FPSAC 2010, San Francisco, USA DMTCS proc. **AN**, 2010, 203–210

Generalized Ehrhart polynomials

Sheng Chen[1] and Nan Li[2] and Steven V Sam[2†]

[1] *Department of Mathematics, Harbin Institute of Technology, Harbin, China 150001*
[2] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*

Abstract. Let P be a polytope with rational vertices. A classical theorem of Ehrhart states that the number of lattice points in the dilations $P(n) = nP$ is a quasi-polynomial in n. We generalize this theorem by allowing the vertices of $P(n)$ to be arbitrary rational functions in n. In this case we prove that the number of lattice points in $P(n)$ is a quasi-polynomial for n sufficiently large. Our work was motivated by a conjecture of Ehrhart on the number of solutions to parametrized linear Diophantine equations whose coefficients are polynomials in n, and we explain how these two problems are related.

Résumé. Soit P un polytope avec sommets rationelles. Un théorème classique des Ehrhart déclare que le nombre de points du réseau dans les dilatations $P(n) = nP$ est un quasi-polynôme en n. Nous généralisons ce théorème en permettant à des sommets de $P(n)$ comme arbitraire fonctions rationnelles en n. Dans ce cas, nous prouvons que le nombre de points du réseau en $P(n)$ est une quasi-polynôme pour n assez grand. Notre travail a été motivée par une conjecture d'Ehrhart sur le nombre de solutions à linéaire paramétrée Diophantine équations dont les coefficients sont des polyômes en n, et nous expliquer comment ces deux problèmes sont liés.

Keywords: Diophantine equations, Ehrhart polynomials, lattice points, quasi-polynomials

1 Introduction.

In this article, we relate two problems, one from classical number theory, and one from lattice point enumeration in convex bodies. Motivated by a conjecture of Ehrhart and a result of Xu, we study linear systems of Diophantine equations with a single parameter. To be more precise, we suppose that the coefficients of our system are given by polynomial functions in a variable n, and also that the number of solutions $f(n)$ in positive integers for any given value of n is finite. We are interested in the behavior of the function $f(n)$, and in particular, we prove that $f(n)$ is **eventually a quasi polynomial**, i.e., there exists some period s and polynomials $f_i(t)$ for $i = 0, \dots, s-1$ such that for $t \gg 0$, the number of solutions for $n \equiv i \pmod{s}$ is given by $f_i(n)$. The other side of our problem can be stated in a similar fashion: suppose that $P(n)$ is a convex polytope whose vertices are given by rational functions in n. Then the number of integer points inside of $P(n)$, as a function of n, enjoys the same properties as that of f as above. We now describe in more detail some examples and the statements of our results.

† Supported by an NSF graduate fellowship and an NDSEG fellowship.

1.1 Diophantine equations.

As a warmup to our result, we begin with two examples. The first is a result of Popoviciu. Let a and b be relatively prime positive integers. We wish to find a formula for the number of positive integer solutions (x, y) to the equation $ax + by = n$. For a real number x, let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x, and define $\{x\} = x - \lfloor x \rfloor$ to be the fractional part of x. Then the number of such solutions is given by the formula

$$\frac{n}{ab} - \left\{ \frac{na^{-1}}{b} \right\} - \left\{ \frac{nb^{-1}}{a} \right\} + 1,$$

where a^{-1} and b^{-1} satisfy $aa^{-1} \equiv 1 \pmod b$ and $bb^{-1} \equiv 1 \pmod a$. See [BR, Chapter 1] for a proof. In particular, this function is a quasi-polynomial in n.

For the second example which is a generalization of the first example, consider the number of solutions $(x, y, z) \in \mathbf{Z}^3_{\geq 0}$ to the matrix equation

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \tag{1}$$

where the x_i and y_i are fixed positive integers and $x_{i+1}y_i < x_i y_{i+1}$ for $i = 1, 2$. Write $Y_{ij} = x_i y_j - x_j y_i$. We assume that $\gcd(Y_{12}, Y_{13}, Y_{23}) = 1$, so that there exist integers (not unique) f_{ij}, g_{ij} such that

$$\gcd(f_{12}Y_{13} + g_{12}Y_{23}, Y_{12}) = 1, \quad \gcd(f_{13}Y_{12} + g_{13}Y_{23}, Y_{13}) = 1, \quad \gcd(f_{23}Y_{13} + g_{23}Y_{12}, Y_{23}) = 1.$$

