Advances in parameterized linear diophantine equations for precise program analysis

Philippe Clauss
ICPS, Université Louis Pasteur, Strasbourg
Pôle API, Bd Sébastien Brant
67400 Illkirch FRANCE
e-mail: clauss@icps.u-strasbg.fr

Abstract

In the field of program analysis and transformation of programs, the development of precise and efficient methods requires advances in symbolic and discrete mathematics. In particular, the number of integer solutions of a parametric system of diophantine equations is an answer to many program analysis criteria. Previous results addressed the case of linearly parameterized systems of equations. In this paper, some advances in the computation of the number of integer solutions of non-linearly parameterized systems of equations are presented, allowing to consider a larger set of programs.

Keywords Integer solutions count, diophantine equations, parameterized polytopes, integer points, Ehrhart polynomial, program analysis, symbolic computation.

1 Introduction

Automatic computation of the number of integer solutions of a system of equations or inequations is a fundamental problem in computer science. Beside its basic arithmetical and geometrical interests, it is essential to achieve precise program analysis (number of loop iterations, number of accessed data, exact data dependence analysis, ...) or program optimization. Moreover, a program is often parameterized by several items as the data size input, the computation accuracy, the available resources, ... For example, considering the following loop nest:

```
for i:=0 to n do
  for j:=0 to i + m/2 do
    for k:=0 to i - n + p do
      statement(s)
```

The exact number of iterations computed in this loop is a useful information in order to evaluate the execution time or the required memory. The automatic method presented in our previous work [3, 5, 6] gives the following answer:

if $n > p$ and $m \ mod \ 2 = 0$,
$\frac{1}{2}np^2 + \frac{3}{2}np + n + \frac{1}{4}mp^2 + \frac{3}{4}mp + \frac{1}{2}m - \frac{1}{6}p^3 + \frac{7}{6}p + 1$
if $n \leq p$ and $m \ mod \ 2 = 1$,
$\frac{1}{2}np^2 + \frac{3}{2}np + n + \frac{1}{4}mp^2 + \frac{3}{4}mp + \frac{1}{2}m - \frac{1}{6}p^3 - \frac{1}{4}p^2 + \frac{15}{12}p + \frac{1}{2}$
if $n > p$ and $m \ mod \ 2 = 0$,
$-\frac{1}{6}n^3 - \frac{1}{4}n^2m + \frac{1}{2}n^2p + \frac{1}{2}nmp + \frac{1}{4}nm + \frac{3}{2}np + \frac{7}{6}n + \frac{1}{2}mp + \frac{1}{2}m + p + 1$
if $n \leq p$ and $m \ mod \ 2 = 1$,
$-\frac{1}{6}n^3 - \frac{1}{4}n^2m + \frac{1}{2}n^2p - \frac{1}{4}n^2 + \frac{1}{2}nmp + \frac{1}{4}nm + np + \frac{11}{12}n + \frac{7}{6}n + \frac{1}{2}mp + \frac{1}{2}m + \frac{1}{2}p + \frac{1}{2}$

The ability for parametric analysis also allows to introduce opportune parameters to achieve symbolic transformations of programs.

But the parameters yield hard questions about symbolic computation in the area of parametric linear diophantine equations. In some previous works [3, 5, 6], we have already proposed an algorithm to compute a symbolic expression of the exact number of integer solutions of linear systems of inequations of the form :

$$A \cdot x \leq B \cdot N + c$$

where x is a d-vector of the free variables, N is a symbolic p-vector of parameters, A and B are constant rational matrices of size $(m \times d)$ and $(m \times p)$ respectively, and c is a constant rational m-vector. The symbolic expressions we compute are called *Ehrhart polynomial* since they are originally due to E. Ehrhart [7, 8, 9, 11, 15] whose work inspired our extensions.

This general problem is also geometric, since the considered systems of inequations define parametric convex polytopes. Hence, the number of integer points in these polytopes can also be expressed by Ehrhart polynomials. As an extension, we also proposed in [4] an algorithm to compute the exact number of integer points resulting from an affine transformation on the integer points of a parametric or not parametric polytope.

Observe that the problems we handle at this time are characterized by parameters situated in the constant part of the inequations. This form is the one classically associated with the notion of Ehrhart polynomials in mathematics, since mathematicians generally have a geometrical view talking about dilatation of lattices from a factor n. From now on, our objective is to consider problems where parameters can also be coefficients for some variables. For example, considering the following program sample:

```
for i:=1 to (5*n-1)/(2*n+1)
  for j:=1 to (n+2)*i+3/2
    if (4-2*n)*i+2*j-3 < 0 then
      statement(s)
```

How many times does this program execute the statement(s) ? The results presented in this paper allow to give the exact answer.

Moreover, handling such problems allows many other analyses and optimizations, as optimal time ordering of calculations in parallel programs, complex data dependence analyses, ...

Results presented in this paper are issued from the last Ehrhart's paper dealing with "new" results on Ehrhart polynomials. It is dated from 1973 [10]. It is situated at the frontier of what is nowadays known about the symbolic number of integer solutions defined by a set of parametric rational linear inequalities. It deals with equations of the form $P + nP' > 0$ where P and P' are affine functions $aX + bY + c$, a, b and c are given integers, n is a positive integer parameter and X and Y are the free variables.

Ehrhart has shown in his works several examples of systems with a parameter n as a coefficient, where the number of integer solutions can be expressed as Ehrhart polynomials. He had the strong intuition that such systems can generally be associated to Ehrhart polynomials. The only paper where a general method and an associated theorem are given, is the one mentioned above and entitled *Sur les systèmes d'inéquations diophantiennes linéaires*. Unfortunately, these general results are limited to equations with only two free variables and one parameter n. But the strong difficulty of this problem, as it will be shown in the following, makes these limitations understandable. Assuredly our ambition is to extend these results to any number of parameters and variables, but the first step towards this objective is to well understand the leads given by Ehrhart, and to test the feasibility of an automatic computation method.

