De l'utilisation des périodiques dans les problèmes polyédriques en nombres entiers

Benoît Meister, LSIIT - ICPS, UMR 7005
Université Louis Pasteur
Strasbourg, France

29 octobre 2003

Résumé

Eugène Ehrhart a montré que le nombre de points à coordonnées entières d'un polytope rationnel paramétré s'exprime comme un polynôme particulier dont les coefficients sont des *nombres périodiques*. Dans ce rapport de recherche, nous proposons une étude de ces objets mathématiques qui dépendent périodiquement de paramètres, et une généralisation à une classe d'objets, les *périodiques*. Ensuite, nous établissons un rapport plus général entre les points à coordonnées entières d'un polyèdre et les périodiques. Finalement, nous présentons un ensemble de problèmes polyédriques en nombres entiers que l'on peut résoudre à l'aide des périodiques.

1 Motivation

La classe des problèmes polyédriques en nombres entiers couvre un nombre important de problèmes mathématiques. Entre autres, les solutions *faisables* en programmation linéaire en nombres entiers sont habituellement l'ensemble des points entiers contenus dans un polyèdre. En compilation de programmes impératifs, un certain type de structures de contrôles de flôt présentes dans la majorité des programmes, les *nids de boucles*, permettent l'exécution répétée d'instructions. Chacune de ces exécutions, appelée *itération*, est indexée par un ensemble de variables entières dont les valeurs sont souvent bornées par des fonctions affines et situées sur un réseau régulier de points. Le *modèle polyédrique* [1] permet de modéliser ces nids de boucles par l'intersection, appelée $\mathbb{Z}$-polyèdre, d'un polyèdre (défini par les bornes affines des indices de boucles) et d'un sous-réseau de $\mathbb{Z}^n$ (où n est le nombre d'indices de boucles).

On peut alors optimiser ces nids de boucles et exécuter certaines de leurs itérations en parallèle (par exemple dans [8, 6, 9, 5]) en analysant leur $\mathbb{Z}$-polyèdre.

Les travaux d'Eugène Ehrhart [3] puis de Philippe Clauss et Vincent Loechner [2] sur le dénombrement de points à coordonnées entières dans un polytope rationnel paramétré ont apporté une information structurelle qui nous intéresse particulièrement ici. Les polynômes d'Ehrhart, dont nous reparlerons et qui donnent le nombre de points entiers dans un polytope paramétré, s'écrivent en fonction de *nombres périodiques*, qui sont des nombres rationnels dépendant périodiquement de paramètres. Nous nous intéressons à cet aspect périodique et cherchons à expliciter son rapport avec l'objet mathématique $\mathbb{Z}$-polyèdre.

Dans un premier temps, nous étudierons en section 2 les nombres périodiques, ainsi qu'une classe plus générale d'objets mathématiques, les *périodiques*. Ensuite, nous montrons en section 3 de quelle manière les points entiers compris dans un polyèdre sont liés aux périodiques. L'utilisation explicite de ce lien permet la résolution d'un certain nombre de problèmes polyédriques en nombres entiers, que nous détaillerons en section 4. Finalement, nous présenterons en section 5 une vue d'ensemble de nos travaux présents et futurs, ainsi que des travaux connexes développés dans notre laboratoire.

2 Les périodiques

Dans la suite de cet exposé, une classe d'objets mathématiques (les *périodiques*) dont la valeur dépend périodiquement d'un ensemble de nombre entiers, sera définie. Cette classe étend la notion de *nombres périodiques*, introduits par Ehrhart dans le contexte du dénombrement de points entiers d'un polyèdre paramétré. Nous présenterons ensuite quelques périodiques qui seront utilisés pour la résolution de problèmes linéaires en nombres entiers dans les sections suivantes.

2.1 Définition

Nous proposons ici plusieurs définitions équivalentes des périodiques, qui seront plus ou moins adaptés à une certaine utilisation. La définition suivante exprime un périodique sous la forme d'une application de variables entières $x \in \mathbb{Z}^n$ vers des éléments du monoïde K sur lequel il est défini, un même élément étant touché périodiquement en fonction de chaque variable de x.