Now define two regions $\Omega_i = \{(x, y) \mid \frac{y_i}{x_i} < \frac{y}{x} < \frac{y_{i+1}}{x_{i+1}}\}$ for $i = 1, 2$. Then if $m = (m_1, m_2) \in \mathbf{Z}^2$ is in the positive span of the columns of the matrix in (1), there exist Popoviciu-like formulas for the number of solutions of (1) which depend only on whether $m \in \Omega_1$ or $m \in \Omega_2$, and the numbers $Y_{ij}, f_{ij}, g_{ij}, x_i, y_i$. See [Xu, Theorem 4.3] for the precise statement.

In particular, one can replace the x_i, y_i, and m_i by polynomials in n in such a way that for all values of n, the condition $\gcd(Y_{12}, Y_{13}, Y_{23}) = 1$ holds. For a concrete example, consider the system

$$\begin{pmatrix} 2n+1 & 3n+1 & n^2 \\ 2 & 3 & n+1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3n^3 + 1 \\ 3n^2 + n - 1 \end{pmatrix}.$$

Then for $n \gg 0$, we have that

$$\frac{3}{3n+1} < \frac{3n^2 + n - 1}{3n^3 + 1} < \frac{n+1}{n^2},$$

so that for these values of n, there exists a quasi-polynomial that counts the number of solutions (x, y, z).

Given these examples, we are ready to state our general theorem. We denote by $\mathbf{QP}_{\gg 0}$ the set of functions $f \colon \mathbf{Z} \to \mathbf{Z}$ which are eventually quasi-polynomial.

Theorem 1.1 *Let $A(n)$ be an $m \times k$ matrix, and $b(n)$ be a column vector of length m, both with entries in $\mathbf{Z}[n]$. If $f(n)$ denotes the number of nonnegative integer vectors x satisfying $A(n)x = b(n)$ (assuming that these values are finite), then $f \in \mathbf{QP}_{\gg 0}$.*

This theorem generalizes the conjecture [Sta, Exercise 4.12]. See [Ehr, p. 139] for a conjectural multivariable analogue.

1.2 Lattice point enumeration.

We first recall a classical theorem due to Pick. Let $P \subset \mathbf{R}^2$ be a convex polygon with integral vertices. If $A(P)$, $I(P)$, and $B(P)$ denote the area of P, the number of integer points in the interior of P, and the number of integer points on the boundary of P, respectively, then one has the equation

$$A(P) = I(P) + \frac{1}{2}B(P) - 1.$$

Now let us examine what happens with dilates of P: define $nP = \{nx \mid x \in P\}$. Then of course $A(nP) = A(P)n^2$ and $B(nP) = nB(P)$ whenever n is a positive integer, so we can write

$$A(P)n^2 = I(nP) + \frac{1}{2}B(P)n - 1,$$

or equivalently,

$$\#(nP \cap \mathbf{Z}^2) = I(nP) + B(nP) = A(P)n^2 + \frac{1}{2}B(P)n + 1,$$

which is a polynomial in n. The following theorem of Ehrhart says that this is always the case independent of the dimension, and we can even relax the integral vertex condition to rational vertices:

Theorem 1.2 (Ehrhart) *Let $P \subset \mathbf{R}^d$ be a polytope with rational vertices. Then the function $L_P(n) = \#(nP \cap \mathbf{Z}^d)$ is a quasi-polynomial of degree $\dim P$. Furthermore, if D is an integer such that DP has integral vertices, then D is a period of $L_P(n)$. In particular, if P has integral vertices, then $L_P(n)$ is a polynomial.*

Proof: See [Sta, Theorem 4.6.25] or [BR, Theorem 3.23]. □

The function $L_P(t)$ is called the **Ehrhart quasi-polynomial** of P. One can see this as saying that if the vertices of P are $v_i = (v_{i1}, \ldots, v_{id})$, then the vertices of nP are given by the linear functions $v_i(n) = (v_{i1}n, \ldots, v_{id}n)$. We generalize this as

