

Minimizing the number of lattice points in a translated polygon

Friedrich Eisenbrand*and Nicolai Hähnle

December 3, 2012

Abstract

The parametric lattice-point counting problem is as follows: Given an integer matrix $A \in \mathbb{Z}^{m \times n}$, compute an explicit formula parameterized by $b \in \mathbb{R}^m$ that determines the number of integer points in the polyhedron $\{x \in \mathbb{R}^n : Ax \leq b\}$. In the last decade, this counting problem has received considerable attention in the literature. Several variants of Barvinok's algorithm have been shown to solve this problem in polynomial time if the number n of columns of A is fixed. Central to our investigation is the following question:

Can one also efficiently determine a parameter b such that the number of integer points in $\{x \in \mathbb{R}^n : Ax \leq b\}$ is minimized?

Here, the parameter b can be chosen from a given polyhedron $Q \subseteq \mathbb{R}^m$. Our main result is a proof that finding such a minimizing parameter is NP -hard, even in dimension 2 and even if the parametrization reflects a translation of a 2-dimensional convex polygon. This result is established via a relationship of this problem to arithmetic progressions and simultaneous Diophantine approximation.

On the positive side we show that in dimension 2 there exists a polynomial time algorithm for each fixed k that either determines a minimizing translation or asserts that any translation contains at most $1 + 1/k$ times the minimal number of lattice points.

1 Introduction

As many combinatorial optimization problems can be formulated as an integer program, also their corresponding counting problems can be formulated as the problem of counting integer points in a polytope. Although both problems are hard in general, they can be efficiently solved if the number of variables is fixed. This was shown by Lenstra [Len83] in the case of integer programming and by Barvinok [Bar94] for the integer point counting problem, see also [Bar02, BR07].

A *parametric polyhedron* is a set of the form $P_b = \{x \in \mathbb{R}^n : Ax \leq b\}$ for some matrix $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$. The right-hand-side b is the *parameter* of P_b . Barvinok and Pommersheim [BP99] extended Barvinok's integer point counting algorithm to the parametric case. They describe an algorithm that runs in polynomial time if the dimension is fixed and that computes a *quasipolynomial* whose value at b equals $|P_b \cap \mathbb{Z}^n|$. Since then, several authors described alternative and more efficient algorithms to compute this quasipolynomial [KV08, VW07]. Effective implementations of Barvinok's algorithm have been provided by De Loera et al. [DLHTY04] and by Köppe and Verdoolaege [KV08]. Applications of parametric integer counting can, for example, be found in compiler optimization [VSB⁺07]. Other very interesting, though not polynomial-time approaches to the parametric integer counting problem can for example be found in [Bec00, BDR02, LZ05].

In this paper we consider the problem of finding a parameter $b \in Q$ such that $|P_b \cap \mathbb{Z}^n|$ is minimized. More precisely, we consider the following decision problem.

*Supported by the Alexander von Humboldt Foundation (AvH) and the German Research Foundation (DFG)

INTEGER POINT MINIMIZATION

Given: $A \in \mathbb{Q}^{m \times n}$, a rational polyhedron $Q \subseteq \mathbb{R}^m$, $k \in \mathbb{N}$
Decide: $\exists b \in Q: |\{x \in \mathbb{Z}^n : Ax \leq b\}| \leq k$

We remark that if $k = 0$ and n is fixed, then this problem can be solved in polynomial time with a technique of Kannan [Kan92], see also [ES08].

Contributions of this paper

Our first result is a proof that integer point minimization is *NP*-complete, even if $n = 2$, i.e. the parametric polyhedron resides in the Euclidean plane and then even if the parametric polyhedra are the translations of some convex polygon along the x -axis. In other words, we show that the following problem is *NP*-complete.

POLYGON TRANSLATION

Given: $A \in \mathbb{Q}^{m \times 2}$ and $b \in \mathbb{Q}^m$ defining a convex polygon $P = \{x \in \mathbb{R}^2 : Ax \leq b\} \subseteq \mathbb{R}^2$ and $k \in \mathbb{N}$
Decide: $\exists \lambda, 0 \leq \lambda \leq 1$ such that $P + \begin{pmatrix} -\lambda \\ 0 \end{pmatrix} = \{x + \begin{pmatrix} -\lambda \\ 0 \end{pmatrix} : x \in P\}$ contains at most k integer points.

Clearly, this is an instance of the parametric integer counting problem with $Q \subseteq \mathbb{R}^m$ being the 1-dimensional polytope $Q = \{x \in \mathbb{R}^m : x = b - \lambda a_1, 0 \leq \lambda \leq 1\}$, with a_1 being the first column of A .

Second, we show that there is a polynomial-time approximation scheme for the optimization version of POLYGON TRANSLATION. More precisely, there exists an algorithm that runs in polynomial time for any fixed integer k and either determines a minimizing translation or asserts that any translation contains at most $1 + 1/k$ times the minimal number of lattice points.

