynomiale. On déduit de ce résultat que le cardinal asymptotique de $F_k(S)$ est polynomial en $k$ pour les systèmes à compteurs à monoïde fini dont les domaines de définition sont des polyèdres. Enfin, dans la sous-section 9.4.1.3, un exemple de parties à intersection exponentielle mais non polynomiale montrera que le cardinal de $F_k(S)$ peut-être exponentiel même pour un système à compteurs à monoïde fini dont les domaines de définition sont Presburger-définissables.

#### 9.4.1.1 Les parties à intersection constante

On caractérise exactement les parties à intersection constante en montrant que ce sont exactement les semi-réseaux.

**Définition 9.29**
*Un semi-réseau $X$ de $\mathbb{Z}^m$ est une partie de $\mathbb{Z}^m$ telle qu'il existe $p \in \mathbb{N}^*$ vérifiant $X + p.\mathbb{Z}^m = X$.*

**Remarque 9.30**
*Rappelons ([Tau92]) qu'un réseau $X$ de $\mathbb{Z}^m$ est une partie de $\mathbb{Z}^m$ telle qu'il existe une partie finie $P \subseteq \mathbb{Z}^m$ telle que $X = \sum_{p \in P} \mathbb{Z}.p$. Pour ne par rentrer dans trop de détails techniques inutiles pour notre étude, on n'introduit pas la notion de réseau.*

Le lemme suivant montre qu'un semi-réseau est la répétition d'un même motif dans toutes les directions de $p.\mathbb{Z}^m$.

**Lemme 9.31**
*Soient $X$ un semi-réseau et $p \in \mathbb{N}^*$ tels que $X + p.\mathbb{Z}^m = X$. On a l'égalité suivante :*

$$X = (X \cap \{0, \dots, p-1\}^m) + p.\mathbb{Z}^m$$

*Démonstration :*

Considérons $Y = X \cap \{0, \dots, p-1\}^m$. Comme $X + p.\mathbb{Z}^m = X$, on déduit de $Y \subseteq X$ l'inclusion $Y + p.\mathbb{Z}^m \subseteq X$. Réciproquement, considérons $x \in X$. Pour chaque $i \in \{1, \dots, m\}$, notons $y_i \in \{0, \dots, p-1\}$ l'unique entier tel que $x_i - y_i$ est divisible par $p$. On a alors $y \in \{0, \dots, p-1\}^m$. De plus, par construction il existe $z \in \mathbb{Z}^m$ tel que $x - y = p.z$. Comme $X + p\mathbb{Z}^m = X$, on déduit de $y = x - p.z$ que $y \in X$. Ainsi $y \in Y$. On a donc prouvé $X \subseteq Y + p.\mathbb{Z}^m$. □

On peut alors caractériser les parties à intersection constante.

**Théorème 9.32**
*La classe des parties à intersection constante est la classe des semi-réseaux.*

*Démonstration :*

Considérons un semi-réseau $X$. Il existe $p \in \mathbb{N}^*$ tel que $X + p.\mathbb{Z}^m = X$. Pour toute partie $V \subseteq \{-n, \dots, n\}^m$, on a $\bigcap_{v \in V}(X - v) = [\bigcap_{v \in V}(X - v)] + p.\mathbb{Z}^m$. Posons $B_V = (\bigcap_{v \in V}(X - v)) \cap \{0, \dots, p-1\}^m$. Le lemme 9.31 montre que $\bigcap_{v \in V}(X - v) = B_V + p.\mathbb{Z}^m$. On a donc prouvé la majoration $\mathrm{card}(\Gamma_n(X)) \leqslant 2^{p^m}$. Ainsi $X$ est à intersection constante.

Réciproquement, considérons une partie $X$ à intersection constante. Remarquons que si $X$ est vide alors $X$ est un semi-réseau. On peut donc supposer que $X$ est non vide. Comme la suite $(\Gamma_n(X))_{n \geqslant 0}$ est une suite croissante pour l'inclusion, et de cardinal borné, elle est stationnaire. Ainsi, il existe un entier $n_0 \geqslant 0$ tel que pour tout $n \geqslant n_0$, on a $\Gamma_n(X) = \Gamma_{n_0}(X)$. La classe $\Gamma_*(X) = \bigcup_{n \geqslant 0} \Gamma_n(X)$ est donc finie. Pour tout $i \in \{1, \dots, m\}$, comme $(X - n.e_i)_{n \geqslant 0}$ est une suite de l'ensemble fini $\Gamma_*(X)$, il existe deux entiers distincts $n' > n$ tels que $X - n.e_i = X - n'.e_i$. Posons $p_i = n' - n \in \mathbb{N}^*$. On a alors $X + p_i.e_i = X$. Considérons le pgcd $p$ de tous les $p_i$. Par construction de $p$, on a bien l'égalité $X + p.\mathbb{Z}^m = X$. □

Rappelons le lien entre la logique et les semi-réseaux dans le lemme suivant.

**Lemme 9.33**
*Une partie $X \subseteq \mathbb{Z}^m$ est un semi-réseau si et seulement elle est définissable dans la logique $\phi := t = c[k] | \phi \wedge \phi | \phi \vee \phi | \neg\phi$.*

*Démonstration :*

Soit $X \subseteq \mathbb{Z}^m$. Supposons qu'il existe $p \in \mathbb{N}^*$ et $B \subseteq \{0, \dots, p-1\}^m$ tels que $X = B + p.\mathbb{Z}^m$. Pour prouver que $X$ est dans la logique $\phi := t = c[k] | \phi \wedge \phi | \phi \vee \phi | \neg\phi$, on peut supposer que $B$ est réduit à un point $b \in \mathbb{Z}^m$. Or la formule $\bigwedge_{i=1}^{m}(x_i = b_i[p])$ définie la partie $b + p.\mathbb{Z}^m$.

Réciproquement, supposons que $X$ soit définie par une formule $\phi$ dans la logique $\phi := t = c[k] | \phi \wedge \phi | \phi \vee \phi | \neg\phi$. Considérons le pgcd $p$ des entiers $k$ intervenant dans la formule $\phi$ et remarquons que l'on a alors $X + p.\mathbb{Z}^m = X$. □

On a donc caractérisé les parties à intersection constante. Cette caractérisation sera utile dans la sous section suivante pour étudier les parties à intersection polynomiale. En effet, une partie à intersection constante est en particulier à intersection polynomiale.

#### 9.4.1.2 Les parties à intersection polynomiale

En montrant que la classe des parties à intersection polynomiale est stable par intersection finie, on prouve que tout polyèdre généralisé (l'intersection d'un polyèdre avec un semi-réseaux) est à intersection polynomiale. On déduit de ce résultat que pour un système à compteurs à monoïde fini dont les domaines de définition sont des polyèdres généralisés, la taille asymptotique de $F_k(S)$ est polynomiale en $k$.

On commence par caractériser les fonctions affines laissant stable par image inverse les parties à intersection polynomiale.

**Proposition 9.34**
*Soit $f : D \to \mathbb{Z}^m$ une fonction affine définie sur une partie $D \subseteq \mathbb{Z}^m$. Les deux assertions suivantes sont équivalentes :*
- *$D$ est à intersection polynomiale.*
- *Pour tout $X$ à intersection polynomiale, $f^{-1}(X)$ est à intersection polynomiale.*

*Démonstration :*
Une des implications est évidente. En effet, si pour tout $X$ à intersection polynomiale, $f^{-1}(X)$ est à intersection polynomiale, comme en particulier $\mathbb{Z}^m$ est à intersection polynomiale, la partie $D = f^{-1}(\mathbb{Z}^m)$ est à intersection polynomiale. Réciproquement, considérons une fonction affine $f : D \to \mathbb{Z}^m$ telle que $D$ est à intersection polynomiale. Montrons que pour tout $X$ à intersection polynomiale, $f^{-1}(X)$ est à intersection polynomiale. Comme $f$ est une fonction affine, il existe $M \in \mathcal{M}_m(\mathbb{Q})$ et $a \in \mathbb{Q}^m$ tels que $f(x) = M.x + a$ pour tout $x \in D$. On considère la fonction affine $g : \mathbb{Q}^m \to \mathbb{Q}^m$ définie par $g(x) = M.x + a$ pour tout $x \in \mathbb{Q}^m$. On a :

$$\begin{aligned}
\bigcap_{v\in V}(f^{-1}(X) - v) &= \bigcap_{v\in V}((g^{-1}(X) \cap D) - v) \\
&= \bigcap_{v\in V}(g^{-1}(X) - v) \bigcap_{v\in V}(D - v) \\
&= g^{-1}(\bigcap_{v\in V}(X - g(v))) \bigcap_{v\in V}(D - v)
\end{aligned}$$

Remarquons que si $V = \emptyset$ alors $\bigcap_{v\in V}(f^{-1}(X) - v) = \mathbb{Z}^m$. On peut donc supposer que $V \neq \emptyset$. Considérons alors un élément $v_0 \in V$. On suppose que $\bigcap_{v\in V}(f^{-1}(X) - v)$ est non vide. On va montrer que $g(V) \subseteq g(v_0) + \mathbb{Z}^m$. Comme $\bigcap_{v\in V}(f^{-1}(X) - v)$ est non vide, l'intersection $\bigcap_{v\in V}(X - g(v))$ est non vide. Ainsi, il existe $y_0 \in \bigcap_{v\in V}(X - g(v))$. Comme $v_0 \in V$, il existe $x_0 \in X$ tel que $y_0 = x_0 - g(v_0)$. De même, pour tout $v \in V$, il existe $x \in X$ tel que $y_0 = x - g(v)$. Ainsi, $g(v) = g(v_0) + (x - x_0)$. Comme $x - x_0 \in \mathbb{Z}^m$, on a prouvé que $g(V) \subseteq g(v_0) + \mathbb{Z}^m$. Posons $W = g(V) - g(v_0)$. On a alors :

$$\bigcap_{v\in V}(f^{-1}(X) - v) = g^{-1}\left(g(v_0) + (\bigcap_{w\in W}(X - w))\right) \bigcap_{v\in V}(D - v)$$

Majorons la norme infini des éléments de $W$ en fonction de $n$. Soit $w \in W$. Il existe $v \in V$ tel que $w = g(v) - g(v_0)$. Donc $||w||_\infty \leqslant m. ||M||_\infty .(||v||_\infty + ||v_0||_\infty) \leqslant 2.m. ||M||_\infty .n$. On a donc prouvé la majoration suivante :

$$\mathrm{card}(\Gamma_n(f^{-1}(X))) \leqslant 2 + (2.n+1)^m.\mathrm{card}(\Gamma_{2.m.||M||_\infty.n}(X)).\mathrm{card}(\Gamma_n(D))$$

Ainsi, $f^{-1}(X)$ est à intersection polynomiale. □

On peut alors prouver le théorème suivant, justifiant l'étude des parties à intersection polynomiale.

**Théorème 9.35**
*Soit $S$ un système à compteurs à monoïde fini dont les domaines de définition sont à intersection polynomiale. Le cardinal asymptotique de $F_k(S)$ est polynomial en $k$.*

*Démonstration :*
Considérons un système à compteurs à monoïde fini $(S, (M_a, v_a)_{a\in\Sigma})$ défini sur des domaines de définition à intersection polynomiale. On note $g_\sigma : \mathbb{Q}^m \to \mathbb{Q}^m$ la fonction affine définie par $g_\sigma(x) = M_\sigma.x+v_\sigma$ pour tout $x \in \mathbb{Q}^m$. On considère des entiers $c_S, d_S \in \mathbb{N}^*$ vérifiant la proposition 7.13.

Considérons une suite $(a_i)_{1\leqslant i\leqslant n}$ avec $n \geqslant 1$ de $\Sigma$ et posons $\sigma = a_1 \dots a_n$, $\sigma_0 = \varepsilon$ et $\sigma_i = a_1 \dots a_i$ pour $i \in \{1, \dots, n\}$. La partie $I_{(M,a)}(\sigma) = \{i \in \{1, \dots, |\sigma|\};\ M_{\sigma_{i-1}} = M;\ a_i = a\}$ permet de décrire facilement le domaine de définition $D_\sigma$ de la fonction $f_\sigma$ :

$$\begin{aligned} D_\sigma &= g_0^{-1}(D_{a_1}) \cap g_1^{-1}(D_{a_2}) \cap \dots \cap g_{n-1}^{-1}(D_{a_n}) \\ &= \bigcap_{\substack{(M,a) \\ i\in I_{(M,a)(\sigma)}}} (d_S.M)^{-1}(d_S.D_a - d_S.v_{\sigma_{i-1}}) \end{aligned}$$

Comme $d_S.\mathbb{Z}^m$ est un semi-réseaux, la proposition 9.32 montre que $d_S.\mathbb{Z}^m$ est à intersection polynomiale. En utilisant la fonction affine $d_S.\mathbb{Z}^m \to \mathbb{Z}^m$ qui à $x$ associe $\frac{1}{d_S}.x$, on déduit de la proposition 9.34 que $d_S.D_a$ est à intersection polynomiale. La précédente égalité montre que le cardinal de $\{D_\sigma;\ |\sigma| \leqslant k\}$ est borné par $\prod_{(M,a)} \Gamma_{c_S.k}(d_S.D_a)$. Comme le cardinal de $\{g_\sigma;\ |\sigma| \leqslant k\}$ est borné par $\mathrm{card}(\mathcal{M}_S).(2.c_S.k+1)^m$, on a prouvé la majoration suivante :

$$\mathrm{card}(F_k(S)) \leqslant \mathrm{card}(\mathcal{M}_S).(2.c_S.k+1)^m.\left(\prod_a \mathrm{card}(\Gamma_{c_S.k}(d_S.D_a))\right)^{\mathrm{card}(\mathcal{M}_S)}$$

Ainsi, $\mathrm{card}(F_k(S))$ est majoré par un polynôme en $k$. □

On se propose d'appliquer le théorème précédent au cas des polyèdres généralisés. Pour cela, on va montrer que la classe des parties à intersection polynomiale est stable par intersection finie et contient les demi-espaces de $\mathbb{Z}^m$.

