UNIVERSITY OF CALIFORNIA
Los Angeles

The Computational Complexity of Presburger Arithmetic

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Danh Nguyen Luu

2018

ABSTRACT OF THE DISSERTATION

The Computational Complexity of
Presburger Arithmetic

by

Danh Nguyen Luu
Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2018
Professor Igor Pak, Chair

A wide variety of problems in Discrete Optimization and Integer Programming can be naturally phrased in the language of *Presburger Arithmetic* (PA), which is the first order logic on the integers with only additions and inequalities. Understanding the exact computational complexity of PA is a classical topic in both logic and computer science. In this dissertation, we give answers to several open questions in this area.

Most important in PA are the numbers of variables and inequalities involved. The main question addressed in Part I of the dissertation is: By restricting the number of variables and inequalities in PA, do we obtain polynomial complexity? We give a negative solution to this, which also settles two questions by Kannan and Barvinok–Woods on *Parametric Integer Programming* and *Short Presburger Arithmetic*, respectively. Our argument combines elements from Number Theory and Discrete Geometry. As applications, we apply our tools to analyze the *VC-dimensions* of PA formulas, as well as a variant theory, called *Parametric Presburger Arithmetic*.

In Part II, we investigate the related theory of *Short Generating Functions* developed by Barvinok and Woods. First, we first extend their polynomial time algorithm for enumerating projected integer points in polytopes to the unbounded polyhedra case. Then we demonstrate several limitations of their general theory under simple point set operations such as

projection and union, in the sense that the lengths of the generating functions do not remain polynomially bounded. The reasoning here parallels with Part I, and crucially exploits the structures of PA definable sets.

In Part III, we present two different problems. The first one concerns an extension of PA with scalar multiplications by algebraic irrationals. We show that it has high non-elementary complexity far exceeding that of classical PA, even with a restricted number of variables and inequalities. The second problem is about minimizing the number of integer points in a polytope under translation. We show that it is NP-hard by embedding arbitrary polynomial functions as integer point counting functions of polytopes. We derive from this a consequence about the universality of *Ehrhart quasi-polynomials*.

The dissertation of Danh Nguyen Luu is approved.

Matthias J. Aschenbrenner

Artem Chernikov

Alexander Sherstov

Igor Pak, Committee Chair

University of California, Los Angeles

2018

For my family.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

First, I would like to thank my advisor, Igor Pak, for his guidance and support throughout my PhD research period at UCLA. I have learnt a lot about mathematics and problem solving from him after five years.

This thesis would not be possible without the emotional support from my parents and my dear wife Quyen Phan. To them I owe the deepest gratitude for always reminding me of my origin and sharing with me so much.

I also thank many friends at UCLA and elsewhere, including Dustan Levenstein, Bonsoon Lin, John Susice, Quang-Nhat Le, Swee Hong Chan and Rupei Xu, with whom I have shared a lot about math and life.

I am grateful to Iskander Aliev, Matthias Aschenbrenner, Sacha Barvinok, Tristram Bogart, Artëm Chernikov, Jesús De Loera, Fritz Eisenbrand, Lenny Fukshansky, John Goodrick, Philipp Hieronymi, Robert Hildebrand, Ravi Kannan, Nathan Kaplan, Oleg Karpenkov, Matthias Köppe, Jamie Pommersheim, Sinai Robins, Sacha Sherstov, Terry Tao, Kevin Woods, and many others, for their very helpful opinions about this work, as well as many valuable suggestions.

All the work in this thesis is are adapted from my earlier joint research papers:

- Chapter 2, 3, 4, 6, 7 and 9 are from the joint works [NP17c, NP17b, NP17a, NP17f, NP17d] and [NP18] with Igor Pak, in that order.
- Chapter 5 is from the joint work [BGNW18] with Tristram Bogart, John Goodrick and Kevin Woods.
- Chapter 8 is from the joint work [HNP18] Philipp Hieronymi and Igor Pak.

Compared to their original versions, some results and proofs here have been improved.

Lastly, part of this work was supported by the 2017–2018 Dissertation Year Fellowship of UCLA. I also thank MSRI for their extraordinary hospitality in hosting the Discrete and Topological Geometry research program in Fall 2018, where I was a participant.

VITA

2005–2008	Ly Tu Trong high school, Can Tho, Vietnam.
2008–2011	BSc in Mathematics, Nanyang Technological University, Singapore.
2011–2013	Research & Teaching Assistant, Nanyang Technology University, Singapore.
2013–2016	MSc in Mathematics, University of California, Los Angeles.
2016–2018	PhD candidate in Mathematics, University of California, Los Angeles.

NOTATIONS AND TERMINOLOGY

- We use $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z}_+ = \{1, 2, \ldots\}$ and $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$.
- The first coordinate vector $(1, 0, \ldots)$ is denoted by $\vec{e}_1$.
- Half-open intervals are denoted by $[\alpha, \beta)$, $(\alpha, \beta]$, etc.
- Variables are denoted by x, y, z, etc.; tuples/vectors of variables are denoted by $\mathbf{x}, \mathbf{y}, \mathbf{z}$, etc.
- We write $\mathbf{x} \leq \mathbf{y}$ if $x_j \leq y_j$ for every i, and $\mathbf{x} \leq N$ if $x_i \leq N$ for every i.
- Constant vectors are denoted by $\overline{a}, \overline{b}, \overline{x}, \overline{y}, \overline{t}, \overline{v}, \overline{\gamma}, \overline{\delta}$ etc.
- We use 0 to denote both zero and the zero vector. Similarly for 1.
- Matrices are denoted by A, B, C, etc.
- The usual matrix-vector multiplication is denoted by $A\mathbf{x}, B\mathbf{y}, C\mathbf{z}$, etc.
- A system of linear inequalities is written in the form $A\mathbf{x} \leq \overline{b}$.
- For $x \in \mathbb{R}$, we denote by $\{\{x\}\}$ the distance from x to the closest integer.
- The usual floor function is denoted by $\lfloor \cdot \rfloor$.
- The the vector $\mathbf{y}$ with coordinates $y_i = \lfloor x_i \rfloor$ is denoted by $\mathbf{y} = \lfloor \mathbf{x} \rfloor$.
- The ℓ_∞–norm of $\mathbf{x}$ is denoted by $\|\mathbf{x}\|_\infty$ or simply $|\mathbf{x}|$.
- For two tuples $\mathbf{x}$ and $\mathbf{t}$ both of length n, we denote by $\mathbf{t}^{\mathbf{x}}$ the monomial $t_1^{x_1} \ldots t_n^{x_n}$.
- Universal/existential quantifiers are denoted by $\forall/\exists$.
- Unspecified quantifiers are denoted by Q_1, Q_2, etc.
- Presburger expressions are denoted by Φ, Ψ, etc.
- The symbols $\neg, \wedge, \vee$ denote negation, conjunction and disjunction, respectively.
- We sometimes write $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ for a disjunction $(a \vee b)$, and $\left\{\begin{smallmatrix} a \\ b \end{smallmatrix}\right\}$ for a conjunction $(a \wedge b)$.
- A *polyhedron* is an intersection of finitely many closed half-spaces in $\mathbb{R}^n$.
- A *polytope* is a bounded polyhedron.
- Polyhedra and polytopes are denoted by P, Q, R, etc.

- $P + \vec{w}$ denotes the translation of P by vector $\vec{w}$.
- The *affine dimension* of P is denoted by $\dim(P)$.
- The *convex hull* of several sets $S_1, \ldots, S_k$ is denoted by $\mathrm{conv}(S_1, \ldots, S_k)$.
- For a bounded set $S \subset \mathbb{R}^n$, we denote by $|S|$ the cardinality of $S \cap \mathbb{Z}^n$.
- Integer lattices are denoted by $\mathcal{L}, \mathcal{T}, \mathcal{U}, \mathcal{W}$, etc.
- A *pattern*, i.e., a union of some cosets of a lattice, is denoted by $\boldsymbol{L}, \boldsymbol{T}, \boldsymbol{S}, \boldsymbol{U}, \boldsymbol{W}$, etc.
- The *rank* of lattice $\mathcal{L}$ is denoted by $\mathrm{rank}(\mathcal{L})$.
- GF is an abbreviation for "*generating function*."
- Multivariate GFs are denoted by $f(\mathbf{t}), g(\mathbf{t}), h(\mathbf{t})$, etc.
- The support of a GF $f(\mathbf{t})$ is denoted by $\mathrm{supp}(f)$.
- We use $\ell(\cdot)$ denotes the *binary length* of a number, vector, matrix, GF, or a logical formula.
- If a polyhedron Q given by a system $A\mathbf{x} \le \overline{b}$, its length $\ell(Q)$ is $\ell(A) + \ell(\overline{b})$.
- If a lattice $\mathcal{L}$ generated by the columns in a matrix A, its length $\ell(\mathcal{L})$ is $\ell(A)$.
- When the ambient space $\mathbb{R}^n$ is clear, we use $\{x_i = \xi_i, \ldots, x_j = \xi_j\}$ to denote the subspace with specified coordinates $x_i = \xi_i, \ldots, x_j = \xi_j$.
- We write $f(t) = O(g(t))$ if $f(t)/g(t) < c$ for some $c \in \mathbb{R}_+$ as $t \to \infty$.
- We write $f(t) = \Omega(g(t))$ if $g(t) = O(f(t))$.
- We write $f(t) = \Theta(g(t))$ if $f(t) = O(g(t))$ and $g(t) = O(f(t))$.
- We write $f(t) \gg g(t)$ or $g(t) = o(f(t))$ if $g(t)/f(t) \to 0$ as $t \to \infty$.
- We write $f(t) \sim g(t)$ for $f(t)/g(t) \to 1$ as $t \to \infty$.
- $\mathrm{Ost}(X)$ denotes the set of *convergents* q_n with non-zero coefficients in the Ostrowski representation of $X \in \mathbb{N}$.
- We write $v \in \mathrm{Ost}(X)$ if v is a convergent with a non-zero coefficient in the Ostrowski representation of X.

Part I

Presburger Arithmetic

CHAPTER 1

Background

The goal of this dissertation is to understand in detail the computational complexity of Presburger Arithmetic (PA). This logic theory was started by Mojżesz Presburger in 1929, and studied extensively later on by many other researchers, notably Skolem. Formally, PA is the first order theory of the natural numbers with additions and the natural ordering, denoted by PA $= \langle \mathbb{N}; +, = \rangle$. One can show that PA is equivalent to $\langle \mathbb{Z}; +, \leq \rangle$, i.e., the first order theory on integers with addition and inequalities. The most important properties of PA are its completeness and decidability ([Pre29]).

Example 1.1. Observe that any integer greater than 12 can be written as a non-negative combination of 3 and 7. In PA, this simply reads $\forall x \geq 13 \;\; \exists y_1, y_2 \geq 0 \;:\; x = 3y_1 + 7y_2$.

Note that we can always express an equality by a pair of inequalities. As a first order theory, PA also allows arbitrarily many $\forall$ and $\exists$ quantifiers. Being decidable, PA admits a decision algorithm to decide the truth of any sentence in it. More generally, PA has *quantifier elimination*, i.e., there is an algorithm to repeatedly eliminate all quantifiers from a given PA sentence or formula. This raised the question: How effective can such an algorithm be, measured with respect to the input length of a PA sentence?

General Complexity

Fischer and Rabin showed in 1974 that PA has very high complexity in the general case:

Theorem 1.2 ([FR74])**.** *Any non-deterministic decision algorithm for PA runs in time at least doubly exponential, i.e.,* $\Omega\big(2^{2^{c\ell}}\big)$*, where* ℓ *is the length of the sentence* Φ *to be decided, and* $c > 0$ *is a constant.*

At the same time, a corresponding upper bound is known:

Theorem 1.3 ([Opp78])**.** *There is a deterministic triply exponential quantifier elimination algorithm for PA. In particular, PA sentences can be decided in deterministic time triply exponential time, i.e.,* $O\big(2^{2^{2^{d\ell}}}\big)$*, for some constant* $d > 0$*.*

This algorithm was originally described by Cooper in [Coo72], and its complexity later analyzed by Oppen [Opp78]. It eliminates all quantifiers from a PA sentence/formula, at the cost of introducing extra congruence relations of the form $x \equiv a \pmod{b}$ for $a, b \in \mathbb{Z}$, which are much easier to verify. Many subsequent improvements to this algorithm were made, notably by Reddy and Loveland [RL78], who showed that the deterministic upper bound drops to doubly exponential if one restricts the number of *alternations* in PA, i.e., the number of times quantifiers switch between $\forall$ and $\exists$ in a sentence. Correspondingly, a nondeterministic exponential lower bound was shown in [Fü82] for restricted alternations (see also [Sca84]).

In fact, completeness results are known for restricted alternations: For every $k \geq 1$, the class PA_{k+1} of sentences with $k+1$ alternating quantifier blocks is complete for the k-th level $\mathbf{\Sigma}_k^{\mathsf{EXP}} \cup \mathbf{\Pi}_k^{\mathsf{EXP}}$ of the Weak Exponential Hierarchy [Haa14]. For the class PA_1, i.e., when quantifiers are all $\exists$ or $\forall$, it is complete for $\mathsf{NP} \cup \mathsf{coNP}$ [BT76]. So overall, the complexity of PA still remains intractable even when alternations are controlled.

Restricted number of variables

As we see from above, it makes sense to reduce the complexity of PA by further restricting the number of variables and inequalities in its sentences. In this direction, progress has been slow. The simplest sentences in PA are those coming from *Integer Programming* (IP), i.e., when all quantifiers are $\exists$, and the rest is a system (conjunction) of inequalities $A\mathbf{x} \leq \overline{b}$ in n variables $\mathbf{x} \in \mathbb{Z}^n$. In 1983, Lenstra proved a pioneer result:

Theorem 1.4 ([Len83])**.** *Fix the number* n *of variables. There is a polynomial time algorithm to decide if* $\exists \mathbf{x} \in \mathbb{Z}^n : A\,\mathbf{x} \leq \overline{v}$*, where* $A \in \mathbb{Z}^{m \times n}$ *and* $\overline{v} \in \mathbb{Z}^m$ *are given as input.*

Hereafter, the sentence's length is measured by the total binary length of all integer coefficients and constants (in this case the entries of A and $\overline{v}$). The polynomial degree of this algorithm crucially depends on the dimension n. Geometrically, it says that given a rational polyhedron P in fixed dimension $\mathbb{R}^n$, an integer solution $\mathbf{x} \in P$ can be found in polynomial time, or we can conclude that $P \cap \mathbb{Z}^n = \varnothing$. As a consequence, Scarpellini [Sca84] showed the system $A\mathbf{x} \leq \overline{b}$ in Theorem 1.4 can actually be replaced by a general Boolean combination of linear inequalities in $\mathbf{x}$. This means that *existential* PA in a fixed number of variables is always polynomial time decidable.

In [Grä87, Grä88], Grädel considered PA sentences with at least two alternating quantifiers and a fixed number of variables. He showed that the problem of deciding such sentences lies in the Polynomial Hierarchy (PH). He also gave, for every level in PH, such a class of sentences which is complete in it. Those results were later strengthened by Schöning in [Sch97]. They can be summed up as follows:

Theorem 1.5 ([Sch97])**.** *Let $Q_1, \ldots, Q_{k+1} \in \{\forall, \exists\}$ be $k+1$ alternating quantifiers. Then:*

i) *For every fixed $k \geq 1$, PA sentences of the form:*

$$Q_1\, x_1 \in \mathbb{Z} \quad \ldots \quad Q_k\, x_k \in \mathbb{Z} \quad Q_{k+1}\, \mathbf{y} \in \mathbb{Z}^3 \quad : \quad \Psi(x_1, \ldots, x_k, \mathbf{y})$$

are $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete if $Q_1 = \exists$, and $\mathbf{\Pi}_k^{\mathsf{P}}$-complete if $Q_1 = \forall$.

ii) *2-variable PA sentences $\exists x\, \forall y : \Psi(x, y)$ are NP-complete; and similar $\forall\exists$ sentences are coNP-complete.*

iii) *4-variable PA sentences $\exists x\, \forall y\, \exists z_1, z_2 : \Psi(x, y, z_1, z_2)$ are $\mathbf{\Sigma}_2^{\mathsf{P}}$-complete.*

Here the input Ψ is a Boolean combination of linear inequalities in the variables it contains. So compared to the existential case, already $\forall\exists$ sentences in two variables are intractable. However, note that Ψ here contains both conjunctions and disjunctions of inequalities. If we restrict Ψ to only a system of inequalities, then an analogue of Theorem 1.4 for $\forall\exists$ is in fact possible. It was a breakthrough when Kannan showed in 1990 that *Parametric Integer Programming* is polynomial in fixed dimensions:

Theorem 1.6 ([Kan90]). *Fix n_1 and n_2. There is a polynomial time algorithm to decide the sentence $\forall \mathbf{x}_1 \in \mathbb{Z}^{n_1} \ \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \ : \ A\,\mathbf{x}_1 + B\mathbf{x}_2 \leq \overline{v}$, given $A \in \mathbb{Z}^{m \times n_1}$, $B \in \mathbb{Z}^{m \times n_2}$ and $\overline{v} \in \mathbb{Z}^m$ as input.*

Compared to Theorem 1.4, this adds one more alternating quantifier to the sentence. Note that the number m of inequalities is still unrestricted. The proofs of theorems 1.4 and 1.6 both rely on geometric ideas, namely the ellipsoid method. The set of integer points in both problems lies in a polyhedron, whose convexity is of crucial importance. A natural way to generalize Theorem 1.6 was also posed by Kannan in 1992:

Question 1.7 ([Kan92]). Fix n_1, n_1 and n_3. Is there a polynomial time algorithm to decide, given $A \in \mathbb{Z}^{m \times n_1}$, $B \in \mathbb{Z}^{m \times n_2}$, $C \in \mathbb{Z}^{m \times n_3}$ and $\overline{v} \in \mathbb{Z}^m$, whether

$$\exists \mathbf{x}_1 \in \mathbb{Z}^{n_1} \quad \forall \mathbf{x}_2 \in \mathbb{Z}^{n_2} \quad \exists \mathbf{x}_3 \in \mathbb{Z}^{n_3} \quad : \quad A\mathbf{x}_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \ \leq \ \overline{v} \quad ? \tag{1.1}$$

In Chapter 2, we prove that deciding (1.1) is NP-complete, thus giving a negative answer to this question. For more alternating quantifiers, we also show that analogous sentences are in fact complete for every level of PH. Thus, restricting PA sentences to systems of inequalities does not improve their complexity beyond two alternating quantifiers. The geometric intuition mentioned earlier with polyhedra is now completely powerless.

Restricted number of variables and inequalities

Short Presburger Arithmetic consists of the most restricted PA sentences that we will study, whose numbers of alternations, variables *and* inequalities are all bounded. Woods proved in his PhD thesis [Woo04] that:

Theorem 1.8 (Woods). *Fix n_1, n_2 and m. Given $\Psi(\mathbf{x}_1, \mathbf{x}_2)$ a Boolean combination of at most m inequalities in the variables $\mathbf{x}_1 \in \mathbb{Z}^{n_1}$ and $\mathbf{x}_2 \in \mathbb{Z}^{n_2}$, then we can decide in polynomial time whether $\forall \mathbf{x}_1 \in \mathbb{Z}^{n_1} \ \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \ : \ \Psi(\mathbf{x}_1, \mathbf{x}_2)$. Moreover, we can also count in polynomial time the set $\left\{\mathbf{x}_1 \in \mathbb{Z}^{n_1} \ : \ \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \ \ \Psi(\mathbf{x}_1, \mathbf{x}_2)\right\}$.*

Note that this result also applies to $\exists\forall$ sentences via a simple negation operation. One should compare between theorems 1.6 and 1.8. In the former, the expression Ψ is a conjunction of an arbitrary number of inequalities, whereas in the latter it could contain both

conjunctions and disjunctions of inequalities, though only in fixed number. One can see that fixing m does restrict the geometric complexity of our formula quite severely. Indeed, now the set $\{(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{R}^{n_1+n_2} : \Psi(\mathbf{x}_1, \mathbf{x}_2) = \text{true}\}$ is determined by at most m halfspaces, which means it is a union of at most a constant number of polyhedral regions.[1] So one might suspect that such short PA sentences, even with more than two alternating quantifiers, are always polynomial time decidable. The following conjecture was our original motivation for this dissertation:

Conjecture 1.9 (Barvinok–Woods)**.** *Fix k, $n_1, \ldots, n_k$ and m. There is a polynomial time algorithm to decide short PA sentences of the form:*

$$Q_1 \mathbf{x}_1 \in \mathbb{Z}^{n_1} \ \ldots \ Q_k \mathbf{x}_k \in \mathbb{Z}^{n_k} \quad : \quad \Psi(\mathbf{x}_1, \ldots, \mathbf{x}_k). \tag{1.2}$$

Here $Q_1, \ldots, Q_k \in \{\exists, \forall\}$ are k alternating quantifiers, and Ψ is a Boolean combination of at most m linear inequalities in $\mathbf{x}_1, \ldots, \mathbf{x}_k$.

We emphasize that the input to (1.2) is just a fixed number of integer coefficients and constants in Ψ. Conjecture 1.9 was proposed in [Woo04, Bar06b], and has remained open since 2003. If true, it would in fact imply both theorems 1.4 and 1.6 as special cases.

In Chapter 3, we disprove Conjecture 1.9 by showing that short PA sentences do become complete for every level of PH, with the first intractable case being NP-hard for $k = 3$. Our proof relies on the arithmetics of continued fractions, which is rich enough to allow embedding of classical NP-hard problems. Geometrically, we exploit the structure of the *sail* of a rational cone C, which consists of the extremal integer point that lie inside C. Such extremal integer points are very well understood in the two dimensional case. They can in fact be obtained directly from the continued fraction expansion of C's slope, via a very simple linear recursion.

For the rest of Part I (chapters 4 and 5), we present two applications of our result in Chapter 3. The first one concerns the *VC-dimensions* of PA formulas, which is certain statistical measure of a logical formula's expressiveness. The second one studies *Parametric*

[1] The number of such regions is at most $O(m^{n_1+n_2})$.

Presburger Arithmetic, which is a variant of PA that allows two sort of variables. The implications of our result are in the negative direction for both problems.

Prerequisite

We will be using basic concepts and notations from logic and computational complexity, such as quantifier elimination, undecidability, halting problem, polynomial time reduction, NP-completeness, the complexity classes $\mathsf{P}, \mathsf{NP}, \#\mathsf{P}$, etc., and the polynomial hierarchy. We refer to the standard references [MM11, Pap94] for these. See [AB09] for a more modern treatment of computational complexity, and [Aa16] for a recent survey on the topic.

CHAPTER 2

Complexity of Integer Programming with alternations

In this chapter, we answer Question 1.7 in the negative: Integer Programming with three alternating quantifiers is NP-complete, even for at most six variables. This complements earlier results by Lenstra and Kannan, which together say that Integer Programming with at most two alternating quantifiers can be done in polynomial time for any fixed number of variables. As a byproduct, we show that for two polytopes $P, Q \subset \mathbb{R}^3$, counting the projections of integer points in $Q \backslash P$ under a linear map is #P-complete. This contrasts the 2003 result by Barvinok and Woods, which allows counting in polynomial time the projection of integer points in P and Q separately. This chapter is a version of the published paper [NP17c].

2.1. Introduction

2.1.A. Integer Programming. In a pioneer paper [Len83], Lenstra showed that Integer Programming in a bounded dimension can be solved in polynomial time (Theorem 1.4). The next breakthrough, Parametric Integer Programming, was obtained by Kannan in [Kan90]:

Theorem 2.1 (Th. 1.6 restated)**.** *Fix n_1 and n_2. Given $A \in \mathbb{Z}^{m \times n_1}$, $B \in \mathbb{Z}^{m \times n_2}$, $\overline{v} \in \mathbb{Z}^m$ and a polyhedron $P \subseteq \mathbb{R}^{n_1}$, the sentence:*

$$\forall \mathbf{x}_1 \in P \cap \mathbb{Z}^{n_1} \quad \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \quad : \quad A\mathbf{x}_1 + B\mathbf{x}_2 \ \leq \ \overline{v}. \tag{2.1}$$

can be decided in polynomial time. Here P is described by another system $W\mathbf{x}_1 \leq \overline{\gamma}$, with $W \in \mathbb{Z}^{m' \times n_1}$ and $\overline{\gamma} \in \mathbb{Z}^{m'}$.

Until recently, this remained the most general result in the positive direction (see [Eis10]).

In [Kan92], Kannan asked if Theorem 2.1 can be extended to three alternating quantifiers (Question 1.7). We give a negative answer to this, even with $n_1 = 1, n_2 = 2, n_3 = 3$:

Theorem 2.2. *Given $A \in \mathbb{Z}^{m\times 1}$, $B \in \mathbb{Z}^{m\times 2}$, $C \in \mathbb{Z}^{m\times 3}$, $\overline{v} \in \mathbb{Z}^m$, a segment $I \subset \mathbb{R}^1$ and a rectangle $J \subset \mathbb{R}^2$, then deciding the sentence:*

$$\exists x_1 \in I \cap \mathbb{Z}^1 \quad \forall \mathbf{x}_2 \in J \cap \mathbb{Z}^2 \quad \exists \mathbf{x}_3 \in \mathbb{Z}^3 \quad : \quad Ax_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \ \leq \ \overline{v} \tag{2.2}$$

is an NP*-complete problem. Here $I = [a, b]$ and $J = [c, d] \times [e, f]$ with $a, b, c, d, e, f \in \mathbb{Z}$ being part of the input.*

Let us emphasize that in both theorems 2.1 and 2.2, there is no bound on m, the number of inequalities involved. Nevertheless, by an easy application of the Doignon–Bell–Scarf theorem (§2.7.A), the sentence (2.1) is in fact polynomial time reducible to the case with a fixed m. The same cannot be said about (2.2), which leaves us with the complexity of (2.2) for a fixed m. This will become the focus of Chapter 3.

For now, recall Theorem 1.5 by Schöning, which says that deciding PA sentences with $k+1$ alternating quantifiers in a fixed number of variables is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete. For two quantifiers $\forall\exists$, theorems 1.5-ii) and 2.1 point to drastically different directions. This is because PA sentences in Theorem 1.5 allow both conjunction and disjunction of many inequalities, whereas Integer Programming sentences contain only conjunctions. This flexibility of PA sentences allows very effective reductions of classical hard decision problems such as QSAT. For some time, it remains open whether such reductions can be carried out using only conjunctions. Our Theorem 2.2 can actually be generalized to:

Theorem 2.3. *Analogues of* (2.2) *in a fixed number of variables with $k + 2$ alternating quantifiers are $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete, depending on whether k is odd or even. Here the sentence is allowed to contain only a system of inequalities.*

We refer to Theorem 2.11 for the precise statement. This result says that for a bounded number of variables, Integer Programming requires only one extra alternation to achieve the same complexity as PA sentences. In other words, we are trading one extra quantifier for a sentence that contains only conjunctions of inequalities.

On can also consider a "hybrid" version of (2.1) and Theorem 1.5-ii) with only two alternating quantifiers $\exists\forall$ and two disjunctions in the sentence. In Section 2.6, we show this is still NP-complete to decide.

2.1.B. Projections of integer points in non-convex polytopes. For polytopes of arbitrary dimensions, counting the number of integer points is classically #P-complete, even for those with 0/1 vertices. In a fixed dimension n, Barvinok famously showed this can be done in polynomial time:

Theorem 2.4 ([Bar93])**.** *Fix n. Given a rational polyhedron $P \subseteq \mathbb{R}^n$ (possibly unbounded), the number of integer points in P can be computed in polynomial time.*

Here the polyhedron can be described either by its facets or by its vertices. This was later generalized by Barvinok and Woods to count the number of *projected* integer points:

Theorem 2.5 ([BW03])**.** *Fix m and n. Given a rational polytope $Q \subset \mathbb{R}^m$ and a linear map $T : \mathbb{Z}^m \to \mathbb{Z}^n$, the number of points in $T(Q \cap \mathbb{Z}^m)$ can be computed in polynomial time.*

For a bounded set $S \subset \mathbb{R}^n$, denote by $|S|$ the cardinality of $S \cap \mathbb{Z}^n$. Also denote by $\mathrm{E}_1(S)$ the projection of $S \cap \mathbb{Z}^n$ on the first coordinate, i.e.,

$$\mathrm{E}_1(S) := \{x \in \mathbb{Z} \,:\, \exists \mathbf{z} \in \mathbb{Z}^{n-1} \text{ s.t. } (x, \mathbf{z}) \in S\}.$$

Now consider two polytopes $P \subset Q \subset \mathbb{R}^n$. We clearly have $|Q \backslash P| = |Q| - |P|$. So the number of integer points in the complement $Q \backslash P$ can also be computed effectively by Theorem 2.4. In the spirit of Theorem 2.5, we can ask whether the projections of integer points in $Q \backslash P$ can also be counted efficiently. We prove the following result:

Theorem 2.6. *Given two polytopes $P \subset Q \subset \mathbb{R}^3$, computing $|\mathrm{E}_1(Q \backslash P)|$ is #P-complete.*

In other words, it is #P-complete to compute the size of the set

$$\mathrm{E}_1(Q \backslash P) = \{x \in \mathbb{Z} \,:\, \exists \mathbf{z} \in \mathbb{Z}^2 \quad (x, \mathbf{z}) \in Q \backslash P\}. \tag{2.3}$$

Note that the corresponding decision problem $|\mathrm{E}_1(Q \backslash P)| \geq 1$ is equivalent to $|Q \backslash P| \geq 1$, and thus can be decided in polynomial time by applying Theorem 2.4.

The contrast between Theorem 2.5 and our negative result can be explained as follows. The proof Theorem 2.5 depends on the polytopal structure of P and exploits convexity in a crucial way. By taking the complement $Q\backslash P$, we no longer have a convex set. In other words, we show that projection of the complement $Q\backslash P$ is complicated enough to allow encoding of hard counting problems, even in $\mathbb{R}^3$ (see also §2.7.D).

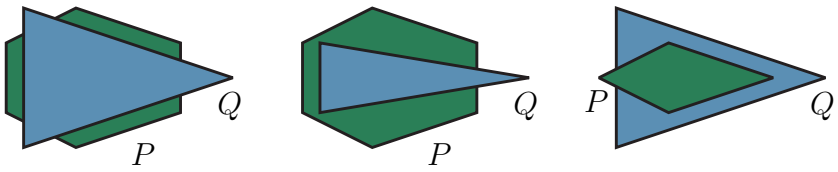


Figure 2.1: Three examples of convex polygons $P, Q \subset \mathbb{R}^2$.

Remark 2.7. To understand Theorem 2.6, consider three examples of polygons $P, Q \subset \mathbb{R}^2$ as in Figure 2.1. Note that the sets of integer points of the vertical projections of P, Q and $P \cup Q$ are the same in all three cases, but the sets number of integer points of the vertical projections of $Q\backslash P$ are quite different.

2.1.C. Outline of the chapter. We begin with a geometric construction of certain polytopes based on Fibonacci numbers (Section 2.2). In Section 2.3 we use this construction to prove Theorem 2.2 via a reduction of the Good Simultaneous Approximation (GSA) problem in Number Theory, which is known to be NP-complete. The proof of Theorem 2.3 is via a reduction of QSAT (Section 2.4). The proof of Theorem 2.6 follows a similar route via reduction of #GSA (Section 2.5). Then we show that a "hybrid" version of (2.2) and Theorem 1.5-ii) with only two quantifiers and two disjunctions is still NP-complete to decide (Section 2.6). We conclude the chapter with final remarks and open problems (Section 2.7).

2.2. Geometric constructions and properties

2.2.A. Fibonacci points. We consider the first $2d$ *Fibonacci numbers*:

$$F_0 = 0, F_1 = 1, F_2 = 1, \ldots, F_{2d-1}.$$

From these, we construct d integer points:

$$\phi_1 = (F_1, F_0),\ \phi_2 = (F_3, F_2),\ \ldots,\ \phi_d = (F_{2d-1}, F_{2d-2}). \tag{2.4}$$

Let

$$\mathcal{F} = \{\phi_1, \ldots, \phi_d\} \subset \mathbb{Z}^2 \quad \text{and} \quad J = [1, F_{2d-1}] \times [0, F_{2d-2}] \cap \mathbb{Z}^2. \tag{2.5}$$

We have $\mathcal{F} \subset J$. Denote by $\mathcal{C}$ the curve consisting of $d-1$ segments connecting ϕ_i to ϕ_{i+1} for $i = 1, \ldots, i-1$.

We also define the following two polygons. Their properties will be mentioned later.

$$R_1 = \left\{ \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2 \ :\ y_1 \geq 1,\ y_2 \leq F_{2d-2},\ y_2 F_{2d-1} - y_1 F_{2d-2} \geq 1 \right\}, \tag{2.6}$$

$$R_2 = \left\{ \mathbf{y} \in \mathbb{R}^2 \ :\ y_1 \leq F_{2d-1},\ y_2 \geq 0 \ \text{ and } \ y_2 F_{2i} - y_1 F_{2i-1} \leq -2 \ \text{ for } \ i = 1, \ldots, d \right\}. \tag{2.7}$$

The following properties are straightforward from the above definitions:

(F1) The points $\phi_1, \ldots, \phi_d$ are in convex position. The curve $\mathcal{C}$ connecting them is convex (upwards). See Figure 2.2.

(F2) Each segment $(\phi_i\, \phi_{i+1})$ and each triangle $\Delta_i = (0\, \phi_i\, \phi_{i+1})$ has no interior integer points. This can be deduced from the facts that two consecutive Fibonacci numbers are co-prime, and also

$$F_i F_{i+3} - F_{i+1} F_{i+2} = (-1)^{i-1} \quad \text{for all } i \geq 0.$$

(F3) The set of integer points in $J \backslash \mathcal{F}$ can be partitioned into two parts: those lying strictly above the convex curve $\mathcal{C}$, and those lying strictly below it.

(F4) The part of $J \backslash \mathcal{F}$ lying above $\mathcal{C}$ is exactly $R_1 \cap \mathbb{Z}^2$. This can be seen as follows. The line $\boldsymbol{l}$ connecting 0 and ϕ_d is defined by:

$$y_2 F_{2d-1} - y_1 F_{2d-2} = 0.$$

So every integer point $\mathbf{y} = (y_1, y_2)$ lying above $\boldsymbol{l}$ satisfies:

$$y_2 F_{2d-1} - y_1 F_{2d-2} \geq 1.$$

By property (F2), there are no integer points $\mathbf{y}$ between $\mathcal{C}$ and $\boldsymbol{l}$. The other two edges of R_1 come from J. See Figure 2.2.

(F5) The part of $J \backslash \mathcal{F}$ lying below $\mathcal{C}$ is exactly $R_2 \cap \mathbb{Z}^2$. This can be seen as follows. The line connecting ϕ_i and ϕ_{i+1} is defined by

$$y_2 F_{2i} - y_1 F_{2i-1} = -1.$$

So all integer points below that line satisfies:

$$y_2 F_{2i} - y_1 F_{2i-1} \leq -2.$$

This gives $d-1$ faces for R_2, one for each $1 \leq i \leq d-1$. The other two faces of R_2 come from J. See Figure 2.2.

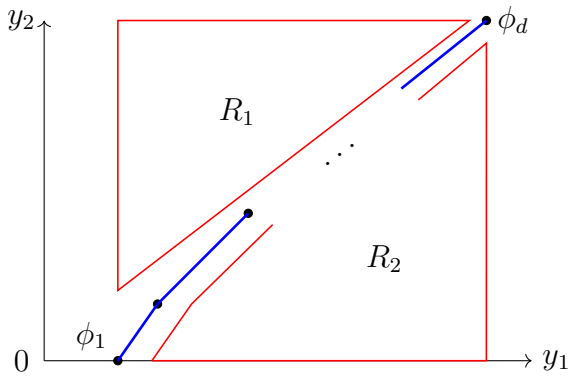


Figure 2.2: The points $\phi_1, \ldots, \phi_d \in \mathcal{F}$ form a convex curve $\mathcal{C}$ (blue).

2.2.B. The polytopes. Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and $\varepsilon \in (0, \frac{1}{2}) \cap \mathbb{Q}$, for each $1 \leq i \leq d$, we define a polygon:

$$P_i = \big\{(x, w) \in \mathbb{R}^2 \ : \ 1 \leq x \leq N, \ \alpha_i x - \varepsilon \leq w \leq \alpha_i x + \varepsilon\big\}. \tag{2.8}$$

Next, for each $1 \le i \le d$, we define a new polygon

$$P_i' = \big\{(x, \phi_i, w) \ : \ (x, w) \in P_i\big\} \subset \mathbb{R}^4. \tag{2.9}$$

Finally, we define the convex hull:

$$P = \text{conv}(P_1', \ldots, P_d') \subset \mathbb{R}^4. \tag{2.10}$$

The following properties are straightforward from the above definitions:

(P1) Each P_i is a parallelogram with vertices $\big\{(1, \alpha_i \pm \varepsilon),\ (N, \alpha_i N \pm \varepsilon)\big\}$.

(P2) Each P_i' is a *parallelogram* in $\mathbb{R}^4$ (i.e., a Minkowski sum of two intervals), with vertices $\big\{(1, \phi_i, \alpha_i \pm \varepsilon),\ (N, \phi_i, \alpha_i N \pm \varepsilon)\big\}$.

(P3) The set of all vertices from $P_1', \ldots, P_d'$ are in convex position. Each P_i' forms a 2-dimensional face of P. This follows from (2.9) and (F1).

(P4) The polytope P has $4d$ vertices, which are all the vertices of $P_1', \ldots, P_d'$.

(P5) For every vertex $(x, \mathbf{y}, w)$ of P, we have $\mathbf{y} = \phi_i \in \mathcal{F}$ for some $1 \le i \le d$. Conversely, for every $\phi_i \in \mathcal{F}$, we have:

$$\big\{(x, w) \in \mathbb{R}^2 : (x, \phi_i, w) \in P\big\} = P_i.$$

We will be using these properties in the latter sections.

2.3. Proof of Theorem 2.2

2.3.A. For convenience, will refer to the variables in (2.2) as $(x, \mathbf{y}, \mathbf{z})$ instead of $(x_1, \mathbf{x}_2, \mathbf{x}_3)$. By a *box* in $\mathbb{Z}^n$, we mean a set of integer points in $[\alpha_1, \beta_1] \times \cdots \times [\alpha_n, \beta_n]$ for some $\alpha_i, \beta_i \in \mathbb{Z}$. Theorem 2.2 can be restated as: Given a polyhedron $U \subset \mathbb{R}^6$ and two finite boxes $I \subset \mathbb{Z}$, $J \subset \mathbb{Z}^2$, deciding the sentence

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in \mathbb{Z}^3 \quad : \quad (x, \mathbf{y}, \mathbf{z}) \in U \tag{2.11}$$

is an NP-complete problem. In fact, we will prove this for a polytope U, i.e., a bounded polyhedron.

For a vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and an integer $x \in \mathbb{Z}$, we define

$$\{\{x\boldsymbol{\alpha}\}\} = \max_{1 \le i \le d} \{\{q\alpha_i\}\}, \tag{2.12}$$

where for each rational $\beta \in \mathbb{Q}$, the quantity $\{\{\beta\}\}$ is defined as:

$$\{\{\beta\}\} := \min_{n \in \mathbb{Z}} |\beta - n| = \min\bigl\{\beta - \lfloor\beta\rfloor, \lceil\beta\rceil - \beta\bigr\}.$$

Consider the following problem in Computational Number Theory:

Good Simultaneous Approximation (GSA)

Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\varepsilon \in \mathbb{Q}$.

Decide: Is an integer $x \in [1, N]$ such that $\{\{x\boldsymbol{\alpha}\}\} \le \varepsilon$?

Here we measure the input by the total binary lengths of the numerators and denominators in the α_i's. Note that GSA is only non-trivial for $\varepsilon < 1/2$. We need the following result by Lagarias:

Theorem 2.8 ([Lag85])**.** GSA *is* NP*-complete.*

Let us emphasize that in GSA, the number d is part of the input. If d is fixed instead, then the problem can be decided in polynomial time (see [Lag85] and [GLS89, Ch. 5]). What follows is a reduction of GSA to a sentence of the form (2.11). First, GSA can be expressed as an Integer Programming problem:

$$\exists\, x, w_1, \ldots, w_d \in \mathbb{Z} \quad : \quad 1 \le x \le N, \quad -\varepsilon \le \alpha_i x - w_i \le \varepsilon. \tag{2.13}$$

The inequalities on w_i can be expressed as $(x, w_i) \in P_i$, where P_i was defined in (2.8). Letting $I = [1, N] \cap \mathbb{Z}$, we see that GSA is equivalent to deciding:

$$\exists x \in I \quad : \quad \bigwedge_{i=1}^{d} \Bigl(\exists w \in \mathbb{Z} \ : \ (x, w) \in P_i\Bigr). \tag{2.14}$$

Lemma 2.9. *Let $\mathcal{F} = \{\phi_1, \ldots, \phi_d\}$ be as in (2.5) and P be as in (2.10). We have:*

$$\{\{x\boldsymbol{\alpha}\}\} \leq \varepsilon \quad \Longleftrightarrow \quad \forall \mathbf{y} \in \mathcal{F} \quad \exists w \in \mathbb{Z} \ : \ (x, \mathbf{y}, w) \in P. \tag{2.15}$$

Proof. Indeed, assume $\{\{x\boldsymbol{\alpha}\}\} \leq \varepsilon$, i.e., x satisfies GSA. By (2.14), for every $i = 1, \ldots, d$, there exists $w_i \in \mathbb{Z}$ with $(x, w_i) \in P_i$. Now (P5) implies that $(x, \phi_i, w_i) \in P$. Since this holds for every $\phi_i \in \mathcal{F}$, the RHS in (2.15) is satisfied. For the other direction, assume the RHS in (2.15) holds. Then for every $\phi_i \in \mathcal{F}$, there exists $w_i \in \mathbb{Z}$ with $(x, \phi_i, w_i) \in P$. By (P5), we have $(x, w_i) \in P_i$. By (2.14), x satisfies GSA, i.e., $\{\{x\boldsymbol{\alpha}\}\} \leq \varepsilon$. □

By the above lemma, GSA is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in \mathcal{F} \quad \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P. \tag{2.16}$$

Consider J from (2.5), which contains $\mathcal{F}$. We can rewrite the above sentence as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \big[(\mathbf{y} \in J \backslash \mathcal{F}) \ \vee \ \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P\big]. \tag{2.17}$$

Recall the polygons R_1 and R_2 defined in (2.6) and (2.7). By properties (F3), (F4) and (F5), we can rewrite $\mathbf{y} \in J \backslash \mathcal{F}$ as $(\mathbf{y} \in R_1) \vee (\mathbf{y} \in R_2)$. Now, we can rewrite (2.17) as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \big[\, (\mathbf{y} \in R_1) \ \vee \ (\mathbf{y} \in R_2) \ \vee \ \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P \,\big]. \tag{2.18}$$

Next, define two polytopes R_1' and R_2' as follows:

$$R_i' := \big\{(x, \mathbf{y}, 0) \in \mathbb{R}^4 : 0 \leq x \leq N, \ \mathbf{y} \in R_i\big\} \subset \mathbb{R}^4 \quad \text{for} \quad i = 1, 2. \tag{2.19}$$

Polytopes R_1' and R_2' are defined in such a way so that for every $x \in I$ and $\mathbf{y} \in J$, we have $\mathbf{y} \in R_i$ if and only if there exists $w \in \mathbb{Z}$ such that $(x, \mathbf{y}, w) \in R_i'$.[1] Now, it is clear that (2.18) is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \left[\left(\bigvee_{i=1}^{2} \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in R_i'\right) \ \vee \ \Big(\exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P\Big)\right].$$

which is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists w \in \mathbb{Z} \quad : \quad (x, \mathbf{y}, w) \in R_1' \cup R_2' \cup P. \tag{2.20}$$

The difference between (2.20) and (2.11) is that we have three polytopes instead of just one.

[1] Such a w must automatically be 0 by the definition of R_i'.

2.3.B. The final step is two compress three polytopes R_1', R_2' and P into one polytope. Recall from (P4) that P has $4d$ vertices, which correspond to the vertices of all P_i for $1 \le i \le d$. The vertices of R_1 and R_2 can be computed in polynomial time from systems (2.6) and (2.7). From there we easily get the vertices of R_1' and R_2'. Since P, R_1' and R_2' are in the fixed dimension 4, we can write down all their facets in polynomial time using their vertices. So we can represent:

$$\begin{aligned} P &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_1(x, \mathbf{y}, w) \le \overline{b}_1\right\}, \\ R_1' &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_2(x, \mathbf{y}, w) \le \overline{b}_2\right\}, \\ R_2' &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_3(x, \mathbf{y}, w) \le \overline{b}_3\right\}. \end{aligned} \tag{2.21}$$

Here each A_i is a matrix of four columns, and $A_i(x, \mathbf{y}, w)$ denotes matrix–vector multiplication. The above three systems all have lengths polynomial in the input $\boldsymbol{\alpha}, N$ and ε. Next, we need the following lemma:

Lemma 2.10. *Fix n and r. Given r polytopes $R_1, \ldots, R_r \subset \mathbb{R}^n$ described by r systems*

$$R_i = \{\mathbf{x} \in \mathbb{R}^n : A_i \mathbf{x} \le \overline{b}_i\},$$

there is a polytope $U \in \mathbb{R}^{n+\ell}$, where $\ell = \lceil \log_2 r \rceil$, such that

$$\mathbf{x} \in \bigcup_{i=1}^{r} R_i \cap \mathbb{Z}^n \quad \Longleftrightarrow \quad \exists \mathbf{t} \in \mathbb{Z}^\ell : (\mathbf{x}, \mathbf{t}) \in U \cap \mathbb{Z}^{n+\ell}. \tag{2.22}$$

Furthermore, the system $A(\mathbf{x}, \mathbf{t}) \le \overline{b}$ that describes U can be found in polynomial time, given A_i's and $\overline{b}_i$'s as input.

Proof. Let $\ell = \lceil \log_2 r \rceil$, we have $2^\ell \ge r$. Pick $\overline{t}_1, \ldots, \overline{t}_r \in \{0,1\}^\ell$ as r different vertices of the ℓ-dimensional unit cube. Define

$$U_j = \{(\mathbf{x}, \overline{t}_j) \in \mathbb{R}^{n+\ell} : \mathbf{x} \in R_j\} \quad \text{for} \quad j = 1, \ldots, r,$$

and

$$U = \operatorname{conv}(U_1, \ldots, U_r).$$

In other words, we form U_j by augmenting each R_j with ℓ coordinates of $\overline{t}_j$. Since $\overline{t}_1, \ldots, \overline{t}_r$ are in convex position, so are the new polytopes $U_1, \ldots, U_j$. So the vertices of U are all the

vertices of all U_j. Note that for every $\mathbf{t} \in \text{conv}(\overline{t}_1, \ldots, \overline{t}_r)$, we have $\mathbf{t} \in \mathbb{Z}^\ell$ if and only if $\mathbf{t} = \overline{t}_j$ for some j. This implies that the only integer points in U are those in U_j's. In other words:

$$(\mathbf{x}, \mathbf{t}) \in U \cap \mathbb{Z}^{n+\ell} \quad \iff \quad \mathbf{x} \in R_j \cap \mathbb{Z}^n \ \text{ and } \ \mathbf{t} = \overline{t}_j \ \text{ for some } \ j = 1, \ldots, r.$$

So we have (2.22).

For each R_j, its vertices can be computed in polynomial time from the system $A_i\mathbf{x} \leq \overline{b}_i$. From these, we easily get the vertices for each U_j. Thus, we can find all vertices of U in polynomial time. Note that U is in a fixed dimension $n+\ell$, since n and r are fixed. Therefore, we can find in polynomial time all the facets of U using those vertices. This gives us a system $A(\mathbf{x}, \mathbf{t}) \leq \overline{b}$ of polynomial length that describes U. □

Applying the above lemma for three polytopes R'_1, R'_2 and P with $n = 4$ and $r = 3$, we find a polytope $U \subset \mathbb{R}^{4+\ell}$ such that:

$$(x, \mathbf{y}, w) \in (R'_1 \cup R'_2 \cup P) \cap \mathbb{Z}^4 \quad \iff \quad \exists \mathbf{t} \in \mathbb{Z}^\ell : (x, \mathbf{y}, w, \mathbf{t}) \in U \cap \mathbb{Z}^{4+\ell}. \tag{2.23}$$

Here we have $\ell = \lceil \log_2 3 \rceil = 2$, which means $\mathbf{t} \in \mathbb{Z}^2$ and $U \subset \mathbb{R}^6$. The lemma also allows us to find a system $A(x, \mathbf{y}, w, \mathbf{t}) \leq \overline{b}$ that describes U, which has size polynomial in the systems in (2.21). Now, we can rewrite (2.20) as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists w \in \mathbb{Z} \quad : \quad \exists \mathbf{t} \in \mathbb{Z}^2 \quad (x, \mathbf{y}, w, \mathbf{t}) \in U,$$

which is equivalent to

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in \mathbb{Z}^3 \quad : \quad A(x, \mathbf{y}, \mathbf{z}) \leq \overline{b}.$$

Here $\mathbf{z} = (w, \mathbf{t}) \in \mathbb{Z}^3$. The final system $A(x, \mathbf{y}, \mathbf{z}) \leq \overline{b}$ still has size polynomial in the original input $\boldsymbol{\alpha}, N$ and ε. Therefore, the original GSA problem is equivalent to (2.11). This implies that (2.11) is NP-hard.

It remains to show that (2.11) is in NP. We argue that more general sentence (2.2) is also in NP. From the results in [Grä87, Grä88], if (2.2) is true, there must be an x satisfying it with $\log x$ at most polynomial in the input lengths of P, A and $\overline{b}$. For such an x, we can apply Theorem 2.1 to check the rest of the sentence, which has the form $\forall \mathbf{y} \exists \mathbf{z}$, in polynomial time. This shows that deciding (2.2) is in NP, and thus NP-complete. □

2.4. Proof of Theorem 2.3

Recall the definition of boxes from Section 2.3. In this section, we prove:

Theorem 2.11. *Fix $k \geq 1$. Given a polytope $U \subset \mathbb{R}^{k+7}$ and finite boxes $I_1, \ldots, I_k \subset \mathbb{Z}$, $J \subset \mathbb{Z}^2$, $K \subset \mathbb{Z}^5$, then the problem of deciding:*

$$Q_1 x_1 \in I_1 \quad \ldots \quad Q_k x_k \in I_k \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in K \quad : \quad (\mathbf{x}, \mathbf{y}, \mathbf{z}) \in U \tag{2.24}$$

is $\boldsymbol{\Sigma}_k^{\mathsf{P}}$ complete if k is odd, and $\boldsymbol{\Pi}_k^{\mathsf{P}}$ complete if k is even. Here $Q_1, \ldots, Q_k \in \{\exists, \forall\}$ are k alternating quantifiers with $Q_k = \exists$.

For the proof, we work with the canonical problem Q3SAT. Let Ψ a Boolean expression of the form:

$$\Psi(\mathbf{u}_1, \ldots, \mathbf{u}_k) = \bigwedge_{i=1}^{n} (a_i \vee b_i \vee c_i). \tag{2.25}$$

Here each $\mathbf{u}_j = (u_{j1}, \ldots, u_{j\ell}) \in \{\text{true, false}\}^\ell$ is a tuple of ℓ Boolean variables, and each a_i, b_i, c_i is a literal in the set $\{u_{js},\ \neg u_{js} \ : \ 1 \leq j \leq k,\ 1 \leq s \leq \ell\}$. From Ψ, we construct a sentence:

$$Q_1 \mathbf{u}_1 \in \{\text{true, false}\}^\ell \ \ldots \ Q_k \mathbf{u}_k \in \{\text{true, false}\}^\ell \quad : \quad \Psi(\mathbf{u}_1, \ldots, \mathbf{u}_k). \tag{2.26}$$

Here $Q_1, Q_2, \ldots, Q_k \in \{\forall, \exists\}$ are k alternating quantifiers with $Q_k = \exists$. The numbers ℓ and n are part of the input.

Quantified 3-Satisfiability (Q3SAT)

Input: A Boolean expression Ψ of the form (2.25).

Decide: The truth of the sentence (2.26).

For clarity, we use the notation Q3SAT_k to emphasize problem (2.26) for a fixed k. It is well-known that Q3SAT_k is $\boldsymbol{\Sigma}_k^{\mathsf{P}}$-complete k is odd and $\boldsymbol{\Pi}_k^{\mathsf{P}}$-complete if k is even. We proceed to reduce (2.26) to (2.24). In fact, by representing each Boolean string $\mathbf{u}_j \in \{\text{true, false}\}^\ell$ as an integer $x_j \in [0, 2^\ell)$, we will only need to use $I_1 = I_2 = \cdots = I_k = [0, 2^\ell) \cap \mathbb{Z}$.

For every string $\mathbf{u}_j = (u_{j1}, \ldots, u_{j\ell}) \in \{\text{true, false}\}^\ell$, let $x_j \in [0, 2^\ell)$ be the corresponding integer in binary. In other words, u_{js} is true or false respectively when the s-th binary digit of x_j is 1 or 0, or equivalently, when $\lfloor x_j/2^{s-1} \rfloor$ is odd or even. Observe that $t = \lfloor x_j/2^{s-1} \rfloor$ is the only integer that satisfies $x_j/2^{s-1} - 1 < t \leq x_j/2^{s-1}$. Now, each term u_{js} or $\neg u_{js}$ can be expressed in x_j as follows:

$$\begin{aligned} u_{js} &\iff \exists w \in \mathbb{Z} \ : \ \begin{Bmatrix} 2w+1 & > & x_j/2^{s-1} - 1 \\ 2w+1 & \leq & x_j/2^{s-1} \end{Bmatrix}, \\ \neg u_{js} &\iff \exists w \in \mathbb{Z} \ : \ \begin{Bmatrix} 2w & > & x_j/2^{s-1} - 1 \\ 2w & \leq & x_j/2^{s-1} \end{Bmatrix}. \end{aligned} \tag{2.27}$$

Let $\mathbf{x} = (x_1, \ldots, x_k) \in [0, 2^\ell)^k$. Recall that each term a_i, b_i, c_i in (2.25) is u_{js} or $\neg u_{js}$ for some j and s. So each clause $a_i \vee b_i \vee c_i$ can be expressed in $\mathbf{x}$ as:

$$a_i \vee b_i \vee c_i \iff \exists w \in \mathbb{Z} \ : \ \big(D_i(\mathbf{x}, w) \leq \overline{d}_i\big) \ \vee \ \big(E_i(\mathbf{x}, w) \leq \overline{e}_i\big) \ \vee \ \big(F_i(\mathbf{x}, w) \leq \overline{f}_i\big). \tag{2.28}$$

Here the three systems $D_i(\mathbf{x}, w) \leq \overline{d}_i$, $E_i(\mathbf{x}, w) \leq \overline{e}_i$, $F_i(\mathbf{x}, w) \leq \overline{f}_i$ are of the form (2.27). Note that the strict inequalities in (2.27) can be sharpened without losing any integer solutions (see Remark 2.14). We define the polytopes:

$$\begin{aligned} K_i &= \big\{(\mathbf{x}, w) \in \mathbb{R}^{k+1} \ : \ x_1, \ldots, x_k, w \in [0, 2^\ell), \ D_i(\mathbf{x}, w) \leq \overline{d}_i\big\}, \\ L_i &= \big\{(\mathbf{x}, w) \in \mathbb{R}^{k+1} \ : \ x_1, \ldots, x_k, w \in [0, 2^\ell), \ E_i(\mathbf{x}, w) \leq \overline{e}_i\big\}, \\ M_i &= \big\{(\mathbf{x}, w) \in \mathbb{R}^{k+1} \ : \ x_1, \ldots, x_k, w \in [0, 2^\ell), \ F_i(\mathbf{x}, w) \leq \overline{f}_i\big\}. \end{aligned}$$

So the RHS in (2.28) can be rewritten as:

$$\exists w \in \mathbb{Z} \ : \ (\mathbf{x}, w) \in K_i \cup L_i \cup M_i.$$

Let $I_1 = I_2 = \cdots = I_k = [0, 2^\ell) \cap \mathbb{Z}$, we see that (2.26) is equivalent to:

$$Q_1 x_1 \in I_1 \quad \ldots \quad Q_k x_k \in I_k \quad : \quad \bigwedge_{i=1}^{n} \Big(\exists w \in \mathbb{Z} \ : \ (\mathbf{x}, w) \in K_i \cup L_i \cup M_i\Big). \tag{2.29}$$

For each i, we apply Lemma 2.10 (with $n = k+1$, $r = 3$) to the polytopes $K_i, L_i, M_i \subset \mathbb{R}^{k+1}$. This gives us another polytope $G_i \subset \mathbb{R}^{k+3}$ that satisfies:

$$(\mathbf{x}, w) \in K_i \cup L_i \cup M_i \quad \iff \quad \exists \mathbf{v} \in \mathbb{Z}^2 \ : \ (\mathbf{x}, w, \mathbf{v}) \in G_i.$$

Substituting this into (2.29), we have an equivalent sentence:

$$Q_1 x_1 \in I_1 \quad \dots \quad Q_k x_k \in I_k \quad : \quad \bigwedge_{i=1}^{n} \Big(\exists \mathbf{w} \in \mathbb{Z}^3 \ : \ (\mathbf{x}, \mathbf{w}) \in G_i \Big), \tag{2.30}$$

where $\mathbf{w} = (w, \mathbf{v}) \in \mathbb{Z}^3$, and each $G_i \subset \mathbb{R}^{k+3}$.

Notice that apart from the quantifiers $Q_1, \dots, Q_k$, (2.30) is a direct analogue of (2.14), with G_i playing the role of P_i and $(\mathbf{x}, \mathbf{w})$ in place of (x, w). The proof now proceeds similarly to the rest of Section 2.3 after (2.14). Along the proof, we need to define G_i' and G in similar manners to (2.9) and (2.10). The variable $\mathbf{y} \in \mathbb{Z}^2$ is again needed to define G_i'. $\mathcal{F}$ and J from (2.5) are reused without change. This gives us $G_i', G \subset \mathbb{R}^{k+5}$. At the end of the proof, we also need to apply Lemma 2.10 one more time to produce a single polytope U, just like in (2.23). The dimension 4 in (2.23) is now $k+5$. As a result, the final polytope U has dimension $k+7$. In the final form (2.24), we will have $\mathbf{x} \in \mathbb{Z}^k, \mathbf{y} \in \mathbb{Z}^2$ and $\mathbf{z} = (\mathbf{w}, \mathbf{t}) \in \mathbb{Z}^5$.

We have converted (2.26) to an equivalent sentence (2.24) with polynomial size. This shows that (2.24) is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-hard. For each tuple $\mathbf{x} = (x_1, \dots, x_k)$, we can check in polynomial time whether $\forall \mathbf{y} \in J \ \ \exists \mathbf{z} \in K : A(\mathbf{x}, \mathbf{y}, \mathbf{z}) \le \overline{b}$ by applying Theorem 2.1. This shows the membership of (2.24) in $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$. We conclude that (2.24) is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete, depending on the parity of k.

2.5. Proof of Theorem 2.6

2.5.A. Now we prove Theorem 2.6. We use the same construction as in the proof of Theorem 2.2. Recall the definition of $\{\{x\boldsymbol{\alpha}\}\}$ from Section 2.3. We reduce the following counting problem to a problem of the form (2.3):

#Good Simultaneous Approximations (#GSA)

Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\varepsilon \in \mathbb{Q}$.

Output: The number of integers $x \in [1, N]$ that satisfy $\{\{x\boldsymbol{\alpha}\}\} \le \varepsilon$.

The argument in [Lag85] is based on a parsimonious reduction. Namely, it gives a bijection between solutions for #GSA and the following problem:

#Weak Partitions

Input: An integer vector $\overline{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$.

Output: The number of $\mathbf{y} \in \{-1, 0, 1\}^d$ for which $\overline{a} \cdot \mathbf{y} = 0$.

It is well known and easy to see that #Weak Partitions is #P-complete. The decision version Weak Partition was earlier shown by [vEB81] to be NP-complete with a parsimonious reduction from Knapsack. Together with Lagarias's reduction, we conclude:

Theorem 2.12. #GSA *is* #P*-complete.*

2.5.B. Now we proceed with the reduction of #GSA to (2.3).

Just like the decision version, #GSA is only non-trivial for $\varepsilon < 1/2$. Define:

$$Q_i = \big\{(x, w) \in \mathbb{R}^2 \quad : \quad 1 \le x \le N, \quad \alpha_i x + \varepsilon < w < \alpha_i x - \varepsilon + 1\big\}. \tag{2.31}$$

Let $I = [1, N] \cap \mathbb{Z}$. We have:

Observation 2.13. An $x \in I$ satisfies $\{\{x\boldsymbol{\alpha}\}\} \le \varepsilon$ if and only if for every $1 \le i \le d$, there is no $w \in \mathbb{Z}$ such that $(x, w) \in Q_i$.

Indeed, consider $x \in I$. By (2.13), we have $\{\{x\boldsymbol{\alpha}\}\} \le \varepsilon$ if and only if for each i, there exists $w_i \in \mathbb{Z}$ with $w_i \in [\alpha_i x - \varepsilon, \alpha_i x + \varepsilon]$. This interval of length 2ε is contained in $[\alpha_i x - \varepsilon, \alpha_i x - \varepsilon + 1)$. The latter is a half-open unit interval, which always contains a unique integer w_i. So $w_i \in [\alpha_i x - \varepsilon, \alpha_i x + \varepsilon]$ if and only if $w_i \notin (\alpha_i x + \varepsilon, \alpha_i x - \varepsilon + 1)$. In other words, for each $1 \le i \le d$, there should be no $w \in \mathbb{Z}$ with $(x, w) \in Q_i$. The converse is also straightforward.

Remark 2.14. Note that each Q_i has two open edges. They can actually sharpened without affecting the integer points in Q_i. Indeed, we can multiply each inequality with the denominators in α_i and ε, which have polynomial length. Each resulting inequality is of the form $a < b$, with a and b having integer values. This is equivalent to $a \le b - 1$. Therefore, we can replace Q_i with a (smaller) closed parallelogram containing the same integer points.

By the above observation, #GSA asks for:

$$N \;-\; \#\Big\{x \in I \;:\; \exists 1 \le i \le d \quad \exists w \in \mathbb{Z} \quad (x,w) \in Q_i\Big\}. \tag{2.32}$$

We convert the union of Q_i into a complement $V \backslash U$ of two polytopes $U, V \subset \mathbb{R}^3$.

2.5.C. Let $T = 1 + N \max_i \alpha_i$. Pick d integers $0 < m_1 < m_2 < \cdots < m_d$ so that

$$\frac{m_{i-1} + m_{i+1}}{2} + 2T < m_i \quad \text{for} \quad 2 \le i \le d-1. \tag{2.33}$$

We embed each parallelogram Q_i into $\mathbb{R}^3$ as

$$R_i = \big\{(x,y,w) \in \mathbb{R}^3 \;:\; (x, w - m_i) \in Q_i,\; y = i\big\}. \tag{2.34}$$

In other words, we translate Q_i by m_i in the direction w, and embed it into the plane $y = i$ inside $\mathbb{R}^3$ (see Figure 2.3). The following is obvious:

Observation 2.15. For each $x \in I$ and $1 \le i \le d$, there exists $w \in \mathbb{Z}$ with $(x,w) \in Q_i$ if and only if there exists $(y,w) \in \mathbb{Z}^2$ with $(x,y,w) \in R_i$.

Denote by A_i, B_i, C_i and D_i the vertices of R_i. Let $K_i = (N, i, 0)$ and $L_i = (1, i, 0)$ for each $1 \le i \le d$. Define:

$$\begin{aligned} U &= \operatorname{conv}\big\{A_i,\, B_i,\, K_i,\, L_i \;:\; 1 \le i \le d\big\} \subset \mathbb{R}^3, \\ V &= \operatorname{conv}\big\{C_i,\, D_i,\, K_i,\, L_i \;:\; 1 \le i \le d\big\} \subset \mathbb{R}^3. \end{aligned} \tag{2.35}$$

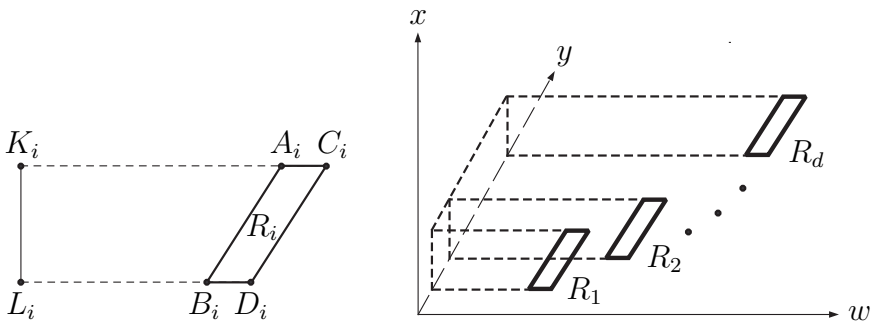


Figure 2.3: The parallelograms R_i.

Since $\text{conv}(A_i, B_i, K_i, L_i) \subset \text{conv}(C_i, D_i, K_i, L_i)$ for each $1 \le i \le d$, we have $U \subset V$. It is also clear that:

$$R_i = \text{conv}(C_i, D_i, K_i, L_i) \backslash \text{conv}(A_i, B_i, K_i, L_i). \tag{2.36}$$

Denote by $\{y = i\}$ the plane $y = i$.

Observation 2.16. We have $\big(U \cap \{y = i\}\big) = \text{conv}(A_i, B_i, K_i, L_i)$. Similarly, we have $\big(V \cap \{y = i\}\big) = \text{conv}(C_i, D_i, K_i, L_i)$.

Indeed, from (2.35), it is clear that $\text{conv}(A_i, B_i, K_i, L_i)$ lies in both U and the plane $y = i$. On the other hand, if $(x, i, w) \in U$, it must be a convex combination of A_j, B_j, K_j, L_j for $1 \le j \le d$. First, assume that

$$(x, i, w) \in \text{conv}\big\{A_j, B_j, K_j, L_j : j \ne i\big\}. \tag{2.37}$$

From (2.31) and (2.34), the w-coordinates of A_j, B_j, C_j, D_j are within the range $[m_j, m_j + T]$. For K_j and L_j, their w-coordinates are 0. Therefore, by the convexity condition (2.33), any point (x, y, w) as in (2.37) must have $w < m_i - T < m_i$. This implies that $(x, i, w) \in \text{conv}\big\{A_i, B_i, K_i, L_i\big\}$, because the w-coordinates of A_i and B_j are at least m_i. So we have

$$\text{conv}\big\{A_j, B_j, K_j, L_j : j \ne i\big\} \cap \{y = i\} \subset \text{conv}\big\{A_i, B_i, K_i, L_i\big\}.$$

Adding A_i, B_i, C_i and D_i to the LHS, we have

$$\text{conv}\big\{A_j, B_j, K_j, L_j : 1 \le j \le d\big\} \cap \{y = i\} = \text{conv}\big\{A_i, B_i, K_i, L_i\big\}.$$

This proves the observation for U. The same argument works for V.