Définition 1 *Un périodique U de période* $S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{Z}^n$ *sur un monoïde K est une application :*

$$\mathbb{Z}^n \longrightarrow K$$

$$\forall j \in [1, n], x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto u(x) = u(x + t_j),$$

$$avec\ t_j = \begin{pmatrix} t_{j1} = 0 \\ \vdots \\ t_{ji-1} = 0 \\ t_{ji} = s_j \\ t_{ji+1} = 0 \\ \vdots \\ t_{jn} = 0 \end{pmatrix}$$

Par convention, un périodique U dépendant de $x \in \mathbb{Z}^n$ est noté U_x. n est appelé la dimension du périodique U. Il découle de cette définition la propriété suivante :

Propriété 1 *U_x est égal à l'élément u_y de K pour tout x tel que $x = y$ mod S.*

On utilise ici l'opérateur *modulo* membre à membre entre éléments de $\mathbb{Z}^n$. Nous définissons cet opérateur, proche de l'opérateur *reste de la division entière*, par :

$$\forall a \in \mathbb{Z}, n, b \in \mathbb{N}, a\ mod\ n = b \Leftrightarrow a = k.n + b\ tel\ que\ b \geq 0\ et\ k \in \mathbb{Z}\ soit\ maximal$$

Le nombre de valeurs distinctes que peut prendre la $i^{ème}$ composante de $x\ mod\ S$ est égal à s_i. Comme les composantes de S sont indépendantes (ce sont des constantes), le nombre de valeurs distinctes que peut prendre le vecteur $x\ mod\ S$ est donc égal à $|S| = s_1 \times s_2 \times \cdots \times s_n$.

Un périodique peut donc se représenter par un tableau $\mathcal{U}$ de dimension n et de taille $S = (s_1, s_2, \cdots, s_n)$ de la manière suivante : $U_x = \mathcal{U}[i_1, i_2, \cdots, i_n]$ si $\forall j \in [1, n]$, $i_j = x_j\ mod\ s_j$.

Exemple 1 Un périodique de dimension 1 sur $\mathbb{Q}$, de période $S = \begin{pmatrix} 3 \end{pmatrix}$ dépendant de $P \in \mathbb{Z}$, dont la valeur est de :

- $\frac{3}{2}$ lorsque $P \bmod 3 = 0$
- 1 lorsque $P \bmod 3 = 1$
- $\frac{7}{8}$ lorsque $P \bmod 3 = 2$

peut se représenter ainsi : $\begin{bmatrix} \frac{3}{2} & 1 & \frac{7}{8} \end{bmatrix}_P$

Un périodique à 2 dimensions sur les fonctions affines $(i, j, k) \in \mathbb{Z}^n$ dépendant périodiquement de $(i, j) \in \mathbb{Z}^2$, dont la valeur est :

- $i + 2j - 3k + 7$ lorsque $i \bmod 3 = 0$, $j \bmod 2 = 0$
- $2i - j + k$ lorsque $i \bmod 3 = 1$, $j \bmod 2 = 0$
- $3j - 5$ lorsque $i \bmod 3 = 2$, $j \bmod 2 = 0$
- $-i - 2j$ +3k -7 lorsque $i \bmod 3 = 0$, $j \bmod 2 = 1$
- $i - 2k + 1$ lorsque $i \bmod 3 = 1$, $j \bmod 2 = 1$
- 0 lorsque $i \bmod 3 = 2$, $j \bmod 2 = 1$

peut se représenter ainsi :

$$\begin{bmatrix} i + 2j - 3k + 7 & -i - 2j + 3k - 7 \\ 2i - j + k & i - 2k + 1 \\ 3j - 5 & 0 \end{bmatrix}_{i,j}$$

mais également de la manière suivante :

$$\begin{bmatrix} 1 & -1 \\ 2 & 1 \\ 0 & 0 \end{bmatrix}_{i,j} i + \begin{bmatrix} 2 & -2 \\ -1 & 0 \\ 3 & 0 \end{bmatrix}_{i,j} j + \begin{bmatrix} -3 & 3 \\ 1 & -2 \\ 0 & 0 \end{bmatrix}_{i,j} k + \begin{bmatrix} 7 & -7 \\ 0 & 1 \\ -5 & 0 \end{bmatrix}_{i,j}$$

(nous appelons cette forme *forme factorisée*, dans laquelle la partie générique d'une fonction affine de (i, j, k) est extraite). ◻

La propriété 1 nous permet de donner une définition plus géométrique des périodiques. L'ensemble des points entiers x tels qu'un périodique U soit égal à un élément donné U_x de K forme un réseau régulier de points. Nous pouvons donc considérer chacun de ces réseaux comme le domaine de définition de chaque élément de U_x