This result combines techniques from the geometry of numbers with classical techniques from discrepancy theory. The *discrepancy* of a polygon is the absolute value of the difference between the number of integer points in the polygon and its area. There is a rich literature bounding this discrepancy, see, e.g. [Hux96], starting with *Gauss' circle problem*. Gauss [Gau73] investigated the discrepancy of a disk of radius R around 0. He showed that this discrepancy is bounded by $O(R)$, which implies that the number of integer points is $\Theta(R^2)$ because the area of the disk is πR^2 . Discrepancy bounds also exist for polygons [Hux96], but they involve the *length* of the boundary. Instead, we bound the discrepancy in terms of the *lattice width* of the input polygon: the number of integer points in a polygon of high lattice width is very close to its area. On the other hand, we adapt a technique of Kannan [Kan90] to solve instances with thin polygons exactly.

2 Polygon translation is NP-complete

In this section, we provide our main hardness result. First, we discuss the relation of *arithmetic progressions* with the polygon translation problem.

2.1 Arithmetic progressions and their pulse functions

The *arithmetic progression* defined by the triple (a, k, d) is the set $A = \{a, a + d, a + 2d, \dots, a + kd\}$. We say that a function of the form

$$p(x) = \begin{cases} 0 & \text{if } |x - y| < \varepsilon \text{ for some } y \in A \\ 1 & \text{else} \end{cases}$$

where $\varepsilon > 0$ is a *pulse function*. The next lemma establishes a relation of pulse functions with the polygon translation problem. Figure 1 illustrates the construction with an example.

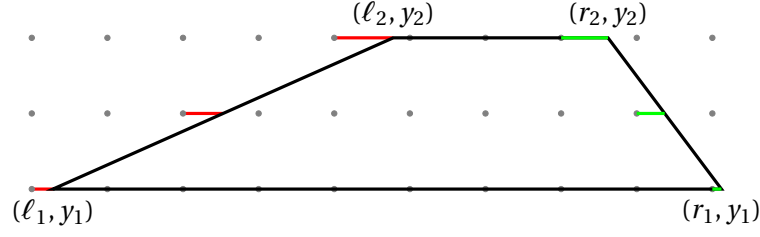


Figure 1: A quadrilateral for a pulse function $p(x)$ defined by the arithmetic progression $\{0.2, 0.45, 0.7\}$ with $\varepsilon = 0.08$. The red line segments have length 0.28, 0.53 and 0.78 (bottom up) and the green line segments have length 0.12, 0.37 and 0.62 (bottom up). As the polygon is translated by x to the left, the number of integer points inside the polygon is $17 + p(x)$.

Lemma 1. Let $p : \mathbb{R} \rightarrow \{0, 1\}$ be a pulse function for the arithmetic progression $A = \{a, a + d, \dots, a + kd\}$ with parameter $0 < \varepsilon \leq \frac{d}{2}$ and discontinuities only in $(0, 1)$. That is, $a - \varepsilon > 0$ and $a + kd + \varepsilon < 1$.

Let $y_1, y_2 \in \mathbb{Z}$ such that $y_2 - y_1 = k$. Consider a convex quadrilateral P with vertices (ℓ_1, y_1) , (r_1, y_1) , (ℓ_2, y_2) , and (r_2, y_2) . If we have

1. $\ell_1 < r_1$ and $\ell_2 < r_2$,
2. $\{\ell_1\} = a + \varepsilon$ and $\{\ell_2\} = a + kd + \varepsilon$,
3. $\{r_1\} = a - \varepsilon$ and $\{r_2\} = a + kd - \varepsilon$, and
4. $k \mid (\lfloor \ell_2 \rfloor - \lfloor \ell_1 \rfloor)$ and $k \mid (\lfloor r_2 \rfloor - \lfloor r_1 \rfloor)$,

then there exists an $M \in \mathbb{N}$ so that

$$|(t \begin{pmatrix} -1 \\ 0 \end{pmatrix} + P) \cap \mathbb{Z}^2| = M + p(\{t\}) \text{ for } t \in [0, 1].$$

Proof. Consider the horizontal slice $L_i = P \cap \{(x, y) \mid y = y_1 + i\}$ for $0 \leq i \leq k$. Using conditions (2) to (4) of the Lemma, one verifies that L_i is a line segment $[\alpha_i, \beta_i] \times \{y_1 + i\}$ with $\{\alpha_i\} = a + id + \varepsilon$ and $\{\beta_i\} = a + id - \varepsilon$. In other words, as the segment sweeps left, an integer point leaves at all times t with $\{t\} = \{\beta_i\} = a + id - \varepsilon$, and an integer point enters at all times t with $\{t\} = \{\alpha_i\} = a + id + \varepsilon$. Taking into account that L_i is relatively closed, one has

$$|(t \begin{pmatrix} -1 \\ 0 \end{pmatrix} + L_i) \cap \mathbb{Z}^2| = M_i + \begin{cases} 0 & \text{if } a + id - \varepsilon < \{t\} < a + id + \varepsilon \\ 1 & \text{otherwise} \end{cases}$$

for some $M_i \in \mathbb{N}$. In fact, $M_i = \lfloor \beta_i \rfloor - \lceil \alpha_i \rceil$.