By Observation 2.16, for $(x, y, w) \in \mathbb{Z}^3$, we have $(x, y, z) \in V \backslash U$ if and only if

$$(x, y, w) \in \text{conv}(C_i, D_i, K_i, L_i) \backslash \text{conv}(A_i, B_i, K_i, L_i)$$

for some $1 \le i \le d$. Combined with (2.36) and Observation 2.15, for every $x \in I$, we have:

$$\exists (y, w) \in \mathbb{Z}^2 \quad (x, y, w) \in V \backslash Q \quad \iff \quad \exists 1 \le i \le d \quad \exists w \in \mathbb{Z} \quad (x, w) \in Q_i.$$

From (2.32), we conclude that #GSA is exactly:

$$N \; - \; \#\Big\{x \in I \; : \; \exists (y, z) \in \mathbb{Z}^2 \quad (x, y, w) \in V \backslash U\Big\} = N - |\text{E}_1(V \backslash U)|.$$

Let $P = U, Q = V$ we have Theorem 2.6.

2.6. Another hard decision problem

Our construction with Fibonacci points also yields the following completeness result with only two quantifiers:

Theorem 2.17. *Given three polytopes $U_1, U_2, U_3 \subset \mathbb{R}^4$ and two boxes $I \subset \mathbb{Z}, K \subset \mathbb{Z}^3$, deciding the sentence:*

$$\exists x \in I \quad \forall \mathbf{z} \in K \quad : \quad (x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3 \tag{2.38}$$

is NP*-complete.*

In Theorem 1.5-ii), we needed many conjunctions and disjunctions in the expression Ψ for NP-completeness. Here, the condition $(x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3$ is a disjunction of only three linear systems in four variables x, z_1, z_2, z_3. So in this perspective, Theorem 2.17 can be viewed as an intermediate result between theorems 1.5-ii) and 2.1.

Proof of Theorem 2.17. We again find a reduction of GSA. Let $T = 1 + N \max_i \alpha_i$. Recall P_i from (2.8). For every $1 \le i \le d$, define two new polygons:

$$L_i = \{(x, w) \in \mathbb{R}^2 \ : \ 1 \le x \le N, \ -1 \le w \le \alpha_i x + \varepsilon - 1\},$$
$$M_i = \{(x, w) \in \mathbb{R}^2 \ : \ 1 \le x \le N, \ \alpha_i x - \varepsilon \le w \le T\}.$$

Observation 2.18. For every $x \in [1, N]$ and $1 \le i \le d$, we have:

$$\exists w \in \mathbb{Z} \ : \ (x, w) \in P_i \quad \iff \quad \forall w \in [-1, T] \cap \mathbb{Z} \ : \ (x, w) \in L_i \cup M_i. \tag{2.39}$$

Indeed, by (2.8), we have $\exists w \in \mathbb{Z} : (x, w) \in P_i$ if and only if $[\alpha_i x - \varepsilon, \alpha_i x + \varepsilon]$ contains an integer point w. Also notice that $[\alpha_i x - \varepsilon, \alpha_i x + \varepsilon] \subset (\alpha_i x + \varepsilon - 1, \alpha_i x + \varepsilon]$ and

$$[-1, T] \ = \ [-1, \alpha_i x + \varepsilon - 1] \ \sqcup \ (\alpha_i x + \varepsilon - 1, \alpha_i x + \varepsilon] \ \sqcup \ (\alpha_i x + \varepsilon, T].$$

Since $(\alpha_i x + \varepsilon - 1, \alpha_i x + \varepsilon]$ is a half-open unit interval, it contains a unique integer point w. So w lies in $[\alpha_i x - \varepsilon, \alpha_i x + \varepsilon]$ if and only if

$$\begin{aligned} [-1, T] \cap \mathbb{Z} \ &= \ \big([-1, \alpha_i x + \varepsilon - 1] \ \sqcup \ [\alpha_i x - \varepsilon, \alpha_i x + \varepsilon] \ \sqcup \ (\alpha_i x + \varepsilon, T]\big) \cap \mathbb{Z} \\ &= \ \big([-1, \alpha_i x + \varepsilon - 1] \ \sqcup \ [\alpha_i x - \varepsilon, T]\big) \cap \mathbb{Z}. \end{aligned}$$

This last condition is exactly the RHS in (2.39).

Recall the Fibonacci points $\mathcal{F} = \{\phi_1, \ldots, \phi_d\}$. We construct L_i', M_i' similarly to (2.9) and L, M similarly to (2.10) using the same Fibonacci points. As a direct analogy to (2.16), GSA is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in \mathcal{F} \quad \forall w \in [-1, T] \cap \mathbb{Z} \quad : \quad (x, \mathbf{y}, w) \in L \cup M. \tag{2.40}$$

Recall J from (2.5). Let $K = J \times \big([-1, T] \cap \mathbb{Z}\big)$, which is a box in $\mathbb{Z}^3$. Let $\mathbf{z} = (\mathbf{y}, w) \in K$. Also recall R_1 and R_2 from (2.6) and (2.7). Define

$$U_1 = [1, N] \times R_1 \times [-1, T], \quad U_2 = \operatorname{conv}\big([1, N] \times R_2 \times [-1, T],\ L\big), \quad U_3 = M.$$

From properties (F3)–(F5), it is not hard to see that (2.40) is equivalent to:

$$\exists x \in I \quad \forall \mathbf{z} \in K \quad : \quad (x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3.$$

This completes the proof. □

2.7. Final remarks

2.7.A. It is in fact sufficient to prove Theorem 2.1 for the case when m, m' are also bounded. In the system $A\mathbf{x}_1 + B\mathbf{x}_2 \le \overline{v}$, we view $\mathbf{x}_1 \in \mathbb{Z}^{n_1}$ as the parameters and $\mathbf{x}_2 \in \mathbb{Z}^{n_2}$ as the variables to be solved for. For a fixed n_2 and $m \ge 2^{n_2}$, the *Doignon–Bell–Scarf theorem* [Sch86, §16.5] implies that the system $A\mathbf{x}_1 + B\mathbf{x}_2 \le \overline{v}$ is solvable in $\mathbf{x}_2 \in \mathbb{Z}^{n_2}$ if and only if *every* subsystem $A'\mathbf{x}_1 + B'\mathbf{x}_2 \le \overline{v}'$ is solvable in $\mathbf{x}_2 \in \mathbb{Z}^{n_2}$. Here (A', B', v') is a subsystem with 2^{n_2} rows taken from $(A, B, \overline{v})$. In other words, for each $\mathbf{x}_1 \in \mathbb{Z}^{n_1}$, we have:

$$\exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \quad A\mathbf{x}_1 + B\mathbf{x}_2 \ \le\ \overline{v} \quad \iff \quad \bigwedge_{(A', B', \overline{v}')} \Big(\exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \quad A'\mathbf{x}_1 + B'\mathbf{x}_2 \ \le\ \overline{v}'\Big).$$

The total number of subsystems $(A', B', \overline{v}')$ is $\binom{m}{2^{n_2}}$, which is clearly polynomial in m.

Note that the conjunction over all subsystems $(A', B', \overline{v}')$ commutes with the universal

quantifier $\forall \mathbf{x}_1$. Therefore:

$$\begin{aligned} &\forall \mathbf{x}_1 \in P \cap \mathbb{Z}^{n_1} \;\; \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \;\; A\mathbf{x}_1 + B\mathbf{x}_2 \;\leq\; \overline{v} \\ \iff \bigwedge_{(A',B',\overline{v}')} &\Big(\forall \mathbf{x}_1 \in P \cap \mathbb{Z}^{n_1} \;\; \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \;\; A'\mathbf{x}_1 + B'\mathbf{x}_2 \;\leq\; \overline{v}'\Big). \end{aligned}$$

Thus, it is equivalent to check each of the smaller subproblems, each of which has $m = 2^{n_2}$. Recall that the number of facets in P is m', which can still be large. However, given the system $W\mathbf{x}_1 \leq \overline{\gamma}$ describing P, we can triangulate P into to a union of simplices $P_1 \sqcup \cdots \sqcup P_k$. Since the dimension n_1 is bounded, such a triangulation can be found in polynomial time (see e.g. [DRS10]). Now for each subsystem $(A', B', \overline{v}')$, we have:

$$\begin{aligned} &\forall \mathbf{x}_1 \in P \cap \mathbb{Z}^{n_1} \;\; \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \;\; A'\mathbf{x}_1 + B'\mathbf{x}_2 \;\leq\; \overline{v}' \\ \iff \bigwedge_{i=1}^{k} &\Big(\forall \mathbf{x}_1 \in P_i \cap \mathbb{Z}^{n_1} \;\; \exists \mathbf{x}_2 \in \mathbb{Z}^{n_2} \;\; A'\mathbf{x}_1 + B'\mathbf{x}_2 \;\leq\; \overline{v}'\Big). \end{aligned}$$

Each simplex $P_i \subset \mathbb{R}^{n_1}$ has $n_1 + 1$ facets. Now each subsentence in the RHS has $m = 2^{n_2}$ and $m' = n_1 + 1$, both of which are fixed. Note that the total number of subsentences is still polynomial, so it suffices to check each of them individually.

For three quantifiers $\exists \mathbf{x}_1 \; \forall \mathbf{x}_2 \; \exists \mathbf{x}_3$, this argument breaks down because the existential quantifier $\exists \mathbf{x}_1$ no longer commutes with a long conjunction.

2.7.B. The GSA Problem plays an important role in both Number Theory and Integer Programming, especially in connection to lattice reduction algorithms (see e.g. [GLS89]). Let us mention that via a chain of parsimonious reductions one can show that #GSA is also hard to approximate (cf. [ER09]). Note also that GSA has been recently used in a somewhat related geometric context in [EH12].

2.7.C. By Lemma 2.10, we easily get the first part of the following result:

Proposition 2.19. *Every set $S = \{\overline{p}_1, \ldots, \overline{p}_r\} \subset \mathbb{Z}^2$ is a projection of integer points of some convex polytope $P \subset \mathbb{R}^{2+d}$, where $d \leq \lceil \log_2 r \rceil$. Moreover, the bound $d \leq \lceil \log_2 r \rceil$ is tight.*

Proof of tightness. Consider a set $S = \{\overline{p}_1, \ldots, \overline{p}_r\}$ of integer points in convex position and with even coordinates. Assume there is a polytope $P \subset \mathbb{R}^{2+\ell}$ with $\ell < \lceil \log_2 r \rceil$ so that S

is exactly the projection of $P \cap \mathbb{Z}^{2+\ell}$ on $\mathbb{Z}^2$. Then there are integer points $\overline{q}_1, \ldots, \overline{q}_r \in \mathbb{Z}^\ell$ so that $(\overline{p}_i, \overline{q}_i) \in P$. Since $r > 2^\ell$, by the pigeonhole principle, we have $\overline{q}_i - \overline{q}_j \in 2\mathbb{Z}^\ell$ for some $i \neq j$. Then the midpoint of $(\overline{p}_i, \overline{q}_i)$ and $(\overline{p}_j, \overline{q}_j)$ is an integer point in $\mathbb{Z}^{2+\ell}$, which also lies in P by convexity. The projection of this midpoint on $\mathbb{Z}^2$ is $(\overline{p}_i + \overline{p}_j)/2$, which must lie in S. However, the points in S are in convex positions and thus contain no midpoints, a contradiction. □

2.7.D. Let us give another motivation behind Theorem 2.6 and put it into context of our other works. In this chapter, we bypass the *short generating functions* (short GFs) technology developed by Barvinok and Woods to prove theorems 2.4 and 2.5 (see Chapter 6). Note, however, that for $X = Q \backslash P$ as in the theorem, the corresponding short GF $f_X(\mathbf{t})$ is simply the difference $f_Q(\mathbf{t}) - f_P(\mathbf{t})$, which can still be computed in polynomial time. Thus, if one could efficiently present the projection of $f_X(\mathbf{t})$ on $\mathbb{Z}$ as a short GF of polynomial size, then one would be able to compute $|\mathrm{E}_1(Q \backslash P)|$, a contradiction. In other words, Theorem 2.6 is an extension of a result of Woods, which shows that computing projecting short GFs is NP-hard (see Theorem 7.23). It is also an effective but weaker version of our main result in Chapter 7, which deals with the size of short GFs of the projections rather than complexity of their computation.

2.7.E. Dimension 3 in Theorem 2.6 is optimal. Indeed, assume $P, Q \subset \mathbb{R}^2$. Then one can decompose $Q \backslash P = R_1 \cup \cdots \cup R_r$, where each R_i is a polygon, so that the projection $\mathrm{E}_1(R_i)$ onto the x-axis of each R_i intersects at most one other $\mathrm{E}_1(R_j)$. This can easily be done by drawing vertical lines through vertices of P, which together with ∂P will divide $Q \backslash P$ into $R_1, \ldots, R_r$. By Theorem 2.5 (see also Theorem 6.14), we can find a generating function $g_i(t)$ for each $\mathrm{E}_1(R_i)$ in polynomial time. From Theorem 7.14, the union $g(t)$ of all $g_i(t)$ can also be found in polynomial time, because each of them intersects at most one another in support. Evaluating $g(1)$, we get the count for $|\mathrm{E}_1(Q \backslash P)|$.

CHAPTER 3

Complexity of short Presburger Arithmetic

In this chapter, we answer Conjecture 1.9 in the negative: Deciding short Presburger sentences with $k+2$ alternating quantifiers is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete. Counting versions and restricted system of inequalities are also analyzed. Applications are given for two natural problems in Integer Optimization. As a byproduct of our proof, we are also able to sharpen the dimensions in Theorem 1.5 by Schöning to best possible. We also discuss about the validity of Kannan's Partition Theorem at the end. This chapter is a version of the published paper [NP17b].

3.1. Introduction

3.1.A. Statements of results. To repeat the definition, for every fixed $m, k, n_1, \ldots, n_k$, we consider *short Presburger sentences*:

$$\exists \mathbf{x}_1 \in \mathbb{Z}^{n_1} \ \forall \mathbf{x}_2 \in \mathbb{Z}^{n_2} \ \ldots \ \forall/\exists \mathbf{x}_k \in \mathbb{Z}^{n_k} \ : \ \Phi\big(\mathbf{x}_1, \ldots, \mathbf{x}_k\big), \qquad \text{(Short-PA}_k\text{)}$$

where $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ is a Boolean combination of at most m linear inequalities in the form:

$$\sum_{i=1}^{k} \sum_{j=1}^{n_i} a_{ij}\, x_{ij} \ \leq \ b,$$

Here, the coefficients a_{ij} and constant term b are integers. In other words, everything is fixed in (Short-PA$_k$), except for the input a_{ij} and b in each inequality, encoded in binary. We also call the quantifier-free $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ a *short Presburger expression*. Hereafter, we will simply write $\exists \mathbf{x}_i$ instead of $\exists \mathbf{x}_i \in \mathbb{Z}^{n_i}$, and similarly for $\forall \mathbf{x}_i$.

Recall Theorem 1.8, which says that short PA sentences with $k \leq 2$ can be decided and

counted efficiently. For $k = 3$ alternating quantifiers, we have the first hard instance:

$$\exists \mathbf{x}_1 \ \forall \mathbf{x}_2 \ \exists \mathbf{x}_3 \ : \ \Phi(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3). \qquad \text{(Short-PA}_3\text{)}$$

The corresponding counting problem is:

$$\#\big\{ \mathbf{x}_1 \ : \ \forall \mathbf{x}_2 \ \exists \mathbf{x}_3 \ \ \Phi(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) \big\}. \qquad \text{(\#Short-PA}_3\text{)}$$

Theorem 3.1. *Deciding* (Short-PA$_3$) *is* NP*-complete, even for* Φ *with at most* 10 *inequalities in* 5 *variables* $x_1 \in \mathbb{Z}$, $\mathbf{x}_2 \in \mathbb{Z}^2$, $\mathbf{x}_3 \in \mathbb{Z}^2$. *Similarly, computing* (\#Short-PA$_3$) *is* \#P*-complete.*

For *restricted* systems of inequalities, we consider:

$$\exists \mathbf{x}_1 \in R \quad \forall \mathbf{x}_2 \in Q \quad \exists \mathbf{x}_3 \quad : \quad A\mathbf{x}_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \leq \overline{b}, \qquad \text{(GIP)}$$

where R and Q are two given polyhedra, described by facets. Here $\mathbf{x}_1$ and $\mathbf{x}_2$ are restricted to integer points in R and Q, respectively. The corresponding counting problem is:

$$\#\big\{ \mathbf{x}_1 \in R \quad : \quad \forall \mathbf{x}_2 \in Q \quad \exists \mathbf{x}_3 \quad A\mathbf{x}_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \leq \overline{b} \big\}. \qquad \text{(\#GIP)}$$

Theorem 3.2. i) *Deciding* (GIP) *is* NP*-complete, even when* $x_1 \in \mathbb{Z}$, $\mathbf{x}_2 \in \mathbb{Z}^2$, $\mathbf{x}_3 \in \mathbb{Z}^6$, *the system* $Ax_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \leq \overline{b}$ *has at most* 24 *inequalities,* R *is an interval and* Q *is a triangle. Similarly, computing* (\#GIP) *in this case is* \#P*-complete.*

ii) *The same conclusions hold when* $\mathbf{x}_3 \in \mathbb{Z}^3$, *but the system* $Ax_1 + B\mathbf{x}_2 + C\mathbf{x}_3 \leq \overline{b}$ *has at most* 8400 *inequalities.*

Note that Theorem 3.2 is substantially strengthen Theorem 2.2, because this earlier result imposed no bound on the length m of the linear system. So in the language of Chapter 2, our new results say that at the level of three quantifiers, both Integer Programming and short Presburger Arithmetic quickly saturate to the same level of complexity. As one can expect, we need very different techniques compared to Chapter 2 in order to prove these statements.

The decision part of Theorem 3.1 can naturally be generalized to short Presburger sentences of more than three quantifiers:

Theorem 3.3 (Main result). *Fix $k \geq 1$. Let $Q_1, \ldots, Q_{k+2} \in \{\forall, \exists\}$ be $k+2$ alternating quantifiers with $Q_1 = \exists$. Deciding short Presburger sentences of the form*

$$Q_1 z_1 \ \ \ldots \ \ Q_k z_k \ \ Q_{k+1} \mathbf{z}_{k+1} \ \ Q_{k+2} \mathbf{z}_{k+2} \ \ : \ \ \Phi(z_1, \ldots, z_k, \mathbf{z}_{k+1}, \mathbf{z}_{k+2})$$

is $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete. Here the short Presburger expression Φ contains at most 10 inequalities in $k+4$ variables $z_1, \ldots, z_k \in \mathbb{Z}$ and $\mathbf{z}_{k+1}, \mathbf{z}_{k+2} \in \mathbb{Z}^2$. Similarly, when $Q_1 = \forall$, deciding short Presburger sentences as above is $\mathbf{\Pi}_k^{\mathsf{P}}$-complete.

3.1.B. Proof features. The proof of the above results uses a chain of reductions. We start with the AP-Cover problem on covering intervals with arithmetic progressions. This problem is NP-compete by a result of Stockmeyer and Meyer [SM73] (see Section 3.8). The arithmetic progressions are encoded via continued fractions by a single rational number p/q. We use the plane geometry of continued fractions and "lift" the construction to a Boolean combination of polyhedra in dimension 5, proving Theorem 3.1. We then further lift the construction to convex polytopes $Q_1 \subset \mathbb{R}^9$ and $Q_2 \subset \mathbb{R}^6$, which give proofs of the two parts in Theorem 3.2. While both constructions are explicit, the first construction gives a description of Q_1 by its 24 facets, while the second gives a description of Q_2 by its 40 vertices; the bound of 8400 facets then comes from McMullen's Upper bound theorem (Theorem 3.11). Finally, we generalize the problem AP-Cover and the chain of reductions to $k \geq 3$ quantifiers.

3.1.C. Applications. The first application of our construction is the following hardness result on the *bilevel optimization* of a quadratic function over integer points in a polytope.

Theorem 3.4. *Given a rational interval $J \subset \mathbb{R}$, a rational polytope $W \subset \mathbb{R}^5$ and a quadratic rational polynomial $h : \mathbb{R}^6 \to \mathbb{R}$, computing:*

$$\max_{z \in J \cap \mathbb{Z}} \ \ \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \ \ h(z, \mathbf{w}) \tag{3.1}$$

is NP-hard. This holds even when W has at most 18 facets.

The second application is to the hardness of the *Pareto optima*. Assume we are given polytope $Q \subset \mathbb{R}^n$, and k functions $f_1, \ldots, f_k : \mathbb{R}^n \to \mathbb{R}$ restricted to the domain $Q \cap \mathbb{Z}^n$.

For a point $\mathbf{x} \in Q \cap \mathbb{Z}^n$, the corresponding outcome vector $\mathbf{y} = (f_1(\mathbf{x}), \ldots, f_k(\mathbf{x}))$ is called a *Pareto minimum*, if there is no other point $\widetilde{\mathbf{x}} \in Q \cap \mathbb{Z}^n$ and $\widetilde{\mathbf{y}} = (f_1(\widetilde{\mathbf{x}}), \ldots, f_k(\widetilde{\mathbf{x}}))$, such that $\widetilde{\mathbf{y}} \le \mathbf{y}$ coordinate-wise and $\widetilde{\mathbf{y}} \neq \mathbf{y}$. The goal is to minimize the value of an *objective function* $g : \mathbb{R}^k \to \mathbb{R}$ over all Pareto minima $\mathbf{y}$ of $(f_1, \ldots, f_k)$ on Q.

Theorem 3.5. *Given a rational polytope $Q \subset \mathbb{R}^6$, two rational linear functions $f_1, f_2 : \mathbb{R}^6 \to \mathbb{R}$, a rational quadratic polynomial $f_3 : \mathbb{R}^6 \to \mathbb{R}$, and rational linear objective function $g : \mathbb{R}^3 \to \mathbb{R}$, computing the minimum of g over the Pareto minima of (f_1, f_2, f_3) on Q is* NP*-hard. Moreover, the corresponding $1/2$-approximation problem is also* NP*-hard. This holds even when Q has at most 38 facets.*

Here by ε-approximation we mean approximating up to a multiplicative factor of ε. Both theorems 3.4 and 3.5 still hold if the polytopes are described by their vertices instead of facets. We prove these results in Section 3.7. See also §3.10.F and §3.10.G for some background and open problems.

As another byproduct of main argument, we can also optimize all the dimensions in Theorem 1.5 to best possible (all equal to 1). This is done in Corollary 3.17.

3.1.D. Kannan's Partition Theorem. In [Kan90], Kannan introduced the technology of *test sets* for an efficient solution of Parametric Integer Programming (PIP) (Theorem 3.18). In that paper, he also gave the technical *Kannan's Partition Theorem* (KPT). This result claims that one can find in polynomial time a partition of the k-dimensional parameter space P in PIP into polynomially many rational partially open polyhedra:

$$P \,=\, P_1 \,\sqcup\, P_2 \,\sqcup\, \ldots \,\sqcup\, P_r\,, \tag{3.2}$$

so that only a bounded number of tests need to be performed (see §3.9.A for a precise statement of KPT).

In another earlier work [NP17e], we showed that KPT if valid would imply a polynomial time decision algorithm for (Short-PA$_k$) for every k, and in particular (GIP). This apparently contradicts our negative results in theorems 3.1, 3.2, and 3.3, which strongly suggests that

KPT may actually be erroneous. In fact, at the time of writing [NP17e], the prevailing view was that (Short-PA$_k$) should always be in P (Conjecture 1.9). Now that we can show hardness of (Short-PA$_3$), our techniques here can be combined with some arguments in [NP17e] to obtain the following quantitative result, which strongly contradicts KPT:

Theorem 3.6. *Fix m, n and let $k = 1$. Let ℓ be the total binary length of the matrix $A \in \mathbb{Z}^{m\times n}$ in* KPT. *Then for the number r of pieces in Kannan's partition $(\circ)$, we must have $r > \exp(\varepsilon\ell)$ for some constant $\varepsilon = \varepsilon(n, m) > 0$.*

Here $k = 1$ refers to the dimension of the parameter space W in (3.24). By this, we can conclude that no polynomial size partition (3.2) exists as claimed by KPT. See Section 3.9 for a detailed presentation of Theorem 3.6 and its implications, §3.10.A for our point of view on the matter, and §3.10.B for the gap in the original proof of KPT.

3.2. Basic properties of finite continued fractions

Every rational number $\alpha > 1$ can be written in the form:

$$\alpha \;=\; [a_0;\, a_1,\, \ldots,\, a_n] \;=\; a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

where $a_0, \ldots, a_n \in \mathbb{Z}_+$. If $a_n > 1$, we have another representation:

$$\alpha \;=\; [a_0;\, a_1,\, \ldots,\, a_n - 1,\, 1] \;=\; a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{(a_n - 1) + \cfrac{1}{1}}}}.$$

On the other hand, if $a_n = 1$, then we also have:

$$\alpha \;=\; [a_0;\, a_1,\, \ldots,\, a_{n-1},\, 1] \;=\; [a_0;\, a_1,\, \ldots,\, a_{n-1} + 1].$$

It is well known that any rational $\alpha > 1$ can be written as a continued fraction as above in exactly two ways (see e.g. [Kar13, Khi64]), one with an odd number of terms and the other one with an even number of terms.

If a continued fraction $[a_0;\ a_1,\ \ldots,\ a_n]$ evaluates to a rational value p/q, we identify it with the integer point (q, p). We write:

$$(q, p) \ \leftrightarrow\ [a_0;\ a_1,\ \ldots,\ a_n].$$

From now on, we will only consider continued fractions with an odd number of terms:

$$\alpha \ =\ [a_0;\ a_1,\ \ldots,\ a_{2m}].$$

To facilitate later computations, we will relabel these $2m + 1$ terms as:

$$\alpha \ =\ [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_{m-1},\ b_{m-1},\ a_m].$$

The *convergents* of α are 2-dimensional integer vectors, defined as:

$$\begin{gathered} C_0 = (1, 0)\,,\ D_0 = (0, 1), \\ C_i = a_{i-1}D_{i-1} + C_{i-1}\,,\ \text{for } i = 1, \ldots, m + 1, \\ D_i = b_{i-1}C_i + D_{i-1}\,,\ \text{for } i = 1, \ldots, m. \end{gathered} \tag{3.3}$$

We call $C_0, D_0, \ldots, C_m, D_m, C_{m+1}$ the convergents for α. If $C_i = (q_i, p_i)$ and $D_i = (s_i, r_i)$ then we have the properties:

P1) $p_0 = 0$, $q_0 = 1$, $r_0 = 1$, $s_0 = 0$.

P2) $p_i = a_{i-1}r_{i-1} + p_{i-1}$, $q_i = a_{i-1}s_{i-1} + q_{i-1}$.

P3) $r_i = b_{i-1}p_i + r_{i-1}$, $s_i = b_{i-1}q_i + s_{i-1}$.

P4) $C_{i+1} = (q_{i+1}, p_{i+1}) \leftrightarrow [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ b_{i-1},\ a_i]$.

P5) The quotients p_i/q_i form an increasing sequence, starting with $p_0/q_0 = 0$ and ending with $p_{m+1}/q_{m+1} = \alpha$.

P6) $D_{i+1} = (s_{i+1}, r_{i+1}) \leftrightarrow [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_i,\ b_i]$.

P7) The quotients r_i/s_i form a decreasing sequence, starting with $r_0/s_0 = \infty$, and ending with $r_m/s_m = [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_{m-1},\ b_{m-1}]$.

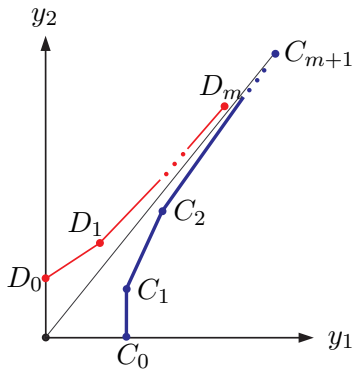


Figure 3.1: The curves $\mathcal{C}$ (bold) and $\mathcal{D}$.

Denote by O the origin in $\mathbb{Z}^2$. The geometric properties of these convergents are:

G1) Each vector $\overrightarrow{OC_i}$ and $\overrightarrow{OD_i}$ is primitive in $\mathbb{Z}^2$, meaning $\gcd(p_i, q_i) = \gcd(r_i, s_i) = 1$.

G2) Each segment C_iC_{i+1} contains exactly $a_i + 1$ integer points, since $\overrightarrow{C_iC_{i+1}} = a_i\overrightarrow{OD_i}$.

G3) Each segment D_iD_{i+1} contains exactly $b_i + 1$ integer points, since $\overrightarrow{D_iD_{i+1}} = b_i\overrightarrow{OC_{i+1}}$.

G4) The curve $\mathcal{C}$ connecting $C_0, C_1, \ldots, C_{m+1}$ is (strictly) convex upward (see Figure 3.1).

G5) The curve $\mathcal{D}$ connecting $D_0, D_1, \ldots, D_m$ is (strictly) convex downward.

G6) There are no interior integer points above $\mathcal{C}$ and below $\overrightarrow{OC_{m+1}}$. In other words, $\mathcal{C}$ is the upper envelope of all non-zero integer points between $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{m+1}}$.

3.3. From arithmetic progressions to short PA

3.3.A. Covering with arithmetic progressions. For a triple $(g, h, e) \in \mathbb{N}^3$, denote by $\mathrm{AP}(g, h, e)$ the arithmetic progression:

$$\mathrm{AP}(g, h, e) \;=\; \{g + je \;:\; 0 \le j \le h\}.$$

We reduce the following classical NP-complete problem to (Short-PA_3):

AP-Cover

Input: An interval $J = [\mu, \nu] \subset \mathbb{Z}$ and m triples (g_i, h_i, e_i) for $i = 1, \ldots, m$.

Decide: Is there $z \in J$ such that $z \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m$, where $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$?

The problem AP-Cover was shown to be NP-complete by Stockmeyer and Meyer in [SM73]. A short proof of this is included in §3.8.A for completeness. We remark that the inputs μ, ν, g_i, h_i, e_i to the problem are in binary. We can assume that each $h_i \ge 1$, i.e., each AP_i contains more than 1 integer. This is because we can always increase $\nu \leftarrow \nu + 1$ and add the last integer $\nu + 1$ to any progression AP_i that previously had only a single element. Note that AP-Cover is also invariant under translation, so we can assume that μ, ν and all g_i, h_i, e_i are positive integers.

Next, let:

$$M \;=\; 1 + \nu \prod_{i=1}^{m} g_i(g_i + h_i e_i).$$

We have:

$$M > \nu \quad \text{and} \quad M > \max_i (g_i + h_i e_i).$$

i.e., the interval $[1, M-1]$ contains J and all AP_i. Moreover, we have:

$$\gcd(M, g_i) = \gcd(M, g_i + h_i e_i) = 1,\ i = 1, \ldots, m. \tag{3.4}$$

Note that M can be computed in polynomial time from the input of AP-Cover, and

$$\log M \;=\; O\left(\sum_{i=1}^{m} \log g_i + \log h_i + \log e_i\right).$$

Let us construct a continued fraction

$$\alpha \;=\; [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_{2m-2},\ b_{2m-2},\ a_{2m-1}]$$

with the following properties:

(1) All $a_i, b_j \in [1, M]$.

(2) For each $1 \le i < m$, we have $a_{2i} = 1$.

(3) For each $1 \le i \le m$, we have $a_{2i-1} = h_i$.

(4) For each $1 \le i \le m$, if

$$C_{2i-1} := (q_{2i-1}, p_{2i-1}) \leftrightarrow [a_0;\ b_0,\ \ldots,\ a_{2i-2}]$$

then we have $p_{2i-1} \equiv g_i \,(\mathrm{mod}\ M)$.

(5) For each $1 \le i \le m$, if

$$C_{2i} := (q_{2i}, p_{2i}) \leftrightarrow [a_0;\ b_0,\ \ldots,\ a_{2i-1}]$$

then we have $p_{2i} \equiv g_i + h_i e_i \,(\mathrm{mod}\ M)$.

(6) For each $1 \le i \le m$, the segment $C_{2i-1}C_{2i}$ contains exactly $h_i + 1$ integer points. Moreover, the set

$$\mathcal{A}_i \ :=\ \{y_2 \bmod M \ :\ (y_1, y_2) \in C_{2i-1}C_{2i}\}$$

is exactly AP_i.

(7) For each $1 \le i < m$, the segment $C_{2i}C_{2i+1}$ contains no integer points apart from the two end points.

We construct α iteratively as follows. We say an integer vector $Y = (y_1, y_2)$ is congruent to $z \bmod M$, denoted $Y \equiv z \,(\mathrm{mod}\ M)$, if $y_2 \equiv z \,(\mathrm{mod}\ M)$. As in (3.3), let $C_0 = (1, 0)$ and $D_0 = (0, 1)$.

Step 1: Let $a_0 = g_1$. Then

$$C_1 = a_0 D_0 + C_0 = (1, g_1) \ \text{ and } \ C_1 \equiv g_1 \,(\mathrm{mod}\ M).$$

Step 2: Take b_0 so that

$$D_1 = b_0 C_1 + D_0 = (b_0, b_0 g_1) + (0, 1) \equiv e_1 \,(\mathrm{mod}\ M),$$

i.e.,

$$b_0 g_1 + 1 \equiv e_1 \,(\text{mod } M).$$

We can solve for $b_0 \bmod M$ because $\gcd(M, g_1) = 1$ from (3.4). So there exists $b_0 \in [1, M]$ s.t. $D_1 \equiv e_1 \,(\text{mod } M)$.

Step 3: Take $a_1 = h_1$. This implies

$$C_2 = a_1 D_1 + C_1 \equiv h_1 e_1 + g_1 \,(\text{mod } M).$$

By Property (G2), we also have exactly $h_1 + 1$ integer points on $C_1 C_2$.

Observation: After these steps, we have $h_1 + 1$ integer points on $C_1 C_2$. Every two such consecutive points differ by $\overrightarrow{OD_1}$. Reduced mod M, they give:

$$g_1,\ g_1 + e_1,\ \ldots,\ g_1 + h_1 e_1.$$

Thus, we have $\mathcal{A}_1 = \text{AP}_1$. Conditions (1)–(7) hold so far.

Step 4: Take b_1 so that $D_2 \equiv g_2 - (g_1 + h_1 e_1) \,(\text{mod } M)$. Since we have the recurrence

$$D_2 = b_1 C_2 + D_1 \equiv b_1 (g_1 + h_1 e_1) + e_1 \,(\text{mod } M)$$

this is equivalent to solving

$$b_1 (g_1 + h_1 e_1) + e_1 \equiv g_2 - (g_1 + h_1 e_1) \,(\text{mod } M).$$

Again we can solve for $b_1 \bmod M$ because $\gcd(M, g_1 + h_1 e_1) = 1$ from (3.4). So there exists $b_1 \in [1, M]$ s.t. $D_2 \equiv g_2 - (g_1 + h_1 e_1) \,(\text{mod } M)$.

Step 5: Take $a_2 = 1$. This implies

$$\begin{aligned} C_3 = a_2 D_2 + C_2 &\equiv g_2 - (g_1 + h_1 e_1) + g_1 + h_1 e_1 \\ &\equiv g_2 \,(\text{mod } M). \end{aligned}$$

This satisfies condition (4) for $i = 2$. Now we can start encoding AP_2 with $C_3 \,(\text{mod } M)$.

Observation: One can see that b_1 in Step 4 was appropriately set up to facilitate Step 5. It is conceptually easier to start with Step 5 and retrace to get the appropriate condition for b_1. Taking $a_2 = 1$ also implies that there are no other integer points on C_2C_3 apart from the two endpoints.

Step 6: Take b_2 so that $D_3 = b_2C_3 + D_2 \equiv e_2 \pmod{M}$. This is similar to Step 2. Again we use condition (3.4).

Step 7: Take $a_3 = h_2$, which implies

$$C_4 = a_3D_3 + C_3 \equiv g_2 + h_2e_2 \pmod{M}.$$

After this, we again get exactly $h_2 + 1$ integer points on C_3C_4. Reduced mod M, they give $\mathcal{A}_2 = \mathrm{AP}_2$. Note that conditions (1)–(7) still hold.

The rest proceeds similarly to Steps 4–7, for $2 \leq j \leq m - 1$:

Step 4j: Take b_{2j-1} so that

$$D_{2j} \equiv g_{j+1} - (g_j + h_je_j) \pmod{M}.$$

Step 4j+1: Take $a_{2j} = 1$, which implies

$$C_{2j+1} = D_{2j} + C_{2j} \equiv g_{j+1} \pmod{M}.$$

Step 4j+2: Take b_{2j} so that $D_{2j+1} \equiv e_{j+1} \pmod{M}$.

Step 4j+3: Take $a_{2j+1} = h_{j+1}$, which implies

$$C_{2j+2} \equiv g_{j+1} + h_{j+1}e_{j+1} \pmod{M}.$$

The segment $C_{2j+1}C_{2j+2}$ contains exactly $h_{j+1} + 1$ integer points.

Observation: After these four steps, we get $\mathcal{A}_{j+1} = \mathrm{AP}_{j+1}$. Conditions (1)–(7) hold throughout.

All modular arithmetic mod M in the above procedure can be performed in polynomial time. The last **Step** $4m-1$ gives:

$$C_{2m} \;=\; (q_{2m}, p_{2m}) \;\leftrightarrow\; [a_0;\; b_0,\; a_1,\; b_1,\; \ldots,\; a_{2m-1}].$$

Observation 3.7. All terms a_i and b_j are in the range $[1, M]$, so the final quotient p_{2m}/q_{2m} can be computed in polynomial time using the recurrence (3.3). This implies that p_{2m} and q_{2m} have polynomial binary lengths compared to the input μ, ν, g_i, h_i, e_i of AP-Cover.

The curve $\mathcal{C}$ connecting $C_0, C_1, \ldots, C_{2m}$ is shown in Figure 3.2.

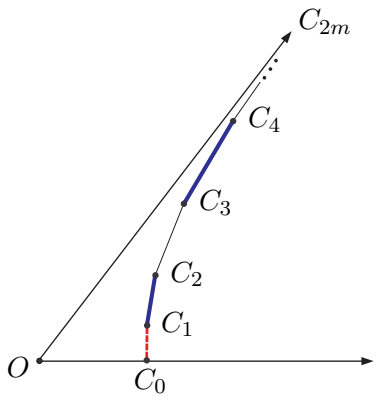


Figure 3.2: The curve $\mathcal{C}$.

Here each bold segment $C_{2i-1}C_{2i}$ contains $h_i + 1$ integer points. Each thin black segment $C_{2i}C_{2i+1}$ contains no interior integer points. The dotted segment C_0C_1 contains g_1+1 integer points, the first g_1 of which we will not need. Let $\mathcal{C}'$ be $\mathcal{C}$ minus the first g_1 integer points on C_0C_1. For brevity, we also denote $C_{2m} = (q_{2m}, p_{2m}) = (q, p)$.

Remark 3.8. Note that we have $\lfloor p/q \rfloor = a_0 = g_1$.

3.3.B. Analysis of the construction. By condition (7), every integer point $\mathbf{y} = (y_1, y_2)$ on $\mathcal{C}'$ lies in one of the segments C_1C_2, C_3C_4, $\ldots$, $C_{2m-1}C_{2m}$. Moreover, by condition (6), for $1 \le i \le m$ we have:

$$\mathrm{AP}_i \;=\; \big\{ z \in [0, M) \;:\; \exists \mathbf{y} \in C_{2i-1}C_{2i} \quad \text{s.t.} \quad z \equiv y_2 \,(\mathrm{mod}\; M) \big\}$$

Taking union over all i, for each $z \in [0, M)$, we have:

$$z \in \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m \quad \iff \quad \exists \mathbf{y} \in \mathcal{C}' \quad z \equiv y_2 \,(\mathrm{mod}\ M). \tag{3.5}$$

So AP-Cover can be restated as:

$$\exists z \in J \quad \forall \mathbf{y} \in \mathcal{C}' \quad z \not\equiv y_2 \,(\mathrm{mod}\ M). \tag{3.6}$$

Next, we express the condition $\mathbf{y} = (y_1, y_2) \in \mathcal{C}'$ in short Presburger Arithmetic. Let $\mathbf{v} = (p, -q)$ and θ be the cone between $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{2m}}$, i.e.,

$$\theta \;=\; \big\{\mathbf{y} \in \mathbb{R}^2 \;:\; y_2 \geq 0,\; \mathbf{v} \cdot \mathbf{y} \geq 0\big\}.$$

For each $\mathbf{y} = (y_1, y_2) \in \theta$, denote by $P_\mathbf{y}$ the parallelogram with two opposite vertices O and $\mathbf{y}$ and sides parallel to $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{2m}}$ (see Figure 3.3). We also require that horizontal edges in $P_\mathbf{y}$ are open, i.e.,

$$P_\mathbf{y} = \left\{ \mathbf{x} \in \mathbb{R}^2 \;:\; \begin{array}{r} \mathbf{v}\cdot\mathbf{y} \;\geq\; \mathbf{v}\cdot\mathbf{x} \;\geq\; 0 \\ y_2 \;>\; x_2 \;>\; 0 \end{array} \right\}. \tag{3.7}$$

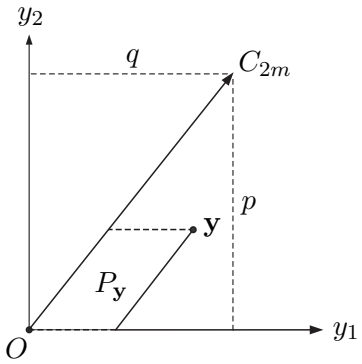


Figure 3.3: The parallelogram $P_\mathbf{y}$.

Note that the upper and lower edges of $P_\mathbf{y}$ are open (dotted). Here $C_{2m} = (q_{2m}, p_{2m}) = (q, p)$.

Lemma 3.9. *For $\mathbf{y} \in \mathbb{Z}^2$, we have $\mathbf{y} \in \mathcal{C}'$ if and only if $\mathbf{v} \in \theta$ and $P_\mathbf{y}$ contains no integer points. In other words:*

$$\mathbf{y} \in \mathcal{C}' \;\iff\; \mathbf{v}\cdot\mathbf{y} \geq 0 \;\wedge\; y_2 \geq g_1 \;\wedge\; \forall \mathbf{x} \neg \left\{ \begin{array}{r} \mathbf{v}\cdot\mathbf{y} \;\geq\; \mathbf{v}\cdot\mathbf{x} \;\geq\; 0 \\ y_2 \;>\; x_2 \;>\; 0 \end{array} \right\}. \tag{3.8}$$

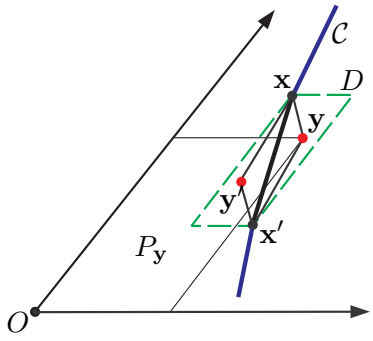


Figure 3.4: $\mathbf{y}'$ is the reflection of $\mathbf{y}$ across the midpoint of $\mathbf{x}\mathbf{x}'$.

Proof. First, assume $\mathbf{y} := (y_1, y_2) \in \mathcal{C}'$. Recall that $\mathcal{C}'$ is $\mathcal{C}$ minus the first g_1 integer points on C_0C_1. Therefore, we have $y_2 \geq g_1$. Since $\mathcal{C}$ sits inside θ, we also have $\mathbf{y} \in \theta$, which implies $\mathbf{v} \cdot \mathbf{y} \geq 0$. Let $\mathcal{R}$ be the concave region above $\mathcal{C}$ and below $\overrightarrow{OC_{2m}}$. By property (G6), $\mathcal{R}$ contains no interior integer points. Since $\mathbf{y} \in \mathcal{C}$, we have $P_{\mathbf{y}} \subset \mathcal{R}$. Therefore, the parallelogram $P_{\mathbf{y}}$ in (3.7) contains no integer points. We conclude that $\mathbf{y}$ satisfies the RHS in (3.8).

Conversely, assume $\mathbf{y}$ satisfies the RHS in (3.8) but $\mathbf{y} \notin \mathcal{C}'$. The following argument is illustrated in Figure 3.4. First, $\mathbf{v} \cdot \mathbf{y} \geq 0 \wedge y_2 \geq g_1$ implies $\mathbf{y} \in \theta$. Also, the parallelogram $P_{\mathbf{y}}$ contains no integer points. By property (G6), if $\mathbf{y} \notin \mathcal{C}'$, it must lie strictly below $\mathcal{C}'$. Let $\mathbf{x}$ and $\mathbf{x}'$ be the integer points on $\mathcal{C}$ that are immediately above and below $\mathbf{y}$ (see Figure 3.4). In other words, $\mathbf{x} \in \mathcal{C}$ is the integer point immediately above the intersection of $\mathcal{C}$ with the upper edge of $P_{\mathbf{y}}$, and $\mathbf{x}' \in \mathcal{C}$ is the integer point immediately below the intersection of $\mathcal{C}$ with the right edge of $P_{\mathbf{y}}$. Since $P_{\mathbf{y}}$ contains no integer points, particularly those on $\mathcal{C}$, the points $\mathbf{x}$ and $\mathbf{x}'$ must be adjacent on $\mathcal{C}$, i.e., they form a segment on $\mathcal{C}$.[1] Now we draw a parallelogram D with two opposite vertices $\mathbf{x}, \mathbf{x}'$ and edges parallel to those of $P_{\mathbf{y}}$ (the dashed bold parallelogram in Figure 3.4). It is clear that D lies inside θ and also contains $\mathbf{y}$. Take $\mathbf{y}'$ to be the reflection of $\mathbf{y}$ across the midpoint of $\mathbf{x}\mathbf{x}'$. Since $\mathbf{x}, \mathbf{x}'$ and $\mathbf{y}$ are integer points, so is $\mathbf{y}'$. We also have $\mathbf{y}' \in D \subset \theta$. Note also that $\mathbf{y}'$ lies on the opposite side of $\mathcal{C}$ compared to $\mathbf{y}$. Therefore, we have $\mathbf{y}' \in \mathcal{R}$, contradicting property (G6). □

[1]Note that $\mathbf{x}$ and $\mathbf{x}'$ are not necessarily two consecutive vertices C_i and C_{i+1} of $\mathcal{C}$. They could be two consecutive points on some segment C_iC_{i+1}.

Remark 3.10. There is a subtle point about the existence of $\mathbf{x}'$ in the above proof. It is clear that $\mathbf{x}$ exists because $\mathbf{y}$ lies below $\mathcal{C}$. However, if $\mathbf{y}$ lies too low, the right edge $P_{\mathbf{y}}$ might not intersect $\mathcal{C}$. For example, in Figure 3.5, we have $g_1 = 1$ and $\mathbf{y}$ lies on the line $y_2 = 1$. This this case, $P_{\mathbf{y}}$ contains no integer points and its right edge does not intersect $\mathcal{C}$. Thus, we have no $\mathbf{x}'$ and the geometric argument in Figure 3.4 does not work. However, this can be easily fixed by requiring $a_0 = g_1 \geq 2$, noting that AP-Cover is invariant under a simultaneous translation of J and all AP_i.

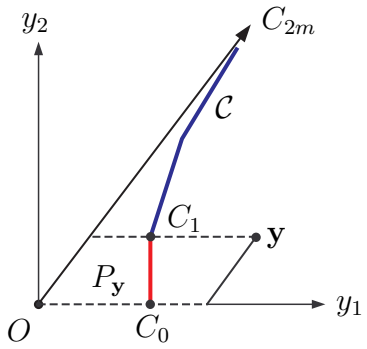


Figure 3.5: An exception.

To conclude, by combining (3.5) and (3.8) we have:

$$z \in J \cap (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m) \iff z \in J \ \wedge \ \exists \mathbf{y} \ \forall \mathbf{x} \left(z \equiv y_2 \,(\mathrm{mod}\, M) \right.$$
$$\left. \wedge\, \mathbf{v} \cdot \mathbf{y} \geq 0 \ \wedge \ y_2 \geq g_1 \ \wedge \ \neg \left\{ \begin{array}{c} \mathbf{v} \cdot \mathbf{y} \geq \mathbf{v} \cdot \mathbf{x} \geq 0 \\ y_2 > x_2 > 0 \end{array} \right\} \right). \tag{3.9}$$

Here $\mathbf{v} = (p, -q)$.

3.4. Proof of Theorem 3.1

3.4.A. Decision. The variables $z, \mathbf{y}, \mathbf{x}$ in the below sentences play the roles of $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ in (Short-PA_3), respectively. Recall that AP-Cover asks whether:

$$\exists z \in J \ \ z \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m$$

By negating (3.9), the above sentence equivalent to:

$$\exists z \in J \quad \forall \mathbf{y} \quad \exists \mathbf{x} \quad \left(z \not\equiv y_2 \,(\mathrm{mod}\ M) \ \vee\ \mathbf{v}\cdot\mathbf{y} < 0 \ \vee\ y_2 < g_1 \ \vee\ \left\{ \begin{matrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{matrix} \right\} \right). \tag{3.10}$$

The condition $z \not\equiv y_2 \,(\mathrm{mod}\ M)$ can be expressed as:

$$\exists t \quad 0 < z - y_2 - Mt < M.$$

This existential quantifier $\exists t$ can be absorbed into $\exists \mathbf{x}$ because they are connected by a disjunction. The restricted quantifier $\exists z \in J$ with $J = [\mu, \nu]$ is just

$$\exists z \quad \mu \leq z \leq \nu.$$

Overall, we can rewrite (3.10) in prenex normal form:

$$\begin{aligned} \exists z \ \ \forall \mathbf{y} \ \ \exists \mathbf{x} \ \ \mu \leq z \leq \nu \ \wedge \ \Bigg(& 0 < z - y_2 - Mx_1 < M \ \vee \\ & \vee \ \mathbf{v}\cdot\mathbf{y} < 0 \ \vee\ y_2 < g_1 \ \vee\ \left\{ \begin{matrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{matrix} \right\} \Bigg). \end{aligned} \tag{3.11}$$

All strict inequalities with integer variables can be sharpened. For example $y_2 > x_2$ is equivalent to $y_2 - 1 \geq x_2$. This final form contains 5 variables and 10 inequalities.

In summary, we have reduced AP-Cover to (3.11). This shows that (3.11) is NP-hard to decide, and so is (Short-PA_3). We still need to check that (Short-PA_3) lies in NP. By Theorem 3.8 in [Grä88], if (Short-PA_3) is true, there must be a satisfying $\mathbf{x}_1$ with binary length bounded polynomially in the binary length of Φ. Given such a polynomial length certificate $\mathbf{x}_1$, one can substitute it into (Short-PA_3) and verify the rest of the sentence, which has the form $\forall \mathbf{x}_2 \ \exists \mathbf{x}_3 \ \Psi(\mathbf{x}_2, \mathbf{x}_3)$. Here Ψ is again a short Presburger expression. By Theorem 1.8, this can be checked in polynomial time. Thus, the whole sentence (Short-PA_3) is in NP. This concludes the proof of the decision part. □

3.4.B. Counting. Notice that the above reduction from AP-Cover to (3.11) is parsimonious. At the same time, by Remark 3.14, the reduction from 3SAT to AP-Cover given in

§3.8.A can also be made parsimonious, i.e., every satisfying assignment $\mathbf{u}$ for 3SAT corresponds to a unique $z \in J \backslash (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m)$ and vice versa. Since #3SAT is a #P-complete, so is counting the number of z satisfying the negation of (3.9), which has the $\forall\exists$ form. This proves the counting part.

3.5. Proof of Theorem 3.3

This is straightforward from the k-AP-Cover problem in §3.8.B. Here we have two conditions $\tau_1 z_1 + \cdots + \tau_k z_k \in J$ and $\tau_1 z_1 + \cdots + \tau_k z_k \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m$. Again, we can use a short formula $\forall \mathbf{y}\ \exists \mathbf{x}\ \Psi(\tau_1 z_1 + \cdots + \tau_k z_k, \mathbf{y}, \mathbf{x})$ with $\mathbf{y}, \mathbf{x} \in \mathbb{Z}^2$ to express the condition $\tau_1 z_1 + \cdots + \tau_k z_k \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m$, as similar to (3.10). This takes only 8 inequalities. We also need 2 inequalities $\mu \le \tau_1 z_1 + \cdots + \tau_k z_k \le \nu$ to express J. The final sentence with the quantifiers $Q_i z_i$ has $k+4$ variables $z_1, \ldots, z_k \in \mathbb{Z}$, $\mathbf{z}_{k+1} = \mathbf{y} \in \mathbb{Z}^2$, $\mathbf{z}_{k+2} = \mathbf{x} \in \mathbb{Z}^2$ and 10 inequalities. □

3.6. Proof of Theorem 3.2

We will recast (3.11) into the form (GIP). For the two polytopes R and Q in (GIP), let $R = J = [\mu, \nu]$ and

$$Q = \big\{ \mathbf{y} \in \mathbb{R}^2 \ :\ y_2 \ge g_1,\ y_1 \le q,\ \mathbf{v} \cdot \mathbf{y} \ge 0 \big\}, \tag{3.12}$$

see Figure 3.6.

We can rewrite (3.11) as:

$$\exists z \in R \quad \forall \mathbf{y} \in Q \quad \exists \mathbf{x} \quad 0 < z - y_2 - M x_1 < M \quad \vee \quad \left\{ \begin{matrix} \mathbf{v} \cdot \mathbf{y} \ge \mathbf{v} \cdot \mathbf{x} \ge 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{matrix} \right\}. \tag{3.13}$$

Here instead of letting $\mathbf{y}$ range over $\mathbb{Z}^2$, we can restrict $\mathbf{y}$ to Q because $\mathcal{C}' \subset Q$ (see (3.6)). To remind ourselves, the inequalities $0 < z - y_2 - M x_1 < M$ say that $z \not\equiv y_2 \pmod{M}$. The

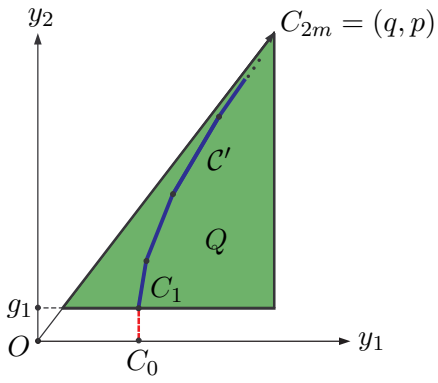


Figure 3.6: The triangle Q (shaded).

remaining step is to covert the expression

$$1 \le z - y_2 - Mx_1 \le M - 1 \ \vee \ \left\{ \begin{matrix} \mathbf{v} \cdot \mathbf{y} \ge \mathbf{v} \cdot \mathbf{x} \ge 0 \\ y_2 - 1 \ge x_2 \ge 1 \end{matrix} \right\} \tag{3.14}$$

into a single system. Here we sharpened all inequalities.

First, observe that for $z \in R$ and $\mathbf{y} \in Q$, there exists $\mathbf{x}$ satisfying (3.14) if and only if there exists such an $\mathbf{x}$ within some bounded range. Indeed, both R and Q are bounded, and (3.14) imply boundedness for $\mathbf{x}$. Therefore, we can take an N large enough so that

$$-N \le z,\, y_1,\, y_2,\, x_1,\, x_2 \le N. \tag{3.15}$$

For instance, $N = (M + p + q)^3$ suffices.

Now we convert (3.14) into a single system. This can be done with two slightly different arguments, leading to parts i) and ii) separately. Both arguments are parsimonious, which automatically imply the corresponding #P-complete statements for counting.

3.6.A. Proof of Part i). Applying the distributive law on (3.14), we get an equivalent expression:

$$\left[\begin{matrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ \mathbf{v} \cdot \mathbf{x} \le \mathbf{v} \cdot \mathbf{y} \end{matrix} \right] \ \wedge \ \left[\begin{matrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ 0 \le \mathbf{v} \cdot \mathbf{x} \end{matrix} \right] \ \wedge \ \ \ldots \tag{3.16}$$

Here each $\left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right]$ stands for a disjunction $a \vee b$ of two terms. In total, there are four such disjunctions.

Now we convert each of the above disjunctions into a conjunction. WLOG, consider the first one in (3.16). By the bounds (3.15), it is equivalent to:

$$\begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ 0 \le \mathbf{v} \cdot \mathbf{y} - \mathbf{v} \cdot \mathbf{x} \le 2N(p+q) \end{bmatrix}. \tag{3.17}$$

Let $t_1 = z - y_2 - Mx_1$ and $t_2 = \mathbf{v} \cdot \mathbf{y} - \mathbf{v} \cdot \mathbf{x}$. By (3.15), we always have

$$|t_1| \le 2N + MN, \quad |t_2| \le 2N(p+q).$$

Define two polygons in $\mathbb{R}^2$:

$$P_1 \;=\; \big\{(t_1, t_2) \in \mathbb{R}^2 \;:\; 1 \le t_1 \le M-1, |t_2| \le 2N(p+q)\big\},$$

$$P_2 \;=\; \big\{(t_1, t_2) \in \mathbb{R}^2 \;:\; |t_1| \le 2N + MN,\; 0 \le t_2 \le 2N(p+1)\big\}.$$

Then (3.17) can be rewritten as:

$$(t_1, t_2) \;\in\; P_1 \;\cup\; P_2\,. \tag{3.18}$$

Next, define:

$$P_1' = (P_1, 0), \quad P_2' = (P_2, 1) \quad \text{and} \quad P = \text{conv}(P_1', P_2').$$

In other words, we embed P_1 into the plane $t_3 = 0$ and P_2 into the plane $t_3 = 1$, all inside $\mathbb{R}^3$. As 3-dimensional polytopes, the convex hull of P_1' and P_2' is another polytope $P \subset \mathbb{R}^3$. It is easy to see that P has 6 facets, whose equations can be found from the vertices of P_1 and P_2. Also observe that for $(t_1, t_2, t_3) \in \mathbb{Z}^3$, we have:

$$(t_1, t_2, t_3) \;\in\; P \iff \begin{array}{l} (t_1, t_2) \;\in\; P_1,\; t_3 = 0, \;\text{ or} \\ (t_1, t_2) \;\in\; P_2,\; t_3 = 1. \end{array}$$

From this, we have:

$$(t_1, t_2) \;\in\; P_1 \;\cup\; P_2 \iff \exists t_3 \;:\; (t_1, t_2, t_3) \;\in\; P. \tag{3.19}$$

Combined with (3.18), it implies that (3.17) is equivalent to:

$$\exists t \;:\; (z - y_2 - Mx_1,\, py_1 - qy_2 - px_1 + qx_2,\, t) \;\in\; P.$$

The above condition is a linear system with 6 equations. Doing this for each disjunction in (3.16), we get four new variables $\mathbf{t} \in \mathbb{Z}^4$ and a combined system of 24 inequalities. Thus, the original disjunction (3.14) is equivalent to a system:

$$\exists \mathbf{t} \in \mathbb{Z}^4 \ : \ A\mathbf{x} + B\mathbf{y} + Cz + D\mathbf{t} \le \overline{b}.$$

The inner existential quantifiers $\exists \mathbf{x} \in \mathbb{Z}^2$ and $\exists \mathbf{t} \in \mathbb{Z}^4$ can be combined into $\exists \mathbf{x} \in \mathbb{Z}^6$. Substituting everything into (3.13), we obtain part i). $\square$

3.6.B. Proof of Part ii). Another way to convert (3.14) into a system is to directly interpret its two clauses and two separate polytopes. The same bounds (3.15) still apply. We will need the following special case of the *Upper Bound Theorem* (see e.g. Theorem 8.23 and Exercise 0.9 in [Zie95]).

Theorem 3.11 (McMullen)**.** *A polytope $P \subset \mathbb{R}^d$ with n vertices has at most*

$$f(d,n) \ := \ \binom{n - \lceil d/2 \rceil}{n-d} + \binom{n - \lfloor d/2 \rfloor - 1}{n-d} \quad \textit{facets.}$$

Similarly, a polytope $Q \subset \mathbb{R}^d$ with n facets has at most $f(d,n)$ vertices.

The first polytope we consider is given by:

$$\big\{(x_1, y_2, z) \in \mathbb{R}^3 \ : \ 1 \le z - y_2 - Mx_1 \le M-1, \ -N \le x_1, y_2, z \le N\big\}.$$

This is a 3-dimensional polytope with 8 facets. Applying Theorem 3.11, we see that it has at most 12 vertices. To interpret it as a polytope in $z, \mathbf{y}$ and $\mathbf{x}$ we need to form its direct product with the interval $-N \le y_2 \le N$ also embed it in the hyperplane $x_2 = 0$. This produces a polytope $P_1 \subset \mathbb{R}^5$ with 24 vertices.

The second polytope we consider is given by:

$$\big\{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^4 \ : \ \mathbf{v} \cdot \mathbf{y} \ \ge \ \mathbf{v} \cdot \mathbf{x} \ \ge \ 0, \ y_2 - 1 \ \ge \ x_2 \ \ge \ 1, \ y \in Q\big\}.$$

As a 4-dimensional polytope it has only 8 vertices. These 8 vertices correspond to the cases when $\mathbf{y}$ lies at one of the three vertices of Q. Two of these vertices give two degenerate

parallelograms $P_{\mathbf{y}}$, each of which is a segment with two vertices. The lower right vertex of Q gives a non-degenerate parallelogram $P_{\mathbf{y}}$ with four vertices. To interpret this as a 5-dimensional polytope in $z, \mathbf{y}$ and $\mathbf{x}$, we need to form its direct product with the polytope $R = [\mu, \nu]$ for z. This results in a polytope $P_2 \subset \mathbb{R}^5$ with 16 vertices.

Altogether, we have two polytopes $P_1, P_2 \subset \mathbb{R}^5$ with 40 vertices in total. We reapply the "lifting" trick in (3.19) to produce another polytope $P \subset \mathbb{R}^6$ with 40 vertices so that:

$$(z, \mathbf{y}, \mathbf{x}) \ \in \ P_1 \ \cup \ P_2 \ \iff \ \exists t \ : \ (z, \mathbf{y}, \mathbf{x}, t) \ \in \ P.$$

By Theorem 3.11, the resulting polytope P has at most

$$f(6, 40) \ = \ \binom{37}{34} \ + \ \binom{36}{34} \ = \ 8400$$

facets, which can all be found in polynomial time from the vertices. Therefore, the disjunction (3.14) is equivalent to a system:

$$\exists t \ : \ A\mathbf{x} \ + \ B\mathbf{y} \ + \ Cz \ + Dt \ \leq \ \overline{b}$$

with at most 8400 inequalities. The existential quantifiers $\exists t$ and $\exists \mathbf{x} \in \mathbb{Z}^2$ can be combined into $\exists \mathbf{x} \in \mathbb{Z}^3$. Substituting all into (3.13), we obtain part ii). $\square$

3.7. Bilevel optimization and Pareto optima

3.7.A. Proof of Theorem 3.4. First, we characterize the convex chains $\mathcal{C}$ and $\mathcal{D}$ from Figure 3.1 using a quadratic function:

Lemma 3.12. *Let $\alpha = p/q \in \mathbb{Q}_+$. If $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^2$ satisfy $\frac{u_2}{u_1} < \alpha < \frac{v_2}{v_1}$ and $v_2u_1 - v_1u_2 = 1$ then both $\frac{u_2}{u_1}$ and $\frac{v_2}{v_1}$ are "weak" convergents of α, i.e., $\mathbf{u} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{D}$.*

Proof. Assume $\mathbf{u} \notin \mathcal{C}$, then $\mathbf{u} = (u_1, u_2)$ lies strictly below $\mathcal{C}$. By the argument from Lemma 3.9, the parallelogram $P_{\mathbf{u}}$ contains another point $\mathbf{u}' = (u_1', u_2') \in \mathbb{Z}^2$ with $\frac{u_2'}{u_1'} < \alpha$. Draw a line $\boldsymbol{l}$ parallel to $\vec{\mathbf{v}}$ and passing through $\mathbf{u}$. Since $\frac{v_2}{v_1} > \alpha$, $P_{\mathbf{u}}$ lies completely to the left of $\boldsymbol{l}$ (See Figure 3.7). From this, we conclude that $1 = v_2u_1 - v_1u_2 > v_2u_1' - v_1u_2' > 0$.

In other words, the triangle $O\mathbf{uv}$ has larger area than that of $O\mathbf{u}'\mathbf{v}$. This is impossible, because $v_2u_1' - v_1u_2' \in \mathbb{Z}$. Therefore, we must have $\mathbf{u} \in \mathcal{C}$. By the same argument, we have $\mathbf{v} \in \mathcal{D}$. □

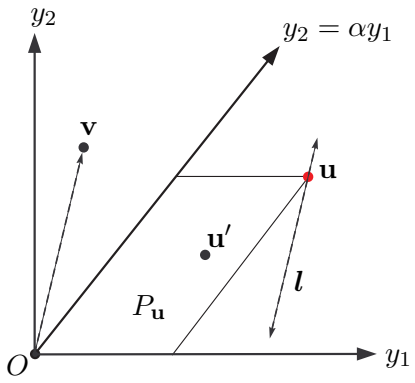


Figure 3.7: The points $\mathbf{u}$ and $\mathbf{v}$.

Conversely, for any weak convergent $\mathbf{u} \in \mathcal{C}$, we can find $\mathbf{v} \in \mathcal{D}$ with $v_2u_1 - v_1u_2 = 1$. This comes from the fact that any two consecutive convergents $\frac{p_i}{q_i}$ and $\frac{p_{i+1}}{q_{i+1}}$ of α satisfy $p_{i+1}q_i - p_iq_{i+1} = (-1)^i$.

Proof of Theorem 3.4. We use the same reduction from AP-Cover as earlier. With the same rational number $\alpha = p/q$, let

$$Q = \big\{(u_1, u_2) \in \mathbb{R}^2 \ : \ u_2 \geq g_1, \ u_1 \leq q, \ pu_1 - qu_2 \geq 0\big\},$$
$$P = \big\{(v_1, v_2) \in \mathbb{R}^2 \ : \ v_2 \leq p - 1, \ v_1 \geq 0, \ pv_1 - qv_2 \leq 0\big\}.$$

Recall (3.6), where $\mathcal{C}'$ is the part of the convex chain $\mathcal{C}$ lying inside Q. Now let $\mathbf{w} = (\mathbf{u}, \mathbf{v}, t)$, $W = Q \times P \times [0, T]$ and

$$h(z, \mathbf{w}) \quad = \quad K(v_2u_1 - v_1u_2 - 1) \quad + \quad (u_2 - z - tM)^2.$$

Here T and K are two appropriately chosen constants. Specifically, let $T = p/M$ so that if $z \equiv u_2 \pmod{M}$ then there always exists $t \in [0, T]$ with $t = \frac{u_2 - z}{M}$. For K, we pick it sufficiently large so that $K \gg (u_2 - z - tM)^2$ for every $\mathbf{u} \in Q$, $z \in J$ and $t \in [0, T]$. Clearly $K = (2TM + p)^3$ suffices.

