Études

Sur les extensions et les utilisations en informatique d'un résultat mathématique :

Les polynômes d'Ehrhart*

Philippe CLAUSS

Les polynômes d'Ehrhart constituent un résultat mathématique important, permettant d'exprimer le nombre de solutions entières d'un système d'équations et d'inéquations rationnelles et paramétriques. L'informatique trouve ici un outil permettant une analyse symbolique exacte des programmes. Nous montrons dans cet article que le mathématicien Eugène Ehrhart a posé les bases d'un vaste domaine d'investigations, tant en mathématique, permettant d'intéressantes extensions, qu'en informatique, où les applications de ses résultats augmentent encore les possibilités des ordinateurs.

Au début des années soixante, Eugène Ehrhart, mathématicien strasbourgeois bien connu des lecteurs de ce bulletin, a mis en évidence des résultats concernant le domaine de la géométrie algébrique. Plus précisément, ses résultats portent sur le nombre de solutions entières d'un système d'égalités et d'inégalités linéaires rationnelles, dépendant d'un paramètre entier positif [5, 6, 7, 9, 8, 10, 12, 13] .

** La composition du Bulletin ne nous a pas permis de placer la totalité de l'article dans ce numéro. Nous prions l'auteur et les lecteurs de bien vouloir nous en excuser.*
Le paragraphe V et la conclusion figureront dans le bulletin n° 419.

Par exemple, si l'on considère le système d'inégalités suivant :

$$\begin{cases} 0 & \leq & x & \leq & n \\ x+y & \leq & 2n & & \\ 0 & \leq & y & \leq & n \end{cases}$$

où n est un paramètre entier positif, le nombre de solutions entières de ce système est donné par son polynôme d'Ehrhart qui est $\frac{3}{2}n^2+\frac{5}{2}n+1$.

Ce problème étant bien cerné, E. Ehrhart l'a tout de suite posé en terme de problème géométrique. En effet, tout système d'équations linéaires définit un polyèdre convexe.

Ses résultats sont notamment d'un grand intérêt pour la recherche en informatique, et plus particulièrement en informatique *parallèle*, domaine de recherche dédié à la conception et à l'utilisation des ordinateurs les plus puissants du monde, appelés communément *super-calculateurs*. Nous montrons dans cet article, comment ils sont utilisés pour résoudre de nombreux problèmes liés à l'utilisation de ces machines.

Ces ordinateurs sont caractérisés par une architecture matérielle composée de plusieurs processeurs, contrairement aux micro-ordinateurs que l'on trouve aujourd'hui sur nos bureaux, qui n'en possèdent qu'un seul. Les processeurs sont interconnectés afin de pouvoir se transmettre données et résultats de calculs, et s'occupent simultanément à résoudre le même problème général, comme par exemple le calcul des éléments d'une matrice de taille 10 000 x 10 000.

Dans une première partie, nous rappelons quelques notions géométriques ainsi que les principaux résultats d'E. Ehrhart. Nous présentons ensuite nos extensions de ses résultats, à savoir, les polynômes d'Ehrhart à plusieurs variables, puis les polynômes d'Ehrhart de la projection affine d'un polytope. Nous décrivons, au paragraphe 4, comment sont calculés automatiquement ces polynômes par ordinateur. Au paragraphe 5, après avoir introduit le contexte informatique, nous montrons quelques utilisations à des problèmes d'analyse et de transformation de programmes (*Bulletin* n° 419).

I.- Géométrie et polynômes d'Ehrhart

Rappelons tout d'abord la définition d'un polyèdre convexe :

Définition 1 *Un polyèdre convexe P est un sous-ensemble de $\mathbb{R}^d$ qui est l'intersection d'un nombre fini de demi-espaces fermés. Il peut être défini par un système d'inégalités linéaires de la forme $P = x \in \mathbb{R}^d \mid A.x \leq B$, où A est* *une matrice de taille m×d de réels et B un vecteur de taille m de réels, m étant le nombre d'inégalités linéaires.*

Les équations composant les systèmes linéaires paramétriques considérés par E. Ehrhart sont de la forme générale suivante :

$$\sum_i a_i x_i < bn + c \qquad \sum_i a_i x_i = bn + c \qquad \sum_i a_i x_i \leq bn + c$$

où les a_i, b et c sont des constantes entières, les x_i sont les variables du système, et n est un paramètre entier positif.

Ces systèmes dépendant d'un paramètre entier positif n, les polyèdres ainsi définis sont donc également *paramétriques*. D'un point de vue géométrique, les solutions entières du système initial sont les points de coordonnées entières appartenant au polyèdre. Compter le nombre de solutions entières du système initial revient donc à compter le nombre de points entiers du polyèdre.