This paper is organized as follows. In the second section, some geometrical and arithmetical notions are recalled, required to well understand the third section. In this main section, the results on the computation of the Ehrhart polynomials for systems of inequations of the form:

$$\begin{array}{l} P + nP' > 0 \\ P = aX + bY + c, P' = a'X + b'Y + c \end{array}$$

are detailed, each case being illustrated with an example. In section 4, analysis and comments are made on the feasibility of an automatic method and some possible directions to extend these results to any number of parameters and variables.

2 Some arithmetical and geometrical notions

We first recall some basic notions dealing with geometry of numbers [12, 14] and enumerative combinatorics [15, 16]. Then some more specific concepts, closely related to the content of the paper, are introduced.

A linearly parameterized convex polytope in the set Z^d of integer d-uples is defined by:

$$P_N = \{x \in Z^d \mid A \cdot x \leq B \cdot N + c\}$$

where N is a symbolic p-vector of parameters, A and B are constant rational matrices of size $(m \times d)$ and $(m \times p)$ respectively, and c is a constant rational m-vector.

We denote as j_N the enumerator of P_N, i.e. the number of integer points in P_N. It is formulated using *polynomials* and *pseudo-polynomials* according to the following definitions.

Definition 1 (periodic number) *A one-dimensional periodic number $u(n) = [u_1, u_2, \ldots, u_p]_n$ is equal to the item whose rank is equal to n mod p, p is called the period of $u(n)$.*

$$u(n) = \begin{cases} u_1 & if\ n = 1\ (mod\ p) \\ u_2 & if\ n = 2\ (mod\ p) \\ \ldots & \\ u_p & if\ n = 0\ (mod\ p) \end{cases}$$

Let $N = (n_j)$ be a q-dimensional vector, $j \in [1 \ldots q]$. A q-periodic number $u(N)$ is defined by a q-dimensional array $U_{(i_1,i_2,\ldots,i_q)}$ of size $p_1 \times p_2 \times \ldots \times p_q$ such that

$$u(N) = U_{(i_1,i_2,\ldots,i_q)}$$
$$if\ \forall j \in [1 \ldots q],\ n_j = i_j \bmod p_j$$

The vector $p = (p_j)$ is called the multi-period of $u(N)$ and the least common multiple of the p_i's is called the period of $u(N)$.

For example,

- $(-1)^n = [-1, 1]_n$
- $(-1)^{n-m} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}_{(n,m)}$

Ehrhart in [11] gives the basic properties of one-dimensional periodic numbers which can be easily extended to the multi-dimensional case: Let $u(N)$ and $u'(N)$ be q-periodic numbers of multi-period p and p' respectively. They can be reduced to the same multi-period $m = (m_i)$, where $m_i = p_i\alpha = p'_i\beta$ is the least common multiple of p_i and p'_i, by repeating α times (respectively β times) the sequence of items in the i^{th} dimension of $u(N)$ (respectively $u'(N)$). Since $u(N)$ and $u'(N)$ are reduced to the same period, $u(N) + u'(N) = (u_I + u'_I)_N$ and $u(N)u'(N) = (u_I u'_I)_N$.

Definition 2 (pseudo-polynomial) *A polynomial $f(N)$ is a pseudo-polynomial if some of its coefficients are periodic numbers instead of constants. The least common multiple of the periods of its periodic coefficients is the pseudo-period of $f(N)$. Thus, a pseudo-polynomial has two characteristics, its degree and its pseudo-period.*

The following theorem is the main result of our previous work [6].

Theorem 1 (Ehrhart polynomials) *The enumerator j_N of any k-polytope P_N linearly parameterized, is expressed at different domains of the parameters values by different multi-variable polynomials in N of degree k^p if P_N is integral, and by different multi-variable pseudo-polynomials in N of degree k^p whose pseudo-period is the denominator of P_N if P_N is rational. These polynomials or pseudo-polynomials are of the form:*

$$j_N = \sum_{i_1=0}^{k} \sum_{i_2=0}^{k} \ldots \sum_{i_p=0}^{k} c_{i_1,i_2,\ldots,i_p} n_1^{i_1} n_2^{i_2} \ldots n_p^{i_p}$$

where the $c_{i_1,i_2,\ldots,i_p}$'s are periodic numbers whose dimensions are at most p.

The underlying theory on Ehrhart polynomials includes *rational generating functions.* These functions, which allow the expression of integer series in a general way, can be a better formalism than Ehrhart polynomials, as it is shown in example 4. The following definitions concern systems depending on one parameter, but can be extended to any number of parameters as it was done in [2].

Definition 3 (rational generating function) *A rational generating function is of the form,*

$$F(x) = \sum_{n \geq 0} f(n)x^n = \frac{P(x)}{Q(x)}$$

It is assumed that $Q(0) \neq 0$, so that $Q(x)^{-1}$ exists.

The reader can refer to [16] for further investigations on rational generating functions. Such functions have a dual representation as linear recurrence relations.

Definition 4 (Eulerian recurrence relation) *Let us consider the product*

$$\Pi(u) = (1 - u^{a_1})(1 - u^{a_2}) \ldots (1 - u^{a_s}) \qquad (1)$$

where any $a_i \in Z_+$. When this product is simplified, if each power u^r is replaced by u_{n-r}, it is obtained a linear and homogeneous recurrence relation, denoted by $\{\Pi(u)\} = 0$ and called eulerian recurrence relation. The general solution of such a relation is a pseudo-polynomial. It is determined by some boundary conditions, by a rational generating function $\frac{P(t)}{\Pi(t)} = \sum_0^\infty f(n)t^n$, and it can be reduced to a real polynomial in n of degree k, if $\Pi(t) = (1-t)^{k+1}$.

Such a recurrence relation can be associated to any polytope.

Definition 5 (characteristic product) *The characteristic product of any rational polytope is* (1) *where the a's are the denominators of its vertices.*

It comes that the number of integer points of any rational polytope is determined by the recurrence relation $\{\Pi(u)\} = 0$ deduced from its characteristic product. It is also determined by the generating function $\frac{P(t)}{\Pi(t)}$ associated to the recurrence relation. The number of integer points for a given value of the parameter n will then be the n^{th} term in the Laurent expansion of the generating function.