**Définition 9.36**
*Un polyèdre généralisé est l'intersection d'un polyèdre et d'un semi-réseau.*

**Remarque 9.37**
*Comme $\mathbb{Z}^m$ est un semi-réseau, un polyèdre est un cas particulier de polyèdres généralisés.*

**Proposition 9.38**
*La classe des parties à intersection polynomiale est stable par intersection finie.*

*Démonstration :*
Considérons une suite finie $(X_i)_{i\in I}$ de parties à intersection polynomiale et posons $X = \bigcap_{i\in I} X_i$. Soit $V \subseteq \{-n,\dots,n\}^m$, on a :

$$\bigcap_{v\in V}(X-v) = \bigcap_{i\in I}(\bigcap_{v\in V}(X_i - v))$$

De l'égalité précédente, on déduit la majoration suivante :

$$\mathrm{card}(\Gamma_n(X)) \leqslant \prod_{i\in I}\mathrm{card}(\Gamma_n(X_i))$$

Ainsi, la partie $X$ est à intersection polynomiale. □

**Proposition 9.39**
*Tout demi-espace de $\mathbb{Z}^m$ est à intersection polynomiale.*

*Démonstration :*
Soit $X$ un demi-espace de $\mathbb{Z}^m$. Il existe $\alpha \in \mathbb{Q}^m$ et $c \in \mathbb{Q}$ tels que $X = \{x \in \mathbb{Z}^m;\ \langle\alpha, x\rangle \leqslant c\}$. Quitte à multiplier $\alpha$ et $c$ par un entier non nul assez grand, on peut supposer que $\alpha \in \mathbb{Z}^m$ et $c \in \mathbb{Z}$. Considérons une partie $V \subseteq \{-n,\dots,n\}^m$ non vide. La partie $\bigcap_{v\in V}(X-v)$ est alors définie par la formule $\langle\alpha, x\rangle \leqslant c + c_V$ où $c_V = \min(\{\langle\alpha, v\rangle;\ v \in V\})$. Comme $|\langle\alpha, v\rangle| \leqslant \sqrt{\langle\alpha,\alpha\rangle}.\sqrt{\langle v, v\rangle} \leqslant \sqrt{\langle\alpha,\alpha\rangle}.n^m$, on a $c_V \in \{-\sqrt{\langle\alpha,\alpha\rangle}.n^m, \dots, \sqrt{\langle\alpha,\alpha\rangle}.n^m\} \cap \mathbb{Z}$. Comme la partie $\bigcap_{v\in V}(X-v)$ est définie par la formule $\langle\alpha, x\rangle \leqslant c + c_V$, on a prouvé la majoration suivante :

$$\mathrm{card}(\Gamma_n(X)) \leqslant 2.(\sqrt{\langle\alpha,\alpha\rangle}.n^m + 1)$$

On a donc prouvé que $\mathrm{card}(\Gamma_n(X))$ est polynomial en $n$. □

Comme un polyèdre généralisé est une intersection finie de semi-réseaux et de demi-espaces, on déduit les corollaires suivants :

**Corollaire 9.40**
*Un polyèdre généralisé est à intersection polynomiale.*

**Corollaire 9.41**
*Soit $S$ un système à compteurs à monoïde fini dont les domaines de définition sont des polyèdres généralisés. Le cardinal asymptotique de $F_k(S)$ est polynomial en $k$.*

Le corollaire précédent explique pourquoi en pratique, le cardinal asymptotique de $F_k(S)$ est polynomial en $k$. En effet, sur plus de 40 exemples de systèmes à compteurs analysés avec FAST, seuls 2 ne rentraient pas dans le cadre du corollaire précédent (pour ces deux exemples, le monoïde est infini).

Quand les domaines de définition du système $S$ sont Presburger-définissables, on pourrait envisager de décomposer ces domaines comme une union finie de polyèdres généralisés (voir la proposition 9.42). Cependant, on ne sait pas décomposer efficacement une partie Presburger-définissable représentée par un UBA en une union finie d'UBA représentant des polyèdres généralisés (problème ouvert 5.15).

**Proposition 9.42**
*Une partie $X \subseteq \mathbb{Z}^m$ est Presburger-définissable si et seulement si c'est une union finie de polyèdres généralisés.*

*Démonstration :*
Considérons une partie $X$ Presburger-définissable. Il existe une formule de Presburger $\phi$ définissant $X$. Un algorithme d'élimination des quantificateurs montre que $\phi$ est équivalente à une disjonction de formules de la forme $\bigwedge_{\alpha,c}(\langle \alpha, x\rangle \leqslant c) \bigwedge_{\alpha,c,k}(\langle \alpha, x\rangle = c[k])$. Ainsi, $X$ est une union finie de polyèdres généralisés. Un polyèdre généralisé étant Presburger-définissable, la réciproque est immédiate. □

**Remarque 9.43**
*La partie $X = \{2^n;\ n \geqslant 0\}$ est à intersection polynomiale. Il existe donc des parties à intersection polynomiale qui ne sont pas Presburger-définissables. La caractérisation des parties Presburger-définissables à intersection polynomiale est un problème difficile.*

**Problème ouvert 9.44**
*Caractériser les parties Presburger-définissables à intersection polynomiale.*

#### 9.4.1.3 Les parties à intersection exponentielle

À partir d'une partie Presburger-définissable à intersection exponentiel mais non polynomial, on déduit un exemple de système à compteurs $S$ à monoïde fini dont les domaines de définition sont Presburger-définissables et tel que le cardinal de $F_k(S)$ est exponentiel en $k$.

**Lemme 9.45**
*La partie $X = \{(x_1, x_2) \in \mathbb{N}^2;\ x_1 \neq x_2\}$ n'est pas à intersection polynomiale.*

*Démonstration :*
En effet, $\Gamma_n(X)$ contient toutes les parties $\bigcap_{i\in I} X - (0, i) = \bigcap_{i\in I}\{(x_1, x_2) \in \mathbb{N}^2;\ x_1 + i \neq x_2\}$ pour tout $I \subseteq \{0, \dots, n\}$ avec $0 \in I$. Ainsi $\text{card}(\Gamma_n(X)) \geqslant 2^n$ qui n'est donc pas polynômial. □

**Exemple 9.46**
*Soit $S_{exp} = (\mathbb{N}^2, \Sigma, (\mathcal{R}_a)_{a\in\Sigma})$ le système à compteurs à monoïde fini défini par $\Sigma = \{a, b\}$ et par*

$$\begin{cases} (x_1, x_2) \to_a (x_1, x_2) & \textit{pour tout } (x_1, x_2) \in \{(x_1, x_2) \in \mathbb{N}^2;\ x_1 \neq x_2\} \\ (x_1, x_2) \to_b (x_1 + 1, x_2) & \textit{pour tout } (x_1, x_2) \in \mathbb{N}^2 \end{cases}$$

**Proposition 9.47**
*Pour tout entier $n \geqslant 1$, on a* $\mathrm{card}(F_{3.n}(S_{exp})) \geqslant 2^n$.

*Démonstration :*

Soit $n \geqslant 1$. Considérons une partie $I \subseteq \{1, \ldots, n\}$. Les suites $(u_i^I)_{1 \leqslant i \leqslant n}$ et $(w_i^I)_{1 \leqslant i \leqslant n}$ de $\Sigma^*$ sont définies par :

$$u_i^I = \begin{cases} bb & \text{si } i \in I \\ b & \text{si } i \notin I \end{cases}$$

$$w_i^I = \begin{cases} \varepsilon & \text{si } i \in I \\ b & \text{si } i \notin I \end{cases}$$

Soit $\sigma^I = (u_n^I a w_n^I) \ldots (u_1^I a w_1^I)$. Le domaine de définition $D_I$ de $f_{\sigma^I}$ est donné par l'égalité suivante :

$$D_I = \bigcap_{i=1}^{n} \{(x_1, x_2) \in \mathbb{N}^2;\ x_1 + 2.(i-1) + |w_i^I| \neq x_2\}$$

Considérons alors une autre partie $I' \subseteq \{1, \ldots, n\}$ telle que $I \neq I'$ et montrons que $D_I \neq D_{I'}$. Soit il existe $i \in I$ tel que $i \notin I'$ soit il existe $i \in I'$ tel que $i \notin I$. Par symétrie, on peut supposer qu'il existe $i \in I$ tel que $i \notin I'$. Remarquons que $(0, 2.(i-1)+1) \in D_I$ alors que $(0, 2.(i-1)+1) \notin D_{I'}$. Ainsi, on a bien prouvé que $D_I \neq D_{I'}$.

Comme pour toute partie $I \subseteq \{1, \ldots, n\}$, on a $|\sigma^I| = 3.n$, on a prouvé la minoration $\mathrm{card}(F_{3.n}(S_{exp})) \geqslant 2^n$. □

### 9.4.2 Réduction de $F_k(S)$

On a montré dans la précédente section que le cardinal de $F_k(S)$ pouvait-être exponentiel en $k$. Pour obtenir une taille polynomial en $k$ quelque soit le système à compteur à monoïde fini $S$, on va étudier dans cette section une méthode de réduction de l'ensemble $F_k(S)$.

Dans la sous-section 9.4.2.1, on introduit la notion de réduction d'un ensemble de fonctions affines décorées. Cette réduction est appliquée à l'ensemble $F_k(S)$ dans la sous-section 9.4.2.2. On prouve alors que le réduit de $F_k(S)$ est calculable en temps polynomial en fonction de $k$. Enfin, l'accélération des fonctions réduite est étudiée dans la sous-section 9.4.2.3.

Toutes les fonctions affines décorées $(f, M_f, v_f)$ de cette section sont définies sur une partie $D_f \subseteq \mathbb{Z}^m$ et à valeur dans $\mathbb{Z}^m$.

**Définition 9.48**
*Soient $F_1$ et $F_2$ deux ensembles de fonctions affines décorées. On note* $F_1 \circ F_2 = \{f_1 \circ f_2;\ f_1 \in F_1;\ f_2 \in F_2\}$.

#### 9.4.2.1 Réduction d'un ensemble de fonctions affines décorées

À partir de deux fonctions affines $f$ et $g$ de même décoration $(f, M, v)$ et $(g, M, v)$, on peut construire une unique fonction affine décorée $(h, M, v)$ dont le domaine de définition est l'union des domaines de définition de $f$ et $g$. Cette nouvelle fonction affine a de bonnes propriétés vis-à-vis de l'accessibilité car pour tout $X \subseteq \mathbb{Z}^m$, on a :

$$\begin{cases} f(X) \cup g(X) = h(X) \\ f^{-1}(X) \cup g^{-1}(X) = h^{-1}(X) \end{cases}$$

Après avoir défini la réduction, on montre que la réduction commute avec l'union et la composition.

**Définition 9.49**
*Le réduit d'un ensemble $F$ de fonctions affines décorées est l'ensemble $[F]$ des fonctions affines décorées $(g, M_g, v_g)$ telles que le domaine de définition $D_g$ défini par l'égalité suivante est non vide.*

$$D_g = \bigcup_{\substack{(f,M_f,v_f)\in F \\ (M_f,v_f)=(M_g,v_g)}} D_f$$

**Proposition 9.50**
*Soit $F$ un ensemble fini de fonctions affines décorées. On a :*

$$\mathrm{card}([F]) \leqslant \mathrm{card}(F)$$

*Démonstration :*
Par définition immédiate du réduit. □

Le lemme technique suivant est utilisé pour démontrer que la réduction commute avec l'union et la composition.

**Lemme 9.51**
*Soient $F_1$ et $F_2$ deux ensembles de fonctions affines décorées tels que*
- *pour tout $(f_1, M, v) \in F_1$ et pour tout $x \in D_{f_1}$, il existe $(f_2, M, v) \in F_2$ vérifiant $x \in D_{f_2}$, et*
- *pour tout $(f_2, M, v) \in F_2$ et pour tout $x \in D_{f_2}$, il existe $(f_1, M, v) \in F_1$ vérifiant $x \in D_{f_1}$.*

*Alors $[F_1] = [F_2]$.*

*Démonstration :*
Par symétrie, il suffit de montrer l'inclusion $[F_1] \subseteq [F_2]$. Remarquons que si $[F_1] = \emptyset$ alors l'inclusion est triviale. On peut donc supposer que $[F_1] \neq \emptyset$. Considérons $(g, M, v) \in [F_1]$ et $x \in D_g$. Par définition de $D_g$, il existe $(f_1, M, v) \in F_1$ telle que $x \in D_{f_1}$. Par hypothèse, il existe $(f_2, M, v) \in F_2$ telle que $x \in D_{f_2}$. Par définition du réduit, il existe une unique fonction affine $g'$ telle que $(g', M, v) \in [F_2]$. De plus, comme $x \in D_{f_2}$, on a $x \in D_{g'}$.

On a donc prouvé que $D_g \subseteq D_{g'}$. Considérons alors $x \in D_{g'}$. Il existe $(f_2, M, v) \in F_2$ telle que $x \in D_{f_2}$. Par hypothèse du lemme, il existe une fonction $(f_1, M, v) \in F_1$ telle que $x \in D_{f_1}$. Par définition du réduit, on a $x \in D_g$. Ainsi, $D_g = D_{g'}$. Comme pour tout $x \in D_g$ on a $g(x) = M.x + v$ et pour tout $x \in D_{g'}$ on a $g'(x) = M.x + v$, on a prouvé que $g = g'$. Ainsi, $(g, M, v) \in [F_2]$. On a prouvé l'inclusion $[F_1] \subseteq [F_1]$. □

**Corollaire 9.52**
*Soient $F_1$ et $F_2$ deux ensembles de fonctions affines décorées. On a*

$$[F_1 \cup F_2] = [[F_1] \cup [F_2]]$$

**Proposition 9.53**
*Soient $F_1$ et $F_2$ deux ensembles de fonctions affines décorées. On a*

$$[F_1 \circ F_2] = [[F_1] \circ [F_2]]$$

*Démonstration :*

On va utiliser le lemme 9.51 pour prouver l'égalité.

