ON THE NUMBER OF INTEGER POINTS IN TRANSLATED AND EXPANDED POLYHEDRA

DANNY NGUYEN* AND IGOR PAK*

Abstract. We prove that the problem of minimizing the number of integer points in parallel translations of a rational convex polytope in $\mathbb{R}^6$ is NP-hard. We apply this result to show that given a rational convex polytope $P \subset \mathbb{R}^6$, finding the largest integer t s.t. the expansion tP contains fewer than k integer points is also NP-hard. We conclude that the Ehrhart quasi-polynomials of rational polytopes can have arbitrary fluctuations.

1. Introduction

In integer and combinatorial optimization, many problems are computationally hard when the dimension is unbounded. In fixed dimensions, the situation is markedly different as many classical problems become tractable. Notably Lenstra's algorithm for *Integer Programming*, and Barvinok's algorithm for *counting integer points* in finite dimensional rational polytopes are polynomial.

In recent years, there has been a lot of work, including by the authors, to show that many problems in bounded dimension remain computationally hard as soon as one leaves the classical framework (see below). This paper proves hardness of two integer optimizations problems related to translation and expansion of rational polytopes in bounded dimensions.

We then consider the problem of describing *Ehrhart quasi-polynomials* of rational polytopes. These quasi-polynomials are of fundamental importance in both discrete geometry and integer optimization, yet they remain somewhat mysterious and difficult to study. We apply our result to prove a rather surprising property: that Ehrhart quasi-polynomials of rational polytopes can have arbitrary *fluctuations* of consecutive values (see below).

1.1. Translation of polytopes.

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$. The following problem was considered by Eisenbrand and Hähnle in [EH12].

Integer Point Minimization (IPM)
Input: $A \in \mathbb{Q}^{m \times n}$, a rational polyhedron $Q \subset \mathbb{R}^m$, $k \in \mathbb{N}$.
Decide: $\exists b \in Q$ s.t. $\#\{\mathbf{x} \in \mathbb{Z}^n : A\mathbf{x} \leq b\} \leq k$?

Parametric polytopes $P_b := \{x \in \mathbb{R}^n : Ax \leq b\}$ were introduced by Kannan [Kan90], who gave a polynomial time algorithm for IPM with $k = 0$ and n bounded. For larger fixed values k, Aliev, De Loera and Louveaux [ADL16] proved that IPM is also polynomial time by employing the *short generating functions* technique by Barvinok and Woods [BW03] (see also [Bar06b, Bar08]). The following problem is an especially attractive special case:

*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {ldnguyen,pak}@math.ucla.edu.
January 12, 2020.

Polytope Translation
Input: $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$, $\vec{v} \in \mathbb{Q}^n$, and $k \in \mathbb{N}$.
Decide: $\exists \lambda,\ 0 \le \lambda \le 1$ s.t. $\#\{\mathbf{x} \in \mathbb{Z}^n : A(\mathbf{x} - \lambda\vec{v}) \le b\} \le k$?

In terms of parametric polytopes, this asks for a translation of the original polytope P by $\lambda\vec{v}$ so that it has at most k integer points. Polytope Translation is a special case of the Integer Point Minimization problem, when Q is 1-dimensional.

Eisenbrand and Hähnle proved that the Polytope Translation is NP-hard for $n = 2$ and m unbounded:

Theorem 1.1 ([EH12]). *Given a rational m-gon $Q \subset \mathbb{R}^2$, minimizing $|Q+\lambda\vec{e}_1|$ over $\lambda \in \mathbb{R}$ is NP-hard.*

Here and everywhere below, $|P|$ denotes the number of integer points in a polytope P, and $\vec{e}_1 = (1, 0, \dots)$ is the standard first coordinate vector. We prove a similar result for $n = 6$ with a *fixed* number m of vertices.

Theorem 1.2. *Given a rational polytope $P \subset \mathbb{R}^6$ with at most 64 vertices, minimizing $|P + \lambda\vec{e}_1|$ over $\lambda \in \mathbb{R}$ is NP-hard.*

This resolves a problem by Eisenbrand.[1] Since the dimension is fixed, the number of facets of P is at most an explicit constant. An integer version of this is:

Theorem 1.3. *Given a rational polytope $P \subset \mathbb{R}^6$ with at most 60 vertices and an integer $N \in \mathbb{N}$, minimizing $|P + t\vec{e}_1/N|$ over $t \in \mathbb{Z}$ is NP-hard.*

While Theorem 1.3 is implied by Theorem 1.2 by a simple argument on rationality, its proof is simpler and will be presented first (cf. Section 3). The technique differs from those in [EH12] and our earlier work on the subject.

To prove Theorem 1.3, we show how to embed a classical NP-hard quadratic optimization problem into Polytope Translation. This is done by viewing each term in the quadratic objective as the integer volume of a separate polygon in $\mathbb{R}^2$, which are then merged in a higher dimension into a single convex polytope (cf. [NP17a, NP17b]). Let us mention that positivity and convexity are major obstacles here, and occupy much of the proof.

1.2. **Expansions of polytopes.** A *quasi-polynomial* $p(t) : \mathbb{Z} \to \mathbb{Z}$ is an integer function

$$p(t) \,=\, c_0(t)t^d + c_1(t)t^{d-1} + \ldots + c_d(t),$$

where $c_i(t)$, $0 \le i \le d$, are periodic with integer period, and $c_d(t) \not\equiv 0$. We call d the degree of the quasi-polynomial. For a rational polytope $P \subset \mathbb{R}^n$ of full dimension, consider the counting function:

$$f_P(t) \,\coloneqq\, \big|tP \cap \mathbb{Z}^n\big|.$$

Ehrhart famously proved that $f_P(t)$ is a degree d quasi-polynomial, called the *Ehrhart quasi-polynomial*, see e.g. [Bar08, §18]. Furthermore, it is also known (and not hard to see) that $c_0(t) = \mathrm{vol}_n(P)$, or equivalently $f_P(t) \sim \mathrm{vol}_n(P)t^n$.

Many interesting combinatorial problems can be restated in the language of Ehrhart quasi-polynomials. We start with the following classical problem:

Frobenius Coin Problem
Input: $\overline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $\gcd(\alpha_1, \dots, \alpha_n) = 1$.
Output: $g(\overline{a}) \coloneqq \max\big\{t \in \mathbb{N} \,:\, \nexists\, c_1, \dots, c_n \in \mathbb{N} \ \text{ s.t. } t = c_1\alpha_1 + \ldots + c_n\alpha_n\big\}$.

[1] F. Eisenbrand, personal communication (September 2017).

In other words, this problem asks for the largest integer t that cannot be written as a combination of the coins α_i's. Such a t exists by the $\gcd(\cdot) = 1$ condition. Finding $g(\overline{a})$ is an NP-hard problem when the dimension n is not bounded, see [RA96]. For a fixed n, Kannan proved that the problem can be solved in polynomial time [Kan92, BW03].

We can restate the Frobenius Coin Problem as follows. Let

$$\Delta_{\overline{\alpha}} \coloneqq \{\mathbf{x} \in \mathbb{R}^n \ : \ \overline{\alpha} \cdot \mathbf{x} = 1, \ \mathbf{x} \geq 0\} \quad \text{and} \quad f_{\overline{\alpha}} \coloneqq f_{\Delta_{\overline{\alpha}}}.$$

Then $f_{\overline{\alpha}}(t)$ counts the number of ways to write $t \geq 0$ as an $\mathbb{N}$-combination of the α_i's. Thus, $g(\overline{\alpha})$ is the largest $t \geq 0$, such that $f_{\overline{\alpha}}(t) = 0$. Beck and Robins [BR04] used this setting to consider the following generalization:

k-Frobenius Problem
Input: $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\gcd(\alpha_1, \ldots, \alpha_n) = 1$, $k \in \mathbb{N}$.
Output: $g(\alpha, k) \coloneqq \max\big\{t \in \mathbb{N} \ : \ f_{\overline{\alpha}}(t) < k\big\}$.

In other words, the problem asks for the largest integer t that cannot be represented as a combinations of α_i's in k different ways. Aliev, De Loera and Louveaux [ADL16] generalized Kannan's theorem to prove that for fixed n and k the problem is still in P. Motivated by the above interpretation with the simplex $\Delta_{\overline{\alpha}}$, they also considered the following generalization:

k-Ehrhart Threshold Problem (k-ETP)
Input: A rational polytope $P \subset \mathbb{R}^n$ and $k \in \mathbb{N}$.
Output: $g(P, k) \coloneqq \max\big\{t \in \mathbb{N} \ : \ f_P(t) < k\big\}$.