3 Towards the handling of non-linearly parameterized systems

Our objective is now to consider *non-linearly parameterized polytopes*, defined by:

$$P_N = \{x \in Z^d \mid P + C \cdot N \cdot P' > 0\}$$

where N is the symbolic p-vector of the parameters, C is a constant rational matrix of size $(m \times p)$. P and P' are polynomials of the form $A \cdot x + b$, where A is a constant rational matrix of size $(m \times d)$ and b a rational d-vector. Our first step toward this objective, detailed in this section, is to consider such polytopes when $d = 2$ and $p = 1$.

For an easier understanding, it is given advice to the reader to draw some figures. It was not possible to include such figures in the paper for evident space reasons.

Let us consider a system S_n of inequations of the form $P + nP' > 0$ where P and P' are affine functions $aX + bY + c$ and $a'X + b'Y + c'$ respectively, a, b, a', b', c and c' are given integers, n is a positive integer parameter and X and Y are the free variables. Such a system is said to be *significant* if it defines a polygonal domain P_n (necessarily convex) from a given value n_{min} of n, $n \geq n_{min}$, whose integer points represent the integer solutions of S_n.

If P_n is finite while n is tending to infinity, there is no integer point in the region between P_n and P_∞ from a given value of n. Hence the number of integer points $p(n)$ in P_n is constant in this case. It is therefore more interesting (and difficult) to determine $p(n)$ when P_n becomes infinite with n. In this case, there is at least one vertex of P_n which moves to infinity. Such a vertex is said to be *fleeting*.

If a line $P + nP' = 0$ is constant for any value of n, it will be considered as a particular case of a line with a point always belonging to it (a fixed point), for any value of n. Hence, we assume in the following that neither $\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c}$ nor $a = b = c = 0$.

When n tends to infinity, the line $P + nP' = 0$ can behave in three ways:

- if $ab' - a'b \neq 0$, the line has a fixed point, named the pivot defined by $P = P' = 0$, and tends to a fixed line defined by $P' = 0$. Such a line is called a *pivoting line*.
- if $ab' - a'b = 0$ and not $a' = b' = 0$, the line has a constant direction and tends to a fixed line defined by $P' = 0$. Such a line is called a *directive line*.
- if $a' = b' = 0$, the line has a fixed direction which is the one of $P = 0$ and moves to infinity. Such a line is called a *directional line*.

In this section, each underlying case of the following theorem, which is due to E. Ehrhart [10], are detailed and illustrated with an example.

Theorem 2 *The number of integer solutions of a significant system with two free variables, composed of linear diophantine inequations linearly depending on one positive integer parameter n, is a pseudo-polynomial from a given value of $n \geq n_{min}$.*

A fleeting vertex is defined as the intersection between two lines $P+nP' = 0$ and $Q+nQ' = 0$. Such an homography shows that it can move along a line, an hyperbola or a parabola, which is the hardest case.

Ehrhart's reasoning is based on a decomposition of the domain P_n, by constructing a triangle T_n whose sides are defined by $P + nP' = 0$, $Q + nQ' = 0$ and a fixed line, so that $P_n = T_n + R_n$ where R_n denotes $P_n \backslash T_n$. Since R_n is treated in the same way if necessary, the number of integer points $p(n)$ in P_n is defined by $t(n) + r(n)$, where $t(n)$ and $r(n)$ define respectively the number of integer points in T_n and R_n.

Hence the problem is to show that $t(n)$ can be defined by an Ehrhart polynomial. There are six cases that can occur:

- the fleeting vertex is the intersection of two directional lines (3.1)
- the fleeting vertex is the intersection of a directional line and a directive line (3.2)
- the fleeting vertex is the intersection of a directional line and a pivoting line whose maximum position is parallel to the directional line (3.3)
- the fleeting vertex is the intersection of two pivoting lines whose maximum positions are parallel (3.4)

- the fleeting vertex is the intersection of a directional line D and a pivoting line p whose maximum position is not parallel to the directional line (3.5)
- the fleeting vertex is the intersection of a directional line D and a pivoting line p whose maximum position is parallel to D (3.6)

3.1 The fleeting vertex is the intersection of two directional lines

This case is the "classical" case. It is fully resolved in our previous works for any number of parameters and free variables [3, 5, 6].

3.2 The fleeting vertex is the intersection of a directional line and a directive line

In this case, the directive line d tends to a *rational line* d', i.e. a fixed line $aX + bY + c = 0$ where a, b and c are integers. Hence, from a given value of $n \geq n_{min}$, there is no integer point between d and d'. So the triangle whose sides are defined by d', the directional line and a fixed line is a "classical" homothetic-bordered polytope as defined in our previous works whose Ehrhart polynomial can be computed.

It is even unnecessary to use a triangle, since the constraint which defines the directive line can be simply replaced by the constraint defining the rational line. Let us see an illustrative example.

Example 1 Let us consider the following system:

$$\begin{cases} X + Y & < 2n - 3 \\ (n-2)(2X + 3Y) & > n + 1 \\ X & > 0 \\ Y & < 5 \end{cases}$$

We can observe that the first equation defines a directional line and the second equation defines a directive line. Hence, the directive line tends to a rational line defined by $2X + 3Y = lim_{n \to \infty} \frac{n+1}{n-2} = 1$.

The next line, near to the rational line, which contains integer points is $2X + 3Y = 2$. Hence the number of integer solutions of the initial system for $\frac{n+1}{n-2} < 2$, or $n > 5$, is equal to the one of the following system:

$$\begin{cases} X + Y & < 2n - 3 \\ 2X + 3Y & > 1 \\ X & > 0 \\ Y & < 5 \end{cases}$$

coming under the "classical" case and whose Ehrhart polynomial can be directly computed:

$$\forall n > 5, p(n) = 4n^2 - 8n - 10$$

3.3 The fleeting vertex is the intersection of a directional line and a pivoting line whose maximum position is parallel to the directional line

Since the directive line d tends to a rational line d', and since there is no more any integer point between d and d', from a given value of $n \geq n_{min}$ there is a fixed number of lines parallel to d, and containing integer points between the fleeting vertex V and the pivot of the pivoting line p. Hence the fleeting vertex can be replaced by the vertex V' defined by the intersection of d' and p since the resulting polytope P'_n has the same number of integer points as the original one P_n.