Le dénombrement des solutions entières n'a bien sûr de sens que si ce nombre est fini. Les polyèdres considérés sont donc eux aussi finis, ou *bornés*. On les appelle alors des *polytopes*. Ils sont l'enveloppe convexe d'un nombre fini de points de l'espace. On distingue les *polytopes entiers*, dont les sommets possèdent tous des coordonnées entières, et les polytopes rationnels, pour lesquels au moins un sommet possède des coordonnées rationnelles.

Le résultat majeur d'E. Ehrhart est d'avoir démontré que les nombres de points entiers de tels polytopes sont des polynômes en n, de degré égal à la dimension du plus petit espace contenant le polytope, si le polytope est entier, et sont des *pseudo-polynômes* de mêmes caractéristiques si le polytope est rationnel [11].

Les *pseudo-polynômes* sont des polynômes particuliers : leurs coefficients sont des *nombres périodiques*, c'est à dire des listes finies de valeurs rationnelles, où la valeur prise par le coefficient est déterminée par le rang de la valeur dans la liste, donné par la valeur du modulo de n par rapport au nombre de valeurs de cette liste. Pour être plus clair, prenons un exemple simple :

Exemple 1 Soit le pseudo-polynôme $f(n) = [0, 1, 2]\, n^2 + [1, \frac{1}{2}]\, n + [0, \frac{1}{4}]$

Selon les valeurs de n modulo 3 et n modulo 2, f(n) prendra les valeurs suivantes :

Si n modulo 3 = 1 et n modulo 2 = 1, $f(n) = n$
Si n modulo 3 = 1 et n modulo 2 = 0, $f(n) = \frac{1}{2}n + \frac{1}{4}$
Si n modulo 3 = 2 et n modulo 2 = 1, $f(n) = n^2 + n$
Si n modulo 3 = 2 et n modulo 2 = 0, $f(n) = n^2 + \frac{1}{2}n + \frac{1}{4}$

Si n modulo 3 = 0 et n modulo 2 = 1, $f(n) = 2n^2 + n$
Si n modulo 3 = 0 et n modulo 2 = 0, $f(n) = 2n^2 + \frac{1}{2}n + \frac{1}{4}$

□ Le nombre maximum de valeurs prises par les coefficients périodiques est donné par le dénominateur du polytope, c'est à dire par le plus petit commun multiple des dénominateurs des coordonnées des sommets du polytope. Un autre résultat assure que le coefficient du terme du plus haut degré est constant (non périodique), si l'on est sûr que le système possède au moins une solution entière.

Voyons un exemple simple afin d'illustrer ces rappels.

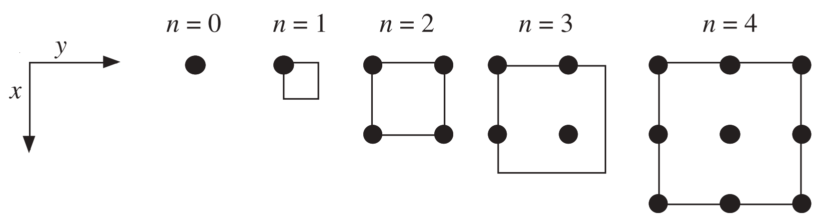
Exemple 2 Soit S_n le système linéaire suivant :

$$(S_n) \left\{ \begin{array}{lcl} x & \geq & 0 \\ x & \leq & \frac{1}{2}\,n \\ y & \geq & 0 \\ y & \leq & \frac{1}{2}\,n \\ n & \geq & 0 \end{array} \right.$$

Ce système S_n définit un polytope rationnel paramétrique P_n et, plus précisément, un carré dont les sommets ont pour coordonnées :

$$(0,0),\ (\tfrac{1}{2}\,n,0),\ (0,\tfrac{1}{2}\,n) \text{ et } (\tfrac{1}{2}\,n,\tfrac{1}{2}\,n)$$

Le carré et ses points entiers sont représentés sur la figure suivante pour n de 0 à 4 :



Le dénominateur de P_n est 2, la dimension de l'espace le contenant est 2, et on est sûr que S_n possède au moins une solution entière. Par conséquent, le pseudo-polynôme d'Ehrhart de P_n a donc la forme générale suivante : $pe(n) = c_1\, n^2 + [c_2,c_3]\, n + [c_4,c_5]$. Afin de déterminer les coefficients c_i, 5 valeurs numériques de $pe(n)$, $n \in [0,4]$, déterminées en comptant les points entiers de la figure ci-dessus, permettent de poser un système d'égalités linéaires dont les solutions sont leurs valeurs numériques :