Theorem 1.3 *Given polynomials $v_{ij}(x), w_{ij}(x) \in \mathbf{Z}[x]$ for $0 \leq i \leq s$ and $1 \leq j \leq d$, let n be a positive integer such that $w_{ij}(n) \neq 0$ for all i, j. This is satisfied by n sufficiently large, so we can define a rational polytope $P(n) = \operatorname{conv}(p^0(n), p^1(n), \ldots, p^s(n)) \in \mathbf{R}^d$, where $p^i(n) = (\frac{v_{i1}(n)}{w_{i1}(n)}, \ldots, \frac{v_{id}(n)}{w_{id}(n)})$. Then $\#(P(n) \cap \mathbf{Z}^d) \in \mathbf{QP}_{\gg 0}$.*

We call the function $\#(P(n) \cap \mathbf{Z}^d)$ a **generalized Ehrhart polynomial**.

2 Equivalence of the two problems

As we shall see, the two problems of the Diophantine equations and lattice point enumeration are closely intertwined. In this section, we want to show that Theorem 1.1 is equivalent to Theorem 1.3. Before this, let us see the equivalence of Theorem 1.3 with the following result. For notation, if x and y are vectors, then $x \geq y$ if $x_i \geq y_i$ for all i.

Theorem 2.1 *For $n \gg 0$, define a rational polytope $P(n) = \{x \in \mathbf{R}^d \mid V(n)x \geq c(n)\}$, where $V(x)$ is an $r \times d$ matrix, and $c(x)$ is an $r \times 1$ column vector, both with entries in $\mathbf{Z}[x]$. Then $\#(P(n) \cap \mathbf{Z}^d) \in \mathbf{QP}_{\gg 0}$.*

Notice that the difference of Theorem 1.3 and Theorem 2.1 is that one defines a polytope by its vertices and the other by hyperplanes. So we will show their equivalence by presenting a generalized version of the algorithm connecting "vertex description" and "hyperplane description" of a polytope.

The connection is based on the fact that we can compare two rational functions $f(n)$ and $g(n)$ when n is sufficiently large. For example, if $f(n) = n^2 - 4n + 1$ and $g(n) = 5n$, then $f(n) > g(n)$ for all $n > 9$, we denote this by $f(n) >_{\text{even}} g(n)$ ("even" being shorthand for "eventually"). Therefore, given a point and a hyperplane, we can test their relative position. To be precise, let $p(n) = (r_1(n), \dots, r_k(n))$ be a point where the $r_i(n)$ are rational functions and let $F(x, n) = a_1(n)x_1 + a_2(n)x_2 + \cdots + a_k(n)x_k = 0$ be a hyperplane where all the $a_i(n)$ are polynomials of n. Then exactly one of the following will be true:

$$F(p, n) =_{\text{even}} 0; \quad F(p, n) >_{\text{even}} 0; \quad F(p, n) <_{\text{even}} 0.$$

Given this, we can make the following definition. We say that two points $p(n)$ and $q(n)$ **lie** (resp., **weakly lie**) **on the same side of** $F(p, n)$ if $F(p, n)F(q, n) >_{\text{even}} 0$ (resp., $F(p, n)F(q, n) \geq_{\text{even}} 0$).

2.1 Equivalence of Theorem 1.3 and Theorem 2.1.

Going from the "vertex description" to the "hyperplane description":

Given all vertices of a polytope $P(n)$, whose coordinates are all rational functions of n, we want to get its "hyperplane description" for $n \gg 0$. Let $F(x, n)$ be a hyperplane defined by a subset of vertices. If all vertices lie weakly on one side of $F(x, n)$, we will keep it together with ≥ 0, or ≤ 0 or $= 0$ indicating the relative position of this hyperplane and the polytope. We can get all the hyperplanes defining the polytope by this procedure.