For a polytope P, this asks for the largest t so that tP contains fewer than k integer points. Again, when both n and k are fixed, it was shown in [ADL16] that this problem is in P. However, for varying k we have:

Theorem 1.4. *The* k-ETP *is* NP*-hard for rational polytopes* $P \subset \mathbb{R}^6$ *with at most* 60 *vertices.*

It is an open problem whether the k-Frobenius Problem is NP-hard when k is a part of the input (see §6.1).

1.3. **Fluctuations of the Ehrhart quasi-polynomial.** It is well known that every quasi-polynomial $p(t) : \mathbb{Z} \to \mathbb{Z}$ can be written in the form:

$$p(t) \ = \ \sum_{i=1}^{r} \gamma_i \prod_{j=1}^{n} \big\lfloor \alpha_{ij} t + \beta_{ij} \big\rfloor, \tag{1.1}$$

where $\alpha_i, \beta_i, \gamma_i \in \mathbb{Q}$. The smallest n for which $p(t)$ is representable in this form is called the *degree* of $f(t)$. It is also known how to compute $f_P(t)$ in the from (1.1) efficiently when n is fixed (see e.g. [VW08]).

Not all n quasi-polynomial arise as Ehrhart quasi-polynomials of full-dimensional polytopes $P \subset \mathbb{R}^n$. For instance, $p(t) = 1 + t\lfloor \frac{t}{2} \rfloor - t\lfloor \frac{t-1}{2} \rfloor$ cannot be an Ehrhart quasi-polynomial because $p(t) > 0$ for all t, yet its leading term fluctuates between odd and even values of t. However, when restricted to finite intervals, every quasi-polynomial can be realized as f_P of a polytope P, in the following sense:

Theorem 1.5. *Let $N \in \mathbb{N}$ and $p : \mathbb{Z} \to \mathbb{Z}$ be a quasi-polynomial of the form (1.1), with $\gamma_i \in \mathbb{Z}$, $\alpha_{ij}, \beta_{ij} \in \mathbb{Q}$ for $1 \le i \le r$ and $1 \le j \le n$. Then there exists a rational polytope $Q \subset \mathbb{R}^d$ and integers $K, M \in \mathbb{N}$, such that:*

$$p(t) + K \ = \ f_Q(t+M) \quad \text{for every} \quad 0 \le t < N.$$

Moreover, we have $d = O(n + \lceil \log r \rceil)$, and polytope Q has at most $r4^{n+1}$ vertices. Here the vertices of Q and the constants K, M can be computed in polynomial time.

Roughly, this theorems say that locally, Ehrhart quasi-polynomials can fluctuate as badly as general quasi-polynomials. In particular, we have:

Corollary 1.6. *For every sequence $c_0, \ldots, c_{r-1} \in \mathbb{N}$, there exists a polytope $Q \subset \mathbb{R}^d$ and $K, M \in \mathbb{N}$ such that:*

$$c_i + K \ = \ f_Q(i+M) \quad \text{for every} \quad 0 \le i < r.$$

Moreover, we have $d = O(\log r)$ and polytope Q has at most $O(r)$ vertices. Here the vertices of Q and the constants K, M can be computed in polynomial time.

Proof. Consider the degree 1 quasi-polynomial

$$f(t) \ = \ \sum_{i=0}^{r-1} c_i \left(\left\lfloor \frac{t-i}{r} \right\rfloor - \left\lfloor \frac{t-i-1}{r} \right\rfloor \right).$$

Then $f(i) = c_i$ for $0 \le i < r$. Now we apply Theorem 1.5 to $f(t)$ with $N = r$. □

1.4. **Brief historical overview.** Integer Programming (IP) asks for given $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$, to decide whether

$$\exists \mathbf{x} \in \mathbb{Z}^n \ : \ A\mathbf{x} \le b.$$

Equivalently, the problem ask whether a rational polytope contains an integer point.

When n is unbounded, this problem includes Knapsack as a special case, and thus NP-complete (see e.g. [GJ79]). For fixed n, the situation is drastically different. Lenstra [Len83] famously showed that IP is in P, even when m is unbounded (see also [Sch86]). Barvinok [Bar93] showed that the corresponding counting problem is in FP, pioneering a new technique in this setting (see also [Bar08, Bar17]).

The Parametric Integer Programming (PIP) asks for a given $A \in \mathbb{Q}^{m \times n}$, $B \in \mathbb{Q}^{m \times \ell}$ and $b \in \mathbb{Q}^m$, to decide whether

$$\forall \mathbf{y} \in Q \cap \mathbb{Z}^\ell \quad \exists \mathbf{x} \in \mathbb{Z}^n \ : \ A\mathbf{x} + B\mathbf{y} \le b,$$

where $Q \subset \mathbb{Q}^\ell$ is a convex polyhedron given by $K\mathbf{y} \le u$, for some $K \in \mathbb{Q}^{\ell \times r}$, $u \in \mathbb{Q}^r$. Kannan showed that PIP is in P (see also [ES08, NP17b]). In [Kan92], Kannan used the PIP interpretation to show that for a fixed number ℓ of coins, the Frobenius Coin Problem is in P. Barvinok and Woods [BW03] showed that the corresponding counting problem is in FP, but only when the dimensions ℓ and n are fixed (see also [Woo04]).

Although the above list is not exhaustive, most other problems in this area with fixed dimensions are computationally hard, especially in view of our recent works. Let us single out one negative small-dimensional result. We showed in [NP17a] that given two rational polytopes $P, Q \subset \mathbb{R}^3$, it is #P-complete to compute

$$\#\big\{x \in \mathbb{Z} \ : \ \exists \mathbf{z} \in \mathbb{Z}^2, \quad (x, \mathbf{z}) \in P \setminus Q\big\}.$$

Note that the corresponding decision problem is a special case of PIP, and thus can be decided in polynomial time. This elucidated the limitations of the Barvinok–Woods approach (see also [NP18, NP17b]).

The Frobenius problem and its many variations is thoroughly discussed in [RA05], along with its connections to lattice theory, number theory and convex polyhedra. There are also some efficient practical algorithms for solving it, see [BHNW05]. The k-Frobenius Problem, also called the *generalized Frobenius problem*, has been intensely studied in recent years, see e.g. [AHL13, FS11].

Ehrhart quasi-polynomials become polynomials for integer polytopes, in which case there is a large literature on their structure and properties (see e.g. [Bar08, Bar17] and references therein). We discuss integer polytopes in Section 5. A bounded number of leading coefficients of Ehrhart quasi-polynomials in arbitrary dimensions can be computed in polynomial time [Bar06a] (see also [B+12]). There is also some interesting analysis of the periods of the coefficients $c_i(t)$, see [BSW08, MR18, Woo05]. It seems that fluctuations of Ehrhart quasi-polynomials have not been considered until now.

1.5. **Notations.** As mentioned earlier, $|P|$ always denote the number of integer points in a convex polytope $P \subset \mathbb{R}^n$. We use $P + \vec{w}$ to denote translation of P by vector $\vec{w}$. The first coordinate vector $(1, 0, \dots)$ is denoted by $\vec{e}_1$.

When the ambient space $\mathbb{R}^n$ is clear, we use $\{x_i = \xi_i, \dots, x_j = \xi_j\}$ to denote the subspace with specified coordinates $x_i = \xi_i, \dots, x_j = \xi_j$. We write $f(t) \gg g(t)$ for $g(t) = o\big(f(t)\big)$ as $t \to \infty$. Finally, we use the notations $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{Z}_+ = \{1, 2, \dots\}$.

2. Proof of Theorem 1.3

2.1. **General setup.** We start with the following classical problem:

Quadratic Diophantine Equations (QDE)
Input: $\alpha, \beta, \gamma \in \mathbb{N}$.
Decide: $\exists u \in \mathbb{N}$, $0 \le u < \gamma$ s.t. $u^2 \equiv \alpha \pmod{\beta}$?

Manders and Adleman [MA78] proved that QDE is NP-complete (see also [GJ79, §7.2]). Observe that the problem remains NP-complete when we assume $\alpha, \gamma < \beta$, Thus, the problem can be rephrased as the problem of minimizing

$$f(u, v) \coloneqq (u^2 - \alpha - \beta v)^2 \quad \text{over} \quad (u, v) \in \mathrm{B} \cap \mathbb{Z}^2. \tag{2.1}$$

where $\mathrm{B} = [0, \gamma) \times [0, \beta)$. Indeed, we have $\min_{(u,v)\in \mathrm{B}} f(u, v) = 0$ if and only if the congruence in QDE is feasible.