Définition 2 *Un périodique n-dimensionnel M de période* $S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{N}^n$ *sur un monoïde K est donné par :*

- $q = s_1 \times s_2 \times \ldots \times s_n$ *éléments M_I de K, indexés par :*

$$I = \begin{pmatrix} i_1 \\ i_2 \\ \vdots \\ i_n \end{pmatrix} \in \mathbb{Z}^n \text{ avec } 0 \leq i_k < s_k, k \in [1..n]$$

- *leur domaine de définition respectif $\mathcal{D}_I$, qui est le réseau de points entiers défini par :*

$$\begin{pmatrix} s_1 & 0 & \cdots & 0 \\ 0 & s_2 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & s_m \end{pmatrix} J + I, J \in \mathbb{Z}^n$$

$\bigcup_I \mathcal{D}_I = \mathbb{Z}^n$ *: tout élément $X \in \mathbb{Z}^n$ est associé à un unique M_I par la relation $I = X$ mod S.*

2.2 Quelques périodiques intéressants

Cette section énumère des périodiques sur des monoïdes K particuliers. Certains d'entre eux existent déjà, les autres seront utiles à l'analyse de problèmes linéaires en nombres entiers.

Définition 3 *On appelle* nombres périodiques *les périodiques sur $\mathbb{Q}$.*

Ils ont été introduits par Ehrhart [3], où il montre qu'ils forment un anneau.

Exemple 2 $\begin{bmatrix} 0 & 2 & 4 \\ 3 & 5 & 1 \end{bmatrix}_{i,j}$ est un nombre périodique de période $S = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ en $\begin{pmatrix} i \\ j \end{pmatrix}$ □

Définition 4 *On appelle* expressions périodiques *les périodiques sur les expressions affines à coefficients rationnels.*

Exemple 3 $\begin{bmatrix} \frac{1}{3} & 2 \\ -1 & \frac{3}{2} \end{bmatrix}_{N,j} .i + \begin{bmatrix} 0 & 4 & 1 \end{bmatrix}_{i} .j$ est une expression périodique de période $S = \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}$ en $\begin{pmatrix} i \\ j \\ N \end{pmatrix}$.

□

Définition 5 *On appelle* polyèdres périodiques *les périodiques sur les polyèdres dans* $\mathbb{Q}^d, d \in \mathbb{N}$.

Exemple 4

$$\begin{cases} \begin{bmatrix} 1 & 2 \\ \frac{-1}{2} & 3 \end{bmatrix}_{N,j} .i + \begin{bmatrix} 0 & 4 & 1 \end{bmatrix}_{i} .j \geq 0 \\ \begin{bmatrix} 0 & 3 & \frac{2}{5} \\ 1 & \frac{3}{4} & 5 \end{bmatrix}_{i,j} .i + 5 \geq 0 \\ N \geq 0 \end{cases}$$ est un polyèdre périodique. □

Selon la définition 2, un polyèdre périodique P peut être vu comme un ensemble de polyèdres P_I sur un réseau de points entiers (leur domaine de définition). Chaque P_I est donc l'intersection d'un polyèdre et d'un réseau de points entiers, c'est-à-dire un $\mathbb{Z}$-*polyèdre*.

Définition 6 *Introduits par Ehrhart [3] et étendus par Clauss et Loechner [2], on peut définir les* polynômes d'Ehrhart *(ou encore* pseudo-polynômes, polynômes arithmétique *ou* polars*) comme les périodiques sur l'anneau des polynômes de variables entières à coefficients rationnels.*

Exemple 5 $\mathcal{E}(i, j, n) = \begin{bmatrix} 0 & 3 & 2 \\ 1 & 4 & 5 \end{bmatrix}_{i,j} .i^4 j^2 N + \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}_{N,j} .ij^3 + 4N$ est un pseudo-polynôme. □

2.3 Opérations sur les périodiques

Notation On notera $P[K]$ les périodiques sur le monoïde K. □

Si $\exists k \in [1..n]$ tel que $s_k = 1$, on dit que le périodique est indépendant de x_k. En effet, l'élément de K atteint par U_x est le même quelque soit x_k pour des valeurs de $x_1, x_2, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n$ données.