Going from the "hyperplane description" to the "vertex description":

Let $P(n) = \{x \in \mathbf{R}^d \mid V(n)x \geq c(n)\}$ be a polytope, where $V(x)$ is an $r \times d$ matrix, and $c(x)$ is an $r \times 1$ column vector, both with entries in $\mathbf{Z}[x]$. Without loss of generality, we may assume that $P(n)$ is full-dimensional. We want to find its vertex description. Let $f_1(n), \dots, f_r(n)$ be the linear functionals defined by the rows of $V(n)$. So we can rewrite $P(n)$ as

$$P(n) = \{x \in \mathbf{R}^d \mid \langle f_i(n), x\rangle \geq c_i(n) \text{ for all } i\}.$$

The vertices of $P(n)$ can be obtained as follows. For every d-subset $I \subseteq \{1, \dots, m\}$, if the equations $\{\langle f_i(n), x\rangle = c_i(n) \mid i \in I\}$ are linearly independent for $n \gg 0$, and their intersection is nonempty, then it consists of a single point, which we denote by $v_I(n)$. If $\langle f_j(n), v_I(n)\rangle \geq c_j(n)$ for all j, then $v_I(n) \in \mathbf{Q}(n)^d$ is a vertex of $P(n)$, and all vertices are obtained in this way. We claim that the subsets I for which $v_I(n)$ is a vertex remains constant if we take n sufficiently large. First, the notion of being linearly independent equations can be tested by showing that at least one of the $d \times d$ minors of the rows of $V(n)$ indexed by I does not vanish. Since these minors are all polynomial functions, they can only have finitely many roots unless they are identically zero. Hence taking $n \gg 0$, we can assume that $\{f_i(n) \mid i \in I\}$ is either always linearly dependent or always linearly independent. Similarly, the sign of $\langle f_j(n), v_I(n)\rangle$ is determined by the sign of a polynomial, and hence is constant for $n \gg 0$.

2.2 Equivalence of Theorem 1.1 and Theorem 2.1.

We can easily transform an inequality to an equality by introducing some slack variables and we can also represent an equality $f(n, x) = 0$ by two inequalities $f(n, x) \geq 0$ and $-f(n, x) \geq 0$. So the main difference between the two theorems is that Theorem 1.1 is counting nonnegative solutions while Theorem 2.1 is counting all integral solutions. But we can deal with this by adding constraints on each variable.

A more interesting connection between Theorem 1.1 and Theorem 2.1 is worth mentioning here. First consider any fixed integer n. Then the entries of $A(n)$ and $b(n)$ in the linear Diophantine equations $A(n)x = b(n)$ of Theorem 1.1 all become integers. For an integer matrix, we can calculate its Smith normal form. Similarly, we can use a generalized Smith normal form for matrices over $\mathbf{QP}_{\gg 0}$ to get a transformation from Theorem 1.1 to Theorem 2.1.

Theorem 2.2 *For any matrix $M \in (\mathbf{QP}_{\gg 0})^{k\times s}$, define a matrix function $D\colon \mathbf{Z} \to \mathbf{Z}^{k\times s}$ such that $D(n)$ is the Smith normal form of $M(n)$. Then $D \in (\mathbf{QP}_{\gg 0})^{k\times s}$ and there exists $U \in (\mathbf{QP}_{\gg 0})^{k\times k}$, $V \in (\mathbf{QP}_{\gg 0})^{s\times s}$ such that $U(n), V(n)$ are unimodular (determinant is $+1$ or -1) for $n \gg 0$ and $UMV = D$. We call this matrix function D the* ***generalized Smith normal form*** *of M.*

Then given $A(n)$ and $b(n)$, by Theorem 2.2, we can put $A(n)$ into generalized Smith normal form: $D(n) = U(n)A(n)V(n)$ for some matrix

$$D(n) = (\mathrm{diag}(d_1(n), \ldots, d_r(n), 0, \ldots, 0)|\mathbf{0})$$

with nonzero entries only on its main diagonal, and unimodular matrices $U(n)$ and $V(n)$. Then the equation $A(n)x = b(n)$ can be rewritten as $D(n)V(n)^{-1}x = U(n)b(n)$. Set $y = V(n)^{-1}x$ and $b'(n) = U(n)b(n)$. By the form of $D(n)$, we have a solution y if and only if $d_i(n)$ divides $b'_i(n)$ for $i = 1, \ldots, r$, and for any given solution, the values $y_{r+1}, \ldots, y_k$ can be arbitrary. However, since $V(n)y = x$, we require that $V(n)y \geq 0$, and any such y gives a nonnegative solution x to the original problem. Simplifying $V(n)y \geq 0$, where $V(n) = (v_1(n), \ldots, v_k(n))$, we get $V'(n)X \geq c(n)$, where $V'(n) = (v_{r+1}(n), \ldots, v_k(n))$, $X = (y_{r+1}, \ldots, y_k)$ and $c(n) = -(v_1(n)y_1 + \cdots + v_r(n)y_r)$. Although $V'(n)$ and $c(n)$ has entries in $\mathbf{QP}_{\gg 0}$, we can assume that they are polynomials by dealing with each constituent of the quasi-polynomials separately. So we reduce Theorem 1.1 to Theorem 2.1.