Montrons que pour tout $(g, M, v) \in F_1 \circ F_2$ et pour tout $x \in D_g$, il existe $(g', M, v) \in [F_1] \circ [F_2]$ vérifiant $x \in D_{g'}$. Si pour tout $(g, M, v) \in F_1 \circ F_2$ on a $D_g = \emptyset$, alors la propriété est prouvée. On peut donc supposer qu'il existe $(g, M, v) \in F_1 \circ F_2$ telle que $D_g \neq \emptyset$. Considérons une telle fonction affine décorée $(g, M, v) \in F_1 \circ F_2$ et un vecteur $x \in D_g$. Il existe $(f_1, M_1, v_1) \in F_1$ et $(f_2, M_2, v_2) \in F_2$ telles que $(f_1, M_1, v_1) \circ (f_2, M_2, v_2) = (g, M, v)$. De $D_g \neq \emptyset$, on déduit $D_{f_1} \neq \emptyset$ et $D_{f_2} \neq \emptyset$. Comme $(f_1, M_1, v_1) \in F_1$ et $D_{f_1} \neq \emptyset$, il existe $(f'_1, M_1, v_1) \in [F_1]$. De même, comme $(f_2, M_2, v_2) \in F_2$ et $D_{f_2} \neq \emptyset$, il existe $(f'_2, M_2, v_2) \in [F_2]$. Par définition du réduit, on a $D_{f_1} \subseteq D_{f'_1}$ et $D_{f_2} \subseteq D_{f'_2}$. Posons $g' = f'_1 \circ f'_2$. De $D_{f_1 \circ f_2} \subseteq D_{f'_1 \circ f'_2}$, on obtient $x \in D_{g'}$. Comme $(g, M, v) \in [F_1] \circ [F_2]$, on bien prouvé que pour tout $(g, M, v) \in F_1 \circ F_2$ et pour tout $x \in D_g$, il existe $(g', M, v) \in [F_1] \circ [F_2]$ vérifiant $x \in D_{g'}$.

Montrons alors que pour tout $(g, M, v) \in [F_1] \circ [F_2]$ et pour tout $x \in D_g$, il existe $(g', M, v) \in F_1 \circ F_2$ vérifiant $x \in D_{g'}$. Si pour tout $(g, M, v) \in [F_1] \circ [F_2]$ on a $D_g = \emptyset$, alors la propriété est prouvée. On peut donc supposer qu'il existe $(g, M, v) \in [F_1] \circ [F_2]$ telle que $D_g \neq \emptyset$. Considérons une telle fonction affine décorée $(g, M, v) \in [F_1] \circ [F_2]$ et un vecteur $x \in D_g$. Il existe $(f_1, M_1, v_1) \in [F_1]$ et $(f_2, M_2, v_2) \in [F_2]$ tels que $(g, M, v) = (f_1, M_1, v_1) \circ (f_2, M_2, v_2)$. Comme $x \in D_g$, on a $x \in D_{f_2}$ et $f_2(x) \in D_{f_1}$. Par définition du réduit, il existe $(f'_2, M_2, v_2) \in F_2$ telle que $x \in D_{f'_2}$ et il existe $(f'_1, M_1, v_1) \in F_1$ telle que $f_2(x) \in D_{f'_1}$. Comme $x \in D_{f'_2}$, on a $f_2(x) = M_2.x + v_2 = f'_2(x)$. Ainsi, on a bien $x \in D_{f'_1 \circ f'_2}$. Posons $g' = f'_1 \circ f'_2$. Comme $x \in D_{g'}$ et $(g', M, v) \in F_1 \circ F_2$, on bien prouvé que pour tout $(g, M, v) \in [F_1] \circ [F_2]$ et pour tout $x \in D_g$, il existe $(g', M, v) \in F_1 \circ F_2$ vérifiant $x \in D_{g'}$.

D'après le lemme 9.51, on a prouvé l'égalité $[F_1 \circ F_2] = [[F_1] \circ [F_2]]$. □

#### 9.4.2.2 Calcul polynomial en $k$ de $[F_k(S)]$

On va alors s'intéresser au réduit $[F_k(S)]$ pour un système $S$ à monoïde fini dont les domaines de définition sont UBA-représentables. En plus de prouver que le cardinal de cet ensemble est polynomial en $k$, on montre qu'il est calculable en temps polynomial en fonction de $k$. Cela est vraiment surprenant car l'on pouvait s'attendre à un coût au minimum exponentiel du à la taille des UBA représentant les domaines de définition des fonctions réduites.

Par définition du réduit, on peut facilement montrer que le cardinal de $[F_k(S)]$ est polynomial en $k$.

**Proposition 9.54**
*Pour tout système à compteurs $S$ à monoïde fini, le cardinal de $[F_k(S)]$ est en $O(k^m)$.*

*Démonstration :*
Considérons un système à compteurs décoré $(S, (M_a, v_a)_{a\in\Sigma})$ à monoïde fini. On considère $c_S, d_S \in \mathbb{N}^*$ vérifiant la proposition 7.13. Par définition du réduit, pour tout $\sigma \in \Sigma^{\leqslant k}$, il existe une unique fonction affine $g$ telle que $(g, M_\sigma, v_\sigma) \in [F_k(S)]$. Comme $d_S.v_k \in \mathbb{Z}^m$ et $||d_S.v_k||_\infty \leqslant c_S.k$, on a :

$$\mathrm{card}([F_k(S)]) \leqslant \mathrm{card}(\mathcal{M}_S).(2.c_S.k+1)^m$$

On a ainsi prouvé la proposition. □

Après avoir défini la taille d'un ensemble fini de fonctions affines décorées dont les domaines de définition sont UBA-représentables, on montre que la taille de $[F_k(S)]$ est polynomial en $k$.

**Définition 9.55**
*La taille d'un ensemble fini de fonctions affines décorées dont les domaines de définition sont UBA-représentables est égale à :*

$$\mathrm{taille}(F) = \sum_{(f,M_f,v_f)\in F} \mathrm{taille}(\mathcal{A}(D_f)) + \mathrm{taille}(M_f) + \mathrm{taille}(v_f)$$

**Proposition 9.56**
*La taille asymptotique de $[F_k(S)]$ est en $O(k^{2.m})$.*

*Démonstration :*
D'après la proposition 7.14, il existe une classe finie de parties $\mathcal{C}_S$ telle que pour tout $w \in \Sigma_r^*$ et pour tout $\sigma \in \Sigma^*$, on a :

$$|w| \geqslant m.\frac{\ln(1+|\sigma|)}{\ln(r)} \implies \gamma_w^{-1}(D_\sigma) \in \mathcal{C}_S$$

De plus, d'après la proposition 7.13, il existe deux entiers $c_S, d_S \in \mathbb{N}^*$ tels que pour tout $\sigma \in \Sigma^*$, on a $d_S.v_\sigma \in \mathbb{Z}^m$ et $||d_S.v_\sigma||_\infty \leqslant c_S.|\sigma|$.

Rappelons que le cardinal de $[F_k(S)]$ est en $k^m$ (proposition 9.54). Il suffit donc de prouver que taille$(D_f)$, taille$(M_f)$ et taille$(v_f)$ sont en $k^m$ pour $(f, M_f, v_f) \in [F_k(S)]$. Comme taille$(M_f) \leqslant \max(\{\mathrm{taille}(M);\ M \in \mathcal{M}_S\})$ et taille$(v_f) \leqslant \ln(1+d_S)+\ln(1+c_S.k)$, il suffit de majorer taille$(D_f)$ par une fonction en $k^m$. Par définition du réduit, il existe une partie $U_f \subseteq \Sigma^{\leqslant k}$ telle que $D_f = \bigcup_{\sigma \in U_f} D_\sigma$. Ainsi pour tout mot $w \in \Sigma_r^*$ tel que $w \geqslant m.\frac{\ln(1+k)}{\ln(r)}$, on a $\gamma_w^{-1}(D_f)$ dans la classe finie $\mathcal{C}$ de parties de $\mathbb{N}^m$ définie par :

$$\mathcal{C} = \{\bigcup_{X \in F} X;\ F \subseteq \mathcal{C}_S\}$$

On a donc prouvé la majoration suivante :

$$\text{taille}(\mathcal{A}(D_f)) \leqslant \frac{1}{r-1}(1+k)^m + \text{card}(\mathcal{C})$$

Ainsi, taille($[F_k(S)]$) est en $O(k^{2.m})$. □

Pour calculer efficacement $[F_k(S)]$, on ne va pas calculer $[F_k(S)]$ en fonction de $F_k(S)$ car ce dernier peut être exponentiel en $k$. En fait, en le calculant par récurrence en fonction de $[F_{k-1}(S)]$, on montre que l'on obtient un algorithme polynomial en $k$.

**Proposition 9.57**
*Soit $(S, (M_a, v_a)_{a\in\Sigma})$ un système à compteurs à monoïde fini et $F_S = [\{(\text{id}_{\mathbb{Z}^m}, I, 0)\} \cup \{(f_a, M_a, v_a);\ a \in \Sigma\}]$. On a la récurrence suivante :*

$$\begin{cases} [F_1(S)] = F_S \\ [F_{k+1}(S)] = [[F_k(S)] \circ F_S] \quad \textit{pour } k \geqslant 1 \end{cases}$$

*Démonstration :*

D'après le corollaire 9.52 et la proposition 9.53, on déduit de $F_{k+1}(S) = F_k(S) \circ F_S$, l'égalité $[F_{k+1}(S)] = [[F_k(S)] \circ F_S]$. □

On peut alors prouver que le calcul de $[F_k(S)]$ est polynomial en $k$.

**Théorème 9.58**
*Soit $S$ un système à compteurs à monoïde fini. L'ensemble $[F_k(S)]$ est calculable en temps polynômial en fonction de $k$.*

*Démonstration :*

Soit $G$ un ensemble réduit de fonctions affines décorées. Par définition du réduit, pour tout $(M, v) \in \mathcal{M}_m(\mathbb{Q}) \times \mathbb{Q}^m$, il existe au plus une fonction affine $g$ telle que $(g, M, v) \in G$. Quand une telle fonction existe, on la note $G(M, v)$. Si une telle fonction n'existe pas, on note $G(M, v) = (g_\emptyset, M, v)$ la fonction affine décorée définie sur l'ensemble vide. On note $D_G$ le sous ensemble des couples $(M, v) \in \mathcal{M}_m(\mathbb{Q}) \times \mathbb{Q}^m$ tels que $G(M, v)$ n'est pas la fonction définie sur l'ensemble non vide.

Posons $G_k = [F_k(S)]$. D'après la proposition 9.56, il suffit de montrer que l'on peut calculer $G_{k+1}$ en fonction de $G_k$ en temps polynomial en fonction de $k$. La proposition 9.57 montre que $G_{k+1} = [G_k \circ [F_S]] = [G_k \circ F_S]$ où $F_S = \{(\text{id}_{\mathbb{Z}^m}, I, 0)\} \cup \{(f_a, M_a, v_a);\ a \in \Sigma\}$. Considérons l'ensemble $D_{k+1}$ défini par :

$$D_{k+1} = \{(M_k.M, M_k.v + v_k);\ (M_k, v_k) \in D_{G_k};\ (M, v) \in D_F\}$$

On a alors l'inclusion $D_{G_{k+1}} \subseteq D_{k+1}$ où $D_{k+1}$ est calculable en temps polynomial en fonction de $k$. De plus, pour tout $(M', v') \in D_{k+1}$, le domaine de définition de la fonction $G_{k+1}(M', v')$ est donné par :

$$D_{G_{k+1}(M',v')} = \bigcup_{\substack{(f,M,v)\in F \\ (M_k,v_k)\in D_{G_k} \\ M'=M_k.M \\ v'=M_k.v+v_k}} f^{-1}(D_{G_k(M_k,v_k)})$$

Pour chaque fonction affine décorée $(f, M, v) \in F$, on considère l'UBA $\mathcal{A}_f$ représentant la relation $x' = f(x)$. D'après le théorème 7.3, on peut calculer pour toute partie $X$ représentée par l'UBA $\mathcal{A}(X)$, l'UBA $\mathcal{A}(f^{-1}(X))$ en temps $O((\text{taille}(\mathcal{A}(X)) + 1)^{\text{taille}(\mathcal{A}_f)})$. Ainsi, $\mathcal{A}(D_{G_{k+1}(M',v')})$ est calculable en temps polynomial en $k$ comme le montre l'égalité suivante :

$$O\left(\prod_{(f,M,v)\in F} \prod_{\substack{M_k\in\mathcal{M}_S \\ M'=M_k.M}} (\text{taille}(\mathcal{A}(D_{G_k(M_k,v'-M_k.v)})) + 1)^{\text{taille}(\mathcal{A}_f)}\right)$$
$$= O\left(\text{taille}(G_k)^{\text{taille}(F_S).\text{card}(\mathcal{M}_S)}\right)$$

L'ensemble $G_{k+1}$ est alors calculable en temps polynomial en $k$ en utilisant l'égalité suivante :

$$G_{k+1} = \bigcup_{\substack{(M',v')\in D_{k+1} \\ D_{G_{k+1}(M',v')}\neq\emptyset}} \{(f', M', v');\ D_{f'} = D_{G_{k+1}(M',v')}\}$$

□

On a prouvé que l'ensemble $[F_k(S)]$ est calculable en temps polynomial en $k$. Dans la sous-section suivante, on montre comment utiliser cet ensemble pour calculer $\text{Post}_S^*(X)$ ou $\text{Pre}_S^*(X)$ par accélération de fonctions dans $[F_k(S)]$.

#### 9.4.2.3 Accélération de fonctions réduites

On montre comment utiliser les fonctions affines de $[F_k(S)]$ pour calculer l'ensemble des états accessibles $\text{Post}_S^*(X)$ (l'ensemble $\text{Pre}_S^*(X')$ se calcule symétriquement).

**Définition 9.59**
*L'ensemble des composées réduites d'au plus $k \geqslant 0$ actions d'un système à compteurs affine décoré $S$ est l'ensemble des fonctions affines $[F_k(S)]$.*

Rappelons que l'accélération de toute composée d'actions d'un système à compteurs effectif à monoïde fini est effectivement représentable par un UBA. Le théorème suivant montre que même après réduction, l'accélération des fonctions affines de $[F_k(S)]$ restent effectivement représentables par des UBA.