Tout élément k d'un monoïde K est donc un périodique U_x sur K égal à k quelque soit x. Dans cette section, nous donnons d'autres propriétés des périodiques, concernant les opérations. Celles-ci seront utiles à la compréhension des techniques que nous exposerons ensuite.

Les périodiques sont définis sur un monoïde K. Par définition un monoïde K comporte une opération interne, c'est à dire une application de $K \times K \longrightarrow K$. Considérons les opérations entre périodiques, et observons comment elles se rapprochent des opérations entre éléments d'un monoïde.

Théorème 1 *Il existe pour toute opération C sur des monoïdes vers un monoïde :*

$$K_A \times K_B \longrightarrow K$$

$$\alpha, \beta \mapsto \mu = C(\alpha, \beta)$$

une opération C' :

$$P[K_A] \times P[K_B] \longrightarrow P[K]$$

$$(A_x, B_x) \mapsto U_x = C'(A_x, B_x)$$

pout tout $(0) \leq x \leq S$.

Preuve Sans entamer la généralité de l'approche, supposons que les périodiques A et B soient de dimension n et de périodes respectives S^A et S^B. Soit $S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{Z}^n$ tel que $s_i = ppcm(s_i^A, s_i^B)$ $\forall i \in [1, n]$. Soit $t_i^A \in \mathbb{Z}^n, \forall i \in [1, n]$ de composantes $t_{i,j}^A = \begin{cases} s_i^A & si\ i = j \\ 0 & sinon \end{cases}$. On construit de la même manière le vecteurs t_i^B et t_i à partir des périodes S^B, et S. D'apres la définition 2.1 des périodiques, $A_x = A_{(x+t_i^A)}$ et $B_x = B_{(x+t_i^B)}$. Comme s_i est un multiple de s_i^A et de s_i^B pour tout $i \in [1, n]$, on a aussi : $A_x = A_{(x+t_i)}$ et $B_x = B_{(x+t_i)}$. Par substitution, on obtient la propriété suivante : $C(A_x, B_x) = C(A_{(x+s_i)}, B_{(x+s_i)})$. $C(A_x, B_x)$ est donc périodique de période S. □

D'après le théorème 1, le résultat de C' est un périodique. De plus, les éléments atteints par U_x appartiennent au monoïde K : U_x est un périodique sur K.

Corollaire 1 *Les périodiques* $P[K]$ *sur le monoïde* K *forment un monoïde.*

Preuve Par définition, une opération interne sur un monoïde K est une application de $K \times K \longrightarrow K$. D'après le théorème 1, il existe donc pour tout monoïde K muni d'une opération $C : K \times K \longrightarrow K$ une classe $P[K]$ munie d'une opération $C' : P[K] \times P[K] \longrightarrow P[K]$. La conservation de l'associativité de l'opération et d'un élément neutre se démontrent aisément. □

Il en découle que les périodiques sur $P[K]$ sont des périodiques sur K.

Exemple 6 Considérons le monoïde des polyèdres dans $\mathbb{Q}^d, d \in \mathbb{N}$ munis de l'opération *intersection* ($\cap$). Nous avons par exemple :

$$\begin{cases} i+j \geq 0 \\ i \geq -3 \end{cases} \cap \begin{cases} i-j \geq 0 \\ i \leq 10 \end{cases} = \begin{cases} i+j \geq 0 \\ i-j \geq 0 \\ i \leq 10 \end{cases}$$

On peut donc définir une application *intersection*, que l'on notera également $\cap$, des périodiques sur les polyèdres dans $\mathbb{Q}^d$. Nous aurons par exemple :

$$\begin{bmatrix} \begin{cases} i-j \geq 0 \\ i \leq 0 \end{cases} \\ \begin{cases} i+j \geq 0 \\ i \geq -3 \end{cases} \end{bmatrix}_N \cap \begin{bmatrix} \begin{cases} i-j \geq 0 \\ i \leq 10 \end{cases} & \begin{cases} 2i-j \geq 0 \\ i \geq -3 \end{cases} \end{bmatrix}_M$$

$$= \begin{bmatrix} \begin{cases} i-j \geq 0 \\ i \leq 0 \end{cases} & \begin{cases} -3 \leq i \leq 0 \\ 2i-j \geq 0 \end{cases} \\ \begin{cases} i \leq 10 \\ -i \leq j \leq i \end{cases} & \begin{cases} 2i-j \geq 0 \\ i+j \geq 0 \end{cases} \end{bmatrix}_{N,M}$$

□

Toutefois, l'opération C' définie dans le théorème 1 existe, mais n'a pas forcément la même sémantique que l'opération C. En effet, d'après la définition 2, les éléments de K touchés par un périodique $A_x \in P[K]$ sont définis sur un réseau de points entiers. Si la sémantique de l'opération C est dépendante du fait que x soit sur un réseau de points, alors la sémantique de l'opération C' définie dans le théorème 1 n'est la même que celle de C que si ses opérandes sont de période (1).