The proof of Theorem 2.2 is based on a theory of generalized division and GCD over the ring $\mathbf{Z}[x]$, which mainly says that for $f(x), g(x) \in \mathbf{Z}[x]$, the functions $\left\lfloor \frac{f(n)}{g(n)} \right\rfloor$, $\left\{ \frac{f(n)}{g(n)} \right\}$, and $\gcd(f(n), g(n))$ lie in the ring $\mathbf{QP}_{\gg 0}$. Once interesting consequence of these results is that every finitely generated ideal in $\mathbf{QP}_{\gg 0}$ is principal, despite the fact that $\mathbf{QP}_{\gg 0}$ is not Noetherian. We developed this theory in order to appoach Theorem 1.1 at first, but subsequently have found a proof that circumvents its use. Further development of these results will appear elsewhere.

3 Lemmas and examples

By the equivalence discussed in Section 2, we only need to prove Theorem 1.1. We give an outline of the proof. The key idea is an elementary "writing in base n" trick, whose use allows us to reduce equations with polynomial coefficients to linear functions. The idea of the following "writing in base n" trick is the following: given a linear Diophantine equation

$$a_1(n)x_1 + a_2(n)x_2 + \cdots + a_k(n)x_k = m(n)$$

with polynomial coefficients $a_i(n)$ and $m(n)$, fix an integer n so that the coefficients all become integers. Now consider a solution $(x_1, x_2, \ldots, x_k)$ with $x_i \in \mathbf{Z}_{\geq 0}$. Substituting the values of $(x_1, x_2, \ldots, x_k)$ into the equation, both sides become integers. Then we use the fact that any integer has a unique representation in base n (n is a fixed number), and compare the coefficient of each power of n in both sides of the equation.

One can show (Lemma 3.1) that the form of this representation in base n is uniform for both sides when n is sufficiently large. Moreover, the coefficient of each power of n in both sides of the equation are all linear functions of n. Using Lemma 3.2, this uniform expression can be reduced to a system of inequalities of the form $f(x) \geq An + B$ where A, B are integers and $f(x)$ is a linear form with constant coefficients. Then by Lemma 3.4, we can reduce these equations with linear coefficients to a case where we can apply Ehrhart's theorem (Theorem 1.2) to show that the number of solutions are quasi-polynomials of n. This completes the proof of Theorem 1.1.

We finish this section with the statements of the above mentioned lemmas and include examples.

Lemma 3.1 *Given $p(x) \in \mathbf{Z}[x]$ with $p(n) > 0$ for $n \gg 0$ (i.e., $p(x)$ has positive leading coefficient), there is a unique representation of $p(n)$ in base n:*

$$p(n) = c_d(n)n^d + \cdots + c_1(n)n + c_0(n),$$

where $c_i(n)$ is a linear function of n such that for $n \gg 0$, $0 \leq c_i(n) \leq n-1$ for $i = 0, 1, \ldots, d$ and $0 < c_d(n) \leq n - 1$. We denote $d = \deg_n(p(n))$.

Note that $\deg_n(p(n))$ may not be equal to $\deg(p(n))$. For example, $n^2 - n + 3$ is represented as $c_1(n)n + c_0(n)$ with $d = 1$, $c_1(n) = n - 1$, and $c_0(n) = 3$.

Now fix a positive integer n. We have a unique expression of any integer x written in base n, if we know an upper bound d of the highest power, as $x = x_d n^d + x_{d-1}n^{d-1} + \cdots + x_1 n + x_0$ with $0 \leq x_i < n$. This gives us a bijection between the set $\{(x_1, \ldots, x_k) \in \mathbf{Z}^k_{\geq 0}\}$ and the set

$$\{0 \leq (x_{ij})_{\substack{1 \leq i \leq k \\ 0 \leq j \leq d - d_i}} < n, x_{ij} \in \mathbf{Z}\}.$$

Then by a direct "base n" comparison starting from the lowest power to the highest power, we have the following lemma.