Summing over all L_i , $0 \leq i \leq k$, and using the fact that the intervals $(a + id - \varepsilon, a + id + \varepsilon)$ are pairwise disjoint, we obtain the claim of the Lemma. \square

Next we consider a decision problem involving several pulse functions.

ARITHMETIC PROGRESSION MEETING

Given: pulse functions p_1, \dots, p_n (encoded as their parameters $a^{(j)}, k^{(j)}, d^{(j)}, \varepsilon^{(j)} \in \mathbb{Q}$)

Decide: $\exists x \in \mathbb{R} : p(x) = \sum_{j=1}^n p_j(x) = 0$

We delay the proof of the next theorem to Section 2.2.

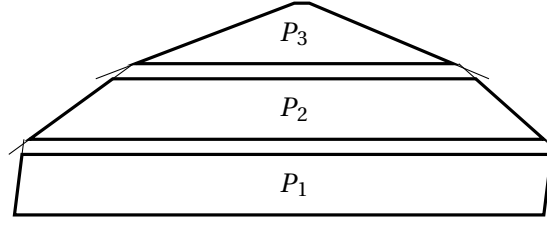


Figure 2: The construction of P in the proof of Theorem 3.

Theorem 2. *Arithmetic Progression Meeting is NP-hard.*

We are now in the position to prove that POLYGON TRANSLATION is NP-complete. In our reduction to arithmetic progression meeting, we restrict ourselves to pulse functions whose discontinuities lie in the open interval $(0, 1)$. We can always reduce to this special case using an affine transformation of the pulse functions, so that this restriction is without loss of generality.

Theorem 3. *Polygon Translation is NP-hard.*

Proof. Let $p_1, \dots, p_n : \mathbb{R} \rightarrow \{0, 1\}$ be an instance of Arithmetic Progression Meeting. We will assume without loss of generality that all discontinuities of the p_j lie in the open interval $(0, 1)$. Let $p = \sum_{j=1}^n p_j$. The goal is to construct a convex polygon P such that

$$|(t \begin{pmatrix} -1 \\ 0 \end{pmatrix} + P) \cap \mathbb{Z}^2| = M + p(\{t\}) \text{ for all } t \in \mathbb{R}$$

for some $M \in \mathbb{N}$. Then P , $v = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, and M form an instance of Polygon Translation which is a Yes-instance if and only if p_1, \dots, p_n is a Yes-instance for Arithmetic Progression Meeting.

The idea for the construction of P is straightforward. Lemma 1 gives us a tool for constructing quadrilaterals P_1, \dots, P_n corresponding to the pulse functions p_1, \dots, p_n , which we then stack vertically to form the polygon P with $2n + 2$ edges. This is illustrated in Figure 2.

Formally, we define the polygon P as the convex polygon constrained by $2n + 2$ lines: the $2n$ lines defined by the left and right edges of the P_j , and the lines through the bottom edge of P_1 and the top edge of P_n . We will argue that, given a proper choice of coordinates for the P_j , the resulting polygon P satisfies the following properties:

1. P has $2n + 2$ edges: the bottom edge of P_1 , the top edge of P_n , and n edges each on the left and right sides, which are extensions of the left and right edges of the P_j , respectively.
2. P has $2n + 2$ vertices: the two bottom vertices of P_1 , the two top vertices of P_n , and $2(n - 1)$ vertices which are obtained as the intersection points of lines through the left or right edges of adjacent P_j .
3. Any horizontal translate of P contains exactly the same integer points as the union of the corresponding translates of the P_j .

The last property is the result that we really need for the reduction. The first two properties merely guide us along during the proof.

We will use the same notation as in Lemma 1, but with superscripts indicating which polygon P_j we are talking about. We choose $y_1^{(j+1)} = y_2^{(j)} + 1$ for all $j = 1 \dots n - 1$, and $y_2^{(j)} = y_1^{(j)} + k^{(j)}$ for all

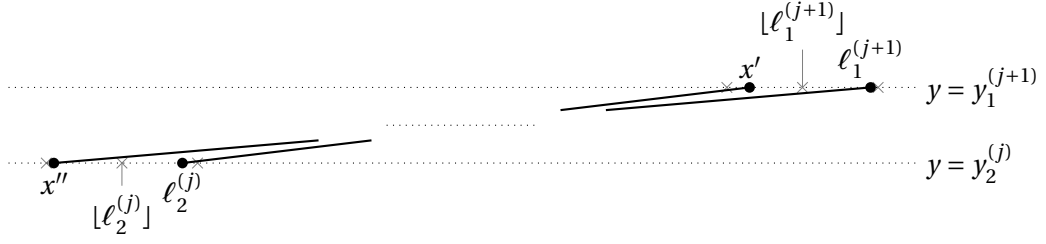


Figure 3: Intersection of the lines through the left edges of P_j and P_{j+1} in the proof of Theorem 3.