Exemple 7 L'opération *valeur entière supérieure*, $\lceil a \rceil$, est définie de la manière suivante pour $a \in \mathbb{Q}$:

$$\lceil a \rceil = \{n \in \mathbb{Z} \mid n-1 < a \leq n\}, a \in \mathbb{Q}$$

On peut en déduire, par le théorème 1, une opération ayant la même définition sur $P[\mathbb{Q}]$:

$$entier\_sup(U_x) = \{N_x \in P[\mathbb{Z}] \mid N_x - 1 < U_x \leq N_x\}, U_x \in P[\mathbb{Q}]$$

Supposons que l'on souhaite résoudre $x = \lceil U_x \rceil = \lceil \begin{bmatrix} \frac{y}{2} & \frac{y}{3} \end{bmatrix}_x \rceil$. On aura $entier\_sup(U_x) = \begin{bmatrix} \lceil \frac{y}{2} \rceil & \lceil \frac{y}{3} \rceil \end{bmatrix}_x$. Résoudre notre équation à l'aide de l'opérateur *entier_sup* donnerait le résultat suivant :

$$x = \begin{bmatrix} \{n_0 \mid n_0 - 1 < \frac{y}{2} \leq n_0\} & \{n_1 \mid n_1 - 1 < \frac{y}{3} \leq n_1\} \end{bmatrix}_x$$

Pour $y = 5$, nous aurions donc $x = \begin{bmatrix} 3 & 2 \end{bmatrix}_x$, c'est à dire :

$$x = \begin{cases} 3 & pour\ x\ pair \\ 2 & pour\ x\ impair \end{cases}$$

ce qui se réduit à $x = \emptyset$. La sémantique de l'opérateur *entier_sup* n'est donc pas d'extraire l'entier supérieur d'un périodique, comme on aurait pu le croire. On peut voir que l'opérateur sémantiquement correspondant est :

$$\lceil U_x \rceil = \begin{bmatrix} \{2n_0 \mid 2n_0 - 2 < \frac{y}{2} \leq 2n_0\} & \{2n_1 + 1 \mid 2n_1 - 1 < \frac{y}{3} \leq 2n_1 + 1\} \end{bmatrix}_x$$

□

De manière générale, on peut rendre explicite la valeur de x dans le périodique U_x de période p afin de mettre au point un opérateur adapté aux périodiques :

$$x = px' + x_0, x_0 = x\ mod\ p$$

Nous voyons dans la section suivante l'interaction plus générale entre les opérateurs *partie entière* et *modulo* et les périodiques, dans le cadre de problèmes linéaires en nombres entiers.

3 Parties entières

Nous souhaitons modéliser des problèmes linéaires en nombres entiers. Ceux-ci peuvent prendre la forme d'un ensemble d'inéquations entre parties entières, inférieure ou supérieure, d'expressions rationelles. Dans cette section, nous montrons le lien entre ce type de problèmes et les périodiques.

Propriété 2 *Soit une expression affine entière de* $I = \begin{pmatrix} i_1 \\ i_2 \\ \vdots \\ i_n \end{pmatrix} \in \mathbb{Z}^n$ *:*

$$f(I) = c_0 + c_1 i_1 + c_2 i_2 + \cdots + c_n i_n, c_k \in \mathbb{Z}$$

$f(I)\ mod\ m$ est un périodique sur $\mathbb{Z}$ en I de période $B = (b_k)$, où $b_k = \frac{m}{pgcd(m, c_k)}, \forall k \in [1, n]$.