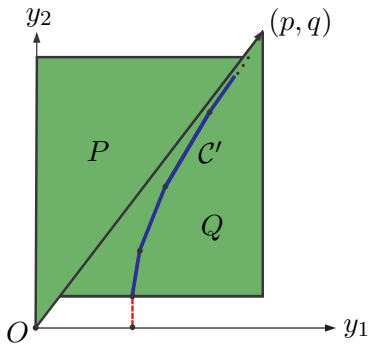


Figure 3.8: P and Q.

With $\mathbf{u} \in Q \cap \mathbb{Z}^2$ and $\mathbf{v} \in P \cap \mathbb{Z}^2$, we have $v_2u_1 - v_1u_2 \geq 1$. Furthermore, by Lemma 3.12, equality happens if and only if $\mathbf{u} \in \mathcal{C}'$ and $\mathbf{v} \in \mathcal{D}$. For a fixed $z \in J$ consider the $\mathbf{w} \in W$ that minimizes $h(z, \mathbf{w})$. Since $K \gg (z - tM - u_2)^2$, the first term in h always dominate the second one. So we must have $v_2u_1 - v_1u_2 = 1$ when h is minimized, which implies $\mathbf{u} \in \mathcal{C}'$. Furthermore, among all $\mathbf{y} \in \mathcal{C}'$, $\mathbf{u}$ must be the one for which $u_2 \bmod M$ is closest to z, so that the second term in h is minimized. Thus,

$$\min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \quad \geq \quad 0,$$

and equality holds if and only if there is some $\mathbf{y} \in \mathcal{C}'$ with $z \equiv y_2 \pmod{M}$. Therefore,

$$\max_{z \in J \cap \mathbb{Z}} \quad \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \quad > \quad 0$$

if and only if there exists some $z \in J$ for which no $\mathbf{y} \in \mathcal{C}'$ satisfies $z \equiv y_2 \pmod{M}$. We conclude that computing (3.1) is NP-hard, as it implies AP-Cover. □

3.7.B. Proof of Theorem 3.5. First recall the definition of Pareto optima defined in §3.1.C. To summarize §3.7.A, we showed that computing

$$\max_{z \in J \cap \mathbb{Z}} \quad \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \tag{3.20}$$

is NP-hard for $I \subset \mathbb{R}^1$ an interval, $W \subset \mathbb{R}^5$ a polytope with 18 facets and $h : \mathbb{R}^6 \to \mathbb{R}$ a quadratic function. Let $Q = I \times W \subset \mathbb{R}^6$, which has 38 facets. For $\mathbf{x} = (z, \mathbf{w}) \in Q \cap \mathbb{Z}^6$, let

$$f_1(\mathbf{x}) = z, \quad f_2(\mathbf{x}) = -z \quad \text{and} \quad f_3(\mathbf{x}) = h(z, \mathbf{w}).$$

Consider the set of Pareto minima of (f_1, f_2, f_3) on Q. For convenience, we denote an outcome vector $\mathbf{y} = \big(f_1(\mathbf{x}), f_2(\mathbf{x}), f_3(\mathbf{x})\big)$ by $\mathbf{y} = f(\mathbf{x})$. Consider two points $\mathbf{x} = (z, \mathbf{w})$ and $\mathbf{x}' = (z, \mathbf{w}')$ in $Q \cap \mathbb{Z}^6$. If $h(z, \mathbf{w}) < h(z, \mathbf{w}')$ then $f_1(\mathbf{x}) = f_1(\mathbf{x}')$, $f_2(\mathbf{x}) = f_2(\mathbf{x}')$, and $f_3(\mathbf{x}) < f_3(\mathbf{x}')$. Then $\mathbf{y}' = f(\mathbf{x}')$ is not a Pareto minimum in this case. Therefore, all Pareto minima must be of the form $\mathbf{y} = f(\mathbf{x})$, where $\mathbf{x} = (z, \mathbf{w}_{\min})$ with $h(z, \mathbf{w}_{\min}) = \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} h(z, \mathbf{w})$. Furthermore, if $\mathbf{x} = (z, \mathbf{w}_{\min})$ and $\mathbf{x}' = (z', \mathbf{w}'_{\min})$ are two such points with $z \neq z'$, then the outcome vectors $\mathbf{y} = f(\mathbf{x})$ and $\mathbf{y}' = f(\mathbf{x}')$ are incomparable, simply because either $f_1(\mathbf{x}) < f_1(\mathbf{x}')$ and $f_2(\mathbf{x}) > f_2(\mathbf{x}')$, or the other way around.

We conclude that the set Pareto minima of (f_1, f_2, f_3) on Q is given as:

$$\mathcal{P} = \Big\{ \mathbf{y} = \big(z, -z, h(z, \mathbf{w}_{\min})\big) \ : \ z \in J \cap \mathbb{Z},\ h(z, \mathbf{w}_{\min}) = \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} h(z, \mathbf{w}) \Big\}.$$

For $\mathbf{y} \in \mathbb{R}^3$, let $g(\mathbf{y}) = -y_3$. Then minimizing $g(\mathbf{y})$ over $\mathbf{y} \in \mathcal{P}$ is the same as computing the negated value of (3.20). This proves the first part of Theorem 3.5.

To show the hardness of approximating $\min_{\mathbf{y} \in \mathcal{P}} g(\mathbf{y})$ within a multiplicative factor of $1/2$, recall from §3.7.A that the value of (3.20) determines the AP-Cover. To be precise, (3.20) is equal to the largest squared distance of an integer $z \in J$ from the union $\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m$, which is 0 if and only if $J \cap \mathbb{Z}$ is entirely covered by these APs.

In Theorem 3.13, where we reduce 3SAT to AP-Cover. There, we pick the first ℓ odd primes $p_1, p_2, \ldots, p_\ell$. We can modify this construction by also including $p_0 = 2$, and require that $z \equiv 1 \,(\mathrm{mod}\ 2)$. In other words, now we have $J = [0, N)$, where $N = p_0 p_1 \ldots p_\ell$, and we add in an extra $\mathrm{AP}_0 = \{z \in Z : z \equiv 0 \,(\mathrm{mod}\ 2)\}$. Then the final condition is $z \in J \backslash (\mathrm{AP}_0 \cup \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m)$. So all even numbers in J are covered by AP_0, which implies that the largest squared distance of an $z \in J$ to $\mathrm{AP}_0 \cup \cdots \cup \mathrm{AP}_m$ is at most 1. Therefore, the value of (3.20) is either 1 or 0. So getting a $1/2$-approximation is equivalent to deciding AP-Cover, and thus NP-hard. □

3.8. Covering with arithmetic progressions

3.8.A. NP-completeness of AP-Cover. Let us restate the problem:

AP-Cover

Input: An interval $J = [\mu, \nu] \subset \mathbb{Z}$ and m triples (g_i, h_i, e_i) for $i = 1, \ldots, m$.

Decide: Is there $z \in J \backslash (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m)$, where $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$?

Theorem 3.13 ([SM73])**.** AP-Cover *is* NP*-complete.*

Proof. We reduce 3SAT to AP-Cover. Consider a 3-CNF Boolean formula:

$$\Psi(\mathbf{u}) \;=\; \bigwedge_{i=1}^{n} (a_i \vee b_i \vee c_i) \tag{3.21}$$

where $\mathbf{u} = (u_1, \ldots, u_\ell) \in \{\text{true}, \text{false}\}^\ell$ are the Boolean variables, and each a_i, b_i, c_i literals from the set

$$\{u_s, \neg u_s \;:\; 1 \le s \le \ell\}.$$

Deciding if there exists $\mathbf{u}$ satisfying $\Phi(\mathbf{u})$ is NP-complete.

Let $p_1, \ldots, p_\ell$ be the first ℓ odd primes. We have $p_\ell = O(\ell \log \ell)$ by the Prime Number Theorem (see [HW]), so $p_1, \ldots, p_\ell$ can all be found in time poly(ℓ). Let $N \coloneqq p_1 \cdots p_\ell$ and $J \coloneqq [0, N)$. We encode all the Boolean variables u_s by an integer variable $z \in J$ such that:

$$u_s = \text{true} \iff z \not\equiv 0 \,(\mathrm{mod}\, p_s)\,, \quad u_s = \text{false} \iff z \equiv 0 \,(\mathrm{mod}\, p_s). \tag{3.22}$$

Now for each clause $a_i \vee b_i \vee c_i$, we consider its negation. Say $a_i \vee b_i \vee c_i = u_r \vee \neg u_s \vee u_t$ for some $1 \le r, s, t \le \ell$. Then its negation is $\neg u_r \wedge u_s \wedge \neg u_t$. Now in the interval J, we exclude all z for which:

$$z \equiv 0 \,(\mathrm{mod}\, p_r), \quad z \not\equiv 0 \,(\mathrm{mod}\, p_s), \quad z \equiv 0 \,(\mathrm{mod}\, p_t). \tag{3.23}$$

By Chinese Remainder Theorem, the set of such $z \in J$ is periodic modulo $p_r p_s p_t$. Thus, they can be decomposed into a union of no more than $p_r p_s p_t$ APs, each lying inside J with period $p_r p_s p_t$. The first and last term of each such AP can also be found easily from (3.23). Denote these APs by $\mathrm{AP}_{i,1}, \ldots, \mathrm{AP}_{i,m_i}$ with $m_i < p_r p_s p_t = O(\ell^3 \log^3 \ell)$. Then we have $a_i \vee b_i \vee c_i = \text{true}$ if and only if $z \notin \mathrm{AP}_{i,1} \cup \cdots \cup \mathrm{AP}_{i,m_i}$. Therefore, by Chinese Remainder Theorem, we have:

$$\exists \mathbf{u} \in \{\text{true, false}\}^\ell \quad \Psi(\mathbf{u}) = \text{true} \quad \iff \quad \exists z \in J \;:\; z \notin \bigcup_{i=1}^{n} \bigcup_{i'=1}^{m_i} \mathrm{AP}_{i,i'}.$$

The RHS is exactly AP-Cover. In total, we have $m = \sum_{i=1}^{n} m_i < O(n\,\ell^3\,\log^3\ell)$ APs. □

Remark 3.14. Compared to the original proof in [SM73], our reduction here is *not* parsimonious, in the sense that each satisfying tuple $\mathbf{u} \in \{\text{true, false}\}^\ell$ can correspond to several $z \in J$. This is because of condition (3.22), which says that $z \,(\mathrm{mod}\, p_s)$ can be $1, 2, \ldots, p-1$ in case $u_s = \text{true}$. To make it parsimonious, we simply need to exclude the cases when $z \equiv 2, 3, \ldots, p-1 \,(\mathrm{mod}\, p_s)$, i.e., for each p_s, we require that z does not lie in $(p_s - 2)$ extra progressions $\mathrm{AP}_{s,t} = \{z \in J : z \equiv t \,(\mathrm{mod}\, p_s)\}$ with $2 \le t \le p_s - 1$. In other words, the parsimonious reduction should be:

$$z \;\notin\; \Big(\bigcup_{i=1}^{n}\bigcup_{i'=1}^{m_i} \mathrm{AP}_{i,i'}\Big) \cup \Big(\bigcup_{s=1}^{\ell}\bigcup_{t=2}^{p_s-1} \mathrm{AP}_{s,t}\Big).$$

Our simplified non-parsimonious argument has the advantage that it is directly generalizable to k quantifiers (see below).

Remark 3.15. In [GJ79, §A7], the problem AP-Cover is phrased differently under the name Simultaneous Incongruences problem.

3.8.B. Generalization of AP-Cover to k quantifiers. We consider the following direct generalization of AP-Cover.

k-AP-Cover

Input: The following elements:

- an intervals $J = [\mu, \nu]$,
- k integers $\tau_1, \ldots, \tau_k \in \mathbb{Z}$.
- $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$, with $1 \le i \le m$,

Decide: $Q_1 z_1 \in \mathbb{Z} \;\ldots\; Q_k z_k \in \mathbb{Z} \;\;:\;\; \tau_1 z_1 + \ldots + \tau_m z_m \in J \backslash (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_m)$.

Here $Q_1, \ldots, Q_k \in \{\forall, \exists\}$ are k alternating quantifiers with $Q_k = \exists$.

Theorem 3.16. *k-AP-Cover is $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete for k odd and $\mathbf{\Pi}_k^{\mathsf{P}}$-complete for k even.*

Proof. This is similar to Theorem 3.13's proof, but instead of 3SAT we use Q3SAT in (2.26). Now we need the first $k\ell$ odd primes $p_{11}, \ldots, p_{1\ell}, \ldots, p_{k1}, \ldots, p_{k\ell}$. Here ℓ is the length of

each Boolean tuple $\mathbf{u}_j \in \{\text{true, false}\}^\ell$ in (2.26). Again we have $p_{js} = O(\ell \log \ell)$ for each such prime. We associate to each tuple $\mathbf{u}_j$ an integer variable $z_j \in \mathbb{Z}$ such that:

$$u_{js} = \text{true} \iff z_j \not\equiv 0 \,(\text{mod } p_{js}) \,, \quad u_{js} = \text{false} \iff z_j \equiv 0 \,(\text{mod } p_{js}) \,, \quad 1 \le s \le \ell.$$

By Chinese Remainder Theorem, we can pick $\tau_1, \ldots, \tau_k$ such that:

$$\tau_j \equiv 1 \,(\text{mod } p_{js}) \quad \text{and} \quad \tau_j \equiv 0 \,(\text{mod } p_{j's}) \quad \text{for every} \quad 1 \le j \ne j' \le k,\, 1 \le s \le \ell.$$

Let $z \coloneqq \tau_1 z_1 + \ldots \tau_k z_k$. Then we have:

$$u_{js} = \text{true} \iff z \not\equiv 0 \,(\text{mod } p_{js}) \,, \quad u_{js} = \text{false} \iff z \equiv 0 \,(\text{mod } p_{js}).$$

Let $N \coloneqq \tau_k N_k$ and $J \coloneqq [0, N)$. Observe that by adding/subtracting from z_k a suitable multiple of N_k, we can guarantee that $z \in J$, meanwhile still keeping all the congruences $z \bmod p_{js}$ the same for $1 \le j \le k, 1 \le s \le \ell$. So since the last quantifier in k-AP-Cover is $\exists z_k$, we can always assume that $z \in J$.

Now for each clause $a_i \vee b_i \vee c_i$ in the Q3SAT statement, we again consider its negation $\neg a_i \vee \neg b_i \vee \neg c_i$. Then $a_i \vee b_i \vee c_i$ is not satisfied if and only if $z \in \text{AP}_{i,1} \cup \cdots \cup \text{AP}_{i,m_i}$, where the progressions $\text{AP}_{i,i'} \subset [0, N)$ are chosen as in Theorem 3.13's proof. The period of each such $\text{AP}_{i,i'}$ is still a product of at most three primes among $\{p_{js}\}_{1 \le j \le k, 1 \le s \le \ell}$, which is at most $O(\ell^3 \log^3 \ell)$. Doing this for all clauses, the original Q3SAT sentence in (2.26) is then equivalent to:

$$Q_1 z_1 \in J_1 \ \ldots \ Q_k z_k \in J_k \ : \ \tau_1 z_1 + \ldots \tau_k z_k \ \in \ J \setminus \left(\bigcup_{i=1}^{n} \bigcup_{i'=1}^{m_i} \text{AP}_{i,i'} \right).$$

This is exactly k-AP-Cover with $m = \sum_{i=1}^{n} m_i$ APs. □

3.8.C. An improvement of Theorem 1.5. Here is an easy consequence of k-AP-Cover:

Corollary 3.17. *For every fixed k, Theorem 1.5-i) still holds when all dimensions are 1. In other words, deciding PA sentences of the form:*

$$Q_1 z_1 \in \mathbb{Z} \ \ldots \ Q_{k+1} z_{k+1} \in \mathbb{Z} \quad : \quad \Psi(z_1, \ldots, z_{k+1})$$

is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete. Here Ψ is a Boolean combination of arbitrarily many linear inequalities. Furthermore, this still holds when the coefficients and constants of Ψ are encoded in unary.

Proof. Observe that in Theorem 3.16's proof, the finite condition $z \in J$ can be removed at the cost of making all progressions AP_i's infinite. So now we have a congruence $z \equiv \alpha_i \pmod{\beta_i}$ instead of a finite progression AP_i for each $1 \leq i \leq m$. The "infinite" k-AP-Cover sentence simply reads:

$$Q_1 z_1 \in \mathbb{Z} \ \ldots \ Q_k z_k \in \mathbb{Z} \quad : \quad \bigwedge_{i=1}^{m} \tau_1 z_1 + \cdots + \tau_k z_k \not\equiv \alpha_i \pmod{\beta_i}$$

with $Q_k = \exists$. All have to do is express each condition $\tau_1 z_1 + \cdots + \tau_k z_k \not\equiv \alpha_i \pmod{\beta_i}$ in Presburger Arithmetic. This can be easily done with one extra variable $z_{k+1} \in \mathbb{Z}$ as:

$$\bigwedge_{i=1}^{m} \tau_1 z_1 + \cdots + \tau_k z_k \not\equiv \alpha_i \pmod{\beta_i} \quad \Longleftrightarrow \quad \forall z_{k+1} \bigwedge_{i=1}^{m} \big(\tau_1 z_1 + \cdots + \tau_k z_k \neq \alpha_i + \beta_i z_{k+1}\big).$$

Here each inequality is a disjunction of two inequalities.

To see why unary input is also hard, we need to look again at Theorem 3.16's proof. There, we picked each AP_i so that its period at most $O(\ell^3 \log^3 \ell)$, where ℓ is the length of the original Q3SAT sentence. So here each α_i and β_i is also at most $O(\ell^3 \log^3 \ell)$, which means they can be input in unary. Also, each incongruence $\tau_1 z_1 + \cdots + \tau_k z_k \not\equiv \alpha_i \pmod{\beta_i}$ can be written as:

$$(\tau_1 \bmod \beta_i) z_1 + \cdots + (\tau_k \bmod \beta_k) z_k \not\equiv \alpha_i \pmod{\beta_i}.$$

Here each coefficient $(\tau_j \bmod \beta_i)$ is again of order $O(\ell^3 \log^3 \ell)$, and can be input in unary. □

3.9. On Kannan's Partition Theorem

3.9.A. Validity of KPT. By *Parametric Integer Programming* (PIP), we mean the following problem. Given an integer matrix $A \in \mathbb{Z}^{m \times n}$ and a k-dimensional polyhedron $W \subset \mathbb{R}^m$, is the following sentence true:

$$\forall \overline{b} \in W \quad \exists \mathbf{x} \in \mathbb{Z}^n \quad : \quad A\mathbf{x} \leq \overline{b}. \tag{3.24}$$

We think of $\overline{b}$ as a parameter varying over W. For every fixed $\overline{b}$, this gives an Integer Programming problem in fixed dimension n. Kannan proved that:

Theorem 3.18 ([Kan90]). *For every fixed n,* (3.24) *can be solved in polynomial time.*

Note the similarity between this and Theorem 2.1, which considered an "integer version" of (3.24). Also in [Kan90], Kannan claimed the following much stronger result, which implies both theorems 2.1 and 3.18. From here on, we use RA to denote *rational affine transformations*. Also let $K_{\overline{b}} := \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \overline{b}\}$ for every $\overline{b} \in W$.

Theorem 3.19 (Kannan's Partition Theorem). *Fix n and k. Given a* PIP *problem, we can find in polynomial time a partition*

$$W = P_1 \sqcup P_2 \sqcup \cdots \sqcup P_r, \tag{3.25}$$

where each P_i is a rational copolyhedron[2]*, so that the partition satisfies the following properties. For each P_i, we can find in polynomial time a finite set $\mathcal{T}_i = \{(S_{ij}, T_{ij})\}$ of pairs of RAs $T_{ij} : \mathbb{R}^m \to \mathbb{R}^n$ and $S_{ij} : \mathbb{Z}^n \to \mathbb{Z}^n$, so that for every $\overline{b} \in P_i$ we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \iff \exists (S_{ij}, T_{ij}) \in \mathcal{T}_i \ : \ S_{ij}\lfloor T_{ij}\overline{b} \rfloor \in K_{\overline{b}}.$$

Furthermore, for each P_i, the set $\mathcal{T}_i$ contains at most n^{4n} pairs (S_{ij}, T_{ij}). The number of all P_i is $r \leq (mn\ell)^{kn^{\delta n}}$, where ℓ is the binary length of A and δ is a universal constant.

KPT claims that in order to solve for an $\mathbf{x} \in \mathbb{Z}^n$ satisfying $A\mathbf{x} \leq \overline{b}$ with $\overline{b}$ varying over W, we only need to preprocess the matrix A in polynomial time and obtain a polynomial number of regions P_i. When queried with $\overline{b} \in P_i$, we only need to check for a fixed number (n^{4n}) of candidates of the form $\mathbf{x} = S_{ij}\lfloor T_{ij}\overline{b} \rfloor$ to get an integer solution in $K_{\overline{b}}$ (if any exists).

Let us prove that KPT, if true, would imply far stronger statements for a PIP problems that involves only a matrix of fixed length m. From now on, fix m, n and k. By KPT and the observation $mn \leq \ell$, the number of regions P_i in (3.25) can be bounded as:

$$r \ \leq \ (mn\ell)^{kn^{\delta n}} \ \leq \ \ell^{\gamma(n,k)}. \tag{3.26}$$

Here $\gamma(n, k)$ is a constant which depends only on n and k. The following structural result is an implication of KPT when the parameter space W is 1-dimensional, i.e. when $k = 1$:

$$W \ = \ \{f(y) \in \mathbb{R}^m \ : \ y \in I\} \tag{3.27}$$

[2] *A copolyhedron is a convex polyhedron with possibly some open facets.*

where $f : \mathbb{R}^1 \to \mathbb{R}^m$ is a RA, and $I \subset \mathbb{R}$ a bounded interval.

Lemma 3.20. *Assume* (3.26) *holds. Given a* PIP *problem with a* 1*-dimensional parameter space* W (3.27)*, there exists a finite set* $\mathcal{T} = \{(S_j, T_j)\}$ *of pairs of RAs* $T_j : \mathbb{R}^1 \to \mathbb{R}^n$ *and* $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ *so that the following hold. For every* $y \in I \cap \mathbb{Z}$ *and* $\overline{b} = f(y) \in \mathbb{R}^m$*, we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \quad \iff \quad \exists (S_j, T_j) \in \mathcal{T} \ : \ S_j \lfloor T_j y \rfloor \in K_{\overline{b}}.$$

Furthermore, the set $\mathcal{T}$ *contains at most* $c(n)$ *pairs* (S_j, T_j)*, where* $c(n)$ *is a constant which depends only on* n*.*

Remark 3.21. The above lemma says that the bound (3.26) as implied by KPT would guarantee a small set of candidates for any "short" PIP problem $A\mathbf{x} \leq f(y)$ with 1-dimensional parameters y. The number of candidates $c(n)$ depends only on the dimension n.

Proof of Lemma 3.20. WLOG, assume $I = [0, N)$ and $A = (a_{ij}) \in \mathbb{Z}^{m \times n}$. Let

$$M \ = \ N \prod_{ij} (|a_{ij}| + 1) \prod_{k} (|p_k q_k| + 1), \tag{3.28}$$

where p_k/q_k runs over all rational coefficients in f. Let $J = [0, MN)$. Consider the following PIP problem with one parameter $y' \in J$ and $n + 2$ integer variables $\mathbf{x} \in \mathbb{Z}^n$, $y_1, y_2 \in \mathbb{Z}$:

$$Ny_1 + y_2 = y', \quad 0 \leq y_1 < M, \quad 0 \leq y_2 < N, \quad A\mathbf{x} - f(y_2) \leq 0. \tag{3.29}$$

Observe that when (3.29) is feasible, the values of y_1 and y_2 are uniquely determined. Indeed, we should have $y_1 = \lfloor y'/N \rfloor$ and $y_2 = y' - Ny_1$. So as y' varies over $J \cap \mathbb{Z}$, the solutions of (3.29) correspond bijectively with the solutions of the original PIP problem $A\mathbf{x} \leq f(y)$ where $y = \lfloor y'/N \rfloor \in I$.

Clearly, (3.29) can be put into the form $B\mathbf{z} \leq g(y')$ where $\mathbf{z} = (\mathbf{x}, y_1, y_2) \in \mathbb{Z}^{n+2}$ are variables and g is an RA. Let $\overline{b}' = g(y')$, then the problem takes the form $B\mathbf{z} \leq \overline{b}'$. Also let $W' = \{\overline{b}' = g(y') : y' \in J\}$. Applying KPT to the PIP problem $B\mathbf{z} \leq \overline{b}'$ with a 1-dimensional parameter space W', we have a partition of W' into polynomially many intervals. Since $\overline{b}' = g(y')$ and g is an RA, this partition induces another partition on J (the space for y') into intervals:

$$J \ = \ J_1 \sqcup \cdots \sqcup J_r. \tag{3.30}$$

By (3.26), the number r of all intervals in this partition is polynomial in the binary length of the matrix B. From (3.28) and (3.29), it is clear that B has no more than $2mn$ entries, each bounded by M. Therefore, we have:

$$r \ \leq \ \left(\sum_{ij} \lceil \log b_{ij} \rceil \right)^{\gamma} \ \leq \ (2mn \log M)^{\gamma} \ L \ M. \tag{3.31}$$

Here $\gamma = \gamma(n,k)$ is some constant degree guaranteed by KPT. Since rLM, some interval J_i from (3.30) must contain an entire subinterval $I' = [kN, (k+1)N)$ for some $0 \leq k < M$. For simplicity, assume $I' = [kN, (k+1)N] \subseteq J_1$.

Also by KPT, for the interval J_1, there is a set of candidates $\mathcal{T}_1 = \{(S_{1j}, T_{1j})\}$ of size at most $c(n) \coloneqq (n+2)^{4(n+2)}$ for the PIP problem $B\mathbf{z} \leq \overline{b}'$. For every $y' \in I' \subseteq J_1$, each solution of (3.29) should have $y_1 = k$ and $y_2 = y' - Nk$. By a translation $y = y' - Nk$, we can map I' back to I. Accordingly, we can modify each candidate $(S_{ij}, T_{ij}) \in \mathcal{T}_i$ to be a pair of RAs in y. Clearly, they serve as candidates for the original PIP problem $A\mathbf{x} \leq f(y)$ with $y \in I$. $\square$

Lemma 3.20 can be easily boosted to a k-dimensional parameter space W for a fixed k:

$$W \ = \ \{f(\mathbf{y}) \in \mathbb{R}^m \ : \ \mathbf{y} \in R\} \tag{3.32}$$

with $f : \mathbb{R}^k \to \mathbb{R}^m$ an RA and $R \subset \mathbb{R}^k$ a rectangular box.

Lemma 3.22. *Assume* (3.26) *holds. Given a* PIP *problem with a k-dimensional parameter space W* (3.32)*, there exists a finite set $\mathcal{T} = \{(S_j, T_j)\}$ of pairs of RAs $T_j : \mathbb{R}^k \to \mathbb{R}^n$ and $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ so that the following hold. For every $\mathbf{y} \in R \cap \mathbb{Z}^k$ and $\overline{b} = f(\mathbf{y}) \in \mathbb{R}^m$, we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \quad \iff \quad \exists (S_j, T_j) \in \mathcal{T} \ : \ S_j \lfloor T_j \mathbf{y} \rfloor \in K_{\overline{b}}.$$

Furthermore, the set $\mathcal{T}$ contains at most $c(n,k)$ pairs (S_j, T_j), where $c(n,k)$ is a constant which depends only on n and k.

Proof. WLOG, assume $R = [0, r_1) \times \ldots \times [0, r_k)$. We "flatten" the k-dimensional parameter $\mathbf{y}$. For every $\mathbf{y} = (y_1, \ldots, y_k) \in R$, let:

$$y' \ = \ y_1 + y_2 r_1 + y_3 (r_1 r_2) + \ldots + y_k (r_1 \cdots r_{k-1}) \ \in \ [0, \, r_1 \cdots r_k). \tag{3.33}$$

This RA maps the integer points in R bijectively to those in $I = [0,\, r_1 \cdots r_k)$. We rewrite $A\mathbf{x} \le f(\mathbf{y})$ as another PIP problem with a 1-dimensional parameter $y' \in I$ and $n+k$ variables $\mathbf{x} \in \mathbb{Z}^n$, $\mathbf{y} \in \mathbb{Z}^k$:

$$\begin{aligned} y' \;&=\; y_1 + y_2 r_1 + y_3(r_1 r_2) + \ldots + y_k(r_1 \cdots r_{k-1}), \\ 0 \le y_i < r_i \;&\text{ for }\; 1 \le i \le k, \quad A\mathbf{x} - f(\mathbf{y}) \le 0. \end{aligned} \tag{3.34}$$

Note that (3.34) has a solution if and only if the original PIP problem $A\mathbf{x} \le f(\mathbf{y})$ has a solution. Furthermore, in every solution of (3.34), the variables $\mathbf{y}$ are uniquely determined by y' via the RA (3.33). Applying Lemma 3.20, we get a set $\mathcal{T}' = \{(S'_j, T'_j)\}$ of at most $c(n,k) \coloneqq (n+k+2)^{4(n+k+2)}$ candidates for (3.34), where $T'_j : \mathbb{R}^1 \to \mathbb{R}^{n+k}$ and $S'_j : \mathbb{Z}^{n+k} \to \mathbb{Z}^{n+k}$ are pairs of RAs. Using (3.33), we can re-express each pair (S'_j, T'_j) as a pair (S_j, T_j) with $T_j : \mathbb{R}^k \to \mathbb{R}^n$ and $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ so that (3.34) has a solution if and only if $\mathbf{x} = S_j \lfloor T_j \mathbf{y} \rfloor$ satisfies $A\mathbf{x} \le f(\mathbf{y})$ for some j. In other words, $\mathcal{T} = \{(S_j, T_j)\}$ is a finite set of at most $c(n,k)$ candidates for the original PIP problem $A\mathbf{x} \le f(\mathbf{y})$. □

Remark 3.23. Since the dimensions of A are fixed, each condition $S_{ij}\lfloor T_{ij}\mathbf{y} \rfloor \in K_{\overline{b}}$ can be expressed as a short Boolean combination of linear inequalities, at the cost of introducing a few extra $\exists$ or $\forall$ quantifiers. For example, a condition $\frac{1}{2} + \lfloor y/5 \rfloor \le 3$ for $y \in \mathbb{Z}$ can be expressed as either

$$\exists t \left\{ \begin{array}{rcl} t & \le & y/5 \\ t & > & y/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right\} \quad \text{or} \quad \forall t \left[\begin{array}{rcl} t & > & y/5 \\ t & \le & y/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right]. \tag{3.35}$$

Here $\{\cdot\}$ is a conjunction and $[\cdot]$ is a disjunction.

Now we relax the parameter space W to an arbitrary k-dimensional polyhedron, i.e.,

$$W \;=\; \{f(\mathbf{y}) \in \mathbb{R}^m \;:\; \mathbf{y} \in Q\} \tag{3.36}$$

with $f : \mathbb{R}^k \to \mathbb{R}^m$ an RA and $Q \subset \mathbb{R}^k$ a polyhedron.

Corollary 3.24. *Assume* (3.26) *holds. Then for every fixed m, n and k, there is a constant $d(m,n,k)$ so that the following holds. For a* PIP *problem with a k-dimensional parameter*

space W (3.36), let:

$$Q' \;=\; \big\{\mathbf{y} \in Q \cap \mathbb{Z}^k \;:\; A\mathbf{x} \le f(\mathbf{y}) \;\; \textit{has no solutions} \;\; \mathbf{x} \in \mathbb{Z}^n\big\}.$$

If $|Q'| > d(m,n,k)$, then it contains three distinct points $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3$ with $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$.

Proof. Let R be a large enough box that contains Q. Applying Lemma 3.22 to the PIP problem $A\mathbf{x} \le f(\mathbf{y})$ with $\mathbf{y} \in R$, we get a set of candidates $\mathcal{T} = \{(S_j, T_j)\}$ of size at most $c(n,k)$ so that:

$$A\mathbf{x} \le f(\mathbf{y}) \;\text{ has no solutions} \quad\Longleftrightarrow\quad \forall (S_j,T_j) \in \mathcal{T} \;:\; S_j\lfloor T_j\mathbf{y}\rfloor \not\le f(\mathbf{y}).$$

By the argument in Remark 3.23, each condition $S_j\lfloor T_j\mathbf{y}\rfloor \not\le f(\mathbf{y})$ can be expressed by a short Presburger formula $\exists \mathbf{t}\; \Phi_j(\mathbf{y},\mathbf{t})$ with length bounded in m (fixed). Taking conjunction over all such formulas for $1 \le j \le c(n,k)$, we have:

$$A\mathbf{x} \le f(\mathbf{y}) \;\text{ has no solutions} \quad\Longleftrightarrow\quad \exists \widetilde{\mathbf{t}} \quad \Phi(\mathbf{y}, \widetilde{\mathbf{t}}).^3 \tag{3.37}$$

Here Φ is still a short Presburger expression in a bounded number of variables. Denote by λ and μ the total number of variables and inequalities in Φ, respectively. Both of these are constants in m, n and k. Let $d = d(m,n,k) = 2^{\lambda+\mu}$. The μ inequalities in Φ determine μ hyperplanes in $\mathbb{R}^\lambda$. These hyperplanes partition $\mathbb{R}^\lambda$ into polyhedral regions:

$$\mathbb{R}^\lambda \;=\; W_1 \sqcup \cdots \sqcup W_\eta,$$

with $\eta \le 2^\mu$. Observe that as $(\mathbf{y}, \widetilde{\mathbf{t}})$ varies over a single region W_j, the value of $\Phi(\mathbf{y}, \widetilde{\mathbf{t}})$ is always true or always false. Since $|Q'| > d$, we have at least $d+1$ distinct pairs $(\mathbf{y}_1, \widetilde{\mathbf{t}}_1), \ldots, (\mathbf{y}_{d+1}, \widetilde{\mathbf{t}}_{d+1})$ for each of which $\Phi(\mathbf{y}_i, \widetilde{\mathbf{t}}_i) =$ true. By the pigeon hole principle, some region W_j contains at least $2^\lambda + 1$ of these pairs. Each such pair is a point in $\mathbb{Z}^\lambda$, so at least two of them must have coordinates equal modulo 2 pairwise. Assume $(\mathbf{y}_1, \widetilde{\mathbf{t}}_1)$ and $(\mathbf{y}_2, \widetilde{\mathbf{t}}_2)$ are two such two pairs. By convexity, $(\mathbf{y}_1 + \mathbf{y}_2, \widetilde{\mathbf{t}}_1 + \widetilde{\mathbf{t}}_2)/2$ is another integer point in W_j. Since Φ is always true over W_j, this pair also satisfies Φ. By (3.37), the point $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$ also lies in Q'. We conclude that $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \in Q'$. □

[3] Separate variables $\mathbf{t}$ for different Φ_j must be concatenated into $\widetilde{\mathbf{t}}$.

Theorem 3.25. *The bound* (3.26) *as claimed by* KPT *does not hold in full generality. In other words, even for* $k = 1$ *and fixed* m, n*, the number of pieces* r *in the partition* (3.25) *must be at least* $\exp(\varepsilon\ell)$ *for some constant* $\varepsilon = \varepsilon(m, n) > 0$*.*

Proof. Assume (3.26) holds. Consider the following continued fraction of length $(2\varkappa + 1)$:

$$\alpha_\varkappa \;=\; [2;\, 1, \ldots, 1] \;=\; p/q,$$

where $p = F_{2\varkappa+3}$, $q = F_{2\varkappa+1}$ are the Fibonacci numbers. From Properties (G1)–(G6) in Section 3.2, we see that the lower convex curve $\mathcal{C}$ for α connects $\varkappa + 2$ integer points:

$$C_0 = (0, 1),\; C_1 = (2, 1),\; C_2 = (5, 2),\; \ldots,\; C_{\varkappa+1} = (p, q).^4$$

Here $C_i = (F_{2i+1}, F_{2i-1})$ for $1 \le i \le s+1$. Let $\mathcal{C}'$ be the convex curve connecting $C_1, \ldots, C_{\varkappa+1}$ (see Figure 3.1). Property (G2), for every $1 \le i \le \varkappa$, the segment C_iC_{i+1} has exactly two integer points, C_i and C_{i+1}. In other words, we have $\mathcal{C}' \cap \mathbb{Z}^2 = \{C_1, \ldots, C_{\varkappa+1}\}$.

Let Q be the triangle defined in (3.12). By Lemma 3.9, an integer point $\mathbf{y} = (y_2, y_1) \in Q$ lies on $\mathcal{C}'$ if and only if $P_\mathbf{y}$ is integer point free, where $P_\mathbf{y}$ was defined in (3.7).[5] In other words, we have:

$$\begin{aligned} Q' \;&=\; \left\{ \mathbf{y} \in Q \cap \mathbb{Z}^2 \;:\; \begin{Bmatrix} py_1 - qy_2 \;\ge\; px_1 - qx_2 \;\ge\; 0 \\ y_2 - 1 \;\ge\; x_2 \;\ge\; 1 \end{Bmatrix} \text{ has no solutions } \mathbf{x} \in \mathbb{Z}^2 \right\} \\ &=\; \mathcal{C}' \cap \mathbb{Z}^2. \end{aligned}$$

The above is a PIP problem with parameters $\mathbf{y} \in Q$ and variables $\mathbf{x} = (x_1, x_2) \in \mathbb{Z}^2$. Note that the system has fixed length $m = 4$. By Corollary 3.24, there exists a constant d, so that if $|\mathcal{C}' \cap \mathbb{Z}^2| = \varkappa + 1 > d$ then there are three distinct points $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \in \mathcal{C}' \cap \mathbb{Z}^2$ with $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$. However, by the previous paragraph, the only integer points on $\mathcal{C}'$ are $C_1, \ldots, C_{\varkappa+1}$, which are in convex position, see Property (G4). Thus, none among them can be the midpoint of two others. We get a contradiction. Therefore, (3.26) cannot hold in general.

[4]Recall that the vertical coordinate is put in the first position.

[5]We take the first term in α to be 2 because of Remark 3.10

Recall the PIP problem (3.29) with a 1-dimensional parameter y', i.e., $k = 1$. From (3.26), we deduced rLM in (3.31). This led to the observation that at least one interval I' must lie in a single piece J_i. The chain of deductions continued from there through Lemma 3.22 and Corollary 3.24 and led to the above contradiction. Therefore, we must have $r > M$, which implies $r \geq 2^{\varepsilon \ell}$ for some constant $\varepsilon = \varepsilon(m, n) > 0$. □

3.9.B. Implications. To summarize, Theorem 3.25 shows that a polynomial size decomposition into polyhedral pieces as in (3.25) does not exist. If one is willing to sacrifice the polyhedral structure of the pieces, then a polynomial size partition similar to (3.25) does in fact exist [ES08] (see also [Eis10]):

Theorem 3.26 (Eisenbrand–Shmonin)**.** *Fix n and k. Let $A\mathbf{x} \leq \overline{b}$ be a* PIP *problem with a k-dimensional parameter space W. Then we can find in polynomial time a partition*

$$W \;=\; S_1 \sqcup S_2 \sqcup \ldots \sqcup S_r\,, \tag{3.38}$$

where each S_i is an integer projection *of another polyhedron $S'_i \subseteq \mathbb{R}^{m+\ell}$, defined as:*

$$S_i \;=\; \big\{\overline{b} \in \mathbb{R}^m \;:\; \exists \mathbf{t} \in \mathbb{Z}^\ell \;\; (\overline{b}, \mathbf{t}) \in S'_i\big\}.$$

Here $\ell = \ell(n)$ is a constant that depends only on n. All polyhedra S'_i can be found in polynomial time. The partition (3.38) *satisfies all other properties as claimed in* KPT.

Note that the integer projection of a polyhedron defined in the theorem is not necessarily a polyhedron as the following example shows.

Example 3.27. Consider the polytope $S' = \big\{(y_2, y_1) \in \mathbb{R}^2 \;:\; 0 \leq y_2 \leq 1,\; 0 \leq y_1 - 3y_2 \leq 2\big\}$. The integer projection of S' on the coordinate y_1 is $S = [0, 2] \cup [3, 4]$ (see Figure 3.9).

We emphasize that theorems 1.8, 2.1 and 3.18 remain valid, because their proofs still hold true if KPT is substituted by Theorem 3.26 (see [ES08]). Overall, the only discrepancy between KPT and Theorem 3.26 is about the structures of the pieces in the partition. This does not at all affect all known results about decision with two quantifiers or less. Also

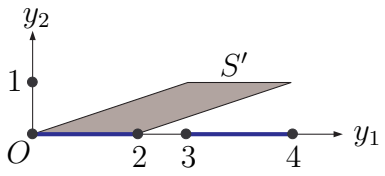


Figure 3.9: A polytope S' (shaded) and is integer projection (bold).

worth mentioning is Theorem 2.5 by Barvinok and Woods for counting projections of integer points in a polytope. This algorithm uses a weaker (valid) partitioning procedure also due to Kannan [Kan92, Lem. 3.1]. However, as we pointed out in §3.1.D, for three quantifiers or more, the structural discrepancy between KPT and Theorem 3.26 is of crucial importance.

3.10. Final remarks and open problems

3.10.A. Niels Bohr, the inventor of quantum theory, is quoted saying:

> "It is the hallmark of any deep truth that its negation is also a deep truth."

This roughly reflects our attitude towards KPT. A pioneer result at the time, it only slightly overstated the truth compared to the Eisenbrand–Shmonin theorem (Theorem 3.26). In fact, for many applications, including Kannan's Theorem 2.1 and Barvinok–Woods algorithm [BW03], Kannan's weaker result in [Kan92] is sufficient.

Let us emphasize that, of course, it would be natural to have a partition into convex (co)polyhedra rather than general semilinear sets, since convex polyhedra are much easier to work with. The fact that it took nearly 30 years until KPT was disproved, shows both the delicacy and the technical difficulty of the issue.

3.10.B. The gap in the proof of KPT (Theorem 3.1 in [Kan90]) could be traced to the following lines:

> "... for each $(b, x) \in S_i$ (with $b \in P$, $x \in \mathbb{Z}^n$), there is a unique $y \in \mathbb{Z}^l$ so that (b, x, y) belongs to S'_i. In fact, each component of y is of the form $F' \lfloor Fx \rfloor$, where F', F are

affine transformations. This is easily proved by induction on n, noting that (4.5) of [8], the z is in fact forced to be $\lfloor \alpha + 1 - \beta \rfloor$."

Here [8] refers to the conference proceedings version of the paper [Kan92]. In equation (4.5) of [Kan92], variable z is in fact forced to be $\lfloor \alpha + 1 - \beta \rfloor$. However, the quantity α in (4.5) actually depends on b, which makes $\lfloor \alpha + 1 - \beta \rfloor$ a function of b instead of a constant. This implies that y in the above quoted paragraph could also depend on b. This technical error was perhaps due to the unclear notation α, which does not reflect its dependence on b, or due to the complicated cross referencing between [Kan90] and [Kan92].

3.10.C. There is a delicate difference between the treatment of (PIP) in §3.9.A versus that in the Integer Programming literature (see e.g. [CL98, V+07, VW08]). In the latter, the parameter space W is also partitioned into convex polyhedra P_i, and over each P_i the number of solutions $\mathbf{x}$ is given by a quasi-polynomial $p_i(\overline{b})$ in $\overline{b}$. However, since there are no test sets, this does not allow us to solve (PIP) for *all* $\overline{b}$. In other words, even though a quasi-polynomial $p_i(\overline{b})$ is obtained, which evaluates to $|K_{\overline{b}} \cap \mathbb{Z}^n|$, there is no easy way to test whether $p_i(\overline{b}) \neq 0$ for all $\overline{b}$ within P_i. In general, we prove in Chapter 7 that there are strong obstacles in using (short) generating functions to decide feasibility of Presburger sentences.

3.10.D. Now that we have Theorem 3.1, one can ask if the dimension 5 is tight. Observe that for three variables and three quantifiers, there is essentially a unique form of short Presburger sentence:

$$\exists z \ \forall y \ \exists x \ : \ \Phi(x, y, z).$$

Despite Theorem 3.6, KPT actually holds for a PIP problem $ax \leq f(y, z)$ with a single variable x, i.e., when $n = 1$. Therefore, this sentence can be decided by the approach in [NP17e]. The only remaining special case of (Short-PA_3) is

$$\exists z \ \forall y \ \exists \mathbf{x} \ : \ \Phi(\mathbf{x}, y, z), \quad \text{where } \mathbf{x} \in \mathbb{Z}^2, \ y, z \in \mathbb{Z}.$$

It would be interesting to see if this case is also NP-complete.

Similarly, for sentences (GIP), one can ask if dimension 6 in Theorem 3.2-ii) can be lowered. We believe it can be, at least for the counting part.

3.10.E. Motivated in part by the *Hilbert's tenth problem*, Manders and Adleman [MA78] (see also [GJ79, §A7.2]) proved the following classical result: feasibility over $\mathbb{N}$ of

$$ax^2 + by = c$$

is NP-complete, given $a, b, c \in \mathbb{Z}$. One can view our Theorem 3.2 as a related result, where a single quadratic equation and two linear inequalities $x, y \geq 0$ (over $\mathbb{Z}$) are replaced with a system of 24 linear inequalities.

3.10.F. Minimizing polynomial functions over integer points in a convex polytope is an interesting problem of Integer Programming. Already for polynomials of degree 4 in two variables this is known to be NP-hard [DHKW06], but for lower degree polynomials some such problems can be solved in polynomial time [DHWZ16]. The survey paper [Köp12] contains extensive background on various related problems. Curiously, the following natural problem remains open:

Question 3.28. Let n be fixed. Given a polytope $P \subset \mathbb{R}^n$ and a rational quadratic function $f : \mathbb{R}^n \to \mathbb{R}$, can the optimization problem $\min_{\mathbf{x} \in P \cap \mathbb{Z}^n} f(\mathbf{x})$ be solved in polynomial time?

The case $n = 2$ was resolved positively in [DW14]. Note that the case $n = 3$ with f homogeneous is known to have an FPTAS [HWZ17].

3.10.G. Our Theorem 3.5 strongly contrasts with the positive results in [DHK09], which require that all f_i's are linear. There, it is proved that optimizing over the Pareto minima can be done in polynomial time when g is linear. Furthermore, if g is non-linear then an FPTAS also exists. Here, we say that having even one f_i quadratic is enough to make the problem hard.

Note that in Theorem 3.5 we use three polynomial functions, two or which are linear. It would be interesting to see if just two polynomial functions suffice for the hardness.

CHAPTER 4

VC-dimensions of Presburger formulas

We study VC-dimensions of *short Presburger formulas*, defined similarly to short Presburger sentences in Chapter 3. We give both lower and upper bounds, which are tight up to a polynomial factor in the binary length of the formula. This chapter is a version of the preprint [NP17a].

4.1. Introduction

The notion of VC-dimension was introduced by Vapnik and Chervonenkis in [VC71]. Although originally motivated by applications in probability and statistics, it was quickly adapted to computer science, learning theory, combinatorics, logic and other areas. We refer to [Vap98] for the extensive review of the subject, and to [Che16] for an accessible introduction to combinatorial and logical aspects.

4.1.A. Definitions of VC-dimension and VC-density. Let X be a set and $\mathcal{S} \subseteq 2^X$ be a family of subsets of X. For a subset $A \subseteq X$, let $\mathcal{S} \cap A \coloneqq \{S \cap A : S \in \mathcal{S}\}$ be the family of subsets of A cut out by $\mathcal{S}$. We say $A \subseteq X$ is *shattered* by $\mathcal{S}$ if $\mathcal{S} \cap A = 2^A$, i.e., for every subset $B \subseteq A$, there is $S \in \mathcal{S}$ with $B = S \cap A$. The largest size $|A|$ among all subsets $A \subseteq X$ shattered by $\mathcal{S}$ is called the *VC-dimension* of $\mathcal{S}$, denoted by $\mathrm{VC}(\mathcal{S})$. If no such largest size $|A|$ exists, we write $\mathrm{VC}(\mathcal{S}) = \infty$.

The *shatter function* $\pi_{\mathcal{S}}$ is defined as follows:

$$\pi_{\mathcal{S}}(n) \,=\, \max\big\{|\mathcal{S} \cap A| : A \subseteq X, |A| = n\big\},$$

The *VC-density* of $\mathcal{S}$, denoted by $\mathrm{vc}(\mathcal{S})$ is defined as

$$\inf\Big\{r \in \mathbb{R}^+ \ : \ \mathrm{limsup}_{n\to\infty}\frac{\pi_{\mathcal{S}}(n)}{n^r} < \infty\Big\}.$$

The classical theorem of Sauer and Shelah [Sa72, Sh72] states that

$$\mathrm{vc}(\mathcal{S}) \ \leq \ \mathrm{VC}(\mathcal{S}).$$

In other words, $\pi_{\mathcal{S}}(n) = O(n^d)$ in case $\mathcal{S}$ has finite VC-dimension d. In general, VC-density can be much smaller than VC-dimension, and also behaves a lot better under various operations on $\mathcal{S}$.

4.1.B. NIP theories and bounds on VC-dimension/density. It is of interest to distinguish the first-order theories in which VC-dimension and VC-density behave nicely. Let $\mathcal{L}$ be a first-order language and $\boldsymbol{M}$ be an $\mathcal{L}$-structure. Consider a *partitioned $\mathcal{L}$-formula* $F(\mathbf{x};\mathbf{y})$ whose free variables are separated into two groups $\mathbf{x} \in M^m$ (objects) and $\mathbf{y} \in M^n$ (parameters). For each parameter tuple $\mathbf{y} \in M^n$, let

$$S_{\mathbf{y}} \ = \ \big\{\mathbf{x} \in M^m : \boldsymbol{M} \models F(\mathbf{x};\mathbf{y})\big\}.$$

Here $\boldsymbol{M} \models F(\mathbf{x};\mathbf{y})$ means $F(\mathbf{x},\mathbf{y})$ evaluates to true in $\boldsymbol{M}$. Associated to F is the family $\mathcal{S}_F = \big\{S_{\mathbf{y}} : \mathbf{y} \in M^n\big\}$. We say that F is NIP, short for "F does *not* have the independence property", if $\mathcal{S}_F$ has finite VC-dimension. The structure $\boldsymbol{M}$ is called NIP if every partitioned $\mathcal{L}$-formula F is NIP in $\boldsymbol{M}$.

One prominent example of an NIP structure is our familiar Presburger Arithmetic. The main result of this chapter are the lower and upper bounds on the VC-dimensions of PA formulas. These are contrasted with the following notable bounds on the VC-density:

Theorem 4.1 ([A+16])**.** *Given a PA formula $F(\mathbf{x};\mathbf{y})$ with $\mathbf{y} \in \mathbb{Z}^n$, $\mathrm{vc}(\mathcal{S}_F) \leq n$ holds.*

In other words, VC-density in the setting of PA can be bounded solely by the dimension of the parameter variables $\mathbf{y}$. It cannot grow very large when we vary the number of object variables $\mathbf{x}$, quantified variables or the description of F. This follows from a more general

result in [A+16], which says that every *quasi-o-minimal* structure satisfies a similar bound on the VC-density. We refer to [A+16] for the precise statement of this result and for the powerful techniques used to bound the VC-density.

Karpinski and Macintyre raised a natural question whether similar bounds would hold for the VC-dimension. In [KM97], they gave upper bounds for the VC-dimension in some *o-minimal* structures (PA is not one), which are polynomial in the parameter dimension n. Later, they extended their arguments in [KM00] to obtain upper bounds on the *VC-density*, this time linear in n. Also in [KM00], the authors claimed to have an effective bound on the VC-dimensions of PA formulas. However, we cannot locate such an explicit bound in any papers. To our knowledge, no effective upper bounds on the VC-dimensions of general PA formulas exist in the literature.

4.1.C. Statements of results. For fixed k and t, denote by Short-PA(k,t) the family of PA formulas with at most k variables (both free + quantified) and t linear inequalities. When k and t are clear, a formula $F \in$ Short-PA(k,t) is simply called a short PA formula (see §3.1.A). Denote by $\ell(F)$ the length of F, which is essentially the total binary length of a fixed number of integer coefficients and constants in its linear inequalities. Our main result is a lower bound on the VC-dimensions of short Presburger formulas:

Theorem 4.2. *For every d, there is a formula $F(x;y) = \exists \mathbf{u}\ \forall \mathbf{v}\ \Psi(x,y,\mathbf{u},\mathbf{v})$ in the class* Short-PA$(10,18)$ *with*

$$\ell(F) \,=\, O(d^2) \quad \textit{and} \quad \mathrm{VC}(F) \geq d.$$

Here x, y are singletons and $\mathbf{u} \in \mathbb{Z}^6, \mathbf{v} \in \mathbb{Z}^2$. The expression Ψ is quantifier-free, and can be computed in probabilistic polynomial time in d.

So in contrast with VC-density, the VC-dimension of a PA formula F crucially depends on the actual length $\ell(F)$. For the formulas in the theorem, we have:

$$\mathrm{VC}(F) \,=\, \Omega\big(\ell(F)^{1/2}\big), \quad \text{and} \quad \mathrm{vc}(F) \leq 1,$$

where the last inequality follows from Theorem 4.1. Note that if one is allowed an unrestricted number of inequalities in F, a similar lower bound to Theorem 4.2 can be easily established

by an elementary combinatorial argument. However, since the formula F is short, we can only work with a few integer coefficients and constants.

The proof of Theorem 4.2 directly uses the AP-Cover construction from Chapter 3. The probabilistic feature of Theorem 4.2 comes from picking a prime number roughly as large as 4^d (explained in proof). By the Prime Number Theorem, this can be done in probabilistic polynomial time in d. We can actually modify this to a deterministic algorithm with run-time polynomial in d, at the cost of increasing $\ell(F)$:

Theorem 4.3. *For every d, there is a formula $F(x; y) = \exists \mathbf{u}\ \forall \mathbf{v}\ \Psi(x, y, \mathbf{u}, \mathbf{v})$ in the class* Short-PA$(10, 18)$ *with*

$$\ell(F) \,=\, O(d^3) \quad \textit{and} \quad \mathrm{VC}(F) \geq d.$$

Here x, y are singletons and $\mathbf{u} \in \mathbb{Z}^6, \mathbf{v} \in \mathbb{Z}^2$. The expression Ψ is quantifier-free, and can be computed in deterministic polynomial time in d.

We conclude with the following polynomial upper bound for the VC-dimensions of all (not necessarily short) Presburger formulas in a fixed number of variables:

Theorem 4.4. *For a PA formula $F(\mathbf{x}; \mathbf{y})$ with at most k variables (both free and quantified), we have:*

$$\mathrm{VC}(F) \,=\, O\big(\ell(F)^c\big),$$

where c and the $O(\cdot)$ constant depend only on k.

This upper bound implies that Theorem 4.2 is tight up to a polynomial factor. The proof of Theorem 4.4 uses an algorithm from Chapter 6 for decomposing a *semilinear* set, i.e., one defined by a PA formula, into polynomially many simpler pieces. Each such piece is a polyhedron intersecting a periodic set, whose VC-dimension can be bounded by elementary arguments.

We note that the bounded number of quantified variables is vital in Theorem 4.4. In §4.3.C, we construct PA formulas $F(x; y)$ with free singleton variables x, y and many quantified variables, for which $\mathrm{VC}(F)$ grows doubly exponentially compared to $\ell(F)$.

4.2. Proofs

We start with Theorem 4.3, and then show how it can be modified to give Theorem 4.2.

Proof of Theorem 4.3. Let $A = \{1, 2, \ldots, d\}$ and $\mathcal{S} = 2^A$. Since $\mathcal{S}$ contains all of the subsets of A, we have $\mathrm{VC}(\mathcal{S}) = d$. We order the sets in $\mathcal{S}$ lexicographically. In other words, for $S, S' \in \mathcal{S}$, we have $S < S'$ if $\sum_{i \in S} 2^i < \sum_{i \in S'} 2^i$. Thus, the sets in $\mathcal{S}$ can be indexed as $S_0 < S_1 < \cdots < S_{2^d-1}$, where $S_0 = \varnothing, S_1 = \{1\}, \ldots, S_{2^d-1} = A$. Next, define:

$$T \coloneqq \bigsqcup_{0 \le j < 2^d} \{i + dj \ : \ i \in S_j\}. \tag{4.1}$$

We show in Lemma 4.5 below that the set T is definable by a short PA formula $G_T(t)$ with only 8 quantified variables and 18 inequalities. Using this, it is clear that the parametrized formula

$$F_T(x; y) \ \coloneqq \ G_T(x + dy)$$

describes the family $\mathcal{S}$ (with y as the parameter), and thus has VC-dimension d. We remark that G_T has only 1 quantifier alternation (see below). □

Lemma 4.5. *The set T is definable by a short PA formula $G_T(t) = \exists \mathbf{u}\ \forall \mathbf{v}\ \Psi(t, \mathbf{u}, \mathbf{v})$ with $\mathbf{u} \in \mathbb{Z}^6, \mathbf{v} \in \mathbb{Z}^2$ and Ψ a combination of 18 inequalities with length $\ell(\Psi) = O(d^3)$.*

Proof. Our strategy is to represent the set T as a union of arithmetic progressions (APs). In Chapter 3, we gave a method to define any union of APs by a short PA formula of polynomial length. For each $1 \le i \le d$, let $J_i = \{j : 0 \le j < 2^d, i \in S_j\}$. From (4.1), we have:

$$T = \bigsqcup_{i=1}^{d} (i + dJ_i). \tag{4.2}$$

From the lexicographic ordering of the sets S_j, we can easily describe each set J_i as:

$$J_i = \{m + 2^{i-1} + 2^i n \ : \ 0 \le m < 2^{i-1},\ 0 \le n < 2^{d-i}\}. \tag{4.3}$$

So each set J_i is not simply an AP, but the Minkowski sum of two APs. However, we can easily modify each J_i into an AP by defining:

$$J_i' = \{2^d(m + 2^{i-1}) + 2^i n \ : \ 0 \le m < 2^{i-1},\ 0 \le n < 2^{d-i}\}. \tag{4.4}$$

It is clear that J'_i is an AP that starts at 2^{d+i-1} and ends at $2^{d+i} - 2^i$ with step size 2^i. Let $\mathrm{AP}_i \coloneqq i + dJ'_i$ and

$$T' = \bigsqcup_{i=1}^{d} \mathrm{AP}_i. \tag{4.5}$$

This is a union of d arithmetic progressions. Using the construction from Sections 3.3, we can define T' by a short PA formula:

$$t' \in T' \quad \iff \quad \exists \mathbf{w} \quad \forall \mathbf{v} \quad \Phi\big(t', \mathbf{w}, \mathbf{v}\big),$$

where $t' \in \mathbb{Z}$, $\mathbf{w}, \mathbf{v} \in \mathbb{Z}^2$ and Φ is a Boolean combination of at most 10 inequalities. Recall that this construction works by finding a single continued fraction $\alpha = [a_0; b_0, a_1, b_1, \ldots, a_{2d-1}]$ whose successive convergents encode the starting and ending points of our $\mathrm{AP}_1, \ldots, \mathrm{AP}_d$. For each i, the first and last terms in AP_i are respectively $\beta_i = i + d2^{d+i-1}$ and $\gamma_i = i + d(2^{d+i} - 2^i)$, which have binary lengths $O(d)$. By Observation 3.7, each term a_k and b_k in α is at most the product of these β_i and γ_i. Since $\prod_{i=1}^{d} \beta_i \gamma_i$ has binary length $O(d^2)$, and so does each term a_k and b_k. Therefore, the final continued fraction α is a rational number p/q with binary length $O(d^3)$. This implies that $\ell(\Phi) = O(d^3)$ as well.

To get a formula for T, note that from (4.2), (4.3), (4.4) and (4.5), we have:

$$\begin{aligned} t \in T \quad \iff \quad \exists\, t', i, r, s \quad : \quad & t' \in T', \quad 1 \le i \le d, \quad 0 \le s < 2^d, \\ & t' = i + d(2^d r + s), \quad t = i + d(r + s).^{1} \end{aligned}$$

Here r and s respectively stand for $m + 2^{i-1}$ and $2^i n$ in (4.3). Using $\exists \mathbf{w}\ \forall \mathbf{v}\ \Phi(t', \mathbf{w}, \mathbf{v})$ to express $t' \in T'$, we get a formula $G_T(t)$ defining T with 8 quantified variables $t', i, r, s \in \mathbb{Z}$, $\mathbf{w}, \mathbf{v} \in \mathbb{Z}^2$ and 18 inequalities. Note that t', i, r, s and $\mathbf{w}$ are existential variables, so G_T has the form $\exists \mathbf{u}\ \forall \mathbf{v}\ \Psi(t, \mathbf{u}, \mathbf{v})$ with $\mathbf{u} \in \mathbb{Z}^6, \mathbf{v} \in \mathbb{Z}^2$ and Ψ quantifier-free. □

Proof of Theorem 4.2. Note that the above construction of F_T and G_T is deterministic with run-time polynomial in d. For Theorem 4.2, only the existence of a short PA formula with high VC-dimension is needed. In this case, our lower bound can be improved to $\mathrm{VC}(F) \ge c\sqrt{\ell(F)}$, for some $c > 0$, as follows. Recall that $\beta_i = i + d2^{d+i-1}$

[1] Here each equality is a pair of inequalities.

and $\gamma_i = i + d(2^{d+i} - 2^i)$ are the smallest and largest terms of AP_i in (4.5). Pick the smallest prime p larger than $\max(\gamma_1, \ldots, \gamma_d) \approx d4^d$. This prime p can substitute for the number M in Section 3.3, which was (deterministically) chosen as $1 + \prod_{i=1}^{d} \beta_i \gamma_i$, so that it is larger and coprime to all of them. The rest of the construction follows verbatim as before. Note that $\log p = O(d)$ by Chebyshev's theorem. So the final continued fraction $\alpha = [a_0; b_0, a_1, b_1, \ldots, a_{2d-1}]$ has length $O(d^2)$, because now each term a_k, b_k has length at most $\log p$. This completes the proof. $\square$

Proof of Theorem 4.4. Let $F(\mathbf{x}; \mathbf{y})$ be any PA formula with free variables $\mathbf{x} \in \mathbb{Z}^m$, $\mathbf{y} \in \mathbb{Z}^n$ and n' other quantified variables, where m, n, n' are fixed. In Theorem 6.17, we give the following polynomial decomposition for the semilinear set defined by F:

$$\Sigma_F \;\coloneqq\; \big\{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^{m+n} \;:\; F(\mathbf{x}; \mathbf{y}) = \text{true}\big\} \quad = \quad \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j. \tag{4.6}$$

Here each R_j is a polyhedron in $\mathbb{R}^{m+n}$, and each $\boldsymbol{T}_j \subseteq \mathbb{Z}^{m+n}$ is a periodic set, i.e., a union of several cosets of some lattice $\mathcal{T}_j \subseteq \mathbb{Z}^{m+n}$. In other words, the set defined by F is a union of r pieces, each of which is a polyhedron intersecting a periodic set. Our decomposition is algorithmic, in the sense that the pieces R_j and lattices $\mathcal{T}_j$ can be found in time $O\big(\ell(F)^c\big)$, with c and $O(\cdot)$ depending only on m, n, n'. The algorithm describes each piece R_j by a system of inequalities and each lattice $\mathcal{T}_j$ by a basis. Denote by $\ell(R_j)$ and $\ell(\mathcal{T}_j)$ the total binary lengths of these systems and basis vectors, respectively. These also satisfy:

$$\sum_{j=1}^{r} \ell(R_j) + \ell(\mathcal{T}_j) = O\big(\ell(F)^c\big). \tag{4.7}$$

Each R_j can be written as the intersection $H_{j1} \cap \cdots \cap H_{jf_j}$, where each H_{jk} is a half-space in $\mathbb{R}^{m+n}$, and f_j is the number of facets of R_j. Note that $f_j \le \ell(R_j) = O\big(\ell(F)^c\big)$. We rewrite (4.6) as:

$$\Sigma_F \quad = \quad \bigsqcup_{j=1}^{r} H_{j1} \cap \cdots \cap H_{jf_j} \cap \boldsymbol{T}_j. \tag{4.8}$$

Therefore, the set Σ_F is a Boolean combination of $f_1 + \cdots + f_r$ half-spaces and r periodic sets. In total, there are

$$f_1 + \cdots + f_r + r = O\big(\ell(F)^c\big) \tag{4.9}$$

of those basic sets.

For a set $\Gamma \subseteq \mathbb{R}^{m+n}$ and $\mathbf{y} \in \mathbb{Z}^n$, denote by $\Gamma_{\mathbf{y}}$ the subset $\{\mathbf{x} \in \mathbb{Z}^m : (\mathbf{x}, \mathbf{y}) \in \Gamma\}$ and by $\mathcal{S}_\Gamma$ the family $\{\Gamma_{\mathbf{y}} : \mathbf{y} \in \mathbb{Z}^n\}$. For a half-space $H \subset \mathbb{R}^{m+n}$, it is easy to see that $\mathrm{VC}(\mathcal{S}_H) = 1$. For each periodic set $\boldsymbol{T}_j$ with period lattice $\mathcal{T}_j$, the family $\mathcal{S}_{\boldsymbol{T}_j}$ has cardinality at most $\det(\mathcal{T}_j \cap \mathbb{Z}^n) \leq 2^{O(\ell(\mathcal{T}_j))}$. Thus, we have

$$\mathrm{VC}(\mathcal{S}_{\boldsymbol{T}_j}) \leq \log |\mathcal{S}_{\boldsymbol{T}_j}| = O\big(\ell(\mathcal{T}_j)\big). \tag{4.10}$$

Let $\Gamma_1, \ldots, \Gamma_t \subseteq \mathbb{Z}^{m+n}$ be any t sets with $\mathrm{VC}(\mathcal{S}_{\Gamma_i}) = d_i$. By an application of the Sauer-Shelah lemma ([Sa72, Sh72]), if Σ is any Boolean combination of $\Gamma_1, \ldots, \Gamma_t$, then we can bound $\mathrm{VC}(\mathcal{S}_\Sigma)$ as:

$$\mathrm{VC}(\mathcal{S}_\Sigma) = O\big((d_1 + \cdots + d_t) \log(d_1 + \cdots + d_t)\big).$$

Applying this to (4.8), we get $\mathrm{VC}(\mathcal{S}_{\Sigma_F}) = O(\ell \log \ell)$, where

$$\ell \;=\; \sum_{j=1}^{r} \left(\mathrm{VC}(\mathcal{S}_{\boldsymbol{T}_j}) + \sum_{j'=1}^{f_j} \mathrm{VC}(\mathcal{S}_{H_{jj'}}) \right) \;\leq\; \sum_{j=1}^{r} \mathrm{VC}(\mathcal{S}_{\boldsymbol{T}_j}) + f_j.$$

By (4.7), (4.9) and (4.10), we have $\ell = O\big(\ell(F)^c\big)$. We conclude that $\mathrm{VC}(F) = O\big(\ell(F)^{2c}\big)$.

□

4.3. Final remarks and open problems

4.3.A. The proof of Theorem 4.2 is almost completely deterministic except for finding a small prime p larger than a given integer N. This problem is considered to be computationally very difficult in the deterministic case, where only exponential algorithms are known (see [LO87, TCH12]).