Let $N = \beta\gamma$. The two variables $(u, v) \in \mathrm{B}$ can be encode into a single integer variable $0 \le t < N$ by:

$$u = \lfloor t/\beta \rfloor \quad \text{and} \quad v = t \pmod{\beta} = t - \beta \lfloor t/\beta \rfloor.$$

It is clear that each pair $(u, v) \in \mathrm{B} \cap \mathbb{Z}^2$ corresponds to such a unique $t \in [0, N-1]$ and vice versa. So we can restate the problem as minimizing $f\big(\lfloor t/\beta \rfloor, t - \beta \lfloor t/\beta \rfloor\big)$ over $t \in [0, N)$.

Now we have:

$$\begin{aligned} f\big(\lfloor t/\beta\rfloor, t-\beta\lfloor t/\beta\rfloor\big) \;&=\; \Big(\lfloor t/\beta\rfloor^2 - \alpha - \beta\big(t-\beta\lfloor t/\beta\rfloor\big)\Big)^2 \\ &=\; \Big(\lfloor t/\beta\rfloor\big(\lfloor t/\beta\rfloor+\beta^2\big) - \big(\alpha+\beta t\big)\Big)^2 \\ &=\; \underbrace{\lfloor t/\beta\rfloor^2\big(\beta^2+\lfloor t/\beta\rfloor\big)^2}_{T_1(t)} + \underbrace{\big(\alpha+\beta t\big)^2}_{T_2(t)} - \underbrace{2\lfloor t/\beta\rfloor\big(\beta^2+\lfloor t/\beta\rfloor\big)\big(\alpha+\beta t\big)}_{S(t)} \end{aligned} \tag{2.2}$$

Here we denote by $T_1(t), T_2(t)$ and $S(t)$ the three terms in the above sum. First, we need to convert $-S(t)$ into a positive term. Fix a large constant σ, say $\sigma := 10\beta^5$ will suffice for our purposes. We have:

$$\begin{aligned} -S(t) \;&=\; -S(t) \,+\, 2\beta(\beta^2+\beta)(\alpha+\beta t) \,-\, 2\beta(\beta^2+\beta)(\alpha+\beta t) \,+\, \sigma \,-\, \sigma \\ &=\; \Big[\beta(\beta^2+\beta) - \lfloor t/\beta\rfloor\big(\beta^2+\lfloor t/\beta\rfloor\big)\Big]2(\alpha+\beta t) \,+\, \sigma \,-\, 2\beta(\beta^2+\beta)(\alpha+\beta t) - \sigma \\ &=\; \underbrace{\big(\beta-\lfloor t/\beta\rfloor\big)\big(\beta^2+\beta+\lfloor t/\beta\rfloor\big)(2\alpha+2\beta t)}_{T_3(t)} + \underbrace{\big[\sigma \,-\, 2\beta(\beta^2+\beta)(\alpha+\beta t)\big]}_{T_4(t)} - \sigma. \end{aligned} \tag{2.3}$$

Thus,

$$f\big(\lfloor t/\beta\rfloor, t-\beta\lfloor t/\beta\rfloor\big) \;=\; T_1(t) \,+\, T_2(t) \,+\, T_3(t) \,+\, T_4(t) \,-\, \sigma.$$

Note that $T_1(t), \ldots, T_4(t) > 0$ for $0 \le t < N$. Let

$$g(t) \;:=\; \sigma + f\big(\lfloor t/\beta\rfloor, t-\beta\lfloor t/\beta\rfloor\big).$$

We can rephrase the original NP-hard problem as the problem of computing the following minimum:

$$\min_{0\le t<N} g(t) \;=\; \min_{0\le t<N} T_1(t) \,+\, \ldots \,+\, T_4(t). \tag{2.4}$$

Note that each function $T_i(t)$ is a product of terms of the form $p \pm qt$ or $r \pm \lfloor t/\beta\rfloor$ for some constants $p, q, r > 0$. We encode each of these three types of functions as the number of integer points in some translated polytope. From this point on, we assume that $0 \le t < N$, unless stated otherwise.

2.2. **Trapezoid constructions.** To illustrate the idea, we start with the simplest function qt with $q \in \mathbb{Z}_+$. Let $\varepsilon = 1/4N^2$ and $\vec{v} = \vec{e}_1/N = (1/N, 0, \ldots, 0)$. Consider the following triangle:

$$\Delta \;=\; \big\{(x,y) \in \mathbb{R}^2 \,:\, x, y \ge \varepsilon,\, qN(1-x) \ge y\big\}.$$

(see Figure 1). Fix a line $\ell := \{x = 1\}$. It is easy to see that the hypotenuse of $\Delta + t\vec{v}$ intersects ℓ at the point $y = qNt/N = qt$. So we have $(\Delta + t\vec{v}) \cap \ell = [\varepsilon, qt]$, and thus $|\Delta + t\vec{v}| = qt$.

To encode a function $p+qt$ with $p, q \in \mathbb{Z}_+$, we take Δ and extend vertically by a distance $p - \frac{1}{2}$ below the line $y = 0$ to make a trapezoid F_A. Similarly, to encode a function $p' - qt$ with $p' > qN$, we translate the hypotenuse of Δ up by 2ε, and then extend upward by p' to get a trapezoid F_B (see Figure 1). Formally, let:

$$\begin{aligned} F_A \;&=\; \big\{(x,y) \in \mathbb{R}^2 \,:\, 1 \ge x \ge \varepsilon,\, qN(1-x) \ge y \ge 1/2 - p\big\} \;\text{ and} \\ F_B \;&=\; \big\{(x,y) \in \mathbb{R}^2 \,:\, 1 \ge x \ge \varepsilon,\, p' \ge y \ge qN(1-x) + 2\varepsilon\big\}. \end{aligned}$$

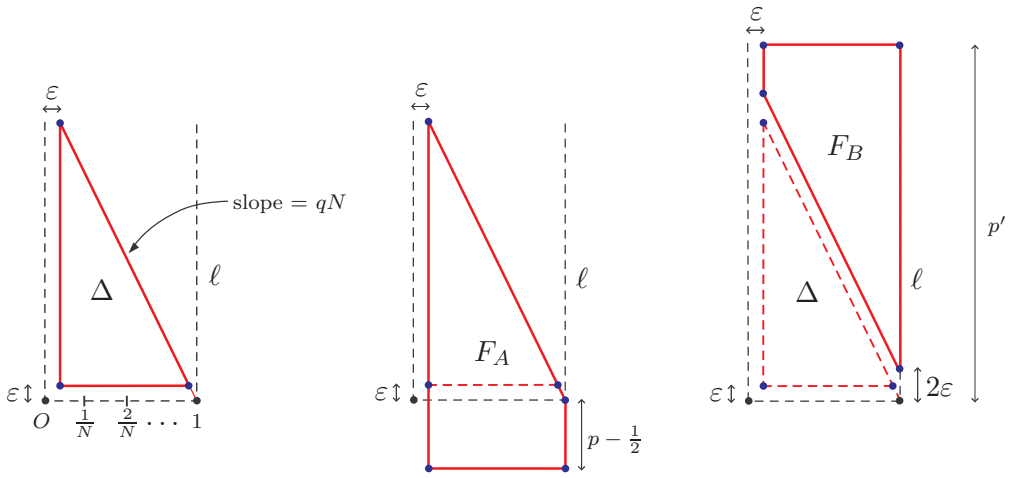

FIGURE 1. The triangle Δ and trapezoids F_A, F_B.

Let us show that these trapezoids encode the function as stated above. For F_A, we have $(F_A + t\vec{v}) \cap \ell = \left[\frac{1}{2} - p,\, qt\right]$, and thus $|F_A + t\vec{v}| = p + qt$. For F_B, the hypotenuse of $F_B + t\vec{v}$ intersects ℓ at $qt + 2\varepsilon$. So we have $(F_B + t\vec{v}) \cap \ell = \left[qt + 2\varepsilon,\, p'\right]$, and thus $|F_B + t\vec{v}| = p' - qt$ as desired.