If the equation of d' is of the form $\alpha X + \beta Y = \gamma$ (with α and β relatively prime), and since the maximum position of p is parallel to d, V' is defined by:

$$\left\{ \begin{array}{lll} aX + bY + c + n(k\alpha X + k\beta Y + c') & = 0 & (p) \\ \alpha X + \beta Y & = \gamma & (d') \end{array} \right.$$

Hence, the denominator of V' is $|a\beta - b\alpha|$, giving the form of the Ehrhart polynomial allowing to compute it.

Example 2 Let us consider the following system:

$$\left\{ \begin{array}{ll} 4X + 2Y - 3 - 2nX & < 0 \\ (2n+1)X & < 5n - 1 \\ Y & > 0 \end{array} \right.$$

The first equation defines a pivoting line p whose pivot is the point $P(0, \frac{3}{2})$. The second equation defines a directive line d whose maximum position is the rational line d' defined by $X = \frac{5}{2}$. The nearest line to d' containing integer points is $X = \lfloor \frac{5}{2} \rfloor = 2$. Hence there is no more integer point in d or between d and d' for $\frac{5n-1}{2n+1} > 2$, i.e. $n > 3$.

For any $n > 3$, the fleeting vertex V can be replaced by V' defined by:

$$\left\{ \begin{array}{ll} 4X + 2Y - 3 - 2nX & = 0 \\ X & = \frac{5}{2} \end{array} \right.$$

It comes that the denominator of V' is $|4 \times 0 - 2 \times 1| = 2$.

Let f be the line parallel to $Y = 0$, i.e. the line OX, and containing the pivot P. Since P is a fixed point, the number of integer points in the trapezoid (p, OX, d', f) is constant. The two others vertices of the triangle (p, f, d) are $P(0, \frac{3}{2})$ and $(\frac{5}{2}, \frac{3}{2})$.

Hence, the period of the Ehrhart polynomial is 2: it is of the form $p(n) = c_1 n^2 + [c_2, c_3]n + [c_4, c_5]$. We determine 5 necessary initial values, from $n > 3$: $i_4 = 9, i_5 = 12, i_6 = 15, i_7 = 28, i_8 = 41$. By resolving the following system:

$$\left\{ \begin{array}{ll} 16c_1 + 4c_2 + c_4 & = 9 \\ 25c_1 + 5c_3 + c_5 & = 12 \\ 36c_1 + 6c_2 + c_4 & = 15 \\ 49c_1 + 7c_3 + c_5 & = 28 \\ 64c_1 + 8c_2 + c_4 & = 41 \end{array} \right.$$

we determine the Ehrhart polynomial of P_n:

$$\forall n > 3, p(n) = \frac{5}{2}n^2 - 22n + [\frac{119}{2}, 57]$$

One can think that this example is particular. But for any given directive and pivoting line d and p, such that the maximum position of p, say p', is parallel to d, an unimodular transformation can always be applied, without changing the set of integer points, and such that d and p' are parallel to $X = 0$. The equations of d and p have then the following simple form:

$$(an + b)X = cn + d, \qquad P + n(a'X + b') = 0$$

3.4 The fleeting vertex is the intersection of two pivoting lines whose maximum positions are parallel

Since the maximum positions of the two pivoting lines p and p' are parallel, the fleeting vertex V is defined by:

$$\begin{cases} aX + bY + c + n(k\alpha X + k\beta Y + c') & = 0 \quad (p) \\ a'X + b'Y + c' + n(k'\alpha X + k'\beta Y + c'') & = 0 \quad (p') \end{cases}$$

with α and β relatively prime.

When n tends to infinity, the fleeting vertex moves along an hyperbola whose asymptote Δ is defined by $\alpha X + \beta Y = r$, with r being a rational number.

Let P and P' be respectively the pivots of p and p'. Let us assume that Δ cuts the line segments PP' and PV (the reasoning is similar in the other cases).

Let $p_1(n)$ be the number of integer points inside the triangle (p, Δ, PP'). In the same way as in the precedent case, the period of the Ehrhart polynomial $p_1(n)$ is given by the denominators of the three vertices of (p, Δ, PP'): P, P' and the vertex defined by $\Delta \cap p$ whose denominator is $|a\beta - b\alpha|$.

From a given value of $n \geq n_{min}$, there is no line parallel to Δ between V and Δ which contains integer points. Let $p_2(n)$ be the number of integer points inside the triangle (p', Δ, PP'), the number of integer points in the triangle (p, p', PP') is then $p_1(n) + p_2(n)$. The Ehrhart polynomial $p_2(n)$ of (p', Δ, PP') has a period given by the three vertices P', $PP' \cap \Delta$ and $\Delta \cap p'$ whose denominator is $|a'\beta - b'\alpha|$.

Example 3 Let us consider the following system:

$$\begin{cases} 3X - 2Y - 2 + n(4X - 2Y) & < 0 \\ 3X - Y + n(2X - Y - 1) & > 0 \\ Y & > -4 \end{cases}$$

It defines a triangle bordered by the pivoting line p whose pivot is the point $P(-2, 2)$, the pivoting line p' whose pivot is the point $P'(1, 1)$ and the line f defined by $Y = -4$. When n tends to infinity, the fleeting vertex moves along an hyperbola whose asymptote Δ is defined by $2X - Y = r$, with r being a rational number.

Let M be the point intersection of p and Δ, and M' be the point intersection of p' and Δ. The denominator of M is $|a\beta - b\alpha| = |-3 \times 1 + 2 \times 2| = 1$, and the denominator of M' is $|-3 \times 1 + 1 \times 2| = 1$. Since P and P' are also integer points, the Ehrhart polynomial of the triangle (p, p', PP') is of period 1.