Preuve Soit le vecteur $I'_k = \begin{pmatrix} i'_1 \\ i'_2 \\ \vdots \\ i'_n \end{pmatrix}$, avec $i'_j = \begin{cases} i_j + b_k \ si \ j = k \\ i_j \ sinon \end{cases}$

$$f(I'_k) = f(I) + c_k b_k$$

Or $c_k b_k = \frac{mc_k}{pgcd(m,c_k)}$ et $pgcd(m, c_k)$ divise c_k. $c_k b_k$ est donc un multiple entier de m, d'où $f(I'_k) \ mod \ m = (f(I) + c_k b_k) \ mod \ m = f(I) \ mod \ m$. Chaque valeur de $f(I) \ mod \ m$ est atteinte périodiquement en fonction des valeurs de i_k, avec une période b_k. □

Soit un périodique monodimensionnel $A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} \end{bmatrix}_{f(I)}$ de période m et dépendant périodiquement de $f(I)$. Nous avons :

$$A = a_j \iff f(I) \ mod \ m = j$$

avec $j \in [0, m-1]$. Les valeurs de A sont donc atteintes périodiquement en fonction des valeurs de i_k, avec une période b_k. A peut donc être représenté par un périodique de période $S = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$. Notons A° cette représentation. Chaque valeur ${a^\circ}_I$ de A° est égale à la valeur $a_{f(I)}$ de A. On peut donc obtenir la représentation A° en parcourant chacune de ses entrées, qui sera égale à $a_{f(I)}$.

Exemple 8

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}_{(3i+4j)} = \begin{bmatrix} 0 & 2 & 4 \\ 3 & 5 & 1 \end{bmatrix}_{i,j}$$

□

Propriété 3 *La période B de la représentation A° de A est minimale : il n'existe pas de périodique de période inférieure (selon chaque composante) dépendant directement de ses indices I .*

Preuve Soit q le dénominateur de $b_k, k \in [1, n]$. Par définition, les périodiques ont des périodes entières : la période b_k doit être entière, son dénominateur q doit donc diviser m. De plus, $c_k b_k$ doit être un multiple de m, donc q doit diviser c_k. La valeur minimale possible pour b_k est donc obtenue avec la plus grande valeur de q divisant à la fois m et c_k, c'est à dire $pgcd(m, c_k)$. $b_k = \frac{m}{pgcd(m,c_k)}$ est donc la plus petite période possible de A° selon i_k. □

Il est donc possible de représenter un périodique monodimensionnel dépendant d'une fonction affine de $\mathbb{Z}^n$ vers $\mathbb{Z}$ par un périodique multidimensionnel dépendant des variables de cette fonction affine. On étudiera ultérieurement l'opération inverse : représenter un périodique dépendant directement de variables (entières) par un périodique monodimensionnel dépendant d'une fonction affine de ces variables. Il pourrait aussi être utile de généraliser cette notion d'équivalence aux périodiques multidimensionnels dépendant de fonctions affines de variables entières. Cette opération n'étant pas nécessaire dans le cadre de notre étude, nous ne la développerons pas.

Nous nous sommes maintenant munis d'objets mathématiques qui seront notre support pour l'analyse de problèmes linéaires en nombres entiers, ainsi que de certaines de leurs propriétés. Une application fondamentale est le calcul de parties entières d'expressions affines rationnelles, que nous présentons dans la section suivante.

3.1 Parties entières d'expressions rationnelles

Nous souhaitons calculer la partie entière supérieure (resp. inférieure) d'une fonction affine de variables I et de paramètres N, de coefficients rationnels de la forme : $f(I,N) = \sum a_k i_k + \sum b_k n_k + c$ avec $a_k, b_k, c \in \mathbb{Q}$. Soit q le dénominateur commun de tous les coefficients a_k, b_k et c. Nous pouvons alors écrire $f(I,N)$ de la façon suivante :

$$f(I,N) = \frac{\sum a'_k i_k + \sum b'_k n_k + c'}{q} = \frac{f'(I,N)}{q}$$

avec $a'_k, b'_k, c' \in \mathbb{Z}$. Les parties entières inférieures et supérieures de $f(I,N)$ peuvent s'exprimer de la façon suivante :

$$\lfloor f(I,N) \rfloor = \frac{f'(I,N) - (f'(I,N) \ mod \ q)}{q} = f(I,N) - \frac{f'(I,N) \ mod \ q}{q}$$

$$\lceil f(I,N) \rceil = \frac{f'(I,N) + (-f'(I,N) \ mod \ q)}{q} = f(I,N) + \frac{(-f'(I,N)) \ mod \ q}{q}$$