**Théorème 9.60**
*Soit $S$ un système à compteurs effectif à monoïde fini. L'accélération de toute fonction affine décorée de $\bigcup_{k\geqslant 0}[F_k(S)]$ est effectivement représentable par un UBA. Si de plus les domaines de définition du système sont Presburger-définissables, alors l'accélération est aussi Presburger-définissable.*

*Démonstration :*

Considérons un système à compteur $S$ à monoïde fini. Pour toute fonction affine $f \in \bigcup_{k\geqslant 0}[F_k(S)]$, il existe $M \in \mathcal{M}_S$ et $v \in \mathbb{Q}^m$ tels que $f(x) = M.x + v$ pour tout $x \in D_f$. Comme $\mathcal{M}_S$ est fini, on déduit le théorème du théorème 9.18. □

On définit la notion de partie calculable par accélération.

**Définition 9.61**
*Soit $S$ un système à compteurs décoré. Une partie $X'$ est dite calculable à partie d'une partie $X$ :*
- *en $n \geqslant 0$ accélérations de longueur $k$ s'il existe $n$ fonctions affines $f_1$, ..., $f_n$ dans $F_k(S)$ telles que $X' = f_n^* \circ \cdots \circ f_1^*(X)$.*
- *en $n \geqslant 0$ accélérations réduites de longueur $k$ s'il existe $n$ fonctions affines $g_1$, ..., $g_n$ dans $[F_k(S)]$ telles que $X' = g_n^* \circ \cdots \circ g_1^*(X)$.*

La proposition suivante est importante car elle montre que l'accélération de composées réduites est exacte vis à vis de l'ensemble des états accessibles.

**Proposition 9.62**
*Soit $S$ un système à compteurs affine décoré et $X$ une partie de $\mathbb{Z}^m$. Pour toute partie $X'$ calculable par accélérations ou par accélérations réduites à partie de $X$, on a :*

$$X' \subseteq \mathrm{Post}_S^*(X)$$

*Démonstration :*

Il suffit de prouver que l'accélération de toute fonction de $[F_k(S)]$ est une relation incluse dans la relation d'accessibilité $\mathcal{R}_S^*$. Considérons une fonction $(g, M, v) \in [F_k(S)]$ et un couple $(x, x')$ tels que $x' \in g^*(\{x\})$ et montrons que $(x, x') \in \mathcal{R}_S^*$. Il existe $i \geqslant 0$ tel que $x' = g^i(x)$. Considérons la suite $(x_n)_{0\leqslant n\leqslant i}$ définie par la récurrence $x_0 = x$ et $x_{n+1} = g(x_n)$. Par définition du réduit, comme pour tout $n \in \{0, \dots, i-1\}$, on a $x_n \in D_g$, il existe une fonction affine $(f_n, M, v) \in F_k(S)$ telle que $x_n \in D_{f_n}$. Ainsi, on a $x' = f_{i-1} \circ \cdots f_0(x)$. On a donc prouvé que $(x, x') \in \mathcal{R}_S^*$. □

**Proposition 9.63**
*Soit $S$ un système à compteurs affine décoré et $X$ une partie de $\mathbb{Z}^m$. Si la partie $\mathrm{Post}_S^*(X)$ est calculable par $n$ accélérations de longueur $k$, alors elle est aussi calculable par $n$ accélérations réduites de longueur $k$.*

*Démonstration :*

Il suffit de prouver que l'accélération de toute fonction de $F_k(S)$ est une relation incluse dans l'accélération d'une fonction de $[F_k(S)]$. Considérons alors une fonction $(f, M, v) \in F_k(S)$. Remarquons que si $D_f = \emptyset$ alors l'accélération de cette fonction est la relation identité qui est incluse dans l'accélération de la fonction $(\mathrm{id}_{\mathbb{Z}^m}, I, 0) \in [F_k(S)]$. On peut donc supposer que $D_f \neq \emptyset$. Par définition du réduit, il existe alors une fonction affine $(g, M, v) \in [F_k(S)]$ telle que $D_f \subseteq D_g$. L'accélération de $f$ est dans ce cas une relation incluse dans l'accélération de $g$. □

On obtient ainsi le corollaire suivant :

**Corollaire 9.64**
*Soit $S$ un système à compteur effectif à monoïde fini et $X$ une partie représentée par un UBA. Si $\mathrm{Post}_S^*(X)$ est calculable par accélération réduite, alors on peut construire effectivement l'UBA $\mathcal{A}(\mathrm{Post}_S^*(X))$.*

*Démonstration :*

Pour une suite finie $s = g_1, \dots g_n$ de fonctions affines de $\bigcup_{k\geqslant 0}[F_k(S)]$, on note $X_s = g_n^* \circ \dots \circ g_1^*(X)$. D'après la proposition 9.62, on a $X_s \subseteq \mathrm{Post}_S^*(X)$. Le théorème 9.60 montre que l'UBA $\mathcal{A}(X_s)$ est effectivement calculable.

Montrons que l'on peut effectivement décider si $X_s = \mathrm{Post}_S^*(X)$. Comme $X \subseteq X_s \subseteq \mathrm{Post}_S^*(X)$, on a l'égalité $X_s = \mathrm{Post}_S^*(X)$ si et seulement si $f_a(X_s) \subseteq X_s$ pour tout $a \in \Sigma$. Ainsi, on peut décider l'égalité $X_s = \mathrm{Post}_S^*(X)$ en construisant les UBA $\mathcal{A}(f_a(X_s))$.

Si $\mathrm{Post}_S^*(X)$ est calculable par accélération réduite, un algorithme qui énumère toutes les suites finies de $\bigcup_{k\geqslant 0}[F_k(S)]$ termine et calcule bien l'UBA $\mathcal{A}(\mathrm{Post}_S^*(X))$. □

## 9.5 Cas où l'accélération suffit à calculer la relation d'accessibilité

On s'intéresse à une classe de systèmes à compteurs à monoïde fini pour lesquels l'accélération suffit pour calculer la relation d'accessibilité.

**Théorème 9.65**
*Soit $S$ un système à compteurs à monoïde fini dont les domaines de définition sont égaux à tous $\mathbb{Z}^m$. Il existe $n$ composées d'actions $f_1$, ..., $f_n$ dans $F_{\mathrm{card}(\mathcal{M}_S)}(S)$ telles que $x\mathcal{R}_S^* x'$ si et seulement si :*

$$x' \in f_n^* \circ \dots \circ f_1^*(\{x\})$$

*De plus, on peut supposer que $n$ est majoré par :*

$$n \leqslant 3.(\mathrm{card}(\mathcal{M}_S).\mathrm{card}(\Sigma)^2)^{1+\mathrm{card}(\mathcal{M}_S)}$$

*Démonstration :*

Commençons par prouver que $M_a$ et $v_a$ sont à coefficient dans $\mathbb{Z}$. De $0 \in D_a = \mathbb{Z}^m$, on déduit $v_a = f_a(0) \in \mathbb{Z}^m$. De même, pour tout $i \in \{1, \dots, m\}$, on a $e_i \in D_a = \mathbb{Z}^m$. Ainsi $M_a.e_i = f_a(e_i) - f_a(0) \in \mathbb{Z}^m$. Pour chaque composition d'actions $\sigma \in \Sigma^*$, on considère la relation affine $\mathcal{R}_\sigma$ définie par $\mathcal{R}_\sigma = \{(x, M_\sigma.x + v_\sigma);\ x \in \mathbb{Q}^m\}$.

Comme l'ensemble des mots $\Sigma^{\leqslant \mathrm{card}(\mathcal{M}_S)}$ est fini, on peut indexer cet ensemble $\Sigma^{\leqslant \mathrm{card}(\mathcal{M}_S)} = \{w_i;\ 1 \leqslant i \leqslant c\}$ où $c = \mathrm{card}(\Sigma^{\leqslant \mathrm{card}(\mathcal{M}_S)})\}$. Considérons la relation $\mathcal{R} = \mathcal{R}_{w_1}^* \cdots \mathcal{R}_{w_c}^*$.

Posons $n_0 = 1 + 2.(\mathrm{card}(\mathcal{M}_S).\mathrm{card}(\Sigma))^{1+\mathrm{card}(\mathcal{M}_S)}$.

Montrons que $\bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma = \mathcal{R}^{n_0}$. D'après la proposition 8.49, pour tout mot $\sigma \in \Sigma^*$, il existe une suite $\sigma_1$, ..., $\sigma_{n'}$ de $\Sigma^{\leqslant \mathrm{card}(\mathcal{M}_S)}$ telle que $n' \leqslant n_0$ et $\mathcal{R}_\sigma \subseteq \mathcal{R}_{\sigma_1}^* \cdots \mathcal{R}_{\sigma_{n'}}^*$. Par construction de $\mathcal{R}$, pour tout $i \in \{1, \ldots, n'\}$, on a $\mathcal{R}_{\sigma_i}^* \subseteq \mathcal{R}$. On a donc $\bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma \subseteq \mathcal{R}^{n_0}$. Comme de plus $\mathcal{R}_{w_i} \subseteq \bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma$ pour tout $i$, par transitivité de $\bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma$, on déduit $\mathcal{R}^{n_0} \subseteq \bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma$.

Remarquons que $\left(\bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma\right) \cap (\mathbb{Z}^m \times \mathbb{Z}^m) = \mathcal{R}_S^*$. Il suffit donc de prouver l'égalité suivante :

$$\mathcal{R}^{n_0} \cap (\mathbb{Z}^m \times \mathbb{Z}^m) = \left( \xrightarrow{w_1^*} \cdots \xrightarrow{w_c^*} \right)^{n_0}$$

Pour tout mot $\sigma \in \Sigma^*$, on a $\mathcal{R}_\sigma \cap (\mathbb{Z}^m \times \mathbb{Z}^m) = \xrightarrow{\sigma}$. Comme de plus $\mathcal{R}_{\sigma\sigma'} = \mathcal{R}_\sigma . \mathcal{R}_{\sigma'}$ et $\xrightarrow{\sigma\sigma'} = \xrightarrow{\sigma} . \xrightarrow{\sigma'}$ pour tout $\sigma, \sigma' \in \Sigma^*$, une récurrence sur $c$ montre que $\mathcal{R}^{n_0} \cap (\mathbb{Z}^m \times \mathbb{Z}^m) = \left( \xrightarrow{w_1^*} \cdots \xrightarrow{w_c^*} \right)^{n_0}$.

Par intersection de l'égalité $\bigcup_{\sigma \in \Sigma^*} \mathcal{R}_\sigma = \mathcal{R}^{n_0}$ avec $\mathbb{Z}^m \times \mathbb{Z}^m$, on déduit le théorème avec $n = c.n_0$ □

**Remarque 9.66**
*Comme $\mathbb{Z}^m$ est Presburger-définissable, on déduit du théorème précédent et du théorème 9.60 que la relation d'accessibilité d'un système à compteurs à monoïde fini dont les domaines de définition sont égaux à $\mathbb{Z}^m$, est effectivement Presburger-définissable.*

**Remarque 9.67**
*On peut décider si la relation d'accessibilité d'un VASS est Presburger-définissable ([Lam94]). La question naturelle est de savoir si pour un tel réseau de Petri, l'accélération suffit à calculer la relation d'accessibilité.*

**Problème ouvert 9.68**
*Soit $S$ un réseau de Petri dont la relation d'accessibilité est Presburger-définissable. Peut-on calculer par accélération cette relation ?*

Troisième PARTIE

# FAST : Fast Acceleration of Symbolic Transition systems

CHAPITRE 10

# L'outil Fast

Le "Model-Checking" est une technique utilisée pour vérifier des systèmes critiques, temps réel, embarqués. Il a donné lieu à la réalisation de nombreux outils efficaces tels que Smv [Smv], Spin [Spi] ou Design/CPN [Des] qui analysent des systèmes dont l'ensemble des états accessibles est fini. Mais les systèmes réels sont souvent intrinsèquement infinis car ils utilisent des paramètres ou des structures non bornées.

Fast ([BFLP03]) est un outil qui vérifie automatiquement les systèmes à compteurs à monoïde fini avec des fonctions affines Presburger-définissables. Cet outil calcule principalement l'ensemble des états accessibles à partir d'un ensemble d'états initiaux.

Rappelons que la vérification des problèmes de type "safety" [EFM99] se réduit à l'accessibilité d'un état à partir d'un ensemble d'états initiaux. Comme ce problème n'est pas décidable en général ([DFS98]), aucune garantie de terminaison ne peut-être donnée pour un semi-algorithme calculant l'ensemble des états accessibles. Cependant, le semi-algorithme implémenté dans Fast, utilisant les techniques d'accélération développées dans le chapitre 9, a prouvé son intéret en calculant dans plus de 80% des cas (sur une base de plus de 40 systèmes à compteurs), une représentation symbolique de l'ensemble des états accessibles.

L'outil Fast, est disponible librement dans sa version 1.0 à l'adresse [Fas].

## 10.1 Comparaison avec les autres outils

Le tableau 10.1 donne un comparatif des outils d'analyse des systèmes à compteurs à états infini. Remarquons que Fast est le seul outil calculant l'ensemble des états accessibles par des accelérations trouvées automatiquement. C'est en effet sur ce point que Fast se distingue de Lash, en réduisant des composées d'actions qui ne peut-être directement implémenté dans ce dernier (les domaines de définitions des fonctions réduites ne sont alors plus convexes [FL02]).

| | type de variables | gardes | actions | accélération | réduction des composées | Pre* | Post* | calcul exact | représentation symb. |
|---|---|---|---|---|---|---|---|---|---|
| FAST [Fas] | $\mathbb{N}$ | Presburger | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | oui | oui | oui | oui | oui | MONA, UBA [KMS02] |
| LASH [Las] | $\mathbb{Z}$ | polyèdre | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | oui | non | oui | oui | oui | NDD [WB00] |
| | $\mathbb{R}$ | polyèdre | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | oui | non | oui | oui | oui | RVA [BJW01] |
| TREX [Tre] [ABS01] | $\mathbb{Z}$ | $x_i \leqslant x_j + c$ <br> $x_i \leqslant c$ <br> $x_i \geqslant c$ | $x_i = x_j + c$ <br> $x_i = c$ | oui | non | oui | oui | oui | PDBM [AAB00] |
| | $\mathbb{R}$ | | $x_i = x_j$ <br> $x_i = 0$ | oui | non | oui | oui | non | PDBM |
| BRAIN [Bra] | $\mathbb{N}$ | $x_i \leqslant x_j + c$ | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | non | non | oui | non | oui | base & période [GS66] [Huy85] [Reu89] |
| BABYLON [Bab] [DRV01] | $\mathbb{N}$ | $x_i \leqslant x_j + c$ | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | non | non | oui | non | non | CST [DRB02] |
| HYTECH [Hyt] | $\mathbb{R}$ | polyèdre | $\overrightarrow{x} = M.\overrightarrow{x} + \overrightarrow{v}$ | non | non | oui | oui | non | polyèdre |
| CSL-ALV [Alv] | $\mathbb{Z}$ | Presburger | Presburger | non | non | oui | oui | oui | NDD, BDD OMEGA,MONA [Ome] [Bry92] |

TAB. 10.1 – Tableau comparatif de différents outils de calcul d'ensemble d'états accessibles

## 10.2 Architecture

FAST prend en entrée un fichier contenant une description du système à compteurs à analyser, et une stratégie permettant à l'utilisateur d'avoir "un contrôle" de ce que FAST doit calculer. On peut ainsi demander un calcul automatique de l'ensemble des états accessibles, ou réaliser des constructions plus avancées pour analyser incrémentalement des systèmes en les décomposant en plusieurs sous-systèmes plus simples à analyser. Cette dernière méthode a été utilisée avec succès pour vérifier le protocole TTP (section 10.3).