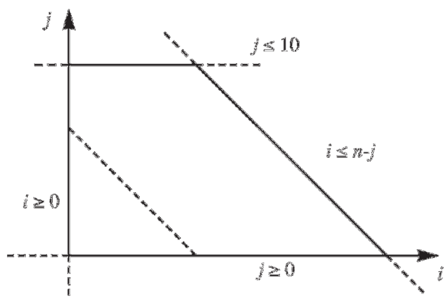
$$\left.\begin{array}{llll} pe\,(0) = & c_5 & = & 1 \\ pe\,(1) = & c_1 + c_2 + c_4 & = & 1 \\ pe\,(2) = & 4\,c_1 + 2\,c_3 + c_5 & = & 4 \\ pe\,(3) = & 9\,c_1 + 3\,c_2 + c_4 & = & 4 \\ pe\,(4) = & 16\,c_1 + 4\,c_3 + c_5 & = & 9 \end{array}\right\} \Rightarrow pe(n) = \frac{1}{4}\,n^2 + [\,\frac{1}{2}, 1]\,n + [\,\frac{1}{4}, 1]$$

Ainsi, le carré (ou système d'inéquations) défini avec n = 9 999 999 possède 100 000 009 999 998 points entiers (ou solutions entières).

☐ Plus généralement, la «forme» du polytope P_n varie selon des intervalles de valeurs de n. Ainsi, déterminer une expression paramétrique du nombre de points entiers contenus dans n'importe quel polytope paramétrique P_n, consiste tout d'abord, à décomposer P_n en une union de polytopes P_{n1}, P_{n2} …, définis sur des domaines adjacents de valeurs du paramètre n, et pour lesquels les coordonnées des sommets sont des expressions affines en n, puis à calculer le polynôme d'Ehrhart pour chacun de ces polytopes.

Exemple 3 Dans la figure ci-dessous, le polytope défini par

$P_n = \{(x,y) \mid x \geq 0,\ y \geq 0,\ x + y \leq n,\ y \leq 10\}$ est représenté, montrant le changement de sa forme par rapport au paramètre n.



Lorsque n est compris entre 0 et 10, P_n est un triangle, et lorsque n est supérieur à 10, P_n est un quadrilatère. Ainsi, P_n est décomposé en 2 polytopes :

$$P_n = \begin{cases} P_{n1} & si \quad 0 \leq n \leq 10, \textit{ de sommets } (0,0), (n,0) \textit{ et } (0,n) \\ P_{n2} & si \quad 10 \leq n, \textit{ de sommets } (0,0), (n,0), (0,10) \textit{ et } (n\text{-}10,10) \end{cases}$$

II.- Les polynômes d'Ehrhart à plusieurs variables

Dans notre contexte d'utilisation de ces résultats, ceux-ci doivent être étendus à un nombre quelconque de paramètres. Les systèmes considérés plus généraux sont alors de la forme :

$$\textstyle\sum_i a_i x_i < \sum_j b_j n_j + c \qquad \sum_i a_i x_i = \sum_j b_j n_j + c \qquad \sum_i a_i x_i \leq \sum_j b_j n_j + c$$

où les a_i, b_j et c sont des constantes entières, les x_i sont les variables du système, et les n_j sont des paramètres entiers positifs. E. Ehrhart a entammé une étude de ces systèmes. Cette étude se termine par la conjecture suivante [10, p. 139] :

Conjecture 1 (conjecture d'Ehrhart) *Pour tout système linéaire diophantien de dimension quelconque, dépendant linéairement de plusieurs paramètres entiers positifs, le nombre symbolique de solutions entières exprimé en fonction de ces paramètres s'exprime sur plusieurs domaines de valeurs de ces paramètres par différents pseudo-polynômes.*

Nous démontrons cette conjecture dans [2]. Cette extension passe également par une redéfinition des nombres périodiques en tableaux de valeurs rationnelles possibles de dimension égale au nombre de paramètres. Par exemple, $(-1)^{n-m}$ peut être représenté par le tableau à deux dimensions :

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

Le résultat final de notre extension se traduit par le théorème suivant :

Théorème 1 (théorème fondamental d'Ehrhart étendu) *Soit P_N, $N = (n_1, n_2, \ldots, n_p)$, un polytope dans un espace de dimension k, et tel que les coordonnées de ses sommets sont des expressions affines en N. Le nombre de points entiers de P_N est un polynôme à plusieurs variables $n_1, n_2, \ldots, n_p$, de degré k, si P_N est entier, et est un pseudo-polynôme à plusieurs variables $n_1, n_2, \ldots, n_p$, de degré k, et dont la pseudo-période est le dénominateur de P_N, si P_N est rationnel. Ce pseudo-polynôme est de la forme :*