La valeur de $\lfloor f(I,N) \rfloor$ dépend de $f'(I,N) \ mod \ q$, nombre dont la valeur est périodique en fonction de $f'(I,N)$. En effet, $f'(I,N) \ mod \ q$ est le périodique sur $\mathbb{Z}$ suivant :

$$f'(I,N) \ mod \ q = \begin{bmatrix} 0 & 1 & \cdots & q-2 & q-1 \end{bmatrix}_{f'(I,N)}$$

Nous avons vu précédemment que $f'(I,N) \ mod \ q$ est un périodique sur $\mathbb{Z}$:

- de dimension $n = Dim(I) + Dim(N)$,

– dépendant directement de $x = \begin{pmatrix} N \\ I \end{pmatrix} \in \mathbb{Z}^n$.

Le même raisonnement est valable sur la valeur de $\lceil f(I,N) \rceil$

Exemple 9

$$\begin{aligned}
\lfloor \tfrac{2}{3}i + \tfrac{j}{2} \rfloor &= \lfloor \tfrac{4i+3j}{6} \rfloor \\
&= \tfrac{4i+3j-((4i+3j)\ mod\ 6)}{6} \\
&= \frac{4i+3j-\begin{bmatrix} 0 & 3 \\ 4 & 1 \\ 2 & 5 \end{bmatrix}_{i,j}}{6} \\
&= \tfrac{2}{3}i + \tfrac{j}{2} - \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{2}{3} & \frac{1}{6} \\ \frac{1}{3} & \frac{5}{6} \end{bmatrix}_{i,j}
\end{aligned}$$

□

L'application principale de cette mise sous forme périodique explicite des parties entières d'une expression affine rationnelle vient du fait qu'un polyèdre rationnel s'exprime comme un ensemble d'égalités et d'inégalités sur des expressions affines rationnelles. Beaucoup de problèmes s'expriment comme la recherche d'un point à coordonnées entières dans un polyèdre rationnel. Nous présentons dans la section suivante une vue d'ensemble des problèmes qui nous intéressent particulièrement, et que nous souhaitons résoudre par ce type de méthode.

4 Applications

L'application qui nous intéresse directement est celle des nids de boucles dans les programmes informatiques. En particulier, nous focalisons sur les boucles dont les indices prennent des valeurs entières et sont bornés par des fonctions affines des indices de boucles englobantes et de paramètres, qui constituent une grande part des boucles existantes. Ces bornes de boucles sont donc des parties entières d'expressions affines.

Exemple 10 Soit la boucle suivante :

```
for k = (2*j)/3 + i/2 to  7*j + i
```

La borne inférieure de k est donnée par :

$$
\begin{aligned}
\lceil \tfrac{2}{3}i + \tfrac{j}{2} \rceil &= \lceil \tfrac{4i+3j}{6} \rceil \\
&= \frac{4i+3j+((-4i-3j)\ mod\ 6)}{6} \\
&= \frac{4i+3j+\begin{bmatrix} 0 & 3 \\ 2 & 5 \\ 4 & 1 \end{bmatrix}_{i,j}}{6} \\
&= \tfrac{2}{3}i + \tfrac{i}{2} + \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{3} & \frac{5}{6} \\ \frac{2}{3} & \frac{1}{6} \end{bmatrix}_{i,j}
\end{aligned}
$$

L'extraction des valeurs entières des bornes d'un nid de boucles définit de manière plus explicite les valeurs prises par les bornes de boucles. Le modèle polyédrique modélise les nids de boucles, dont les indices prennent des valeurs entières et sont bornés par une fonction affine des indices des boucles englobantes et de paramètres, par des $\mathbb{Z}$-polyèdres rationnels. Nous pouvons considérer des $\mathbb{Z}$-polyèdres dont le réseau support est $\mathbb{Z}^n$ sans dégrader la généralité de la méthode. Il est connu que la solution d'un problème linéaire (lorsqu'elle est unique) est un sommet du polyèdre qui représente toutes les valeurs possibles des variables du problème. Le problème, lorsque l'on cherche une solution entière, vient généralement du fait que l'on cherche des solutions entières appartenant à un polyèdre dont les sommets sont rationnels. On peut fabriquer, à partir d'un polyèdre rationnel P, le polyèdre P' contenant tous les points entiers de P et dont les sommets sont entiers. Ce polyèdre, qui est l'enveloppe convexe des points entiers de P, s'appelle l'*enveloppe entière* de P. La connaissance de l'enveloppe entière de P permettra en particulier le calcul du minimum et du maximum lexicographique entiers d'un polyèdre [4], qui correspondent respectivement à la première et la dernière itérations d'un nid de boucles modélisé par le polyèdre P. Un solveur plus général pourra utiliser l'enveloppe entière pour résoudre un programme linéaire entier, de la forme