FAST est constitué de 7400 lignes de codes C++. Les ensembles Presburger-définissables calculés par FAST sont représentés en interne par des UBA minimaux pour la base de décomposition $r = 2$. On utilise la bibliotheque MONA [KMS02] [Mon] pour manipuler les UBA (intersection, complémentaire, quantification et minimisation). Les espaces affines calculés par FAST sont représentés par la technique développée au chapitre 3. On utilise les bibliotheques GMP [Gmp] et LiDIA [Lid] pour manipuler des matrices d'entiers non bornés. Enfin, on utilise la bibliotheque GTL[Gtl] pour représenter les couvertures affines et semi-affines d'UBA.

## 10.3 Études de cas

Le tableau 10.2 montre les résultats obtenus avec FAST sur un large spectre de systèmes à compteurs, allant du réseau de Petri à l'abstraction de programmmes "multi-threaded" JAVA provenant en grande partie de [Del]. Pour 9 des systèmes à compteurs, on n'a pu calculer une représentation de l'ensemble des états accessible. On peut expliquer cette difficulté par deux raisons. D'une part, on atteint les limites de la représentation symbolique par UBA lorsque le nombre de compteurs devient trop grand, et d'autre part, on atteint les limites de la réduction lorsque le nombre de transitions est trop important.

Dans les sous-sections suivantes, on étudie précisément deux systèmes à compteurs : le "Swimming Pool" et le "Moesi". Le premier est intéressant car on doit accelérer des composées d'actions de longeur 4 pour calculer l'ensemble des états accessibles. On a choisit d'étudier le "Moesi", car un calcul d'enveloppe semi-affine étoile permet de vérifier ce protocole. Enfin, pour ces deux systèmes, FAST calcule automatiquement une formule de Presburger définissant l'ensemble des états accessibles à partir d'un UBA le représentant.

### 10.3.1 Swimming Pool

On considère le système à compteurs "Swimming Pool" $S_{sp}$ ([FO97b], [FO97a]) défini à la figure 10.1. C'est un réseau de Petri utilisant 9 compteurs dont 2 paramètres (un paramètre est un compteur dont la valeur n'est pas modifiée par les transitions), notées $x_1$, ..., $x_7$, $p_1$, $p_2$. L'ensemble des états initiaux $X_0$ du Swimming Pool est la partie de $\mathbb{N}^9$ définie par la formule de Presburger suivante :

$$(x_1 = 0) \wedge (x2 = 0) \wedge (x3 = 0) \wedge (x4 = 0) \wedge (x5 = 0) \wedge (x6 = p1) \wedge (x7 = p2)$$

On cherche a savoir si quelque soit la valeur des paramètres $p_1$ et $p_2$, le système peut rentrer dans un état bloquant. Rappelons que l'ensemble des états bloquants $X_b(S)$ d'un système $S$ est défini par :

$$X_b(S) = \{x \in E;\ \forall a \in \Sigma\ \forall x' \in E\ \ (x, x') \not\in \xrightarrow{a}\}$$

Dans le cas de $S_{sp}$, l'ensemble des états bloquants est donc défini par la formule de Presburger suivante :

$$(x_6 = 0) \wedge ((x_1 = 0) \vee (x_7 = 0)) \wedge (x_2 = 0) \wedge (x_4 = 0) \wedge (x_5 = 0)$$

La propriété $(P)$ à vérifier est donc :

$$(P) : \forall q_1, q_2\ \ \mathrm{Post}^*_{S_{sp}}(X_0 \cap \{p_1 = q_1 \wedge p_2 = q_2\}) \cap X_b \neq \emptyset$$

Dans la sous-section 10.3.1.1, on calcule l'enveloppe affine étoile de $S_{sp}$ avec FAST. Cette enveloppe ne suffira pas a prouver ou infirmer la propriété (P). Dans la sous-section 10.3.1.2, on montre que FAST calcule par acceleration un UBA représentant l'ensemble des états accessibles $\mathrm{Post}^*_{S_{sp}}(X_0)$. De cet UBA on déduit automatiquement que la propriété (P) est vraie. Enfin, dans la sous-section 10.3.1.3, on prouve que l'ensemble des états accessibles est non-quantifié et on calcule avec FAST une formule de Presburger non-quantifiée définissant cet ensemble.

TAB. 10.2 – Résulats obtenu avec FAST sur un processeur Intel Pentium 933 Mhz avec 512Mo

| Étude de cas | variables | transitions | time (s) | memory (MB) | n. of states | n. of accelerations | cycle length | n. of cycles |
|---|---|---|---|---|---|---|---|---|
| *Réseaux de Petri bornés* | | | | | | | | |
| Producer/Consumer | 5 | 3 | 0.41 | 2.37 | 7 | 3 | 1 | 3 |
| Lamport ME | 11 | 9 | 2.70 | 2.88 | 5 | 11 | 1 | 9 |
| Dekker ME | 22 | 22 | 21.72 | 5.48 | 5 | 36 | 1 | 22 |
| RTP | 9 | 12 | 2.24 | 2.76 | 5 | 8 | 1 | 12 |
| Peterson ME | 14 | 12 | 4.97 | 3.78 | 5 | 12 | 1 | 12 |
| Reader/Writer | 13 | 9 | 9.68 | 23.14 | 9 | 23 | 1 | 9 |
| *Réseaux de Petri* | | | | | | | | |
| CSM | 13 | 13 | 45.57 | 6.31 | 6 | 32 | 2 | 35 |
| FMS | 22 | 20 | 157.48 | 8.02 | 21 | 23 | 2 | 46 |
| Multipoll | 17 | 20 | 22.96 | 5.13 | 35 | 13 | 1 | 20 |
| Kanban | 16 | 16 | 10.43 | 6.54 | 4 | 2 | 1 | 16 |
| Mesh2x2 | 32 | 32 | $\geqslant$ 1800 | - | - | - | - | - |
| Mesh3x2 | 52 | 54 | $\geqslant$ 1800 | - | - | - | - | - |
| Manufacturing system | 7 | 6 | $\geqslant$ 1800 | - | - | - | - | - |
| Manufacturing system (check deadlock freedom) | 13 | 6 | $\geqslant$ 1800 | - | - | - | - | - |
| PNCSA | 31 | 38 | $\geqslant$ 1800 | - | - | - | - | - |
| extended ReaderWriter | 24 | 22 | $\geqslant$ 1800 | - | - | - | - | - |
| SWIMMING POOL | 9 | 6 | 111 | 29.06 | 30 | 9 | 4 | 47 |
| *Réseau de Petri Reset/Transfert* | | | | | | | | |
| Last-in First-served | 17 | 10 | 1.89 | 2.74 | 9 | 12 | 1 | 10 |
| Esparza-Finkel-Mayr | 6 | 5 | 0.79 | 2.55 | 5 | 2 | 1 | 5 |
| *Protocoles Broadcasts* | | | | | | | | |
| Inc/Dec | 32 | 28 | $\geqslant$ 1800 | - | - | - | - | - |
| Producer/Consumer with Java threads - 2 | 18 | 14 | 13.27 | 3.81 | 13 | 53 | 1 | 14 |
| Producer/Consumer with Java threads - N | 18 | 14 | 723.27 | 12.46 | 58 | 86 | 2 | 75 |
| 2-Producer/2-Consumer with Java threads *2 types of producers and 2 types of consumers* | 44 | 38 | $\geqslant$ 1800 | - | - | - | - | - |
| Central Server system | 13 | 8 | 20.82 | 6.83 | 5 | 11 | 2 | 25 |
| Consistency Protocol | 12 | 8 | 275 | 7.35 | 7 | 9 | 3 | 98 |
| M.E.S.I. Cache Coherence Protocol | 4 | 4 | 0.42 | 2.44 | 6 | 3 | 1 | 4 |
| M.O.E.S.I. Cache Coherence Protocol | 4 | 5 | 0.56 | 2.49 | 7 | 3 | 1 | 5 |
| Synapse Cache Coherence Protocol | 3 | 3 | 0.30 | 2.23 | 6 | 2 | 1 | 3 |
| Illinois Cache Coherence Protocol | 4 | 6 | 0.97 | 2.64 | 6 | 4 | 1 | 6 |
| Berkeley Cache Coherence Protocol | 4 | 3 | 0.49 | 2.75 | 7 | 2 | 1 | 3 |
| Firefly Cache Coherence Protocol | 4 | 8 | 0.86 | 2.59 | 7 | 3 | 1 | 8 |
| Dragon Cache Coherence Protocol | 5 | 8 | 1.42 | 2.72 | 6 | 5 | 1 | 8 |
| Futurebus+ Cache Coherence Protocol | 9 | 10 | 2.19 | 3.38 | 12 | 8 | 1 | 10 |
| *Autres* | | | | | | | | |
| lift controller - N | 4 | 5 | 4.56 | 2.90 | 14 | 4 | 3 | 20 |
| bakery | 8 | 20 | $\geqslant$ 1800 | - | - | - | - | - |
| barber m4 | 8 | 12 | 1.92 | 2.68 | 5 | 8 | 1 | 12 |
| ticket 2i | 6 | 6 | 0.88 | 2.54 | 22 | 5 | 1 | 6 |
| ticket 3i | 8 | 9 | 3.77 | 3.08 | 77 | 10 | 1 | 9 |
| TTP | 10 | 17 | 1186.24 | 73.24 | 1140 | 31 | 1 | 17 |
| TTP (ad hoc strategy) | 10 | 17 | 246.67 | 72.87 | 1140 | 16 | 1 | 17 |

**Figure 10.1** Le “Swimming Pool” $S_{sp}$

**Var** $= x_1, x_2, x_3, x_4, x_5, x_6, x_7, p_1, p_2$

$$\begin{cases} t_1 : \begin{cases} x'_1 = x_1 + 1 \\ x'_6 = x'_6 - 1 \end{cases} & \text{si } (x_6 \geqslant 1) \\ t_2 : \begin{cases} x'_2 = x_2 + 1 \\ x'_1 = x_1 - 1 \\ x'_7 = x_7 - 1 \end{cases} & \text{si } (x_1 \geqslant 1) \wedge (x_7 \geqslant 1) \\ t_3 : \begin{cases} x'_6 = x_6 + 1 \\ x'_3 = x_3 + 1 \\ x'_2 = x_2 - 1 \end{cases} & \text{si } (x_2 \geqslant 1) \\ t_4 : \begin{cases} x'_4 = x_4 + 1 \\ x'_3 = x_3 - 1, \\ x'_6 = x_6 - 1 \end{cases} & \text{si } (x_3 \geqslant 1) \wedge (x_6 \geqslant 1) \\ t_5 : \begin{cases} x'_5 = x_5 + 1 \\ x'_7 = x_7 + 1 \\ x'_4 = x_4 - 1 \end{cases} & \text{si } (x_4 \geqslant 1) \\ t_6 : \begin{cases} x'_6 = x_6 + 1 \\ x'_5 = x_5 - 1 \end{cases} & \text{si } (x_5 \geqslant 1) \end{cases}$$

#### 10.3.1.1 Par enveloppe étoile

Comme $S_{sp}$ est un réseau de Petri, la proposition 8.11 montre que l'enveloppe affine étoile et l'enveloppe semi-affine étoile coïncident. En utilisant l'outil Fast, pour calculer ces relations, on trouve bien deux fois la même définie par :

$$\begin{array}{l} (p'_1 = p_1) \wedge \\ (p'_2 = p_2) \wedge \\ (x'_2 + x'_3 + x'_4 + x'_7 = x_2 + x_3 + x_4 + x_7) \wedge \\ (x'_1 + x'_2 + x'_4 + x'_5 + x'_6 = x_1 + x_2 + x_4 + x_5 + x_6) \end{array}$$

De cette relation affine, on déduit que l'ensemble des états accessibles $\mathrm{Post}^*_{S_{sp}}(X_0)$ est inclus dans la partie de $X' \subseteq \mathbb{N}^9$ définie par la formule de Presburger suivante :

$$(x_1 + x_2 + x_4 + x_5 + x_6 = p_1) \wedge (x_2 + x_3 + x_4 + x_7 = p_2)$$

Remarquons que pour tout $(p_1, p_2) \in \mathbb{N}^2$, le couple $(p_1, 0, p_2, 0, 0, 0, 0, p_1, p_2) \in X' \cap X_b$. Il est donc possible que quelque soit la valeur des paramètres, le système puisse atteindre un état bloquant. La sur-approximation $X'$ de $\mathrm{Post}^*_{S_{sp}}(X_0)$ ne permet donc pas de valider ou d'infirmer la propriété $(P)$.

#### 10.3.1.2 Par accélération

Fast parvient à calculer en moins d'une minute l'ensemble des états accessibles $\mathrm{Post}^*_{S_{sp}}(X_0)$ en utilisant des composées réduites d'actions de longueur 4. Comme le calcul diverge pour

**Figure 10.2** Effet de la réduction pour le “Swimming pool”

| $k$ | card($\|\Sigma\|^{\leqslant k}$) | card($F_k(S_{sp})$) | card($[F_k(S_{sp})]$) | card($[R_k(S_{sp})]$) |
|---|---|---|---|---|
| 1 | 7 | 7 | 7 | 7 |
| 2 | 43 | 36 | 21 | 16 |
| 3 | 259 | 156 | 56 | 28 |
| 4 | 1555 | 578 | 126 | 47 |
| 5 | 9331 | 1890 | 252 | 86 |

des composées de longueur 3, il semble que cette longueur soit nécessaire pour obtenir l'ensemble des états accessibles.