4.3.B. Our constructed short formula F is of the form $\exists\forall$. It is interesting to see if similar polynomial lower bounds are obtainable with existential short PA formulas. For such a formula $F(\mathbf{x}; \mathbf{y}) = \exists \mathbf{z}\, \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$, the quantifier-free expression $\Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ captures the set of

integer points Γ lying in a union of some polyhedra P_i's. Note that the total number of polyhedra and their facets should be bounded, since we are working with short formulas. Therefore, F simply capture the pairs $(\mathbf{x}, \mathbf{y})$ in the projection of Γ along the $\mathbf{z}$ direction. Denote this set by $\text{proj}(\Gamma)$. By Theorem 1.8, $\text{proj}(\Gamma)$ has a *short generating function*, and can even be counted efficiently in polynomial time. In our construction, the set that yields high VC-dimension is a union arithmetic progressions, which cannot be counted efficiently unless $\mathsf{P} = \mathsf{NP}$ (Theorem 3.13). This difference indicates that $\text{proj}(\Gamma)$ has a much simpler combinatorial structure, and may not possess high enough VC-dimension.

4.3.C. One can ask about the VC-dimension of a general PA formula with no restriction on the number of variables, quantifier alternations or atoms. By the famous Theorem 1.2 of Fischer and Rabin, PA has decision complexity at least doubly exponential in the general setting. For every $\ell > 0$, they constructed a formula $\text{Prod}_\ell(a, b, c)$ of length $O(\ell)$ so that for every triple

$$0 \le a, b, c < 2^{2^{2^\ell}},$$

we have $\text{Prod}_\ell(a, b, c) = \text{true}$ if and only if $ab = c$. Using this "partial multiplication" relation, one can easily construct a formula $F_\ell(x; y)$ of length $O(\ell)$ and VC-dimension at least 2^{2^ℓ}. This can be done by constructing a set similar to T in (4.1) with d replaced by 2^{2^ℓ} using Prod_ℓ. We leave the details to the reader.

Regarding upper bound, by Theorem 1.3 of Oppen, any general PA formula F of length ℓ is equivalent to a quantifier-free formula G of length $2^{2^{2^{c\ell}}}$, where $c > 0$ is a universal constant. This implies that $\text{VC}(G)$, and thus $\text{VC}(F)$, is at most triply exponential in $\ell(F)$. We conjecture that a doubly exponential upper bound on $\text{VC}(F)$ holds in the general setting. It is unlikely that such an upper bound could be established by straightforward quantifier elimination, which generally results in triply exponential blow up (see [Wei97, Thm 3.1]).

CHAPTER 5

Parametric Presburger Arithmetic

We consider *k-parametric Presburger Arithmetic*, which allows multiplication by k parameters $\mathbf{t} = (t_1, \ldots, t_k)$. A formula in this language defines a parametric set $S_{\mathbf{t}} \subseteq \mathbb{Z}^d$ as $\mathbf{t}$ varies over $\mathbb{Z}^k$, and we examine the cardinality $|S_{\mathbf{t}}|$ as a function of $\mathbf{t}$. For $k = 1$, i.e., a single parameter t, it is known that $|S_t|$ always has a nice *eventual quasi-polynomial* form, which implies that $|S_t|$ is a polynomial-time computable function of t. Our main result (Theorem 5.10) says that such a nice expression is likely impossible with $k \geq 2$: Assuming $\mathsf{P} \neq \mathsf{NP}$, we construct a 2-parametric set S_{t_1,t_2} such that $|S_{t_1,t_2}|$ is not polynomial-time computable on input (t_1, t_2). In contrast, for any k-parametric set $S_{\mathbf{t}} \subseteq \mathbb{Z}^d$ defined in a similar language without the ordering relation, we show in Theorem 5.24 that $|S_{\mathbf{t}}|$ is always polynomial-time computable in $\mathbf{t}$, and in fact can be represented using gcd and similar functions. This chapter is a version of the preprint [BGNW18].

5.1. Introduction

5.1.A. Formulations and examples. We study the difficulty of counting points in parametric sets of the form

$$S_{\mathbf{t}} = \{\mathbf{x} \in \mathbb{Z}^d \quad : \quad Q_1 y_1 \, Q_2 y_2 \, \ldots Q_m y_m \;\; \Psi_{\mathbf{t}}(\mathbf{x}, \mathbf{y})\}. \tag{5.1}$$

Here $\mathbf{x} = (x_1, \ldots, x_d)$ are the *free* variables, $\mathbf{y} = (y_1, \ldots, y_m)$ are the *quantified* variables and $\mathbf{t} = (t_1, \ldots, t_k)$ are the *parameters*, all ranging over $\mathbb{Z}$; $Q_i \in \{\forall, \exists\}$ are the quantifiers; and $\Psi_{\mathbf{t}}(\mathbf{x}, \mathbf{y})$ is a Boolean combination, in disjunctive normal form, of linear inequalities in $\mathbf{x}, \mathbf{y}$

with coefficients in $\mathbb{Z}[\mathbf{t}]$. That is,

$$\Psi_{\mathbf{t}}(\mathbf{x},\mathbf{y}) = \left[A_1(\mathbf{t})\cdot(\mathbf{x},\mathbf{y})^T \ \leq\ \overline{b}_1(\mathbf{t})\right] \ \vee\ \ldots\ \vee\ \left[A_\ell(\mathbf{t})\cdot(\mathbf{x},\mathbf{y})^T \leq \overline{b}_\ell(\mathbf{t})\right], \tag{5.2}$$

where each $A_i(\mathbf{t})$ is a $r_i \times (d+m)$ matrix, each $\overline{b}_i(\mathbf{t})$ is a length r_i column vector, all with entries in $\mathbb{Z}[\mathbf{t}]$, and the concatenation $(\mathbf{x},\mathbf{y})$ of the $\mathbf{x}$ and $\mathbf{y}$ variables is treated as a row vector. If there are k parameters $t_1,\ldots,t_k$, we say that the family of sets $\{S_{\mathbf{t}} : \mathbf{t}\in\mathbb{Z}^k\}$ is a *k-parametric Presburger family*. A general expression of the type

$$\Phi_{\mathbf{t}}(\mathbf{x}) = Q_1 y_1\ Q_2 y_2\ \ldots Q_m y_m\ \ \Psi_{\mathbf{t}}(\mathbf{x},\mathbf{y}) \tag{5.3}$$

with $\Psi_{\mathbf{t}}(\mathbf{x},\mathbf{y})$ as in (5.1) is called a *formula in k-parametric Presburger Arithmetic* (often abbreviated as k-parametric PA). Classic Presburger Arithmetic corresponds to $k=0$. Below is the main question addressed in this.

Question 5.1. Given a k-parametric Presburger family defined by $S_{\mathbf{t}} = \{\mathbf{x}\in\mathbb{Z}^d : \Phi_t(\mathbf{x})\}$, under what conditions on $\Phi_{\mathbf{t}}$ is the counting function $|S_{\mathbf{t}}|$ a "nice" function of $\mathbf{t}$?

Of course, "nice" is a vague qualifier, so let's start with some nice examples. We will assume that the parameters t_i are nonnegative in the following examples, which simplifies the number of cases:

Example 5.2. If we define $S_{t_1,t_2} = \{x\in\mathbb{Z} :\ x\geq 0\ \ \wedge\ \ t_1 x \leq t_2\}$, then

$$|S_{t_1,t_2}| = \lfloor t_2/t_1\rfloor + 1.$$

Example 5.3. The set $S_{t_1,t_2} = \left\{(x_1,x_2)\in\mathbb{Z}^2 :\ x_1,x_2\geq 0\ \ \wedge\ \ t_1x_1+t_2x_2 = t_1t_2\right\}$ consists of the integer points on a line segment with endpoints $(t_2,0)$ and $(0,t_1)$, and so

$$|S_{t_1,t_2}| = \gcd(t_1,t_2)+1.$$

Example 5.4. If $S_{t_1,t_2} = \{(x_1,x_2)\in\mathbb{Z}^2 :\ x_1,x_2\geq 0\ \ \wedge\ \ x_1+x_2=t_1\ \ \wedge\ \ 2x_1+x_2\leq t_2\}$, then the equality forces $x_2 = t_1 - x_1$ (which is only valid if $x_1\leq t_1$) and substituting into

the inequality shows that

$$|S_{t_1,t_2}| \;=\; |\{x_1 \in \mathbb{Z} :\; 0 \le x_1 \le \min(t_1, t_2 - t_1)\}|$$
$$= \begin{cases} t_1 + 1 & \text{if } 2t_1 \le t_2, \\ t_2 - t_1 + 1 & \text{if } t_1 \le t_2 < 2t_1, \\ 0 & \text{if } t_2 < t_1. \end{cases}$$

Example 5.5. If $S \;=\; \big\{x \in \mathbb{N} \;:\; \forall y, z \in \mathbb{N} \quad x \;\neq\; (t^2+2)y + (3t)z\big\}$, then we have:

$$|S| \;=\; \begin{cases} \infty \quad \text{if} \quad 3 \nmid t \quad \text{or} \quad 2 \mid t \\ (t^2+1)(3t-1)/2 \quad \text{otherwise} \end{cases}.$$

We are seeing many types of "nice" functions in these examples, and the question is now how to generalize. In fact, Example 5.5 generalizes to any family in 1-parametric PA by the result in [BWG17], as described below.

5.1.B. 1-parametric Presburger Arithmetic. In the case of a single parameter t, our perspective means studying families $\{S_t \;:\; t \in \mathbb{Z}\}$ of subsets of $\mathbb{Z}^d$ of the form

$$S_t = \{\mathbf{x} \in \mathbb{Z}^d \quad : \quad Q_1 y_1 \; Q_2 y_2 \; \ldots Q_m y_m \;\; \Psi_t(\mathbf{x}, \mathbf{y})\}, \tag{5.4}$$

where $\Psi_t(\mathbf{x}, \mathbf{y})$ is exactly as in (5.2) except that the entries of the A_i's and the $\overline{b}_i$'s come from the univariate polynomial ring $\mathbb{Z}[t]$. The study of such *1-parametric PA families* was proposed by Woods in [Woo14]. These families were further analyzed in [BWG17], in which the main result is that they exhibit *quasi-polynomial* behavior:

Definition 5.6. A function $g : \mathbb{Z} \to \mathbb{Z}$ is a *quasi-polynomial* if there exists a period m and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that

$$g(t) = f_i(t), \text{ for } t \equiv i \bmod m.$$

We allow special cases when some $f_i(t) = \infty$. A function $g : \mathbb{Z} \to \mathbb{Z}$ is an *eventual quasi-polynomial*, abbreviated *EQP*, if it agrees with a quasi-polynomial for sufficiently large $|t|$.

Example 5.5 is a family where $|S_t|$ is an EQP.

Theorem 5.7 ([BWG17]). *Let $\{S_t : t \in \mathbb{Z}\}$ be a 1-parametric PA family. There exists an EQP $g : \mathbb{Z} \to \mathbb{N}$ such that $g(t) = |S_t|$. The set of t such that S_t has finite cardinality is eventually periodic.*

Remark 5.8. In [BWG17], the parameter t takes values in $\mathbb{N}$ instead of $\mathbb{Z}$. However, one can see that the same proofs and conclusions also hold when t ranges over $\mathbb{Z}$.

Note that any fixed EQP is a polynomial-time computable function, so we easily get:

Corollary 5.9 ([BWG17]). *Let S_t be any fixed 1-parametric PA family. Then there are polynomial time algorithms to:* i) *check if $|S_t| = \infty$,* ii) *compute $|S_t|$ if $|S_t| < \infty$.*

There are several other forms of quasi-polynomial behavior that 1-parametric PA families exhibit (such as possessing EQP Skolem functions; see [BWG17]). Here we focus on the cardinality, $|S_t|$. We hope the reader agrees that EQPs are relatively "nice" functions.

5.1.C. Statements of results. Abusing the notation, we also denote a parametric PA family $\{S_{\mathbf{t}} : \mathbf{t} \in \mathbb{Z}^k\}$ just by $S_{\mathbf{t}}$ when the dimension k is clear.

Theorem 5.10. *Assume $\mathsf{P} \neq \mathsf{NP}$. Then there exists a 2-parametric $\exists\forall$ PA family S_{t_1,t_2} for which $|S_{t_1,t_2}|$ is always finite but cannot be expressed as a polynomial time computable function in t_1 and t_2.*

Here, by an $\exists\forall$ PA family, we mean S_{t_1,t_2} is of the form (5.1) where the quantifiers are $\exists \ldots \exists \forall \ldots \forall$. We also remark that technically, only the weaker assumption $\#\mathsf{P} \neq \mathsf{FP}$ is needed. Two consequences of this result are:

Corollary 5.11. *There is a 2-parametric PA family S_{t_1,t_2} such that the set of $(t_1, t_2) \in \mathbb{Z}^2$ for which $|S_{t_1,t_2}|$ is positive cannot be described using polynomial-time relations in t_1, t_2.*

Corollary 5.12. *Any extension of 2-parametric PA with only polynomial-time computable predicates cannot have full quantifier elimination.*

5.1.D. Structure of the chapter. We will present what amount to two different proofs of Theorem 5.10 in the following two sections. In each case, we leverage the main result of Chapter 3, which gives a "hard" 3-parametric $\exists\forall$ PA formula, and then show how this can be reduced to a 2-parametric $\exists\forall$ PA formula. For the first reduction presented in Section 5.2, we use a trick due to Glivický and Pudlák [GP17] to encode multiplication with three different parameters by multiplications with only two parameters. This reduction has the advantage of not increasing the number of free variables in the formula. Next, in Section 5.3 we present a more general counting-reduction technique which is less *ad hoc* and reduces any k-parametric PA formula to a 2-parametric PA formula with the same number of quantifier alternations; the idea here is a little more transparent than in Section 5.2, but it has the disadvantage of introducing many more new free and quantified variables to the formula, so we consider that it is interesting to present both reductions.

In Section 5.4 we consider a variant of Question 5.1 in which there is no order relation in our language; that is, we can only express linear equations but not linear inequalities. Quantifier-free formulas in this language define finite unions of *lattice translates*. This setting was studied in detail from a model-theoretic perspective by van den Dries and Holly [vdDH92], and we apply their results to show that, in contrast to Theorem 5.10, the counting functions in the unordered setting can be computed in polynomial time, regardless of the number of parameters and of quantifier alternations. Indeed, these functions can be expressed using gcd and related functions.

Finally, in Section 5.5 we discuss the optimality of Theorem 5.10 by explaining what happens when we weaken or modify some of the hypotheses.

5.2. Proof of Theorem 5.10 and its corollaries

Recall from Chapter 3 that a *short PA sentence* is a sentence in classical PA whose numbers of alternations, variables and linear inequalities are all bounded. We proved in Theorem 3.1 that $\exists\forall\exists$ short PA sentences of at most 5 variables and 10 inequalities are NP-complete to

decide by reducing the NP-complete problem AP-Cover to them.

Recall the statement of AP-Cover from §3.3.A. It asks whether there is some integer in a given interval $J = [\mu, \nu]$, which is not covered by several given arithmetic progressions $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$. The problem is clearly invariant under a translation of both J and the AP_i's, so we can assume $\mu = 1$. Also without affecting the complexity, we can assume that $g_1 = \nu, h_1 = 1$ and $e_1 = 0$, i.e., $\mathrm{AP}_1 = \{\nu\}$. The main argument in §3.3.A constructs an integer M and a rational number p/q such that the convergents[1] of p/q encode $\bigcup_{i=1}^{n} \mathrm{AP}_i$ modulo M. A nice feature of p/q is that $\lfloor p/q \rfloor = g_1$ (Remark 3.8), which combined with our choice of $g_1 = \nu$ implies that $[\mu, \nu] = [1, p/q]$. The formula in (3.9) can be rewritten equivalently as:

$$\begin{aligned} \Phi_{p,q,M}(z) \quad :=\quad & 1 \le z \le p/q \ \wedge\ \exists \mathbf{y}\ \ y_2 \equiv z \,(\mathrm{mod}\ M) \ \wedge\ \lfloor p/q \rfloor \le y_2 < p \ \wedge\ q y_2 < p y_1 \ \wedge \\ & \wedge\, \forall \mathbf{x}\, \neg \left\{ \begin{array}{c} p y_1 - q y_2 \ \ge\ p x_1 - q x_2 \ \ge\ 0 \\ y_2 \ >\ x_2 \ >\ 0 \end{array} \right\}, \end{aligned} \tag{5.5}$$

which satisfies the property:

$$\{z \in \mathbb{Z} : \Phi_{p,q,M}(z) = \mathrm{true}\} \ =\ [\mu, \nu] \ \cap\ \big(\bigcup_{i=1}^{n} \mathrm{AP}_i\big). \tag{5.6}$$

So the original AP-Cover problem is *not* satisfied if and only if $|S_{p,q,M}| = |[\mu, \nu]| = \lfloor p/q \rfloor$. We emphasize that p, q, M can be computed in polynomial time from μ, ν, g_i, h_i, e_i.

From here, a hardness result for 3-parameter PA immediately follows.

Proposition 5.13. *Assume* $\mathsf{P} \neq \mathsf{NP}$. *There exists a 3-parametric* $\exists\forall$ *PA family* $S_{p,q,M}$ *such that* $|S_{p,q,M}|$ *is always finite but cannot be expressed as a polynomial-time computable function in* p, q, *and* M.

Proof. We can clear the integer denominators in (5.5) by cross multiplications. The condition

$$y_2 \equiv z \,(\mathrm{mod}\ M)$$

can be expressed with existential quantifiers. Thus we obtain a 3-parametric $\exists\forall$ PA formula $\Phi_{p,q,M}$, which defines a family $S_{p,q,M}$. The set of satisfying values z is finite by $1 \le z \le p/q$.

[1] See Section 3.2 for basic concepts of continued fractions

Now assume $|S_{p,q,M}|$ is a polynomial-time computable function $f(p,q,M)$. Then given any AP-Cover instance, we can compute p, q, M in polynomial time from the AP_i's, and then evaluate $f(p,q,M)$ in polynomial time to check whether $f(p,q,M) = \lfloor p/q \rfloor$. This contradicts $\mathsf{P} \neq \mathsf{NP}$. □

It remains to reduce the three parameters p, q, M to two. To do this, we will adapt a trick of Glivický and Pudlák [GP17]. Their context is slightly different from ours in that they use nonstandard integers rather than parameters that range over $\mathbb{Z}$, and that their results involve computability rather than complexity. However their key idea and its proof apply in our context. The two parameters that will be involved are

$$t_1 = pM, \quad t_2 = pqM^2 + M. \tag{5.7}$$

For convenience, we will assume for the rest of this section that all the parameters in our formulas (t_1, t_2, p, q, and M) only take nonnegative integer values. Although in other parts of this chapter the parameters are assumed to range over $\mathbb{Z}$, this restriction does not affect the hardness results we are proving here.

Proposition 5.14 ([GP17] §3.2)**.** *For $0 \leq j < p$, the three multiplications $j \mapsto pMj$, $j \mapsto qMj$, $j \mapsto Mj$ can be defined by using just two multiplications $j \mapsto t_1 j$ and $j \mapsto t_2 j$.*

Proof. By definition, we have $t_1 j = pMj$ for all j, so it remains to define the multiplications by qMj and Mj for $0 \leq j < p$. By the division algorithm, for every $j \geq 0$ we can uniquely write

$$(pqM^2 + M)j = (pM)r + s, \quad \text{where} \quad 0 \leq r \ \text{ and } \ 0 \leq s < pM.$$

If $0 \leq j < p$, then $s = Mj \pmod{pM} = Mj$ and we can then solve to obtain $r = qMj$. Thus for $0 \leq j < p$, the formula

$$\mathrm{Div}_{t_1,t_2}(j,r,s) \ \coloneqq \ (t_2 j = t_1 r + s) \ \wedge \ 0 \leq r \ \wedge \ 0 \leq s < t_1$$

is satisfied by the triple (j, qMj, Mj). Furthermore, for such j this formula cannot be satisfied by any other values of the second and third arguments. □

We now prove some additional capabilities of the parameters $t_1 = pM$, $t_2 = pqM^2 + M$ that will be required in order to transform the entire formula (5.5) into a formula in t_1 and t_2 alone.

Lemma 5.15. *The congruence relation modulo M is definable using just the multiplications by t_1 and t_2.*

Proof. Consider the formula

$$\text{Cong-M}_{t_1,t_2}(b, c, w_1, w_2) \;\coloneqq\; (b - c - t_1 w_1 - t_2 w_2 = 0).$$

Since $\gcd(t_1, t_2) = M$, the condition $b \equiv c \pmod{M}$ is expressed as:

$$\exists w_1, w_2 \quad \text{Cong-M}_{t_1,t_2}(b, c, w_1, w_2).$$

□

Lemma 5.16. *The constant p is definable using just the multiplications by t_1 and t_2.*

Proof. Since $t_2/t_1 = qM + 1/p$, p is the smallest positive integer v such that $t_1 | t_2 v$. Since $t_2 p/t_1 = t_2/M = pqM + 1$, we can express that a pair of variables u, v satisfy $(u, v) = (pqM + 1, p)$ by the formula

$$\text{Equal-p}_{t_1,t_2}(v, u) \;\coloneqq\; u > 0 \;\wedge\; t_2 v = t_1 u \;\wedge\; (\forall v', u' \;\; 0 < v' < v \to t_2 v' \neq t_1 u').$$

□

Lemma 5.17. *Suppose p, q, and M are positive integers such that $p/q \notin \mathbb{Z}$. If $t_1 = pM$ and $t_2 = pqM^2 + M$ then $\lfloor t_1^2/t_2 \rfloor = \lfloor p/q \rfloor$.*

Proof. First, we have

$$t_1^2/t_2 = p^2M^2/(pqM^2 + M) = p/(q + 1/pM) < p/q,$$

so $\lfloor t_1^2/t_2 \rfloor \leq \lfloor p/q \rfloor$. On the other hand, since $p/q \notin \mathbb{Z}$ we have:

$$p \geq \lfloor p/q \rfloor q + 1 > \lfloor p/q \rfloor q + \lfloor p/q \rfloor / pM = \lfloor p/q \rfloor (q + 1/pM).$$

This means $t_1^2/t_2 = p/(q + 1/pM) > \lfloor p/q \rfloor$, and thus $\lfloor t_1^2/t_2 \rfloor = \lfloor p/q \rfloor$. □

Proof. Theorem 5.10 In order to apply Proposition 5.14, we must first multiply by M every inequality in (5.5) that involves multiplication by p or q. This works because multiplications by p, q, and M appear separately in (5.5). After doing so and clearing some denominators, we obtain the equivalent formula:

$$\begin{aligned}
\Phi'_{p,q,M}(z) &= \exists y_1, y_2 \ : \ 0 < z \leq p/q && (5.8)\\
&\quad \wedge \ y_2 \equiv z \,(\mathrm{mod}\ pM) && (5.9)\\
&\quad \wedge \ p/q < y_2 + 1 \leq p && (5.10)\\
&\quad \wedge \ qMy_2 < pMy_1 && (5.11)\\
&\quad \wedge \ \forall x_1, x_2 \ \ \neg \left\{ \begin{array}{c} pMy_1 - qMy_2 \ \geq \ pMx_1 - qMx_2 \ \geq \ 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{array} \right\}. && (5.12)
\end{aligned}$$

Here (5.10) is equivalent to $\lfloor p/q \rfloor \leq y_2 < p$ in (5.5) because $y_2 \in \mathbb{Z}$. Now consider the formula:

$$\begin{aligned}
\Psi_{t_1,t_2}(z) &= \exists y_1, y_2, w_1, w_2, u, v, r, s \ : \ 0 < t_2 z \leq t_1^2 && (5.13)\\
&\quad \wedge \ \text{Cong-M}_{t_1,t_2}(y_2, z, w_1, w_2) && (5.14)\\
&\quad \wedge \ \text{Equal-p}_{t_1,t_2}(u, v) \wedge \ t_1^2 < t_2(y_2 + 1) \leq t_2 v && (5.15)\\
&\quad \wedge \ \text{Div}_{t_1,t_2}(y_2, r, s) \wedge \ r < t_1 y_1 && (5.16)\\
\wedge \forall x_1, x_2 \ \big(0 < x_2 < y_2 \ \wedge \ \text{Div}_{t_1,t_2}(x_2, r', s')\big) &\rightarrow \neg\big(0 \leq t_1 x_1 - r' \leq t_1 y_1 - r\big). && (5.17)
\end{aligned}$$

It only remains to show that $\Phi'_{p,q,M}(z)$ and $\Psi_{t_1,t_2}(z)$ are equivalent. We have:

• (5.8) $\leftrightarrow$ (5.13) This follows by rounding down both equations to the nearest integer and applying Lemma 5.17.

• (5.9) $\leftrightarrow$ (5.14) This is Lemma 5.15.

• (5.10) $\leftrightarrow$ (5.15) We can again apply Lemma 5.17 to replace p/q in (5.10) by t_1^2/t_2, since every other quantity in 5.10 is an integer. By Lemma 5.16, the formula $\text{Equal-p}_{t_1,t_2}(v, u)$ fixes the value of v to be p, so we can now replace p by v to obtain 5.15.

• (5.10) $\rightarrow$ [(5.11) $\leftrightarrow$ (5.16)] By (5.10), we have $0 \leq y_2 < p$, so by Proposition 5.14, the condition $\text{Div}_{t_1,t_2}(y_2, r, s)$ fixes the value of r to be qMy_2. Here we modify (5.11) by replacing

qMy_2 by r and pMy_1 by t_1y_1 to obtain (5.16).

• (5.11) $\rightarrow$ [(5.12) $\leftrightarrow$ (5.17)] Using (5.16) which we have already shown to be equivalent to (5.11), we can replace qMy_2 by r. Using the definition of t_1, we can also replace pMy_1 by ty_1 and pMx_1 by t_1x_1. So (5.12) is equivalent to

$$\forall x_1, x_2 \quad \neg \left\{ \begin{array}{c} ty_1 - r \ \geq \ t_1x_1 - qMx_2 \ \geq \ 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{array} \right\},$$

or in another form

$$\forall x_1, x_2 \quad 0 < x_2 < y_2 \rightarrow \neg[ty_1 - r \ \geq \ t_1x_1 - qMx_2 \ \geq \ 0].$$

Since the hypothesis $x_2 < y_2$ along with $y_2 < p$ from (5.10) implies $x_2 < p$, we can (by Proposition 5.14) insert the condition $\mathrm{Div}_{t_1,t_2}(x_2, r', s')$ into the hypothesis to fix r' equal to qMx_2. Accordingly substituting in r' for qMx_2, we obtain (5.17).

So $\Phi_{p,q,M}, \Phi'_{p,q,M}$ and Ψ_{t_1,t_2} are all equivalent. Note that since all variables are integers, all strict inequalities can be sharpened, e.g., $x_2 < y_2$ is just $x_2 + 1 \leq y_2$. This finishes the proof of Theorem 5.10. □

Proof of corollaries 5.11 and 5.12. The formula $\Psi'_{t_1,t_2}(z) \coloneqq (0 < z \leq t_1^2/t_2) \wedge \neg\Psi_{t_1,t_2}(z)$ is satisfied only by those $z \in [\mu, \nu] \backslash \bigcup_{i=1}^{n} \mathrm{AP}_i$ (see (5.6)). This formula defines a 2-parametric family S_{t_1,t_2}. So the condition $|S_{t_1,t_2}| > 0$, which is equivalent to AP-Cover, cannot be expressed using polynomial-time relations in t_1 and t_2. Similarly, any expansion of parametric PA with polynomial-time predicates cannot have full quantifier elimination. For otherwise we can apply it to the sentence $\exists z \ \Psi'_{t_1,t_2}(z)$ and get an equivalent Boolean combination of polynomial-time relations in t_1, t_2. □

5.3. Counting-universality of 2-parametric PA

Consider a k-parametric PA formula:

$$\Phi_{\mathbf{u}}(\mathbf{x}) = Q_1y_1 \ Q_2y_2 \ \ldots Q_my_m \ \ \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y}). \tag{5.18}$$

Here $\mathbf{u} \in \mathbb{Z}^k$ are the k scalar parameters, $\mathbf{x} \in \mathbb{Z}^d$ are the free variables, $\mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{Z}^m$ are the quantified variables, $Q_1, \ldots Q_m \in \{\forall, \exists\}$ are the quantifiers, and $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$ is a Boolean combination of linear inequalities in $\mathbf{x}, \mathbf{y}$ with coefficients and constants from $\mathbb{Z}[\mathbf{u}]$. This formula defines a parametric family $S_{\mathbf{u}}$.

Definition 5.18. We say that a k_1-parametric family $S_{\mathbf{u}}$ *counting-reduces* to an k_2-parametric family $S'_{\mathbf{t}}$ if there exists $f = (f_1, \ldots, f_{k_2}) : \mathbb{Z}^{k_1} \to \mathbb{Z}^{k_2}$ with $f_i \in \mathbb{Z}[\mathbf{u}]$ such that for every $\mathbf{u} \in \mathbb{Z}^{k_1}$ we have:

$$|S_{\mathbf{u}}| = \infty \;\Rightarrow\; |S'_{f(\mathbf{u})}| = \infty \quad \text{and} \quad |S_{\mathbf{u}}| < \infty \Rightarrow |S_{\mathbf{u}}| = |S'_{f(\mathbf{u})}|.$$

Theorem 5.19. *Every k-parametric PA family $S_{\mathbf{u}}$ counting-reduces to another 2-parametric PA family $F_{s,t}$ with the same number of alternations. In other words, 2-parametric PA families are counting-universal.*

First we prove the following lemma.

Lemma 5.20. *For every formula $\Phi_{\mathbf{u}}$ of the form (5.18), there exist $\mu, \mu', \nu_1, \ldots, \nu_m \in \mathbb{Z}[\mathbf{u}]$ such that for every value $\mathbf{u} \in \mathbb{Z}^k$ we have:*

i) *$|S_{\mathbf{u}}| = \infty$ if and only if:*

$$\exists \mathbf{x} \;\left[\mu(\mathbf{u}) \le \|\mathbf{x}\|_\infty \le \mu'(\mathbf{u}) \;\wedge\; \Big(Q_1\big(|y_1| \le \nu_1(\mathbf{u})\big) \ldots Q_m\big(|y_m| \le \nu_m(\mathbf{u})\big) \;\; \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})\Big)\right]$$

ii) *If $|S_{\mathbf{u}}| < \infty$ then for every $\mathbf{x} \in \mathbb{Z}^d$:*

$$S_{\mathbf{u}}(\mathbf{x}) = \text{true} \iff \|\mathbf{x}\|_\infty \le \mu(\mathbf{u}) \wedge \Big(Q_1\big(|y_1| \le \nu_1(\mathbf{u})\big) \ldots Q_m\big(|y_m| \le \nu_m(\mathbf{u})\big) \;\; \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})\Big).$$

Here $\|\cdot\|_\infty$ is the ℓ_∞–norm. So $\mu(\mathbf{u}) \le \|\mathbf{x}\|_\infty$ stands for $\bigvee_{i=1}^d \big(x_i \le -\mu(\mathbf{u}) \;\vee\; \mu(\mathbf{u}) \le x_i\big)$ and $\|\mathbf{x}\|_\infty \le \mu'(\mathbf{u})$ stands for $\bigwedge_{i=1}^d \big(-\mu'(\mathbf{u}) \le x_i \le \mu'(\mathbf{u})\big)$. Each restricted quantifier $Q_i\big(|y_i| \le \nu_i(\mathbf{u})\big)$ means exits/for all y_i in the interval $[-\nu_i(\mathbf{u}), \nu_i(\mathbf{u})]$.[2]

[2] *Here we understand that μ, μ', ν_i have positive values for all $\mathbf{u} \in \mathbb{Z}^k$.*

Proof. Consider a usual, non-parametrized PA formula:

$$\Phi(\mathbf{x}) \;=\; Q_1 y_1 \, Q_2 y_2 \; \ldots Q_m y_m \;\; \Theta(\mathbf{x}, \mathbf{y}), \quad \mathbf{x} \in \mathbb{Z}^n,$$

which defines some set $S \subseteq \mathbb{Z}^n$. Recall Cooper's quantifier elimination procedure for Presburger Arithmetic (see [Opp78]). Applying it to $\Phi(\mathbf{x})$, we obtain an *equivalent* quantifier-free formula $\Phi'(\mathbf{x})$, which may contain some extra divisibility predicates. By Theorem 2 of [Opp78], after eliminating all m quantifiers from Φ, we obtain the following bounds:

$$c' \;\leq\; c^{4^m}, \quad s' \;\leq\; s^{(4c)^{4^m}}, \quad a' \;\leq\; a^{4^m} s^{(4c)^{4^m}},$$

where:

- c is the number of distinct integers that appeared as coefficients or divisors in Φ,
- s is the largest absolute value of all integers that appeared in Φ (coefficients + divisors + constants),
- a is the total number of atomic formulas in Φ (inequalities + divisibilities),

and c', s', a' are the corresponding quantities for Φ'. Now assume c, m and n are fixed. Then we have:

$$c' \;\leq\; \text{const}, \quad s' \;\leq\; s^{\text{const}}, \quad a' \;\leq\; a^{\text{const}} s^{\text{const}},$$

where $\text{const} = \text{const}(c, m)$ is fixed. So in this case Φ' has at most a fixed number of coefficients and divisors.

Denote by D the common multiple of all divisors in Φ'. We have $D \leq s^{\text{const}}$. Let $\mathcal{L} = \langle De_1, \ldots, De_n \rangle$ be the lattice of $\mathbb{Z}^n$ consisting of $\mathbf{x} \in \mathbb{Z}^n$ whose coordinates are all divisible by D. Fix some particular coset $\mathbf{C}$ of $\mathcal{L}$ and restrict $\mathbf{x}$ to $\mathbf{C}$. Then in $\Phi'(\mathbf{x})$, all divisor predicates have fixed values (either true or false) as $\mathbf{x}$ varies over $\mathbf{C}$. So over $\mathbf{C}$, the formula $\Phi'(\mathbf{x})$ is just a Boolean combination of linear inequalities in $\mathbf{x}$, which represents a *disjoint union* of some rational polyhedra in $\mathbb{R}^n$. Each such polyhedron P can be described by a system of *fixed* length, because there are only at most c' different coefficients for the $\mathbf{x}$

variables. The integers in the system are also bounded by s^{const}. We consider $P \cap \mathbf{C}$. By the fundamental theorem of Integer Programming[3] (see [Sch86, Th. 16.4 and Th. 7.1]), we have:

$$P \cap \mathbf{C} \;=\; \text{conv}(\overline{v}_1, \ldots, \overline{v}_p) \;+\; \mathbb{Z}_+\langle \overline{w}_1, \ldots, \overline{w}_q \rangle$$

for some $\overline{v}_i, \overline{w}_j \in \mathbb{Z}^n$ with $\|\overline{v}_i\|_\infty, \|\overline{w}_j\|_\infty < s^{\text{const}'}$. Here $\text{const}' = \text{const}'(c, m, n)$ is fixed. From this, it is easy to see that there is $\text{const}'' = \text{const}''(c, m, n)$ such that for every polyhedron P in the disjoint union, we have:

$$|P \cap \mathbf{C}| = \infty \quad \Longleftrightarrow \quad \text{there is } \mathbf{x} \in P \cap \mathbf{C} \text{ with } s^{\text{const}''} < \|\mathbf{x}\|_\infty < s^{2\text{const}''},$$
$$|P \cap \mathbf{C}| < \infty \quad \Longrightarrow \quad P \cap \mathbf{C} \subseteq [-s^{\text{const}''}, s^{\text{const}''}]^n.$$

Since this holds for every coset $\mathbf{C}$ of $\mathcal{L}$, we conclude that there is $\text{const}_0 = \text{const}_0(c, m, n)$ such that:

$$|S| = \infty \quad \Longleftrightarrow \quad \exists\, \mathbf{x} \text{ with } s^{\text{const}_0} < \|\mathbf{x}\|_\infty < s^{2\text{const}_0} \text{ and } \Phi'(\mathbf{x}) = \text{true} \tag{5.19}$$
$$|S| < \infty \quad \Longrightarrow \quad \forall\, \mathbf{x} \;\; \big(\Phi'(\mathbf{x}) = \text{true} \;\rightarrow\; \|\mathbf{x}\|_\infty \le s^{\text{const}_0}\big)\,. \tag{5.20}$$

This gives us a bound for $\mathbf{x}$. Now for every $\mathbf{x}$ with $\|\mathbf{x}\|_\infty \le s^{\text{const}_0}$, by the same argument, it is enough to decide the (substituted) sentence $\Phi(\mathbf{x})$ over those y_1 with $|y_1| \le s^{\text{const}_1}$. In other words, for every such value for $\mathbf{x}$, we may replace $Q_1 y_1$ by $Q_1\big(|y_1| \le s^{\text{const}_1}\big)$ in $\Phi(\mathbf{x})$ to obtain a new formula $\Phi_1(\mathbf{x})$, which is equivalent to the original formula $\Phi(\mathbf{x})$. Working inwards, we can likewise bound $|y_2|$ by s^{const_2}, $|y_3|$ by s^{const_3}, etc. Therefore, in case $|S| < \infty$, the whole formula Φ is equivalent to one with bounded quantifiers on all y_i. Also by (5.19), we have $|S| = \infty$ if and only if some $s^{\text{const}_0} < \|\mathbf{x}\|_\infty < s^{2\text{const}_0}$ satisfies it. For $\mathbf{x}$ in this range, we can again bound y_1, y_2, etc., accordingly by some other powers of s. Note that we can bound each y_i by a common larger power of s for both cases (5.19) and (5.20).

In a k-parametric PA formula $\Phi_{\mathbf{u}}(\mathbf{x})$, we consider m, n and c to be fixed. Since all coefficients and constants of $\Phi_{\mathbf{u}}$ are in $\mathbb{Z}[\mathbf{u}]$, we can bound s by some polynomial in $\mathbf{u}$. Thus, every s^{const} is also bounded by some polynomial in $\mathbf{u}$. This proves Lemma 5.20. □

[3]We are rescaling $\mathcal{L}$ to $\mathbb{Z}$ before applying this bound.

Remark 5.21. In the above application of Cooper's elimination, if only m, n are fixed but not c, then we no longer have the bound $s' \leq s^{\text{const}}$. Instead, we would have $c', \log s' \leq \text{poly}(c, \log s)$. A bound of this type is important for showing that the decision problem for classical PA with a bounded number of variables falls within the Polynomial Hierarchy (see e.g. [Grä87, Grä88]). However, it would not be strong enough for our argument, which crucially needs $\log s' = O(\log s)$.

From Lemma 5.20, it is easy to see that $S_{\mathbf{u}}$ counting-reduces to the family $\widetilde{S}_{\mathbf{u}}$ defined by the following formula $\widetilde{\Phi}_{\mathbf{u}}(\mathbf{x}, \widetilde{x})$:

$$\widetilde{\Phi}_{\mathbf{u}}(\mathbf{x}, \widetilde{x}) \coloneqq \Big[\widetilde{x} = 0 \wedge \Big(Q_1\big(|y_1| \leq \nu_1(\mathbf{u})\big) \ldots Q_m\big(|y_m| \leq \nu_m(\mathbf{u})\big)\ \ \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})\ \wedge\ \|\mathbf{x}\|_\infty \leq \mu(\mathbf{u})\Big)\Big]$$
$$\vee\ \Big[\widetilde{x} \geq 0 \wedge \Big(Q_1\big(|y_1| \leq \nu_1(\mathbf{u})\big) \ldots Q_m\big(|y_m| \leq \nu_m(\mathbf{u})\big)\ \ \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})\ \wedge\ \mu(\mathbf{u}) \leq \|\mathbf{x}\|_\infty \leq \mu'(\mathbf{u})\Big)\Big].$$

Here the bounds on $\|\mathbf{x}\|_\infty$ can be placed after the quantifiers Q_i without affecting the meaning. The dummy variable $\widetilde{x}$ is used to make sure that $|\widetilde{S}_{\mathbf{u}}| = \infty$ in the second case.

Proof of Theorem 5.19. We show that $\widetilde{S}_{\mathbf{u}}$ counting-reduces to a 2-parameter family $F_{s,t}$, defined by a new formula $\Psi_{s,t}$. First, we list all the different scalar terms that appear in $\widetilde{\Phi}_{\mathbf{u}}$, either as coefficients or constants (including all μ, μ', ν_i) as $\delta_0(\mathbf{u}), \ldots, \delta_r(\mathbf{u})$. Now suppose we need to multiply some $z \in \mathbb{N}$ by $\delta_0(\mathbf{u}), \ldots, \delta_r(\mathbf{u})$ and also know that

$$-t/2 < \delta_0(\mathbf{u})\, z,\ \ldots,\ \delta_r(\mathbf{u})\, z < t/2 \tag{5.21}$$

for some $t \in \mathbb{Z}$. The following base-t concatenation, which is similar to (5.7), can be used. Essentially, we encode the "multi"-product $(\delta_0(\mathbf{u})\, z, \ldots, \delta_r(\mathbf{u})\, z)$ as a single product:

$$\delta_0(\mathbf{u})\, z\ +\ t\, \delta_1(\mathbf{u})\, z\ +\ \ldots\ + t^r\, \delta_r(\mathbf{u})\, z\ =\ (\delta_0(\mathbf{u}) + t\, \delta_1(\mathbf{u}) + \cdots + t^r \delta_r(\mathbf{u}))\, z.$$

In other words, if $s = \delta_0(\mathbf{u}) + t\, \delta_1(\mathbf{u}) + \cdots + t^r \delta_r(\mathbf{u})$ and the formula

$$\text{Div}_{s,t}(z, z_0, \ldots, z_r)\ \coloneqq\ (sz = z_0 + t\, z_1 + \cdots + t^r z_r)\ \wedge\ (t/2 < z_0, \ldots, z_r < -t/2)$$

is true, then we must have $z_0 = \delta_0(\mathbf{u})\, z,\ \ldots,\ z_r = \delta_r(\mathbf{u})\, z$. Indeed, by subtracting we have $z_0 - \delta_0(\mathbf{u})\, z \equiv 0 \,(\text{mod } t)$, so $z_0 = \delta_0(\mathbf{u})\, z$ because $-t/2 < z_0,\ \delta_0(\mathbf{u})\, z < t/2$. The same argument applies to other z_i.

Observe that in $\widetilde{\Phi}_{\mathbf{u}}$, all variables $\mathbf{x}$ and $\mathbf{y}$ are bounded by polynomials in $\mathbf{u}$. Hence, we can pick $\eta(\mathbf{u}) \in \mathbb{Z}[\mathbf{u}]$ so that for every value $\mathbf{u} \in \mathbb{Z}^k$, the condition (5.21) is always satisfied when $t = \eta(\mathbf{u})$ and z is either the constant 1 or any of the possible values of the $\mathbf{x}, \mathbf{y}$ variables. Our reduction map $f : \mathbb{Z}^k \to \mathbb{Z}^2$ can now be defined by letting

$$t = \eta(\mathbf{u}); \quad s = \delta_0(\mathbf{u}) + t\,\delta_1(\mathbf{u}) + \cdots + t^r \delta_r(\mathbf{u}).$$

Now we can define $\Psi_{s,t}(\mathbf{x}, \widetilde{x})$ from $\widetilde{\Phi}_{\mathbf{u}}(\mathbf{x}, \widetilde{x})$ using $(m + d + 1)(r + 1)$ extra variables:

$$\mathbf{w} = (w_{ij})_{1 \le i \le d,\, 0 \le j \le r},\ \mathbf{w}' = (w'_{ij})_{1 \le i \le m,\, 0 \le j \le r} \quad \text{and} \quad \mathbf{v} = (v_j)_{0 \le j \le r}.$$

Assuming the last quantifier Q_m in $\widetilde{\Phi}_{\mathbf{u}}$ is $\exists$, we insert

$$\begin{aligned} \exists\, \mathbf{w}, \mathbf{w}', \mathbf{v}\ \ \mathrm{Div}_{s,t}(1, v_0, \ldots, v_r)\ \wedge \bigwedge_{i=1}^{d} \mathrm{Div}_{s,t}(x_i, w_{i0}, \ldots, w_{ir}) \\ \wedge \bigwedge_{i=1}^{m} \mathrm{Div}_{s,t}(y_i, w'_{i0}, \ldots, w'_{ir}) \end{aligned} \tag{$\star$}$$

right before $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$, i.e., replace $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$ by $(\star) \wedge \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$. Then in $\widetilde{\Phi}_{\mathbf{u}}$ we replace every term $\delta_j(\mathbf{u})\, x_i$ by w_{ij}, every term $\delta_j(\mathbf{u}) y_i$ by w'_{ij} and every term $\delta_j(\mathbf{u})$ by v_j. Now $\widetilde{\Phi}_{\mathbf{u}}$ becomes the desired $\Psi_{s,t}$. In case $Q_m = \forall$, we insert:

$$\begin{aligned} \forall\, \mathbf{w}, \mathbf{w}', \mathbf{v}\ \ \neg\mathrm{Div}_{s,t}(1, v_0, \ldots, v_r)\ \vee \bigvee_{i=1}^{d} \neg\mathrm{Div}_{s,t}(x_i, w_{i0}, \ldots, w_{ir}) \\ \vee \bigvee_{i=1}^{m} \neg\mathrm{Div}_{s,t}(y_i, w'_{i0}, \ldots, w'_{ir}) \end{aligned} \tag{$\star\star$}$$

right before $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$, i.e., replace $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$ by $(\star\star) \vee \Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$. Again, replace every term $\delta_j(\mathbf{u})\, x_i$ by w_{ij}, every term $\delta_j(\mathbf{u}) y_i$ by w'_{ij} and every term $\delta_j(\mathbf{u})$ by v_j. This gives $\Psi_{s,t}$.

Note that $\Psi_{s,t}$ still has the disjunctive form $\big[\ldots\big] \vee \big[\ldots\big]$ with each disjunct containing m alternations $Q_1 \ldots Q_m$. This formula is equivalent to a formula in prenex normal form with m quantifier alternations, so we are done. □

Remark 5.22. In case $S_{\mathbf{u}}$ is defined by a quantifier-free formula, i.e., $m = 0$, we only need to insert $(\star)$, without the $\exists$ quantifiers, before $\Theta_{\mathbf{u}}(\mathbf{x}, \mathbf{y})$. This is because $\mathrm{Div}_{s,t}(z, z_0, \ldots, z_r)$

uniquely determines $z_0, \ldots, z_r$ in z. So in this case $S_{\mathbf{u}}$ also counting-reduces to a quantifier-free $F_{s,t}$, although the latter has many more free variables. Thus, the study of integer point counting functions on k-parametric polyhedra reduces to the case of 2-parametric polyhedra in higher dimensions.

5.4. Counting in parametric unordered PA

In this section, we consider the reduct of multi-parametric Presburger Arithmetic to the language without ordering, so that basic quantifier-free formulas are equivalent to Boolean combinations of equations of the form $f_1(\mathbf{t})x_1 + \ldots + f_n(\mathbf{t}) = g(\mathbf{t})$, where $\mathbf{t} = (t_1, \ldots, t_k)$ is a tuple of parameters and $f_1, \ldots, f_m, g \in \mathbb{Z}[\mathbf{t}]$. As always, we are allowed to quantify over the variables x_i but not over the parameters $\mathbf{t}$. Note that if there is no parameter $\mathbf{t}$, this would correspond to studying the first-order logic of the additive group $(\mathbb{Z}; +)$. More precisely:

Definition 5.23. A *k-parametric unordered PA family* is a collection

$$\{S_{\mathbf{t}} : \mathbf{t} = (t_1, \ldots, t_k) \in \mathbb{Z}^k\}$$

of subsets of $\mathbb{Z}^d$ which can be defined by an equation of the form

$$S_{\mathbf{t}} = \{\mathbf{x} \in \mathbb{Z}^d \ : \ Q_1 y_1 \, Q_2 y_2 \, \ldots Q_m y_m \ \Theta_{\mathbf{t}}(\mathbf{x}, \mathbf{y})\},$$

where the $Q_i \in \{\forall, \exists\}$ are quantifiers for variables y_i ranging over $\mathbb{Z}$ and $\Theta_{\mathbf{t}}(\mathbf{x}, \mathbf{y})$ is a Boolean combination of linear equations with coefficients in $\mathbb{Z}[\mathbf{t}]$.

For example,

$$x_1 = 0 \ \wedge \ \exists y_1, y_2 \ (y_1 t_1 + y_2 t_2 = 1)$$

defines a 2-parametric unordered PA family $\{S_{\mathbf{t}} \subseteq \mathbb{Z} : \mathbf{t} \in \mathbb{Z}^2\}$ such that $S_{\mathbf{t}} = \{0\}$ if $\gcd(t_1, t_2) = 1$ and $S_{\mathbf{t}} = \varnothing$ otherwise.

Theorem 5.24. *Suppose that $S_{\mathbf{t}} \subseteq \mathbb{Z}^d$ is a k-parametric unordered PA family. Then:*

(1) *There is a polynomial-time algorithm to decide whether $S_{\mathbf{t}}$ is nonempty.*

(2) *There is a polynomial-time algorithm on input* $\mathbf{t}$ *which decides whether or not* $S_{\mathbf{t}}$ *is finite or infinite.*

(3) *There is a polynomial-time computable function* $g : \mathbb{Z}^k \to \mathbb{N}$ *such that whenever* $S_{\mathbf{t}}$ *is finite,* $g(\mathbf{t}) = |S_{\mathbf{t}}|$.

In fact, the proof of Theorem 5.24 will show that the decision algorithms for (1) and (2) rely upon only a few basic, concrete number-theoretic operations on $\mathbf{t}$, such as gcd and a couple of related functions.

To prove Theorem 5.24, we need to recall some notation from [vdDH92]. To eliminate quantifiers, they work in a two-sorted language L_2 in which variables x_i and parameters in $\mathbf{t}$ are assigned to objects of distinct domains, called the *group sort* and the *ring sort*, respectively. **For our purposes, the group sort and the ring sort are two disjoint copies of $\mathbb{Z}$.** The variables x_i and y_i will always range over values in the group sort, and the parameters t_i will always range over values in the scalar sort. In other words, we can think of the parameters $t_1, \ldots, t_k$ as "typed variables" ranging over a domain of possible parameter values in the scalar sort (a copy of $\mathbb{Z}$), and $x_1, x_2, \ldots$ as variables of a distinct type ranging over values in the group sort (which is a different copy of $\mathbb{Z}$), and the parameters t_i act upon the group sort by scalar multiplication.

The language L_2 consists of the following nonlogical symbols (in addition to equality):

- Within the scalar sort, constant symbols for 0 and 1, a unary operation $-$ for negation, ring operations $+$ and $\cdot$, and four additional binary operations g, α, β, and γ (whose interpretation is explained below);
- Within the group sort, a constant symbol for 0, a unary operation $-$ for negation, and a symbol $+$ for addition;
- A binary operation $\cdot$ such that $s \cdot x$ is a value in the group sort whenever s is a value in the scalar sort and x is a value in the group sort, denoting multiplication by s in the usual sense; and

- A binary relation symbol $|$ to be interpreted such that whenever s is in the scalar sort and x is in the group sort,

$$s|x \iff \exists y\,(s \cdot y = x)\,.$$

The binary operations g, α, β, and γ between values in the scalar sort are interpreted so that $g(r,s) = gcd(r,s)$ and the following axioms hold for all values r, s in the scalar sort:

$$r = \gamma(r,s) \cdot g(r,s),$$

$$1 = \alpha(r,s) \cdot \gamma(r,s) + \beta(r,s) \cdot \gamma(s,r).$$

For distinction, we will denote the variable tuple by $\overline{x}$, and the parameter tuple by $\mathbf{t}$. We will use the following fact, proved in [vdDH92]:

Theorem 5.25. *Any formula $\varphi_{\mathbf{t}}(\mathbf{x})$ in k-parametric unordered Presburger Arithmetic is logically equivalent to a quantifier-free L_2-formula $\psi(\overline{x}, \mathbf{t})$: that is, with the natural interpretations of the symbols from L_2 given above, then we have*

$$\varphi_{\mathbf{t}}(\overline{x}) \leftrightarrow \psi(\overline{x}, \mathbf{t}) \quad \textit{for every} \quad \overline{x} \in \mathbb{Z}^d \quad \textit{and} \quad \mathbf{t} \in \mathbb{Z}^k,$$

where $\psi(\overline{x}, \mathbf{t})$ is a Boolean combination of equations $s_1(\overline{x}, \mathbf{t}) = s_2(\overline{x}, \mathbf{t})$ and divisibility relations $s_3(\mathbf{t})|s_1(\overline{x}, \mathbf{t})$, where $s_1(\overline{x}, \mathbf{t})$, $s_2(\overline{x}, \mathbf{t})$, and $s_3(\mathbf{t})$ are L_2-terms, i.e. expressions built up using only the operations in L_2 and the displayed parameters and variables.

Proof of Theorem 5.24: Say $\varphi_{\mathbf{t}}(\overline{x})$ defines a k-parametric unordered PA family in $\mathbb{Z}^d$.

Note that (1) follows almost immediately from quantifier elimination: by Theorem 5.25, the formula $\exists \overline{x}\, \varphi_t(\overline{x})$ is equivalent to a quantifier-free L_2-formula $\psi(\mathbf{t})$ in only the scalar sort of $\mathbf{t}$, which is a Boolean combination of equations and divisibility relations $|$ in the k parameters using ring operations and the functions g, α, β, and γ, but all of these operations are polynomial-time computable.

For (2), let us assume (by Theorem 5.25) that $\varphi_{\mathbf{t}}(\overline{x})$ is a quantifier-free L_2-formula, and that $\varphi_t(\overline{x})$ is in disjunctive normal form:

$$\varphi_t(\overline{x}) = \bigvee_{i=1}^{m} \theta_i(\overline{x}, \mathbf{t}),$$

where each $\theta_i(\overline{x}, \mathbf{t})$ is a conjunction of *literals*.[4]

Claim 5.26. For any fixed value of $\mathbf{t} \in \mathbb{Z}^k$ and $1 \leq i \leq m$, if $S_i := \{\overline{x} \in \mathbb{Z}^d : \theta_i(\overline{x}, \mathbf{t}) = \text{true}\}$, then $|S_i|$ is either 0, 1, or ∞.

Proof of claim. By rearranging terms, we may assume that all atomic L_2-formulas in $\theta_i(\overline{x}, \mathbf{t})$ have the form

$$\text{(A)} \quad r \mid s(\overline{x}, \mathbf{t}) \qquad \text{or} \qquad \text{(B)} \quad s(\overline{x}, \mathbf{t}) = 0.$$

where $s(\overline{x}, \mathbf{t}) = r_0 + \sum_{i=1}^{d} r_i \cdot x_i$ and $r_0, r_1, \ldots, r_n$, and r are terms in the scalar sort. The terms r and r_i may involve the parameters $\mathbf{t}$ and the operations g, α, β, γ, but the details of this are irrelevant since $\mathbf{t}$ has a fixed value.

Write

$$\theta_i(\overline{x}, \mathbf{t}) = \theta_A(\overline{x}, \mathbf{t}) \ \wedge \ \theta_B(\overline{x}, \mathbf{t})$$

where $\theta_A(\overline{x}, \mathbf{t})$ is the conjunctions of all literals of type (A) and $\theta_B(\overline{x}, \mathbf{t})$ is the conjunction of all literals of type (B).

First we consider the atomic formulas of type (A). Each one defines some coset of a finite-index subgroup of $\mathbb{Z}^d$, and so the negation of such a formula defines a finite union of cosets of finite-index subgroups. Since the intersection of finitely many finite-index subgroups is of finite index, there is a single subgroup $H \leq \mathbb{Z}^d$ such that $[\mathbb{Z}^d : H] < \infty$ and $\theta_A(\overline{x}, \mathbf{t})$ defines a Boolean combination of cosets of H.

Now consider the atomic formulas of type (B). We decompose $\theta_B(\overline{x}, \mathbf{t})$ further as

$$\theta_B(\overline{x}, \mathbf{t}) \ = \ \theta_B^+(\overline{x}, \mathbf{t}) \ \wedge \ \theta_B^-(\overline{x}, \mathbf{t})$$

where $\theta_B^+(\overline{x}, \mathbf{t})$ is the conjunction of all positive (non-negated) atomic formulas of type (B) and $\theta_B^-(\overline{x}, \mathbf{t})$ is the conjunction of all negative literals of type (B). Note that the set of solutions to $\theta_B^+(\overline{x}, \mathbf{t})$ is of the form $(\vec{v} + S) \cap \mathbb{Z}^d$ where S is a vector subspace of $\mathbb{R}^d$ and $\vec{v} \in \mathbb{Z}^d$.

[4] A literal is an *atomic* L_2-formula, i.e. one containing no logical operations $\wedge$, $\vee$ or $\neg$, or the negation of an atomic formula.

Finally, suppose that there are at least two distinct elements $\overline{x}_1, \overline{x}_2 \in \mathbb{Z}^d$ in S_i, and to finish the proof of the Claim we will show that S_i has infinitely many elements. In particular, both $\overline{x}_1$ and $\overline{x}_2$ are solutions to $\theta_A(\overline{x}, \mathbf{t})$, so there are cosets C_1, C_2 of H such that $\overline{x}_1 \in C_1$, $\overline{x}_2 \in C_2$, and any element $\overline{x} \in C_1 \cup C_2$ satisfies $\theta_A(\overline{x}, \mathbf{t})$. Let $L \subseteq \mathbb{R}^d$ be the line passing through $\overline{x}_1$ and $\overline{x}_2$, and observe that since $\overline{x}_1$ and $\overline{x}_2$ satisfy $\theta_B^+(\overline{x}, \mathbf{t})$ (which defines the intersection of an affine subspace with $\mathbb{Z}^d$), any other element of $L \cap \mathbb{Z}^d$ will also satisfy $\theta_B^+(\overline{x}, \mathbf{t})$.

For any $j \in \mathbb{Z}$, let $\overline{x}(j) := \overline{x}_1 + j \cdot (\overline{x}_2 - \overline{x}_1)$ and

$$X := \{j \in \mathbb{Z} : \overline{x}(j) \text{ satisfies } \theta_i(\overline{x}, \mathbf{t})\}.$$

Since H is a finite-index subgroup of $\mathbb{Z}^d$, adding successive copies of the element $(\overline{x}_2 - \overline{x}_1)$ to $\overline{x}_1$ causes the $\overline{x}(j)$ to cycle through cosets of H, and the set of j for which $\theta_A(\overline{x}(j), \mathbf{t})$ is true is infinite (and periodic). As observed in the previous paragraph, *every* $\overline{x}(j)$ lies on the line L, and hence $\theta_B^+(\overline{x}(j), \mathbf{t})$ is always true, and we need only worry about the truth of $\theta_B^-(\overline{x}(j), \mathbf{t})$. Now $\theta_B^-(\overline{x}(j), \mathbf{t})$ is true whenever $\overline{x}(j)$ *avoids* every one of a finite number of affine subspaces $A_1, \ldots, A_\ell$ of $\mathbb{R}^d$, but given that L is a line which contains some points satisfying the formula $\theta_B^-(\overline{x}, \mathbf{t})$, each A_i can only intersect L in at most one point. Therefore X is infinite, as we wanted. □

The Claim shows that we can define the set of values of the parameter $\mathbf{t}$ for which any given $\theta_i(\overline{x}, \mathbf{t})$ has infinitely many solutions (for $\overline{x}$) by the formula

$$\exists \overline{x}_1, \overline{x}_2 \left(\overline{x}_1 \neq \overline{x}_2 \ \wedge \ \theta_i(\overline{x}_1, \mathbf{t}) \ \wedge \ \theta_i(\overline{x}_2, \mathbf{t}) \right),$$

and as before this is equivalent to a quantifier-free L_2-formula $\psi_i(\mathbf{t})$ whose truth can be decided by a polynomial-time algorithm in $\mathbf{t}$. Finally, our original formula $\bigvee_{i=1}^m \theta_i(\overline{x}, \mathbf{t})$ has infinitely many solutions just in case any one of the formulas $\theta_i(\overline{x}, \mathbf{t})$ does, establishing (2).

By the argument above, for any k-parametric unordered PA family $S_{\mathbf{t}}$, there is a finite partition $\mathbb{Z}^k = X_1 \cup \ldots \cup X_\ell$ which is definable by quantifier-free L_2-formulas in $\mathbf{t}$ and such that $|S_{\mathbf{t}}|$ is constant as $\mathbf{t}$ varies over any of the sets X_i. Since deciding whether $\mathbf{t} \in X_i$ is polynomial-time decidable, this establishes (3). □

5.5. Summary of complexity results

To conclude, we summarize the complexity results which suggest that Theorem 5.10 may be the best we could hope for: weakening or changing various assumptions results in problems which can be resolved in polynomial time, or else (with unrestricted multiplication) have no algorithmic solutions at all.

Recall that Theorem 5.10 states that, if $\mathsf{P} \neq \mathsf{NP}$, then there is a $\exists\forall$ parametric PA family $S_{\mathbf{t}}$ with two parameters $\mathbf{t} = (t_1, t_2)$ such that $|S_{\mathbf{t}}|$ cannot be computed in polynomial time given $\mathbf{t}$ as input.

However:

• If we allow only a single parameter $t \in \mathbb{N}$ (or $\mathbf{t} \in \mathbb{Z}$), then for any PA family S_t, we can compute $|S_t|$ in polynomial, by Corollary 5.9.

• If $S_{\mathbf{t}}$ is a k-parametric PA family defined by an $\exists$ or $\forall$ formula, then Theorem 1.8 implies that there is a polynomial time algorithm to evaluate $|S_{\mathbf{t}}|$, for any finite number k of parameters. If $S_{\mathbf{t}}$ is defined by a quantifier-free formula, then a polynomial-time algorithm was earlier given in Theorem 2.4.

• If $S_{\mathbf{t}}$ is any k-parametric PA family defined by a formula with no inequalities (only equations), as in Section 5.4, then $|S_{\mathbf{t}}|$ can be evaluated in polynomial time, regardless of the number of quantifier alternations in the defining formula or the number of parameters.

• In k-parametric PA formulas, we allow a restricted version of multiplication: the non-quantified parameters in $\mathbf{t}$ can be multiplied by terms containing the variables $\mathbf{x}$ and $\mathbf{y}$, but no multiplication between the $\mathbf{x}$ and $\mathbf{y}$ variables is allowed. Permitting unrestricted multiplication amongst the $\mathbf{x}$ and $\mathbf{y}$ variables in a parametric PA formula would obviously be bad, since the full first-order theory of $(\mathbb{N}, +, \cdot)$ is undecidable (by theorems of Church and Turing – see, e.g., [Chu36]). In fact, the Matiyasevich-Robinson-Davis-Putnam theorem [Dav73] states that there is a *single* multivariate polynomial $p(t, x_1, \ldots, x_d)$ such that if

$\Phi_t(x_1, \ldots, x_d)$ is the formula expressing

$$p(t, x_1, \ldots, x_d) = 0,$$

then the set of $t \in \mathbb{N}$ for which $\Phi_t(x_1, \ldots, x_d)$ defines a nonempty subset of $\mathbb{Z}^d$ is not computable (much less in polynomial time). Note that here we have only a single parameter t, no quantifiers in the formula Φ_t, and mere equations rather than inequalities.

• On the other hand, if we allow *no multiplication*, even by parameters (cf. Example 5.4), then $|S_{\mathbf{t}}|$ will be computable in polynomial time; in fact, it has a nice form as a piecewise-defined quasi-polynomial [Woo15].

Part II

Short generating functions

CHAPTER 6

A strengthening of the Barvinok–Woods theorem

We extend the *Barvinok–Woods algorithm* for enumeration of integer points in projections of polytopes to unbounded polyhedra. For this, we obtain a new structural result on projections of *semilinear subsets* of the integer lattice. We extend the results to general formulas in *Presburger Arithmetic*. We also give an application to the *k-feasibility problem*. This chapter is a version of the published paper [NP17f].

6.1. Introduction

6.1.A. Statements of results. Barvinok famously showed in [Bar93] that the number of integer points in a possibly unbounded polyhedron of a fixed dimension n can be computed in polynomial time:

Theorem 6.1 (Th. 2.4 restated)**.** *Let $n \in \mathbb{N}$ be fixed. Given a (possibly unbounded) rational polyhedron $P = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \le \overline{b}\}$, there is a polynomial time algorithm to write:*

$$\sum_{\mathbf{x}\in P\cap\mathbb{Z}^n} \mathbf{t}^{\mathbf{x}} \;=\; \sum_{i=1}^{M} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1-\mathbf{t}^{\overline{b}_{i1}})\,\ldots\,(1-\mathbf{t}^{\overline{b}_{in}})}, \tag{$\divideontimes$}$$

where $c_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$, $\overline{b}_{ij} \neq 0$ for all i and j. Furthermore, the total binary length of all c_i, $\overline{a}_i$ and $\overline{b}_{ij}$ in the RHS is polynomial in the input length of A and $\overline{b}$.

The RHS expression in ($\divideontimes$) called a *short generating function* (short GF), which fully enumerates the integer points in P. By taking limit $\mathbf{t} \to 1$ in ($\divideontimes$), one can count the number of integer points P if it's finite, or conclude that $|P \cap \mathbb{Z}^n| = \infty$. Hence, it also implies

Lenstra's result on Integer Programming (Theorem 1.4).[1]

Barvinok's algorithm was extended to count projections of integer points in polytopes by Barvinok and Woods [BW03] (Theorem 6.14). This theorem in turns implies Kannan's result on Parametric Integer Programming (2.1). Even though this result has found many other applications, there is a major technical drawback: on the enumeration level, it only applies to *polytopes*, i.e., bounded polyhedra. The main result of this chapter is an extension of the Barvinok–Woods algorithm to the unbounded case:

Theorem 6.2. *Let $m, n \in \mathbb{N}$ be fixed dimensions. Given a (possibly unbounded) polyhedron $Q = \{\mathbf{x} \in \mathbb{R}^m : A\mathbf{x} \leq \overline{b}\}$ and an integer linear transformation $T : \mathbb{R}^m \to \mathbb{R}^n$ which satisfies $T(Q) \subseteq \mathbb{R}^n_+$, let $g(\mathbf{t})$ be the generating function for $T(Q \cap \mathbb{Z}^m)$, i.e.,*

$$g(\mathbf{t}) \,=\, \sum_{\mathbf{y} \,\in\, T(Q \cap \mathbb{Z}^m)} \mathbf{t}^{\mathbf{y}}\,.$$

Then there is a polynomial time algorithm to compute $g(\mathbf{t})$ in the form of a short GF ($\divideontimes$).

Here by an integer linear transformation we mean that the linear map T is presented by a matrix $T \in \mathbb{Z}^{n \times m}$. To illustrate our theorem, consider:

Example 6.3. Let $Q = \{(x, y, z) \in \mathbb{R}^3_+ : x = 2y + 5z\}$ and T be the projection from $\mathbb{Z}^3$ onto the first coordinate $\mathbb{Z}^1$. Then $T(Q \cap \mathbb{Z}^3)$ has a short GF:

$$\frac{1}{(1-t^2)(1-t^5)} - \frac{t^{10}}{(1-t^2)(1-t^5)} = 1 + t^2 + t^4 + t^5 + t^7 + \ldots$$

To prove Theorem 6.2, our main tool is a structural result describing projections of *semilinear sets*, i.e., sets definable by formulas in Presburger Arithmetic. Geometrically, such a set is always a disjoint union of intersections of polyhedra and lattice cosets (see Definition 6.6). We first prove that the image of a semilinear set under a linear transformation is also semilinear, and give bound on the complexity of the projection (Theorem 6.8). This is done purely by geometric arguments, without resorting to classical results on quantifier elimination for Presburger Arithmetic. Combined with the Barvinok–Woods theorem, this

[1] Though the run-time cost of Lenstra's algorithm is lower.

gives the extension to unbounded polyhedra (Theorem 6.2). Our geometric argument can in fact be generalized to arbitrary formulas in Presburger Arithmetic (Theorem 6.17 and 6.19). We illustrate the power of our generalizations in the case of the *k-feasibility problem* (Section 6.5).