For the function $\lfloor t/\beta \rfloor$, we can encode it with the following triangle:

$$\Delta' \;=\; \big\{(x, y) \in \mathbb{R}^2 \;:\; x, y \geq \varepsilon,\, \gamma(1 - x) \geq y\big\}.$$

(see Figure 2). It is easy to see that the hypotenuse of $\Delta' + t\vec{v}$ intersects ℓ at the point $y = \gamma t/N = t/\beta$. So $(\Delta' + t\vec{v}) \cap \ell = [\varepsilon, t/\beta]$ and thus $|\Delta' + t\vec{v}| = \lfloor t/\beta \rfloor$.

By modifying Δ' and keeping the same slope γ, we can encode the functions $r + \lfloor t/\beta \rfloor$ and $r' - \lfloor t/\beta \rfloor$ with $r, r' \in \mathbb{Z}_+$, $r' > \gamma$, by using the following trapezoids:

$$\begin{aligned} F_C \;&=\; \big\{(x, y) \in \mathbb{R}^2 \;:\; 1 \geq x \geq \varepsilon,\, \gamma(1 - x) \geq y \geq 1/2 - r\big\} \;\text{ and} \\ F_D \;&=\; \big\{(x, y) \in \mathbb{R}^2 \;:\; 1 \geq x \geq \varepsilon,\, r' \geq y \geq \gamma(1 - x) + 2\varepsilon\big\}, \end{aligned}$$

respectively (see Figure 2).

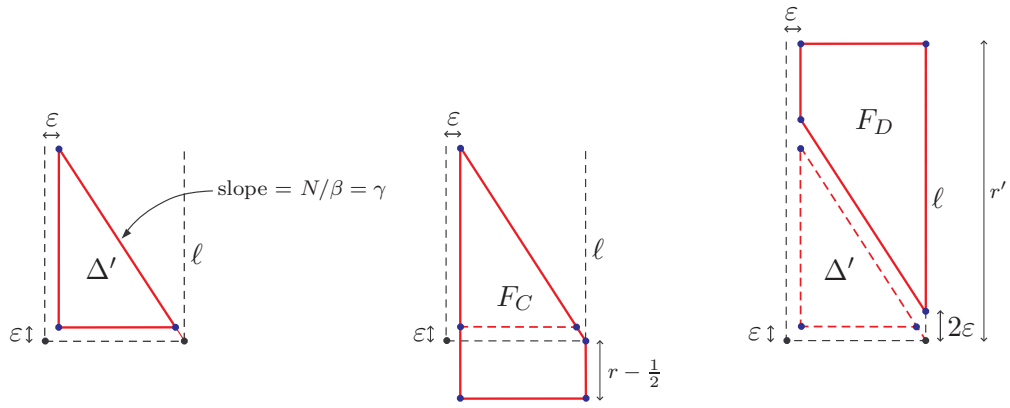

FIGURE 2. The triangle Δ' and trapezoids F_C, F_D.

Let us show that these trapezoids encode the function as stated above. For F_C, we have $(F_C + t\vec{v}) \cap \ell = \left[\frac{1}{2} - r,\ \frac{t}{\beta}\right]$, and thus $|F_C + t\vec{v}| = r + \lfloor t/\beta \rfloor$. Similarly, for F_D, the hypotenuse of $(F_D + t\vec{v})$ intersects ℓ at $y = t/\beta + 2\varepsilon$, and thus $(F_D + t\vec{v}) \cap \ell = \left[\frac{t}{\beta} + 2\varepsilon,\ r'\right]$. Since $t/\beta < t/\beta + 2\varepsilon < (t+1)/\beta$, we have $|F_D + t\vec{v}| = r' - \lfloor t/\beta \rfloor$, as desired.

Note that the counting function for each constructed trapezoid is periodic modulo N. In other words, $|F_A + t\vec{v}| = |F_A + (t \bmod N)\vec{v}|$ for every $t \in \mathbb{Z}$, and the same result holds for F_B, F_C, F_D. From this point on, we let t take values over $\mathbb{Z}$ in place of our earlier restriction $t \in [0, N)$.

2.3. **The product construction.** The next step is to construct polytopes that encode products functions of the form $p \pm qt$ and $r \pm \lfloor t/\beta \rfloor$.

Consider any d functions $h_1(t), \ldots, h_d(t)$ of these forms. We take the trapezoids $F_1, \ldots, F_d$ whose counting functions encode h_i's. Each $F_i \subset \mathbb{R}^2$ is described by a system:

$$F_i \ = \ \big\{(x, y) \in \mathbb{R}^2 \ : \ \mu_i \le x \le \nu_i,\ \rho_i + \tau_i x \le y \le \rho_i' + \tau_i' x\big\}.$$

We embed F_i into the 2-dimensional subspace spanned by coordinates x, y_i inside $\mathbb{R}^{d+1}$ (with coordinates $x, y_1, \ldots, y_d$). Then define:

$$P \ = \ \big\{(x, y_1, \ldots, y_d) \in \mathbb{R}^{d+1} \ : \ \max_{1 \le i \le d} \mu_i \le x \le \min_{1 \le i \le d} \nu_i,\ \rho_i + \tau_i x \le y_i \le \rho_i' + \tau_i' x\big\}. \tag{2.5}$$

It is clear that for every t and every vertical hyperplane $H = \{x = x_0\}$ in $\mathbb{R}^{d+1}$, we have $(P + t\vec{v}) \cap H = \big((F_1 + t\vec{v}) \cap H\big) \times \cdots \times \big((F_d + t\vec{v}) \cap H\big)$.[2] Therefore, we have

$$|P \cap t\vec{v}| \ = \ |F_1 \cap t\vec{v}| \ldots |F_d \cap t\vec{v}| \ = \ h_1(t) \ldots h_d(t).$$

So the $(d+1)$-dimensional polytope P encodes the product $h_1(t) \ldots h_d(t)$. Note that P is combinatorially a cube, which means it has $2(d+1)$ facets and 2^{d+1} vertices.

2.4. **Putting it all together.** We apply this product construction to each of the four terms T_1, T_2 in (2.2), T_3, T_4 in (2.3) and get four polytopes $P_1 \in \mathbb{R}^5$, $P_2 \in \mathbb{R}^3$, $P_3 \in \mathbb{R}^4$, $P_4 \in \mathbb{R}^2$ such that

$$|P_i + t\vec{v}| \ = \ T_i(t \bmod N) \quad \text{for every } t \in \mathbb{Z}. \tag{2.6}$$

Now we embed them into $\mathbb{R}^6$ as follows:

$$\begin{aligned} Q_1 \ &= \ \{\mathbf{x} \in \mathbb{R}^6 \ : \ (x_1, \ldots, x_5) \in P_1,\ x_6 = 1\}, \\ Q_3 \ &= \ \{\mathbf{x} \in \mathbb{R}^6 \ : \ (x_1, \ldots, x_4) \in P_3,\ x_5 = 1,\ x_6 = 0\}, \\ Q_2 \ &= \ \{\mathbf{x} \in \mathbb{R}^6 \ : \ (x_1, \ldots, x_3) \in P_2,\ x_4 = 1,\ x_5 = 0,\ x_6 = 0\}, \\ Q_4 \ &= \ \{\mathbf{x} \in \mathbb{R}^6 \ : \ (x_1, x_2) \in P_4,\ x_3 = 1,\ x_4 = 0,\ x_5 = 0,\ x_6 = 0\}. \end{aligned} \tag{2.7}$$

Define the polytope

$$W = \operatorname{conv}(Q_1, \ldots, Q_4). \tag{2.8}$$

First, note that $Q_1, \ldots, Q_4$ are disjoint. They also have the property that for every $t \in \mathbb{Z}$:

$$(W + t\vec{v}) \cap \mathbb{Z}^6 \ = \ \bigsqcup_{i=1}^{4} \Big((Q_i + t\vec{v}) \cap \mathbb{Z}^6\Big).$$

To see this, consider some lattice point $\mathbf{z} = (z_1, \ldots, z_6) \in (W + t\vec{v}) \cap \mathbb{Z}^6$. Since W is the convex hull of $Q_1, \ldots, Q_4$, and each Q_i sits in one of the two hyperplanes $\{x_6 = 1\}$, $\{x_6 = 0\}$,

[2] Note that each $F_i + t\vec{v}$ intersects exactly one such hyperplane H with $x_0 \in \mathbb{Z}$.

we must have $z_6 = 1$ or $z_6 = 0$. This means $\mathbf{z} \in (Q_1 + t\vec{v})$ or $\mathbf{z} \in (\mathrm{conv}(Q_2, Q_3, Q_4) + t\vec{v})$. Assume the latter case, then we continue considering the coordinate z_5. By a similar argument, we must have $\mathbf{z} \in (Q_3 + t\vec{v})$ or $\mathbf{z} \in (\mathrm{conv}(Q_2, Q_4) + t\vec{v})$. For the latter case, the coordinate z_4 should finally tell us either $\mathbf{z} \in (Q_2 + t\vec{v})$ or $\mathbf{z} \in (Q_4 + t\vec{v})$.