**Remarque 10.1**
*Rappelons que cette longueur 4 de cycles a aussi été observée dans [FO97b]. Par une méthode différente, utilisant la “semi-commutation” des transitions, il a été prouvé que la relation d'accessibilité de $S_{sp}$ est égale à $t_1^*(t_2t_3t_1)^*(t_2t_3)^*t_4^*t_5^*(t_2t_3)^*(t_4t_5t_2t_3)^*(t_4t_5)^*t_1^*t_4^*$.*

Le tableau donné à la figure 10.2, représente l'effet de la réduction pour le “Swimming pool”. Il contient une colonne card($[R_k(S_{sp})]$) qui correspond à une réduction non documentée dans cette thèse qui consiste à ne pas considérer des composées $f \circ g$ de fonctions affines si $f$ et $g$ commutent. En effet, dans ce cas $(f \circ g)^*$ est égale à $f^* \circ g^*$. Remarquons que le cardinal de $[R_4(S)]$ est 12 fois plus petit que celui de $F_4(S)$.

On parvient ainsi avec FAST à prouver automatiquement la propriété $(P)$ en calculant l'UBA $\mathcal{A}(\mathrm{Post}^*_{S_{sp}}(X_0))$. En effet, pour vérifier la propriété, il suffit de calculer l'UBA $\mathcal{A}(Y)$ où $Y$ est donné par :

$$Y = \{(q_1, q_2) \in \mathbb{N}^; \exists (x_1, \ldots x_7) \in \mathbb{N}^7;\ \mathrm{Post}^*_{S_{sp}}(X_0) \cap X_b \neq \emptyset\}$$

Et de vérifier que $\mathcal{L}(\mathcal{A}(Y)) = \Sigma_r^*$.

#### 10.3.1.3 Synthèse de formules

En utilisant FAST, en plus de pouvoir calculer l'UBA de l'ensemble des états accessibles, on peut demander le calcul d'une formule de Presburger dans la logique des non-quantifiés représentant cet ensemble (théorème 5.40). Les semi-affines $S_i = \mathrm{saff}(\delta^i(\mathrm{Post}^*_{S_{sp}}(X_0)))$ sont alors donnés par :

$$\begin{array}{ll}
S_0 & =\{(x_1+x_2+x_4+x_5+x_6=p_1)\wedge(x_2+x_3+x_4+x_7=p_2)\} \\
\hline
 & \quad\{(x_1=0)\wedge(x_2=0)\wedge(x_3+x_7=p_2)\wedge(x_4=0)\wedge(x_5=0)\wedge(x_6=0)\wedge(p_1=0)\} \\
S_1 & =\cup\{(x_1+x_5+x_6=p_1)\wedge(x_2=0)\wedge(x_3=0)\wedge(x_4=0)\wedge(x_7=0)\wedge(p_2=0)\} \\
 & \quad\cup\{(x_1=0)\wedge(x_2=0)\wedge(x_3=p_2)\wedge(x_4=0)\wedge(x_5=p_1)\wedge(x_6=0)\wedge(x_7=0)\} \\
\hline
S_2 & =\emptyset
\end{array}$$

**Figure 10.3** Le "Moesi" $S_{moesi}$

$$
\textbf{Var} = m, o, e, s, i
$$

$$
\begin{cases}
t_1 : \begin{cases} s' = s + e + 1 \\ o' = o + m \\ e' = 0 \\ m' = 0 \\ i' = i - 1 \end{cases} & \text{si } (i \geqslant 1) \\
t_2 : \begin{cases} m' = m + 1 \\ e' = e - 1 \end{cases} & \text{si } (e \geqslant 1) \\
t_3 : \begin{cases} i' = i + m + e + s + o - 1 \\ m' = 0 \\ e' = 1 \\ s' = 0 \\ o' = 0 \end{cases} & \text{si } (s + o \geqslant 1) \vee (i \geqslant 1)
\end{cases}
$$

Cela prouve que l'ensemble des états accessibles $\text{Post}^*_{S_{sp}}(X_0)$ est non-quantifié et défini par la formule de Presburger non-quantifiée suivante :

$$
\begin{array}{l}
[(x_1 + x_2 + x_4 + x_5 + x_6 = p_1) \wedge (x_2 + x_3 + x_4 + x_7 = p_2)] \wedge \\
\neg \left[ \begin{array}{l}
((x_1 = 0) \wedge (x_2 = 0) \wedge (x_3 + x_7 = p_2) \wedge (x_4 = 0) \wedge (x_5 = 0) \wedge (x_6 = 0) \wedge (p_1 = 0)) \vee \\
((x_1 + x_5 + x_6 = p_1) \wedge (x_2 = 0) \wedge (x_3 = 0) \wedge (x_4 = 0) \wedge (x_7 = 0) \wedge (p_2 = 0)) \vee \\
((x_1 = 0) \wedge (x_2 = 0) \wedge (x_3 = p_2) \wedge (x_4 = 0) \wedge (x_5 = p_1) \wedge (x_6 = 0) \wedge (x_7 = 0))
\end{array} \right]
\end{array}
$$

### 10.3.2 Moesi

On étudie le protocole de cohérence de mémoire cache, le "Moesi" $S_{moesi}$ [Del00a] [Del01] représenté à la figure 10.3. C'est un système broadcast utilisant 5 compteurs : $m$, $o$, $e$, $s$, $i$. L'ensemble des états initiaux $X_0$ de ce système est défini par la formule de Presburger suivante :

$$
(m = 0) \wedge (o = 0) \wedge (e = 0) \wedge (s = 0) \wedge (i \geqslant 1)
$$

On souhaite prouver que $e + o$ n'est jamais strictement plus grand que 1. C'est une propriété dite "d'exclusion mutuelle". Notons $X_{bad}$ l'ensemble des mauvais états $X_{bad} = \{(m, o, e, s, i) \in \mathbb{N}^5;\ e + o \geqslant 1\}$. On doit prouver la propriété suivante :

$$
\text{Post}^*_{S_{moesi}}(X_0) \cap X_{bad} = \emptyset
$$

Dans les sous-sections 10.3.2.1, 10.3.2.2 et 10.3.2.3, on montrera comment vérifier la propriété (P) par trois méthodes différentes utilisant respectivement un point fixe de la suite $\text{Pre}^{\leqslant k}_{S_{moesi}}(X_{bad})$, un calcul de $\text{Post}^*_{S_{moesi}}(X_0)$ par accélération, et une sur-approximation de la relation d'accessibilité de $S_{moesi}$ par un calcul d'enveloppe semi-affine étoile.

#### 10.3.2.1 Par un calcul de $\mathrm{Pre}_S^{\leqslant k}(X_{bad})$

Comme les fonctions affines $f_a$ sont définies sur des clos par le haut et que $X_{bad}$ est un clos par le haut, le théorème 7.25 prouve qu'il existe un entier $k \geqslant 0$ tel que $\mathrm{Pre}_S^{\leqslant k}(X_{bad}) = \mathrm{Pre}_S^*(X_{bad})$. En calculant avec Fast cet ensemble on prouve automatiquement que $\mathrm{Pre}_{S_{moesi}}^*(X_{bad}) \cap X_0 = \emptyset$. Comme cette dernière propriété est équivalente à (P), on vérifie ainsi automatiquement la propriété (P). Remarquons que l'on n'a pas calculé l'ensemble des états accessibles $\mathrm{Post}_{S_{moesi}}^*(X_0)$. Ainsi, pour vérifier une autre propriété (P'), il faudra à nouveau faire un calcul d'états accessibles.

#### 10.3.2.2 Par accélération

En accélérant les transitions du système $S_{moesi}$, l'outil Fast calcule l'UBA $\mathcal{A}(\mathrm{Post}_{S_{moesi}}^*(X_0))$ en quelques secondes. En prenant l'intersection de l'ensemble $\mathrm{Post}_{S_{moesi}}^*(X_0)$ avec $X_{bad}$ on prouve automatiquement la propriété (P). En utilisant la synthèse de formule implémentée dans Fast, on déduit automatiquement de l'UBA représentant l'ensemble des états accessibles, la formule de Presburger non quantifiée suivante :

$$
\begin{array}{rl}
& \left[\begin{array}{l}
((m=0)\wedge(o=0)\wedge(e=0))\vee\\
((m=0)\wedge(o=1)\wedge(e=0))\vee\\
((m=0)\wedge(o=0)\wedge(e=1))\vee\\
((m=1)\wedge(o=0)\wedge(e=0))
\end{array}\right]\wedge\\
\neg & \left[\begin{array}{l}
((m=0)\wedge(o=0)\wedge(e=0)\wedge(s=0)\wedge(i=0))\vee\\
((m=0)\wedge(o=1)\wedge(e=0)\wedge(s=0))
\end{array}\right]
\end{array}
$$

Remarquons que la formule précédente est "humainenement" plus facile à comprendre que l'UBA $\mathcal{A}(\mathrm{Post}_{S_{moesi}}^*(X_0))$ à 25 états calculé par Fast.

#### 10.3.2.3 Par enveloppe semi-affine étoile

Remarquons que (P) est vraie si et seulement si la relation $(X_0 \times X_{bad}) \cap \mathcal{R}_{S_{moesi}}^*$ est vide où $\mathcal{R}_{S_{moesi}} = \bigcup_{a\in\Sigma} \to_a$ est la relation d'accessibilité en une étape du Moesi. Ainsi, en calculant une sur-approximation $\mathcal{R}$ de $\mathcal{R}_{S_{moesi}}^*$ telle que $(X_0 \times X_{bad}) \cap \mathcal{R} = \emptyset$, on peut prouver la propriété (P). On va montrer que l'enveloppe semi-affine étoile est suffisamment précise pour déduire (P) alors que l'enveloppe affine étoile est trop large.

Fast calcule l'enveloppe semi-affine étoile $\mathrm{saff}^*(\mathcal{R}_{S_{moesi}})$ de la relation d'accessibilité en une étape $\mathcal{R}_{S_{moesi}} = \bigcup_{a\in\Sigma} \to_a$, et produit la relation semi-affine suivante :

$$
\begin{array}{l}
((m'+e'=0)\wedge(s'+i'+o'=m+e+s+i+o))\vee\\
((m'=m)\wedge(e'=e)\wedge(s'=s)\wedge(i'=i)\wedge(o'=o))\vee\\
((m'+e'=m+e)\wedge(s'=s)\wedge(i'=i)\wedge(o'=o))\vee\\
((m'+e'=1)\wedge(s'=0)\wedge(m+o+e+s+i=i'+1)\wedge(o'=0))
\end{array}
$$

En remarquant (ou en calculant l'UBA associé) que la relation $(X_0 \times X_{bad}) \cap \mathrm{saff}^*(\mathcal{R}_{S_{moesi}}) = \emptyset$, on déduit que la propriété (P) est vraie. Cependant, on ne peut pas faire de même avec l'enveloppe affine étoile. En effet, Fast calcule l'enveloppe affine étoile $\mathrm{aff}^*(\mathcal{R}_{S_{moesi}})$ et renvoie la relation affine suivante :

$$(m'+o+e'+s'+i' = m+o+e+s+i)$$

La relation $(X_0 \times X_{bad}) \cap \mathrm{aff}^*(\mathcal{R}_{S_{moesi}})$ n'est alors pas vide.

CHAPITRE 11

# Conclusions et perspectives

Nous avons défini une nouvelle *représentation symbolique* par automates, les UBA. Son expressivité a été comparée à celle des NDD, une autre représentation symbolique par automate, et nous avons montré que tout ensemble représenté par un NDD pouvait être représenté par un UBA *plus concis*. Sa structure a été étudiée et nous avons montré que l'UBA minimal représentant un sous-ensemble $X$ est donné par des images réciproques de $X$ par des fonctions affines. De cette *caractérisation algébrique* nous avons développé des algorithmes pour calculer des *sur-approximations* d'ensembles représentés par UBA. Un algorithme calculant *l'enveloppe affine* et *l'enveloppe semi-affine* d'un UBA en temps respectivement polynomial et exponentiel a ainsi pu être implémenté.

Ces approximations ont été utilisées pour faire *la synthèse d'une formule de Presburger* à partir d'un UBA. En utilisant l'enveloppe semi-affine d'un UBA, nous avons montré qu'en temps exponentiel, on peut décider si un UBA décrit un ensemble définissable par une formule de Presburger non-quantifiée, et nous avons montré comment calculer une telle formule.

Nous avons aussi utilisé l'approximation d'un UBA pour généraliser la notion *d'invariants de place*, définis pour les réseaux de Petri. Pour cela, la notion *d'enveloppe affine étoile* et *d'enveloppe semi-affine étoile* a été introduite. Alors que ces deux enveloppes coïncident pour les réseaux de Petri, nous avons montré que dans le cas général des systèmes à compteurs, l'enveloppe semi-affine étoile est plus précise. Un algorithme polynomial de calcul de l'enveloppe affine étoile d'un système à compteurs et un semi-algorithme de calcul de l'enveloppe semi-affine étoile a été implémenté.

Nous avons étudié la *structure des UBA* représentant $\mathrm{Pre}_S^{\leqslant k}(X')$ en fonction de $k$. Bien que de taille asymptotiquement exponentielle en $k$, sous une condition globale ou locale sur $S$ et $X'$, nous avons pu établir qu'elle pouvait devenir simplement *polynomiale*. C'est en effet le cas lorsque le système $S$ est *à monoïde fini* (condition globale), ou quand les domaines de définition de $S$ et l'ensemble $X'$ sont définissables dans la logique des intervalles (condition locale).

Nous avons étudié le problème du calcul de l'ensemble des *états accessibles* d'un système à compteurs par des méthodes *d'accélération* (le choix des séquences à accélérer, le calcul de l'accélération). Nous avons complètement automatisé ces deux étapes (la première n'a jamais été automatisée de façon efficace). Pour cela, nous avons *réduit* l'ensemble (*de taille exponentielle*) des composées de $k$ actions à un ensemble (*de taille polynomial*) contenant des fonctions calculables en temps polynomial (en fonction de $k$). En montrant comment accélérer les fonctions de cet ensemble réduit, on a donné une méthode automatique de calcul de l'ensemble d'accessibilité d'un système à compteurs par accélération.