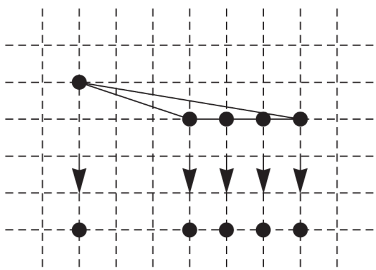
$$pe(n_1, n_2, \ldots, n_p) = \sum_{i_1=0}^{k} \sum_{i_2=0}^{k-i_1} \ldots \sum_{i_3=0}^{k-i_1-i_2-\ldots-i_{p-1}} c_{i_1, i_2, \ldots, i_p} n_1^{i_1} n_2^{i_2} \ldots n_p^{i_p}$$

où les $c_{i1,i2, \ldots, ip}$ sont des nombres périodiques définis par des tableaux de valeurs rationnelles de dimension p.

Notons que bien que les polynômes d'Ehrhart soient une expression paramétrique du nombre de solutions entières, ils servent également au dénombrement des solutions entières de systèmes d'inéquations instanciés, ou non-paramétriques, par simple introduction d'un paramètre «artificiel» dans les inéquations.

III.- Le polynôme d'Ehrhart de la projection affine d'un polytope

La projection affine d'un polytope pose une difficulté supplémentaire. Les points entiers contenus dans un polytope P_N sont organisés en un réseau régulier. Si l'on applique une projection affine à un tel polytope, l'objet géométrique résultant n'est plus, en général, un réseau régulier de points entiers. On ne peut donc plus modéliser ces points par leur enveloppe convexe, comme il est montré sur l'exemple de la figure ci-dessous.



Le dénombrement des points résultants d'une telle projection affine ne peut donc plus s'effectuer par la méthode décrite dans les paragraphes précédents. Toutefois, là aussi, les polynômes d'Ehrhart nous apportent l'information nécessaire au calcul du polynôme d'Ehrhart d'une projection affine d'un polytope (paramétrique ou non). Dans le cas d'une projection d'un polytope paramétrique, nous obtenons le résultat suivant démontré dans [3] :

Théorème 2 *Le nombre de points entiers, résultants d'une projection affine des points entiers contenus dans un polytope paramétrique, est défini sur plu-*

sieurs domaines adjacents de valeurs des paramètres, par différents polynômes d'Ehrhart.

Un exemple d'application informatique de ces résultats à un problème d'accès en mémoire locale (ou mémoire cache) d'un processeur par un programme est décrit dans la suite. Voyons à présent comment le calcul de ces polynômes s'effectue de manière automatique par un ordinateur.

IV.- Le calcul des polynômes d'Ehrhart par ordinateur

Nous avons écrit un programme en langage *C* calculant les polynômes d'Ehrhart (à une ou plusieurs variables) pour n'importe quel polytope entier ou rationnel défini par un système d'inégalités linéaires paramétriques de la forme décrite plus haut. Ce programme se décompose en plusieurs étapes principales de calculs :

1. Lecture du système d'inégalités paramétriques S_N.

2. Calcul des coordonnées paramétriques des sommets de P_N défini par S_N, et des domaines d'existence de ces sommets définis par q contraintes linéaires sur les paramètres, de la forme $C.N \leq D$, où C est une matrice de taille q x p et D un vecteur de taille q. Pour cette étape, nous utilisons un programme écrit par V. Loechner et D.K. Wilde décrit dans [17].
   Chaque domaine de définition des sommets paramétriques correspond à un polytope associé à un unique polynôme d'Ehrhart : les coordonnées des sommets sur un domaine donné sont des combinaisons affines des paramètres.

3. Pour chacun de ces domaines d'existence, calcul du polynôme d'Ehrhart correspondant, par résolutions successives de systèmes d'équations linéaires symboliques.
   Les valeurs initiales numériques nécessaires à la résolution des systèmes s'obtiennent par la détermination préalable de *boucles de parcours* du polytope P_N. Pour le lecteur non familier du jargon informatique, il s'agit de structures de contrôle d'un programme permettant d'effectuer un même traitement sur un domaine convexe de points entiers, par parcours de ce domaine selon l'ordre *lexicographique* des coordonnées. Dans notre cas, ce traitement consiste tout simplement en un dénombrement des éléments de ce domaine d'indices, pour quelques petites valeurs des paramètres.
   Ces boucles de parcours s'obtiennent notamment par la méthode de

Fourier-Motzkin [19], dont nous utilisons une implémentation logicielle.