Since the number of integer points in (p, f, p', PP') is obviously constant, i.e., 6 points, the Ehrhart polynomial of the triangle (p, p', f) is also of period 1. Hence, it is of the form $p(n) = c_1 n^2 + c_2 n + c_3$. We count 3 necessary initial values: $p(1) = 10, p(2) = 13, p(3) = 16$, yielding $p(n) = 3n + 7$.

3.5 The fleeting vertex is the intersection of a directional line D and a pivoting line p whose maximum position is not parallel to the directional line

Such a case is defined by the homography:

$$\left\{ \begin{array}{lll} aX + bY + c + n(k\alpha X + k\beta Y + c') & = 0 & (p) \\ a'X + b'Y & = c'n + d' & (D) \end{array} \right.$$

with α and β relatively prime, and $a' > 0$.

When n tends to infinity, the fleeting vertex V moves along an hyperbola whose asymptote Δ is parallel to the maximum position of the pivoting line. The asymptote Δ is defined by:

$$\alpha X + \beta Y = r$$

with r being a rational number.

Let f be the fixed line containing the pivot P and defined by $Y = Y_P$. Hence, the edges of the triangle (p, Δ, f) are defined by:

$$\left\{ \begin{array}{lll} aX + bY + c + n(k\alpha X + k\beta Y + c') & = 0 & (p) \\ \alpha X + \beta Y & = r & (\Delta) \\ Y & = Y_P & (f) \end{array} \right.$$

It is a bordered polytope whose Ehrhart polynomial is characterized by its denominator. This denominator gives an upper bound of the periodicity of the Ehrhart polynomial. A lower bound can be obtained by considering the kernel of the bordered polytope, i.e., the homothetic polytope whose edges are defined by:

$$\left\{ \begin{array}{lll} aX + bY + c + n(k\alpha X + k\beta Y + c') & = 0 & (1) \\ \alpha X + \beta Y & = 0 & (2) \\ Y & = 0 & (3) \end{array} \right.$$

The unique vertex whose denominator is greater than one is defined as the intersection of (1) and (2). Hence, the denominator of (p, Δ, f) is $|a\beta - b\alpha|$.

In the same way, the kernel of the triangle (D, Δ, f) is characterized by the edges:

$$\left\{ \begin{array}{lll} a'X + b'Y & = c'n & (1) \\ \alpha X + \beta Y & = 0 & (2) \\ Y & = 0 & (3) \end{array} \right.$$

The denominator of the vertex defined by the intersection of (1) and (2) is $|a'\beta - b'\alpha|$, the one defined by the intersection of (2) and (3) is 1 and the one defined by the intersection of (1) and (3) is a'. Hence, the periodicity of the Ehrhart polynomial of (D, Δ, f) is the lowest common multiple (lcm) of $|a'\beta - b'\alpha|$ and a', and globally, the one of the triangle (p, D, f) is the lcm of $|a\beta - b\alpha|$, $|a'\beta - b'\alpha|$ and a'.

Example 4 Let us consider the following system:

$$\begin{cases} 3X - 4Y + 3 - 2n(X + Y + 1) & < 0 \\ 2X - Y & < 2n - 1 \\ Y & < 2 \\ X & > -2 \end{cases}$$

It defines a convex quadrilateral (p, D, f, f') where p is pivoting around the point $P(-1, 0)$, D is the directional line defined by $Y = 2X - 2n + 1$ and the fixed lines f and f' are defined respectively by $Y = 2$ and $X = -2$.

The directional line D cuts the X-axis into the point $A(n - \frac{1}{2}, 0)$. The line defined by $Y = 1$ cuts D into the point $B(n, 1)$ and cuts f' into the point $C(-2, 1)$.

According to the first part of this subsection, the periodicity of the Ehrhart polynomial of the triangle (p, D, OX) is the lcm of $|a\beta - b\alpha| = 7$, $|a'\beta - b'\alpha| = 3$ and $a' = 2$, where (a, b), (α, β) and (a', b') are the coefficients of X and Y in the terms $3X - 4Y\,(D)$, $X + Y\,(\Delta)$ and $2X - Y\,(p)$.

Since the denominator of $PABC$ does not change the denominator of the triangle (p, D, OX), the periodicity of the Ehrhart polynomial $EP(n)$ for the whole convex quadrilateral (p, D, f, f') is $7 \times 3 \times 2 = 42$. Hence, $42 \times 2 + 1 = 85$ coefficients have to be computed.

A pseudo-polynomial with 85 coefficients can be unexploitable due to its large size. A better way to express $EP(n)$ could be to determine either the associated linear recurrence relation or the associated generating function. Since the denominators of its vertices are 7, 3 and 2, the characteristic product of (p, D, f, f') is

$$\{(1 - z^2)(1 - z^7)(1 - z^3)\} = \{1 - z^2 - z^3 + z^5 - z^7 + z^9 + z^{10} - z^{12}\}$$

yielding the linear recurrence relation:

$$EP(n) = EP(n-2) + EP(n-3) - EP(n-5) + EP(n-7) - EP(n-9) - EP(n-10) + EP(n-12)$$

where $n - 12 > 1$, since for $n = 1$, the point A is outside the quadrilateral (p, D, f, f'). The initial values of the recurrence relation are counted for $n = 2..13$, $EP(n)$ =5, 7, 10, 13, 19, 24, 29, 37, 43, 51, 59, 69.

From the recurrence relation and its initial values, the corresponding generating function t(z) can be computed, whose n^{th} term in its serie expansion is $EP(n)$. For example, the function `rsolve` in *Maple* gives the following answer:

$$t(z) = \frac{5z^2 + 7z^3 + 5z^4 + z^5 + 2z^6 + 6z^7 + 4z^8 - z^9 - 4z^{10} - z^{11} + 2z^{12} + 2z^{13}}{-1 + z^{12} + z^2 + z^3 - z^5 + z^7 - z^9 - z^{10}}$$

Any n^{th} term in its serie expansion can be directly computed by using the function `rgf_term` from the `genfunc` package in *Maple*. For example, for the 10000^{th} term, it gives the answer $EP(10000) = 33341906$.