$$min\{x \mid f(x, N) \in P\}$$

où x sont les variables du problème et N sont des paramètres intervenant dans la partie constante des contraintes (égalités et inégalités) de P.

De plus, l'expression de l'enveloppe entière de P donne une nouvelle façon de dénombrer les points à coordonnées entières inclus dans P. En effet, l'enveloppe entière de P contient exactement le même nombre de points entiers que P. Le nombre de points entiers de P (son polynôme d'Ehrhart) est donc celui de P'.

On peut souhaiter savoir pour quelles valeurs des paramètres un nid de boucles sera exécuté ou non. Ce domaine de valeurs est celui pour lequel il existe un point entier dans son polyèdre associé P. Nous pensons que ce domaine d'existence d'un point entier dans P permettra le calcul du polynôme d'Ehrhart de la projection D' entière d'un $\mathbb{Z}$-polyèdre D par une transformation π. En effet, il est possible qu'une partie des points entiers contenus dans l'enveloppe convexe de D' ne soit pas l'image d'un point entier de D. Le nombre de points entiers dans D' est le nombre de points x de D' dont la préimage [1] par π est dans D. La mise en forme des coordonnées de x sous la forme de nouvelles variables du problème permettent d'établir le domaine δ pour lequel x existe. Le nombre de points entiers dans D' est alors le polynôme d'Ehrhart de δ.

5 Conclusion

Nous avons présenté la classe des périodiques, en montrant leur lien avec les problèmes linéaires en nombres entiers. L'utilisation des périodiques dans ce cadre permet une représentation explicite de parties entières de rationnels, ce qui permet de passer de problèmes rationnels à leur équivalent entier. Nous pensons que cette approche peut donner lieu à un certain nombre de nouvelles méthodes de résolution de problèmes linéaires en nombres entiers. En particulier, nous chercherons à résoudre les extréma lexicographiques entiers d'un polyèdre, ainsi que le polynôme d'Ehrhart d'une projection entière d'un $\mathbb{Z}$-polyèdre, dont les applications sont connues en analyse, optimisation et compilation de programmes (par exemple [8, 6, 9, 5, 10, 7]).

Références

[1] C. Ancourt and F. Irigoin. Scanning polyhedra with DO loops. In *Proc. ACM SIGPLAN '91*, pages 39–50, june 1991.

[2] Ph. Clauss and V. Loechner. Parametric analysis of polyhedral iteration spaces. *Journal of VLSI Signal Processing*, 19(2) :179–194, July 1998. http ://icps.u-strasbg.fr/pub-98.

[3] E. Ehrhart. *Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire*, volume 35 of *International Series of Numerical Mathematics*. Birkhäuser Verlag, Basel/Stuttgart, 1977.

[4] P. Feautrier. Parametric integer programming. *RAIRO Recherche Opérationnelle*, 22 :243–268, September 1988.

[1] La préimage de D' par π est l'endemble de points dont l'image par π est dans D'

[5] P. Feautrier. Lncs 1132. In *The Data Parallel Programming Model*, chapter Automatic parallelization in the Polytope Model, pages 79–100. 1996.

[6] C. Lengauer. Loop parallelization in the polytope model. In *CONCUR 93*, 1993.

[7] V. Loechner, B. Meister, and Ph. Clauss. Precise data locality optimization of nested loops. *The Journal of Supercomputing*, 21(1) :37–76, January 2002. Kluwer Academic Pub.

[8] M.E. Wolf and M.S. Lam. A loop transformation theory and an algorithm to maximize parallelism. *IEEE Transactions on Parallel and Distributed Systems*, 2(4) :452–471, October 1991.

[9] M. Wolfe. *High Performance Compilers for Parallel Computing.* Addison Wesley, 1996.

[10] J. Xue. Unimodular transformations of non-perfectly nested loops. *Parallel Computing*, 22(12) :1621–1645, 1997.