$j = 1 \dots n$. We then choose

$$\begin{aligned} \lfloor \ell_2^{(j)} \rfloor &= \lfloor \ell_1^{(j)} \rfloor + k^{(j)} \cdot (3j) \\ \lfloor \ell_1^{(j+1)} \rfloor &= \lfloor \ell_2^{(j)} \rfloor + 3j + 2 \end{aligned}$$

The fractional part of the $\ell_i^{(j)}$ is chosen to satisfy the conditions of Lemma 1. Observe that this fixes the $y_i^{(j)}$ and $\ell_i^{(j)}$ up to an integer translation of P .

Let us describe how our choice of the $\lfloor \ell_i^{(j)} \rfloor$ establishes the first two properties listed above on the left side of P . Observe that the slopes of the left edges of the P_j are strictly decreasing: the slope of the left edge of P_{j+1} is always strictly less than the slope of the left edge of P_j .

Furthermore, we claim that the lines through the left edges of P_j and P_{j+1} intersect in a point (x, y) with $y_2^{(j)} < y < y_1^{(j+1)}$; that is, they intersect “between” P_j and P_{j+1} . To see this, consider the point (x', y') where the line through the left edge of P_j intersects the horizontal line $y = y_1^{(j+1)}$. By our choice of the $\lfloor \ell_i^{(j)} \rfloor$, we know that

$$x' < \ell_2^{(j)} + 3j + 1 < \lfloor \ell_2^{(j)} \rfloor + 3j + 2 = \lfloor \ell_1^{(j+1)} \rfloor.$$

On the other hand, if (x'', y'') is the intersection of the line through the left edge of P_{j+1} with the horizontal line $y' = y_2^{(j)}$, then

$$x'' < \ell_1^{(j+1)} - 3(j+1) < \lfloor \ell_1^{(j+1)} \rfloor - 3j - 2 = \lfloor \ell_2^{(j)} \rfloor.$$

This establishes the claim. The situation is illustrated in Figure 3.

An analogous choice of coordinates is used for the right edges of the P_j , to obtain negative slopes with strictly decreasing absolute value, and well-placed intersection points of the lines through right edges of adjacent P_j .

Together, these properties imply that the boundary of P is indeed an extension of the boundaries of the P_j . In particular, every horizontal slice of P with integer vertical coordinates coincides with a slice of one of the P_j , and vice versa. This establishes also the third property listed above. Hence

$$\left| t \begin{pmatrix} -1 \\ 0 \end{pmatrix} + P \right| = \sum_{j=1}^n \left| t \begin{pmatrix} -1 \\ 0 \end{pmatrix} + P_j \right| = \sum_{j=1}^n (M^{(j)} + p_j(\{t\})) = \underbrace{\left(\sum_{j=1}^n M^{(j)} \right)}_{=: M} + p(\{t\})$$

for all $t \in \mathbb{R}$, which completes the reduction. \square

2.2 Simultaneous Diophantine approximation and arithmetic progression meeting

Dirichlet's theorem is a classical result in number theory about the approximation of a vector of real numbers using rational numbers of equal denominator, see e.g. [HW08, chapter 11]. It states that given $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ and $Q \in \mathbb{N}$, there exist $q \in \{1, \dots, Q\}$ and $p_1, \dots, p_n \in \mathbb{Z}$ such that

$$|\alpha_j - \frac{p_j}{q}| \leq \frac{1}{qQ^{1/n}} \quad \text{for all } j = 1 \dots n$$

This result is best possible up to constants for the general case. However, we may ask whether a better approximation is possible for a specific set of numbers. This motivates the following decision problem, which was shown to be *NP*-hard by Lagarias [Lag85].

SIMULTANEOUS DIOPHANTINE APPROXIMATION

Given: $\alpha_1, \dots, \alpha_n \in \mathbb{Q}, Q \in \mathbb{N}, \varepsilon > 0$

Decide: $\exists q \in \{1, \dots, Q\}$ such that $|q\alpha_j - \lceil q\alpha_j \rceil| \leq \varepsilon$ for all $j = 1 \dots n$

We use $\lceil \cdot \rceil$ to denote the nearest integer (breaking ties by rounding down). For computational purposes, the α_j must be rational numbers, though their denominators will typically be much larger than Q .

Proof of Theorem 2. Let $\alpha_1, \dots, \alpha_n \in \mathbb{Q}, Q \in \mathbb{N}, \varepsilon > 0$ be an instance of Simultaneous Diophantine Approximation. We assume without loss of generality that $\alpha_j \in (0, 1)$.