6.1.B. Connections and applications. After Lenstra's algorithm (Theorem 1.4), many other methods for fast Integer Programming in fixed dimensions have been found (see [Eis03, FT87]). Kannan's algorithm (Theorem 2.1) for Parametric Integer Programming was also strengthened in [ES08]. Barvinok's algorithm (Theorem 6.1) has been simplified and improved in [DK97, KV08]. Both this and Barvinok–Woods' algorithm (Theorem 6.14) have been implemented and used for practical computation [DHTY04, Köp07, V+07].

Let us emphasize two main reasons to study unbounded polyhedra:

(1) Working with short GFs of integer points in unbounded polyhedra allows to compute to various integral sums and valuations over convex polyhedra. We refer to [B+12, Bar08, BV07] for many examples and further references.

(2) In the context of Parametric Integer Programming (2.1), the higher dimensional polyhedron $Q = \{(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{R}^{n_1+n_2} : A\mathbf{x}_1 + B\mathbf{x}_2 \leq \overline{v}\}$ could be unbounded. One would like to count the projections of points in $Q \cap \mathbb{Z}^{n_1+n_2}$ which fall within a lower dimensional polytope $P \subset \mathbb{R}^{n_1}$. To apply the Barvinok–Woods algorithm, one needs to intersect Q with a big enough box $B \subset \mathbb{R}^{n_1+n_2}$, and then project it. When P varies, the Barvinok–Woods algorithm needs to be called multiple times for different boxes, depending on the size of P. Our approach allows one to call the Barvinok–Woods algorithm only once to project the entire set $Q \cap \mathbb{Z}^{n_1+n_2}$ (unbounded), and then call a more economical algorithm to compute its intersection with P. See Section 6.5 for an explicit example.

In conclusion, let us mention that semilinear sets are well studied subjects in both computer science and logic. The fact that the category of semilinear sets are closed under taking projections is not new. Ginsburg and Spanier [GS64] showed that semilinear sets are exactly those sets definable in Presburger Arithmetic, which are closed under Boolean operations

and projections. Woods [Woo15] also characterized semilinear sets as exactly those sets with rational generating functions, which also implies closedness under Boolean operations and projections. In this chapter, we prove the structural result on projections of semilinear sets by a direct argument, without using tools from logic (e.g. quantifier elimination). By doing so, we obtain effective polynomial bounds for the number of polyhedral pieces and the facet complexity of each piece in the projection.

6.2. Structure of a projection

6.2.A. Semilinear sets and their projections. In this section, we assume all dimensions m, n, etc., are fixed. We emphasize that all lattices mentioned are of full rank. All inputs are in binary.

Definition 6.4. Given a set $X \subseteq \mathbb{R}^{n+1}$, the *projection* of X onto $\mathbb{R}^n$, denoted by $\operatorname{proj}(X)$, is defined as

$$\operatorname{proj}(X) \coloneqq \{(x_2, \dots, x_n) : (x_1, x_2, \dots, x_{n+1}) \in X\} \subseteq \mathbb{R}^n.$$

For any $\mathbf{y} \in \operatorname{proj}(X)$, denote by $\operatorname{proj}^{-1}(\mathbf{y}) \subseteq X$ the preimage of $\mathbf{y}$ in X.

Definition 6.5. Let $\mathcal{L} \subseteq \mathbb{Z}^n$ be a full-rank lattice. A *pattern* $\boldsymbol{L}$ *with period* $\mathcal{L}$ is a union of finitely many (integer) cosets of $\mathcal{L}$. For any other lattice $\mathcal{L}'$, if $\boldsymbol{L}$ can be expressed as a finite union of cosets of $\mathcal{L}'$, then we also call $\mathcal{L}'$ a period of $\boldsymbol{L}$.

Given a rational polyhedron Q and a pattern $\boldsymbol{L}$, the set $Q \cap \boldsymbol{L}$ is called a *patterned polyhedron*. When the pattern $\boldsymbol{L}$ is not emphasized, we simply call Q a *patterned polyhedron with period* $\mathcal{L}$.

Definition 6.6. A *semilinear* set X is a set of the form

$$X = \bigsqcup_{i=1}^{k} Q_i \cap \boldsymbol{L}_i\,, \tag{6.1}$$

where each $Q_i \cap \boldsymbol{L}_i$ is a patterned polyhedron with period $\mathcal{L}_i$, and the polyhedra Q_i are

pairwise disjoint. The *period length* $\psi(X)$ of X is defined as

$$\psi(X) = \sum_{i=1}^{k} \ell(Q_i) + \ell(\mathcal{L}_i).$$

Note that $\psi(X)$ does not depend on the number of cosets in each $\boldsymbol{L}_i$. Define

$$\eta(X) \coloneqq \sum_{i=1}^{k} \eta(Q_i),$$

where each $\eta(Q_i)$ is the number of facets of the polyhedron Q_i.

Remark 6.7. In Theoretical CS literature, semilinear sets are often explicitly presented as a finite union of *linear sets*. Each linear set is a translated semigroup generated by a finite set of vectors in $\mathbb{Z}^n$. This explicit representation by generators makes operations like projections easy to compute, while structural properties harder to establish (see e.g. [CH16] and the references therein). The equivalence of the two representations is proved in [GS64].

Our main structural result is the following theorem.

Theorem 6.8. *Let $m \in \mathbb{N}$ be fixed. Let $X \subseteq \mathbb{Z}^m$ be a semilinear set of the form* (6.1)*. Let $T : \mathbb{R}^m \to \mathbb{R}^n$ be a linear map satisfying $T(\mathbb{Z}^m) \subseteq \mathbb{Z}^n$. Then $T(X)$ is also a semilinear set, and there exists a decomposition*

$$T(X) \;=\; \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j\,, \tag{6.2}$$

where each $R_j \cap \boldsymbol{T}_j$ is a patterned polyhedron in $\mathbb{R}^n$ with period $\mathcal{T}_j \subseteq \mathbb{Z}^n$. The polyhedra R_j and lattices $\mathcal{T}_j$ can be found in time $\mathrm{poly}(\psi(X))$*. Moreover,*

$$r = \eta(X)^{O(m!)} \quad \textit{and} \quad \eta(R_j) = \eta(X)^{O(m!)},\ 1 \le j \le r.$$

Remark 6.9. The above result describes all pieces R_j and periods $\mathcal{T}_j$ in polynomial time. However, it does not explicitly describe the patterns $\boldsymbol{T}_j$. The latter is actually an NP-hard problem (see Remark 6.20).

Remark 6.10. In the special case when X is just one polyhedron $Q \cap \mathbb{Z}^m$, the first piece $R_1 \cap \boldsymbol{T}_1$ in (6.2) has a simple structure. Theorem 1.7 in [AOW14] identifies and describes

$R_1 \cap \boldsymbol{T}_1$ as $R_1 = T(Q)_\gamma$ and $\boldsymbol{T}_1 = T(\mathbb{Z}^m)$. Here $T(Q)_\gamma$ is the γ-*inscribed* polyhedron inside $T(Q)$ (see [AOW14, Def. 1.6]). However, their result does not characterize the remaining pieces $R_j \cap \boldsymbol{T}_j$ in the projection $T(X)$. Thus, Theorem 6.8 can also be seen as a generalization of the result in [AOW14] to semilinear sets, with a complete description of the projection.

For the proof of Theorem 6.8, we need a technical lemma:

Lemma 6.11. *Let $n \in \mathbb{N}$ be fixed. Consider a patterned polyhedron $(Q \cap \boldsymbol{L}) \subseteq \mathbb{R}^{n+1}$ with period $\mathcal{L}$. There exists a decomposition*

$$\operatorname{proj}(Q \cap \boldsymbol{L}) = \bigsqcup_{j=0}^{r} R_j \cap \boldsymbol{T}_j \,, \tag{6.3}$$

where each $R_j \cap \boldsymbol{T}_j$ is a patterned polyhedron in $\mathbb{R}^n$ with period $\mathcal{T}_j \subseteq \mathbb{Z}^n$. The polyhedra R_j and lattices $\mathcal{T}_j$ can be found in time $\operatorname{poly}(\ell(Q) + \ell(\mathcal{L}))$. *Moreover,*

$$r = O\big(\eta(Q)^2\big) \quad \textit{and} \quad \eta(R_j) = O\big(\eta(Q)^2\big), \quad \textit{for all } \ 0 \le j \le r\,.$$

We postpone the proof of the lemma until §6.2.C.

6.2.B. Proof of Theorem 6.8. We begin with the following definitions and notation.

Definition 6.12. A *copolyhedron* $P \subseteq \mathbb{R}^d$ is a polyhedron with possibly some open facets. If P is a rational copolyhedron, we denote by $\lfloor P \rfloor$ the (closed) polyhedron obtained from P by sharpening each open facet $(\overline{a}\,\mathbf{x} < b)$ of P to $(\overline{a}\,\mathbf{x} \le b - 1)$, after scaling $\overline{a}$ and b to integers. Clearly, we have $P \cap \mathbb{Z}^d = \lfloor P \rfloor \cap \mathbb{Z}^d$.

WLOG, we can assume $n \le m$ and the linear map $T : \mathbb{R}^m \to \mathbb{R}^n$ has $\operatorname{rank}(T) = n$. Also denote by T the integer matrix in $\mathbb{Z}^{n\times m}$ representing this linear map. We can rearrange the coordinates in $\mathbb{R}^m$ so that the first n columns in T form a non-singular minor.

Recall that X has the form (6.1) with each $Q_i \cap \boldsymbol{L}_i$ having period $\mathcal{L}_i$. For each i, define the polyhedron

$$\widehat{Q}_i \coloneqq \big\{(\mathbf{x}, \mathbf{y}) : \mathbf{y} = T\mathbf{x} \ \text{ and } \ \mathbf{x} \in Q_i\big\} \subseteq \mathbb{R}^{m+n}. \tag{6.4}$$

Consider the pattern $\boldsymbol{U}_i = \boldsymbol{L}_i \oplus \mathbb{Z}^n \subseteq \mathbb{Z}^{m+n}$ with period $\mathcal{U}_i = \mathcal{L}_i \oplus \mathbb{Z}^n$. Then $\widehat{Q}_i \cap \boldsymbol{U}_i$ is a patterned polyhedron in $\mathbb{R}^{m+n}$ with period $\mathcal{U}_i$. Define the projection $S : \mathbb{R}^{m+n} \to \mathbb{R}^n$ with $S(\mathbf{x}, \mathbf{y}) = \mathbf{y}$. By (6.4), we have:

$$T(Q_i \cap \boldsymbol{L}_i) = S(\widehat{Q}_i \cap \boldsymbol{U}_i) \quad \text{and} \quad T(X) = S\left(\bigsqcup_{i=1}^{r} \widehat{Q}_i \cap \boldsymbol{U}_i\right) = \bigcup_{i=1}^{r} S(\widehat{Q}_i \cap \boldsymbol{U}_i),$$

We can represent $S = S_m \circ \cdots \circ S_1$, where each $S_i : \mathbb{R}^{m+n-i+1} \to \mathbb{R}^{m+n-i}$ is a projection along the x_i coordinate.

Let $H \subset \mathbb{R}^{m+n}$ be the subspace defined by $\mathbf{y} = T\mathbf{x}$. First, we show that the initial n projections $F = S_n \circ \cdots \circ S_1$ are injective on H. Indeed, assume $(\mathbf{x}, \mathbf{y})$, $(\mathbf{x}', \mathbf{y}')$ are two points in H with $F(\mathbf{x}, \mathbf{y}) = F(\mathbf{x}', \mathbf{y}')$. Since F projects along the first n coordinates of $\mathbf{x}$ and $\mathbf{x}'$, we have $(x_{n+1}, \ldots, x_m, \mathbf{y}) = (x'_{n+1}, \ldots, x'_m, \mathbf{y}')$. Thus, $\mathbf{y} = \mathbf{y}'$, which implies $T\mathbf{x} = T\mathbf{x}'$. Let $B \in \mathbb{Z}^{n \times n}$ be the first n columns in T, which forms a non-singular minor as assumed earlier. Since $T\mathbf{x} = T\mathbf{x}'$ and $(x_{n+1}, \ldots, x_m) = (x'_{n+1}, \ldots, x'_m)$, we have $B\,(x_1, \ldots, x_n) = B\,(x'_1, \ldots, x'_n)$. This implies $(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n)$. We conclude that $(\mathbf{x}, \mathbf{y}) = (\mathbf{x}', \mathbf{y}')$, and F is injective on H.

By (6.4), we have $\widehat{Q}_i \cap \boldsymbol{U}_i \subseteq H$ for every i. Because $F : \mathbb{R}^{m+n} \to \mathbb{R}^m$ is injective on H, the semilinear structure of $\left(\bigsqcup \widehat{Q}_i \cap \boldsymbol{U}_i\right)$ is preserved by F. For convenience, we also denote by $\left(\bigsqcup \widehat{Q}_i \cap \boldsymbol{U}_i\right)$ the semilinear set after applying F, which is now a subset of $\mathbb{Z}^m$. Now we repeatedly apply Lemma 6.11 to the remaining projections $S_m \circ \cdots \circ S_{n+1}$. Starting with the projection S_{n+1} applied on each piece $Q_i \cap \boldsymbol{U}_i \subseteq \mathbb{Z}^m$, we get:

$$S_{n+1}(\widehat{Q}_i \cap \boldsymbol{U}_i) \;=\; \bigsqcup_{j=0}^{r_i} R_{ij} \cap \boldsymbol{T}_{ij} \quad \text{for } \; 1 \le i \le k,\, 1 \le j \le r_i, \tag{6.5}$$

where each $R_{ij} \cap \boldsymbol{T}_{ij}$ is a patterned polyhedron in $\mathbb{Z}^{m-1}$ with period $\mathcal{T}_{ij}$. Note that two polyhedra R_{ij} and $R_{i'j'}$ can be overlapping if $i \neq i'$. However, we can refine all R_{ij} into polynomially many disjoint copolyhedra $P_1, \ldots, P_e \subseteq \mathbb{R}^{m-1}$, so that

$$\bigcup_{i=1}^{k} \bigcup_{j=1}^{r_i} R_{ij} \;=\; \bigsqcup_{d=1}^{e} P_d\,. \tag{6.6}$$

For each P_d, there is a pattern $\boldsymbol{W}_d$ with period $\mathcal{W}_d \subseteq \mathbb{Z}^{m-1}$ which fits with those $\boldsymbol{T}_{ij}$ for which $P_d \subseteq R_{ij}$. The (full-rank) period $\mathcal{W}_d$ can simply be taken as the intersection of polynomially

many (full-rank) periods $\mathcal{T}_{ij}$ for which $P_d \subseteq R_{ij}$. Taking intersections of lattices in a fixed dimension can be done in polynomial time using Hermite Normal Form (see [KB79]). We also round each P_d to $\lfloor P_d \rfloor$ (see Definition 6.12). From (6.5) and (6.6) we have:

$$S_{n+1}\Big(\bigsqcup_{i=1}^{k} \widehat{Q}_i \cap \boldsymbol{U}_i\Big) \;=\; \bigcup_{i=1}^{k} S_{n+1}(\widehat{Q}_i \cap \boldsymbol{U}_i) \;=\; \bigsqcup_{d=1}^{e} \lfloor P_d \rfloor \cap \boldsymbol{W}_d\,.$$

The above RHS is a semilinear set in $\mathbb{Z}^{m-1}$. A similar argument applies to $S_m \circ \cdots \circ S_{n+2}$. In the end, we have a semilinear decomposition for $T(X) \subseteq \mathbb{Z}^n$, as in (6.2).

Using Lemma 6.11, we can bound the number of polyhedra r_i in (6.5), and also the number of facets $\eta(R_{ij})$ for each R_{ij}. It is well known that any q hyperplanes in $\mathbb{R}^m$ partition the space into at most $O(q^m)$ polyhedral regions. This gives us a polynomial bound on e, the number of refined pieces in (6.6). By a careful analysis, after m projections, the total number r of pieces in the final decomposition (6.2) is at most $\eta(X)^{O(m!)}$. Each piece R_j also has at most $\eta(X)^{O(m!)}$ facets. $\square$

6.2.C. Proof of Lemma 6.11. The proof is by induction on n. The case $n = 0$ is trivial. For the rest of the proof, assume $n \geq 1$.

Let $\boldsymbol{L} \subseteq \mathbb{Z}^{n+1}$ be a full-rank pattern with period $\mathcal{L}$ as in the lemma. Then, the projection of $\boldsymbol{L}$ onto $\mathbb{Z}^n$ is another pattern $\boldsymbol{L}'$ with full-rank period $\mathcal{L}' = \mathrm{proj}(\mathcal{L})$.[2] Since $\mathcal{L}$ is of full rank, we can define

$$\gamma = \min\{x \in \mathbb{Z}_+ : (x, 0, \ldots, 0) \in \mathcal{L}\}. \tag{6.7}$$

Let $R = \mathrm{proj}(Q)$. Assume Q is described by the system $A\mathbf{x} \leq \overline{b}$. Recall the *Fourier–Motzkin elimination method* (see [Sch86, §12.2]), which gives the facets of R from those of Q. First, rewrite and group the inequalities in $A\mathbf{x} \leq \overline{b}$ into

$$A_1\mathbf{y} + \overline{b}_1 \leq x_1, \quad x_1 \leq A_2\mathbf{y} + \overline{b}_2 \quad \text{and} \quad A_3\mathbf{y} \leq \overline{b}_3, \tag{6.8}$$

where $\mathbf{y} = (x_2, \ldots, x_{n+1}) \in \mathbb{R}^n$. Then R is described by a system $C\mathbf{y} \leq \overline{d}$, which consists of $(A_3\mathbf{y} \leq \overline{b}_3)$ and $(\overline{a}_1\mathbf{y} + b_1 \leq \overline{a}_2\mathbf{y} + b_2)$ for every possible pair of rows $\overline{a}_1\mathbf{y} + b_1$ and $\overline{a}_2\mathbf{y} + b_2$

[2]Here a basis for $\mathcal{L}'$ can be computed in polynomial time by applying Hermite Normal Form to a basis of $\mathcal{L}$, whose first coordinates x_1 should be set to 0.

from the first two systems in (6.8).

In case one of the two systems $A_1\mathbf{y} + \overline{b}_1 \leq x_1$ and $x_1 \leq A_2\mathbf{y} + \overline{b}_2$ is empty, then R is simply described by $A_3\mathbf{y} \leq \overline{b}_3$. Also in this case, the preimage $\mathrm{proj}^{-1}(\mathbf{y})$ of every point $\mathbf{y} \in R$ is infinite. By the argument in Lemma 6.13 below, we have a simple description $\mathrm{proj}(Q \cap \boldsymbol{L}) = R \cap \boldsymbol{L}'$, which finishes the proof. So now assume that the two systems $A_1\mathbf{y} + \overline{b}_1 \leq x_1$ and $x_1 \leq A_2\mathbf{y} + \overline{b}_2$ are both non-empty. Then we can decompose

$$R = \bigsqcup_{j=1}^{r} P_j, \tag{6.9}$$

where each P_j is a copolyhedron, so that over each P_j, the largest entry in the vector $A_1\mathbf{y}+\overline{b}_1$ is $\overline{a}_{j1}\mathbf{y} + b_{j1}$ and the smallest entry in the vector $A_2\mathbf{y} + \overline{b}_2$ is $\overline{a}_{j2}\mathbf{y} + b_{j2}$. Thus, for every $\mathbf{y} \in P_j$, we have $\mathrm{proj}^{-1}(\mathbf{y}) = [\alpha_j(\mathbf{y}), \beta_j(\mathbf{y})]$, where $\alpha_j(\mathbf{y}) = \overline{a}_{j1}\mathbf{y} + b_{j1}$ and $\beta_j(\mathbf{y}) = \overline{a}_{j2}\mathbf{y} + b_{j2}$ are affine rational functions. Let $m = \eta(Q)$. Note that the system $C\mathbf{y} \leq \overline{d}$ describing R contains at most $O(m^2)$ inequalities, i.e., $\eta(R) = O(m^2)$. Also, we have $r = O(m^2)$ and $\eta(P_j) = O(m)$ for $1 \leq j \leq r$.

For each $\mathbf{y} \in R$, the preimage $\mathrm{proj}^{-1}(\mathbf{y}) \subseteq Q$ is a segment in the direction x_1. Denote by $|\mathrm{proj}^{-1}(\mathbf{y})|$ the Euclidean length of this segment. Now we refine the decomposition (6.9) to

$$R = R_0 \sqcup R_1 \sqcup \cdots \sqcup R_r\,, \qquad \text{where} \tag{6.10}$$

a) Each R_j is a copolyhedron in $\mathbb{R}^n$, with $\eta(R_j) = O(m^2)$ and $r = O(m^2)$.

b) For every $\mathbf{y} \in R_0$, we have the length $|\mathrm{proj}^{-1}(\mathbf{y})| \geq \gamma$.

c) For every $\mathbf{y} \in R_j$ $(1 \leq j \leq r)$, we have the length $|\mathrm{proj}^{-1}(\mathbf{y})| < \gamma$. Furthermore, we have $\mathrm{proj}^{-1}(\mathbf{y}) = [\alpha_j(\mathbf{y}), \beta_j(\mathbf{y})]$, where α_j and β_j are affine rational functions in $\mathbf{y}$.

This refinement can be obtained as follows. First, define

$$R_0 = \mathrm{proj}[Q \cap (Q + \gamma\overline{v}_1)] \subseteq R,$$

where $\overline{v}_1 = (1, 0, \ldots, 0)$. The facets of R_0 can be found from those of $Q \cap (Q + \gamma\overline{v}_1)$ again by Fourier–Motzkin elimination, and also $\eta(R_0) = O(m^2)$. Observe that $|\mathrm{proj}^{-1}(\mathbf{y})| \geq \gamma$ if

and only if $\mathbf{y} \in R_0$. Define $R_j \coloneqq P_j \backslash R_0$ for $1 \le j \le r$. Recall that for every $\mathbf{y} \in P_j$, we have $\text{proj}^{-1}(\mathbf{y}) = [\alpha_j(\mathbf{y}), \beta_j(\mathbf{y})]$. Therefore,

$$R_j \;=\; P_j \backslash R_0 \;=\; \{\mathbf{y} \in P_j : |\text{proj}^{-1}(\mathbf{y})| < \gamma\} \;=\; \{\mathbf{y} \in P_j : \alpha_j(\mathbf{y}) + \gamma > \beta_j(\mathbf{y})\}.$$

It is clear that each R_j is a copolyhedron satisfying condition c). Moreover, for each $1 \le j \le r$, we have $\eta(R_j) \le \eta(P_j) + 1 = O(m)$. By (6.9), we can decompose:

$$R \;=\; R_0 \sqcup (R \backslash R_0) \;=\; R_0 \;\sqcup \bigsqcup_{j=1}^{r} (P_j \backslash R_0) \;=\; \bigsqcup_{j=0}^{r} R_j \,.$$

This decomposition satisfies all conditions a)–c) and proves (6.10). Note also that by converting each R_j to $\lfloor R_j \rfloor$, we do not lose any integer points in R. Let us show that the part of $\text{proj}(Q \cap \boldsymbol{L})$ within R_0 has a simple pattern:

Lemma 6.13. $\text{proj}(Q \cap \boldsymbol{L}) \cap R_0 \;=\; R_0 \cap \boldsymbol{L}'$.

Proof. Recall that $\text{proj}(\boldsymbol{L}) = \boldsymbol{L}'$, which implies LHS $\subseteq$ RHS. On the other hand, for every $\mathbf{y} \in \boldsymbol{L}'$, there exists $\mathbf{x} \in \boldsymbol{L}$ such that $\mathbf{y} = \text{proj}(\mathbf{x})$. If $\mathbf{y} \in R_0 \cap \boldsymbol{L}'$, we also have $|\text{proj}^{-1}(\mathbf{y})| \ge \gamma$ by condition b), with γ defined in (6.7). The point $\mathbf{x}$ and the segment $\text{proj}^{-1}(\mathbf{y})$ lie on the same vertical line. Therefore, since $|\text{proj}^{-1}(\mathbf{y})| \ge \gamma$, we can find another $\mathbf{x}'$ such that $\mathbf{x}' \in \text{proj}^{-1}(\mathbf{y}) \subseteq Q$ and also $\mathbf{x}' - \mathbf{x} \in \mathcal{L}$. Since $\boldsymbol{L}$ has period $\mathcal{L}$, we have $\mathbf{x}' \in \boldsymbol{L}$. This implies $\mathbf{x}' \in Q \cap \boldsymbol{L}$, and $\mathbf{y} \in \text{proj}(Q \cap \boldsymbol{L})$. Therefore we have RHS $\subseteq$ LHS, and the lemma holds. □

It remains to show that $\text{proj}(Q \cap \boldsymbol{L}) \cap R_j$ also has a pattern for every $j > 0$. By condition c), every such R_j has a "thin" preimage. Let $Q_j = \text{proj}^{-1}(R_j) \subseteq Q$. If $\dim(R_j) < n$, we have $\dim(Q_j) < n + 1$. In this case we can apply the inductive hypothesis. Otherwise, assume $\dim(R_j) = n$. For convenience, we refer to R_j and Q_j as just R and Q. We can write $R = R' + D$, where $R' \subseteq R$ is a polytope and D is the recession cone of R.

Consider $\mathbf{y} \in R$, $\mathbf{v} \in D$ and $\lambda > 0$. Since $\mathbf{y} + \lambda\mathbf{v} \in R$, from c) we have $\text{proj}^{-1}(\mathbf{y} + \lambda\mathbf{v}) = [\alpha(\mathbf{y} + \lambda\mathbf{v}), \beta(\mathbf{y} + \lambda\mathbf{v})]$. Denote by $\widetilde{\alpha}$ and $\widetilde{\beta}$ the linear parts of the affine maps α and β. By a property of affine maps, we have:

$$\text{proj}^{-1}(\mathbf{y} + \lambda\mathbf{v}) = [\alpha(\mathbf{y} + \lambda\mathbf{v}), \beta(\mathbf{y} + \lambda\mathbf{v})] = [\alpha(\mathbf{y}) + \lambda\widetilde{\alpha}(\mathbf{v}),\ \beta(\mathbf{y}) + \lambda\widetilde{\beta}(\mathbf{v})]. \tag{6.11}$$

Therefore,

$$|\text{proj}^{-1}(\mathbf{y}+\lambda\mathbf{v})| = \beta(\mathbf{y}) - \alpha(\mathbf{y}) + \lambda\big(\widetilde{\beta}-\widetilde{\alpha}\big)(\mathbf{v}).$$

Since $(\mathbf{y}+\lambda\mathbf{v}) \in R$, by c) we have:

$$0 \le |\text{proj}^{-1}(\mathbf{y}+\lambda\mathbf{v})| = \beta(\mathbf{y}) - \alpha(\mathbf{y}) + \lambda\big(\widetilde{\beta}-\widetilde{\alpha}\big)(\mathbf{v}) < \gamma.$$

Because $\lambda > 0$ is arbitrary, we must have $\big(\widetilde{\beta}-\widetilde{\alpha}\big)(\mathbf{v}) = 0$. This holds for all $\mathbf{v} \in D$. We conclude that $\widetilde{\beta}-\widetilde{\alpha}$ vanishes on the whole subspace $H := \text{span}(D)$, i.e., for any $\mathbf{v} \in H$ we have $\widetilde{\alpha}(\mathbf{v}) = \widetilde{\beta}(\mathbf{v})$. Thus, we can rewrite (6.11) as

$$\text{proj}^{-1}(\mathbf{y}+\lambda\mathbf{v}) = [\alpha(\mathbf{y}), \beta(\mathbf{y})] + \lambda\widetilde{\alpha}(\mathbf{v}) = \text{proj}^{-1}(\mathbf{y}) + \lambda\widetilde{\alpha}(\mathbf{v}). \tag{6.12}$$

Define $C := \widetilde{\alpha}(D)$ and $G := \widetilde{\alpha}(H)$. Note that $\text{span}(C) = G$, because $\text{span}(D) = H$. Recall that $R = R' + D$ with R' a polytope. In (6.12), we let $\mathbf{y}$ vary over R', λ vary over $\mathbb{R}_+$ and $\mathbf{v}$ vary over D. The LHS becomes $Q = \text{proj}^{-1}(R)$. The RHS becomes $\text{proj}^{-1}(R') + C$. Therefore, we have $Q = \text{proj}^{-1}(R') + C$. Since $\text{proj}^{-1}(R')$ is a polytope, we conclude that C is the recession cone for Q.

Because $\text{proj}^{-1}(\mathbf{y}) = [\alpha(\mathbf{y}), \beta(\mathbf{y})]$ for every $\mathbf{y} \in R$, the last n coordinates in $\alpha(\mathbf{y})$ and $\beta(\mathbf{y})$ are equal to $\mathbf{y}$. This also holds for $\widetilde{\alpha}(\mathbf{y})$ and $\widetilde{\beta}(\mathbf{y})$, i.e., $\text{proj}(\widetilde{\alpha}(\mathbf{y})) = \text{proj}(\widetilde{\alpha}(\mathbf{y})) = \mathbf{y}$. This implies $\text{proj}(G) = H$, because $G = \widetilde{\alpha}(H)$. In other words, $\widetilde{\alpha}$ is the inverse map for proj on G. In Figure 6.1, we illustrate R and $Q = \text{proj}^{-1}(R)$, with R' and $\text{proj}^{-1}(R')$ shown in blue. The cones C and D span G and H, respectively.

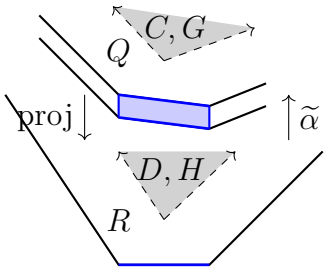


Figure 6.1: R and Q.

Recall that $Q \cap \boldsymbol{L}$ is a patterned polyhedron with period $\mathcal{L}$, and $\text{proj}(Q) = R$. Define

$$\mathcal{S} \coloneqq \mathcal{L} \cap G \quad \text{and} \quad \mathcal{T} \coloneqq \text{proj}(\mathcal{S}) \subset \text{proj}(G) = H.$$

Since $\mathcal{L}$ is full-rank, we have $\text{rank}(\mathcal{S}) = \dim(G)$. Since $\widetilde{\alpha}$ and proj are inverse maps, we have $\mathcal{S} = \widetilde{\alpha}(\mathcal{T})$. We claim that $\text{proj}(Q \cap \boldsymbol{L}) \subset R$ is a patterned polyhedron with period $\mathcal{T}$. Indeed, consider any two points $\mathbf{y}_1, \mathbf{y}_2 \in R$ with $\mathbf{y}_2 - \mathbf{y}_1 \in \mathcal{T}$. Assume that $\mathbf{y}_1 \in \text{proj}(Q \cap \boldsymbol{L})$, i.e., there exists $\mathbf{x}_1 \in Q \cap \boldsymbol{L}$ with $\text{proj}(\mathbf{x}_1) = \mathbf{y}_1$. We show that $\mathbf{y}_2 \in \text{proj}(Q \cap \boldsymbol{L})$. First, we have $\text{proj}^{-1}(\mathbf{y}_1) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)]$ and $\text{proj}^{-1}(\mathbf{y}_2) = [\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)]$. Let $\mathbf{v} = \mathbf{y}_2 - \mathbf{y}_1 \in \mathcal{T} \subset H$. Since $\mathbf{y}_2 = \mathbf{y}_1 + \mathbf{v}$, we can apply (6.12) with $\lambda = 1$ and get:

$$[\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)] = \text{proj}^{-1}(\mathbf{y}_2) = \text{proj}^{-1}(\mathbf{y}_1 + \mathbf{v}) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)] + \widetilde{\alpha}(\mathbf{v}). \tag{6.13}$$

Thus, we have $\alpha(\mathbf{y}_1) - \beta(\mathbf{y}_1) = \alpha(\mathbf{y}_2) - \beta(\mathbf{y}_2)$. In other words, the points $\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1), \alpha(\mathbf{y}_2)$ and $\beta(\mathbf{y}_2)$ form a parallelogram inside Q. Since $\text{proj}(\mathbf{x}_1) = \mathbf{y}_1$, we have:

$$\mathbf{x}_1 \in \text{proj}^{-1}(\mathbf{y}_1) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)] \subseteq Q.$$

So $\mathbf{x}_1$ lies on the edge $[\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)]$ of the parallelogram mentioned above. Therefore, we can find another point $\mathbf{x}_2$ lying on the other edge $[\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)] = \text{proj}^{-1}(\mathbf{y}_2)$ with

$$\mathbf{x}_2 - \mathbf{x}_1 = \alpha(\mathbf{y}_2) - \alpha(\mathbf{y}_1) = \widetilde{\alpha}(\mathbf{y}_2 - \mathbf{y}_1) = \widetilde{\alpha}(\mathbf{v}) \in \widetilde{\alpha}(\mathcal{T}) = \mathcal{S}.$$

This $\mathbf{x}_2$ satisfies $\text{proj}(\mathbf{x}_2) = \mathbf{y}_2$. Recall that $\mathbf{x}_1 \in \boldsymbol{L}$, with $\boldsymbol{L}$ having period $\mathcal{L}$. Since $\mathbf{x}_2 - \mathbf{x}_1 \in \mathcal{S} \subset \mathcal{L}$, we have $\mathbf{x}_2 \in \boldsymbol{L}$. This implies $\mathbf{x}_2 \in Q \cap \boldsymbol{L}$ and $\mathbf{y}_2 \in \text{proj}(Q \cap \boldsymbol{L})$.

So we have established that $\text{proj}(Q \cap \boldsymbol{L}) \subset R$ is a patterned polyhedron with period $\mathcal{T}$. Note that

$$\text{rank}(\mathcal{T}) = \text{rank}(\mathcal{S}) = \dim(G) = \dim(H) = \dim(D).$$

If $\dim(D) = n$ then $\mathcal{T}$ is full-rank. If $\dim(D) < n$, recall that $R = R' + D$ where R' is a polytope, and $\text{span}(D) = H$. Let $H^\perp$ be the complement subspace to H in $\mathbb{R}^n$, and $R^\perp$ be the projection of R' onto $H^\perp$. Since $R^\perp$ is bounded, we can take a large enough lattice $\mathcal{T}^\perp \subset H^\perp$ such that there are no two points $\mathbf{z}_1 \neq \mathbf{z}_2 \in R^\perp$ with $\mathbf{z}_1 - \mathbf{z}_2 \in \mathcal{T}^\perp$. Now the lattice $\mathcal{T}^\perp \oplus \mathcal{T}$ is full-rank, which can be taken as a period for $\text{proj}(Q \cap \boldsymbol{L})$.

To summarize, for every piece R_j and $Q_j = \text{proj}^{-1}(R_j)$, $1 \le j \le r$, the projection $\text{proj}(Q_j \cap \boldsymbol{L}) \subset R_j$ has period $\mathcal{T}_j$. Thus $\text{proj}(Q_j \cap \boldsymbol{L})$ is a patterned polyhedron. This completes the proof. $\square$

6.3. Finding short GF for unbounded projection

6.3.A. The Barvinok–Woods algorithm. In this section, we are again assuming that dimensions m and n are fixed. We recall the Barvinok–Woods algorithm from [BW03], which finds in polynomial time a short GF for the projection of integer points in a polytope:

Theorem 6.14 (Th. 2.5 restated)**.** *Let $m, n \in \mathbb{N}$ be fixed dimensions. Given a rational polytope $Q = \{\mathbf{x} \in \mathbb{R}^m : A\mathbf{x} \le \overline{b}\}$, and a linear transformation $T : \mathbb{R}^m \to \mathbb{R}^n$ represented as a matrix $T \in \mathbb{Z}^{n \times m}$, there is a polynomial time algorithm to compute a short GF for $T(Q \cap \mathbb{Z}^m)$ as:*

$$g(\mathbf{t}) \;=\; \sum_{\mathbf{y} \,\in\, T(Q \cap \mathbb{Z}^m)} \mathbf{t}^{\mathbf{y}} \;=\; \sum_{i=1}^{M} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1 - \mathbf{t}^{\overline{b}_{i1}}) \ldots (1 - \mathbf{t}^{\overline{b}_{is}})}, \tag{6.14}$$

where $c_i = p_i/q_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$, $\overline{b}_{ij} \neq 0$ for all i, j, and s is a constant depending only on m. Furthermore, the short GF $g(\mathbf{t})$ has length $\ell(g) = \text{poly}(\ell(Q) + \ell(T))$, where

$$\ell(g) \;=\; \sum_i \lceil \log_2 |p_i\, q_i| + 1 \rceil \;+\; \sum_{i,j} \lceil \log_2 a_{ij} + 1 \rceil \;+\; \sum_{i,j,k} \lceil \log_2 b_{ijk} + 1 \rceil \,. \tag{6.15}$$

Clearly, our main result Theorem 6.2 is an extension of Theorem 6.14. The proof of Theorem 6.2 is based on Theorem 6.8 and uses the following standard result:

Proposition 6.15 (see e.g. [Mei93])**.** *Let $n \in \mathbb{N}$ be fixed. Let $R = \{\mathbf{x} \in \mathbb{R}^n : C\mathbf{x} \le \overline{d}\}$ be a possibly unbounded polyhedron. There is a decomposition*

$$R = \bigsqcup_{k=1}^{t} R_k \oplus D_k \,, \tag{6.16}$$

where each R_k is a copolytope, and each D_k is a simple cone. Each part $R_k \oplus D_k$ is a direct sum, with R_k and D_k affinely independent. All R_k and D_k can be found in time $\text{poly}(\ell(R))$.

Before proving Theorem 6.2, we make an important remark:

Remark 6.16. The extra condition $T(Q) \subseteq \mathbb{R}^n_+$ in Theorem 6.2 is to make sure that the power series $\sum \mathbf{t}^{\mathbf{y}}$ of $T(Q \cap \mathbb{Z}^m)$ converges on a non-empty open domain to the computed short GF. In general, without the condition $T(Q) \subseteq \mathbb{R}^n_+$, we can still make sense of the infinite GF (see §6.6.C).

6.3.B. Proof of Theorem 6.2. WLOG, we can assume $\dim(Q) = m$ and $\dim(T(Q)) = n$. Clearly, the set $X = Q \cap \mathbb{Z}^m$ is a semilinear set, and we want to find a short GF for $T(X)$.

First, we argue that for any bounded polytope $P \subset \mathbb{R}^n$, a short GF for $T(X) \cap P$ can be found in time $\text{poly}(\ell(Q) + \ell(P))$. Assume P is given by a system $C\mathbf{y} \leq \overline{d}$. For any $\overline{v} \in P$, we have $\overline{v} \in T(X)$ if and only if the following system has a solution $\mathbf{x} \in \mathbb{Z}^m$:

$$\begin{cases} A\mathbf{x} & \leq & \overline{b} \\ T(\mathbf{x}) & = & \overline{v} \end{cases}. \tag{6.17}$$

By a well known bound on Integer Programming solutions (see [Sch86, Cor. 17.1b]), it is equivalent to find such a solution $\mathbf{x}$ with binary length at most polynomial in the binary length of the system (6.17). The parameter $\overline{v}$ lies in P, which is bounded. Therefore, we can find a number N with $\log N = \text{poly}(\ell(P) + \ell(Q))$, such that (6.17) is equivalent to:

$$\begin{cases} A\mathbf{x} & \leq & \overline{b} \\ C\,T(\mathbf{x}) & \leq & \overline{d} \\ -N \leq \mathbf{x} & \leq & N \end{cases}.$$

This system describes a polytope $\widehat{Q} \subset \mathbb{R}^m$. Applying Theorem 6.14 to $\widehat{Q}$, we obtain a short GF $g(\mathbf{t})$ for $T(\widehat{Q} \cap \mathbb{Z}^m) = T(X) \cap P$.

Now we are back to finding a short GF for the entire projection $T(X)$. Applying Theorem 6.8 to X, we have a decomposition:

$$T(X) = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j\,. \tag{6.18}$$

We proceed to find a short GF g_j for each patterned polyhedron $R_j \cap \boldsymbol{T}_j$ with period $\mathcal{T}_j$. For convenience, we refer to R_j, $\boldsymbol{T}_j$, $\mathcal{T}_j$, g_j simply as R, $\boldsymbol{T}$, $\mathcal{T}$ and g. By Proposition 6.15,

we can decompose

$$R = \bigsqcup_{i=1}^{t_j} R_i \oplus D_i \quad \text{and} \quad R \cap \boldsymbol{T} = \bigsqcup_{i=1}^{t_j} (R_i \oplus D_i) \cap \boldsymbol{T}. \tag{6.19}$$

Recall from Theorem 6.8 that $\mathcal{T}$ has full rank. Let $d_i = \dim(D_i)$ and $\overline{v}_i^1, \ldots, \overline{v}_i^{d_i}$ be the generating rays of the (simple) cone D_i. For each $\overline{v}_i^t$, we can find a $n_t \in \mathbb{Z}_+$ such that $\overline{w}_i^t = n_t \mathbf{v}_i^t \in \mathcal{T}$. Let P_i and $\mathcal{T}_i$ be the parallelepiped and lattice spanned by $\overline{w}_i^1, \ldots, \overline{w}_i^{d_i}$, respectively. We have $D_i = P_i + \mathcal{T}_i$ and therefore

$$R_i \oplus D_i = R_i \oplus (P_i + \mathcal{T}_i) = (R_i \oplus P_i) + \mathcal{T}_i. \tag{6.20}$$

Each $R_i \oplus P_i$ is a copolytope. Note that Theorem 6.14 is stated for (closed) polytopes. We round each $R_i \oplus P_i$ to $\lfloor R_i \oplus P_i \rfloor$, where $\lfloor . \rfloor$ was described in Definition 6.12. By the earlier argument, we can find a short GF $h_i(\mathbf{t})$ for $T(X) \cap (R_i \oplus P_i) = (R_i \oplus P_i) \cap \boldsymbol{T}$. Since $\mathcal{T}_i \subseteq \mathcal{T}$, the pattern $\boldsymbol{T}$ also has period $\mathcal{T}_i$. By (6.20), the short GF $f_i(\mathbf{t})$ for $(R_i \oplus D_i) \cap \boldsymbol{T}$ is:

$$f_i(\mathbf{t}) = \sum_{\mathbf{y} \in (R_i \oplus D_i) \cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} = \left(\sum_{\mathbf{y} \in (R_i \oplus P_i) \cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} \right) \cdot \left(\sum_{\mathbf{y} \in \mathcal{T}_i} \mathbf{t}^{\mathbf{y}} \right) = h_i(\mathbf{t}) \prod_{t=1}^{d_i} \frac{1}{1 - \mathbf{t}^{\overline{w}_i^t}}. \tag{6.21}$$

By (6.19), we obtain

$$g(\mathbf{t}) = \sum_{\mathbf{y} \in R \cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} = \sum_{1 \le i \le t_j} f_i(\mathbf{t}). \tag{6.22}$$

In summary, we obtained a short GF $g_j(\mathbf{t})$ for each piece $R_j \cap \boldsymbol{T}_j$ $(1 \le j \le r)$. Summing over all j in (6.18), we get a short GF for $T(X)$, as desired. $\square$

6.4. Generalization to Presburger formulas

Now we employ Theorem 6.8 to analyze the structure of general semilinear sets, i.e., those definable by formulas in Presburger Arithmetic (PA). Recall that such formulas have the form:

$$F \;=\; \big\{ \mathbf{x}_1 \in \mathbb{Z}^{n_1} \;:\; Q_2 \mathbf{x}_2 \in \mathbb{Z}^{n_2} \;\ldots\; Q_k \mathbf{x}_k \in \mathbb{Z}^{n_k} \quad \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k) \big\}, \tag{$*$}$$

where Φ is a Boolean combination of linear inequalities in the form:

$$\sum_{i=1}^{k} \sum_{j=1}^{n_i} a_{ij}\, x_{ij} \;\le\; b,$$

Here, $Q_2, \ldots, Q_k \in \{\forall, \exists\}$ are quantifiers, and $a_{ij}, b \in \mathbb{Z}$. The length $\ell(F)$ of F is the total binary length of its symbols, coefficients a_{ij} and constants b.

By a classical result of Ginsburg and Spanier [GS64], semilinear sets (Definition 6.6) are exactly those definable in PA, i.e., representable by some PA formula F of the form $(*)$. Below is our main result for this section, which generalizes Theorem 6.8. Roughly speaking, it allows us to compute in polynomial time the "periods" of a semilinear set when represented as a PA formula. We fix $k \in \mathbb{Z}_+$ and the dimensions $\overline{n} = (n_1, \ldots, n_k) \in \mathbb{Z}_+^k$. Denote by $\mathrm{PA}_{k,\overline{n}}$ the class of PA formulas $(*)$.

Theorem 6.17. *Fix k and $\overline{n} = (n_1, \ldots, n_k)$. Given a formula $F \in \mathrm{PA}_{k,\overline{n}}$, there exists a decomposition*

$$F = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j \,,$$

where each $R_j \cap \boldsymbol{T}_j$ is a patterned polyhedron in $\mathbb{R}^{n_1}$ with period $\mathcal{T}_j \subseteq \mathbb{Z}^{n_1}$. The polyhedra R_j and lattices $\mathcal{T}_j$ can be found in time $\mathrm{poly}(\ell(F))$.

Proof. Hereafter, we abbreviate $\mathbf{x}_i \in \mathbb{Z}^{n_i}$ to just $\mathbf{x}_i$. Consider any $F \in \mathrm{PA}_{k,\overline{n}}$:

$$F = \{\mathbf{x}_1 \ : \ Q_2 \mathbf{x}_2 \ldots Q_k \mathbf{x}_k \ \ \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)\}.$$

Let $\overline{\mathbf{x}} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ and $n = n_1 + \ldots + n_k$. First, we show that $X = \{\overline{\mathbf{x}} \in \mathbb{Z}^n : \Phi(\overline{\mathbf{x}})\}$ is semilinear, i.e., satisfies Definition 6.6. Recall that Φ is quantifier-free, i.e., a Boolean combination of linear inequalities. We need the following very useful result about quantifier-free PA expressions:

Proposition 6.18 ([Woo04, Prop. 5.2.2])**.** *Fix n. Let $\Phi(\mathbf{x})$ be a Boolean combination of linear inequalities in integer variables $\mathbf{x} = (x_1, \ldots, x_n)$. Then we have:*

$$\Phi(\mathbf{x}) = \text{true} \quad \Longleftrightarrow \quad \bigvee_{i=1}^{r} \mathbf{x} \in P_i \cap \mathbb{Z}^n,$$

where $P_1, \ldots, P_r \subseteq \mathbb{R}^n$ are disjoint polyhedra and $r \leq \mathrm{poly}(\ell(\Phi))$. The system defining each P_i can be computed in time $\mathrm{poly}(\ell(\Phi))$.

Using this, we can rewrite Φ in a disjunctive normal form of polynomial length:

$$\Phi(\overline{\mathbf{x}}) \;=\; A_1\overline{\mathbf{x}} \le \overline{b}_1 \;\vee\; \ldots \;\vee\; A_r\overline{\mathbf{x}} \le \overline{b}_r.$$

Here, each $A_i\overline{\mathbf{x}} \le \overline{b}_i$ is a system of inequalities, describing a polyhedron $P_i \subseteq \mathbb{R}^n$. Moreover, all polyhedra $P_1, \ldots, P_r$ are pairwise disjoint, and $\sum_{i=1}^r \ell(P_i) = \mathrm{poly}(\ell(F))$. In other words, the set X consists of integer points in a disjoint union of r polyhedra. Thus, X is a semilinear set with $\psi(X) = \mathrm{poly}(\ell(F))$, in the notation of Definition 6.6.

The proof goes by recursive construction of sets $X^{(k)}, X^{(k-1)}, \ldots, X^{(1)}$. Let $X^{(k)} \coloneqq X$. If $Q_k = \exists$, we consider the set

$$X^{(k-1)} \coloneqq \big\{(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; \Phi(\overline{\mathbf{x}})\big\} \;=\; \big\{(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; [\overline{\mathbf{x}} \in X^{(k)}]\big\}.$$

This set $X^{(k-1)}$ is obtained from $X^{(k)}$ by projecting along the last variable $\mathbf{x}_k$, i.e., the last n_k coordinates in $\overline{\mathbf{x}}$. By Theorem 6.8, we can find in polynomial time a decomposition of the form (6.2) for $X^{(k-1)}$. Moreover, we have $\psi(X^{(k-1)}) = \mathrm{poly}(\psi(X^{(k)}))$.

Similarly, if $Q_k = \forall$, we consider

$$X^{(k-1)} \coloneqq \big\{(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) : \forall \mathbf{x}_k \; \Phi(\overline{\mathbf{x}})\big\} \;=\; \neg\big\{(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; [\overline{\mathbf{x}} \in \neg X^{(k)}]\big\}.$$

Here $\neg$ denotes the complement of a set. Observe that the complement $\neg X$ of a semilinear set X is also semilinear, and $\psi(\neg X) = \mathrm{poly}(\psi(X))$. Indeed, assume that X has a decomposition

$$X = \bigsqcup_{i=1}^{p} P_i \cap \boldsymbol{L}_i \,.$$

Recall that the polyhedral pieces P_i are pairwise disjoint, but do not necessarily cover $\mathbb{R}^n$.

Let us prove that the complement $\big(\mathbb{R}^n \setminus \bigsqcup_{i=1}^p P_i\big)$ can also be partitioned into polynomially many pairwise disjoint polyhedra. Indeed, we can represent $\bigsqcup_{i=1}^p P_i$ by a Boolean expression of linear inequalities in $\mathbf{x}$. Therefore, the complement can also be represented by a Boolean expression. By Proposition 6.18 mentioned above, we can rewrite the complement as a disjoint union of polynomially many polyhedra $P'_1, \ldots, P'_q$. From here, we obtain the decomposition:

$$\neg X = \bigsqcup_{i=1}^{p} P_i \cap \boldsymbol{L}'_i \;\sqcup\; \bigsqcup_{j=1}^{q} P'_j \cap \mathbb{Z}^n \,,$$

where $\boldsymbol{L}_i'$ is the complement of $\boldsymbol{L}_i$, with the same period $\mathcal{L}_i$. Therefore, we have $\psi(\neg X^{(k)}) = \mathrm{poly}(\psi(X^{(k)}))$. Applying Theorem 6.8, we can obtain $X^{(k-1)}$ by projecting $\neg X^{(k)}$.

Applying the above argument recursively for quantifiers $Q_{k-1}, \ldots, Q_2$, we obtain a polynomial length decomposition for the semilinear set

$$X^{(1)} = \{\mathbf{x}_1 : Q_2 \mathbf{x}_2 \ldots Q_k \mathbf{x}_k \; \Phi(\mathbf{x})\} = F.$$

This completes the proof. □

Theorem 6.19. *Fix k and $\overline{n} = (n_1, \ldots, n_k)$. Given a formula $F \in \mathrm{PA}_{k,\overline{n}}$ and a positive integer M, denote by $f_M(\mathbf{t})$ the partial GF*

$$f_M(\mathbf{t}) \coloneqq \sum_{\mathbf{x} \in F \cap [-M,M]^{n_1}} \mathbf{t}^{\mathbf{x}}. \tag{6.23}$$

Suppose there is an oracle computing $f_M(\mathbf{t})$ as a short GF ($\divideontimes$) in time $\mu(F, M)$. Then there is an integer $N = N(F)$ with $\log N = \mathrm{poly}(\ell(F))$, such that the GF $f(\mathbf{t}) = \sum_{\mathbf{x} \in F} \mathbf{t}^{\mathbf{x}}$ for the entire set F can be computed as a short GF in time $\mathrm{poly}(\mu(F, N))$. The integer $N = N(F)$ can be computed in time $\mathrm{poly}(\ell(F))$.

In other words, Theorem 6.19 says that the full GF $f(\mathbf{t})$ can be computed in polynomial time from the partial GF $f_N(\mathbf{t})$ for a suitable N.

Proof. Let $n = n_1$. By Theorem 6.17, we have a decomposition

$$F = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j \,.$$

We proceed similarly to the proof of Theorem 6.2. Denote R_j and $\boldsymbol{T}_j$ by R and $\boldsymbol{T}$ respectively, for convenience. We have the decomposition (6.19) for R and $R \cap \boldsymbol{T}$, which leads to (6.20). Eventually, we can compute a short GF $g(\mathbf{t})$ for $R \cap \boldsymbol{T}$ using (6.21) and (6.22). The only difference is that the GF h_i for each patterned polytope $(R_i \oplus P_i) \cap F$, which was $(R_i \oplus P_i) \cap \boldsymbol{T}$ in (6.21), cannot be obtained from Theorem 6.14, since F is no longer the result of a single projection on a polyhedron.

Recall that each $R_i \oplus P_i$ is a polytope, with facets of total length $\mathrm{poly}(\ell(F))$. Therefore, the vertices of $R_i \oplus P_i$ can be found in polynomial time given F. This holds for all $1 \le i \le t_j$ and all $1 \le j \le r$. Thus, we can find a positive integer $N = N(F)$, for which

$$\log N = \mathrm{poly}(\ell(F)) \quad \text{and} \quad R_i \oplus P_i \subseteq [-N, N]^n \quad \text{for all } 1 \le i \le t_j.$$

Given the partial GF $f_N(\mathbf{t})$, the GF $h_i(\mathbf{t})$ for each $(R_i \oplus P_i) \cap F$ can be computed as follows.

Theorem 6.1 allows us to compute in polynomial time a short GF

$$g_i(\mathbf{t}) = \sum_{\mathbf{x} \in (R_i \oplus P_i) \cap \mathbb{Z}^n} \mathbf{t}^{\mathbf{x}}$$

for each polytope $R_i \oplus P_i$. Theorem 7.14 allows us to compute in polynomial time a short GF for the intersection of two finite sets, given their short GFs as input. Since $(R_i \oplus P_i) \cap F$ is the intersection of $(R_i \oplus P_i) \cap \mathbb{Z}^n$ and $F \cap [-N, N]^n$, we can compute

$$h_i(\mathbf{t}) \;=\; \sum_{\mathbf{x} \in (R_i \oplus P_i) \cap F} \mathbf{t}^{\mathbf{x}} \;=\; \left(\sum_{\mathbf{x} \in (R_i \oplus P_i) \cap \mathbb{Z}^n} \mathbf{t}^{\mathbf{x}} \right) \star \left(\sum_{\mathbf{x} \in F \cap [-N, N]^n} \mathbf{t}^{\mathbf{x}} \right) \;=\; g_i(\mathbf{t}) \star f_N(\mathbf{t}).$$

in time $\mathrm{poly}(\mu(F, N))$. Here $\star$ is the *Hadamard product* of two power series (see Definition 7.9). The short GF $f_N(\mathbf{t})$ is obtained by a single call to the oracle in time $\mu(F, N)$. This completes the proof. □

Remark 6.20. We emphasize that Theorem 6.19 does not directly compute the GF $f(\mathbf{t})$ in polynomial time, for a general F. It only claims that $f(\mathbf{t})$ can be computed in time $\mathrm{poly}\big(\mu(F, N)\big)$ given the oracle. In fact, computing $f(\mathbf{t})$ directly from F is an NP-hard problem, even for $F \in \mathrm{PA}_{2,(1,1)}$ (Theorem 7.23).

6.5. The k-feasibility problem

We present an application of Theorem 6.19. Let n, d and k be fixed integers and $A \in \mathbb{Z}^{d \times n}$. In [ADL16], the authors defined a set $\mathrm{Sg}_{\ge k}(A) \in \mathbb{Z}^d$ of *k-feasible* vectors as

$$\mathrm{Sg}_{\ge k}(A) = \{\mathbf{y} \in \mathbb{Z}^d \,:\, \exists \mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{N}^n,\ \mathbf{y} = A\mathbf{x}_j,\ \mathbf{x}_i \ne \mathbf{x}_j \text{ if } i \ne j,\ 1 \le i, j \le k\}. \quad (6.24)$$

In other words, $\mathrm{Sg}_{\geq k}(A)$ consists of vectors that are representable in at least k different ways as a non-negative combination of columns of A. In addition to some results about $\mathrm{Sg}_{\geq k}(A)$, the authors also gave an algorithm to compute a short GF for $\mathrm{Sg}_{\geq k}(A)$ within a finite box:

Theorem 6.21 ([ADL16, Th. 5])**.** *Fix n, d and k. Let $A \in \mathbb{Z}^{d\times n}$, and let N be a positive integer. Let*

$$f_N(\mathbf{t}) = \sum_{\mathbf{x} \in \mathrm{Sg}_{\geq k}(A)\cap[-N,N]^d} \mathbf{t}^{\mathbf{x}}$$

be the partial GF for $\mathrm{Sg}_{\geq k}(A)$ within the box $[-N, N]^d$. Then there is a polynomial time algorithm to compute $f_N(\mathbf{t})$ as a short GF.

Using Theorem 6.19, we can extend Theorem 6.21 as follows:

Theorem 6.22. *Fix n, d and k. Then there is a polynomial time algorithm to compute*

$$f(\mathbf{t}) = \sum_{\mathbf{x} \in \mathrm{Sg}_{\geq k}(A)} \mathbf{t}^{\mathbf{x}}$$

for the entire set $\mathrm{Sg}_{\geq k}(A)$, as a short GF.

Proof. From the definition (6.24), we see that $\mathrm{Sg}_{\geq k}(A)$ is a PA formula in the variables $\mathbf{y}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k$ with only an existential quantifiers. Indeed, each condition $\mathbf{y} = A\mathbf{x}_j$ is a system of $2d$ inequalities. Each condition $\mathbf{x}_i \neq \mathbf{x}_j$ is a disjunction of $2n$ inequalities $(x_{it} < x_{jt})$ or $(x_{it} > x_{jt})$ for $1 \leq t \leq n$. Therefore, we have $\mathrm{Sg}_{\geq k}(A) \in \mathrm{PA}_{k+1,\overline{n}}$, where $\overline{n} = (d, n, \ldots, n)$.

Applying Theorem 6.19, we can compute in polynomial time a short GF $f(\mathbf{t})$ for $\mathrm{Sg}_{\geq k}(A)$ given the partial short GF $f_N(\mathbf{t})$. Finally, Theorem 6.21 allows us to compute $f_N(\mathbf{t})$ in polynomial time. □

Theorem 6.21 was stated in [ADL16] for fixed n and k, but arbitrary d. The following result is a straightforward consequence of the previous theorem and an argument by P. van Emde Boas described in [Len83, §4].

Theorem 6.23. *Fix n and k, but let d be arbitrary. Then there is a polynomial time algorithm to compute*

$$f(\mathbf{t}) = \sum_{\mathbf{x} \in \mathrm{Sg}_{\geq k}(A)} \mathbf{t}^{\mathbf{x}}$$

for the entire set $\mathrm{Sg}_{\geq k}(A)$*, as a short GF.*

Proof. This can be easily reduced to the case when d is also fixed. Indeed, let $\mathcal{L}_A \subseteq \mathbb{Z}^d$ be the lattice generated by the n columns of $A \in \mathbb{Z}^{d\times n}$. We have $\mathrm{rank}(\mathcal{L}_A) = \mathrm{rank}(A) \leq n$. Hence, we can find a $d \times d$ unimodular matrix U so that UA is non-zero only in the first n rows. Let $B \in \mathbb{Z}^{n\times n}$ be the first n rows of UA, and $\mathcal{L}_B$ be the lattice generated by the columns of B. Observe that $\mathcal{L}_B$ and $\mathcal{L}_A$ are isomorphic. Therefore, the set of k-representable vectors in $\mathcal{L}_A$ are in bijection with those in $\mathcal{L}_B$. Now we apply Theorem 6.22 to get a short GF $g(\mathbf{t})$ for $\mathrm{Sg}_{\geq k}(B)$. Finally, the GF for $\mathrm{Sg}_{\geq k}(A)$ is easily obtained from $g(\mathbf{t})$ by a variable substitution via U^{-1}. □

6.6. Final remarks

6.6.A. To summarize, we extended the Barvinok–Woods algorithm to compute short GFs for projections of polyhedra. The result fills a gap in the literature on parametric Integer Programming which remained open since 2003. We also proved a structural result on the projection of semilinear sets by a direct argument. Let us emphasize that we get effective polynomial bounds for the number of polyhedral pieces and the facet complexity of each piece in the projection, but not on the complexity of the pattern within each piece.

6.6.B. The study of semilinear sets has numerous applications in computer science, such as analysis of *number decision diagrams* (see [Ler05]), and *context-free languages* (see [Par66]). We refer to [Gi66] for background on semilinear sets with their connections to Presburger Arithmetic, and to [CH16] for most recent developments.

6.6.C. Without the extra condition $T(Q) \subseteq \mathbb{R}^n_+$ in Theorem 6.2 we can still treat the GF of $T(Q \cap \mathbb{Z}^m)$ as formal power series. In some cases, this power series might not converge under numerical substitutions. For example, if $Q = \mathbb{R}^m$ and T projects $\mathbb{Z}^m$ onto $\mathbb{Z}$, then

every $y \in \mathbb{Z}$ lies in $T(Q \cap \mathbb{Z}^m)$. In this case, we have

$$\sum_{y \in T(Q \cap \mathbb{Z}^m)} t^y \;=\; \ldots + t^{-2} + t^{-1} + 1 + t + t^2 + \ldots,$$

which is not convergent for any non-zero t. However, when $T(Q)$ has a pointed characteristic cone, for example $T(Q) \subseteq \mathbb{R}^n_+$, then the power series converges on a non-empty open domain. For any $\mathbf{t}$ in that domain, the power series converges to the computed rational function $g(\mathbf{t})$. For the general case when $T(Q)$ could possibly contain infinite lines, we can resort to the theory of valuations (see [Bar08, BP99]) to make sense of the GF. Alternatively, one can always decompose any such Q into a finite union of at most $n+1$ polyhedra Q_i, each of which projects within a pointed cone in $\mathbb{R}^n$. Then the GF for the projection of $Q \cap \mathbb{Z}^m$ can be thought of as a formal sum of at most $n+1$ short GFs, each with its own domain of convergence and a rational representation $g_i(\mathbf{t})$.

6.6.D. Our generalization of the Barvinok–Woods theorem also simplifies many existing proofs in the literature when one needs to compute a short generating function for unbounded sets. See for example the computation of Hilbert series in [BW03, Sec. 7.3] and the computation of optimal points for Integer Programming in [HS07, Lem. 3.3].

CHAPTER 7

Complexity of short generating functions

We give complexity analysis for the class of *short generating functions* (short GFs). Assuming $\#\mathsf{P} \not\subseteq \mathsf{FP}/\mathsf{poly}$, we show that this class is not closed under taking many intersections, unions or projections of GFs, in the sense that these operations can increase the binary length of coefficients of GFs by a super-polynomial factor. We also prove that *truncated theta functions* are hard in this class. This chapter is a version of the published paper [NP17d].

7.1. Introduction

7.1.A. Combinatorics and complexity of GFs. A univariate *short generating function* (short GF) is a rational generating function written in the form

$$f(t) \,=\, \sum_{i=1}^{M} \frac{c_i\, t^{a_i}}{(1-t^{b_{i\,1}})\cdots(1-t^{b_{i\,k_i}})}\,, \qquad (*)$$

where $c_i = p_i/q_i \in \mathbb{Q}$, $a_i, b_{ij} \in \mathbb{Z}$ and $b_{ij} \neq 0$ for all i, j. The $\operatorname{index}(f) \coloneqq \max\{k_1, \ldots, k_M\}$ is the maximum number of terms in the denominators. This is always assumed to be bounded by some constant. The *length* $\ell(f)$ is defined as the total binary length of all constants a_i, c_i and b_{ij} in $(*)$. Of course, the same rational generating function f can have many presentations as a short GF.[1]

In this chapter we study of complexity of short GFs with bounded index and polynomial lengths. For a finite set $S \subset \mathbb{N}$, denote by $f_S(t) = \sum_{n\in S} t^n$ the GF of S. We are interested in deciding if it is possible to write f_S as a short GF with polynomial length for a variety of

[1] We also caution the reader that in general, the word *short* in "short GF" only means that the GF is given in the form $(*)$. It does not necessarily mean the GF has polynomial length.

sets S coming from Combinatorics, Number Theory and Discrete Geometry. Showing that some sets do not have short GFs of polynomial lengths turns out to be a surprisingly difficult problem. We are also interested in operations on short GFs and how they affect the short GFs' lengths.

Our approach is motivated by ideas from the study of integer points in convex polyhedra in fixed dimension (see §7.11.A). All such polyhedra turn out to have (multivariate) short GFs of polynomial lengths (see Barvinok's Theorem 7.20 and Chapter 6). We refer to [Bar06b, Bar08] for a thorough review of past and recent work on short GFs in Discrete Geometry, and to Section 7.11 for connections to Arithmetic Combinatorics and other areas.

7.1.B. Squares. Define the *truncated theta function* to be the GF over squares $\leq 2^r$:

$$\vartheta_r(t) \,=\, \sum_{n=0}^{2^{r/2}} t^{n^2} \,.$$

Conjecture 7.1 (=Conjecture 7.56)**.** *For every fixed $k \geq 1$, the truncated theta function $\vartheta_r(t)$* cannot *be written a short GF of length* $\mathrm{poly}(r)$ *and* $\mathrm{index}(\vartheta_r) \leq k$.

The following result is the most surprising in this chapter:

Theorem 7.2 (=Theorem 7.58)**.** *If $\#\mathsf{P} \not\subseteq \mathsf{FP}/\mathsf{poly}$, then Conjecture 7.1 holds.*

To put this in plain words, if truncated theta functions can be represented as short GFs of polynomial lengths and bounded index, then any $\#\mathsf{P}$ counting problem (e.g. number of Hamiltonian cycles) can be solved with polynomial size Boolean circuits. See §7.11.E for more on the complexity assumption, and Section 7.8 for the related results on primes.

7.1.C. One variable operations. Recall that we only consider GFs of finite sets. We define operations on GFs based on their supports. For example, taking the union of two GFs $f(t)$ and $g(t)$ means finding another GF $h(t)$ with $\mathrm{supp}(h) = \mathrm{supp}(f) \cup \mathrm{supp}(g)$. We can similarly define other Boolean operations.

Short GFs are known to be very versatile and useful in applications. Notably, given a bounded number of short GFs, it is known how to perform all Boolean operations on in

polynomial time (Theorem 7.14). The result is again a short GF with polynomial length. However, when the number of short GFs is large, no such polynomial time procedures are known. The following result gives a strong evidence against such possibility:

Theorem 7.3 (=Theorem 7.52)**.** *If* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$*, then taking intersection/union of many short GFs does not preserve polynomiality in length.*

This says taking union of many short GFs is hard structurally. It should be compared to an earlier result by Woods, which says that taking union of many short GFs is hard algorithmically, assuming $\mathsf{P} \neq \mathsf{NP}$ (see Theorem 7.23 and the following remark).