Exemple 4 Considérons le système d'inégalités linéaires suivant :

$$H_{n,m}\quad \begin{cases} 0 \leq x \leq \frac{m-1}{2} \\ 0 \leq y \leq \frac{m-2x-1}{2} \\ x + y \geq m - n - 1 \\ 1 \leq m \leq 2n + 1 \end{cases}$$

A partir de cette définition du polytope $P_{n,m}$, le programme calcule tout d'abord les coordonnées paramétriques de ses sommets ainsi que leurs domaines d'existence :

- Si $1 \leq m \leq n + 1$ (**domaine 1**), alors les coordonnées des sommets de $P_{n,m}$ sont $(\frac{m-1}{2}, 0)$, $(0, \frac{m-1}{2})$ et $(0,0)$.
- Si $n+1 \leq m \leq 2n + 1$ (**domaine 2**), alors les coordonnées des sommets de $P_{n,m}$ sont $(m - n- 1,0)$, $(\frac{m-1}{2}, 0)$, $(0, m - n- 1)$, $(0, \frac{m-1}{2})$

Sur chacun des domaines 1 et 2, un polynôme d'Ehrhart est calculé. Voyons cela en détail pour le domaine 1.

Le polynôme d'Ehrhart $pe(n,m)$ est exprimé d'abord par un polynôme à une variable (un des paramètres). Son degré est donné par la dimension du polytope $P_{n,m}$, ici 2, et la période des coefficients par son dénominateur, ici 2. D'où $pe(n,m) = c_1 m^2 + [c_2,c_3]\, m + [c_4,c_5]$, où les c_i sont des pseudo-polynômes en n de mêmes caractéristiques. Le calcul des 5 coefficients $c_1, \ldots, c_5$ s'effectue par le système linéaire de 5 équations suivant, utilisant 5 valeurs initiales symboliques $pe(n,1), \ldots, pe(n,5)$:

$$\begin{cases} c_1 + c_2 + c_4 & = & pe(n,1) \\ 4c_1 + 2c_3 + c_5 & = & pe(n,2) \\ 9c_1 + 3c_2 + c_4 & = & pe(n,3) \\ 16c_1 + 4c_3 + c_5 & = & pe(n,4) \\ 25c_1 + 5c_2 + c_4 & = & pe(n,5) \end{cases}$$

La résolution de ce système nécessite le calcul préalable de $pe(n,1), \ldots, pe(n,5)$, qui possèdent tous la même forme générale suivante : $c_1 n^2 + [c_2,c_3]\, n + [c_4,c_5]$. Nous avons donc 5 systèmes linéaires de 5 équations à résoudre, nécessitant chacun la détermination de 5 valeurs numériques initiales. Pour cela, notre programme détermine une boucle de parcours de $P_{n,m}$:

```
init_val := 0 ;
pour x de 0 à (m-1)/2 faire
    pour y de max(0,m-n-x-1) à (m-2*x-1)/2 faire
        init_val := init_val + 1 ;
```

Par exemple, pour le calcul de $pe(n,1)$, nous exécutons 5 fois cette boucle de parcours avec $m = 1$, et en faisant varier la valeur de n à chaque fois, de 1 à 5. Les valeurs numériques ainsi obtenues permettent alors de résoudre le système suivant :

$$\begin{cases} c_1 + c_2 + c_4 = pe(1,1) = 1 \\ 4c_1 + 2c_3 + c_5 = pe(2,1) = 1 \\ 9c_1 + 3c_2 + c_4 = pe(3,1) = 1 \\ 16c_1 + 4c_3 + c_5 = pe(4,1) = 1 \\ 25c_1 + 5c_2 + c_4 = pe(5,1) = 1 \end{cases} \Rightarrow pe\,(n,1) = 1$$

De la même manière, le programme calcule $pe(n,2) = 1$, $pe(n,3) = 3$, $pe(n,4) = 4$, $pe(n,5) = 6$. Le tout premier système peut donc maintenant être résolu :

$$\forall\ \mathrm{m} \in [1..n+1], pe(n, m) = \frac{1}{8}m^2 + \left[\frac{1}{2}, \frac{1}{4}\right]_m + \left[\frac{3}{8}, 0\right]_m$$

L'application des mêmes opérations sur le domaine 2 donne le résultat suivant :

$$\forall\ \mathrm{m} \in [n+1..2n+1], pe(n, m) = nm - \frac{1}{2}n^2 - \frac{1}{2}n - \frac{3}{8}m^2 + \left[1, \frac{3}{4}\right]_m m + \left[\frac{3}{8}, 0\right]_m$$