We will define an instance of Arithmetic Progression Meeting with pulse functions p_0, p_1, \dots, p_n as follows. We scale numerators and denominators so that the denominators of the α_j and ε are all equal and we denote their common denominator by D . For every $j = 1 \dots n$, let

$$p_j(x) = \begin{cases} 0 & |x - \frac{i}{\alpha_j}| < \frac{\varepsilon}{\alpha_j} + \frac{1}{2D} \text{ for some } i \in \{0, 1, \dots, \lceil Q\alpha_j \rceil\} \\ 1 & \text{else} \end{cases}$$

The intuition behind this definition is that we would like to have $p_j(x) = 0$ if and only if $|x\alpha_j - \lceil x\alpha_j \rceil| \leq \varepsilon$ as in the definition of simultaneous Diophantine approximation. The correction term $\frac{1}{2D}$ is needed due to the strict inequality required in pulse functions. Furthermore, we define

$$p_0(x) = \begin{cases} 0 & |x - i| < \frac{1}{2D} \text{ for some } i \in \{1, 2, \dots, Q\} \\ 1 & \text{else} \end{cases}$$

It remains to be shown that the original instance of Simultaneous Diophantine Approximation is a Yes-instance if and only if $p = \sum_{j=0}^n p_j$ has a root.

Suppose $q \in \{1, \dots, Q\}$ satisfies $|q\alpha_j - \lceil q\alpha_j \rceil| \leq \varepsilon$ for all $j = 1 \dots n$. Then dividing by α_j yields

$$|q - \frac{\lceil q\alpha_j \rceil}{\alpha_j}| \leq \frac{\varepsilon}{\alpha_j}$$

and hence one obtains $p(q) = 0$.

Conversely, suppose that $p(q) = 0$. Define $\hat{q} := \lceil q \rceil$. As $p_0(q) = 0$, we have $\hat{q} \in \{1, \dots, Q\}$. Furthermore, $|q - \hat{q}| < \frac{1}{2D}$. Let $i_j \in \{0, \dots, \lceil Q\alpha_j \rceil\}$ with $|q - i_j/\alpha_j| < \varepsilon/\alpha_j + 1/(2D)$. Then

$$\begin{aligned} |q - i_j/\alpha_j| &= |\hat{q} + q - \hat{q} - i_j/\alpha_j| \\ &\geq |\hat{q} - i_j/\alpha_j| - |q - \hat{q}| \\ &\geq |\hat{q} - i_j/\alpha_j| - 1/(2D) \end{aligned}$$

From this, it follows that

$$|\hat{q} - i_j/\alpha_j| < \varepsilon/\alpha_j + 1/D$$

and since $\alpha_j \in (0, 1)$ also that

$$|\hat{q}\alpha_j - i_j| < \varepsilon + 1/D.$$

Since the denominator of α_j and ε is D one has

$$|\hat{q}\alpha_j - i_j| \leq \varepsilon$$

which shows that \hat{q} is a solution to simultaneous Diophantine approximation. □

3 A polynomial time approximation scheme

In this section, we show the following theorem, which implies a polynomial time approximation scheme for the POLYGON TRANSLATION problem.

Theorem 4. *For every $k \in \mathbb{N}$, there is a polynomial-time algorithm which, given a polygon P and a direction $v \in \mathbb{Z}^2$ as input, either computes a translate $tv + P$ containing a minimal number of integer points or asserts that every translate of P is a $(1 + 1/k)$ -approximation to the optimal solution.*

The intuition behind this result is that when P is small, we can use integer programming in fixed dimension and adapt a technique of Kannan [Kan90] to find an optimum. On the other hand, if P is large and contains many lattice points, then only a small fraction of them is close to the boundary, and hence the *discrepancy* relative to the average number of lattice points that one expects based on the area of P is small.

This idea goes back to Gauss' circle problem. Gauss showed that as r grows, the number of integer points $L(r)$ in a disk of radius r is asymptotically equal to its area, πr^2 . In fact, he gave a bound on the error term $|L(r) - \pi r^2|$ that is linear in r . The heart of the argument lies in counting unit squares intersecting the disk and showing that only $O(r)$ of them lie near the boundary. Observe that if one transforms the setting of Gauss' circle problem by a linear map, the disk becomes an ellipse E and \mathbb{Z}^2 becomes a general lattice Λ . Instead of unit squares we now count fundamental parallelepipeds of Λ ; the trick is to use the right parallelepiped.