3.6 The fleeting vertex is the intersection of a directional line D and a pivoting line p whose maximum position is parallel to D

In such a case, the fleeting vertex moves along a parabola. An unimodular transformation, yielding the same set of integer points and yielding D parallel to the Y-axis, is always possible. Hence, the equations defining D and p', denoting p transformed, can always be considered of the form:

$$(D) \quad X = \frac{en+f}{b} \qquad (p') \quad Y = \frac{cn+d}{a}X$$

where a, b, c, d, e and f are integers.

Let us consider two cases.

3.6.1 The pivot P is an integer point

The integer translation moving the pivot P to the origin O does not change neither the set of integer points nor the form of the two above equations, where the second one defines the line p itself. Hence, the number of integer points in the triangle (D, p, OX) is the number of integer solutions of the system:

$$Y < \frac{cn+d}{a}X, \quad X < \frac{en+f}{b}, \quad Y > 0$$

where a, b, c and e are assumed to be positive.

Let $k = n \div (ab)$ and $r = n \ mod \ (ab)$. So the ordinate Y_i of the point of p whose abscissa equals i is,

$$Y_i = \frac{c(kab + r) + d}{a} i = ikbc + \frac{d + cr}{a} i$$

It comes that the values of Y_i from $i = 1..eka$ are,

$$\left\{\begin{array}{l} Y_1 = kbc + \frac{d+cr}{a} \\ Y_1 = 2kbc + 2\frac{d+cr}{a} \\ \ldots \\ Y_a = akbc + d + cr \end{array}\right.$$
$$\left\{\begin{array}{l} Y_{a+1} = (a+1)kbc + (d+cr) + \frac{d+cr}{a} \\ Y_{a+2} = (a+2)kbc + (d+cr) + 2\frac{d+cr}{a} \\ \ldots \\ Y_{2a} = 2akbc + (d+cr) + d + cr \end{array}\right.$$
$$\ldots$$
$$\left\{\begin{array}{l} Y_{(ek-1)a+1} = [(ek-1)a+1]kbc + (ek-1)(d+cr) + \frac{d+cr}{a} \\ Y_{(ek-1)a+2} = [(ek-1)a+2]kbc + (ek-1)(d+cr) + 2\frac{d+cr}{a} \\ \ldots \\ Y_{eka} = ekakbc + (ek-1)(d+cr) + d + cr \end{array}\right.$$

Let $\overline{Y_i}$ be the number of integer points inside the line segment $(i, 0)(i, Y_i)$. When summing all the Y_i's in each parenthesis, we get the same sum

$$u_r = \frac{d+cr}{a} + 2\frac{d+cr}{a} + 3\frac{d+cr}{a} + \ldots + a\frac{d+cr}{a}$$

Observe that u_r is a periodic number of period ab.

It comes that the whole sum results in,

$$\begin{aligned}\textstyle\sum_{i=1}^{eka}\overline{Y_i} &= kbc[1+2+3+\ldots+eka]+a(d+cr)[1+2+3+\ldots+(ek-1)]+eku_r\\ &= kbc\tfrac{eka(eka+1)}{2}+a(d+cr)\tfrac{ek(ek-1)}{2}+eku_r\end{aligned}$$

Let us assume that $\frac{en+f}{b} \geq eka$ (the reasoning is similar when $\frac{en+f}{b} < eka$). The computation of the number of points for the whole domain needs to consider the Y_i's for $i = eka+1..\lfloor\frac{en+f}{b}\rfloor$, i.e., for $i = eka+1..V_r$ where $V_r = \lfloor\frac{er+f}{b}\rfloor$. It comes that,

$$\begin{aligned}Y_{eka+1} &= (eka+1)kbc+ek(d+cr)+\tfrac{d+cr}{a}\\ Y_{eka+2} &= (eka+2)kbc+ek(d+cr)+2\tfrac{d+cr}{a}\\ &\ldots\\ Y_{eka+V_r} &= (eka+V_r)kbc+ek(d+cr)+V_r\tfrac{d+cr}{a}\end{aligned}$$

Hence,

$$\sum_{i=eka+1}^{eka+V_r}\overline{Y_i} = kbc[V_reka+(1+2+3+\ldots+V_r)]+ek(d+cr)V_r+W_r$$

where W_r is the periodic number of integer points resulting from the sum,

$$W_r = \frac{d+cr}{a}+2\frac{d+cr}{a}+3\frac{d+cr}{a}+\ldots+V_r\frac{d+cr}{a}$$

Finally,

$$\begin{aligned}EP(n) = \textstyle\sum_{i=1}^{eka+V_r}\overline{Y_i} &= \tfrac{k^2}{2}(kea+1)abce+\tfrac{k}{2}(ke-1)ae(d+cr)+keu_r\\ &+k\left[kea+\tfrac{1}{2}(V_r+1)\right]bcV_r+ke(d+cr)V_r+W_r\end{aligned}$$

$EP(n)$ can also be expressed as being,

$$\begin{aligned}EP(n) &= Ak^3+B_rk^2+C_rk+D_r = A\left(\tfrac{n-r}{ab}\right)^3+B_r\left(\tfrac{n-r}{ab}\right)^2+C_r\tfrac{n-r}{ab}+D_r\\ &= A'n^3+B'_rn^2+C'_rn+D'_r\end{aligned}$$

where A and A' are integer constants, B'_r, C'_r and D'_r are periodic numbers of period ab. Hence, $2(ab+1)$ coefficients have to be computed.

3.6.2 The pivot P is a rational point

Let α be the denominator of P. It is always possible by an integer translation, to translate Y_P such that $0 \leq Y_P < 1$, and such that, for a sufficiently big value of n, $0 \leq X_A < 1$, where A is the intersection of p with the new X-axis. The lines D, p' and p are defined by equations of the form,

$$(D)\;\; X = \tfrac{en+f}{b}, \quad (p')\;\; Y' = \tfrac{cn+d}{a}X, \quad (p)\;\; Y = (X-X_P)\tfrac{cn+d}{a}+Y_P \quad (a,b,c,e>0)$$

Let j_n be the number of integer points in the trapezoid (OX, p, D, p') and let i_n and i'_n be the number of integer points in the triangles (p, D, OX) and (p', D, OX). Then for a sufficiently high value of n, $i_n = i'_n - j_n$.