Lemma 3.2 *For $n \gg 0$, there is a one to one correspondence between the following two sets:*

$$S_1 = \{(x_1, \ldots, x_k) \in (\mathbf{Z}_{\geq 0})^k \mid a_1(n)x_1 + a_2(n)x_2 + \cdots + a_k(n)x_k = m(n)\}$$

where $a_i(n) = \sum_{\ell=0}^{d_i} a_{i\ell} n^\ell$ (as a usual polynomial) with $a_{id_i} > 0$, $i = 1, \ldots, k$, and $m(n) = \sum_{\ell=0}^{d} b_\ell n^\ell$ (represented in base n as in Lemma 3.1), with $b_d > 0$ and $d \geq \max_{1 \leq i \leq k}\{d_i\}$.

$$S_2 = \{0 \leq (x_{ij})_{\substack{1 \leq i \leq k \\ 0 \leq j \leq d - d_i}} < n, x_{ij} \in \mathbf{Z} \mid \text{ all constraints on } x = (x_{ij}) \text{ are of the form } An + B \leq f(x)\}$$

where $A, B \in \mathbf{Z}$ and $f(x)$ is a linear form of x with constant coefficients.

For a lower bound on n in the above lemma, the sum of all absolute value of coefficients $1 + \sum_{i=1}^{k} \sum_{\ell=0}^{d_i} |a_{i\ell}| + \sum_{\ell=0}^{d} |b_\ell|$ is sufficient.

Example 3.3 We give an example of Lemma 3.2. Consider nonnegative integer solutions for

$$2x_1 + (n+1)x_2 + n^2 x_3 = 4n^2 + 3n - 5.$$

For any $n > 5$, RHS $= 4n^2 + 2n + (n-5)$ is the expression in base n. Now consider the left hand side. Writing x_1, x_2, x_3 in base n, let $x_1 = x_{12}n^2 + x_{11}n + x_{10}$, $x_2 = x_{21}n + x_{20}$ and $x_3 = x_{30}$ with $0 \le x_{ij} < n$. Then we have

$$\text{LHS} = (2x_{12} + x_{21} + x_{30})n^2 + (2x_{11} + x_{21} + x_{20})n + (2x_{10} + x_{20}).$$

Now we can write the left hand side in base n with extra constraints on (x_{ij})'s.

We start with comparing the coefficient of n^0 in both sides. We have the following three cases:

$$\begin{aligned} A_0^0 &= \{0 \le 2x_{10} + x_{20} < n, 2x_{10} + x_{20} = n - 5\}, \\ A_1^0 &= \{n \le 2x_{10} + x_{20} < 2n, 2x_{10} + x_{20} = (n-5) + n\}, \\ A_2^0 &= \{2n \le 2x_{10} + x_{20} < 3n, 2x_{10} + x_{20} = (n-5) + 2n\}. \end{aligned}$$

We next consider the n^1 term. If x satisfies A_i^0 for n^0, $i \in I_0 = \{0, 1, 2\}$, then the equation is reduced to

$$(2x_{12} + x_{21} + x_{30})n^2 + (2x_{11} + x_{21} + x_{20} + i)n = 4n^2 + 2n.$$

Now compare the n^1 terms. We have five cases for each $i \in I_0 = \{0, 1, 2\}$.

$$A_{ij}^1 = \{jn \le 2x_{11} + x_{21} + x_{20} + i < (j+1)n,\ 2x_{11} + x_{21} + x_{20} + i = jn + 2\},$$

where $j \in I_1 = \{0, 1, 2, 3, 4\}$.