The dual of a lattice Λ is $\Lambda^* = \{y \in \mathbb{R}^2 : \forall x \in \Lambda : y^T x \in \mathbb{Z}\}$. The *width* $w_y(K)$ of a convex body K along a dual lattice vector $y \in \Lambda^* \setminus \{0\}$ is defined as

$$w_y(K) := \max_{x \in K} y^T x - \min_{x \in K} y^T x.$$

The *lattice width* $w(K)$ of K is the minimum over all choices of $y \in \Lambda^* \setminus \{0\}$. Note that in the linear transformation of Gauss' circle problem, the diameter of the disk becomes the lattice width of the ellipse E . The lattice width and the corresponding dual lattice vector can be computed efficiently in fixed dimension [?]. x

Theorem 5. *For every lattice $\Lambda \subset \mathbb{R}^2$ and convex body $K \subseteq \mathbb{R}^2$ with lattice width at least $k \geq 1$, one has $|N - \frac{\text{vol}(K)}{\det(\Lambda)}| \leq \frac{3}{2k} \frac{\text{vol}(K)}{\det(\Lambda)}$, where $N = |K \cap \Lambda|$.*

Proof. Using a linear transformation, we can assume that the Löwner-John ellipsoid [Bal97] of K is a unit disk centered at some $z \in \mathbb{R}^2$:

$$B(z, 1) \subseteq K \subseteq B(z, 2)$$

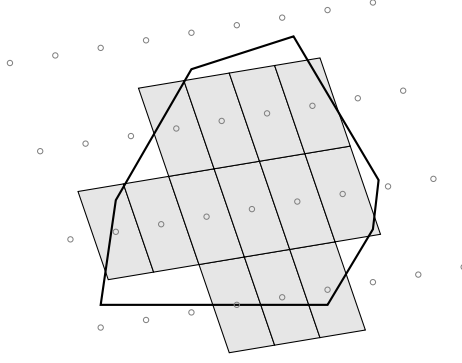


Figure 4: The set $\mathcal{P}(K)$ from the proof of Theorem 5.

Let $B = (b_1, b_2)$ be a reduced basis of the dual lattice Λ^* . In other words, $\|b_1\| \leq \|b_2\|$ and its Gram-Schmidt orthogonalization satisfies

$$b_2 = b_2^* + \mu b_1, \quad b_2^* \perp b_1, \quad |\mu| \leq \frac{1}{2}. \quad (1)$$

It is well known that b_1 is a shortest non-zero lattice vector. Thus it is the lattice width direction of disks. In particular, $4\|b_1\| = w(B(z, 2)) \geq w(K) \geq k$. Let

$$\mathcal{P} = \{x \in \mathbb{R}^2 : 0 \leq b_1^T x < 1 \text{ and } 0 \leq b_2^T x < 1\}$$

be the fundamental parallelepiped of Λ associated to B and let $\overline{\mathcal{P}}$ be its closure. We relate the lattice points in K to the area of K by centering one copy of \mathcal{P} at each lattice point, see Fig. 4:

$$\mathcal{P}(K) = (K \cap \Lambda) \pm \frac{1}{2} \mathcal{P} = \bigcup_{x \in K \cap \Lambda} x \pm \frac{1}{2} \mathcal{P}.$$

Let $R = \partial K \pm \frac{1}{2} \overline{\mathcal{P}}$. We have

$$K \setminus R \subseteq \mathcal{P}(K) \subseteq K \cup R.$$

Since K is a convex body, we can estimate

$$\text{vol}(R \setminus K) \leq \text{vol}((K + B(0, \delta)) \setminus K) \leq |\partial K| \delta + \pi \delta^2,$$

where $|\partial K|$ is the length of the boundary and δ is the radius of \mathcal{P} . By Lemma 6 below, we have $\delta \leq \frac{1.2}{\|b_1\|} \leq \frac{1}{3k}$. Furthermore, $|\partial K| \leq |\partial B(z, 2)| = 4\pi$ because K is convex and contained in $B(z, 2)$.

$$\text{vol}(R \setminus K) \leq \frac{4\pi}{3} \frac{1}{k} + \frac{\pi}{9k} \frac{1}{k} \leq \frac{3}{2k} \text{vol}(K),$$

where the last inequality follows from $\text{vol}(K) \geq \text{vol}(B(z, 1)) = \pi$ and $k \geq 1$. It follows that

$$\text{vol}(\mathcal{P}(K)) \leq \text{vol}(K) + \text{vol}(R \setminus K) \leq \text{vol}(K) + \frac{3}{2k} \text{vol}(K).$$

A lower bound follows from an analogous argument, and combining these inequalities with $\text{vol}(\mathcal{P}(K)) = N \cdot \text{vol}(\mathcal{P}) = N \cdot \det(\Lambda)$ yields the statement of the Theorem. \square

Lemma 6. *Let $B = (b_1, b_2)$ be a reduced basis of Λ^* and $\mathcal{P} = \{x \in \mathbb{R}^2 : 0 \leq b_1^T x < 1 \text{ and } 0 \leq b_2^T x < 1\}$ the associated fundamental parallelepiped of Λ . Then the diameter d of \mathcal{P} is bounded by $d \leq \frac{2.4}{\|b_1\|}$.*