Thus, for every $t \in \mathbb{Z}$, we have:

$$|W + t\vec{v}| \;=\; \sum_{i=1}^{4} |Q_i + t\vec{v}| \;=\; \sum_{i=1}^{4} |P_i + t\vec{v}| \;=\; \sum_{i=1}^{4} T_i(t \bmod N) \;=\; g(t \bmod N).$$

By (2.4), we conclude that computing the following minimum is NP-hard:

$$\min_{t\in\mathbb{Z}} |W + t\vec{v}| \;=\; \min_{0\le t<N} g(t).$$

Note that the polytopes Q_1, Q_2, Q_3, Q_4 have $32, 8, 16, 4$ vertices, respectively. Thus, the polytope W has in total 60 vertices, and satisfies Theorem 1.3. □

3. Proof of Theorem 1.2

We modify the construction in the proof of Theorem 1.3 by perturbing all its ingredients to ensure that the desired minimum coincides with the one in the integer case. This construction is rather technical and assumes the reader is familiar with details in the proof above.

Recall that $0 \le \alpha, \gamma < \beta$, $N = \beta\gamma$, $\varepsilon = 1/4N^2$ and $\vec{v} = \vec{e}_1/N$. We perturb all constructed trapezoids as follows. Denote by s the maximum slope over all hypotenuses of all constructed trapezoids. By a quick inspection of the terms $T_1, \ldots, T_4$ in (2.2) and (2.3), one can see that $s < 4\beta^4 N < 4\beta^6$. Take $\delta > 0$ much smaller than ε and $(\beta s)^{-1}$. For example, $\delta := 1/4\beta^8$ works. Now translate each constructed trapezoid F by a distance $+\delta$ horizontally in $\mathbb{R}^2$. Let F' be such a translated copy of some F.[3] Then it is not hard to see that $|F+t\vec{v}| = |F'+t\vec{v}|$ for all $t \in \mathbb{Z}$. In fact, due to the δ perturbation, we have:

$$|F + t\vec{v}| \;=\; |F' + t\vec{v}| \;=\; \Big|F' + \Big(\frac{t}{N} + \tau\Big)\vec{e}_1\Big|$$

for every $t \in \mathbb{Z}$ and $\tau \in [-\delta/4, \delta/4]$. This can be checked directly for all the trapezoid of types F_A, F_B, F_C, F_D constructed in the proof of Theorem 1.3. Define the real set

$$Z_\delta \;=\; \Big\{\frac{t}{N} + \tau \;:\; t \in \mathbb{Z},\, -\delta/4 \le \tau \le \delta/4\Big\}. \tag{3.1}$$

For $\lambda \in Z_\delta$, denote by $t(\lambda)$ the (unique) integer t such that $|\lambda - t/N| \le \delta/4$. By the above observations, we have $|F'+\lambda\vec{e}_1| = |F+t(\lambda)\vec{v}|$ for every $\lambda \in Z_\delta$. Now we take these perturbed trapezoids and construct $P'_1, \ldots, P'_4$ as similar to $P_1, \ldots, P_4$ above, using the same product construction (see (2.5)). Note that $P'_i = P_i + \delta\vec{e}_1$ and by (2.6), for every $\lambda \in Z_\delta$ we have:

$$|P'_i + \lambda\vec{e}_1| \;=\; |P_i + t(\lambda)\vec{v}| \;=\; T_i(t(\lambda) \bmod N) \quad (1 \le i \le 4). \tag{3.2}$$

We need to "patch up" Z_δ to make it the whole real line $\mathbb{R}$. Let

$$Y_\delta \;=\; \Big\{\frac{t}{N} + \tau \;:\; t \in \mathbb{Z},\, \frac{\delta}{8} \le \tau \le \frac{1}{N} - \frac{\delta}{8}\Big\}. \tag{3.3}$$

[3]Recall that each F encodes some function $h(t)$ as $|F + t\vec{v}| = h(t \bmod N)$ for every $t \in \mathbb{Z}$.

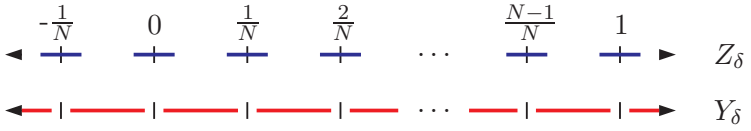

FIGURE 3. The sets Z_δ and Y_δ consisting of bold segments.

It is clear that $Z_\delta \cup Y_\delta = \mathbb{R}$. Take a large constant ω, s.t. $\omega \gg g(t)$ for all $0 \le t < N$. For example, $\omega := 10\beta^{10}$ will suffice for our purposes, by (2.2)–(2.4). Now consider the following parallelogram:

$$R \;=\; \Big\{(x,y) \in \mathbb{R}^2 \;:\; \omega N - \frac{1}{2} \ge y \ge 0,\; 1 - \frac{\delta}{8} - \frac{y}{N} \ge x \ge 1 - \frac{1}{N} + \frac{\delta}{8} - \frac{y}{N}\Big\}$$

(see Figure 4).

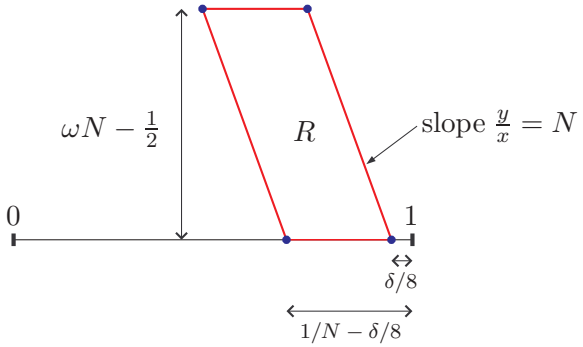

FIGURE 4. The parallelogram R.

Lemma 3.1. *We have:* $|R + \lambda\vec{e}_1| = \omega$ *if* $\lambda \in Y_\delta$, *and* $|R + \lambda\vec{e}_1| = 0$ *otherwise.*

Proof. Denote by $R_{(i)}$ the horizontal slice of R at height $i \in \mathbb{Z}$. Then for the bottom edge $R_{(0)}$, we have $|R_{(0)} + \lambda\vec{e}_1| = 1$ if $\delta/8 \le \lambda \bmod 1 \le 1/N - \delta/8$, and $|R_{(0)} + \lambda\vec{e}_1| = 0$ otherwise. In other words, $|R_{(0)} + \lambda\vec{e}_1| = 1$ if and only if λ lies in some jN-th segment of Y_δ ($j \in \mathbb{Z}$). Also every next slice is translated by $-1/N$, i.e., $R_{(i+1)} = R_{(i)} - \vec{e}_1/N$. There are in total ωN non-empty slices, which implies the claim. □

Recall the perturbed polytopes $P_1', \ldots, P_4'$ above, see (3.2). We embed them into $\mathbb{R}^5$ similarly to (2.7):

$$\begin{aligned}
Q_1' \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1,\ldots,x_5) \in P_1',\; x_6 = 1\},\\
Q_3' \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1,\ldots,x_4) \in P_3',\; x_5 = 1,\; x_6 = 0\},\\
Q_2' \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1,\ldots,x_3) \in P_2',\; x_4 = 1,\; x_5 = 0,\; x_6 = 0\},\\
Q_4' \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1,x_2) \in P_4',\; x_3 = 1,\; x_4 = 0,\; x_5 = 0,\; x_6 = 0\}.
\end{aligned} \tag{3.4}$$

We also embed R into $\mathbb{R}^5$ as:

$$Q_5' \;=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1,x_2) \in R, \quad x_3 = 0,\; x_4 = 0,\; x_5 = 0,\; x_6 = 0\}.$$

Let $W' = \text{conv}(Q'_1, \dots, Q'_5)$. By the above embeddings, we have:

$$|W' + \lambda\vec{e}_1| \;=\; \sum_{i=1}^{5} |Q'_i + \lambda\vec{e}_1| \;=\; |R + \lambda\vec{e}_1| \;+\; \sum_{i=1}^{4} |P'_i + \lambda\vec{e}_1|.$$