Next, define the *Minkowski sum* $f \oplus g$ of two GFs $f(t)$ and $g(t)$, to be the GF $h(t)$ with $\operatorname{supp}(h) = \operatorname{supp}(f) \oplus \operatorname{supp}(g) = \{a + b \mid a \in \operatorname{supp}(f), b \in \operatorname{supp}(g)\}$.

Theorem 7.4 (=Theorem 7.55)**.** *If* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$*, then taking Minkowski sum of* two *short GFs does not preserve polynomiality in length.*

Giving precise formulations of these results requires some effort, see Section 7.7. Let us mention that in both theorems we can substitute the complexity assumptions with Conjecture 7.1. These results show strong limitations of the "short GF technology" from a geometric point of view (see §7.11.A). Below we give further evidence of this phenomenon.

7.1.D. Projections. For multivariate short GFs, taking projections is a key operation. Projection is crucial for applications such as Integer Programming (see Section 6.1), and theoretical considerations such as Presburger Arithmetic (see Section 6.4). In a crucial development, Barvinok and Woods [BW03] showed that given a polytope P in bounded dimension, the projections of its integer points on some subspace have a short GF of polynomial length, which can also be computed in polynomial time (Theorem 6.14). This result exploited the polytopal structure of P and its convexity in a crucial way. Unfortunately, these are also the reasons that prevent their result to apply on a non-geometric level. In other words, the algorithm by Barvinok and Woods cannot produce a short GF for the projections if the input is presented only as short GF, without a polytope associated to it.

An important negative result by Woods in fact shows that given only a multivariate short GF $f(\mathbf{t})$, computing its projection is NP-hard (see Theorem 7.23 and the Remark 7.24). The following theorem is the central result of the chapter. Roughly speaking, it both weakens the assumptions and strengthens the conclusions of Woods's theorem.

Theorem 7.5 (=Corollary 7.48)**.** *If* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$*, then taking projection of a short GF does not preserve polynomiality in length.*

This says that in general not only we cannot *compute* the projection of a short GF in polynomial time, any short GF that represents the projection must have a super-polynomial length. In other words, the barriers of using the "short GF technology" in this case are structural rather than algorithmic.

The next result can be viewed as a refinement of the previous theorem, giving a precise characterization of complexity of projections.

Theorem 7.6 (=Theorem 7.46)**.** *Repeated projections of short GFs can encode every language in the non-uniform polynomial hierarchy* $\mathsf{PH/poly}$*. In fact, they form a hierarchy that coincides with* $\mathsf{PH/poly}$*.*

We postpone the precise formulations of these results, especially of Theorem 7.6 where the technicalities are unavoidable. Let us also mention Proposition 7.49 which can be viewed as a partial converse of Theorem 7.5.[2]

7.1.E. Structure of the chapter. Our results are largely self-contained and require little more than a few technical lemmas from [BP99], which are all stated in Section 7.2 and can be treated as black boxes. We do however employ a fair amount of definitions and notations (Section 7.2).

Our Section 7.3 is the key as it describes the connection between languages and short GFs. From this point on, the reader can proceed to the development of the short GF hierarchy,

[2]By itself, Conjecture 7.1 does not necessarily imply that $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$, so a stronger assumption is used in Proposition 7.49.

culminating in the proofs of theorems 7.5 and 7.6 (sections 7.4–7.6). Alternatively, modulo a few definitions in earlier section, the reader proceed directly to the proof of theorems 7.3 and 7.4 in Section 7.7. Similarly, the reader can also proceed to study complexity of squares and primes (Section 7.8). In Section 7.9 we investigate more technical questions on relative complexity of short GFs, and in Section 7.10 we give a proof of a technical Lemma 7.34. We conclude with final remarks and open problems in Section 7.11.

7.2. Preliminaries on short GFs

7.2.A. Polynomial time operations. A power series $f(\mathbf{t}) = \sum \alpha_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ is called a GF if each coefficient $\alpha_{\mathbf{x}}$ is either 0 or 1. When needed, we will write $f(\mathbf{t}) = \sum \mathbf{t}^{\mathbf{x}}$ to emphasize that f is a GF.

Definition 7.7. The support of an n-variable GF $g(\mathbf{t}) = \sum \mathbf{t}^{\mathbf{x}}$ is defined as:

$$\operatorname{supp}(g) \coloneqq \{\mathbf{x} \in \mathbb{Z}^n : [\mathbf{t}^{\mathbf{x}}]g(\mathbf{t}) = 1\}.$$

Here $[\mathbf{t}^{\mathbf{x}}]$ denotes the coefficient of the monomial $\mathbf{t}^{\mathbf{x}}$ in $g(\mathbf{t})$.

Definition 7.8. Given a multi-variable GF $f(\mathbf{t}, \mathbf{u}) = \sum \mathbf{t}^{\mathbf{x}}\mathbf{u}^{\mathbf{y}}$ with $\mathbf{x} \in \mathbb{Z}^m, \mathbf{y} \in \mathbb{Z}^n$, the $\mathbf{x}$-*projection* $g = \operatorname{proj}_{\mathbf{x}}(f)$ is the unique GF $g(\mathbf{t}) = \sum \mathbf{t}^{\mathbf{x}}$ with support satisfying

$$\operatorname{supp}(g) = \{\mathbf{x} \in \mathbb{Z}^m : \exists\, \mathbf{y} \in \mathbb{Z}^n \;\; (\mathbf{x}, \mathbf{y}) \in \operatorname{supp}(f)\}.$$

If f satisfies the extra property that for every $\mathbf{x} \in \mathbb{Z}^m$ there is at most one $\mathbf{y} \in \mathbb{Z}^n$ such that $(\mathbf{x}, \mathbf{y}) \in \operatorname{supp}(f)$, then $\operatorname{proj}_{\mathbf{x}}(f)$ is called the $\mathbf{x}$-*specialization* of f, denoted by $\operatorname{spec}_{\mathbf{x}}(f)$.

Definition 7.9. Consider two power series $f(\mathbf{t}) = \sum \alpha_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ and $g(\mathbf{t}) = \sum \beta_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$. The *Hadamard product* of f and g, denoted by $f \star g$, is another GF $h(\mathbf{t}) = \sum \gamma_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ with

$$\gamma_{\mathbf{x}} = \alpha_{\mathbf{x}}\, \beta_{\mathbf{x}} \;\text{ for every } \mathbf{x}.$$

If f and g are GFs then the above condition is equivalent to $\operatorname{supp}(h) = \operatorname{supp}(f) \cap \operatorname{supp}(g)$.

Definition 7.10. For a rational function in n variables $\mathbf{t} = (t_1, \ldots, t_n)$ of the form

$$f(\mathbf{t}) \;=\; \sum_{i=1}^{M} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1 - \mathbf{t}^{\overline{b}_{i1}}) \cdots (1 - \mathbf{t}^{\overline{b}_{ik_i}})}, \tag{$\divideontimes$}$$

the length $\ell(f)$ of f is defined as

$$\ell(f) \;=\; \sum_{i} \lceil \log_2 |p_i\, q_i| + 1 \rceil \;+\; \sum_{i,j} \lceil \log_2 a_{ij} + 1 \rceil \;+\; \sum_{i,j,m} \lceil \log_2 b_{ijm} + 1 \rceil,$$

where $c_i = p_i/q_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$, $\overline{b}_{ij} \neq 0$ and $\mathbf{t}^{\overline{a}} = t_1^{a_1} \cdots t_n^{a_n}$ if $\overline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$.

Definition 7.11. For a power series $f(\mathbf{t}) = \sum \alpha_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ given in the form ($\divideontimes$), the *index* of f is defined as

$$\text{index}(f) = \max\{k_i \;:\; i = 1, \ldots, M\},$$

where k_i is the number of factors in the denominator of the i-th summand.

Definition 7.12. For every number of variables n and integer s, we define two classes:

$$\mathcal{GF}_{n,s} = \big\{\text{GFs } g(\mathbf{t}) \text{ given in the form } (\divideontimes) \text{ with ind} g \leq s\big\} \tag{7.1}$$

and

$$\mathcal{GF}^*_{n,s} = \big\{\text{power series } g(\mathbf{t}) \text{ given in the form } (\divideontimes) \text{ with ind} g \leq s\big\}. \tag{7.2}$$

Members of $\mathcal{GF}_{n,s}$ are called *short GFs*, while those of $\mathcal{GF}^*_{n,s}$ are called *short power series*.

We recall the following important results from [BP99] (see also [BW03]):

Theorem 7.13 ([BP99])**.** *Fix a class $\mathcal{GF}_{m,s}$. Given a short GF $f(\mathbf{t}) \in \mathcal{GF}_{m,s}$ of finite support. We can compute in time* $\text{poly}(\ell(f))$ *the following:*

1) *The norm* $N = \max\{|\mathbf{x}| : \mathbf{x} \in \text{supp}(f)\}$,[3]

2) *The cardinality* $M = |\text{supp}(f)|$, *which is equal to* $f(1)$,

3) *The substitution* $q(\mathbf{u}) = f(\mathbf{t}(\mathbf{u}))$, *where* $\mathbf{t}$ *is substituted by monomials in some other variables* $\mathbf{u} = (u_1, \ldots, u_n)$. *Furthermore, we have* $q(\mathbf{u}) \in \mathcal{GF}^*_{n,s}$.

[3] *Here* $|\mathbf{x}|$ *can be any polyhedral norm on* $\mathbf{x}$, *including* $|\mathbf{x}|_\infty$ *and* $|\mathbf{x}|_1$.

Theorem 7.14 ([BP99]). *Fix two classes $\mathcal{GF}_{m,s_1}$ and $\mathcal{GF}_{m,s_2}$. Given $f(\mathbf{t}) \in \mathcal{GF}_{m,s_1}$ and $g(\mathbf{t}) \in \mathcal{GF}_{m,s_2}$ of finite supports, we can compute in time* $\mathrm{poly}(\ell(f)+\ell(g))$ *the following:*

1) *A short GF $h(\mathbf{t})$ with* $\mathrm{supp}(h) = \mathrm{supp}(f) \cap \mathrm{supp}(g)$, *i.e., $h(\mathbf{t}) = f(\mathbf{t}) \star g(\mathbf{t})$,*

2) *A short GF $k(\mathbf{t})$ with* $\mathrm{supp}(k) = \mathrm{supp}(f) \cup \mathrm{supp}(g)$.

3) *A short GF $p(\mathbf{t})$ with* $\mathrm{supp}(p) = \mathrm{supp}(f) \backslash \mathrm{supp}(g)$.

Moreover, we have $h, k, p \in \mathcal{GF}_{m,s_1+s_2}$.

Remark 7.15. In fact, a more general version of Theorem 7.14 part 1) was shown in [BP99], which also allows taking $f \star g$ for short power series.

The following is the reason why we emphasized the bounded dimension n and index s in Definition 7.12.

Proposition 7.16. *Fix n and s. Given a short power series $f(\mathbf{t}) = \sum \beta_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ in $\mathcal{GF}_{n,s}$ and a vector $\overline{a}_0 \in \mathbb{Z}^n$, the coefficient $\beta_{\overline{a}_0}$ can be computed in time* $\mathrm{poly}(\ell(f)+\ell(\overline{a}_0))$.

Proof. We let $g(\mathbf{t}) = \mathbf{t}^{\overline{a}_0}$ and define $h(\mathbf{t}) = f(\mathbf{t}) \star g(\mathbf{t})$. Clearly, we have $h(\mathbf{t}) = \beta_{\overline{a}_0} \mathbf{t}^{\overline{a}_0}$, which implies $\beta_{\overline{a}_0} = h(1)$. Applying Theorem 7.14, we can compute $h(\mathbf{t})$ (see also Remark 7.15). By Theorem 7.13, we can compute $h(1)$. All can be done in time $\mathrm{poly}(\ell(f)+\ell(\overline{a}_0))$. □

Remark 7.17. A similar result for n and s unbounded is unlikely to hold, considering the fact that Knapsack is NP-complete. An instance of Knapsack asks if an equation $a = \overline{b}\,\mathbf{x}$ is solvable, where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{N}$ are variables, and $a \in \mathbb{N}, \overline{b} \in \mathbb{N}^n$ are given as input. This is equivalent to checking if $[t^a]f \neq 0$, where:

$$f(t) = \frac{1}{(1-t^{b_1}) \cdots (1-t^{b_n})}.$$

Here n is not bounded. Note that Knapsack has a polynomial time algorithm if a and $\overline{b}$ are given in unary. In our case, short GFs are encoded in binary.

If f is a short GF, Proposition 7.16 allows us to decide in polynomial time whether $\overline{a}_0 \in \mathrm{supp}(f)$. Now one may ask whether is it still easy to decide if a point $\overline{a}_0$ lies in a projection of f . The answer is still positive:

Proposition 7.18. *Fix m, n and s. Given a short GF $f(\mathbf{t}, \mathbf{u}) = \sum \mathbf{t}^{\mathbf{x}}\mathbf{u}^{\mathbf{y}} \in \mathcal{GF}_{m+n,s}$ of finite support and a vector $\overline{a}_0 \in \mathbb{Z}^m$, checking whether $\overline{a}_0 \in \text{supp}(\text{proj}_{\mathbf{x}}(f))$ can be done in time $\text{poly}(\ell(f) + \ell(\overline{a}_0))$. Here $\mathbf{x} \in \mathbb{Z}^m, \mathbf{y} \in \mathbb{Z}^n$.*

Proof. Let $g(\mathbf{t}) = f(\mathbf{t}, 1)$. Clearly, we have $\overline{a}_0 \in \text{supp}(\text{proj}_{\mathbf{x}}(f))$ if and only if the coefficient of $\mathbf{t}^{\overline{a}_0}$ in $g(\mathbf{t})$ is non-zero. By Theorem 7.13, we can compute g in time $\text{poly}(\ell(f))$. By Proposition 7.16, we can compute $[\mathbf{t}^{\overline{a}_0}]g$ in time $\text{poly}(\ell(g) + \ell(\overline{a}_0)) \leq \text{poly}(\ell(f) + \ell(\overline{a}_0))$. □

7.2.B. Short GFs and Presburger formulas. We summarize known results relating short GFs to Presburger formulas. Recall the definition of PA formulas from Section 6.4.

Definition 7.19. For a set $S \subseteq \mathbb{Z}^n$, denote by $\mathbf{F}(S; \mathbf{t})$ the GF

$$\mathbf{F}(S; \mathbf{t}) \coloneqq \sum_{\mathbf{x} \in S} \mathbf{t}^{\mathbf{x}}.$$

Theorem 6.1 by Barvinok can be restated as:

Theorem 7.20 ([Bar93])**.** *Fix n. Let $P \subseteq \mathbb{R}^n$ be a rational polyhedron described by $A\mathbf{x} \leq \overline{b}$. Then we can compute in time $\text{poly}(\ell(Q))$ a short GF $f(\mathbf{t}) = \mathbf{F}(P \cap \mathbb{Z}^n; \mathbf{t})$ with $f \in \mathcal{GF}_{n,n}$.*

A generalization of this to all quantifier-free PA formulas is:

Theorem 7.21 ([Woo04, Prop. 5.3.1])**.** *Fix n. Let $G = \{\mathbf{x} \in \mathbb{Z}^n : \Phi(\mathbf{x})\}$ be quantifier-free PA formula, with Φ a Boolean combination of linear inequalities in $\mathbf{x}$. Then we can compute in time $\text{poly}(\ell(\Phi))$ a short GF $g(\mathbf{t}) = \mathbf{F}(G; \mathbf{t})$ with $g \in \mathcal{GF}_{n,n}$.*

Proof. By Proposition 6.18, we can rewrite Φ as a disjoint union of polyhedra $P_1, \ldots, P_r$ with $r \leq \text{poly}(\ell(\Phi))$. The system defining each P_i can be computed in polynomial time. Applying Theorem 7.20, we get a short GF $f_i \in \mathcal{GF}_{n,n}$ of polynomial length for each P_i. Summing up all f_i, we get a short GF $g \in \mathcal{GF}_{n,n}$ of length $\text{poly}(\ell(\Phi))$ for G. □

Next, we consider PA formulas with quantifiers. In the simplest case, an existential formula F encodes the projection of integer points in a polyhedron.

Theorem 7.22 (Th. 6.2 restated)**.** *Fix $m, n \in \mathbb{N}$. Let $Q \subseteq \mathbb{R}^m$ be a rational polyhedron given by a system $A\mathbf{x} \leq \overline{b}$, and $T : \mathbb{Z}^m \to \mathbb{Z}^n$ a linear map. Consider the PA formula*

$$G = \left\{\mathbf{y} \in \mathbb{Z}^n \,:\, \exists \mathbf{x} \in \mathbb{Z}^m \,(\mathbf{x} \in Q) \wedge (\mathbf{y} = T\mathbf{x})\right\}.$$

Then we can compute in time $\mathrm{poly}(\ell(Q) + \ell(T))$ *a short GF $g(\mathbf{t}) = \mathbf{F}(G; \mathbf{t})$. Furthermore, we have $g \in \mathcal{GF}_{n,s}$, where $s = s(m)$ is a constant.*

However, for general $\exists$ PA formulas, finding short GFs becomes hard:

Theorem 7.23 ([Woo04, Th. 5.3.2])**.** *Let $\Phi(x, y)$ be a quantifier-free Boolean combination of linear inequalities in x and y (singletons). Let $F = \{y \in \mathbb{Z} : \exists x \in \mathbb{Z} \;\; \Phi(x, y)\}$. Then computing a short GF for F is* NP*-hard.*

Remark 7.24. By Theorem 7.21, we still can find a short GF of length $\mathrm{poly}(\ell(\Phi))$ for $\Phi(x, y)$. So this result says that projecting a short GF is hard algorithmically. This should be compared to our Theorem 7.5, which says that projecting short GF is hard structurally. Actually, by Proposition 6.18, we can also decompose $\Phi(x, y)$ into a union of polynomially many polygons $P_i \subseteq \mathbb{R}^2$. By Theorem 7.22, the projection of integer points in each P_i on x has a short GF, which can be found in polynomial time. So taking union of these short GFs is again hard algorithmically. This should be compared to Theorem 7.3.

7.3. Short GFs and the class P/poly

7.3.A. Encoding languages in P/poly as short GFs. For technical reasons regarding the convergence of GFs under numerical evaluation, we consider only GFs with support in $\mathbb{N}^n$ from this section onwards. Theorem 7.14 still applies to short GFs supported on $\mathbb{N}^n$.

Definition 7.25. For every language $\mathcal{L} \in \{0, 1\}^*$, and every $r > 0$, we denote by $\mathcal{L}_r$ the segment

$$\mathcal{L}_r \coloneqq \left\{\widetilde{x} \in \{0, 1\}^r : \widetilde{x} \in \mathcal{L}\right\}. \tag{7.3}$$

For $\widetilde{x} \in \mathcal{L}_r$, let x be the corresponding integer with binary representation $\widetilde{x}$. We will also use $\mathcal{L}_r$ to denote the set of all such x with $\widetilde{x} \in \mathcal{L}_r$.

Lemma 7.26. *For every language $\mathcal{L} \in \mathsf{P/poly}$, and every $r > 0$, the segment $\mathcal{L}_r$ can be characterized in PA as:*

$$\widetilde{x} \in \mathcal{L}_r \quad \Longleftrightarrow \quad x \in [0, 2^r) \wedge \big[\exists y \in [0, 2^p)\ \forall \mathbf{z} \in [0, 2^q)^3 : \Phi_r(x, y, \mathbf{z})\big], \tag{7.4}$$

where Φ_r is a quantifier-free PA expression in $x, y \in \mathbb{N}$ and $\mathbf{z} \in \mathbb{N}^3$. Moreover, we have $p, q, \ell(\Phi_r) \leq \mathrm{poly}_{\mathcal{L}}(r)$.[4] *If in addition $\mathcal{L} \in \mathsf{P}$, then there is an algorithm to compute p, q and Φ_r in time $\mathrm{poly}_{\mathcal{L}}(r)$.*

Proof. By definition of the class $\mathsf{P/poly}$, there is a Boolean circuit C_r such that:

$$\mathcal{L}_r = \{\widetilde{x} \in \{0,1\}^r \,:\, C_r(\widetilde{x}) = \text{true}\}.$$

Here the circuit C_r has r input gates, and as many as $p \leq \mathrm{poly}_{\mathcal{L}}(r)$ non-input gates, each with in-degree at most two. We encode the values of the non-input gates as a Boolean string $\widetilde{y} \in \{0,1\}^p$. Let $\widetilde{x} = (x_1, \ldots, x_r)$ and $\widetilde{y} = (y_1, \ldots, y_p)$. By a standard reduction (see e.g. [MM11, Pap94]), we can encode the computation of C_r by a Boolean formula F in 3-Conjunctive Normal Form. Explicitly, we have:

$$\mathcal{L}_r = \{\widetilde{x} \in \{0,1\}^r \,:\, \exists \widetilde{y} \in \{0,1\}^p\ F(\widetilde{x}, \widetilde{y}) = \text{true}\}, \tag{7.5}$$

where

$$F(\widetilde{x}, \widetilde{y}) \;=\; \bigwedge_k (a_k \vee b_k \vee c_k). \tag{7.6}$$

Here each a_k, b_k, c_k is a literal in the set $\{x_i, \neg x_i,\, y_j, \neg y_j \,:\, 1 \leq i \leq r,\, 1 \leq j \leq p\}$.

Let $x \in [0, 2^r)$ and $y \in [0, 2^p)$ be the integers corresponding to $\widetilde{x}$ and $\widetilde{y}$, respectively. Every literal x_i corresponds to the i-th digit in x being 1, and $\neg x_i$ corresponds that digit being 0.[5] In other words, x_i is true or false respectively when $\lfloor x/2^{i-1} \rfloor$ is odd or even. The same applies to y_i and y. Observe that $t = \lfloor x/2^{i-1} \rfloor$ is the only integer that satisfies $x/2^{i-1} - 1 < t \leq x/2^{i-1}$. Let $q = \max(r, p) \leq \mathrm{poly}(r)$. Each term x_i or $\neg x_i$ can be coded with an extra $\exists z$ quantifier as follows:

[4] *We denote by $\ell(\Phi_r)$ the total length of all symbols Φ_r, written in binary. The notation $\mathrm{poly}_{\mathcal{L}}(r)$ denotes a polynomial in r, with the polynomial degree depending on the language $\mathcal{L}$.*

[5] The least significant digit in x corresponds to x_0 in $\widetilde{x}$.

$$
\begin{aligned}
x_i &\iff \exists z \in [0, 2^q) : \begin{Bmatrix} 2z+1 & > & x/2^{i-1} - 1 \\ 2z+1 & \leq & x/2^{i-1} \end{Bmatrix}, \\
\neg x_i &\iff \exists z \in [0, 2^q) : \begin{Bmatrix} 2z & > & x/2^{i-1} - 1 \\ 2z & \leq & x/2^{i-1} \end{Bmatrix}.
\end{aligned} \tag{7.7}
$$

Here $\{\cdot\}$ denotes a system (conjunction) of inequalities. Analogously, each y_j or $\neg y_j$ can be coded using $\exists z$. Note that the two strict inequalities in (7.7) can be sharpened by multiplying both sides with 2^{i-1} to make all coefficients integer, and add 1 to the RHS.

Now we show how to code (7.6) using $\forall \mathbf{z}$ with $\mathbf{z} \in \mathbb{N}^3$. For each clause $(a_k \vee b_k \vee c_k)$, we consider its negation $(\neg a_k \wedge \neg b_k \wedge \neg c_k)$. Each term $\neg a_k, \neg b_k, \neg c_k$ is still one of $x_i, \neg x_i, y_i, \neg y_i$. By (7.7), we have

$$
(\neg a_k \wedge \neg b_k \wedge \neg c_k) \quad \iff \quad \exists \mathbf{z} \in [0, 2^q)^3 : \Phi_k(x, y, \mathbf{z}),
$$

where $\mathbf{z} \in \mathbb{N}^3$, and Φ_k is a conjunction of 6 inequalities. Taking negation, we have:

$$
\begin{aligned}
(a_k \vee b_k \vee c_k) \quad &\iff \quad \forall \mathbf{z} \in [0, 2^q)^3 : \neg \Phi_k(x, y, \mathbf{z}), \\
&\iff \quad \forall \mathbf{z} \in [0, 2^q)^3 : \Psi_k(x, y, \mathbf{z}),
\end{aligned}
$$

where Ψ_k is a disjunction of 6 inequalities. Taking conjunction over all k in (7.6), we have:

$$
F(\widetilde{x}, \widetilde{y}) \quad \iff \quad \forall \mathbf{z} \in [0, 2^q)^3 : \Phi_r(x, y, \mathbf{z}), \tag{7.8}
$$

where

$$
\Phi_r(x, y, \mathbf{z}) \ = \ \bigwedge_k \Psi_k(x, y, \mathbf{z}). \tag{7.9}
$$

Substituting (7.8) into (7.5), we have (7.4). If we assume in addition that $\mathcal{L} \in \mathsf{P}$, then the circuit C_r can be built from a Turing Machine in time $\mathrm{poly}_{\mathcal{L}}(r)$, so the expression Φ_r can also be found in time $\mathrm{poly}_{\mathcal{L}}(r)$. This completes the proof. □

Recall that for a set $S \subseteq \mathbb{Z}^n$ we defined $\mathbf{F}(S; \mathbf{t}) := \sum_{\mathbf{x} \in S} \mathbf{t}^{\mathbf{x}}$.

Definition 7.27. Given $f(\mathbf{t}) = \mathbf{F}(S; \mathbf{t})$, where S is a subset of a finite box $B \subset \mathbb{N}^n$. The *finite complement* $B \backslash f$ is $\mathbf{F}(B \backslash S; \mathbf{t})$.

Definition 7.28. Given $f_1(\mathbf{t}) = \mathbf{F}(S_1; \mathbf{t})$, ..., $f_k(\mathbf{t}) = \mathbf{F}(S_k; \mathbf{t})$ with $S_1, \ldots, S_k \subseteq \mathbb{N}^n$, the *intersection* $f_1 \cap \cdots \cap f_k$ is $\mathbf{F}(S_1 \cap \cdots \cap S_k; \mathbf{t})$. The *union* $f_1 \cup \cdots \cup f_k$ is $\mathbf{F}(S_1 \cup \cdots \cup S_k; \mathbf{t})$.

Theorem 7.29. *For every language $\mathcal{L} \in \mathsf{P/poly}$ and $r > 0$, there exist a finite box B_r and short GF $f_r(t, u, \mathbf{v}) \in \mathcal{GF}_{5,5}$ with $\mathrm{supp}(f_r) \subseteq B_r$, so that*

$$\mathbf{F}(\mathcal{L}_r; t) \;=\; \mathrm{spec}_x(B_r \backslash \mathrm{proj}_{x,y}(f_r)) \tag{7.10}$$

and $\ell(B_r)$, $\ell(f_r) \leq \mathrm{poly}_{\mathcal{L}}(r)$.[6] *Furthermore, there exists $p_{r,1}, \ldots, p_{r,k_r} \in \mathcal{GF}_{2,s}$ of finite supports, with $k_r \leq \mathrm{poly}_{\mathcal{L}}(r)$ and $\ell(p_{r,i}) \leq \mathrm{poly}_{\mathcal{L}}(r)$, so that:*

$$\mathrm{proj}_{x,y}(f_r) \;=\; p_{r,1} \cup \cdots \cup p_{r,k_r}. \tag{7.11}$$

Here $\mathcal{GF}_{2,s}$ is some fixed class that does not depend on $\mathcal{L}$. If we assume in addition that $\mathcal{L} \in \mathsf{P}$, then there is also an algorithm to compute B_r, f_r and each $p_{r,i}$ in time $\mathrm{poly}_{\mathcal{L}}(r)$.

Proof. For the notations $\mathrm{proj}, \mathrm{spec}, \cup$ and $\backslash$, we refer back to definitions 7.8, 7.27 and 7.28. By the previous lemma, there is a PA expression Φ_r satisfying (7.4). First, define

$$B_r = \{(x, y) : x \in [0, 2^r),\, y \in [0, 2^p)\},$$
$$D_r = \{(x, y, \mathbf{z}) : x \in [0, 2^r),\, y \in [0, 2^p),\, \mathbf{z} \in [0, 2^q)^3\},$$

where r, p and q are from (7.4). Define:

$$f_r(t, u, \mathbf{v}) \;=\; \sum_{\substack{(x,y,\mathbf{z}) \in D_r \\ \neg\Phi_r(x,y,\mathbf{z})}} t^x\, u^y\, \mathbf{v}^{\mathbf{z}}. \tag{7.12}$$

Recall that Φ_r is a quantifier-free PA expression with length $\mathrm{poly}_{\mathcal{L}}(r)$. Applying Theorem 7.21 to $\neg\Phi_r$, we can write f_r as a short GF in $\mathcal{GF}_{5,5}$ of finite support, which has length $\ell(f_r) \leq \mathrm{poly}(\ell(\Phi_r)) \leq \mathrm{poly}_{\mathcal{L}}(r)$. For the rest of the proof, we always assume $(x, y, \mathbf{z}) \in D_r$. We will simply write $\exists \mathbf{z}$ instead of $\exists \mathbf{z} \in [0, 2^q)^3$. Projecting f_r on (x, y), we have:

$$\mathrm{proj}_{x,y}(f_r) \;=\; \sum_{(x,y)\,:\,\exists \mathbf{z}\, \neg\Phi_r(x,y,\mathbf{z})} t^x u^y. \tag{7.13}$$

[6] *Here $\ell(Br)$ denotes the total bit length of all sides in B_r, written in binary.*

Taking the complement of $\text{proj}_{x,y}(f_r)$, which lies within the box B_r, we have:

$$B_r \backslash \text{proj}_{x,y}(f_r) \;=\; \sum_{(x,y)\,:\,\forall \mathbf{z}\,\Phi_r(x,y,\mathbf{z})} t^x\, u^y. \tag{7.14}$$

Recall that in the proof of Lemma 7.26, the variable y describes the values of non-input gates in the circuit C_r, with input gates coming from x. Since the values of non-input gates are uniquely determined by the input gates, for every x that satisfies C_r we have a unique y. Substituting $u \leftarrow 1$, the RHS in (7.14) becomes $\mathbf{F}(\mathcal{L}_r; t)$. We obtain (7.10).

We proceed to show (7.11). Since $\neg\Phi_r$ is quantifier-free with 5 variables, we can apply Proposition 6.18 on it and get:

$$\neg\Phi_r(x,y,\mathbf{z}) \quad\Longleftrightarrow\quad \bigvee_{i=1}^{k_r} (x,y,\mathbf{z}) \in P_{r,i} \cap \mathbb{N}^5,$$

where $P_{r,1}, \ldots, P_{r,k_r} \subseteq \mathbb{R}^5$ are disjoint polytopes (in the box D_r) and $k_r \le \text{poly}(\ell(\Phi_r)) \le \text{poly}_{\mathcal{L}}(r)$. Each polytope $P_{r,i}$ also satisfies $\ell(P_{r,i}) \le \text{poly}(r)$. Therefore:

$$\exists \mathbf{z}\; \neg\Phi_r(x,y,\mathbf{z}) \quad\Longleftrightarrow\quad \bigvee_{i=1}^{k_r} \exists \mathbf{z}\; \big[(x,y,\mathbf{z}) \in P_{r,i} \cap \mathbb{N}^5\big]. \tag{7.15}$$

Combined with (7.13), we see that $(x,y) \in \text{supp}(\text{proj}_{x,y}(f_r))$ if and only if it lies in the projection of some $P_{r,i} \cap \mathbb{N}^5$. By Theorem 7.22, for each i, we can find a short GF $p_{r,i} \in \mathcal{GF}_{2,s}$ for the projection of $P_{r,i} \cap \mathbb{N}^5$. In other words, we have $p_{r,i} \in \mathcal{GF}_{2,s}$ that satisfies:

$$\text{supp}(p_{r,i}) = \{(x,y) : \exists \mathbf{z}\; (x,y,\mathbf{z}) \in P_{r,i} \cap \mathbb{N}^5\}.$$

Here s is an absolute constant because each $P_{r,i}$ has (fixed) dimension 5. We also have $\ell(p_{r,i}) \le \text{poly}(\ell(P_{r,i})) \le \text{poly}(r)$. The union of all short GFs $p_{r,i}$ contains exactly all (x,y) satisfying (7.15). From (7.13) and (7.15), we have:

$$\text{proj}_{x,y}(f_r) = p_{r,1} \cup \cdots \cup p_{r,k_r}.$$

This proves (7.11) and completes the proof. □

Example 7.30. Since SQUARES and PRIMES are both in P, we can represent all squares or primes up to 2^r in the form (7.10), with f_r and B_r computable in time $\text{poly}(r)$.

Remark 7.31. Even though $\mathrm{spec}_x(B_r \backslash \mathrm{proj}_{x,y}(f_r))$ may seem complicated, the specialization and complement are "inexpensive operations", which can be performed in polynomial time by theorems 7.13 and 7.14. The main complexity resides in taking the projection of f.

Remark 7.32. The same representation (7.10) applies to every language $\mathcal{L}$ in the complexity class $\mathsf{UP/poly}$. Such a language is characterized as follows. For every r, there is a *non-deterministic* polynomial-time Turing machine that accepts only $x \in \mathcal{L}_r$, each with a unique accepting path. Given $\mathcal{L} \in \mathsf{UP/poly}$, we can obtain (7.10) by the same argument as above. In fact, (7.10) is an equivalent characterization of the class $\mathsf{UP/poly}$. Indeed, assume $\mathcal{L}_r$ can be represented as (7.10). Given f_r, for any $x \in \mathcal{L}_r$ there should be a unique certificate y such that $(x, y) \in B_r \backslash \mathrm{proj}_{x,y}(f_r)$, which is checkable in polynomial time by Proposition 7.18.

7.3.B. Compressing short GFs of finite supports. We describe a technical tool which will be useful later. This section can be skipped at first reading.

Definition 7.33. Consider $N = 2^r$ and a vector $\mathbf{x} = (x_1, \ldots, x_d) \in \mathbb{N}^n$ with $x_i \in [0, N)$ for all $1 \le i \le d$. We define the τ_N map on $\mathbf{x}$ as:

$$\tau_N(\mathbf{x}) \;=\; x_1 + Nx_2 + \cdots + N^{n-1}x_d \;\in [0, N^n).$$

For an array of vectors $\overline{\mathbf{x}} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ with $\mathbf{x}_i \in [0, N)^{n_i}$, we define:

$$\tau_N(\overline{\mathbf{x}}) \;=\; (\tau_N(\mathbf{x}_1), \ldots, \tau_N(\mathbf{x}_k)) \;\in\; [0, N^{n_1}) \times \cdots \times [0, N^{n_k}).$$

Finally, for a set $S \subseteq [0, N)^{n_1} \times \cdots \times [0, N)^{n_k}$, we define $\tau_N(S) = \{\tau_N(\overline{\mathbf{x}}) : \overline{\mathbf{x}} \in S\}$.

The following technical tool allows us to reduce the number of variables in a short GF of finite support.

Lemma 7.34. *Fix k, s and $n_1, \ldots, n_k \in \mathbb{N}$. Let $n = n_1 + \ldots + n_k$.*

a) **Compressing**: *Given a short GF $g(\overline{\mathbf{t}}) = \sum \mathbf{t}_1^{\mathbf{x}_1} \ldots \mathbf{t}_k^{\mathbf{x}_k}$ of finite support in the class $\mathcal{GF}_{n,s}$, there exist an $N = 2^r$ with $\mathrm{supp}(g) \subseteq [0, N)^{n_1} \times \cdots \times [0, N)^{n_k}$ and a short GF $f(\mathbf{u}) = \sum u_1^{z_1} \ldots u_k^{z_k}$ in the class $\mathcal{GF}_{k,s}$ so that*

$$\mathrm{supp}(f) = \tau_N(\mathrm{supp}(g)) \;\subseteq\; [0, N^{n_1}) \times \cdots \times [0, N^{n_k}). \tag{7.16}$$

Both f and N can be computed in time $\mathrm{poly}(\ell(g))$ *with* $\ell(f), \log N \le \mathrm{poly}(\ell(g))$.

b) **Decompressing**: *Conversely, given* $f(\mathbf{u}) = \sum u_1^{z_1} \dots u_k^{z_k} \in \mathcal{GF}_{k,s}$ *and* $N = 2^r$ *such that*

$$\mathrm{supp}(f) \ \subseteq \ [0, N^{n_1}) \times \cdots \times [0, N^{n_k}),$$

there exists $g(\overline{\mathbf{t}}) = \sum \mathbf{t}_1^{\mathbf{x}_1} \dots \mathbf{t}_k^{\mathbf{x}_k} \in \mathcal{GF}_{n,n+s}$ *with* $\mathrm{supp}(g) \subseteq [0, N)^{n_1} \times \cdots \times [0, N)^{n_k}$ *which satisfies* (7.16). *The short GF g can be computed in time* $\mathrm{poly}(\ell(f) + \log N)$.

Proof for the lemma is technical and is postponed until Section 7.10. We note that the compression map τ_N in Definition 7.33 is similar to that used in the polynomial identity testing algorithm of Klivans and Spielman [KS01]. Using Lemma 7.34, we can reduce the number of variables of f_r in (7.10) down to three.

Corollary 7.35. *For every language* $\mathcal{L} \in \mathsf{P/poly}$ *and* $r > 0$, *there exist a finite box* B_r *and short GF* $f_r(t, u, v) \in \mathcal{GF}_{3,5}$ *with* $\mathrm{supp}(f_r) \subseteq B_r$, *so that* (7.10) *holds. The rest is identical to Theorem 7.29.*

Proof. We have (7.10) with $f_r(t, u, \mathbf{v}) = \sum t^x u^y \mathbf{v}^{\mathbf{z}} \in \mathcal{GF}_{5,5}$ a short GF of finite support in five variables (t, u, v_1, v_2, v_3). Using part a) of Lemma 7.34, we can compress $\mathbf{z}$ into a single-variable w, leaving both x and y unchanged. In other words, $t^x u^y \mathbf{v}^{\mathbf{z}}$ becomes $t^x u^y v^w$. Note that $\mathrm{proj}_{x,y}$ is not affected by compression. This gives us a short GF $\widetilde{f_r} \in \mathcal{GF}_{3,5}$ with

$$\mathrm{proj}_{x,y}(\widetilde{f_r}) \ = \ \mathrm{proj}_{x,y}(f_r) \quad \text{and} \quad \ell(\widetilde{f_r}) \le \mathrm{poly}(\ell(f_r)) \le \mathrm{poly}(r).$$

So we can substitute $\widetilde{f_r}$ for f_r in (7.10). □

7.4. Short GFs and the hierarchy PH/poly

The *non-uniform polynomial hierarchy* $\mathsf{PH/poly}$ starts with $\mathsf{P/poly} = \mathbf{\Sigma}_0^{\mathsf{P}}/\mathsf{poly} = \mathbf{\Pi}_0^{\mathsf{P}}/\mathsf{poly}$ at the 0th level. For $k > 0$, a language $\mathcal{L}$ is in $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly}$ if for every $r > 0$, there is a circuit C_r of size $\mathrm{poly}_{\mathcal{L}}(r)$ so that for every string $\widetilde{x}$ of length r we have:

$$\widetilde{x} \in \mathcal{L}_r \quad \iff \quad \exists \widetilde{y}_1 \, \forall \widetilde{y}_2 \dots \ Q_k \widetilde{y}_k : C_r(x, y_1, \dots, y_k) = 1.$$

Here $Q_1, \ldots, Q_k$ are k alternating quantifiers with $Q_1 = \exists$, and $\widetilde{y}_1, \ldots, \widetilde{y}_k$ are binary strings of length polynomial in r. For $\mathbf{\Pi}^{\mathsf{P}}_k/\mathsf{poly}$ the alternating quantifiers are reversed ($Q_1 = \forall$). We have a the following analogue to Lemma 7.26 for each level in $\mathsf{PH}/\mathsf{poly}$:

Lemma 7.36. *For every language $\mathcal{L} \in \mathbf{\Sigma}^{\mathsf{P}}_k/\mathsf{poly}$ and $r > 0$, there exists a quantifier-free PA expression in $k+4$ variables $x \in \mathbb{N}$, $\mathbf{y} \in \mathbb{N}^k$, $\mathbf{z} \in \mathbb{N}^3$, so that $\widetilde{x} \in \mathcal{L}_r$ if and only if:*

$$x \in [0, 2^r) \,\wedge\, \Big[Q_1 y_1 \in [0, 2^{p_1}) \,\ldots\, Q_k y_k \in [0, 2^{p_k})\; Q_{k+1}\mathbf{z} \in [0, 2^q)^3 \;:\; \Phi_r(x, \mathbf{y}, \mathbf{z}) \Big]. \tag{7.17}$$

Here $Q_1, \ldots, Q_{k+1}$ are $k+1$ alternating quantifiers with $Q_1 = \exists$. Moreover, we have $p_1, \ldots, p_k, q, \ell(\Phi_r) \le \mathrm{poly}_{\mathcal{L}}(r)$. For the case $\mathcal{L} \in \mathbf{\Pi}^{\mathsf{P}}_k/\mathsf{poly}$, the quantifiers Q_i are reversed.

Proof. For simplicity, we prove the claim for $\mathcal{L} \in \mathbf{\Sigma}^{\mathsf{P}}_1 = \mathsf{NP}/\mathsf{poly}$. The higher levels $\mathbf{\Sigma}^{\mathsf{P}}_k/\mathsf{poly}$ and $\mathbf{\Pi}^{\mathsf{P}}_k/\mathsf{poly}$ can be argued similarly. Since $\mathcal{L} \in \mathsf{NP}/\mathsf{poly}$, for each r, there is a circuit C_r of size $\mathrm{poly}_{\mathcal{L}}(r)$ such that

$$\widetilde{x} \in \mathcal{L}_r \quad \Longleftrightarrow \quad \exists\, \widetilde{c} \in \{0,1\}^s \,:\, C_r(\widetilde{x}, \widetilde{c}) = 1, \tag{7.18}$$

where $s \le \mathrm{poly}_{\mathcal{L}}(r)$ is the certificate length. The circuit C_r also has p non-input gates with $p \le \mathrm{poly}_{\mathcal{L}}(r)$. Let $p' = s + p$. Note that the certificate gates $\widetilde{c} \in \{0,1\}^s$ and the non-input gates $\widetilde{y} \in \{0,1\}^p$ can be coded by a single integer $y \in [0, 2^{p'})$. The argument now proceeds similarly to Lemma 7.4 with p' in place of p. □

Remark 7.37. In [Grä88, Lem. 5.2], Grädel gave a similar representation to (7.17). In his representation, each string $\widetilde{x} = (x_1, \ldots, x_r) \in \{0,1\}^r$ is not simply mapped to its binary integer value, but to:

$$x = p_1^{x_1} \ldots p_r^{x_r}\, q_1^{1-x_1} \ldots q_r^{1-x_r},$$

where $p_1, \ldots, p_r, q_1, \ldots, q_r$ are the first $2r$ prime numbers.

Definition 7.38. Let $f = \sum \mathbf{t}^{\mathbf{x}}\mathbf{u}^{\mathbf{y}} = \mathbf{F}(S; \mathbf{t}, \mathbf{u})$, where S is a subset of a finite box $I \times J$. The *anti-projection* $\overline{\mathrm{proj}}_{\mathbf{x}}(f)$ is $F(I; \mathbf{t}) - \mathrm{proj}_{\mathbf{x}}(f)$, where the projection $\mathrm{proj}_{\mathbf{x}}(f)$ is from Definition 7.8. The box $I \times J$ is always specified before taking the anti-projection.

Theorem 7.39. *For every language $\mathcal{L} \in \mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly}$ and $r > 0$, there exists a short GF $f_r \in \mathcal{GF}_{k+2,k+4}$ of the form $f_r(t, u_1, \ldots, u_k, v) = \sum t^x u_1^{y_1} \ldots u_k^{y_k} v^z$ such that*

$$\mathbf{F}(\mathcal{L}_r; t) = \mathrm{proj}_x\Big(\overline{\mathrm{proj}}_{x,y_1}\big(\mathrm{proj}_{x,y_1,y_2}(\cdots(f_r)\cdots)\big)\Big), \tag{7.19}$$

where the k alternating projections and anti-projections are taken in a finite box

$$B_r = [0, 2^r) \times [0, 2^{p_1}) \times \cdots \times [0, 2^{p_k}) \times [0, 2^q).$$

Moreover, we have $p_1, \ldots, p_k, q, \ell(f_r) \le \mathrm{poly}_{\mathcal{L}}(r)$. For $\mathcal{L} \in \mathbf{\Pi}_k^{\mathsf{P}}/\mathsf{poly}$, the projections and anti-projections are reversed.

Proof. By Lemma 7.36, we can represent $\mathcal{L}_r$ in the form (7.17). Applying the same argument in Theorem 7.29, we get $f_r(t, u_1, \ldots, u_k, \mathbf{v}) = \sum t^x u_1^{y_1} \ldots u_k^{y_k} \mathbf{v}^{\mathbf{z}} \in \mathcal{GF}_{k+4,k+4}$ that satisfy (7.19). Applying Lemma 7.34 a), we can compress the last three variables $\mathbf{v}^{\mathbf{z}} = v_1^{z_1} v_2^{z_2} v_3^{z_3}$ into just one variable v^w without affecting the projections (see the proof of Corollary 7.35). This reduces f_r to a short GF in $\mathcal{GF}_{k+2,k+4}$. □

Remark 7.40. If in addition $L \in \mathsf{PH}$, then both Φ_r and f_r in Lemma 7.36 and Theorem 7.39 can be computed in time $\mathrm{poly}_{\mathcal{L}}(r)$. Indeed, if $\mathcal{L} \in \mathsf{PH}$, the circuit C_r for $\mathcal{L}_r$ in Lemma 7.36's proof can be automatically generated by some polynomial time Turing Machine M. We can convert C_r to Φ_r in polynomial time, which allows us to find f_r.

As a consequence, we obtain the following result.

Corollary 7.41. *Assume we are given $a_0 \in \mathbb{N}$, a short GF $f(t, u, v) = \sum t^x u^y v^z \in \mathcal{GF}_{3,5}$, and a finite box $B \subset \mathbb{N}^3$ with $\mathrm{supp}(f) \subseteq B$. Then deciding whether $a_0 \in \mathrm{supp}(h)$ is NP-complete, where $h = \mathrm{proj}_x(\overline{\mathrm{proj}}_{x,y}(f))$. Here the projection and anti-projection are taken within B.*

Proof. If $a_0 \in \mathrm{supp}(h)$, there exists some b_0 so that (a_0, b_0) lies in the support of $\overline{\mathrm{proj}}_{x,y}(f)$. Since $\overline{\mathrm{proj}}_{x,y}(f)$ is taken within B, which is bounded, both a_0 and b_0 must have polynomial lengths. Given such a certificate b_0, we can verify if (a_0, b_0) lies in the support of $\mathrm{proj}_{x,y}(f)$

in polynomial time, by applying Proposition 7.18. Taking a negation, we can also check whether (a_0, b_0) lies in the anti-projection $\overline{\text{proj}}_{x,y}(f)$. This shows the problem is in NP.

The problem is also NP-hard. Indeed, let $\mathcal{L}$ be an NP language. Applying Theorem 7.39 for the case $\mathcal{L} \in \mathsf{NP}$, we have $\mathbf{F}(\mathcal{L}_r; t) = \text{proj}_x\big(\overline{\text{proj}}_{x,y}(f_r)\big)$, where f_r is supported inside a box B_r. By Remark 7.40, we can compute f_r and B_r in polynomial time. So checking $x \in \mathcal{L}_r$ is equivalent to checking $x \in \text{supp}(h_r)$, where $h_r = \text{proj}_x(B_r \backslash \text{proj}_{x,y}(f_r))$. □

Remark 7.42. Compared to Proposition 7.18, we see that it is no longer easy to check for membership after taking two separate projections on a short GF.

7.5. A hierarchy of generating functions

We introduce a hierarchy GH of languages expressible as projections of generating functions. First, we define the lowest level $\mathsf{G} = \mathbf{\Sigma}_0^{\mathsf{G}} = \mathbf{\Pi}_0^{\mathsf{G}}$.

Definition 7.43. For a language $\mathcal{L} \in \{0,1\}^*$, we say that $\mathcal{L} \in \mathsf{G}$ if there is an $s > 0$ so that for every $r > 0$, we can represent $\mathbf{F}(\mathcal{L}_r; t) = f_r(t)$ where $f_r \in \mathcal{GF}_{1,s}$ and $\ell(f_r) \leq \text{poly}_{\mathcal{L}}(r)$. In other words, every segment $\mathcal{L}_r$ can be represented as a short GF of polynomial length in some fixed class $\mathcal{GF}_{1,s}$.

We define higher classes $\mathbf{\Sigma}_k^{\mathsf{G}}$ and $\mathbf{\Pi}_k^{\mathsf{G}}$ by taking repeated projections/anti-projections.

Definition 7.44. For a language $\mathcal{L} \in \{0,1\}^*$, we say that $\mathcal{L} \in \mathbf{\Sigma}_k^{\mathsf{G}}$ if there is an $s > 0$ so that for every $r > 0$, we can represent:

$$\mathbf{F}(\mathcal{L}_r; t) = \text{proj}_x\Big(\overline{\text{proj}}_{x,y_1}\big(\text{proj}_{x,y_1,y_2}(\cdots(f_r)\cdots)\big)\Big), \tag{7.20}$$

where $f_r(t, u_1, \ldots, u_k) = \sum t^x u_1^{y_1} \ldots u_k^{y_k} \in \mathcal{GF}_{k+1,s}$ is supported inside a finite box B_r, with both $\ell(B_r), \ell(f_r) \leq \text{poly}_{\mathcal{L}}(r)$. The k alternating projections/anti-projections are taken within B_r. The class $\mathbf{\Pi}_k^{\mathsf{G}}$ is defined similarly, with the projections/anti-projections in (7.20) reversed. Alternatively, $\mathcal{L} \in \mathbf{\Pi}_k^{\mathsf{G}}$ if and only if the complement language $\neg\mathcal{L}$ is in $\mathbf{\Sigma}_k^{\mathsf{G}}$.

Definition 7.45. GH is the union of all $\mathbf{\Sigma}_k^{\mathsf{G}}$ and $\mathbf{\Pi}_k^{\mathsf{G}}$ for all $k \geq 0$.

We list some properties of GH:

- $\mathbf{\Sigma}_k^{\mathsf{G}}, \mathbf{\Pi}_k^{\mathsf{G}} \subseteq \mathbf{\Sigma}_{k+1}^{\mathsf{G}} \cap \mathbf{\Pi}_{k+1}^{\mathsf{G}}$ for all $k \geq 0$.
- G, $\mathbf{\Sigma}_1^{\mathsf{G}}$, $\mathbf{\Pi}_1^{\mathsf{G}} \subseteq \mathsf{P/poly}$ (propositions 7.16 and 7.18).
- $\mathsf{P/poly} \subseteq \mathsf{U}\mathbf{\Pi}_1^{\mathsf{G}}$, the subclass of $\mathbf{\Sigma}_2^{\mathsf{G}}$ with only spec_x and $\overline{\text{proj}}_{x,y}$ (Theorem 7.29).
- In fact, $\mathsf{U}\mathbf{\Pi}_1^{\mathsf{G}} = \mathsf{UP/poly}$ (Remark 7.32).
- $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly} \subseteq \mathbf{\Sigma}_{k+1}^{\mathsf{G}}$, $\mathbf{\Pi}_k^{\mathsf{P}}/\mathsf{poly} \subseteq \mathbf{\Pi}_{k+1}^{\mathsf{G}}$ for all $k \geq 1$ (Theorem 7.39).

The last property can actually be strengthened to:

Theorem 7.46. $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly} = \mathbf{\Sigma}_{k+1}^{\mathsf{G}}$ *and* $\mathbf{\Pi}_k^{\mathsf{P}}/\mathsf{poly} = \mathbf{\Pi}_{k+1}^{\mathsf{G}}$ *for every* $k \geq 1$. *So* $\mathsf{GH} = \mathsf{PH/poly}$, *i.e.,* GH *is exactly the non-uniform version of* PH.

Proof. Theorem 7.39 already showed inclusion in one direction. For the other direction, assume $\mathcal{L} \in \mathbf{\Sigma}_{k+1}^{\mathsf{G}}$. From Definition 7.44, for every $r > 0$, we have:

$$\mathbf{F}(\mathcal{L}_r; t) \;=\; \text{proj}_x\Big(\overline{\text{proj}}_{x,y_1}\big(\text{proj}_{x,y_1,y_2}(\cdots(f_r)\cdots)\big)\Big),$$

where f_r is a short GF of length $\text{poly}_{\mathcal{L}}(r)$ in some fixed class $\mathcal{GF}_{k+2,s}$. Here we are taking $k+1$ alternating projections and anti-projections on $f_r(x, y_1, \ldots, y_{k+1}) = \sum t^x u_1^{y_1} \ldots u_{k+1}^{y_{k+1}}$ within some finite box B_r. Note that by Proposition 7.18, we can check in polynomial time if $(x, y_1, \ldots, y_k)$ lies in the inner most projection/anti-projection. So given f_r as an advice string, we can decide if $x \in \mathcal{L}_r$ by calling a $\mathbf{\Sigma}_k^{\mathsf{P}}$ oracle for the remaining k projections/anti-projections. This implies $\mathcal{L} \in \mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly}$. The case $\mathcal{L} \in \mathbf{\Pi}_{k+1}^{\mathsf{G}}$ is similar. □

7.6. Short GFs have long projections

7.6.A. Proof of Theorem 7.5.

Theorem 7.47. *If* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$, *then* $\mathsf{G} \subsetneq \mathsf{P/poly}$.

Proof. We saw in Section 7.5 that $\mathsf{G} \subseteq \mathsf{P/poly}$. Now we show $\mathsf{P/poly}$ is strictly larger than G. Let $\#\mathcal{L}$ be an $\#\mathsf{P}$-complete problem (e.g. #3SAT), which is outside of $\mathsf{FP/poly}$ by the assumption $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$. Associated to $\#\mathcal{L}$ is a polynomial time Turing machine M. Given $\widetilde{x} \in \{0,1\}^r$, $\#\mathcal{L}$ asks for the number of certificates $\widetilde{c} \in \{0,1\}^r$ that satisfy $M(\widetilde{x}, \widetilde{c}) = 1$. Define a language:

$$\mathcal{M} = \{(\widetilde{x}, \widetilde{c}) : \text{length}(\widetilde{x}) = \text{length}(\widetilde{c}) \text{ and } M(\widetilde{x}, \widetilde{c}) = 1\}.^7 \tag{7.21}$$

Since M runs in polynomial time, we also have $\mathcal{M} \in \mathsf{P/poly}$. We show that $\mathcal{M} \notin \mathsf{G}$.

Assume the contrary, i.e., $\mathcal{M} \in \mathsf{G}$. Then there is a fixed s so that for every $r > 0$, we have $\mathcal{M}_r = \text{supp}(f_r)$, where $f_r \in \mathcal{GF}_{1,s}$ and $\ell(f_r) \leq \text{poly}(r)$. Let $x, c \in [0, 2^r)$ be the integers corresponding to $\widetilde{x}, \widetilde{c} \in \{0,1\}^r$. Then the concatenated string $(\widetilde{x}, \widetilde{c})$ corresponds to $x + 2^r c$. We assumed that there is an $f_{2r} \in \mathcal{GF}_{1,s}$ such that

$$\ell(f_{2r}) \leq \text{poly}(r) \quad \text{and} \quad \sum_{(\widetilde{x},\widetilde{c}) \in \mathcal{M}_{2r}} t^{x+2^r c} = f_{2r}(t).$$

Given $\widetilde{x} \in \{0,1\}^r$, we must compute the number of $\widetilde{c} \in \{0,1\}^r$ which satisfy $(\widetilde{x}, \widetilde{c}) \in \mathcal{M}_{2r}$. Define

$$g_x(t) = \sum_{0 \leq c < 2^r} t^{x+2^r c} = t^x \frac{1 - t^{2^{2r}}}{1 - t^{2^r}}. \tag{7.22}$$

We have $\ell(g_x) \leq \text{poly}(r)$. We also have $f_{2r} \in \mathcal{GF}_{1,s}$ and $g_x \in \mathcal{GF}_{1,1}$. Therefore, by Theorem 7.14, the short GF $h_x = f_{2r} \star g_x$ can be computed in time $\text{poly}(\ell(f_{2r}) + \ell(g_x)) \leq \text{poly}(r)$. The number of certificates $\widetilde{c}$ for $\widetilde{x}$ is simply $h_x(1)$. This substitution can be computed in time $\text{poly}(r)$ by Theorem 7.13.

To summarize, the short GF f_{2r} gives us a polynomial size circuit to solve $\#\mathcal{L}$ for all inputs $\widetilde{x} \in \{0,1\}^r$ in time $\text{poly}(r)$. We conclude that $\#\mathcal{L} \in \mathsf{FP/poly}$, a contradiction. □

Now we can formulate Theorem 7.5 in precise terms:

Corollary 7.48. *If $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$, then GH does not collapse to its 0th level G. In other words, there is a sequence $\{f_r\}_{r>0}$ in some fixed class $\mathcal{GF}_{2,s}$ with $\ell(f_r) \leq \text{poly}(r)$ so that for every d, $\text{proj}_x(f_r)$ cannot be written as a short GF $h_r \in \mathcal{GF}_{1,d}$ with $\ell(h_r) \leq \text{poly}(r)$.*

[7] In general, the instance $\widetilde{x}$ and certificate $\widetilde{c}$ can have different lengths. However, the Turing Machine M can always be modified to accept only $\widetilde{c}$ and $\widetilde{x}$ of equal lengths.

Proof. Recall that $\mathsf{G} \subseteq \mathsf{P/poly} \subseteq \mathsf{GH}$ (Section 7.5). Now this follows from Theorem 7.47. □

7.6.B. A partial converse. One can ask if the above argument in the proof above can be reversed, i.e., if $\#\mathsf{P} \subseteq \mathsf{FP/poly}$, does it imply that GH collapses to G? We present below a weaker result.

Recall from Section 7.5 that $\mathsf{U\Pi_1^G}$ the subclass of $\mathbf{\Sigma}_2^{\mathsf{G}}$ that uses only spec_x and $\overline{\mathrm{proj}}_{x,y}$. In other words, $\mathcal{L} \in \mathsf{U\Pi_1^G}$ if for every $r > 0$, we have $\mathbf{F}(\mathcal{L}_r; t) = \mathrm{spec}_x(\overline{\mathrm{proj}}_{x,y}(f_r))$ for some f_r in some fixed class $\mathcal{GF}_{3,s}$ with $\ell(f_r) \leq \mathrm{poly}_{\mathcal{L}}(r)$. We also know that $\mathsf{U\Pi_1^G} = \mathsf{UP/poly}$.

Proposition 7.49. *If* $\#\mathsf{P} \subseteq \mathsf{FP/poly}$*, then* GH *collapses to* $\mathsf{U\Pi_1^G}$*.*

Proof. Since $\mathsf{GH} = \mathsf{PH/poly}$ and $\mathsf{U\Pi_1^G} = \mathsf{UP/poly}$, it equivalent to show $\mathsf{PH/poly} = \mathsf{UP/poly}$. In fact, we have a stronger collapse, namely $\mathsf{PH/poly} = \mathsf{P/poly}$. This follows easily from *Toda's theorem*, which says that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathrm{SAT}}$. Replacing the #SAT oracle by polynomial size circuits, we have $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{P/poly}} = \mathsf{P/poly}$. Taking the non-uniform version of PH, we still have $\mathsf{PH/poly} \subseteq \mathsf{P/poly}$. □

Remark 7.50. The proposition implies that proving GH does not collapse to between its 1st and 2nd levels is at least as hard as showing $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$. However, there might still be hope of showing that GH does not collapse to its 0th level G, e.g., by proving Conjecture 7.1.

Remark 7.51. We do not claim that Proposition 7.49 is a new collapse result assuming $\#\mathsf{P} \subseteq \mathsf{FP/poly}$. Here we are only putting things in the context of short GFs. Observe that $\#\mathsf{P} \subseteq \mathsf{FP/poly}$ implies $\mathsf{NP} \subseteq \mathsf{P/poly}$. In turn, $\mathsf{NP} \subseteq \mathsf{P/poly}$ implies $\mathsf{PH} = \mathsf{S}_2^{\mathsf{P}}$ (see [Cai07]), which is the strongest collapse currently known, assuming $\mathsf{NP} \subseteq \mathsf{P/poly}$. Note that the classical *Karp–Lipton theorem* says that $\mathsf{NP} \subseteq \mathsf{P/poly}$ implies $\mathsf{PH} = \mathbf{\Sigma}_2^{\mathsf{P}}$, which is weaker because $\mathsf{S}_2^{\mathsf{P}} \subseteq \mathbf{\Sigma}_2^{\mathsf{P}} \cap \mathbf{\Pi}_2^{\mathsf{P}}$.

7.7. Intersections, unions and Minkowski sums

7.7.A. Proof of Theorem 7.3. Below is the precise statement of Theorem 7.3.

Theorem 7.52. *Assume* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$. *Then there is an* $s > 0$ *and a family of finite subsets* $\{S_r\}_{r>0}$ *with each* $S_r = \{p_{r,1}, \ldots, p_{r,k_r}\} \subset \mathcal{GF}_{1,s}$ *so than the following hold:*

a) *The total length of all* $p_{r,i}$ *in* S_r *is* $\mathrm{poly}(r)$.

b) *For every fixed* d, *the intersection/union of all* $p_{r,i}$ *in* S_r *cannot be written as a short GF* $h_r \in \mathcal{GF}_{2,d}$ *with* $\ell(h_r) \leq \mathrm{poly}(r)$.

Proof. By Theorem 7.47, there exists a language $\mathcal{L} \in \mathsf{P/poly}$ which is outside of G. By Theorem 7.29, for every $r > 0$, we can represent:

$$\mathbf{F}(\mathcal{L}_r; t) \,=\, \mathrm{spec}_x(B_r \backslash \mathrm{proj}_{x,y}(f_r)) \quad \text{and} \quad \mathrm{proj}_{x,y}(f_r) \,=\, p_{r,1} \cup \cdots \cup p_{r,k_r},$$

where $f_r \in \mathcal{GF}_{5,5},\ p_{r,i} \in \mathcal{GF}_{2,s}$ and $\ell(B_r),\ \ell(f_r),\ \sum \ell(p_{r,i}) \leq \mathrm{poly}(r)$. Here s is some universal constant.

Let $S_r = \{p_{r,1}, \ldots, p_{r,k_r}\}$. This family $\{S_r\}$ satisfies condition a). We show that the union of $p_{r,i}$ cannot be written as a short GF of length $\mathrm{poly}(r)$. Indeed, assume there is d for which we can write $\mathrm{proj}_{x,y}(f_r) = p_{r,1} \cup \cdots \cup p_{r,k_r}$ as $h_r \in \mathcal{GF}_{2,d}$ with $\ell(h_r) \leq \mathrm{poly}(r)$. By Theorem 7.14, the complement $B_r \backslash h_r$ can be written as a short GF $g_r \in \mathcal{GF}_{2,2d}$ of length $\mathrm{poly}(r)$. Taking the specialization $\mathrm{spec}_x(g_r)$, we still have a short GF in $\mathcal{GF}_{2,2d}$ of length $\mathrm{poly}(r)$, which represents $\mathcal{L}_r$. Since this holds for all $r > 0$, we have $\mathcal{L} \in \mathsf{G}$, a contradiction. So the family $\{S_r\}$ also satisfies b).

Note that each $p_{r,i}$ still has two variables x, y. By Lemma 7.34 part a), we can compress each $p_{r,i}$ into a single variable short GF $\widetilde{p}_{r,i} \in \mathcal{GF}_{1,s}$ of polynomial length. Then the new subsets $\widetilde{S}_r = \{\widetilde{p}_{r,1}, \ldots, \widetilde{p}_{r,k_r}\} \subset \mathcal{GF}_{1,s}$ still satisfy condition a). We show they still satisfy condition b). Indeed, note that compressing/decompression preserves intersection and union. So if $\widetilde{p}_{r,i}$ has a polynomial length union then Lemma 7.34 part b) allows us the decompress it into a polynomial length union of $p_{r,i}$. This completes the proof for the case of union. The case of intersection follows by taking complements of $p_{r,i}$. □

7.7.B. Proof of Theorem 7.4.

Definition 7.53. Given two GFs $a = \mathbf{F}(S_1; \mathbf{t})$ and $b = \mathbf{F}(S_2; \mathbf{t})$ with $S_1, S_2 \subseteq \mathbb{N}^n$, the *Minkowski sum* $a \oplus b$ is $\mathbf{F}(S_1 \oplus S_2; \mathbf{t})$, where $S_1 \oplus S_2$ is the usual Minkowski sum of two point sets.

Example 7.54. Given $\overline{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, the semigroup $\mathbb{N}\langle b_1, \ldots, b_n\rangle$ consists of all non-negative integer combinations of the b_j's. Its generating function is given by:

$$f_{\overline{b}}(t) \,=\, \frac{1}{1-t^{b_1}} \,\oplus\, \ldots \,\oplus\, \frac{1}{1-t^{b_n}}.$$

Given such $\overline{b} \in \mathbb{N}^n$ and $a \in \mathbb{N}$, the KNAPSACK problem asks if $a \in \operatorname{supp}(f_{\overline{b}})$.

Below is the precise statement of Theorem 7.4.

Theorem 7.55. *Assume* $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$. *Then there is an* $s > 0$ *and two sequences* $\{a_r\}_{r>0}$, $\{b_r\}_{r>0} \subset \mathcal{GF}_{1,s}$ *such that*

a) $\ell(a_r) + \ell(b_r) \le \operatorname{poly}(r)$.

b) *For every fixed* d, *the Minkowski sum* $a_r \oplus b_r$ *cannot be written as a short GF* h_r *in* $\mathcal{GF}_{1,d}$ *of length* $\ell(h_r) \le \operatorname{poly}(r)$.

Proof. By Theorem 7.52, there exists an $s > 0$, and for each r a subset

$$S_r = \{p_{r,1}, \ldots, p_{r,k_r}\} \subset \mathcal{GF}_{1,s} \quad \text{with} \quad \sum \ell(p_{r,i}) \le \operatorname{poly}(r)$$

with the following property. For every fixed d, the union $h_r = p_{r,i} \cup \cdots \cup p_{r,k_r}$ cannot be written as a short GF of length $\operatorname{poly}(r)$ in $\mathcal{GF}_{1,d}$. Define

$$a_r(t,u) \,=\, \sum_{i=1}^{k_r} p_{r,i}(t)\, u^i \,\in\, \mathcal{GF}_{2,s}. \tag{7.23}$$

and

$$b_r(t,u) \,=\, \sum_{i=0}^{k_r-1} t^0 u^i = \frac{1-u^{k_r}}{1-u} \,\in\, \mathcal{GF}_{1,1} \subset \mathcal{GF}_{2,s}. \tag{7.24}$$

Since $\sum \ell(p_{r,i}) \le \operatorname{poly}(r)$, we also have $\ell(a_r) + \ell(b_r) \le \operatorname{poly}(r)$.