Proof. Using the triangle inequality, we bound $d \leq \|x\| + \|y\|$, where x and y are vertices of \mathcal{P} adjacent to 0. In particular, let x be the vertex satisfying $b_1^T x = 0$ and $b_2^T x = 1$. Using notation from the proof of Theorem 5, we compute $(b_2^*)^T x = b_2^T x + \mu b_1^T x = 1$. Since $x \perp b_1$ and hence x is parallel to b_2 , we get

$$\|x\|^2 = \frac{1}{\|b_2^*\|^2} \leq \frac{4}{3} \frac{1}{\|b_1\|^2}.$$

The inequality follows from (1) and $\|b_1\| \leq \|b_2\|$. Similarly, let y be the vertex satisfying $b_1^T y = 1$ and $b_2^T y = 0$. We compute $(b_2^*)^T y = b_2^T y - \mu b_1^T y = -\mu$, and conclude using Pythagoras' theorem:

$$\|y\|^2 \leq \frac{1}{\|b_1\|^2} + \frac{\mu^2}{\|b_2^*\|^2} \leq \frac{1}{\|b_1\|^2} + \frac{4}{3} \frac{\mu^2}{\|b_1\|^2} \leq \frac{4}{3} \frac{1}{\|b_1\|^2}.$$

The statement of the lemma follows from $2\sqrt{4/3} = 2.309\dots$ □

In the second part of this section, we will show how to find an optimal translate when the lattice width of P is at most a constant. We extend a technique which was introduced by Kannan for parametric integer programming [Kan90]. Kannan determines the lattice width direction of the parametric polyhedron P_b as a function of the parameter b , and partitions the parameter space according to width direction and according to how the respective lattice hyperplanes interact with the boundary of the polyhedron. In our case, the lattice width direction is the same for all parameters, since we only translate the input polygon. We partition the parameter space only based on interactions of the boundary of $t\nu + P$ with the lattice hyperplanes orthogonal to the width direction of P . Our main extension is that we encode counting the number of integer points on lattice slices in an integer program, where Kannan's work only tested for feasibility. Our approach is compatible with partitioning the parameter space based on the lattice width direction, and hence the following Lemma can be extended to even more general 2-dimensional INTEGER POINT MINIMIZATION problems, provided that the lattice width is bounded by a constant for all possible parameter values.

Lemma 7. *Given a dual lattice vector $y \in \mathbb{Z}^2 \setminus \{0\}$ such that $w_y(P) \leq k$, the optimal translate of P in direction $v \in \mathbb{Z}^2$ can be computed in time $2^{O(k \log k)} b^{O(1)}$, where b is the encoding length of P , v , and y .*

Proof. Using a unimodular transformation if necessary, we can assume without loss of generality that $y = e_1$. Let us sketch a simple algorithm to compute the number of integer points in a translate $t\nu + P$. Let us denote $\beta = \min_{x \in t\nu + P} e_1^T x$ the first coordinate of the leftmost point in the translate. Let

$$S_i = (t\nu + P) \cap \{x \in \mathbb{R}^2 : x_1 = \lceil \beta \rceil + i\}, i = 0 \dots k$$

denote the integral vertical slices of $t\nu + P$. Note that some of the S_i may be empty. For each slice, we can compute the lower end a_i and upper end b_i and write $S_i = \{\lceil \beta \rceil + i\} \times [a_i, b_i]$. It follows that

$$|(t\nu + P) \cap \mathbb{Z}^2| = \sum_{i=0}^k |S_i \cap \mathbb{Z}^2| = \sum_{i=0}^k \lfloor b_i \rfloor - \lceil a_i \rceil + 1$$

We will argue that this algorithm can be encoded into a small number of integer programs that allow us to find the optimal t . We start by writing down the minimization of the number of integer points

based on the a_i and b_i .

$$\begin{aligned}
\min \sum_{i=0}^k y_i & \\
y_i &\geq B_i - A_i + 1 & (\forall i) \\
y_i &\geq 0 & (\forall i) \\
b_i - 1 &< B_i \leq b_i & (\forall i) \\
a_i &\leq A_i < a_i + 1 & (\forall i) \\
A_i, B_i &\in \mathbb{Z} & (\forall i)
\end{aligned}$$

We can obtain $\gamma = \lceil \beta \rceil$ similarly:

$$\begin{aligned}
\beta &= \beta_0 + tv_1 \\
\beta &\leq \gamma < \beta + 1 \\
\gamma &\in \mathbb{Z},
\end{aligned}$$

where we precompute β_0 as the value of β for $t = 0$. The only remaining task is to encode the computation of the a_i and b_i given t and γ .

Suppose that we know which edge of $tv + P$ the point $(\gamma + i, a_i)$ lies on, and suppose that the corresponding edge of P lies on the straight line defined by $c^T x = d$. Then a_i is defined uniquely by the equation

$$c^T(\gamma + i, a_i)^T - c^T tv = d,$$

hence we can express a_i as a linear function in t and γ and add a corresponding constraint to the integer program.

Unfortunately, the point $(\gamma + i, a_i)$ does not always lie on the same edge. Let us separate the translation of the polygon into a horizontal and a vertical component, because a vertical translation does not affect the incidence between edges and vertical lines. As the polygon is translated horizontally, the point $(\gamma + i, a_i)$ moves onto a different edge of the polygon when a corresponding vertex of the polygon crosses the vertical line $x_1 = \gamma + i$. Over all points $(\gamma + i, a_i)$ and $(\gamma + i, b_i)$, such an event happens n times – once per vertex – for one unit of horizontal movement.