See Section 2.4 for an explanation on the additivity of the counting functions. Now if $\lambda \in Y_\delta$, we have:

$$|W' + \lambda\vec{e}_1| \;\geq\; |R + \lambda\vec{e}_1| \;=\; \omega \;\gg\; \max_{0\leq t<N} g(t).$$

On the other hand, if $\lambda \notin Y_\delta$, then $\lambda \in Z_\delta$ by (3.1) and (3.3). In this case, by (3.2) and Lemma 3.1, we have:

$$|W' + \lambda\vec{e}_1| \;=\; \sum_{i=1}^{4} |P'_i + \lambda\vec{e}_1| \;=\; \sum_{i=1}^{4} T_i(t(\lambda) \bmod N) \;=\; g(t(\lambda) \bmod N).$$

We conclude that the following minimum is NP-hard to compute:

$$\min_{\lambda\in\mathbb{R}} |W' + \lambda\vec{e}_1| \;=\; \min_{0\leq t<N} g(t).$$

Note that the polytopes $Q'_1, Q'_2, Q'_3, Q'_4, Q'_5$ have $32, 8, 16, 4, 4$ vertices, respectively. Thus, polytope W' has in total 64 vertices. This completes the proof of Theorem 1.2. □

4. Applications

4.1. **Proof of Theorem 1.4.** Recall from Section 2 the polytope $W \subset \mathbb{R}^6$ with 60 vertices and the translation vector $\vec{v} = \vec{e}_1/N$. From now on, we refer to W as P (its intended role in Theorem 1.3). From the construction in Section 2, P is a closed polytope containing at least one integer point, which we call $\vec{p} \in \mathbb{Z}^n$. We translate P by $-\vec{p}$ so that $\vec{0} \in P$, meanwhile still keeping $|P + t\vec{v}|$ the same for every $t \in \mathbb{Z}$.

Consider a very large multiple M of N (quantified later). For some $0 \leq t < N$, consider the two polytopes

$$R_t = P + (t + M)\vec{v} \quad \text{and} \quad R'_t = \frac{t+M}{M}P + (t + M)\vec{v}$$

First note that these are closed polytopes with $R_t \subset R'_t$. Also since $N|M$ and $N\vec{v} = (1, 0, \dots)$, R_t is just an integer translate of $P + t\vec{v}$. Thus, the distance from R_t to its closest outer integer point is exactly the same as that for $P + t\vec{v}$. So if R'_t is only slightly larger than R_t, they should contain the same set of integer points, which is again an integer translate of the set $(P + t\vec{v}) \cap \mathbb{Z}^n$. Therefore, if $M \gg N > t$, we should have $|R_t| = |R'_t|$.

To ensure $|R_t| = |R'_t|$ for all $0 \leq t < N$, it suffices to have $N/M < d_1/D_2$, where:

$$d_1 = \min_{0\leq t<N} \delta\big(P + t\vec{v},\; \mathbb{Z}^6 \backslash (P + t\vec{v})\big) \quad \text{and} \quad D_2 = \text{diameter of } P.$$

Here $\delta(\cdot, \cdot)$ denotes the shortest distance between 2 sets. Both $1/d_1$ and D_2 are polynomially bounded in N and the largest pq over all vertex coordinates p/q of P (see [Sch86, Ch.10]). So M only needs to be polynomially large in N and the coordinates of P.

Now we have $|R_t| = |R'_t|$ for every $0 \leq t < N$. Let $Q = \frac{1}{M}P + \vec{v}$, then $R'_t = (t + M)Q$. Thus, $|R_t| = |(t + M)Q|$ for every $0 \leq t < N$. Recall that $|P + t\vec{v}|$ is periodic modulo N and $N|M$. So $|R_t| = |P + (t + M)\vec{v}| = |P + t\vec{v}|$ for very t. We conclude that

$$|P + t\vec{v}| = |(t + M)Q| \quad \text{for every} \quad 0 \leq t < N.$$

Thus, computing $\min_{0\leq t<N} |(t + M)Q| = \min_{0\leq t<N} |P + t\vec{v}|$ is NP-hard.

By binary search, finding $\min_{0\le t<N} |(t+M)Q|$ is equivalent to deciding polynomially many sentences of the from $\min_{0\le t<N} |(t+M)Q| < k$ for varying k. From the definition of k-ETP, we have $\min_{0\le t<N} |(t+M)Q| < k$ if and only if $g(Q,k) \ge M$. This implies that computing $g(Q,k)$ is NP-hard. □

4.2. **Proof of Theorem 1.5.** The constants K, M will be later quantified. Recall that

$$p(t) \,=\, \sum_{i=1}^{r} \gamma_i \prod_{j=1}^{n} \big\lfloor \alpha_{ij} t + \beta_{ij} \big\rfloor \tag{4.1}$$

with $\gamma_i \in \mathbb{Z}$. By increasing n by 1 and writing $\gamma_i = \lfloor 0t + \gamma_i \rfloor$, we can assume that all coefficients $\gamma_i = 1$. Let $\vec{v} = \vec{e}_1/N$. First, we construct a polytope $W \subset \mathbb{R}^d$ such that $p(t \bmod N) + K = |W + t\vec{v}|$ for all $t \in \mathbb{Z}$. We need a technical lemma:

Lemma 4.1. *For every $n \ge 2$, we have the algebraic identity:*

$$3^{n-1} g_1 \cdots g_n + h_1 \cdots h_n = \sum_{S\subseteq[n],\, S\neq\varnothing} 3^{\delta(S)} \prod_{i\in[n]\setminus S} g_i \cdot \prod_{j\in S} (g_j \, + \sigma_j(S)\, \tau_j(S)\, h_j) \tag{4.2}$$

where

$$\sigma_j(S) = \begin{cases} 1 & \text{if} \quad j-1 \in S \\ -1 & \text{if} \quad j-1 \notin S \end{cases}, \quad \tau_j(S) = \begin{cases} 1 & \text{if} \quad \max(S) > j \\ -1 & \text{if} \quad \max(S) = j \end{cases}, \quad \delta(S) = \max(0, n - \max(S) - 1).$$

Proof. We show the indentity by induction. The base case $n = 2$ can be easily checked:

$$3g_1g_2 + h_1h_2 = (g_1+h_1)(g_2+h_2) + g_1(g_2-h_2) + g_2(g_1-h_1). \tag{4.3}$$

Assume (4.2) holds up to $n-1$, we show it for n. First, by substituting $3^{n-2} g_2 \dots g_n$ for g_2 and $h_2 \dots h_n$ for h_2 in (4.3), we have:

$$\begin{aligned} 3^{n-1} g_1 \dots g_n + h_1 \dots h_n \;=\; (g_1+h_1) \underbrace{(3^{n-2} g_2 \dots g_n + h_2 \dots h_n)}_{A} \,+ \\ g_1 \underbrace{(3^{n-2} g_2 \dots g_n - h_2 \dots h_n)}_{B} + \underbrace{3^{n-2} g_2 \dots g_n (g_1 - h_1)}_{C}. \end{aligned}$$

Now for term A, we directly apply (4.2) for $n-1$ and variables $g_2, \dots, g_n$, $h_2, \dots, h_n$. For term B, we change variable from $-h_2$ to h_2 and also apply (4.2) with $n-1$. Term C corresponds to that in (4.2) with $S = \{1\}$. The sign functions $\sigma_j(S)$ and $\tau_j(S)$ can be understood as follows. If $j = \max(S)$ then h_j switches sign, just like h_1 in term C. If $j-1 \in S$ then h_j does not switch sign, just like h_2 in term A. If $j-1 \notin S$ then h_j does switch sign, just like h_2 in term B. Finally, the function $\delta(S)$ corresponds to the power 3^{n-2} in term C. □

The point of Lemma 4.1 is that if $q_i(t) = \prod_{j=1}^{n} h_{ij}(t)$, where $h_{ij}(t) = \lfloor \alpha_{ij} t + \beta_{ij} \rfloor$, and $g \in \mathbb{N}$ is big enough then we can write:

$$q_i(t) + 3^{n-1} g^n = h_{i1}(t) \dots h_{in}(t) + 3^{n-1} g^n = \sum_{S\subseteq[n],\, S\neq\varnothing} 3^{\delta(S)}\, g^{n-|S|} \prod_{j\in S} \big(g \,\pm\, h_{ij}(t)\big). \tag{4.4}$$