Enfin, nous avons construit *un outil de vérification* de systèmes à compteurs, FAST. Il permet de calculer par accélération des ensembles d'accessibilité, de faire la synthèse d'une formule de Presburger à partir d'un UBA, de calculer des enveloppes affines et semi-affines d'UBA et des enveloppes affines et semi-affines étoiles.

Plusieurs directions de recherche prolongeant cette thèse sont ouvertes.

Une des directions est l'étude de *représentations symboliques concises*, combinant par exemple, plusieurs UBA pour représenter un ensemble. On peut en effet construire des suites finies d'UBA dont l'union est un UBA de taille exponentielle. Pour réduire la taille d'un UBA en le décomposant de la sorte, une *analyse structurelle* de l'ensemble représenté doit être menée.

Une autre direction est l'utilisation de méthodes *d'abstractions* combinées avec des méthodes *d'accélérations*. L'abstraction par prédicat construit à partir d'un système à compteurs, *un système fini*. En utilisant des prédicats dépendant de variables entières, l'abstraction d'un système à compteurs, reste un système à compteurs. L'intérêt est de pouvoir utiliser des *abstractions plus fines*. On pourrait alors calculer l'ensemble d'accessibilité du système abstrait par accélération.

Enfin, une autre direction est l'extension de l'outil FAST, pour pouvoir vérifier des systèmes dont les *variables sont hétérogènes* : compteurs, files, pointeurs, variables réelles. Des représentation symboliques et des techniques d'accélération adaptées restent à trouver.

Résumons les quatres principaux problèmes laissés ouverts dans cette thèse :

- (problème ouvert 9.68) Soit $S$ un réseau de Petri dont la relation d'accessibilité est Presburger-définissable. Peut-on calculer par accélération cette relation ?
- (problème ouvert 8.44) Prouver la terminaison du semi-algorithme 3 calculant l'enveloppe semi-affine étoile d'une relation semi-affine.
- (problème ouvert 5.15) Soit $\mathcal{C}_P$ la classe des automates binaires canoniques représentant des parties définissables dans la logique de Presburger. Pour tout automate $\mathcal{A}$ dans $\mathcal{C}_P$, on note $l(\mathcal{A})$ la taille de la plus petite formule de Presburger dont l'ensemble des solutions est représenté par $\mathcal{A}$. La fonction $l(\mathcal{A})$ est-elle bornée de façon élémentaire en la taille de $\mathcal{A}$ ?
- (problème ouvert 5.39) Trouver la complexité pour décider si un automate binaire non ambigu représente une partie non quantifiée.

D'autres problèmes techniques restent ouverts :

- (problème ouvert 4.64) Caractériser les parties UBA-représentables dont l'étoile est UBA-représentable.

- (problème ouvert 7.27) Soit $S$ un système à compteurs affine dont les domaines de définitions sont clos par le haut et soit $X'$ un clos par le haut. Montrer que l'on ne peut pas borner le plus petit $k \geqslant 0$ tel que $\mathrm{Pre}_S^{\leqslant k}(X') = \mathrm{Pre}_S^*(X')$ par une fonction élémentaire en taille$(S)$ et en taille$(\mathcal{A}(X'))$.
- (problème ouvert 9.22) Peut-on effectivement et efficacement caractériser les fonctions affines $f$ dont l'accélération est Presburger-définissable ?
- (problème ouvert 9.44) Caractériser les parties Presburger-définissables à intersection polynomiale.

# Bibliographie


[AAB00] Aurore Annichini, Eugene Asarin, and Ahmed Bouajjani. Symbolic techniques for parametric reasoning about counter and clock systems. In *Proc. 12th Int. Conf. Computer Aided Verification (CAV'2000), Chicago, IL, USA, July 2000*, volume 1855 of *Lecture Notes in Computer Science*, pages 419–434. Springer, 2000.

[ABJ98] Parosh Aziz Abdulla, Ahmed Bouajjani, and Bengt Jonsson. On-the-fly analysis of systems with unbounded, lossy FIFO channels. In *Proc. 10th Int. Conf. Computer Aided Verification (CAV'98), Vancouver, BC, Canada, June-July 1998*, volume 1427 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 1998.

[ABJN99] Parosh Aziz Abdulla, Ahmed Bouajjani, Bengt Jonsson, and Marcus Nilsson. Handling global conditions in parameterized system verification. In *Proc. 11th Int. Conf. Computer Aided Verification (CAV'99), Trento, Italy, July 1999*, volume 1633, pages 134–145. Springer, 1999.

[ABS01] Aurore Annichini, Ahmed Bouajjani, and Mihaela Sighireanu. TReX : A tool for reachability analysis of complex systems. In *Proc. 13th Int. Conf. Computer Aided Verification (CAV'2001), Paris, France, July 2001*, volume 2102 of *Lecture Notes in Computer Science*, pages 368–372. Springer, 2001.

[ADG+02] Pierluigi Ammirati, Giorgio Delzanno, Pierre Ganty, Gilles Geeraerts, Jean-François Raskin, and Laurent Van Begin. Babylon : An integrated toolkit for the specification and verification of parameterized systems. In Giorgio Delzanno, Sandro Etalle, and Maurizio Gabbrielli, editors, *Specification, Analysis and Validation for Emerging Technologies in Computational Logic*, volume 94 of *Datalogiske Skrifter*, page (unpaginated), July 27 2002.

[AF88] J-M. Arnaudiès and H. Fraysse. *Cours de mathématiques — 1 : Algèbre.* Dunod Université, 1988.

[AFP02] David Avis, Komei Fukuda, and Stefano Picozzi. On canonical representations of convex polyhedra. In *ICMS 2002*, Mathematical Software, pages 350–360. World Scientific, 2002.

[AJ93] Parosh Aziz Abdulla and Bengt Jonsson. Verifying programs with unreliable channels. In *Proc. 8th IEEE Symp. Logic in Computer Science (LICS'93), Montreal, Canada, June 1993*, pages 160–170. IEEE Comp. Soc. Press, 1993.

[AJNd02] Parosh Aziz Abdulla, Bengt Jonsson, Marcus Nilsson, and Julien d'Orso. Regular model checking made simple and efficient. In *Proc. 13th Int. Conf. Concurrency Theory (CONCUR'2002), Brno, Czech Republic, Aug. 2002*, volume 2421 of *Lecture Notes in Computer Science*, pages 116–130. Springer, 2002.

[Alv] ALV homepage. `http://www.cs.ucsb.edu/~bultan/composite/`.

[APSY02] Eugene Asarin, Gordon Pace, Gerardo Schneider, and Sergio Yovine. SPeeDI — A verification tool for polygonal hybrid systems. In *Proc. 14th Int. Conf. Computer Aided Verification (CAV'2002), Copenhagen, Denmark, July 2002*, volume 2404 of *Lecture Notes in Computer Science*, pages 354–358. Springer, 2002.

[ASY01] Eugene Asarin, Gerardo Schneider, and Sergio Yovine. On the decidability of the reachability problem for planar differential inclusions. In *Proc. 4th Int. Workshop Hybrid Systems : Computation and Control (HSCC'2001), Roma, Italy, Mar. 2001*, volume 2034 of *Lecture Notes in Computer Science*, pages 89–104. Springer, 2001.

[Bab] BABYLON homepage. `http://www.ulb.ac.be/di/ssd/lvbegin/CST/-index.html`.

[Bar77] Jon Barwise. An introduction to first-order logic. In Jon Barwise, editor, *Handbook of Mathematical Logic*, pages 5–46. North-Holland, 1977.

[BB02] Constantinos Bartzis and Tevfik Bultan. Efficient symbolic representations for arithmetic constraints in verification. Technical Report ucsb cs :TR-2002-16, University of California, Santa Barbara, Computer Science, 2002.

[BB03] Constantinos Bartziz and Tevfik Bultan. Efficient image computation in infinite state model checking. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV'2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 249–261. Springer, 2003.

[BC96] Alexandre Boudet and Hubert Comon. Diophantine equations, Presburger arithmetic and finite automata. In *Proc. 21st Int. Coll. on Trees in Algebra and Programming (CAAP'96), Linköping, Sweden, Apr. 1996*, volume 1059 of *Lecture Notes in Computer Science*, pages 30–43. Springer, 1996.

[Ber77] Leonard Berman. Precise bounds for Presburger arithmetic and the reals with addition : Preliminary report. In *Proc. 18th IEEE Symp. Foundations of Computer Science (FOCS'77), Providence, RI, USA, Oct.-Nov. 1977*, pages 95–99, Providence, Rhode Island, 31 October–2 November 1977. IEEE.

[BF] Jean-Paul Bodeveix and Mamoun Filali. Experimenting acceleration methods for the validation of infinite state systems. In *Proc. 20th IEEE Int. Conf. in Distributed Computins Systems (IDCS'00), Taipei, ROC, Taiwan, April 2000.*

[BF99] Béatrice Bérard and Laurent Fribourg. Reachability analysis of (timed) Petri nets using real arithmetic. In *Proc. 10th Int. Conf. Concurrency Theory (CONCUR'99), Eindhoven, The Netherlands, Aug. 1999*, volume 1664 of *Lecture Notes in Computer Science*, pages 178–193. Springer, 1999.

[BFLP03] Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci. FAST : Fast Acceleration of Symbolic Transition systems. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV'2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 118–121. Springer, 2003.

[BG02] Achim Blumensath and Erich Grädel. Finite presentations of infinite structures. In *Proc. 2nd Int. Workshop on Complexity in Automated Deduction (CiAD'2002)*, 2002.

[BGP97] Tevfik Bultan, Richard Gerber, and William Pugh. Symbolic model-checking of infinite state systems using Presburger arithmetic. In *Proc. 9th Int. Conf. Computer Aided Verification (CAV'97), Haifa, Israel, June 1997*, volume 1254 of *Lecture Notes in Computer Science*, pages 400–411. Springer, 1997.

[BGP99] Tevfik Bultan, Richard Gerber, and William Pugh. Model-checking concurrent systems with unbounded integer variables : symbolic representations, approximations, and experimental results. *ACM Transactions on Programming Languages and Systems*, 21(4) :747–789, 1999.

[BGWW97] Bernard Boigelot, Patrice Godefroid, Bernard Willems, and Pierre Wolper. The power of QDDs. In *Proc. 4th Int. Symp. Static Analysis, (SAS '97), Paris, France, Sep. 1997*, volume 1302 of *Lecture Notes in Computer Science*, pages 172–186. Springer, 1997.

[BH99] Ahmed Bouajjani and Peter Habermehl. Symbolic reachability analysis of FIFO-channel systems with nonregular sets of configurations. *Theoretical Computer Science*, 221(1–2) :211–250, 1999.

[BHMV94] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and $p$-recognizable sets of integers. *Bull. Belg. Math. Soc.*, 1(2) :191–238, March 1994.

[BJNT00] Ahmed Bouajjani, Bengt Jonsson, Marcus Nilsson, and Tayssir Touili. Regular model checking. In *Proc. 12th Int. Conf. Computer Aided Verification (CAV'2000), Chicago, IL, USA, July 2000*, volume 1855 of *Lecture Notes in Computer Science*, pages 403–418. Springer, 2000.

[BJW01] Bernard Boigelot, Sébastien Jodogne, and Pierre Wolper. On the use of weak automata for deciding linear arithmetic with integer and real variables. In *Proc. 1st Int, Joint Conf. , IJCAR 2001 Siena, Italy, June 18-23, 2001*, volume 2083 of *Lecture Notes in Computer Science*, pages 588–603. Springer, 2001.

[BM99] Ahmed Bouajjani and Richard Mayr. Model checking lossy vector addition systems. 1563 :323–333, 1999.

[BM02] Ahmed Bouajjani and Agathe Merceron. Parametric verification of a group membership algorithm. In *Proc. 7th Int. Symp. Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'2002), Oldenburg, Germany, Sep. 2002*, volume 2469 of *Lecture Notes in Computer Science*, pages 311–330. Springer, 2002.

[Boi] Bernard Boigelot. On iterating linear transformations over recognizable sets of integers. *Theoretical Computer Science*. To appear.

[Boi98] Bernard Boigelot. *Symbolic Methods for Exploring Infinite State Spaces*. PhD thesis, Université de Liège, 1998.

[Bou01] Ahmed Bouajjani. Languages, rewriting systems, and verification of infinite-state systems. In *Proc. 28th Int. Coll. Automata, Languages, and Programming (ICALP'2001), Crete, Greece, July 2001*, volume 2076 of *Lecture Notes in Computer Science*, pages 24–39. Springer, 2001.

[BPR01] Thomas Ball, Andreas Podelski, and Sriram K. Rajamani. Boolean and Cartesian abstraction for model checking C programs. 2031 :268–283, 2001.

[BPR02] Thomas Ball, Andreas Podelski, and Sriram K. Rajamani. Relative completeness of abstraction refinement for software model checking. 2280 :158–172, 2002.

[Bra] Brain homepage. `http://www.cs.man.ac.uk/~voronkov/BRAIN/\-index.html`.

[Bry92] Randal E. Bryant. Symbolic boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, 24(3) :293–318, 1992.

[BW94] Bernard Boigelot and Pierre Wolper. Symbolic verification with periodic sets. In *Proc. 6th Int. Conf. Computer Aided Verification (CAV'94), Stanford, CA, USA, June 1994*, volume 818 of *Lecture Notes in Computer Science*, pages 55–67. Springer, 1994.

[Cia94] Gianfranco Ciardo. Petri nets with marking-dependent arc cardinality : Properties and analysis. In *Proc. 15th Int. Conf. Application and Theory of Petri Nets (ICATPN'94), Zaragoza, Spain, June 1994*, volume 815 of *Lecture Notes in Computer Science*, pages 179–198. Springer, 1994.

[CJ98] Hubert Comon and Yan Jurski. Multiple counters automata, safety analysis, and Presburger arithmetic. In *Proc. 10th Int. Conf. Computer Aided Verification (CAV'98), Vancouver, BC, Canada, June-July 1998*, volume 1427 of *Lecture Notes in Computer Science*, pages 268–279. Springer, 1998.