Hence we can separate $[0, 1)$ into intervals I_1, \dots, I_n with the property that the combinatorics of incidences between vertical lines and edges of the polygon are constant for all $\gamma - \beta$ within each interval. This allows us to solve one integer program for each of the intervals, each integer program with the added constraint that $\gamma - \beta \in I_j$ for some j , and appropriate constraints computing the a_i and b_i as outlined above. Together, these n integer programs cover the entire space of possible values for t , and we simply take the best solution found among all of them. Each individual integer program has $O(k)$ variables, $2k + 1$ of which are integer variables, and can therefore be solved in time $2^{O(k \log k)} b^{O(1)}$ using Kannan's algorithm for integer programming [Kan87]. \square

Proof of Theorem 4. We summarize the algorithm as follows:

1. Compute the lattice width and width direction $y \in \mathbb{Z}^2 \setminus \{0\}$ of P .
2. If $w(P) \leq 4k$, compute an optimal translate using the algorithm of Lemma 7.
3. Otherwise, assert that every translate is a $(1 + 1/k)$ -approximate solution.

The correctness of the last step follows from Theorem 5: Let A be the area of P and let OPT be the number of integer points in an optimal solution. Then for every $t \in \mathbb{R}$:

$$|(tv + P) \cap \mathbb{Z}^2| \leq \left(1 + \frac{3}{8k}\right)A \leq \left(1 + \frac{3}{8k}\right) \cdot \frac{1}{1 - \frac{3}{8k}} \cdot OPT \leq \left(1 + \frac{1}{k}\right)OPT,$$

as long as $k \geq 2$. □

References

- [Bal97] Keith Ball. An elementary introduction to modern convex geometry. In *Flavors of geometry*, volume 31 of *Math. Sci. Res. Inst. Publ.*, pages 1–58. Cambridge Univ. Press, Cambridge, 1997.
- [Bar94] Alexander I. Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Mathematics of Operations Research*, 19(4):769–779, 1994.
- [Bar02] Alexander Barvinok. *A course in convexity*, volume 54 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.
- [BDR02] Matthias Beck, Ricardo Diaz, and Sinai Robins. The Frobenius problem, rational polytopes, and Fourier-Dedekind sums. *J. Number Theory*, 96(1):1–21, 2002.
- [Bec00] Matthias Beck. Counting lattice points by means of the residue theorem. *Ramanujan J.*, 4(3):299–310, 2000.
- [BP99] A. Barvinok and J. E. Pommersheim. An algorithmic theory of lattice points in polyhedra. In *New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97)*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.
- [BR07] Matthias Beck and Sinai Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, 2007. Integer-point enumeration in polyhedra.
- [DLHTY04] Jesús A. De Loera, Raymond Hemmecke, Jeremiah Tauzer, and Ruriko Yoshida. Effective lattice point counting in rational convex polytopes. *J. Symbolic Comput.*, 38(4):1273–1302, 2004.
- [ES08] Friedrich Eisenbrand and Gennady Shmonin. Parametric integer programming in fixed dimension. *Mathematics of Operations Research*, 33(4):839–850, 2008.
- [Gau73] Carl Friedrich Gauß. *Werke. Band II*. Georg Olms Verlag, Hildesheim, 1973. Reprint of the 1863 original.
- [Hux96] M. N. Huxley. *Area, lattice points, and exponential sums*, volume 13 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1996. Oxford Science Publications.
- [HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
- [Kan87] R. Kannan. Minkowski’s convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.
- [Kan90] Ravi Kannan. Test sets for integer programs, $\forall\exists$ sentences. In *Polyhedral combinatorics (Morristown, NJ, 1989)*, volume 1 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 39–47. Amer. Math. Soc., Providence, RI, 1990.
- [Kan92] R. Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992.
- [KV08] Matthias Köppe and Sven Verdoolaege. Computing parametric rational generating functions with a primal Barvinok algorithm. *Electron. J. Combin.*, 15(1):Research Paper 16, 19, 2008.
- [Lag85] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM J. Computing*, 14(1):196 – 209, 1985.
- [Len83] H. W. Lenstra. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538 – 548, 1983.
- [LZ05] Jean B. Lasserre and Eduardo S. Zeron. An alternative algorithm for counting lattice points in a convex polytope. *Math. Oper. Res.*, 30(3):597–614, 2005.

- [VSB⁺07] Sven Verdoolaege, Rachid Seghir, Kristof Beyls, Vincent Loechner, and Maurice Bruynooghe. Counting integer points in parametric polytopes using Barvinok's rational functions. *Algorithmica*, 48(1):37–66, 2007.
- [VW07] Sven Verdoolaege and Kevin Woods. Counting with rational generating functions. *Journal of Symbolic Computation*, 2007. to appear.