Let $k = n \div (ab\alpha)$ and $r = n\ mod\ (ab\alpha)$. Hence, the equation defining D is

$$(D) \quad X = \frac{e(kab\alpha + r) + f}{b} = kea\alpha + \frac{er + f}{b}$$

And for a given abscissa :

$$\begin{array}{ll} \Delta & = Y' - Y = \frac{cn+d}{a} X_P - Y_P = \frac{\beta n + \omega}{a\alpha} \\ & = \frac{\beta(kab\alpha + r) + \omega}{a\alpha} = kb\beta + \frac{r\beta + \omega}{a\alpha} \end{array}$$

where β and ω are integer constants.

Let $\overline{\Delta}_i$ be the number of integer points in the line segment $((i, Y_i), (i, Y_i'))$. This number is not constant since Y_i and Y_i' are rational numbers. But since the fractional part of any $\overline{\Delta}_i$ is $a\alpha$, we have :

$$\begin{array}{l} \left\{ \begin{array}{l} \overline{\Delta}_1 = kb\beta + u_1 \\ \overline{\Delta}_2 = kb\beta + u_2 \\ \dots \\ \overline{\Delta}_{a\alpha} = kb\beta + u_{a\alpha} \end{array} \right. \\ \left\{ \begin{array}{l} \overline{\Delta}_{a\alpha+1} = kb\beta + u_1 \\ \overline{\Delta}_{a\alpha+2} = kb\beta + u_2 \\ \dots \\ \overline{\Delta}_{2a\alpha} = kb\beta + u_{a\alpha} \end{array} \right. \\ \dots \\ \left\{ \begin{array}{l} \overline{\Delta}_{(ek-1)a\alpha+1} = kb\beta + u_1 \\ \overline{\Delta}_{(ek-1)a\alpha+2} = kb\beta + u_2 \\ \dots \\ \overline{\Delta}_{eka\alpha} = kb\beta + u_{a\alpha} \end{array} \right. \end{array}$$

where the integers $u_1, u_2, \dots, u_{a\alpha}$ are functions depending on r, as it is for their sum s_r. Hence,

$$\sum_{i=1}^{eka\alpha} \overline{\Delta}_i = k^2 ab\alpha\beta e + eks_r$$

Let us assume $er + f \geq 0$ (the reasoning is similar when $er + f < 0$). Let $V_r = \lfloor \frac{er+f}{b} \rfloor$ or $V_r = \lfloor \frac{er+f}{b} \rfloor - 1$, depending if $\frac{er+f}{b}$ is integer or not. Then,

$$\begin{array}{l} \overline{\Delta}_{eka\alpha+1} = kb\beta + u_1 \\ \overline{\Delta}_{eka\alpha+2} = kb\beta + u_2 \\ \dots \\ \overline{\Delta}_{eka\alpha+V_r} = kb\beta + u_{V_r} \end{array}$$

and

$$\sum_{i=eka\alpha+1}^{eka\alpha+V_r} \overline{\Delta}_i = kb\beta V_r + W_r$$

where $W_r = \sum_{i=1}^{V_r} u_i$. Finally,

$$\begin{array}{ll} j_n & = \sum_{i=1}^{eka\alpha+V_r} \overline{\Delta}_i = k^2 ab\alpha\beta e + k(es_r + b\beta V_r) + W_r \\ & = Ak^2 + B_r k + C_r = A\left(\frac{n-r}{ab\alpha}\right)^2 + B_r \frac{n-r}{ab\alpha} + C_r \\ & = A' n^2 + B_r' n + C_r' \end{array}$$

where A and A' are constants and B_r, C_r, B'_r and C'_r are periodic numbers of period $ab\alpha$.

Since the pivot P' of p' is an integer point (the origin $(0,0)$), i'_n is a pseudo-polynomial according to the result of the previous subsection. And since $i_n = i'_n - j_n$, i_n is a pseudo-polynomial of the form :

$$i_n = An^3 + B_{r_1}n^2 + C_{r_2}n + D_{r_2}$$

where A is constant, B_{r_1} is a periodic number of period ab, C_{r_2} and D_{r_2} are periodic numbers of period $ab\alpha$.

Example 5 Let us consider the following system:

$$\begin{cases} -2X - 6Y - 1 + n(2X + 2Y - 1) & > 0 \\ 2X + 2Y & < 2n - 1 \\ X + 2Y & > -2 \end{cases}$$

The maximum position p' of the pivoting line p is parallel to the directional line D. The unimodular transformation defined by:

$$X = 2x - y, \quad Y = -x + y$$

leaves D parallel to the y axis. Hence, the new system is:

$$\begin{cases} 2x - 4y - 1 + n(2x - 1) & > 0 \\ 2x & < 2n - 1 \\ y & > -2 \end{cases}$$

The number of integer points in the so-defined domain is $EP(n) = i_n + j_n$, where i_n is the number of integer points in the triangle (p, D, OX), and j_n is the number of integer points in the trapezoid (p, OX, D, f) (f is the line defined by $y = -2$).

Both equations defining p and D can also be written as:

$$y < \tfrac{n+1}{2}\left(x - \tfrac{1}{2}\right), \quad x < \tfrac{2n-1}{2}$$

According to the general result of this subsection, the number of integer points in (p, D, OX) is given by an Ehrhart polynomial of the following form: $An^3 + B_{r_1}n^2 + C_{r_2}n + D_{r_2}$, where A is constant, B_{r_1} is a periodic number of period $ab = 4$, C_{r_2} and D_{r_2} are periodic numbers of period $ab\alpha = 8$. In fact, (p, OX, D, f) is a trapezoid only for $\frac{n+1}{2} \geq 2$, i.e., $n > 2$. It is easy to determine that $j_n = 2(n-1)$ for $n > 2$. Hence, the number of integer points $EP(n)$ in the whole domain can also be given by an Ehrhart polynomial of the form $An^3+B_{r_1}n^2+C_{r_2}n+D_{r_2}$. So 21 coefficients have to be computed. By use of a scanning loop, initial values of $EP(n)$ for $n = 3..23$ are counted: $EP(n) = 6$, 16, 30, 51, 78, 121, 172, 236, 310, 410, 522, 653, 798, 979, 1176, 1398, 1638, 1924, 2230, 2567, 2926. It comes the following result:

$$\forall n > 2, EP(n) = \frac{n^3}{4} - \frac{n^2}{4} + \left[\frac{5}{4}, \frac{5}{4}, \frac{3}{4}, \frac{5}{4}\right] n + \left[-\frac{5}{4}, -\frac{3}{2}, -\frac{3}{4}, -1\right]$$

The automatic determination of scanning loops for non-linearly parameterized systems can be done using the algorithm described in [1].