Consider the terms $t^x u^{k_r}$ in the Minkowski sum $a_r \oplus b_r$. From (7.23) and (7.24), we have:

$$\big\{x : (x, k_r) \in \operatorname{supp}(a_r \oplus b_r)\big\} \,=\, \bigcup_{i=1}^{k_r} \operatorname{supp}(p_{r,i}) \,=\, \operatorname{supp}(h_r).$$

In other words, we have $[u^{k_r}](a_r \oplus b_r)(t,u) = h_r(t)$. Define

$$g_r(t,u) = \sum_{x \in \mathbb{N}} t^x u^{k_r} = \frac{u^{k_r}}{1-t}.$$

Taking the intersection of g_r with $a_r \oplus b_r$, we get:

$$\big[(a_r \oplus b_r) \star g_r\big](t,u) = u^{k_r}\, h_r(t). \tag{7.25}$$

Now assume there is d so that $a_r \oplus b_r$ can be written as $c_r \in \mathcal{GF}_{2,d}$ with $\ell(c_r) \le \text{poly}(r)$. By Theorem 7.14, we can compute h_r by taking the Hadamard product $c_r \star g_r$ and substitute $u \leftarrow 1$ in (7.25). This would imply that h_r is a short GF of length poly(r) in the fixed class $\mathcal{GF}_{1,d+1}$, which contradicts our first statement on h_r.

So the two sequences $\{a_r\}_{r>0}$ and $\{b_r\}_{r>0} \subset \mathcal{GF}_{2,s}$ do not have Minkowski sums of polynomial lengths. Note that each a_r and b_r still has two variables. By Lemma 7.34 part a), we can compress a_r, b_r into single variable short GFs $\widetilde{a}_r, \widetilde{b}_r \in \mathcal{GF}_{1,s}$. Note that compressing/decompression preserves Minkowski sum. So $\widetilde{a}_r \oplus \widetilde{b}_r$ does not have polynomial length, because otherwise we can decompress it to get $a_r \oplus b_r$ of polynomial length. □

7.8. Squares, primes, and short GFs

7.8.A. Short GFs and squares. Recall the definition of the class G from Section 7.5. We present a candidate for a language $\mathcal{L} \in \mathsf{P/poly}$ which is outside of G. Let SQUARES be the language consisting of all square numbers written in binary. Then

$$\text{SQUARES}_r = \{k^2 : \ k^2 < 2^r\}.^8$$

Conjecture 7.56. SQUARES *is not in* G.

In other words, the conjecture says that for every fixed s, the segment SQUARES_r cannot be represented as $\text{supp}(g_r)$ for a short GF $g_r \in \mathcal{GF}_{1,s}$ of length $\ell(g_r) \le \text{poly}(r)$. Note that this

[8] Strictly speaking, some numbers in SQUARES_r have less than r digits. However, we can always pad them with enough zeroes form a set of strings of the same length.

conjecture is free of complexity assumptions. If true, Conjecture 7.56 shows unconditionally that $\mathsf{G} \subsetneq \mathsf{P/poly}$, which implies $\mathsf{G} \subsetneq \mathsf{GH}$. We already know from Example 7.30 and Section 7.5 that SQUARES $\in \mathsf{U\Pi}_1^{\mathsf{G}} \subseteq \mathsf{GH}$. So Squares should be a candidate that separates G from $\mathsf{U\Pi}_1^{\mathsf{G}}$ according to this conjecture.

We begin with the following attractive result.

Theorem 7.57. *If Conjecture 7.56 is false, then* INTEGER FACTORING $\in \mathsf{P/poly}$.

Proof. We build on an argument in Section 6 of [Bar06b]. Assume there is an $s > 0$ so that for every $N = 2^r$, we can write $\mathbf{F}\big(\text{Squares}_r; t\big) = g_r(t)$, where $g_r(t)$ is a short GF in $\mathcal{GF}_{1,s}$ with $\ell(g) \leq \text{poly}(r)$. Consider:

$$h_r(t) \;=\; g_r(t)^4 \;=\; \left(\sum_{n^2<N} t^{n^2}\right)^4 \;=\; \sum_{k\geq 0} a_r(k)t^k,$$

where

$$a_r(k) \;=\; \#\Big\{(n_1,n_2,n_3,n_4) : n_i^2 < N,\ \sum n_i^2 = k\Big\}.$$

In particular, if $k < N$, then $a_r(k)$ is the number of ways to write k as a sum of four squares. Since $g_r \in \mathcal{GF}_{1,s}$, we have $h_r = g_r^4 \in \mathcal{GF}_{1,4s}$ and also $\ell(h) \leq \text{poly}(\ell(g)) \leq \text{poly}(r)$.

Applying Proposition 7.16, each coefficient $a_r(k)$ can be computed in time $\text{poly}(r)$. By Jacobi's formula (see e.g. [HW]), we also have:

$$a_r(k) \;=\; 8 \sum_{4\nmid d,\, d\mid k} d \quad \text{for} \quad k < N\,.$$

Here d is a divisor of k which is not a multiple of 4. From this, we can compute in time $\text{poly}(r)$ the sum of divisors $\sigma(k)$ for every $k < N = 2^r$. By a standard argument (see e.g. [BMS86]), given $\sigma(k)$, we can factor k in probabilistic polynomial time. □

Theorem 7.58. *If Conjecture 7.56 is false, then* $\#\mathsf{P} \subseteq \mathsf{FP/poly}$.

Proof of Theorem 7.58. In [MA78], it is proved that the following problem is NP-complete: Given $\alpha, \beta, \gamma \in \mathbb{N}$, decide whether there exists $x \in \mathbb{N}$ such that

$$0 \leq x \leq \gamma \quad \text{and} \quad x^2 \equiv \alpha \,(\text{mod } \beta). \tag{7.26}$$

The argument in [MA78] actually gave bijection between the set of Boolean strings satisfying a 3SAT formula and the set of x satisfying (7.26). Here α, β and γ can be computed in polynomial time from the 3SAT formula. Since counting the number of 3SAT solutions is #P-complete, so is counting the number of solutions for (7.26).

Now assume Conjecture 7.56 fails, then SQUARES $\in \mathsf{G}$. This means there is an $s > 0$ so that for every $r > 0$ we can write $\mathbf{F}\big(\text{Squares}_r; t\big) = g_r(t)$ for some $g_r \in \mathcal{GF}_{1,s}$ with $\ell(g_r) \leq \text{poly}(r)$. Given $\alpha, \beta, \gamma \in \mathbb{N}$, we define:

$$h(t) = \sum_{i=0}^{\gamma^2} t^i = \frac{1 - t^{\gamma^2+1}}{1-t} \quad \text{and} \quad k(t) = \sum_{x \equiv \alpha \,(\text{mod } \beta)} t^x = \frac{t^\alpha}{1-t^\beta}.$$

Let $r = 2\lceil \log \gamma \rceil$. The number of solutions for (7.26) can be counted by taking $g_r \star h \star k$ and evaluate at $t = 1$, which are polynomial time operations by theorems 7.13 and 7.14. So the above #P-complete problem can be solved by polynomial size circuits, which are provided by the g_r for different r. This implies $\#\mathsf{P} \subseteq \mathsf{FP/poly}$. □

By Theorem 7.29, we can represent SQUARES_r as $\text{spec}_x(B_r \backslash \text{proj}_y(f_r))$ for some short GF f_r of length $\text{poly}(r)$. Conjecture 7.56 says that it is not possible to do so without using projections.

In the domain of PA formulas, by Lemma 7.26, we can represent SQUARES_r with a $\exists\forall$ PA formula of length $\text{poly}(r)$. A similar question can be asked: Are both quantifiers necessary? The following result shows that two alternating quantifiers $\exists\forall$ are necessary in Lemma 7.26, already in the case of SQUARES:

Proposition 7.59. SQUARES_r *cannot be represented by an* $\exists$ *PA formula of length* $\text{poly}(r)$ *in a fixed number of variables.*

Proof. By AP_k we mean a k-term arithmetic progression. It is well known that SQUARES does not contain any non-trivial AP_4. This was suggested by Fermat in 1640 and proved by Euler in 1780 (see e.g. [Weil84, p. 115]). Also, the cardinality of SQUARES_r is super-polynomial in r. With these two observations, this proposition follows directly from the next theorem when $k = 4$. □

Theorem 7.60. *For every fixed n and k, there exists a polynomial P so that the following holds. If an $\exists$ PA formula*

$$\{x \ : \ \exists \mathbf{y} \in \mathbb{Z}^n \ \ \Phi(x, \mathbf{y})\} \tag{7.27}$$

determines a set of cardinality at least $P(\ell(\Phi))$, then it must contain a non-trivial AP_k.

Proof. By Proposition 6.18, we know that there is a constant $c = c(n) > 0$ so that any quantifier-free expression Φ in n variables describes a disjoint union of m polyhedra $P_1, \ldots, P_m$ in $\mathbb{R}^{n+1}$ with $m < \ell(\Phi)^c$. So the formula (7.27) can be rewritten as:

$$S \ = \ \Big\{x \in \mathbb{Z} \ : \ \exists \mathbf{y} \in \mathbb{Z}^n \ \ \bigvee_{i=1}^{m} (x, \mathbf{y}) \in P_i\Big\}. \tag{7.28}$$

Let $\mathrm{q}(t) = k^{n+1}t^c$. Assume that $|S| \geq \mathrm{q}\big(\ell(\Phi)\big) > k^{n+1}m$. Select any $(k^{n+1}m + 1)$ different integers from S. By the pigeonhole principle, one of the polyhedra, say P_1, contains in its projection at least $k^{n+1}+1$ of these integers. Denote those integers in the projection of P_1 by $x_1, \ldots, x_s$, where $s = k^{n+1} + 1$. For every such x_i, there exists $\mathbf{y}_i \in \mathbb{Z}^n$ so that $(x_i, \mathbf{y}_i) \in P_1$. So we have:

$$(x_1, \mathbf{y}_1), \ldots, (x_s, \mathbf{y}_s) \in P_1 \cap \mathbb{Z}^{n+1}.$$

By the pigeonhole principle, two different pairs $(x_i, \mathbf{y}_i)$ and $(x_j, \mathbf{y}_j)$ have coordinates equal mod k pairwise. Since P_1 is convex, we also have

$$(\lambda x_i + (1-\lambda)x_j, \ \lambda \mathbf{y}_i + (1-\lambda)\mathbf{y}_j) \ \in \ P_1 \cap \mathbb{Z}^{n+1} \ , \quad \text{where } \lambda \in \big\{\tfrac{1}{k}, \ldots, \tfrac{k-1}{k}\big\}.$$

The above points project to $\lambda x_i + (1-\lambda)x_j$. By (7.28), we get a non-trivial AP_{k+1}:

$$\Big(x_i, \ \tfrac{k-1}{k}x_i + \tfrac{1}{k}x_j, \ \ldots, \ \tfrac{1}{k}x_j + \tfrac{k-1}{k}x_i, \ x_j\Big),$$

a contradiction. □

Remark 7.61. Proposition 7.59 combined with Lemma 7.26 implies that there is a sequence of PA formulas $\{x : \exists y \forall \mathbf{z} \ \Phi_r(x, y, \mathbf{z})\}$ of length poly(r) for which there are no equivalent PA formulas $\{x : \exists y \, \Psi_r(x, y)\}$ of length poly(r). So the formulas $\{(x, y) : \forall \mathbf{z} \ \Phi_r(x, y, \mathbf{z})\}$ have no equivalent quantifier-free formulas in x and y of length poly(r). Therefore, quantifier elimination in PA necessarily increases the length of formulas by a super-polynomial factor, even in a bounded number of variables ($x, y \in \mathbb{N}$, $\mathbf{z} \in \mathbb{N}^3$).

Remark 7.62. From SQUARES, one can easily create another a language $\mathcal{L} \in \mathsf{P}$ which $\mathcal{L}_r$ be represented neither by $\forall$ nor by $\exists$ PA formulas of length poly(r). For r odd, we let $\mathcal{L}$ contain all squares between 2^r and 2^{r+1}. For r even, we let $\mathcal{L}$ contain all non-squares between 2^r and 2^{r+1}. It is clear that $\mathcal{L} \in \mathsf{P}$. The above argument shows that $\mathcal{L}_r$ cannot be represented by $\exists$ PA formulas of length poly(r) when r is odd. Under a negation, the same argument also works for $\forall$ PA formulas when r is even. We denote this language by SQUARES$'$.

7.8.B. Short GFs and arithmetic progressions. Generalizing the above observation on sets with no arithmetic progressions, we suggest another conjecture on short GFs. Again, by AP_k we mean a *k-term arithmetic progression.*

Definition 7.63. Fix $c > 0$ and $k \geq 3$. A short GF g is said to have the (c, k)-property if either $|\mathrm{supp}(g)| < \ell(g)^c$ or $\mathrm{supp}(g)$ contains an AP_k.

Conjecture 7.64. *For every s and k, there exists $c > 0$ so that every short GF $g(t) \in \mathcal{GF}_{1,s}$ has the (c, k)-property.*

Proposition 7.65. *Conjecture 7.64 implies Conjecture 7.56.*

Proof. Assume Conjecture 7.64 holds but Conjecture 7.56 fails, i.e., SQUARES $\in \mathsf{G}$. So there is an $s > 0$ such that $\textsc{Squares}_r$ can be represented as $\mathrm{supp}(g_r)$ with $g_r \in \mathcal{GF}_{1,s}$ and $\ell(g_r) \leq \mathrm{poly}(r)$. Conjecture 7.64 applied to s and $k = 4$ gives us a $c > 0$ so that all $g \in \mathcal{GF}_{1,s}$ have the $(c, 4)$-property. We have $\mathrm{supp}(g_r) = |\textsc{Squares}_r| \gg r^c$. So if r is large enough, g_r contains an AP_4. This contradicts the fact that SQUARES is AP_4 free. □

7.8.C. Short GFs and primes. In a similar manner, we ask if primes can be represented by short GFs of polynomial length. Let PRIMES be the language consisting of all primes written in binary. Then

$$\textsc{Primes}_r = \{p \text{ prime} : \ p < 2^r\}.$$

Conjecture 7.66. PRIMES *is not in* G.

In other words, the conjecture says that for every fixed s, the segment $\textsc{Primes}_r$ cannot be

represented as $\operatorname{supp}(g_r)$ for a short GF $g_r \in \mathcal{GF}_{1,s}$ of length $\ell(g_r) \le \operatorname{poly}(r)$. This conjecture, if true, would also show $\mathsf{G} \subsetneq \mathsf{P}/\mathsf{poly}$ unconditionally.

Proposition 7.67. *Let $\pi(n)$ be the number of primes between 1 and n. If Conjecture 7.66 is false then $\pi(n)$ can be computed by circuits of size* $\operatorname{poly}(\log n)$.

Proof. Assume Conjecture 7.66 is false, i.e., there is an $s > 0$ so that for every $r > 0$ we have $\mathbf{F}\big(\textsc{Primes}_r; t\big) = g_r(t)$, where $g_r \in \mathcal{GF}_{1,s}$ and $\ell(g_r) \le \operatorname{poly}(r)$. Given $n < 2^r$, we have:

$$\mathbf{F}\big(\textsc{Primes}_r \cap [0,n];\, t\big) \;=\; g_r(t) \star \frac{1-t^{n+1}}{1-t} \;=\; h_n(t).$$

By Theorem 7.14, we can compute h_n in time $\operatorname{poly}(r)$. Substituting $t \leftarrow 1$, we get $\pi(n)$. □

Remark 7.68. In [LO87], using strong analytic tools, Lagarias and Odlyzko gave an algorithm to compute $\pi(n)$ in time $O(n^{1/2+\varepsilon})$, which is exponential in $\log n$. If Conjecture 7.66 is false, then for each r, a far better $\operatorname{poly}(r)$ algorithm exists for computing $\pi(n)$ for all $n < 2^r$.

7.9. Relative complexity of short GFs

7.9.A. PA complexity classes. We again revisit the relation between short GFs and PA formulas. The most basic PA formulas are quantifier-free, i.e., Boolean combinations of linear inequalities.

Definition 7.69. The class $\mathbf{\Sigma}_0^{\mathsf{PA}} = \mathbf{\Pi}_0^{\mathsf{PA}}$ consists of languages definable by quantifier-free PA formulas of polynomial lengths. In other words, a language $\mathcal{L}$ is in $\mathbf{\Sigma}_0^{\mathsf{PA}}$ if for every $r > 0$, there is a quantifier-free PA expression $\Phi_r(x)$ of length $\ell(\Phi) \le \operatorname{poly}_{\mathcal{L}}(r)$ so that:

$$x \in \mathcal{L}_r \quad \iff \quad \Phi_r(x).$$

By Proposition 6.18, $\mathcal{L} \in \mathbf{\Sigma}_0^{\mathsf{PA}}$ if and only if every initial segment $\mathcal{L}_r$ is a union of polynomially many intervals in $\mathbb{N}$. By Theorem 7.21, we have $\mathbf{\Sigma}_0^{\mathsf{PA}} \subset \mathsf{G}$.

Example 7.70. The language $\textsc{Even}$ of even integers is not in $\mathbf{\Sigma}_0^{\mathsf{PA}}$. However, $\textsc{Even} \in \mathsf{G}$, because:

$$\sum_{x \in \textsc{Even}_r} t^x = t^0 + t^2 + \cdots + t^{2^r-2} = \frac{1-t^{2^r}}{1-t^2}.$$

So we conclude that $\mathbf{\Sigma}_0^{\mathsf{PA}} \subsetneq \mathsf{G}$.

Definition 7.71. The class $\mathbf{\Sigma}_1^{\mathsf{PA}}$ consists of languages definable by $\exists$ PA formulas of polynomial lengths. In other words, $\mathcal{L} \in \mathbf{\Sigma}_1^{\mathsf{PA}}$ if there is an n so that for every $r > 0$, we can represent

$$x \in \mathcal{L}_r \quad \iff \quad \exists \mathbf{y} \in \mathbb{N}^n \;\; \Phi_r(x, \mathbf{y}),$$

where $\Phi_r(x, \mathbf{y})$ is a quantifier-free PA expression of length $\ell(\Phi_r) = \mathrm{poly}_{\mathcal{L}}(r)$. The class $\mathbf{\Pi}_1^{\mathsf{PA}}$ is defined similarly, but with $\forall$ PA formulas. In other words, $\mathcal{L} \in \mathbf{\Pi}_1^{\mathsf{PA}}$ if and only if $\neg\mathcal{L} \in \mathbf{\Sigma}_1^{\mathsf{PA}}$.

Conjecture 7.72. $\mathsf{G} \subseteq \mathbf{\Sigma}_1^{\mathsf{PA}} \cap \mathbf{\Pi}_1^{\mathsf{PA}}$.

To rephrase, this conjecture says that for every fixed s, there is an $n = n(s)$ so that every $g \in \mathcal{GF}_{1,s}$ of finite support has an $\exists$ PA formula representation:

$$G = \{x : \exists \mathbf{y} \in \mathbb{N}^n \;\; \Phi(x, \mathbf{y})\}, \quad \mathbf{F}(G; t) = g(t) \quad \text{and} \quad \ell(\Phi) \le \mathrm{poly}(\ell(g)). \tag{7.29}$$

Note that it would be enough to show $\mathsf{G} \subseteq \mathbf{\Sigma}_1^{\mathsf{PA}}$, because G is closed under taking complement of short GFs.

Proposition 7.73. *Conjecture 7.72 implies Conjecture 7.64, which implies Conjecture 7.56.*

Proof. Assume Conjecture 7.72 holds. Then for every fixed s, we have $n = n(s)$ for which every $g \in \mathcal{GF}_{1,s}$ has an $\exists$ PA formula representation (7.29). The last condition means there is a constant $d = d(s)$ such that $\ell(\Phi) < \ell(g)^d$. By Theorem 7.60, there exists $\gamma = \gamma(n, k) > 0$ so that G contains an AP_k whenever $|G| > \ell(\Phi)^\gamma$. So if $|\mathrm{supp}(g)| \ge \ell(g)^{\gamma d}$ then $|G| = |\mathrm{supp}(g)| \ge \ell(g)^{\gamma d} > \ell(\Phi)^\gamma$, which implies that G contains an AP_k. So $c = \gamma d$ satisfies Conjecture 7.64, which should depend only on s and k. By Proposition 7.65, Conjecture 7.64 implies Conjecture 7.56. □

Figure 7.1 illustrates the relative relations between short GFs and PA formulas if Conjecture 7.72 holds. Here SQUARES′ is the language defined in Remark 7.62.

One can of course define analogues of $\mathbf{\Sigma}_1^{\mathsf{PA}}$ and $\mathbf{\Pi}_1^{\mathsf{PA}}$ with more alternating quantifiers. But it turns out that $\mathbf{\Sigma}_{k+1}^{\mathsf{PA}} = \mathbf{\Sigma}_{k+1}^{\mathsf{G}} = \mathbf{\Sigma}_k^{\mathsf{P}}/\mathsf{poly}$ for every $k \ge 1$. This was implicit in

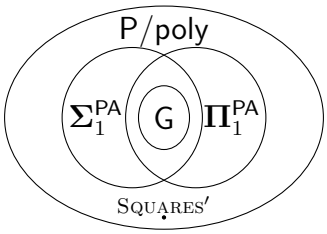
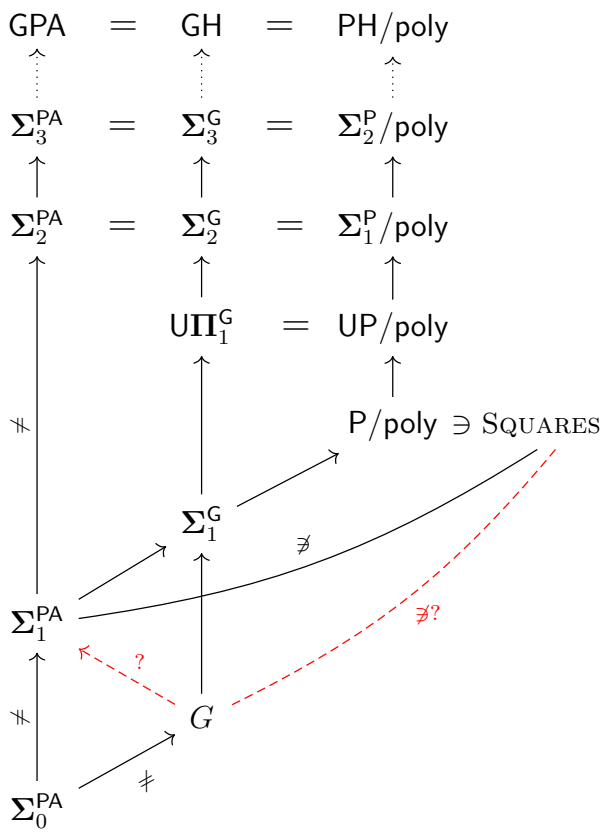


Figure 7.1: Short GFs vs. PA formulas.

Lemma 7.36 and theorems 7.39, 7.46. For the sake of completeness, we call the hierarchy of all classes $\mathbf{\Sigma}_k^{\mathsf{PA}}$ and $\mathbf{\Pi}_k^{\mathsf{PA}}$ as GPA. Obviously GPA = GH = PH/poly.

7.9.B. Complexity classes diagram. The following diagram summarizes various complexity classes that appeared in this chapter and their relationships. An arrow $X \to Y$ indicates $X \subseteq Y$. Known strict subset relations are decorated with $\neq$. Dashed arrows and segments denotes conjectural relationships.



$\mathbf{\Sigma}_{k+1}^{\mathsf{PA}} = \mathbf{\Sigma}_{k+1}^{\mathsf{G}} = \mathbf{\Sigma}_{k}^{\mathsf{P}}/\mathsf{poly}$, $k \geq 1$: sections 7.5, 7.9.

$\mathsf{U}\mathbf{\Pi}_1^{\mathsf{G}} = \mathsf{UP}/\mathsf{poly}$: Remark 7.32.

$\mathbf{\Sigma}_1^{\mathsf{G}} \subseteq \mathsf{P}/\mathsf{poly}$: Proposition 7.18.

$\textsc{Squares} \overset{?}{\notin} \mathsf{G}$: Conjecture 7.56.

$\textsc{Squares} \notin \mathbf{\Sigma}_1^{\mathsf{PA}}$: Proposition 7.59.

$\mathbf{\Sigma}_0^{\mathsf{PA}} \subsetneq \mathbf{\Sigma}_1^{\mathsf{PA}} \subsetneq \mathbf{\Sigma}_2^{\mathsf{PA}}$: Remark 7.61.

$\mathbf{\Sigma}_0^{\mathsf{PA}} \subsetneq \mathsf{G} \overset{?}{\subseteq} \mathbf{\Sigma}_1^{\mathsf{PA}}$: Section 7.9.

7.10. Proof of Lemma 7.34

Let $\overline{\mathbf{x}} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ be the array of multi-variables of dimension $n_1, \ldots, n_k$. We first prove the result when $k = 1$, i.e., when $\overline{\mathbf{x}} = \mathbf{x}_1$, $g(\overline{\mathbf{t}}) = \sum \mathbf{t}_1^{\mathbf{x}_1}$ and $f(u) = \sum u_1^{z_1}$. For convenience, we denote $\mathbf{t}_1$, $\mathbf{x}_1$, u_1, z_1 by $\mathbf{t}$, $\mathbf{x}$, u and z respectively. Also denote by n the dimension of the multi-variable $\mathbf{x}$. So $g(\mathbf{t}) = \sum \mathbf{t}^{\mathbf{x}}$ and

$$\tau_N(\mathbf{x}) = x_1 + Nx_2 + \cdots + N^{n-1}x_n.$$

Part a). Assume we are given $g \in \mathcal{GF}_{n,s}$. By Theorem 7.13, we can find the norm N of g in time $\text{poly}(\ell(g))$. By rounding N to the next power of 2, we still have $\log N \leq \text{poly}(\ell(g))$ and $\text{supp}(g) \subseteq [0, N)^n$. Let $N = 2^r$. We define $f(u)$ be the specialization of $g(\mathbf{t})$ under the following substitutions:

$$t_1 \leftarrow u,\ t_2 \leftarrow u^N, \ldots,\ t_n \leftarrow u^{N^{n-1}},$$

so that

$$\mathbf{t}^{\mathbf{x}} \ = \ u^{x_1 + Nx_2 + \ldots + N^{n-1}x_n} \ = \ u^{\tau_N(\mathbf{x})}.$$

Clearly, we have:

$$\text{supp}(f) \ = \ \tau_N(\text{supp}(g)).$$

By Theorem 7.13, polynomial substitutions can be performed in polynomial time and gives f as a short GF in $\mathcal{GF}_{1,s}$ with $\ell(f) \leq \text{poly}(\ell(g))$. This proves part a).

Part b). Given two power series $A(\mathbf{t}) = \sum \alpha_{\mathbf{x}} \mathbf{t}^{\mathbf{x}} \in \mathcal{GF}_{n,p}$, $B(t) = \sum \beta_x t^x \in \mathcal{GF}_{1,q}$ and a linear map $\tau : \mathbb{Z}^n \to \mathbb{Z}$, we define their *$\tau$-Hadamard product* as

$$C(\mathbf{t}) = A(\mathbf{t}) \star_\tau B(t) \ \coloneqq \ \sum \alpha_{\mathbf{x}} \beta_{\tau(\mathbf{x})} \mathbf{t}^{\mathbf{x}}. \tag{7.30}$$

Now assume $f(u) = \sum u^z \in \mathcal{GF}_{1,s}$, $N = 2^r$, and $\mathrm{supp}(f) \subseteq [0, N)^n$. From the above definition, it is clear that such a $g(\mathbf{t})$ satisfying (7.16) can be obtained as:

$$g(\mathbf{t}) = a(\mathbf{t}) \star_{\tau_N} f(t), \tag{7.31}$$

where

$$a(\mathbf{t}) \,=\, \sum_{\mathbf{x} \in [0,N)^n} \mathbf{t}^{\mathbf{x}} \,=\, \frac{1-t_1^N}{1-t_1} \cdots \frac{1-t_n^N}{1-t_n}.$$

with $a \in \mathcal{GF}_{n,n}$ and $\ell(a) \leq \mathrm{poly}(\log N)$.

Here the map τ_N is from Definition 7.33. So it is enough to show that the τ-Hadamard product of two short GFs is a short GF of polynomial length. The proof follows Barvinok's argument in [Bar06b] (see also lemmas 3.4 and 3.6 in [BW03]). First, notice that the τ-Hadamard product is bilinear in $A(\mathbf{t})$ and $B(t)$. Therefore, we only need to show that $C(\mathbf{t})$ is a short GF when $A(\mathbf{t})$ and $B(\mathbf{t})$ have only 1 term each, i.e., when:

$$A(\mathbf{t}) \,=\, \frac{\mathbf{t}^{\overline{a}}}{\prod_{i=1}^{p}(1-\mathbf{t}^{\overline{b}_i})} \quad \text{and} \quad B(t) \,=\, \frac{t^c}{\prod_{j=1}^{q}(1-t^{d_j})}\,. \tag{7.32}$$

Consider an (unbounded) polyhedron $P \subset \mathbb{R}^{p+q}$ with coordinates $(\zeta_1, \ldots, \zeta_p, \xi_1, \ldots, \xi_q)$, defined as:

$$P \coloneqq \left\{ \begin{array}{rcl} \zeta_1, \ldots, \zeta_p,\, \xi_1, \ldots, \xi_q & \geq & 0 \\ \tau(\overline{a} + \zeta_1\overline{b}_1 + \cdots + \zeta_p\overline{b}_p) & = & c + \xi_1 d_1 + \cdots + \xi_q d_q \end{array} \right\}. \tag{7.33}$$

By Theorem 7.20, we can write a short GF for $P \cap \mathbb{Z}^{p+q}$:

$$D(\mathbf{w}, \mathbf{v}) \coloneqq \sum_{(\boldsymbol{\zeta},\boldsymbol{\xi}) \in P} \mathbf{w}^{\boldsymbol{\zeta}}\mathbf{v}^{\boldsymbol{\xi}} = \sum_{(\boldsymbol{\zeta},\boldsymbol{\xi}) \in P} (w_1)^{\zeta_1} \ldots (w_p)^{\zeta_p} (v_1)^{\xi_1} \ldots (v_q)^{\xi_q}. \tag{7.34}$$

Furthermore, we have $D \in \mathcal{GF}_{p+q,\,p+q}$. By (7.32), the expansions of $A(\mathbf{t})$ and $B(t)$ are:

$$A(\mathbf{t}) = \sum_{\boldsymbol{\zeta} \geq 0} \mathbf{t}^{\overline{a}+\zeta_1\overline{b}_1+\cdots+\zeta_p\overline{b}_p} \quad \text{and} \quad B(t) = \sum_{\boldsymbol{\xi} \geq 0} t^{c+\xi_1 d_1+\cdots+\xi_q d_q}. \tag{7.35}$$

We substitute:

$$w_1 \leftarrow \mathbf{t}^{\overline{b}_1}, \ldots, w_p \leftarrow \mathbf{t}^{\overline{b}_p}, v_1 \leftarrow 1, \ldots, v_q \leftarrow 1.$$

By (7.33), (7.34) and (7.35), we get:

$$\mathbf{t}^{\overline{a}} D(\mathbf{t}^{\overline{b}_1}, \ldots, \mathbf{t}^{\overline{b}_p}, 1, \ldots, 1) = \sum_{(\boldsymbol{\zeta},\boldsymbol{\xi}) \in P} \mathbf{t}^{\overline{a}+\zeta_1\overline{b}_1+\cdots+\zeta_p\overline{b}_p} = A(\mathbf{t}) \,\star_\tau\, B(t) = C(\mathbf{t}).$$

By Theorem 7.13, substitution can be done in polynomial time, and results in a short GF $C(\mathbf{t})$ of index at most $p+q$. Hence, we have $C(\mathbf{t}) \in \mathcal{GF}_{n,p+q}$ and $\ell(C) \le \text{poly}(\ell(A)+\ell(B))$. Note that by taking the τ-Hadamard product, the index of C is increased to $p+q$. This pushes the index of g in (7.31) to $n+s$. So we do not get back exactly the index s for g. But $n+s$ is still a constant, and g is still a short GF in a fixed class $\mathcal{GF}_{n,n+s}$.

This completes the proof for the case $k=1$. The general case can be handled similarly.

7.11. Final remarks and open problems

7.11.A. As we mentioned in the introduction, much of this work is motivated by Barvinok's program implicit in his writing. Specifically, we were inspired by the following quote:

> "It seems hard to prove that a particular finite, but large, set $S \subset \mathbb{Z}^d$ does not admit a short rational generating function: if a particular candidate expression for $f_S(\mathbf{x})$ is not short, one can argue that we have not searched hard enough and that there is another, better candidate." [Bar06b]

In fact, the work in this chapter originally began as a followup to Chapter 6 and [NP17e], aiming to explain why the technology of short GFs was unable to directly derive Theorem 7.22 from Theorem 7.20 without additional use of geometric tools. Our theorems 7.3 and 7.5 are strong versions of this claim.

Let us also recall the main results in chapters 2 and 3, which generally say that we (algorithmically) cannot take projection of integer points in a polytope $P \subset \mathbb{Z}^n$, followed by an anti-projection. This implies that the short GF which contains the projections of $P \cap \mathbb{Z}^n$ cannot be easily projected again after we take its complement.

7.11.B. In notations of the introduction, a short GF $f_S(t)$ of a set $S \subset \mathbb{N}$ can be viewed as a presentation of S by an alternating sum of generalized (k-dimensional) arithmetic progressions. As such, there are many connections between short GFs and Arithmetic Combinatorics, which are yet to be explored (cf. [TV06]). For example, when $k=1$, taking the

positive part of these arithmetic progressions corresponds to variants of Erdős's *covering systems* which received much attention in recent years (see [Guy04, Hou15]).

Conjecture 7.1 has an especially classical feel with its claim that squares and (generalized) arithmetic progression are incompatible. There are of course both classical and recent works on squares in arithmetic progressions, but no known results seem strong enough to apply in this case (see [BGP92, Sze74, Weil84]).

7.11.C. There are two ways to think of the results in this chapters. First and foremost, they provide a very strong evidence in favor of non-polynomiality of projections and other operations with short GFs. In the opposite direction, the apparent connection to arithmetic progressions and a plethora of both analytic and combinatorial tools for working with them suggest a possibility of some lower bounds.

We would like to caution the reader. Initially we were rather optimistic about removing complexity assumptions in Theorem 7.5 by finding a direct proof of Conjecture 7.56 or some other similar lower bound. However, Proposition 7.49 and Remark 7.50 seem to suggest that this might be rather difficult. A sufficiently strong argument that shows $\mathsf{G} \subsetneq \mathsf{GH}$ could potentially show $\mathsf{UP/poly} = \mathsf{U\Pi}_1^{\mathsf{G}} \subsetneq \mathsf{GH}$, which implies $\#\mathsf{P} \not\subseteq \mathsf{FP/poly}$, an important open problem (see §7.11.E below).

On the other hand, the two lowest level G and $\mathbf{\Sigma}_1^{\mathsf{G}}$ in GH seems to behave quite differently from higher ones. So an elementary approach to prove $\mathsf{G} \subsetneq \mathsf{GH}$ is not completely ruled out.

7.11.D. The idea of Section 7.9 is to characterize all short GFs. Roughly, Conjecture 7.72 says that every short GF is the projection of a union of polynomially many polyhedra of bounded dimension. This can viewed as a converse of Theorem 7.22.

Conjecture 7.72 is possibly a wishful thinking. Unfortunately, its validity is hard to judge since we have so few explicit constructions of short GFs other than projections of integer points in polyhedra. If true, Proposition 7.73 implies Conjecture 7.1 and removes the complexity assumptions from all theorems in the introduction. Moreover, it implies exponential lower bounds on the length of short GF for squares, projections and other

theorems in the introduction.[9] These are the same bounds the *exponential time hypothesis* (ETH) implies.

7.11.E. It is worth comparing theorems 7.57 and 7.58 from the computational complexity point of view. Technically speaking, these two results are not comparable. However, one offers a much stronger evidence supporting Conjecture 7.56 than the other.

Recall that Integer Factoring is in $\mathsf{NP} \cap \mathsf{coNP}$. The experts seem to be split on whether Integer Factoring is in P or not. In fact, we do not even know if it is in $\mathsf{P/poly}$. Nor do we know of any collapse result if Integer Factoring is indeed in $\mathsf{P/poly}$. So overall, Theorem 7.57 gives a rather weak evidence for Conjecture 7.56.

On the other hand, $\#\mathsf{P}$ oracles are very powerful by Toda's theorem, and thus very unlikely to be in $\mathsf{FP/poly}$. As mentioned in Remark 7.51, $\#\mathsf{P} \subseteq \mathsf{FP/poly}$ would lead to a collapse of PH the second level. In other words, Theorem 7.58 gives a very strong evidence in favor of Conjecture 7.56.

[9] In the chain of reductions, the exponential factor appears in the proof of Proposition 7.65.

Part III

Related problems

CHAPTER 8

Presburger Arithmetic with algebraic scalar multiplications

We consider the theory $\mathcal{S}_\alpha = (\mathbb{R}, <, +, \mathbb{Z}, x \mapsto \alpha x)$, which is an extension of classical Presburger Arithmetic. It is know that $\mathcal{S}_\alpha$ is decidable for quadratic α, and undecidable for non-quadratic irrationals. We study complexity of deciding sentences in $\mathcal{S}_\alpha$. When α is quadratic and the sentence has k alternating quantifier blocks, we prove both lower and upper bounds, as towers of height $(k-3)$ and k, respectively. We also show that for α non-quadratic, already $k = 4$ alternating quantifier blocks suffice for undecidability. This chapter is a version of the preprint [HNP18].

8.1. Introduction

8.1.A. Statements of results. Let α be a fixed irrational number. The reader can always assume that α is algebraic, although some of the results below also hold in full generality.

Let $\mathcal{S}_\alpha = (\mathbb{R}, <, +, \mathbb{Z}, x \mapsto \alpha x)$. This is a first order theory over the reals, with a predicate for the integers, which also allows addition and scalar multiplication by α. This is an extension of Presburger Arithmetic. It is still decidable when α is quadratic [Hie16], but undecidable otherwise [HTy14] (see §8.1.B).

An *integer sentence* in $\mathcal{S}_\alpha$, is a sentence whose quantified variables are constrained to integer values. Such sentences have the form:

$$S \;=\; Q_1 \mathbf{x}_1 \in \mathbb{Z}^{n_1} \;\ldots\; Q_k \mathbf{x}_k \in \mathbb{Z}^{n_k} \;\; \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k), \tag{8.1}$$

where $Q_1, \ldots, Q_k \in \{\forall, \exists\}$ are k *alternating quantifiers*, and Φ is a Boolean combination of

linear inequalities of the form

$$\sum_{i=1}^{k} \sum_{j=1}^{n_i} \gamma_{ij}\, x_{ij} \;\leq\; \delta$$

with coefficients γ_{ij} and constant term δ in $\mathbb{Z}[\alpha]$. As the number k of alternating quantifier blocks and the dimensions $(n_1, \ldots, n_k)$ increase, such sentences become harder to decide, and determining exactly how hard is an important problem in computational complexity.

The number $\alpha \in \overline{\mathbb{Q}}$ is given by its minimal polynomial $p(x) \in \mathbb{Z}[x]$ of degree d, with a small enough rational interval to single out a unique root. We say that $\alpha \in \overline{\mathbb{Q}}$ is *quadratic* if $d = 2$. Each element $\gamma \in \mathbb{Z}[\alpha]$ is represented in the form $\gamma = c_0 + c_1\alpha + \ldots + c_{d-1}\alpha^{d-1}$, where $c_0, \ldots, c_{d-1} \in \mathbb{Z}$. For example, $\alpha = \sqrt{2}$ is quadratic, is given by $\{\alpha^2 - 2 = 0, \alpha > 0\}$, so that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\, a, b \in \mathbb{Z}\}$.

For $\gamma \in \mathbb{Z}[\alpha]$, the *encoding length* $\ell(\gamma)$ is the total bit length of c_i's defined above. Similarly, the encoding length $\ell(S)$ is defined to be the total bit length of all symbols in S, with integer coefficients and constants represented in binary. In the following results, the constants K, C vary from one context to another.

Theorem 8.1. *Let $\alpha \in \overline{\mathbb{Q}}$ be a quadratic irrational number, and let $k \geq 1$. An integer sentence S in $\mathcal{S}_\alpha$ with k alternating quantifier blocks can be decided in time at most*

$$K\, 2^{2^{\cdot^{\cdot^{\cdot^{2^{C\,\ell(S)}}}}}} \qquad \big(\text{tower of height } k\big).$$

Here the constants $K, C > 0$ depend only on α.

In the opposite direction, we have the following lower bound:

Theorem 8.2. *Let $\alpha \in \overline{\mathbb{Q}}$ be a quadratic irrational number, and let $k \geq 4$. Then, deciding integer sentences in $\mathcal{S}_\alpha$ with k alternating quantifier blocks and at most ck variables and inequalities requires space at least:*

$$K\, 2^{2^{\cdot^{\cdot^{\cdot^{2^{C\,\ell(S)}}}}}} \qquad \big(\text{tower of height } k-3\big),$$

Here the constants $c, K, C > 0$ only depend on α.

Theorem 8.3. *Let $\alpha \in \overline{\mathbb{Q}}$ be a quadratic irrational number. Then, deciding $\exists^6\forall^4\exists^{11}$ integer sentences in $\mathcal{S}_\alpha$ with at most K inequalities is* PSPACE*-hard, where the constant K depends only on α. Furthermore, for $\alpha = \sqrt{2}$, one can take $K = 10^6$.*

On the other hand, for non-quadratic irrationals, we have:

Theorem 8.4. *Let $\alpha \in \overline{\mathbb{Q}}$ be a non-quadratic irrational number. Then $\exists^K\forall^K\exists^K\forall^K$ integer sentences in $\mathcal{S}_\alpha$ are undecidable, where $K = 20000$.*

Theorems 8.3 and 8.2 should be compared to our previous theorems 3.1 and 3.3 in the setting of PA. The the sudden jump from polynomial hierarchy in PA to super-exponential complexity in $\mathcal{S}_\alpha$ is due to the power of irrational quadratics. Specifically, any irrational quadratic α has an infinite periodic continued fraction. From here, we can work with Ostrowski representations of integers in base α, and code string relations such as shifts, suffix/prefix and subset, which were not all possible in PA. Such operations are rich enough to encode arbitrary automata computation, and in fact Turing Machine computation in bounded space.

8.1.B. Decidability background. Hieronymi and Tychonievich showed in [HTy14] that if an expansion of $(\mathbb{R}, <)$ can define a discrete set $D \subseteq \mathbb{R}_{\geq 0}$ and also satisfies a certain reasonable denseness condition, then it can actually define every subset of D^n for every n. As an application, they proved the following result:

Theorem 8.5 ([HTy14])**.** *For any $\alpha, \beta, \gamma \in \mathbb{R}$ that are $\mathbb{Q}$-linearly independent, the structure $(\mathbb{R}, <, +, \alpha\mathbb{Z}, \beta\mathbb{Z}, \gamma\mathbb{Z})$ defines multiplication, and thus its theory is undecidable.*

Since $1, \alpha, \alpha^2$ are $\mathbb{Q}$-linearly independent for a non-quadratic α, the theory of $\mathcal{S}_\alpha$ is undecidable for such α. Indeed, a careful analysis of their work shows that this result can be further specialized to give undecidability of integer sentences in $\mathcal{S}_\alpha$:

Corollary 8.6 ([HTy14])**.** *For any non-quadratic α, integer sentences* (8.1) *of $\mathcal{S}_\alpha$ are undecidable.*

Neither Corollary 8.6 nor an upper bound on k in (8.1) needed for undecidability was stated explicitly in [HTy14], but both can be obtained by careful analysis of the proof. In Theorem 8.4, we not only give a proof of Corollary 8.6, but also explicitly quantify this result by showing that 4 alternating quantifier blocks are enough for undecidability. While our argument is based on the ideas in [HTy14], substantial extra work is necessary to reduce the number of alternations to 4 from the upper bound implicit in the proof of Theorem 8.5.

When α is quadratic, Hieronymi proved the following surprising result:

Theorem 8.7 ([Hie15, Hie16])**.** *For α quadratic, integer sentences* (8.1) *of $\mathcal{S}_\alpha$ are decidable. More generally, the structure $\mathcal{S}_\alpha$ defines a model of* Monadic Second Order Logic (MSO)*, and vice versa.*

By this result for α quadratic, to decide integer sentences (8.1), one can translate them into corresponding sentences in MSO and then decide the latter. Thus, upper and lower complexity bounds for decision in MSO can theoretically be transferred to $\mathcal{S}_\alpha$. However, an efficient direct translation between $\mathcal{S}_\alpha$ and MSO was not described in [Hie15, Hie16]. Ideally, one would like to translate a sentence from $\mathcal{S}_\alpha$ to MSO, and vice versa, with as few extra alternations as possible. In theorems 8.1 and 8.2, we explicitly quantify this translation.

8.1.C. Proofs outline. The most powerful feature of $\mathcal{S}_\alpha$ is that we can talk about Ostrowski representation of integers, which will be used as the main encoding tool. We first obtain the upper bound in Theorem 8.1 by directly translating (8.1) into the language of automata using Ostrowski encoding. Next, we show the lower bound for three alternating quantifiers (Theorem 8.3) by a general argument on the Halting Problem with polynomial space constraint, again using Ostrowski encoding.

We generalize the above argument to get lower bound for any $k \geq 3$ alternating quantifier blocks (Theorem 8.2). This is done by first translating sentences from the *weak Second Order Monadic logic* (WMSO) to $\mathcal{S}_\alpha$ sentences with only one extra alternation, and then invoke a known tower lower bound for WMSO. Overall, the chapter make transitions between $\mathcal{S}_\alpha$, finite automata and WMSO, all of which are different incarnations of the same logic theory.

Finally in the proof of Theorem 8.4, we can again use the expressibility of Ostrowski representation to reduce the upper bound of the number of alternating quantifier blocks needed for undecidability in $\mathcal{S}_\alpha$ for non-quadratic α. The use of Ostrowski representations allows us to replace more general arguments from [HTy14] by explicit computations, and thereby reduce the quantifier-complexity of certain integer sentences in $\mathcal{S}_\alpha$.

8.2. Preliminaries

8.2.A. Continued fractions and Ostrowski representation. Let $\alpha = [a_0; a_1, a_2, \dots]$ be any irrational, with $a_i \in \mathbb{Z}_+$. The convergents of α follow the recurrence relation:

$$\begin{gathered}(p_{-1}, q_{-1}) = (1, 0);\ (p_0, q_0) = (a_0, 1);\\ p_n = a_n p_{n-1} + p_{n-2},\ q_n = a_n q_{n-1} + q_{n-2} \quad \text{for } n \geq 1.\end{gathered} \tag{8.2}$$

This can be written as:

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \Gamma_0 \dots \Gamma_n \tag{8.3}$$

where $\Gamma_i = \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$. Let $\beta_n = \alpha q_n - p_n$. They have the properties:

$$\beta_n > 0 \ \text{ if } \ 2|n, \quad \beta_n < 0 \ \text{ if } \ 2 \nmid n. \tag{8.4}$$

$$\beta_0 \ > \ -\beta_1 \ > \ \beta_2 \ > \ -\beta_3 \ > \ \dots \tag{8.5}$$

$$-\beta_n \ = \ a_{n+2}\beta_{n+1} + a_{n+4}\beta_{n+3} + a_{n+6}\beta_{n+5} + \dots \quad \forall n \in \mathbb{N}. \tag{8.6}$$

These can be easily proved using (8.2). We refer to [RS92] for the basics of continued fractions.

Fact 8.8. Each $X \in \mathbb{N}$ has a unique α-Ostrowski representation:

$$X = \sum_{n=0}^{N} b_{n+1} q_n. \tag{8.7}$$

where $0 \leq b_1 < a_1$, $0 \leq b_{n+1} \leq a_{n+1}$ and $b_n = 0$ whenever $b_{n+1} = a_{n+1}$.

Proof. See [RS92, Ch. II-§4]. □

From now on, when α and X are clear from the context, we refer to (8.7) simply as the Ostrowski representation of X. We also denote the coefficient b_{n+1} by $[q_n]$. Denote by $\mathrm{Ost}(X)$ the set of q_n with $[q_n] > 0$.

We set $\zeta_\alpha \coloneqq [a_1; a_2, \dots]$, so that $\zeta_\alpha = \frac{1}{\alpha - a_0} = \frac{1}{\alpha - \lfloor \alpha \rfloor}$. Let $I_\alpha \coloneqq \big[-\frac{1}{\zeta_{\alpha,1}}, 1 - \frac{1}{\zeta_{\alpha,1}}\big)$. Define $f_\alpha : \mathbb{N} \to [0,1]$ to be the function that maps X to $\alpha X - U$, where U is the unique natural number such that $\alpha X - U \in I_\alpha$. In other words:

$$f_\alpha(X) = \alpha X - U \iff -\frac{1}{\zeta_\alpha} \le \alpha X - U < 1 - \frac{1}{\zeta_\alpha}. \tag{8.8}$$

Define $g_\alpha(X) = U$, so that $\alpha X = f_\alpha(X) + g_\alpha(X)$.

Fact 8.9. Let $\beta_n = \alpha q_n - p_n$. We have:

$$f_\alpha(X) = \sum_{n=0} b_{n+1}\beta_n \qquad \text{and} \qquad g_\alpha(X) = \sum_{n=0} b_{n+1} p_n, \tag{8.9}$$

where the coefficients b_n are from (8.7). Also $f_\alpha(\mathbb{N}) = \{f_\alpha(X) : X \in \mathbb{N}\}$ is a dense subset of the interval $[-\frac{1}{\zeta_\alpha}, 1 - \frac{1}{\zeta_\alpha})$.

Proof. See [RS92, Th. 1 on p. 25] and [RS92, Th. 1 on p. 33]. □

8.2.B. Periodic continued fractions. An irrational α is a quadratic if and only if it has a periodic continued fraction $\alpha = [a_0; a_1, \dots, a_m, \overline{b_0, b_1, \dots, b_{\kappa-1}}]$. Let $\beta = [\overline{b_0; b_1, \dots, b_{\kappa-1}}]$. It is clear that $\beta = (c\alpha + d)/(e\alpha + f)$ for some $c, d, e, f \in \mathbb{Z}$. Therefore, sentences in the theory $(\mathbb{R}, <, +, \mathbb{Z}, x \to \alpha x)$ can be expressed in $(\mathbb{R}, <, +, \mathbb{Z}, x \to \beta x)$ and vice versa. Thus, for our complexity purposes, we can always assume that our quadratic irrational α is purely periodic, i.e.,

$$\alpha = [\overline{a_0; a_1, \dots, a_{\kappa-1}}] \tag{8.10}$$

with the *minimum* period $a_0, \dots, a_{\kappa-1}$.

Fact 8.10. Let $i \in \mathbb{N}$. There exist $c_i, d_i \in \mathbb{Z}$ such that for every $n \in \mathbb{N}$ with $\kappa | n$, we have:

$$(p_{n+i}, q_{n+i}) \;=\; c_i(p_n, q_n) + d_i(p_{n+1}, q_{n+1}).$$

The coefficients c_i, d_i can be computed in time $\mathrm{poly}(i)$.

Proof. By (8.3), we have:

$$\begin{pmatrix} p_{n+i+1} & p_{n+i} \\ q_{n+i+1} & q_{n+i} \end{pmatrix} = \Gamma_0 \dots \Gamma_{n+1}\, \Gamma_{n+2} \dots \Gamma_{n+i+1} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} \Gamma_{n+2} \dots \Gamma_{n+i+1}$$

Since $\Gamma_{\kappa+t} = \Gamma_t$ for every $t \in \mathbb{N}$ and $\kappa | n$, we have $\Gamma_{n+2} \dots \Gamma_{n+i+1} = \Gamma_2 \dots \Gamma_{i+1}$. Let

$$\Gamma_2 \dots \Gamma_{i+1} = \begin{pmatrix} d_i' & d_i \\ c_i' & c_i \end{pmatrix} \tag{8.11}$$

we have

$$\begin{pmatrix} p_{n+i+1} & p_{n+i} \\ q_{n+i+1} & q_{n+i} \end{pmatrix} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} \begin{pmatrix} d_i' & d_i \\ c_i' & c_i \end{pmatrix}$$

So $(p_{n+i}, q_{n+i}) = c_i(p_n, q_n) + d_i(p_{n+1}, q_{n+1})$ and c_i, d_i only depend on i. Note that c_i, d_i can be computed in time poly(i) by (8.11). □

Remark 8.11. For $i = 0$, we have $c_0 = 1, d_0 = 0$. For $i = 1$, we have $c_1 = 0, d_1 = 1$. By (8.11), if we let $\gamma_i(v, v') \coloneqq c_i v + d_i v'$ then they follow the recurrence:

$$\gamma_0(v, v') = v,\ \gamma_1(v, v') = v',\ \gamma_i(v, v') = a_i \gamma_{i-1}(v, v') + \gamma_{i-2}(v, v'), \tag{8.12}$$

as similar to (8.2).

Fact 8.12. There are fixed $\mu, \nu, \mu', \nu' \in \mathbb{Q}$ such that

$$p_n = \mu q_n + \mu' q_{n+\kappa}, \quad q_n = \nu p_n + \nu' p_{n+\kappa}$$

for every $n \in \mathbb{N}$.

Proof. Again from (8.3), for every $n \geq 0$:

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} = \Gamma_0 \Gamma_1 \dots \Gamma_n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Since $\Gamma_{i+\kappa} = \Gamma_i$, we have:

$$\begin{pmatrix} p_{n+\kappa} \\ q_{n+\kappa} \end{pmatrix} = (\Gamma_0 \dots \Gamma_{\kappa-1})\,(\Gamma_\kappa \dots \Gamma_{n+\kappa}) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (\Gamma_0 \dots \Gamma_{\kappa-1})\,(\Gamma_0 \dots \Gamma_n) \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= (\Gamma_0 \dots \Gamma_{\kappa-1}) \begin{pmatrix} p_n \\ q_n \end{pmatrix} = \begin{pmatrix} p_{\kappa-2} & p_{\kappa-1} \\ q_{\kappa-2} & q_{\kappa-1} \end{pmatrix} \begin{pmatrix} p_n \\ q_n \end{pmatrix}.$$

Note that $p_{\kappa-1}, q_{\kappa-1}, p_{\kappa-1}, q_{\kappa-2}$ are constants. From here we easily get μ, ν, μ' and ν'. □

8.2.C. Logical formulas for working with Ostrowski representation. Let α be any irrational, not just quadratic. The convergents $\{p_n/q_n\}$ can be characterized by the *best approximation property*. Namely, u/v with $v > 1$ is a convergent p_n/q_n if and only if

$$\forall w, z\ (0 < z < v) \to |w - \alpha z| > |u - \alpha v|. \tag{8.13}$$

From this, we have $(u, v) = (p_n, q_n)$ and $(u', v') = (p_{n+1}, q_{n+1})$ if and only if they satisfy

$$\begin{aligned} \mathbf{C}_\forall(u, v, u', v') \ :=\ & 1 < v < v' \ \wedge\ \forall w, z\ \big(0 < z < v' \to \\ & |w - \alpha z| \geq |u - \alpha v| > |u' - \alpha v'|\big). \end{aligned} \tag{8.14}$$

Note that $\mathbf{C}_\forall$ is a $\forall$-formula. More generally, consider the formula:

$$\begin{aligned} \mathbf{C}_\forall(u_0, v_0, \dots, u_k, v_k) \ :=\ & 1 < v_0 < v_1 < \cdots < v_k \ \wedge \\ \forall w, z \bigwedge_{i=0}^{k} & \Big(0 < z < v_{i+1} \to |w - \alpha z| \geq |u_i - \alpha v_i| > |u_{i+1} - \alpha v_{i+1}|\Big). \end{aligned} \tag{8.15}$$

Then $\mathbf{C}_\forall$ is true if and only if $(u_0, v_0) = (p_n, q_n), \dots, (u_k, v_k) = (p_{n+k}, q_{n+k})$ for some n with $q_n > 1$, i.e., $k + 1$ consecutive convergents of α.

Remark 8.13. Hereafter, we assume $\mathbf{C}_\forall(u, v, u', v') = \text{true}$, i.e., $(u, v) = (p_n, q_n)$ and $(u', v') = (p_{n+1}, q_{n+1})$ for some $n \in \mathbb{N}$.

Define the following quantifier-free relations:

$$\begin{aligned} \mathbf{After}(u, v, u', v', Z, Z') \ :=\ & \big(-\alpha v + u < \alpha Z - Z' < -\alpha v' + u'\big) \\ & \vee\ \big(-\alpha v' + u' < \alpha Z - Z' < -\alpha v + u\big). \end{aligned} \tag{8.16}$$

$$\begin{aligned} \widetilde{\mathbf{After}}(u, v, u', v', Z, Z') \ :=\ & \big(-\alpha v + u - \alpha v' + u' < \alpha Z - Z' < -\alpha v' + u'\big) \\ & \vee\ \big(-\alpha v' + u' < \alpha Z - Z' < -\alpha v + u - \alpha v' + u'\big). \end{aligned} \tag{8.17}$$

Fact 8.14. We have:

- $\mathrm{Ost}(Z) \subset \{q_{n+1}, q_{n+2}, \dots\}$ if and only if $\mathbf{After}(u, v, u', v', Z, Z')$ holds for some Z'.
- $\mathrm{Ost}(Z) \subset \{q_{n+1}, q_{n+2}, \dots\}$ and $[q_{n+1}] < a_{n+2}$ if and only if $\widetilde{\mathbf{After}}(u, v, u', v', Z, Z')$ holds for some Z'.

Also Z' is uniquely determined by Z if **After** or $\widetilde{\textbf{After}}$ holds.

Proof. (Similar to lemmas 4.6, 4.7 and 4.8 in [Hie16])

i) Assume n is odd. If $\mathrm{Ost}(Z) \subset \{q_{n+1}, q_{n+2}, \dots\}$, then its Ostrowski representation is $Z = \sum_{k=n+1}^{N} b_{k+1} q_k$ for some $N \geq n+1$. From Fact 8.9, we have $f_\alpha(Z) = \sum_{k=n+1}^{N} b_{k+1}\beta_k$. By (8.4), we have $\beta_k > 0$ if k is odd and $\beta_k < 0$ if k is even. Combined with $b_{k+1} \leq a_{k+1}$, we have:

$$a_{n+3}\beta_{n+2} + a_{n+5}\beta_{n+4} + \dots \;<\; f_\alpha(Z) = \sum_{k=n+1}^{N} b_{k+1}\beta_k \;<\; a_{n+2}\beta_{n+1} + a_{n+4}\beta_{n+3} + \dots$$

By (8.6), this can be written as $-\beta_{n+1} < f_\alpha(Z) < -\beta_n$. By (8.8), we have $f_\alpha(Z) = \alpha Z - Z'$, where $Z' \in \mathbb{N}$ is unique such that $aZ - Z' \in I_\alpha$. Also note that $\beta_n = \alpha v - u$ and $\beta_{n+1} = \alpha v' - u'$. So the above inequalities can be written as $-\alpha v' + u' < \alpha Z - Z' < -\alpha v + u$. When n is even, the inequalities reverse to $-\alpha v + u < \alpha Z - Z' < -\alpha v' + u'$. Thus $\mathrm{Ost}(Z) \subset \{q_{n+1}, q_{n+2}, \dots\}$ implies $\textbf{After}(u, v, u', v', Z, Z')$. The converse direction can be proved similarly, using (8.5) and (8.6).

ii) The only difference here is that $[q_{n+1}] = b_{n+2}$ can be at most $a_{n+2} - 1$. Details are left to the reader. □

The relation $v \in \mathrm{Ost}(X)$, meaning that $v = q_n$ appears in $\mathrm{Ost}(X)$, is $\exists$-definable:

$$\exists Z_1, Z_2, Z_3 \;\; (v \leq Z_1 < v') \;\wedge\; \widetilde{\textbf{After}}(u, v, u', v', Z_2, Z_3) \;\wedge\; X = Z_1 + Z_2. \tag{8.18}$$

and also $\forall$-definable:

$$\forall Z_1, Z_2, Z_3 \;\; \Big[(Z_1 < v) \;\wedge\; \textbf{After}(u, v, u', v', Z_2, Z_3)\Big] \to Z_1 + Z_2 \neq X. \tag{8.19}$$

To see this, note that $v \notin \mathrm{Ost}(X)$ if and only if $X = Z_1 + Z_2$ for some Z_1, Z_2 with $\mathrm{Ost}(Z_1) \subseteq \{q_0, q_1, \dots, q_{n-1}\}$ and $\mathrm{Ost}(Z_2) \subset \{q_{n+1}, q_{n+2}, \dots\}$.

We will need one more quantifier-free formula:

$$\begin{aligned}\textbf{Compatible}(u, v, u', v', X, Z, Z') \;\coloneqq\; & X < v' \;\wedge\; \textbf{After}(u, v, u', v', Z, Z') \\ & \wedge\; \Big(X \geq v \to \widetilde{\textbf{After}}(u, v, u', v', Z, Z')\Big).\end{aligned} \tag{8.20}$$

This is satisfied if and only if

- $\mathrm{Ost}(X) \subseteq \{q_0, \ldots, q_n\}$ (by $X < v'$),
- $\mathrm{Ost}(Z) \subset \{q_{n+1}, q_{n+2}, \ldots\}$ (by **After**),
- If $q_n \in \mathrm{Ost}(X)$, then $[q_{n+1}]$ in $\mathrm{Ost}(Z)$ is strictly less than a_{n+2} (by $\widetilde{\textbf{After}}$).

In other words, **Compatible** is satisfied if and only if $\mathrm{Ost}(X)$ and $\mathrm{Ost}(Z)$ can be directly concatenated at the point $v = q_n$ to form $\mathrm{Ost}(X + Z)$ (see (8.7)).

8.3. Quadratic irrationals: Upper bound

In this section we prove Theorem 8.1. It should be emphasized that the tower height in Theorem 8.1 only depends on the number of alternating quantifiers, but not on the number of variables in the sentence S. First, we consider the case of a quantifier-free formula.

Proposition 8.15. *Let $F(\mathbf{x})$ be a quantifier-free (integer) formula in $\mathcal{S}_\alpha$, i.e., a Boolean combination of linear inequalities in $\mathbf{x} \in \mathbb{Z}^n$ with coefficients/constants in $\mathbb{Z}[\alpha]$. Then there is an automaton of size $2^{\delta\,\ell(F)}$ recognizing the set of solutions of F. The constant δ only depends on α.*

Proof. Each variable x in F takes value over $\mathbb{Z}$, but can be replaced by $x_1 - x_2$ for two variables $x_1, x_2 \in \mathbb{N}$. So we can assume that all variables take values over $\mathbb{N}$. Recall that coefficients/constants in $\mathbb{Z}[\alpha]$ are given in the form $c\alpha + d$ with $c, d \in \mathbb{Z}$. So now each inequality in F can be reorganized into the form:

$$\overline{a}\,\mathbf{y} \;+\; \alpha\,\overline{b}\,\mathbf{z} \;\;\leq\;\; \overline{c}\,\mathbf{t} \;+\; \alpha\,\overline{d}\,\mathbf{w}.$$

Here $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ are tuples coefficients in $\mathbb{N}$, and $\mathbf{y}, \mathbf{z}, \mathbf{t}, \mathbf{w}$ are subtuples of $\mathbf{x}$. Now, for each homogeneous term $\overline{a}\,\mathbf{y}$, we add in an additional variable $u = \overline{a}\,\mathbf{y}$ and replace each appearance of $\overline{a}\,\mathbf{y}$ in the inequalities by u. By doing so, we introduce extra variables, but still keep the length $\ell(F)$ linear. Now our formula splits into two parts. The first part consists of integer linear equalities:

$$u = \overline{a}\,\mathbf{y}. \qquad (*)$$

The second part consists of inequalities of the form:

$$u + \alpha v \ \leq \ w + \alpha z. \qquad (**)$$

We encode integer variables by their Ostrowski representations, and build an automaton that recognizes the solutions of F. In other words, each $x \in \mathbb{N}$ is encoded by the string $\widehat{x} = b_1\ b_2\ \ldots$, where the b_n's are from (8.7). Here only a finite number of b_n's are nonzero, so $\widehat{x}$ is a finite string. Since a_n's are periodic (8.10) and $b_n \leq a_n$, we are working with a finite alphabet.

First, by the result in [HTe18], integer addition in Ostrowski representation is recognizable by a finite automaton. In other words, the function $(\widehat{x}, \widehat{y}) \mapsto \widehat{x+y}$ is regular. Now we rewrite each equality $u = \overline{a}\,\mathbf{y}$ into single additions, using the doubling trick. For example, the equality $u = 5y + 2z$ is equivalent to the following system:

$$y_1 = y + y, \quad y_2 = y_1 + y_1, \quad y_3 = y_2 + y, \quad z_1 = z + z, \quad u = y_3 + z_1.$$

Again, we are introducing additional variables while keeping $\ell(F)$ linear. Each single addition $x = y + z$ is recognizable by a finite automaton. Taking product of all such automata, one for each addition, we get a single automaton of size $2^{\gamma\,\ell(F)}$ that recognizes the first part $(*)$. Here γ is some constant dependent on α.

Now we build an automaton for each inequality $(**)$, and later take their product automaton. Recall f_α and g_α from (8.8) and Fact 8.9. We have $\alpha x = f_\alpha(x) + g_\alpha(x)$ for every $x \in \mathbb{Z}$. Here $g_\alpha(x) \in \mathbb{Z}$ and $f_\alpha(x)$ always lies in the unit length interval I_α. For $u, v, w, z \in \mathbb{N}$, we have $u + \alpha v < w + \alpha z$ if and only if:

$$u + g_\alpha(v) < w + g_\alpha(z), \quad \text{or} \quad u + g_\alpha(v) = w + g_\alpha(z),\ f_\alpha(v) < g_\alpha(z).^1$$

So the proof is done if we can show that for input $u, v \in \mathbb{N}$:

i) The relation $u < v$ is recognizable by a finite automaton.

ii) The relation $f_\alpha(u) < f_\alpha(v)$ is recognizable by a finite automaton.

[1]The case of a sharp inequality can be handled similarly.

iii) The function $g_\alpha : \mathbb{Z} \to \mathbb{Z}$ is recognizable by a finite automaton.