Now the trapezoid construction from Section 2 can be applied to each term $g \pm h_{ij}(t)$. In other words, for each j, we construct two trapezoids F_{ij}^{+} and F_{ij}^{-} so that:

$$|F_{ij}^{+} + t\vec{v}| = g + h_{ij}(t \bmod N) \quad \text{and} \quad |F_{ij}^{-} + t\vec{v}| = g - h_{ij}(t \bmod N) \quad \text{for every} \quad t \in \mathbb{Z}.$$

For each $S \subseteq [n]$ in the sum in (4.4), we take product of the trapezoids for the terms $g \pm h_{ij}(t)$ with the construction from Section 2.3. This results in some polytope P'_S in

$\mathbb{R}^{|S|+1}$ with $2^{|S|+1}$ vertices. Then we take a prism of height $3^{\delta(S)}g^{n-|S|}$ over P'_S to get a polytope $P_S \in \mathbb{R}^{|S|+2}$ with $2^{|S|+2}$ vertices such that:

$$|P_S + t\vec{v}| \;=\; 3^{\delta(S)}g^{n-|S|}\prod_{j\in S}\big(g \,\pm\, h_{ij}(t \bmod N)\big) \quad \text{for every} \quad t \in \mathbb{Z}.$$

By padding in extra dimensions, we can assume each $P_S \subset \mathbb{R}^{n+2}$. To sum over all S ($2^n - 1$ of them), we pad in another extra n dimensions, and augment each P_S with the coordinates of a distinct point in $\{0,1\}^n$ similarly to (2.7). The resulting polytopes $Q_S \subset \mathbb{R}^{2n+2}$ still satisfy $|P_S| = |Q_S|$. We then take the convex hull of all Q_S to get a polytope $W_i \subset \mathbb{R}^{2n+2}$ such that:

$$|W_i + t\vec{v}| \;=\; \sum_{S\subseteq[n],\,S\neq\varnothing} 3^{\delta(S)}g^{n-|S|}\prod_{j\in S}\big(g \,\pm\, h_{ij}(t \bmod N)\big) \;=\; q_i(t \bmod N) + 3^{n-1}g^n.$$

for ever $t \in \mathbb{Z}$. See Section 2.4 for an explanation of the additivity in the counting functions. Note that W_i has at most $(2^n-1)2^{n+2} < 4^{n+1}$ vertices.

Now we have a polytope $W_i \subset \mathbb{R}^{2n+2}$ for each term $q_i(t) = \prod_{j=1}^{n}\lfloor \alpha_{ij}t + \beta_{ij}\rfloor$ in (4.1). Again, to sum up q_i over $1 \le i \le r$, we pad each W_i with $\lceil \log r\rceil$ extra dimensions and augment it with a distinct point in $\{0,1\}^{\lceil \log r\rceil}$. Taking their convex hull, we get $P \subset \mathbb{R}^d$ such that

$$p(t \bmod N) + r3^{n-1}g \;=\; |P + t\vec{v}| \quad \text{for every} \quad t \in \mathbb{Z}.$$

Here $d = 2n + 2 + \lceil \log r\rceil$ is the dimension, and P has at most $r4^{n+1}$ vertices. In this construction, we only need $g > |h_{ij}(t)|$ for all $1 \le i \le r, 1 \le j \le n$ and $0 \le j < N$. So $g = 2\lceil \max|\alpha_{ij}|N + \max|\beta_{ij}|\rceil$ suffices. We let $K = r3^{n-1}g$.

Finally, the argument from Section 4.1 can be applied to P. This gives a polytope $Q \subset \mathbb{R}^d$ (with the same number of vertices) and an $M \in \mathbb{N}$ so that:

$$p(t) + K \;=\; |P + t\vec{v}| \;=\; |(t+M)Q| \;=\; f_Q(t+M) \quad \text{for every} \quad 0 \le t < N.$$

This finishes the proof of Theorem 1.5. □

5. Integer polytopes

While much of the paper deals with rational polytopes in fixed dimensions, we can ask similar questions about *integer polytopes* (polytopes with vertices in $\mathbb{Z}^n$).

Proposition 5.1. *For integer polytopes, the* k-ETP *problem can be solved in polynomial time.*

Proof. The Ehrhart polynomial $f_P(t)$ of an integer polytope $P \subset \mathbb{R}^n$ is a monotone polynomial of degree at most n, see e.g. [Bar08]. Since n is fixed, the coefficients of $f_P(t)$ can be computed using Lagrange interpolation. Now apply the binary search to solve the k-ETP problem from definition. □

Note that this approach also extends to (rational) polytopes P with a fixed *denominator*, defined as the smallest $t \in \mathbb{Z}_+$ such that tP is integer.

For Polytope Translation, we do not know if Theorem 1.2 continues to hold for integer polytopes. However, it is not difficult to see that Theorem 1.3 extends to this setting:

Theorem 5.2. *Given an integer polytope* $P \subset \mathbb{R}^6$ *with at most* 64 *vertices and an integer* $N \in \mathbb{N}$*, minimizing* $|P + t\vec{e}_1/N|$ *over* $t \in \mathbb{Z}$ *is* NP*-hard.*

Sketch of proof. The trapezoids in Section 2.2 can be reused, with the ε's removed to make all their vertices integer.[4] A small complication arises for trapezoids of type F_D in Figure 2, because now $|F_D + t\vec{v}| = r' - \lfloor (t-1)/\beta \rfloor$ instead of $r' - \lfloor t/\beta \rfloor$. This is easily circumvented by considering only $t \in [0, N)$ s.t. $\beta \nmid t$, and thus $\lfloor (t-1)/\beta \rfloor = \lfloor t/\beta \rfloor$. The remaining $t \in [0, N)$ with $\beta | t$ can be ignored because they correspond to $v = 0$ in (2.1), which can be checked directly. □

For the special case of *integer polygons*, the number of integer points vary quite nicely under translation (cf. [EH12]).

Proposition 5.3. *For every fixed m, the* Polytope Translation *problem for integer m-gons can be solved in polynomial time.*

Proof. Let $Q \subset \mathbb{R}^2$ be an integer m-gon. Then $f(\lambda) := |Q + \lambda \vec{e}_1|$ is a sum of at most m terms of the form $\big(a_i + b_i \lfloor c_i \, \lambda \rfloor\big)$, for some $a_i, b_i, c_i \in \mathbb{Q}$. Then the generating function

$$F_{Q,N}(z, w) \, := \, \sum_{k=0}^{N-1} z^k \, w^{f(k/N)}$$

can be written in the *short GF form* (see [BP99, BW03]). Here $1/N$ is a small enough refinement of the unit interval. Then the short GF technique of taking projections can be applied to $F_{Q,N}(z, w)$ to find the minimum of $f(k/N)$ in polynomial time. We omit the details. □

Curiously, Alhajjar proved in [Alh17, Prop. 4.15], that for every integer polygon $Q \subset \mathbb{R}^2$, the corresponding maximization problem is trivial:

$$|Q| \, > \, |Q + \lambda \vec{e}_1|, \quad \text{for all } \; 0 < \lambda < 1.$$

This does not extend to $\mathbb{R}^3$, however. For example, take $\Delta \subset \mathbb{R}^3$ defined as the convex hull of points $(0,0,0)$, $(1,0,0)$, $(0,1,k)$ and $(1,-1,k)$. Then $|\Delta| = 4$, while $\big|\Delta + (1/2, 0, 0)\big| = k+1$, which is unbounded.

Finally, let us mention a large body of work on coefficients of the *h^*-vector* for the Ehrhart polynomials of integer polytopes. This gives further restrictions on the values $f_Q(t)$ as in Corollary 1.6. We refer to [Bra16] for a recent survey article and references therein.

6. Final remarks and open problems

6.1. Now that Polytope Translation is NP-hard, it would be interesting to know its true complexity. First, it is clearly in PSPACE. Also our proof is robust enough to allow embedding of general polynomial optimization decision problems (cf. [DHKW06]). Although we were unable to find a more general optimization problem that fits our framework, we hope to return to this in the future.

Note that in computational complexity, counting oracles are extremely powerful, as shown by Toda's theorem (see e.g. [AB09, Pap94]). From this point of view, our Theorem 1.2 is unsurprising, since it uses a counting oracle in a restricted setting.

[4] Those ε's only mattered in Section 3, where we say that small perturbation does not change the number of integer points in the trapezoids.

6.2. In another direction, it would be interesting to see if Polytope Translation remains NP-hard in lower dimensions. We believe that dimension 6 is Theorem 1.2 is not sharp.