Last, we compare the n^2 terms. Note that since we assume $n \gg 0$, the n^0 term won't affect the n^2 term, so the computation of n^2 term only depends on the term n^1. If x satisfies the jth condition for n^1, the equation then becomes

$$(2x_{12} + x_{21} + x_{30} + j)n^2 = 4n^2.$$

So for each $j \in I_1$, we have

$$A_j^2 = \{2x_{12} + x_{21} + x_{30} + j = 4\}.$$

Overall, we have the set

$$\{(x_1, x_2, x_3) \in \mathbf{Z}_{\ge 0}^3 \mid 2x_1 + (n+1)x_2 + n^2 x_3 = 4n^2 + 3n - 5\}$$

is in bijection with the set

$$\{x = (x_{12}, x_{11}, x_{10}, x_{21}, x_{20}, x_{30}) \in \mathbf{Z}_{\ge 0}^6, 0 \le x_{ij} < n\},$$

such that x satisfies the conditions

$$\begin{pmatrix} A_0^0 & A_1^0 & A_2^0 \end{pmatrix} \begin{pmatrix} A_{00}^1 & A_{01}^1 & \cdots & A_{04}^1 \\ A_{10}^1 & A_{11}^1 & \cdots & A_{14}^1 \\ A_{20}^1 & A_{21}^1 & \cdots & A_{24}^1 \end{pmatrix} \begin{pmatrix} A_0^2 \\ A_1^2 \\ \vdots \\ A_4^2 \end{pmatrix}.$$

Here we borrow the notation of matrix multiplication AB to represent intersection of sets $A \cap B$ and matrix summation $A + B$ to represent set union $A \cup B$. Note that here all constrains A_i^j on $x = (x_{12}, x_{11}, x_{10}, x_{21}, x_{20}, x_{30})$ are in the form of $An + B \leq f(x)$, where $A, B \in \mathbf{Z}$ and $f(x)$ is a linear form of x with constant coefficients.

The following lemma allows us to reduce these equations (or inequalities) with linear function coefficients to the case when we can apply Ehrhart's theorem (Theorem 1.2) and show that the number of solutions are quasi-polynomials of n.

Lemma 3.4 *If $P(n) \subset \mathbf{R}^d$ is a polytope defined by inequalities of the form $An + B \leq f(x)$, where $A, B \in \mathbf{Z}$ and $f(x)$ is a linear form of x with constant coefficients, then $\#(P(n) \cap \mathbf{Z}^d) \in \mathbf{QP}_{\gg 0}$.*

Example 3.5 For n a positive integer, let $P(n)$ be the polygon defined by the inequalities $x \geq 0$, $y \geq 0$ and $-2x - y \geq -n - 1$. Then $P'(n)$ is defined by the inequalities $x \geq 0$, $y \geq 0$, and $2x + y \leq n$, and $P_1(n)$ is defined by the inequalities $x \geq 0$, $y \geq 0$, and $n + 1 = 2x + y$. We can rewrite the equality as $y = n + 1 - 2x$, and then the other inequalities become $x \geq 0$ and $n + 1 \geq 2x$.

We see that $P'(n)$ is the convex hull of the points $\{(0,0), (0,n), (n/2, 0)\}$, while $P_1(n)$ is the interval $[0, (n+1)/2]$. The total number of integer points in $P'(n)$ and $P_1(n)$ is given by the quasipolynomial

$$\#(P(n) \cap \mathbf{Z}^2) = \begin{cases} k^2 + 3k + 2 & \text{if } n = 2k \\ k^2 + 4k + 4 & \text{if } n = 2k + 1 \end{cases}.$$

Its rational generating function is

$$\sum_{n \geq 0} \#(P(n) \cap \mathbf{Z}^2) t^n = \frac{t^5 - 3t^3 + 4t + 2}{(1 - t^2)^3} = \frac{t^3 - 2t^2 + 2}{(1-t)^3 (1+t)}.$$

References

[BR] Matthias Beck and Sinai Robins, *Computing the Continuous Discretely: Integer-point enumeration in polyhedra*, Undergraduate Texts in Mathematics, Springer, New York, 2007, available for download from `http://math.sfsu.edu/beck/ccd.html`.

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

[Sta] Richard P. Stanley, *Enumerative Combinatorics, Vol. I*, Cambridge Studies in Advanced Mathematics **49**, Cambridge University Press, 1997.

[Xu] Zhiqiang Xu, An explicit formulation for two dimensional vector partition functions, *Integer Points in Polyhedra—Geometry, Number Theory, Representation Theory, Algebra, Optimization, Statistics*, Contemporary Mathematics **452** (2008), 163–178.