4 Some comments and perspectives

Let us consider again the non-linear example given in the introduction of this paper:

```
for i:=1 to (5*n-1)/(2*n+1)
  for j:=1 to (n+2)*i+3/2
    if (4-2*n)*i+2*j-3 < 0 then
      statement(s)
```

Since this problem corresponds to the third case (3.3), the exact number of statement(s) executed by this program can now be directly computed as being:

$$\forall n > 3, \begin{cases} if\ n\ mod\ 2 = 0, & \frac{5}{2}n^2 - 22n + 57 \\ if\ n\ mod\ 2 = 1, & \frac{5}{2}n^2 - 22n + \frac{119}{2} \end{cases}$$

Since our objective is to develop a program computing the Ehrhart polynomial of any non-linearly dependent system, the method has to be decomposed in these successive steps:

1. decomposition of the problem
2. detection of the occurring cases
3. For each occurring case, computation of the Ehrhart polynomial or the generating function
4. summation of all the Ehrhart polynomials

The first step consists in partitioning the problem into parts corresponding to the six cases of the previous section. From a geometrical point of view, the polytope defined by the initial system of inequations is cut by lines separating domains, each being associated to one of the six cases.

The third step involves the use of our previous implementation dealing with the "classical" case, and many additional computations as limits, basis transformations, scanning loops for non-linearly parameterized systems, generating functions, expansion of generating functions, ...

In our existing implementation handling the "classical" case, the number of integer points or integer solutions is expressed by Ehrhart polynomials. But as it was shown in example 4, some cases can occur where a large number of coefficients has to be computed. In such cases, generating function can be a better expression for the result.

Finally, with the perspective of extending the described results to any number of parameters and variables, some necessary computations are not yet known. But some directions for further investigations are given in the conclusion.

Some close work is done in [13], where the authors propose a method to simplify polynomial constraints over integers. It consists in trying to transform the polynomial constraints into a conjunction of affine constraints and one of a special form that is later affinized. But only constraints that can be factored and affinized are handled by the method.

5 Conclusion

Despite the fact that they are limited to one parameter and two variables, results presented in this paper show the feasibility of a general computation method in this case. For example, loop nests depending on two indices and non-linearly depending on one parameter can be precisely analyzed using the presented results.

The next step of this work is trying to generalize these results to any number of parameters and variables. Such extension could be done following different kind of reasoning as:

- decomposition of the problem into several two-dimensional problems
- substitution of variables and/or parameters, factoring
- extension of the same reasoning to higher dimensions, by the definition of pivoting, directive and directional hyperplanes.
- ...

The last way is assuredly the easiest, but would be inapplicable for a general method handling problems of any dimension, the number of cases being exponentially growing.

References

[1] D. Barthou. *Array Dataflow Analysis in Presence of Non-Affine Constraints.* PhD thesis, Université de Versailles - St Quentin, France, 1998.

[2] P. Boissel. Les polynômes d'Ehrhart pour l'analyse et la transformation de programmes parallèles, extensions et applications. Rapport de DEA, Université Louis Pasteur, Strasbourg, France, 1996.

[3] Ph. Clauss. Counting Solutions to Linear and Nonlinear Constraints through Ehrhart polynomials: Applications to Analyze and Transform Scientific Programs. *10th ACM Int. Conf. on Supercomputing*, Philadelphia, May 1996. Also available as Research Report ICPS 96-03. `http://icps.u-strasbg.fr/pub-96/pub-96-03.ps.gz`

[4] Ph. Clauss. Handling Memory Cache Policy with Integer Points Countings. LNCS 1300, pp 285-293, *Euro-Par'97*, Passau, Germany, August 1997.

[5] Ph. Clauss, V. Loechner. Parametric Analysis of Polyhedral Iteration Spaces. *IEEE Int. Conf. on Application Specific Array Processors, ASAP'94*, pp 224-235, Chicago, Illinois, IEEE Computer Society Press, August 1996.

[6] Ph. Clauss, V. Loechner. Parametric Analysis of Polyhedral Iteration Spaces. Extended version, *Journal of VLSI Signal Processing*, Vol. 19, No. 2, Kluwer Academic Pub., July 1998.

[7] E. Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C.R. Acad. Sci. Paris*, 254:616-618, 1962.

[8] E. Ehrhart. Sur un problème de géométrie diophantienne linéaire I. *J. Reine Angew. Math.*, 226:1-29, 1967.

[9] E. Ehrhart. Sur un problème de géométrie diophantienne linéaire II. *J. Reine Angew. Math.*, 227:25-49, 1967.

[10] E. Ehrhart. Sur les systèmes d'inéquations diophantiennes linéaires. *J. Reine Angew. Math.*, 262/263, pp 45-57, 1973.

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

[12] P.M. Gruber and C.G. Lekkerkerker. *Geometry of Numbers*. North-Holland, Amsterdam, 1987.

[13] V. Maslov, W. Pugh. Simplifying Polynomial Constraints Over Integers to Make Dependence Analysis More Precise. Technical report, Univ. of Maryland, CS-TR-3109.1, February, 1994.

[14] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, New York, 1986.

[15] R. P. Stanley. *Combinatorics and Commutative Algebra*. Birkhäuser, Boston, 1983.

[16] R. P. Stanley. *Enumerative Combinatorics Volume I*. Wadsworth & Brooks/Cole, Monterey, California, 1986.