[CP89] Jean-Marc Champarnaud and Jean-Eric Pin. A maxmin problem on finite automata. *Discrete Applied Mathematics*, 23 :91–96, 1989.

[Del] Home Page – Giorgio Delzanno. `http://www.disi.unige.it/person/DelzannoG/`.

[Del00a] Gorgio Delzanno. Automatic verification of parameterized cache coherence protocols. In *Proc. 12th Int. Conf. Computer Aided Verification (CAV'2000), Chicago, IL, USA, July 2000*, volume 1855 of *Lecture Notes in Computer Science*, pages 53–68. Springer, 2000.

[Del00b] Gorgio Delzanno. Verification of consistency protocols via infinite-state symbolic model checking : A case study. In *Proc. IFIP Joint Int. Conf. Formal Description Techniques & Protocol Specification, Testing, and Verification (FORTE-PSTV'00), Pisa, Italy, Oct. 2000*, volume 183 of *IFIP Conference Proceedings*, pages 171–186. Kluwer Academic, 2000.

[Del01] Giorgio Delzanno. Constraint-based verification of parameterized cache coherence protocols. *Formal Methods in System Design*, 2001. To appear.

[Des] Design/CPN online. `http://www.daimi.au.dk/designCPN`.

[DFS98] Catherine Dufourd, Alain Finkel, and Philippe Schnoebelen. Reset nets between decidability and undecidability. In *Proc. 25th Int. Coll. Automata, Languages, and Programming (ICALP'98), Aalborg, Denmark, July 1998*, volume 1443 of *Lecture Notes in Computer Science*, pages 103–115. Springer, 1998.

[Dil90] David L. Dill. Timing assumptions and verification of finite-state concurrent systems. In *Proc. Int. Workshop Automatic Verification Methods for Finite State Systems (CAV'89), Grenoble, June 1989*, volume 407 of *Lecture Notes in Computer Science*, pages 197–212. Springer, 1990.

[DJS99] Catherine Dufourd, Petr Jančar, and Philippe Schnoebelen. Boundedness of Reset P/T nets. In *Proc. 26th Int. Coll. Automata, Languages, and Programming (ICALP'99), Prague, Czech Republic, July 1999*, volume 1644 of *Lecture Notes in Computer Science*, pages 301–310. Springer, 1999.

[DRB02] Giorgio Delzanno, Jean-François Raskin, and Laurent Van Begin. CSTs (covering sharing trees) : compact data structures for parameterized verification. Technical Report 486, ULB, 2002.

[DRV01] Gorgio Delzanno, Jean-Francois Raskin, and Laurent Van Begin. Attacking symbolic state explosion. In *Proc. 13th Int. Conf. Computer Aided Verification (CAV'2001), Paris, France, July 2001*, volume 2102 of *Lecture Notes in Computer Science*, pages 298–310. Springer, 2001.

[EFM99] Javier Esparza, Alain Finkel, and Richard Mayr. On the verification of broadcast protocols. In *Proc. 14th IEEE Symp. Logic in Computer Science (LICS'99), Trento, Italy, July 1999*, pages 352–359. IEEE Comp. Soc. Press, 1999.

[EN98] E. Allen Emerson and Kedar S. Namjoshi. On model checking for non-deterministic infinite-state systems. In *Proc. 13th IEEE Symp. Logic in Computer Science (LICS'98), Indianapolis, IN, USA, June 1998*, pages 70–80. IEEE Comp. Soc. Press, 1998.

[Fas] Fast homepage. `http://www.lsv.ens-cachan.fr/fast/`.

[FL02] Alain Finkel and Jérôme Leroux. How to compose Presburger-accelerations : Applications to broadcast protocols. In *Proc. 22nd Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS'2002), Kanpur, India, Dec. 2002*, volume 2556 of *Lecture Notes in Computer Science*, pages 145–156. Springer, 2002.

[FMP99] Alain Finkel, Pierre McKenzie, and Claudine Picaronny. A well-structured framework for analysing Petri nets extensions. Research Report LSV-99-2, Lab. Specification and Verification, ENS de Cachan, Cachan, France, February 1999.

[FO97a] Laurent Fribourg and Hans Olsén. A decompositional approach for computing least fixed-points of Datalog programs with Z-counters. *Constraints*, 2(3/4) :305–335, 1997.

[FO97b] Laurent Fribourg and Hans Olsén. Proving safety properties of infinite state systems by compilation into Presburger arithmetic. In *Proc. 8th Int. Conf. Concurrency Theory (CONCUR'97), Warsaw, Poland, Jul. 1997*, volume 1243 of *Lecture Notes in Computer Science*, pages 213–227. Springer, 1997.

[FPS00] Alain Finkel, S. Purushothaman Iyer, and Grégoire Sutre. Well-abstracted transition systems. In *Proc. 11th Int. Conf. Concurrency Theory (CONCUR'2000), University Park, PA, USA, Aug. 2000*, volume 1877 of *Lecture Notes in Computer Science*, pages 566–580. Springer, 2000.

[FPS03] Alain Finkel, S. Purushothaman Iyer, and Grégoire Sutre. Well-abstracted transition systems : Application to FIFO automata. *Information and Computation*, 181(1) :1–31, 2003.

[FR74] Michael J. Fischer and Michael O. Rabin. Super-exponential complexity of Presburger arithmetic. In R. M. Karp, editor, *Complexity of Computation*, volume 7, pages 27–41. American Mathematical Society, Providence, RI, 1974.

[FS00a] Alain Finkel and Grègoire Sutre. An algorithm constructing the semilinear post* for 2-dim Reset/Transfer VASS. In *Proc. 25th Int. Symp. Math. Found. Comp. Sci. (MFCS'2000), Bratislava, Slovakia, Aug. 2000*, volume 1893 of *Lecture Notes in Computer Science*, pages 353–362. Springer, 2000.

[FS00b] Alain Finkel and Grégoire Sutre. Decidability of reachability problems for classes of two counters automata. In *Proc. 17th Ann. Symp. Theoretical Aspects of Computer Science (STACS'2000), Lille, France, Feb. 2000*, volume 1770 of *Lecture Notes in Computer Science*, pages 346–357. Springer, 2000.

[FS01] Alain Finkel and Phillipe Schnoebelen. Well structured transition systems everywhere ! *Theoretical Computer Science*, 256(1–2) :63–92, 2001.

[GBD02] Vijay Ganesh, Sergey Berezin, and David L. Dill. Deciding Presburger arithmetic by model checking and comparisons with other methods. In *Proc. 4th Int. Conf. Formal Methods in Computer Aided Design (FMCAD'02), Portland, OR, USA, nov. 2002*, volume 2517 of *Lecture Notes in Computer Science*, pages 171–186. Springer, 2002.

[Gmp] GMP homepage. `http://www.swox.com/gmp/`.

[GN03] Sumit Gulwani and George C. Necula. Discovering affine equalities using random interpretation. In *Proc. 30th ACM Symp. Principles of Programming Languages (POPL'2003), New Orleans, LA, USA, Jan. 2003*, pages 74–84, 2003.

[Got95] Georg Gottlob. NP trees and Carnap's modal logic. *Journal of the ACM*, 42(2) :421–457, 1995.

[GS66] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger formulas and languages. *Pacific J. Math.*, 16(2) :285–296, 1966.

[Gtl] GTL homepage. `http://infosun.fmi.uni-passau.de/GTL/`.

[HH95] Thomas A. Henzinger and Pei-Hsin Ho. HYTECH : The Cornell HYbrid TECHnology tool. In *Proc. Hybrid Systems II, Ithaca, NY, USA, Oct. 1994*, volume 999 of *Lecture Notes in Computer Science*, pages 265–293. Springer, 1995.

[HJMS02] T. A. Henzinger, R. Jhala, R. Majumdar, and G. Sutre. Lazy abstraction. In *Proc. 29th ACM Symp. Principles of Programming Languages (POPL'2002), Portland, OR, USA, Jan. 2002*, pages 58–70, 2002.

[Hop71] John E. Hopcroft. An $n \log n$ algorithm for minimizing the states in a finite-automaton. In Z. Kohavi, editor, *Theory of Machines and Computations*, pages 189–196. Academic Press, 1971.

[HP79] John Hopcroft and Jean-Jacques Pansiot. On the reachability problem for 5-dimensional vector addition systems. *Theoretical Computer Science*, 8(2) :135–159, 1979.

[HRHY86] Rodney R. Howell, Louis E. Rosier, Dung T. Huynh, and Hsu-Chen Yen. Some complexity bounds for problems concerning finite and 2-dimensional vector addition systems with states. *Theoretical Computer Science*, 46 :107–140, 1986.

[Hue78] Gérard Huet. An algorithm to generate the basis of solutions to homogenous linear diophantine equations. *Information Processing Letters*, 7(3) :144–147, 1978.

[Huy85] Thiet-Dung Huynh. The complexity of semilinear sets. *Elektronische Informationsverarbeitung und Kybernetik (jetzt J. Inf. Process. Cybern. EIK)*, 18 :291–338, 1985.

[Hyt] HyTech homepage. `http://www-cad.eecs.berkeley.edu/~tah/HyTech/`.

[Jac78] Gérard Jacob. La finitude des representations lineaires des semi-groupes est decidable. *Journal of Algebra*, 52 :437–459, 1978.

[KJ87] Fritz Krückeberg and Michael Jaxy. Mathematical methods for calculating invariants in petri nets. In *Advances in Petri Nets 1987, LNCS 266*, pages 196–223. Springer, 1987.

[Kla97] Nils Klarlund. Mona and fido : The logic-automaton connection in practice, 1997.

[KMS02] Nils Klarlund, A. Møller, and M. I. Schwartzbach. MONA implementation secrets. *Int. J. of Foundations Computer Science*, 13(4) :571–586, 2002.

[Knu69] Donald E. Knuth. *The Art of Computer Programming. Volume* 2 *: Seminumerical Algorithms*. Addison-Wesley, Massachusetts, 1969.

[Lam94] Jean-Luc Lambert. Vector addition systems and semi-linearity. 1994. To appear in the SIAM Journal of Computing.

[Las] Lash homepage. `http://www.montefiore.ulg.ac.be/~boigelot/research/lash/`.

[Ler03] Jérôme Leroux. The affine hull of a binary automaton is computable in polynomial time. In *5th Int. Workshop on Verification of Infinite-State Systems*, Electronic Notes in Theor. Comp. Sci., 2003. to appear.

[Lid] LiDIA homepage. `http://www.informatik.tu-darmstadt.de/TI/LiDIA/`.

[Mon] Mona homepage. `http://www.brics.dk/mona/index.html`.

[MOS04] Markus Müller-Olm and Helmut Seidl. Computing interprocedurally valid relations in affine programs. In *Proc. 31th ACM Symp. Principles of Programming Languages (POPL'2004), Venice, Italy, Jan. 2004*, 2004. To appear.

[MS77] Arnold Mandel and Imre Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2) :101–111, October 1977.

[Muc03] Muchnik. The definable criterion for definability in presburger arithmetic and its applications. *Theoretical Computer Science*, 290 :1433–1444, 2003.

[MZ75] R. McNaughton and Y. Zalcstein. The burnside theorem for semi-groups. *Journal of Algebra*, 34 :292–299, 1975.

[Ome] Omega homepage. `http://www.cs.umd.edu/projects/omega/`.

[Reu89] Christophe Reutenauer. *Aspects Mathématiques des Réseaux de Petri*, chapter 3. Collection Études et Recherches en Informatique. Masson, Paris, 1989.

[RV02] Tatiana Rybina and Andrei Voronkov. Brain : Backward reachability analysis with integers. In *Proc. 9th Int. Conf. Algebraic Methodology and Software Technology (AMAST'2002), Saint-Gilles-les-Bains, Reunion Island, France, Sep. 2002*, volume 2422 of *Lecture Notes in Computer Science*, pages 489–494. Springer, 2002.

[Sch87] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley and Sons, New York, 1987.

[Sch02] Philippe Schnoebelen. Verifying lossy channel systems has nonprimitive recursive complexity. *Information Processing Letters*, 83(5) :251–261, 2002.

[Smv] Smv homepage. `http://www-cad.eecs.berkeley.edu/~kenmcmil/`.

[Spi] Spin homepage. `http://spinroot.com/spin/`.

[ST98] Karsten Strehl and Lothar Thiele. Symbolic model checking using interval diagram techniques. Technical Report 40, Computer Engineering and Networks Lab (TIK), Swiss Federal Institute of Technology (ETH) Zurich, Gloriastrasse 35, CH-8092 Zurich, February 1998.

[Str98] Karsten Strehl. Using interval diagram techniques for the symbolic verification of timed automata. Technical Report 53, Computer Engineering and Networks Lab (TIK), Swiss Federal Institute of Technology (ETH) Zurich, Gloriastrasse 35, CH-8092 Zurich, July 1998.

[Tau92] Patrice Tauvel. *Mathématiques générales pour l'agrégation*. MASSON, Paris Milan Barcelone Bonn, 1992.

[Tre] TReX homepage. `http://www.liafa.jussieu.fr/~sighirea/trex/`.

[vzGS78] Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1) :155–158, October 1978.

[WB95] Pierre Wolper and Bernard Boigelot. An automata-theoretic approach to Presburger arithmetic constraints. In *Proc. 2nd Int. Symp. Static Analysis (SAS'95), Glasgow, UK, Sep. 1995*, volume 983 of *Lecture Notes in Computer Science*, pages 21–32. Springer, 1995.

[WB98] P. Wolper and B. Boigelot. Verifying systems with infinite but regular state spaces. In *Proc. 10th Int. Conf. Computer Aided Verification (CAV'98), Vancouver, BC, Canada, June-July 1998*, volume 1427 of *Lecture Notes in Computer Science*, pages 88–97. Springer, 1998.

[WB00] Pierre Wolper and Bernard Boigelot. On the construction of automata from linear arithmetic constraints. In *Proc. 6th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2000), Berlin, Germany, Mar.-Apr. 2000*, volume 1785 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2000.

[Yu97] Sheng Yu. Regular languages. In A. Salomaa and Grzegorz Rozenberg, editors, *Handbook of Formal Languages*, volume 1, Word Language Grammar, pages 41–110. Springer-Verlag, 1997.