Conjecture 6.1. *The* Polytope Translation *problem for rational polytopes $P \subset \mathbb{R}^3$ is* NP*-hard.*

In the plane, the polygon translation problem (with a fixed number of vertices) seem to have additional structures that prevent it from being computationally hard. In the special case of rational trapezoids, it can be reduced to a Diophantine approximation problem of unknown complexity (see the approach in [EH12]). We conjecture that the polygon translation problem is in NP.

Similarly, we believe that hardness still holds for much simpler types of polytopes:

Conjecture 6.2. *For some fixed n, the* Polytope Translation *problem for rational simplices $\Delta \subset \mathbb{R}^n$ is* NP*-hard.*

In $\mathbb{R}^2$, we believe in a weaker claim:

Conjecture 6.3. *The* Polytope Translation *problem for rational triangles $\Delta \subset \mathbb{R}^2$ is* Integer Factoring*-hard.*

By analogy, we believe that Theorem 1.4 also holds for simplices:

Conjecture 6.4. *k-*ETP *is* NP*-hard for rational simplices $\Delta \in \mathbb{R}^n$, for some fixed n.*

A significantly stronger result would be the following:

Conjecture 6.5. *The k-*Frobenius Problem *is* NP*-hard for some fixed n.*

6.3. Corollary 1.6 is the type of universality result which occasionally arise in discrete and algebraic geometry (see e.g. §§12,13 in [Pak09] and references therein). It would be interesting to find a simple or more direct proof of this result. In fact, we conjecture that the dimension bound $d = O(\log r)$ is sharp, cf. Prop. 8.1 in [NP17a].

Acknowledgements. We are thankful to Fritz Eisenbrand for telling us about the IPM problem, to Sasha Barvinok for introducing us to the subject, and to Jesús De Loera for his insights and encouragement. We are also grateful to Elie Alhajjar, Matt Beck, Lenny Fukshansky, Robert Hildebrand, Ravi Kannan, Oleg Karpenkov, Matthias Köppe and Kevin Woods for interesting conversations and helpful remarks. This work was initiated while both authors were in residence of the MSRI long term Combinatorics program in the Fall of 2017; we thank MSRI for the hospitality. The first author was partially supported by the UCLA Dissertation Year Fellowship. The second author was partially supported by the NSF.

References

[Alh17] E. Alhajjar, *A New Valuation on Lattice Polytopes*, Ph.D. thesis, George Mason University, 2017, 100 pp.

[ADL16] I. Aliev, J. A. De Loera and Q. Louveaux, Parametric polyhedra with at least k lattice points: their semigroup structure and the k-Frobenius problem, in *Recent trends in combinatorics*, Springer, Berlin, 2016, 753–778.

[AHL13] I. Aliev, M. Henk and E. Linke, Integer points in knapsack polytopes and s-covering radius, *Electron. J. Combin.* **20** (2013), no. 2, Paper 42, 17 pp.

[AB09] S. Arora and B. Barak, *Computational complexity. A modern approach*, Cambridge Univ. Press, Cambridge, UK, 2009.

[B+12] V. Baldoni, N. Berline, J. A. De Loera, M. Köppe and M. Vergne, Computation of the highest coefficients of weighted Ehrhart quasi-polynomials of rational polyhedra, *Found. Comput. Math.* **12** (2012), 435–469.

[Bar93] A. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the fimension is fixed, in *Proc. 34th FOCS*, IEEE, Los Alamitos, CA, 1993, 566–572.

[Bar06a] A. Barvinok, Computing the Ehrhart quasi-polynomial of a rational simplex, *Math. Comput.* **75** (2006), 1449–1466.

[Bar06b] A. Barvinok, The complexity of generating functions for integer points in polyhedra and beyond, in *Proc. ICM*, Vol. 3, EMS, Zürich, 2006, 763–787.

[Bar08] A. Barvinok, *Integer points in polyhedra*, EMS, Zürich, 2008.

[Bar17] A. Barvinok, Lattice points and lattice polytopes, to appear in *Handbook of Discrete and Computational Geometry* (third edition), CRC Press, Boca Raton, FL, 2017, 26 pp.

[BP99] A. Barvinok and J. E. Pommersheim, An algorithmic theory of lattice points in polyhedra, in *New Perspectives in Algebraic Combinatorics*, Cambridge Univ. Press, Cambridge, 1999, 91–147.

[BW03] A. Barvinok and K. Woods, Short rational generating functions for lattice point problems, *Jour. AMS* **16** (2003), 957–979.

[BR04] M. Beck and S. Robins, A formula related to the Frobenius problem in two dimensions, in *Number theory*, Springer, New York, 2004, 17–23.

[BSW08] M. Beck, S. V. Sam and K. M. Woods, Maximal periods of (Ehrhart) quasi-polynomials, *J. Combin. Theory, Ser. A* **115** (2008), 517–525.

[BHNW05] D. Beihoffer, J. Hendry, A. Nijenhuis and S. Wagon, Faster algorithms for Frobenius numbers, *Electron. J. Combin.* **12** (2005), RP 27, 38 pp.

[Bra16] B. Braun, Unimodality problems in Ehrhart theory, in *Recent trends in combinatorics*, Springer, Cham, 2016, 687–711.

[DHKW06] J. A. De Loera, R. Hemmecke, M. Köppe and R. Weismantel, Integer Polynomial Optimization in Fixed Dimension, *Math. Oper. Research* **31** (2006), 147–153.

[Eis10] F. Eisenbrand, Integer programming and algorithmic geometry of numbers, in *50 years of Integer Programming*, Springer, Berlin, 2010, 505–560.

[EH12] F. Eisenbrand and N. Hähnle, Minimizing the number of lattice points in a translated polygon, in *Proc. 24th SODA*, SIAM, Philadelphia, PA, 2012, 1123–1130.

[ES08] F. Eisenbrand and G. Shmonin, Parametric integer programming in fixed dimension, *Math. Oper. Res.* **33** (2008), 839–850.

[FS11] L. Fukshansky and A. Schürmann, Bounds on generalized Frobenius numbers, *European J. Combin.* **32** (2011), 361–368.

[GJ79] M. R. Garey and D. S. Johnson, *Computers and intractability. A guide to the theory of NP-completeness*, Freeman, San Francisco, CA, 1979.

[Kan90] R. Kannan, Test sets for integer programs, $\forall\exists$ sentences, in *Polyhedral Combinatorics*, AMS, Providence, RI, 1990, 39–47.

[Kan92] R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica* **12** (1992), 161–177.

[Len83] H. Lenstra, Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (1983), 538–548.

[MA78] K. Manders and L. Adleman, NP-complete decision problems for binary quadratics, *J. Comput. System Sci.* **16** (1978), 168–184.

[MR18] T. B. McAllister and H. Rochais, Periods of Ehrhart coefficients of rational polytopes, *Electron. J. Combin.* **25** (2018), no. 1, Paper 1.64, 10 pp.

[NP17a] D. Nguyen and I. Pak, The computational complexity of integer programming with alternations, to appear in *Math. Oper. Research*; extended abstract in *Proc. 32nd CCC* (2017), Art. 6, pp. 6:1–6:18.

[NP17b] D. Nguyen and I. Pak, Short Presburger arithmetic is hard, to appear in *SIAM Jour. Comp.*; extended abstract in *Proc. 58th FOCS*, IEEE, 2017, 37–48.

[NP18] D. Nguyen and I. Pak, Complexity of short generating functions, *Forum Math. Sigma* **6** (2018), paper E1, 37 pp.

[Pak09] I. Pak, *Lectures on Discrete and Polyhedral Geometry*, monograph draft, 2009; availabel at `http://www.math.ucla.edu/~pak/book.htm`

[Pap94] C. H. Papadimitriou, *Computational complexity*, Addison-Wesley, Reading, MA, 1994.

[RA96] J. L. Ramírez Alfonsín, Complexity of the Frobenius problem, *Combinatorica* **16** (1996), 143–147.

[RA05] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Univ. Press, Oxford, 2005.

[Sch86] A. Schrijver, *Theory of linear and integer programming*, John Wiley, Chichester, 1986.

[VW08] S. Verdoolaege, K. Woods, Counting with rational generating functions, *J. Symbolic Comput.* **43** (2008), 75–91.

[Woo04] K. Woods, *Rational Generating Functions and Lattice Point Sets*, Ph.D. thesis, University of Michigan, 2004, 112 pp.

[Woo05] K. Woods, Computing the period of an Ehrhart quasi-polynomial, *Electron. J. Combin.* **12** (2005), RP 34, 12 pp.