Tasks i) and ii) are straightforward from basic properties of Ostrowski representation. We have $x < y$ if and only if $\widehat{x}$ is lexicographically smaller than $\widehat{y}$ when read from right to left. Also if $\widehat{x} = b_1\, b_2 \ldots$ and $\widehat{y} = b'_1\, b'_2 \ldots$ and n is the smallest index where $b_n \neq b'_n$, then:

$$\begin{aligned} n \text{ odd } &: \; b_n < b'_n \quad \text{if and only if} \quad f_\alpha(x) < f_\alpha(y), \\ n \text{ even } &: \; b_n < b'_n \quad \text{if and only if} \quad f_\alpha(x) > f_\alpha(y). \end{aligned}$$

(see [Hie16, Fact 2.13]). We have iii) left to show. □

Lemma 8.16. *The function $g_\alpha : \mathbb{Z} \to \mathbb{Z}$ is recognizable by a finite automaton with Ostrowski encoding.*

Proof of Lemma 8.16. We can assume that α is purely periodic, with minimum period κ (see §8.2.B). Also from Fact 8.12, there are fixed $\mu, \mu' \in \mathbb{Q}$ such that

$$p_n = \mu q_n + \mu' q_{n+\kappa} \quad \text{for every } n \geq 0.$$

For $x \in \mathbb{N}$ with Ostrowski representation $x = \sum_{n=0}^{N} b_{n+1} q_n$ we define:

$$\text{Shift}(x) \;\coloneqq\; \sum_{n=0}^{N} b_{n+1} q_{n+\kappa}.$$

In other words, if $\widehat{x} = b_1\, b_2 \ldots$ then $\widehat{\text{Shift}(x)} = 0^\kappa\; b_1\; b_2 \ldots$. So $x \mapsto \text{Shift}(x)$ is clearly recognizable by a finite automaton. By Fact 8.9:

$$g_\alpha(x) \;=\; \sum_{n=0} b_{n+1} p_n \;=\; \sum_{n=0} b_{n+1}(\mu q_n + \mu' q_{n+\kappa}) \;=\; \mu\, x + \mu'\, \text{Shift}(x).$$

Since $g_\alpha(x)$ is a linear combination of x and $\text{Shift}(x)$ and linear equations are regular ([HTe18]), we have an automaton for $g_\alpha : \mathbb{Z} \to \mathbb{Z}$.[2]

□

[2]By clearing denominators in μ, μ' and building automata for single additions.

Proof of Theorem 8.1. Given the sentence (8.1), by negation, we can assume $Q_1 = \exists$. First, we build an automaton A of size $2^{\delta\,\ell(F)}$ to recognize the quantifier-free part $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$.[3] Then we apply the power set construction (see e.g. [HUM06, §2.3.5]) to successively eliminate the quantifiers $Q_k\mathbf{x}_k, \ldots, Q_2\mathbf{x}_2$. This blows up the size of A by at most $k-1$ exponentiations. Thus, the resulting automaton A' has size at most a tower of height k in $\delta\,\ell(F)$. Now we still have the outer quantifier $Q_1 = \exists$ remaining, i.e., we still need to decide if A' has a solution. This is doable by a simple reachability argument, which runs in linear time relative to the size of A'. □

8.4. Quadratic irrationals: PSPACE-hardness

In this section we prove Theorem 8.3. We will first show the lower bound for a general quadratic irrational α (Theorem 8.17), and then specialize to $\alpha = \sqrt{2}$ (Corollary 8.19). By a *short sentence*, we mean one with an integer sentence in $\mathcal{S}_\alpha$ with a bounded number of variables, quantifiers and atoms (inequalities).

Theorem 8.17. *Let α be a fixed quadratic irrational and $\mathcal{S}_\alpha = (\mathbb{R}, <, +, \mathbb{Z}, x \to \alpha x)$. Then deciding short $\exists\forall\exists$ sentences in the theory $\mathcal{S}_\alpha$ is* PSPACE*-hard.*

The most important property for any quadratic irrational α is the periodicity of its continued fraction. Before proving Theorem 8.17, we construct in §8.4.A some explicit formulas in $\mathcal{S}_\alpha$ to deal with the Ostrowski representation of an integer, in this case exploiting the periodicity of α. Then we recall the definitions of Turing machine computations in Subsection 8.4.B. The proof of Theorem 8.17 is in Subsection 8.4.C, which translates Turing machine computations into Ostrowski representations of integers. An explicit bound on the number of variables and inequalities for the constructed short sentences are given in §8.4.D, where we also treat the case $\alpha = \sqrt{2}$.

[3] Actually, we first need to make $Q_k = \exists$ so that additional variables in the proof of Lemma 8.15 can be inserted after Q_k. After that we make $Q_1 = \exists$. Apply negations whenever necessary.

8.4.A. Ostrowski representation for quadratic irrationals. We only need to consider a purely periodic α with minimum period κ (see §8.2.B). Let $K = \operatorname{lcm}(2, \kappa)$.

We can define the set of convergents (p_n, q_n) for which $K|n$. Recall γ_i from Remark 8.11 (also see Fact 8.10). Now define the formula:

$$\begin{aligned}\mathbf{D}_\forall^K(u,v,u',v') \;\coloneqq\; 1 < v < v' \;\wedge\; 0 < \alpha v - u \;\wedge\; \forall w, z \bigwedge_{i=0}^{\kappa+1} \Big(0 < z < \gamma_{i+1}(v,v') \\ \to |w - \alpha z| \geq |\gamma_i(u,u') - \alpha\gamma_i(v,v')| > |\gamma_{i+1}(u,u') - \alpha\gamma_{i+1}(v,v')|\Big).\end{aligned} \tag{8.21}$$

We claim that $\mathbf{D}_\forall^K$ is satisfied if and only if $(u,v) = (p_{tK}, q_{tK})$ and $(u',v') = (p_{tK+1}, q_{tK+1})$ for some $t > 0$. First, the condition $\forall w, z\,\big[0 < z < \gamma_{i+1}(v,v') \to \dots\big]$ implies that the pairs $\big(\gamma_i(u,u'), \gamma_i(v,v')\big)_{0 \leq i \leq \kappa+1}$ are $\kappa+2$ consecutive convergents (see (8.13) and (8.14)). In other words, there is an $n > 0$ such that:

$$\big(\gamma_i(u,u'), \gamma_i(v,v')\big) = (p_{n+i}, q_{n+i}), \quad 0 \leq i \leq \kappa + 1.$$

Also by Remark 8.11, we have $\big(\gamma_0(u,u'), \gamma_0(v,v')\big) = (u,v)$ and $\big(\gamma_1(u,u'), \gamma_1(v,v')\big) = (u',v')$. So $(u,v) = (p_n, q_n)$ and $(u',v') = (p_{n+1}, q_{n+1})$. Then by (8.12):

$$\big(\gamma_2(u,u'), \gamma_2(v,v')\big) = (a_2u' + u, a_2v' + v) = (a_2p_{n+1} + p_n, a_2q_{n+1} + q_n).$$

must be the next convergent (p_{n+2}, q_{n+2}). Combined with (8.2), we have

$$p_{n+2} = a_{n+2}p_{n+1} + p_n = a_2p_{n+1} + p_n,$$

which implies $a_{n+2} = a_2$. Similarly, we have $a_{n+i} = a_i$ for all $2 \leq i \leq \kappa + 1$. Since κ is the minimum period of α, we must have $\kappa|n$. Also because $0 < \alpha v - u = \alpha q_n - p_n$, we have $2|n$ (see (8.4)). Therefore, $\mathbf{D}_\forall^K(u,v,u',v') =$ true if and only if there is some $t \geq 1$ such that $(u,v) = (p_{tK}, q_{tK})$ and $(u',v') = (p_{tK+1}, q_{tK+1})$. In prenex normal form, $\mathbf{D}_\forall^K$ is a $\forall^2$-formula.

Next, we can also define the set of convergents q_n for which $M|n$, where M is a large multiple of K to be specified later. To do this, we take a large enough prime P and define:

$$\mathbf{D}_\forall^M(u,v,u',v') \;\coloneqq\; \mathbf{D}_\forall^K(u,v,u',v') \;\wedge\; v \equiv q_0 \,(\mathrm{mod}\, P) \;\wedge\; v' \equiv q_1 \,(\mathrm{mod}\, P). \tag{8.22}$$

Let $M > 0$ be the least multiple of K such that $(q_M, q_{M+1}) \equiv (q_0, q_1) \pmod{P}$. Then $\mathbf{D}^M_\forall(u, v, u', v') =$ true if and only if there is a $t \geq 1$ such that $(u, v) = (p_{tM}, q_{tM})$. If P is large then M should also be large. Note that congruences can be expressed by $\forall$ with one extra variable[4]. So $\mathbf{D}^M_\forall$ is a $\forall^3$-formula in prenex normal form.

Remark 8.18. The multiple $M = mK$ exists because we have:

$$\begin{pmatrix} p_{mK+1} & p_{mK} \\ q_{mK+1} & q_{mK} \end{pmatrix} \;=\; \Gamma_0 \,\ldots\, \Gamma_{mK+1} \;=\; \Gamma_0\,\Gamma_1\,(\Gamma_2 \,\ldots\, \Gamma_{K-1}\,\Gamma_0\,\Gamma_1)^m$$

and the matrix $\Gamma_2 \ldots \Gamma_{K-1}\Gamma_0\Gamma_1$ is invertible mod P. So there is a smallest $m > 0$ such that:

$$\begin{pmatrix} p_{mK+1} & p_{mK} \\ q_{mK+1} & q_{mK} \end{pmatrix} \equiv \Gamma_0\Gamma_1 = \begin{pmatrix} p_0 & p_1 \\ q_0 & q_1 \end{pmatrix} \pmod{P}.$$

Also by the recurrence (8.2), we have $(p_{mK+i}, q_{mK+i}) \equiv (p_i, q_i) \pmod{P}$ for ever i.

Recall from (8.7) that every $T \in \mathbb{N}$ has a unique Ostrowski representation:

$$T = \sum_{n=0}^{N} b_{n+1} q_n,$$

with $0 \leq b_1 < a_1$, $0 \leq b_{n+1} \leq a_{n+1}$ and $b_n = 0$ if $b_{n+1} = a_{n+1}$. We denoted $[q_n] \coloneqq b_{n+1}$. For the rest of the proof, we only consider numbers T that satisfy:

$$\begin{aligned} [q_n] \quad &\text{if} \quad 2 \nmid n, \\ [q_n] = 0, 1 \quad &\text{if} \quad 2 | n. \end{aligned} \tag{8.23}$$

This is guaranteed by the following formula:

$$\begin{aligned} \mathbf{ZeroOne}_{\forall\exists}(T) \;\coloneqq\; &\forall u, v, u', v' \; \mathbf{C}_\forall(u, v, u', v') \;\to\; \exists Z_1, Z_2, Z_3 \\ &\Big(0 > \alpha v - u \to \big[Z_1 < v \;\wedge\; \mathbf{After}(u, v, u', v', Z_2, Z_3) \;\wedge\; T = Z_1 + Z_2\big]\Big) \\ &\Big(0 < \alpha v - u \to \big[Z_1 < 2v \;\wedge\; \mathbf{Compatible}(u, v, u', v', Z_1, Z_2, Z_3) \;\wedge\; T = Z_1 + Z_2\big]\Big). \end{aligned} \tag{8.24}$$

Here **After** and **Compatible** were defined earlier. Note that $\mathbf{ZeroOne}_{\forall\exists}$ is a $\forall^4\exists^3$-formula.

[4]We have $x_1 \equiv x_2 \pmod{P}$ if and only if $\forall w \; x_1 - x_2 - Pw = 0 \;\vee\; |x_1 - x_2 - Pw| \geq P$.

For two natural numbers T and X, the formula:

$$\begin{aligned}\mathbf{Pref}_{\forall\exists}(X,T) \;\coloneqq\; \forall u,v,u',v' \left(\mathbf{C}_{\forall}(u,v,u',v') \;\wedge\; v \le X \;\wedge\; X < v'\right) \rightarrow \\ \exists Z,Z'\, \mathbf{Compatible}(u,v,u',v',X,Z,Z') \;\wedge\; T = X+Z.\end{aligned} \tag{8.25}$$

is true exactly when $\mathrm{Ost}(X)$ forms a prefix of $\mathrm{Ost}(T)$ if viewed as 0/1 strings. Note that $\mathbf{Pref}_{\forall\exists}$ is a $\forall^4\exists^2$-formula in prenex normal form.

8.4.B. Turing machines. Consider any PSPACE-complete language $\mathcal{L} \subset \{0,1\}^*$ and a 1-tape Turing Machine $\mathcal{M}$ that can decide it. This means that given an input $x \in \{0,1\}^*$ on its tape $\mathcal{T}$, $\mathcal{M}$ will run in space $\mathrm{poly}(|x|)$ and output 1 if $x \in \mathcal{L}$ and 0 otherwise. More precisely, we have $\mathcal{T} = x0\ldots$ at the beginning, and $\mathcal{T} = 10\ldots$ or $\mathcal{T} = 00\ldots$ at the end. WLOG, we can also assume $\mathcal{M}$ has a unique halting state H.

In [NW06], a small universal 1-tape Turing machine $U = (\mathbf{Q}, \mathbf{\Sigma}, \sigma_1, \delta, q_1, q_2)$, with $|\mathbf{Q}| = 8$ states and $|\mathbf{\Sigma}| = 4$ tape symbols.[5] Using U, we can simulate $\mathcal{M}$ in polynomial time and space. More precisely, suppose $\mathcal{M}$ is a PSPACE-complete TM as describe above and x is an input to $\mathcal{M}$. Then we can encode $\mathcal{M}$ and x in polynomial time as a string $\langle \mathcal{M}x\rangle \in \mathbf{\Sigma}^*$. Upon input $\langle \mathcal{M}x\rangle$, U simulates $\mathcal{M}$ on x, and halts with one of the two possible configurations:

$$U(\langle \mathcal{M}x\rangle) = \text{“yes”} \quad \text{if} \quad \mathcal{M}(x) = 1, \quad U(\langle \mathcal{M}x\rangle) = \text{“no”} \quad \text{if} \quad \mathcal{M}(x) = 0. \tag{8.26}$$

Here “yes” and “no” are the final state-tape configurations of U, which correspond to $\mathcal{M}$'s final configurations (H, $10\ldots$) and (H, $00\ldots$), respectively. By the encoding in [NW06], these final “yes”/“no” configurations of U have lengths $O(|\mathcal{M}|)$, which are constant when we fix $\mathcal{M}$. Furthermore, the computation $U(\langle \mathcal{M}x\rangle)$ takes time/space polynomial in the time/space of the computation $\mathcal{M}(x)$.[6] Since $\mathcal{M}(x)$ runs in space $\mathrm{poly}(|x|)$, so does U upon input $\langle \mathcal{M}x\rangle$.

Consider the simulation $U(\langle \mathcal{M}x\rangle)$. Denote by $\mathcal{T}_i \in \mathbf{\Sigma}^{\lambda-1}$ the contents of U's tape on step i-th. Here $\lambda = \mathrm{poly}(|x|)$ is a polynomial bound on the tape length. Also denote by $\mathbf{s}_i \in \mathbf{Q}$

[5] $\mathbf{Q}$ – states, $\mathbf{\Sigma}$ – tape symbols, $\sigma_1 \in \mathbf{\Sigma}$ – blank symbol, $\delta : \mathbf{Q}\times\mathbf{\Sigma} \to \mathbf{Q}\times\mathbf{\Sigma}\times\{L,R\}$ – transitions, $q_1 \in \mathbf{Q}$ – start state, $q_2 \in \mathbf{Q}$ – unique halt state.

[6] It actually takes linear space and quadratic time.

the state of U on step i-th. The i-th head position of U is some number $1 \le \pi_i \le \lambda - 1$.

Altogether, for step i, we can encode the tape content $\mathcal{T}_i$, the state $\mathbf{s}_i$ and the tape head position π_i by the string:

$$\mathcal{T}_i' \;=\; [\times,\times][\times,\mathcal{T}_i(1)]\;\ldots\;[\times,\mathcal{T}_i(\pi_i-1)]\,[\mathbf{s}_i,\mathcal{T}_i(\pi_i)]\,[\times,\mathcal{T}_i(\pi_i+1)]\;\ldots\;[\times,\mathcal{T}_i(\lambda-1)]. \quad (8.27)$$

Here $\times$ is a special marker symbol and $\mathcal{T}_i(j) \in \mathbf{\Sigma}$ is the j-th symbol of $\mathcal{T}_i$. The marker block $[\times,\times]$ is at the beginning of each $\mathcal{T}_i'$, which is distinct from the other $\lambda - 1$ blocks in $\mathcal{T}_i'$. Note that $\mathcal{T}_i'$ has in total λ blocks. Now we concatenate $\mathcal{T}_i'$ over all steps $1 \le i \le \rho$, where ρ is the terminating step of the simulation. Let

$$\boldsymbol{T} = \mathcal{T}_1'\;\ldots\;\mathcal{T}_\rho'.$$

We call $\boldsymbol{T}$ the transcript of U on input $\langle \mathcal{M}x\rangle$, denoted by $\boldsymbol{T} = U(\langle \mathcal{M}x\rangle)$. The last segment in $\mathcal{T}_\rho'$ contains the "yes" configuration if and only if $\mathcal{M}(x) = 1$. In total, $\boldsymbol{T}$ has $\lambda\rho$ blocks.

Denote by $\mathbf{B} = \{[\times,\times]\} \cup (\{\times\} \times \mathbf{\Sigma}) \cup (\mathbf{Q} \times \mathbf{\Sigma})$ the set of all possible blocks in $\mathcal{T}$, with $|\mathbf{B}| = 37$. Let $B_t \in \mathbf{B}$ be the t-th block in $\mathcal{T}$. By the transition rules of U, the block $B_{t+\lambda}$ should only depend on B_{t-1}, B_t and B_{t+1}. Thus, there is a function $f : \mathbf{B}^3 \to \mathbf{B}$ such that:

$$B_{t+\lambda} = f(B_{t-1}, B_t, B_{t+1}) \quad \text{for every} \quad 0 \le t < \lambda(\rho - 1).$$

Note that for the separator block $[\times,\times]$, we should have $f(B,[\times,\times],B') = \mathbf{0}$ for all B, B'.

8.4.C. Proof of Theorem 8.17. Recall the formulas $\mathbf{D}^K_\forall$, $\mathbf{D}^M_\forall$, $\mathbf{ZeroOne}_{\forall\exists}$, $\mathbf{Pref}_{\forall\exists}$ from §8.4.A. We encode the transcript $\boldsymbol{T}$ by a number $T \in \mathbb{N}$ satisfying (8.23). To be precise, first we view $\mathbf{B}$ as a set of 37 distinct strings in $\{0,1\}^6$, each containing at least one 1. Then we pick a large enough prime P in $\mathbf{D}^M_\forall$ so that $M > 10$. Recall the notation $[q_n]$ in (8.23). If $B_t \in \mathbf{B}$ is the t-th block in $\boldsymbol{T}$, then we should have:

$$[q_{tM}][q_{tM+2}]\ldots[q_{tM+10}] = B_t \quad \text{and} \quad [q_{tM+12}]\ldots[q_{(t+1)M-2}] = 0\ldots0. \quad (8.28)$$

For the rest of the proof, we view $\mathrm{Ost}(T)$ as a binary string, and use B_t to denote its t-th block.

Let $(u,v) = (p_{tM}, q_{tM})$ and $(u',v') = (p_{tM+1}, q_{tM+1})$ for some $t \geq 1$. For every triple $B, B', B'' \in \mathbf{B}$, we will construct a formula $\mathbf{Read}_{\exists}^{B,B',B''}(u,v,u',v',T)$ to check if the three blocks B_{t-1}, B_t, B_{t+1} in T match with B, B', B'' in the sense of (8.28). We will also construct a formula $\mathbf{Next}_{\exists}^{B,B',B'}(u,v,u',v',T)$ to check if the block $B_{t+\lambda}$ in T agrees with the transition function f, i.e., $B_{t+\lambda} = f(B, B'B'')$. For the rest of the proof, the meaning of c_i, d_i, a, b will change depending on the context.

• Constructing $\mathbf{Next}_{\exists}^{B,B',B'}$: Let $r_1 = \lambda M$ and $r_2 = (\lambda+1)M$. Then the block $B_{t+\lambda}$ correspond to those $[q_{tM+i}]$ with $r_1 \leq i < r_2$. By Fact 8.10, we can write each convergent (p_{tM+i}, q_{tM+i}) with $r_1 - 1 \leq i \leq r_2$ as a linear combination $c_i(u,v) + d_i(u',v')$. Here the coefficients $c_i, d_i \in \mathbb{Z}$ are independent of t, but do depend on λ. They can be computed explicitly in time poly(λ). Let $\widetilde{B} = f(B, B', B'')$. Then we sum up all q_{tM+r_1+2j} for every $0 \leq j < 6$ such that the j-th bit in $\widetilde{B}$ is '1'. This sum can be expressed as $av + bv'$ for some $a, b \in \mathbb{Z}$ computable in time poly(λ). Note that c_i, d_i and a, b depend on λ and also the triple B, B', B''. Then $B_{t+\lambda} = \widetilde{B}$ if and only if we can uniquely write $T = W_1 + (av + bv') + W_2$, where $W_1 < q_{tM+r_1-1}$ and $\mathrm{Ost}(W_2) \subset \{q_n : n \geq tM + r_2\}$. Let $Z_1 = W_1 + (av + bv')$ and $Z_2 = W_2$. They satisfy:

i) $0 \leq Z_1 - (av + bv') < q_{tM+r_1-1}$,

ii) $\mathrm{Ost}(Z_2) \subset \{q_n : n \geq tM + r_2\}$.

Then the formula we want is:

$$\mathbf{Next}_{\exists}^{B,B'B''}(u,v,u',v',T) \coloneqq \exists Z_1, Z_2, Z_3 \ \text{i)} \wedge \text{ii)} \wedge T = Z_1 + Z_2. \tag{8.29}$$

Here i) is written directly as linear inequalities in v, v' and Z_1. By (8.16), we can express ii) as $\mathbf{After}(p_{tM+r_2-1}, q_{tM+r_2-1}, p_{tM+r_2}, q_{tM+r_2}, Z_2, Z_3)$, which is again linear inequalities in u, v, u', v' and Z_2, Z_3.

• Constructing $\mathbf{Read}_{\exists}^{B,B',B'}$: Note that the blocks $B_{t-1}B_tB_{t+1}$ in T correspond to $[q_n]$ with $(t-1)M \leq n < (t+2)M$. So we just need to express (p_{tM+i}, q_{tM+i}) for $-M-1 \leq i \leq 2M$ as linear combinations $c_i(u,v) + d_i(u',v')$. Then we sum up all q_{tM+i} that should correspond to the '1' bits in B, B', B'', which is again some linear combination $av + bv'$. This time the

coefficients c_i, d_i, a, b do *not* depend on λ and can be computed in *constant* time. Now we have $B_{t-1}B_tB_{t+1} = BB'B''$ if and only if we can uniquely write $T = Z_1 + Z_2$, where Z_1 and Z_2 satisfy two conditions i'-ii') similar to i-ii) above. The formula we want is:

$$\mathbf{Read}_{\exists}^{B,B',B''}(u,v,u',v',T) \;\coloneqq\; \exists Z_1, Z_2, Z_3 \;\text{ i')} \;\wedge\; \text{ii')} \;\wedge\; T = Z_1 + Z_2. \tag{8.30}$$

Again i'-ii') can be expressed as linear inequalities in u, v, u', v' and Z_1, Z_2, Z_3.

So a single transition of T from B, B', B'' to $f(B, B', B'')$ can be written as:

$$\begin{aligned}\mathbf{Tran}_{\exists}^{B,B',B''}(u,v,u',v',T) \;\coloneqq\; &\mathbf{Read}_{\exists}^{B,B',B''}(u,v,u',v',T) \\ &\wedge\; \mathbf{Next}_{\exists}^{B,B',B''}(u,v,u',v',T).\end{aligned} \tag{8.31}$$

Note that $\mathbf{Tran}_{\exists}$ is an $\exists^6$-formula. To ensure that T obeys the transition rule $f : \mathbf{B}^3 \to \mathbf{B}$ every where, we simply require:

$$\forall u, v, u', v' \left(\mathbf{D}_{\forall}^{M}(u,v,u',v') \;\wedge\; cv + dv' \le T\right) \to \bigvee_{B,B',B''\in\mathbf{B}} \mathbf{Tran}_{\exists}^{B,B',B''}(u,v,u',v',T). \tag{8.32}$$

Here we write $q_{(t+\lambda)M} = cv + dv'$, with c, d computable in $\mathrm{poly}(\lambda)$ time. $\mathbf{D}_{\forall}^{M}(u,v,u',v')$ means $v = q_{tM}$ is the beginning of some block B_t, and $q_{(t+\lambda)M} = cv + dv'$ is the beginning of the block $B_{t+\lambda}$, should it not exceed T.

We need one last formula to say that T ends in the "yes" configuration (see (8.26)). Recall that "yes" has fixed length. Assume "yes" starts at $v = q_{tM}$. Then just like before, we can sum up all q_{tM+i} that correspond to '1' bits in "yes". This sum can be written as $av + bv'$, with $a, b \in \mathbb{Z}$ explicit *constants* independent of λ. Also observe that $q_{tM-1} = q_{tM+1} - a_1 q_{tM} = v' - a_1 v$. So the formula:

$$\mathbf{E}_{\exists\forall}(T) \;\coloneqq\; \exists u, v, u', v', Z \;\; \mathbf{D}_{\forall}^{M}(u,v,u',v') \;\wedge\; Z < v' - a_1 v \;\wedge\; T = Z + av + bv' \tag{8.33}$$

is true if and only if T ends in "yes". Note that $\mathbf{E}_{\exists\forall}$ is a $\exists^5\forall^3$-formula.

Finally, given $x \in \{0,1\}^{\ell}$, we can easily construct in time $\mathrm{poly}(\ell)$ the content of the first segment $\mathcal{T}_1'$ in $\boldsymbol{T}$ (see (8.27)). Again, $\mathcal{T}_1'$ is the starting configuration of the simulation $U(\langle \mathcal{M}x \rangle)$, which is basically just $\langle \mathcal{M}x \rangle$. Then we compute in time $\mathrm{poly}(\ell)$ the $X \in \mathbb{N}$

whose Ostrowski representation corresponds to $\mathcal{T}_1'$. We also compute the tape length bound $\lambda = \text{poly}(\ell)$ to be used in $\mathbf{Tran}_\exists$. Now construct the sentence:

$$\exists T \;\; \mathbf{ZeroOne}_{\forall\exists}(T) \;\wedge\; \mathbf{Pref}_{\forall\exists}(T, X) \;\wedge\; \mathbf{E}_{\exists\forall}(T) \;\wedge\; \Big[\forall u, v, u', v' \\ \big(\mathbf{D}_\forall^M(u, v, u', v') \;\wedge\; cv + dv' \le T\big) \to \bigvee_{B,B',B''\in\mathbf{B}} \mathbf{Tran}_\exists^{B,B',B''}(u, v, u', v', T)\Big]. \tag{8.34}$$

Here $\mathbf{ZeroOne}_{\forall\exists}(T)$ ensures condition (8.23), $\mathbf{Pref}_{\forall\exists}(X, T)$ ensures that X is a prefix of T, $\mathbf{E}_{\exists\forall}(T)$ says that T ends in "yes", and the rest says that T follows the transition rules (see (8.32)). So (8.34) is an $\exists\forall\exists$-sentence with total length $\text{poly}(\ell)$, which is satisfied if and only if $X \in \mathcal{L}$. This proves Theorem 8.17.

8.4.D. Analysis of the construction. We bound the number of variables in (8.34). Consider the last term $[\forall u, v \dots]$. First, there are $\forall^4$ variables u, v, u', v'. Each $\mathbf{Tran}_\exists^{B,B',B''}$ is an $\exists^6$-formula, which also commutes with the big disjunction. Also $\neg\mathbf{D}_\forall^M$ is an $\exists^3$-formula, which can be merged with the $\exists^6$ part.[7] Overall, the last term is of the form $\forall^4\exists^6$.

Next, recall that $\mathbf{ZeroOne}_{\forall\exists}$, $\mathbf{Pref}_{\forall\exists}$ in §8.4.A are of the forms $\forall^4\exists^3$ and $\forall^4\exists^2$ and respectively. Since we are taking their conjunctions with the last term $\forall^4\exists^6$, their outer $\forall^4$ variables can be merged. However, their $\exists$ variables need to be concatenated. Overall, we have $\forall^4\exists^{11}$ for $\mathbf{ZeroOne}_{\forall\exists}$, $\mathbf{Pref}_{\forall\exists}$ and the last term. The term $\mathbf{E}_{\exists\forall}$ is $\exists^5\forall^3$. Merging its $\forall^3$ variables with the other three terms, we have $\exists^5\forall^4\exists^{11}$. Lastly, we add in $\exists T$ and get a $\exists^6\forall^4\exists^{11}$ sentence.

The number of inequalities in all constructed formulas is bounded in the table below. Overall, the number of inequalities in (8.34) is at most:

$$34 + 26 + 14 + 10(\kappa + 2) + 12 + 10(\kappa + 2) + 16|\mathbf{B}|^3 \;=\; 810534 + 20(\kappa + 2).$$

Corollary 8.19. *For $\alpha = \sqrt{2}$ deciding $\exists^6\forall^4\exists^{11}$ sentences with at most 10^6 inequalities in $\mathcal{S}_\alpha$ is* PSPACE*-hard.*

Proof. Note that $\sqrt{2} + 1 = [2; 2, \dots]$ has minimum period $\kappa = 1$. □

[7] We need to rewrite every implication "$a \to b$" as "$\neg a \vee b$".

$x = y$	2
$\lvert x\rvert \geq \lvert y\rvert$, $\lvert x\rvert > \lvert y\rvert$	4
After, $\widetilde{\textbf{After}}$	4
Compatible	10
$\mathbf{C}_\forall$	12
$\mathbf{ZeroOne}_{\forall\exists}$	34
$\mathbf{Pref}_{\forall\exists}$	26
$\mathbf{Read}_\exists$	8
$\mathbf{Next}_\exists$	8
$\mathbf{Tran}_\exists$	16
$\mathbf{D}_\forall^K$	$3 + 10(\kappa + 2)$
$\mathbf{D}_\forall^M$	$11 + 10(\kappa + 2)$
$\mathbf{E}_{\exists\forall}$	$14 + 10(\kappa + 2)$

8.5. Quadratic irrationals: General lower bound

In this section we prove Theorem 8.2. Let us recall Monadic Second Order logic MSO $= (\mathbb{N}, \mathcal{P}(\mathbb{N}), s_\mathbb{N}, \in)$, where $\mathcal{P}(\mathbb{N})$ is the (monadic) predicate for subsets of $\mathbb{N}$, and $s_\mathbb{N}$ is the successor function $n \to n + 1$. Its weak variant is WMSO $= (\mathbb{N}, \mathcal{P}_{\text{fin}}(\mathbb{N}), s_\mathbb{N}, \in)$, which only quantifies over *finite* subsets of $\mathbb{N}$. We refer to [GTW] for the equivalence between WMSO and the theory of automata equipped with quantifiers. First, we prove a similar lower bound for WMSO:

Theorem 8.20. *Deciding a sentence S in* WMSO *with $k + 2$ alternating quantifiers and $O(k)$ variables requires space at least:*

$$\rho\, 2^{\cdot^{\cdot^{\cdot^{2^{\eta \ell(S)}}}}}.$$

Here the tower has height k, and ρ, η are absolute constants.

The proof is similar to that of Theorem 8.17. Recall that in $\mathbf{Next}_\exists^{B,B'B''}$, if $v = q_{tM}$ and

$v' = q_{tM+1}$ then the shifted convergent $q_{(t+\lambda)M}$ can be written as $cv+dv'$, with $c, d \in \mathbb{Z}$ having lengths poly(λ). The resulting sentence (8.34) has length poly(λ), and is PSPACE-complete to decide. To prove a tower lower bound, we need to construct a shift map

$$S_k \ : \ q_{tM} \mapsto q_{(t+g(\lambda))M},$$

so that $g(\lambda)$ is a tower of height $(k-2)$ in λ. Here the formula S_k is allowed to have length poly(λ) and at most $k-2$ alternating quantifiers. The following construction is classical. It was first used in [Mey75] to prove that WMSO has non-elementary decision complexity, and was later improved on in [Sto74]. An expository version is given in [GTW, Ch. 13]. For completeness, we reproduce it below in the setting of WMSO with some improvements on the number of alternating quantifiers. Afterwards, we translate it back to $\mathcal{S}_\alpha$.

We think of each subset $X \in \mathcal{P}_{\text{fin}}(\mathbb{N})$ as a binary string of finite length. The relation $n \in X$ simply means that the n-th bit in X is 1. Let

$$g_0(\lambda) = \lambda \quad \text{and} \quad g_{k+1}(\lambda) = g_k(\lambda)\, 2^{g_k(\lambda)},\ k \geq 0.$$

The idea of the construction is as follows. We will iteratively define formulas $F_k(x, y, A, C)$ such that F_{k+1} is true if and only if:

$$\begin{aligned} y &= x + g_{k+1}(\lambda), \\ A &= 0^x|100\ldots0|100\ldots0|100\ldots0|100\ldots0|\ldots|100\ldots0|10^*, \\ C &= 0^x|000\ldots0|100\ldots0|010\ldots0|110\ldots0|\ldots|111\ldots1|00^*. \end{aligned}$$

Here A, C have $2^{g_k(\lambda)}$ blocks, each of length $g_k(\lambda)$. The blocks in C represent the integers $0, 1, \ldots, 2^{g_k(\lambda)} - 1$ in binary. The blocks in A mark the beginning of the blocks in C. The first '1' in A is at position x and the last '1' in A is at position y.[8] In total, the difference $y - x$ is $g_k(\lambda)2^{g_k(\lambda)} = g_{k+1}(\lambda)$. First, we can define the basic quantifier-free case:

$$F_0(x, y, A, C) \ \coloneqq \ \text{Singleton}(x) \ \wedge \ \text{Singleton}(y) \ \wedge \ y = x + \lambda.^{9}$$

[8] Position indexing starts at 0.

[9] Here $x + \lambda$ represents λ iterations of the successor function $s_{\mathbb{N}}$.

For this case A and C do not matter. Now recall the carry rule for addition by 1 in binary. If $X = x_0x_1\ldots$ in binary then $Y = X + 1 = y_0y_1\ldots$ satisfies:

$$\begin{aligned} x_0 &= \neg y_0 \quad \text{(the least significant digit always switches)} \\ x_i = 1, y_i = 0 &\rightarrow x_{i+1} = \neg y_{i+1} \quad \text{(carry rule)} \\ x_{i+1} &= y_{i+1} \quad \text{otherwise.} \end{aligned}$$

In the context of WMSO, these rules can be summarized as:

$$0 \in X \;\leftrightarrow\; 0 \notin Y; \tag{8.35}$$

$$i \in X \wedge i \notin Y \;\leftrightarrow\; (i+1 \in X \;\leftrightarrow\; i+1 \notin Y). \tag{8.36}$$

Observe that if we apply these rules on blocks of length $g_k(\lambda)$, starting with $0\ldots0$, we get:

$$00\ldots0|10\ldots0|01\ldots0|\ldots|11\ldots1|00\ldots0|10\ldots0|\ldots$$

So the blocks do cycle back to $0\ldots0$ eventually. This needs to be taken care of in the definition of F_{k+1}, because we want each block of C to be unique. We define:

$$F_{k+1}(x,y,A,C) \;\coloneqq\; \text{Singleton}(x) \;\wedge\; \text{Singleton}(y) \;\wedge\; x < y \;\wedge \tag{8.37}$$

$$\forall z,w,t,D,E \Big(\big[F_k(z,w,D,E) \;\wedge\; \text{Singleton}(t)\big] \;\rightarrow$$

$$\Big[z = x \vee z = y \;\rightarrow\; z \in A,\, z \notin C;\;\; z < x \vee y < z \;\rightarrow\; z \notin A,\, z \notin C; \tag{8.38}$$

$$x = z,\, z < t < w \;\rightarrow\; t \notin A,\, t \notin C;\; x \le z < w \le y \;\rightarrow\; (z \in A \leftrightarrow w \in A); \tag{8.39}$$

$$z \in A,\, w < y \;\rightarrow\; (z \in C \leftrightarrow w \notin C) \tag{8.40}$$

$$x \le z < w < y,\, z+1 \notin A \;\rightarrow\; \big(z \in C,\, w \notin C \;\leftrightarrow\; (z+1 \in C \leftrightarrow w+1 \notin C)\big); \tag{8.41}$$

$$x \le z < w < y,\, z+1 \in A \;\rightarrow\; (z \in C \rightarrow w \in C); \tag{8.42}$$

$$w = y,\, z \le t < w \;\rightarrow\; t \in C\Big] \;\Big). \tag{8.43}$$

For readability, we use $\wedge$, and ; interchangeably to denote conjunctions. Lines (8.38) and (8.39) set up the first block in A and C, and say that A and C are all empty outside the range $[x, y]$. Line (8.40) expresses the increment rule (8.35) for every two consecutive blocks in C. Here w and z represent two corresponding digits in two consecutive blocks.

Line (8.41) expresses the carry rule (8.36). Line (8.42) ensures that the blocks in C do not cycle back to $0 \ldots 0$, because their last digits cannot decrease from 1 down to 0. Line (8.43) ensures that the last block is $1 \ldots 1$.

By induction, it is easy to see that F_k has k alternating quantifier blocks, starting with $\forall$. It is also clear that F_{k+1} has 5 more variables (x, y, A, C, t) than F_k. Therefore, F_k has at most $5(k+1)$ variables. We can also bound their lengths:

$$\ell(F_0) = O(\lambda) \quad \text{and} \quad \ell(F_{k+1}) = \ell(F_k) + O(1) = O(\lambda + k).$$

Here $\ell(F_0) = O(\lambda)$ instead of $O(1)$ because we needed to iterate the successor function $s_{\mathbb{N}}$ λ times to represent $y = x + \lambda$.

Proof of Theorem 8.20. Consider the following decidable problem: Given a Turing machine $\mathcal{M}$ and an input string X, does $\mathcal{M}$ halt on X within space $g_k(|\mathcal{M}| + |X|)$. By a basic diagonalization argument, this problem requires space at least $g_k(|\mathcal{M}| + |X|)$ to decide. By the same construction as in Theorem 8.34, we can write down a sentence S with length $O(|\mathcal{M}| + |X|)$ so that $S =$ true if and only if $\mathcal{M}$ halts on x within space $g_k(|\mathcal{M}| + |X|)$. Here $\lambda = \Omega(|\mathcal{M}| + |X|)$. The last part $[\forall u, v, u', v' \ldots]$ in (8.34) should be replaced by:

$$\forall x, y, A, C \; F_k(x, y, A, C) \rightarrow \text{ transition rules} \ldots$$

Here x and y are bits in the transcript $\boldsymbol{T} = U(\langle \mathcal{M} X \rangle)$, with $y = x + g_k(\lambda)$.[10] The resulting sentence S has the form $\exists \ldots \forall \ldots \neg F_k \vee \ldots$ Since F_k has k alternating quantifier blocks, S has $k+2$ alternating quantifier blocks. The length $\ell(S)$ is roughly the input length $|\mathcal{M}| + |X|$ plus $\ell(F_k)$, which is also $O(|\mathcal{M}| + |X|)$. □

Proof of Theorem 8.2. We can easily translate the WMSO formula $F_k(x, y, A, C)$ with k alternating quantifier blocks to a $\mathcal{S}_\alpha$ formula S_k with $(k+1)$ alternating quantifier blocks. To do this, we replace each singleton variable in (8.37), say x, by a separate quadruple (u_x, v_x, u'_x, v'_x), where $(u_x, v_x) = (p_{xM}, q_{xM})$ and $(u'_x, v'_x) = (p_{xM+1}, q_{xM+1})$. The Singleton$(x)$ predicate is replaced by $\mathbf{D}^M_\forall(u_x, v_x, u'_x, v'_x)$, and similarly for other singleton variables. Each

[10] U is the universal TM used to emulate $\mathcal{M}(X)$.

set variable, e.g. A, C, is replaced by an integer variable. The relation $\in$ is now $\exists/\forall$-definable in $\mathcal{S}_\alpha$ (see (8.18) and (8.19)). Recall from Fact 8.10 that if $v = q_{tM}$ and $v' = q_{tM+1}$ then $q_{(t+1)M} = cv + dv'$ for some constants $c, d \in \mathbb{Z}$ independent of t. We replace every $x + 1$ term in (8.37) is replaced by $cv_x + dv'_x$. Also $q_{(t+\lambda)M} = c_\lambda v + d_\lambda v'$ for some $c_\lambda, d_\lambda \in \mathbb{Z}$ with $\log(c_\lambda), \log(d_\lambda) = O(\lambda)$. So the relation $y = x + \lambda$ in F_0 is replaced by $v_y = c_\lambda v_x + d_\lambda v'_x$. Observe that S_0 has just $O(1)$ atoms (inequalities), instead of $O(\lambda)$ atoms like F_0. By induction, S_k has $O(k)$ inequalities and variables. The total length $\ell(S_k)$ (including symbols and integer coefficients) is still $O(k + \lambda)$.

Because of the $\mathbf{D}^M_\forall$ predicate, S_0 now has $\forall$ quantifiers. For $k > 0$, we can merge the $\forall$ quantifiers in $\mathbf{D}^M_\forall$ predicates with the $\forall z, w, t, \ldots$ quantifiers in (8.37) (of course replaced by quadruples). Because $\in$ is $\exists/\forall$-definable in $\mathcal{S}_\alpha$, the body of the sentence S_{k+1}, consisting of Boolean combinations in $\in/\notin$, can be written using only $\forall$ quantifiers. These extra $\forall$ quantifiers can again be merged into the $\forall z, w, t$ part. This means S_{k+1} has only one more quantifier block than S_k. So $S_k(u_x, v_x, u'_x, v'_x, u_y, v_y, u'_y, v'_y, A, C)$ has $(k+1)$ alternating quantifier blocks.

Now we are back to encoding Turing machine computations. In (8.34), we replace the last part $[\forall u, v, u', v' \ldots]$ by:

$$\forall u_x, v_x, u'_x, v'_x, u_y, v_y, u'_y, v'_y, A, C \;\; \big(S_k(u_x, v_x, u'_x, v'_x, u_y, v_y, u'_y, v'_y, A, C) = \text{true} \;\wedge\; v_y \leq \tau\big)$$
$$\rightarrow \text{ transition rules} \ldots$$

In these transition rules, $\mathbf{Read}^{B,B',B''}_\exists$ is kept as before with u_x, v_x, u'_x, v'_x, but $\mathbf{Next}^{B,B',B''}_\exists$ can be rewritten using the shifted convergents u_y, v_y, u'_y, v'_y. Altogether, this expresses the transition rule for each jump $y = x + g_k(\lambda)$. The resulting sentence S has the form $\exists \ldots \forall \ldots \neg S_k \vee \ldots$ Since S_k has $k + 1$ alternating quantifier blocks, S has $k + 3$ alternating quantifier blocks. The number of variables and inequalities used is just $O(k)$. $\square$

8.6. Non-quadratic irrationals: Undecidability

8.6.A. Further tools. Now we are working with two different irrationals α and β. Denote by p_n/q_n and $p'_n/q'_n$the n-th convergent of α and β, respectively. Let $\mathrm{Ost}_\alpha \coloneqq \{q_n : n \in \mathbb{N}\}$ and $\mathrm{Ost}_\beta \coloneqq \{q'_n : n \in \mathbb{N}\}$. For $X \in \mathbb{N}$, denote by $\mathrm{Ost}_\alpha(X)$ the set of q_n with non-zero coefficients in the α-Ostrowski representation of X. Then $\mathrm{Ost}_\beta(X)$ is defined accordingly for the β-Ostrowski representation of X. All earlier notations can be easily adapted to α and β separately. For brevity, we define the remaining functions and notations just for α. The corresponding versions for β are defined accordingly, with obvious relabelings.

For $X \in \mathbb{N}$ and $d \in \mathrm{Ost}_\alpha$, if $\sum_{n=0}^{\infty} b_{n+1}q_n$ is the α-Ostrowski representation of X, then we define

$$X\big|_d^\alpha \coloneqq \sum_{n\in\mathbb{N},\, q_n \le d} b_{n+1}q_n. \tag{8.44}$$

Fact 8.21. Let $X \in \mathbb{N}$. Then there is an interval I around $f_\alpha(X)$ and $d \in \mathrm{Ost}_\alpha$ such that for all $Y \in \mathbb{N}$

$$f_\alpha(Y) \in I \Longrightarrow Y\big|_d^\alpha = X.$$

Proof. Let $\sum_{n=0}^{m} b_{n+1}q_n$ be the α-Ostrowski representation of X. Without loss of generality, we may assume that $\alpha q_m - p_m > 0$. Then set

$$Z_2 = X + q_{m+2} \text{ and } Z_1 = X + q_{m+3}.$$

Since $\alpha q_{m+2} - p_{m+2} > 0$ and $\alpha q_{m+3} - p_{m+3} < 0$, we get from Fact 8.9 that

$$f_\alpha(Z_1) < f_\alpha(X) < f_\alpha(Z_2).$$

Now it follows easily from [Hie16, Fact 2.13] and Fact 8.9 that for all $Y \in \mathbb{N}$

$$f_\alpha(Z_1) < f_\alpha(Y) < f_\alpha(Z_2) \Longrightarrow Y\big|_{q_m}^\alpha = X,$$

as desired. □

Fact 8.22. Let $X \in \mathbb{N}$ and let J be an open interval around $f_\alpha(X)$. Then there is $d \in \mathrm{Ost}_\alpha$ such that for all $Y \in \mathbb{N}$

$$Y\big|_d^\alpha = X \Longrightarrow f_\alpha(Y) \in J.$$

Proof. Let $\sum_{n=0}^{m} b_{n+1}q_n$ be the α-Ostrowski representation of X. Let $n \in \mathbb{N}$ be such that

- $n > m+1$,
- $\alpha q_n - p_n > 0$ and
- $\big(f_\alpha(X) + (\alpha q_{n+1} - p_{n+1}), f_\alpha(X) + (\alpha q_n - p_n)\big) \subseteq J$.

Let $Y \in \mathbb{N}$ be such that $Y\big|_{q_{n+2}}^{\alpha} = X$. It is left to show that $f_\alpha(Y) \in J$. By Fact 8.9 and [Hie16, Fact 2.13] we get that

$$f_\alpha(X) + (\alpha q_{n+1} - p_{n+1}) = f_\alpha(X + q_{n+1}) < f_\alpha(Y) < f_\alpha(X + q_n) = f_\alpha(X) + (\alpha q_n - p_n).$$

Thus $f_\alpha(Y) \in J$. □

8.6.B. Uniform definition of all finite subsets of $\mathbb{N}^2$. Let α, β be two positive irrational numbers such that $1, \alpha, \beta$ are $\mathbb{Q}$-linearly independent. The goal of this section is to produce a predicate $\mathbf{Member} \subseteq \mathbb{N}^6$ such that for every set $S \subseteq \mathbb{N}^2$ there is $\boldsymbol{X} \in \mathbb{N}^4$ such that for all $(s,t) \in \mathbb{N}^2$,

$$(s,t) \in S \iff \mathbf{Member}(\boldsymbol{X}, s, t).$$

The $\mathbb{Q}$-linear independence of $1, \alpha, \beta$ is necessary as the existence of such an relation implies the undecidability of the theory. The failure of our argument in the case of $\mathbb{Q}$-linear dependence of $1, \alpha, \beta$ can be traced back to the fact that the following lemma fails when $1, \alpha, \beta$ are $\mathbb{Q}$-linearly dependent.

Here after, we let $\overline{X} = (X_1, X_2), \overline{Y} = (Y_1, Y_2)$ and $\overline{Z} = (Z_1, Z_2)$.

Lemma 8.23. *Let $\overline{X}, \overline{Y} \in \mathbb{N}^2$. Then*

$$|f_\alpha(X_1) - f_\beta(X_2)| = |f_\alpha(Y_1) - f_\beta(Y_2)| \implies \overline{X} = \overline{Y}.$$

Proof. Then there are $U_1, U_2, V_1, V_2 \in \mathbb{N}$ such that

$$\big|\alpha X_1 - U_1 + \beta X_2 - U_2\big| = \big|\alpha Y_1 - V_1 + \beta Y_2 - V_2\big|.$$

By $\mathbb{Q}$-linear independence of $1, \alpha, \beta$, we get that $X_1 = Y_1$ and $X_2 = Y_2$. □

Definition 8.24. Define $g : \mathbb{N}^4 \to \mathbb{R}$ to be the function that maps $(\overline{X}, \overline{Y})$ to

$$\big|f_\alpha(X_2) - f_\alpha(X_1) - |f_\alpha(Y_2) - f_\beta(Y_1)|\big|.$$

Definition 8.25. Define $\mathbf{Best} \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}^2 \times \mathbb{N}$ to be the set containing all $(d, e, \overline{X}, Y_1)$ for which there is a $Y_2 \in \mathbb{N}$ such that

- $Y_1 \leq d$, $Y_2 \leq e$,
- $g(\overline{X}, \overline{Y}) < g(\overline{X}, \overline{Z})$ for all $\overline{Z} \in \mathbb{N}_{\leq d} \times \mathbb{N}_{\leq e}$ with $\overline{Z} \neq \overline{Y}$.

Observe that for given $(d, e, \overline{X}) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^2$ there is at most one $Y_1 \in \mathbb{N}_{\leq d}$ such that $\mathbf{Best}(d, e, \overline{X}, Y_1)$ holds. We will later see in Lemma 8.27 that for given $d \in \mathbb{N}$ we can take $e \in \mathbb{N}$ large enough such that for all $X_1 \in \mathbb{N}$ and $Y_1 \leq d$ the set

$$\{X_2 \in \mathbb{N} \ : \ \mathbf{Best}(d, e, X_1, X_2, Y)\}$$

is cofinal in $\mathbb{N}$.

Lemma 8.26. Best *is* $\exists\forall$*-definable.*

Proof. Observe that $\mathbf{Best}(d, e, \overline{X}, Y_1)$ holds if and only if

$$\begin{aligned}
&\exists Y_2, U_1, U_2, V_1, V_2 \quad \forall Z_1, Z_2, W_1, W_2 \quad Y_1 \leq d \ \wedge \ Y_2 \leq e \ \wedge \\
&\quad f_\alpha(X_1) = \alpha X_1 - U_1 \ \wedge \ f_\alpha(X_2) = \alpha X_2 - U_2 \ \wedge \ f_\alpha(Y_1) = \alpha Y_1 - V_1 \ \wedge \ f_\beta(Y_2) = \beta Y_2 - V_2 \ \wedge \\
&\quad \Big[\big(Z_1 \leq d \ \wedge \ Z_2 \leq e \ \wedge \ f_\alpha(Z_1) = \alpha Z_1 - W_1 \ \wedge \ f_\beta(Z_2) = \beta Z_2 - W_2 \\
&\quad \wedge \ (Z_1, Z_2) \neq (Y_1, Y_2)\big) \to \big|(\alpha X_2 - U_2) - (\alpha X_1 - U_1) - |(\beta Y_2 - V_2) - (\alpha Y_1 - V_1)|\big| \\
&\qquad\qquad < \big|(\alpha X_2 - U_2) - (\alpha X_1 - U_1) - |(\beta Z_2 - W_2) - (\alpha Z_1 - W_1)|\big|\Big].
\end{aligned}$$

This implies the result. □

The following lemma is crucial in what follows. It essentially says that for every subinterval of $I_\alpha \cap I_\beta$ and every $d \in \mathrm{Ost}_\alpha$, we can recover $(\mathrm{Ost}_\alpha)_{\leq d}$ just using parameters from this interval and Ost_β. This should be compared to condition (ii) in [HTy14, Th. A].

Lemma 8.27. *Let* $d \in \mathrm{Ost}_\alpha$*,* $e_0 \in \mathrm{Ost}_\beta$*,* $\overline{X} \in \mathbb{N}^2$ *and* $s \in \mathbb{N}$ *be such that*

1. $f_\alpha(X_1), f_\alpha(X_2) \in I_\beta$,

2. $f_\alpha(X_1) < f_\alpha(X_2)$,

3. $s \leq d$.

Then there is $e \in \mathrm{Ost}_\beta$ *and an open interval* $J \subseteq \big(f_\alpha(X_1), f_\alpha(X_2)\big)$ *such that* $e \geq e_0$ *and for all* $Z \in \mathbb{N}$

$$f_\alpha(Z) \in J \Longrightarrow \mathbf{Best}(d, e, X_1, Z, s).$$

Proof. Let $e \in \mathrm{Ost}_\beta$ be large enough such that for every $w_1 \in \mathbb{N}_{\leq d}$ there is $w_2 \in \mathbb{N}_{\leq e}$ such that

$$f_\alpha(w_1) \in I_\beta \Longrightarrow |f_\alpha(w_1) - f_\beta(w_2)| < f_\alpha(X_2) - f_\alpha(X_1).$$

The existence of such an e follows from the finiteness of $\mathbb{N}_{\leq d}$ and the density of $f_\beta(\mathbb{N})$ in I_β. Let $w \in \mathbb{N}_{\leq e}$ be such that

$$|f_\alpha(s) - f_\beta(w)| < f_\alpha(X_2) - f_\alpha(X_1).$$

By Lemma 8.23 we can find an $\varepsilon > 0$ such that for all $(w_1, w_2) \in \mathbb{N}_{\leq d} \times \mathbb{N}_{\leq e}$ with $(w_1, w_2) \neq (s, w)$

$$\big||f_\alpha(w_1) - f_\beta(w_2)| - |f_\alpha(s) - f_\beta(w)|\big| > \varepsilon.$$

Set

$$\delta \coloneqq f_\alpha(X_1) + |f_\alpha(s) - f_\beta(w)|.$$

Set $J \coloneqq (\delta - \frac{\varepsilon}{2}, \delta + \frac{\varepsilon}{2})$. Let $Z \in \mathbb{N}$ be such that $f_\alpha(Z) \in J$. It is left to show that $\mathbf{Best}(d, e, X_1, Z, s)$ holds. We have that for all $(w_1, w_2) \in \mathbb{N}_{\leq d} \times \mathbb{N}_{\leq e}$ with $(w_1, w_2) \neq (s, w)$

$$\begin{aligned} g(X_1, Z, w_1, w_2) &= \big|f_\alpha(Z) - f_\alpha(X_1) - |f_\alpha(w_1) - f_\beta(w_2)|\big| \\ &= \big|f_\alpha(Z) - \delta + |f_\alpha(s) - f_\beta(w)| - |f_\alpha(w_1) - f_\beta(w_2)|\big| \\ &\geq \Big||f_\alpha(Z) - \delta| - \big||f_\alpha(s) - f_\beta(w)| - |f_\alpha(w_1) - f_\beta(w_2)|\big|\Big| > \frac{\varepsilon}{2}. \end{aligned}$$

Moreover,

$$g(X_1, Z, s, w) = \big|f_\alpha(Z) - f_\alpha(X_1) - |f_\alpha(s) - f_\beta(w)|\big| \leq \big|f_\alpha(Z) - \delta\big| \leq \frac{\varepsilon}{2}.$$

Thus $\mathbf{Best}(d, e, X_1, Z, s)$ holds, as desired. □

Lemma 8.28. *Let $d \in \mathrm{Ost}_\alpha, s \in \mathbb{N}, \overline{X} \in \mathbb{N}^2$ be such that*

1. $f_\alpha(X_1), f_\alpha(X_2) \in I_\beta$,
2. $f_\alpha(X_1) < f_\alpha(X_2)$,
3. $s \leq d$.

Then there are $e_1 \in \mathrm{Ost}_\beta, e_2 \in \mathrm{Ost}_\alpha, Y \in \mathbb{N}$ such that

(i) $f_\alpha(X_1) < f_\alpha(Y) < f_\alpha(X_2)$,

(ii) $d < e_1 < e_2$

(iii) for all $Z \in \mathbb{N}$

$$Z\big|_{e_2}^{\alpha} = Y \Longrightarrow \mathbf{Best}(d, e_1, X_1, Z, s).$$

Proof. By Lemma 8.27 there is an open interval $J \subseteq \big(f_\alpha(X_1), f_\alpha(X_2)\big)$ and $e_1 \in \mathrm{Ost}_\beta$ such that $e_1 > d$ and for all $Z \in \mathbb{N}$

$$f_\alpha(Z) \in J \Longrightarrow \mathbf{Best}(d, e_1, X_1, Z, s).$$

Take $Y \in \mathbb{N}$ such that $f_\alpha(Y) \in J$. By Fact 8.22 we can find $e_2 \in \mathrm{Ost}_\alpha$ arbitrarily large such that $f_\alpha(Z) \in J$ for all $Z \in \mathbb{N}$ with $Z\big|_{e_2}^{\alpha} = Y$. The statement of the Lemma follows. □

Definition 8.29. Define **Admissible** $\subseteq \mathrm{Ost}_\alpha^4 \times \mathrm{Ost}_\beta^2 \times \mathbb{N}^6$ to be the set of all tuples

$$(d_1, d_2, d_3, d_4, e_1, e_2, X_1, X_2, X_3, X_4, s, t) \in \mathrm{Ost}_\alpha^4 \times \mathrm{Ost}_\beta^2 \times \mathbb{N}^6$$

such that

- d_1, d_2, d_3 are consecutive elements of $\mathrm{Ost}_\alpha(X_1)$,
- $d_4 \in \mathrm{Ost}_\alpha(X_3)$ and $d_1 \leq d_4 < d_2$,
- $e_1, e_2 \in \mathrm{Ost}_\beta(X_2)$ and $d_1 \leq e_1 < d_2 \leq e_2 < d_3$
- $\mathbf{Best}(d_1, e_1, X_4\big|_{d_1}^{\alpha}, X_4, s)$

- $\mathbf{Best}(d_2, e_2, X_4\big|_{d_2}^{\alpha}, X_4, t)$

Define $\mathbf{Member} \subseteq \mathbb{N}^6$ to be the set of all tuples $(X_1, X_2, X_3, X_4, s, t) \in \mathbb{N}^6$ such that there exist $d_1, d_2, d_3, d_4 \in \mathrm{Ost}_\alpha$, $e_1, e_2 \in \mathrm{Ost}_\beta$ with

$$\mathbf{Admissible}(d_1, d_2, d_3, d_4, e_1, e_2, X_1, X_2, X_3, X_4, s, t).$$

Theorem 8.30. *Let $S \subseteq \mathbb{N}^2$ be finite. Then there are $X_1, X_2, X_3, X_4 \in \mathbb{N}$ such that for all $s, t \in \mathbb{N}$*

$$(s, t) \in S \Leftrightarrow \mathbf{Member}(X_1, X_2, X_3, X_4, s, t).$$

Proof. Let $S \subseteq \mathbb{N}^2$ be finite. Let $c_1, \ldots, c_{2n} \in \mathbb{N}$ be such that

$$S = \{(c_1, c_2), \ldots, (c_{2n-1}, c_{2n})\}.$$

Recall that the convergents of α and β are $\{p_n/q_n\}$ and $\{p'_n/q'_n\}$, respectively. We will construct two strictly increasing sequences $(k_i)_{i=0,\ldots,2n}, (l_i)_{i=1,\ldots,2n}$ of non-consecutive natural numbers and another sequence $(W_i)_{i=0,\ldots,2n}$ of natural numbers such that for all $i = 0, \ldots, 2n$

(1) $W_j = W_i\big|_{q_{k_j}}^{\alpha}$ for all $j \leq i$, and $f_\alpha(W_i) \in I_\beta$,

(2) $q_{k_i} > \max\{c_1, \ldots, c_{2n}\}$,

and furthermore if $i \geq 1$, then

(3) $q_{k_{i-1}} < q'_{l_i} < q_{k_i}$,

(4) for all $Z \in \mathbb{N}$

$$Z\big|_{q_{k_i}}^{\alpha} = W_i \Longrightarrow \mathbf{Best}(q_{k_{i-1}}, q'_{l_i}, W_{i-1}, Z, c_i).$$

We construct these sequences recursively. For $i = 0$, pick $k_0 \in \mathbb{N}$ such that

$$q_{k_0} > \max\{c_1, \ldots, c_{2n}\}.$$

Pick $W_0 \in \mathbb{N}$ such that $W_0 = W_0\big|_{q_{k_0}}^{\alpha}$ and $f_\alpha(W_0) \in I_\beta$. Now suppose that $i > 0$ and that we already constructed $k_0, k_1, \ldots, k_{i-1}$, $l_1, \ldots, l_{i-1}$ and $W_1, \ldots, W_{i-1}$ such that the above

conditions (1)-(4) hold for $j = 1, \ldots, i-1$. We now have to find k_i, l_i and W_i that (1)-(4) also hold for i. We do so by applying Lemma 8.28. By Fact 8.21 we can take $T \in \mathbb{N}$ such that

(a) $f_\alpha(T) > f_\alpha(W_{i-1})$, $T\big|^\alpha_{q_{k_{i-1}}} = W_{i-1}$, $f_\alpha(T) \in I_\beta$ and

(b) for all $Z \in \mathbb{N}$, $\big(f_\alpha(W_{i-1}) < f_\alpha(Z) < f_\alpha(T) \Longrightarrow Z\big|^\alpha_{q_{k_{i-1}}} = W_{i-1}\big)$.

We now apply Lemma 8.28 with $X_1 \coloneqq W_{i-1}, X_2 \coloneqq T, d \coloneqq q_{k_{i-1}}$ and $s \coloneqq c_{i-1}$. We obtain $e_1 \in \mathrm{Ost}_\beta$, $e_2 \in \mathrm{Ost}_\alpha$ and $Y \in \mathbb{N}$ such that $d < e_1 < e_2$, $f_\alpha(W_{i-1}) < f_\alpha(Y) < f_\alpha(T)$ and for all $Z \in \mathbb{N}$

$$Z\big|^\alpha_{e_2} = Y \Longrightarrow \mathbf{Best}(q_{k_{i-1}}, e_1, W_{i-1}, Z, c_{i-1}).$$

If necessary, we increase e_2 such that $Y\big|^\alpha_{e_2} = Y$. Choose k_i such that $q_{k_i} = e_2$, choose l_i such that $q'_{l_i} = e_1$. Set $W_i \coloneqq Y$. It is immediate that (2)-(4) hold for $i = 1, \ldots, n$. For (1), observe that since $f_\alpha(W_{i-1}) < f_\alpha(Y) < f_\alpha(T)$, we deduce from (b) that

$$W_i\big|^\alpha_{q_{k_{i-1}}} = Y\big|^\alpha_{q_{k_{i-1}}} = W_{i-1}.$$

Since (1) holds for $j = 1, \ldots, i-1$, we get that for $j < i-1$

$$W_i\big|^\alpha_{q_{k_j}} = W_i\big|^\alpha_{q_{k_j}} = W_j.$$

Thus (1) holds for i.

We have constructed $(k_i)_{i=0,\ldots,2n}, (l_i)_{i=1,\ldots,2n}$ and $(W_i)_{i=0,\ldots,2n}$ satisfying (1)-(4) for each $i = 0, 1, \ldots, 2n$. We now define $(Z_1, Z_2, Z_3, Z_4) \in \mathbb{N}^4$ by

$$Z_1 \coloneqq \sum_{i=0}^{2n} q_{k_i}, \quad Z_2 \coloneqq \sum_{i=1}^{2n} q'_{l_i}$$
$$Z_3 \coloneqq \sum_{i=0}^{n} q_{k_{2i}}, \quad Z_4 \coloneqq W_{2n}.$$

Observe that we require the sequences $(k_i)_{i=0,\ldots,2n}$ and $(l_i)_{i=1,\ldots,2n}$ to be increasing sequences of non-consecutive natural numbers. Therefore the above description of Z_1, Z_2 and Z_3 im-

mediately gives us the α-Ostrowski representations of Z_1 and Z_3 and the β-Ostrowski representation of Z_2. In particular,

$$\begin{gathered}\mathrm{Ost}_\alpha(Z_1) = \{q_{k_i} \ : \ i = 0, \ldots, n\}, \qquad \mathrm{Ost}_\beta(Z_2) = \{q'_{l_i} \ : \ i = 1, \ldots, n\}, \\ \mathrm{Ost}_\alpha(Z_3) = \{q_{k_i} \ : \ i = 0, \ldots, n, \ i \text{ even}\}.\end{gathered} \tag{8.45}$$

It is now left to prove that for all $s, t \in \mathbb{N}$

$$(s,t) \in S \iff \mathbf{Member}(Z_1, Z_2, Z_3, Z_4, s, t).$$

"$\Rightarrow$": Let $(s,t) \in S$. Let $i \in \{1, \ldots, 2n\}$ be such that $(s,t) = (c_i, c_{i+1})$. Observe that i is odd. We show that

$$\mathbf{Admissible}(q_{k_{i-1}}, q_{k_i}, q_{k_{i+1}}, q_{k_{i-1}}, q_{l_i}, q_{l_{i+1}}, Z_1, Z_2, Z_3, Z_4, c_i, c_{i+1}) \tag{8.46}$$

holds. By (8.45) and the fact that $i-1$ is even, we have that

$$q_{k_{i-1}}, q_{k_i}, q_{k_{i+1}} \in \mathrm{Ost}_\alpha(Z_1), \ q'_{l_i}, q'_{l_{i+1}} \in \mathrm{Ost}_\beta(Z_2), \ q_{k_{i-1}} \in \mathrm{Ost}_\alpha(Z_3).$$

Trivially, $q_{k_{i-1}} \leq q_{k_{i-1}} < q_{k_i}$. By (3) $q_{k_{i-1}} < q'_{l_i} < q_{k_i} < q'_{l_{i+1}} < q_{k_{i+1}}$. Now observe that by (1)

$$\begin{aligned} Z_4\big|^\alpha_{q_{k_{i-1}}} &= W_{2n}\big|^\alpha_{q_{k_{i-1}}} = W_{i-1}, \\ Z_4\big|^\alpha_{q_{k_i}} &= W_{2n}\big|^\alpha_{q_{k_i}} = W_i, \\ Z_4\big|^\alpha_{q_{k_{i+1}}} &= W_{2n}\big|^\alpha_{q_{k_{i+1}}} = W_{i+1}. \end{aligned}$$

Thus by (4)

$$\mathbf{Best}(q_{k_{i-1}}, q'_{l_i}, Z_4\big|^\alpha_{q_{k_{i-1}}}, Z_4, c_i) \ \wedge \ \mathbf{Best}(q_{k_i}, q'_{l_{i+1}}, Z_4\big|^\alpha_{q_{k_i}}, Z_4, c_{i+1}).$$

Thus (8.46) holds.

"$\Leftarrow$": Suppose that $\mathbf{Member}(Z_1, Z_2, Z_3, Z_4, s, t)$ holds. Let $d_1, d_2, d_3, d_4 \in \mathrm{Ost}_\alpha, e_1, e_2 \in \mathrm{Ost}_\beta$ be such that

$$\mathbf{Admissible}(d_1, d_2, d_3, d_4, e_1, e_2, Z_1, Z_2, Z_3, Z_4, s, t) \tag{8.47}$$

holds. Then d_1, d_2, d_3 are consecutive elements of $\mathrm{Ost}_\alpha(Z_1)$. Thus there is $i \in \{1, \ldots, 2n-1\}$ such that

$$d_1 \coloneqq q_{k_{i-1}},\ d_2 \coloneqq q_{k_i},\ d_3 \coloneqq q_{k_{i+1}}.$$

Since $d_4 \in \mathrm{Ost}_\alpha(Z_3)$ and $d_1 \leq d_4 < d_2$, it follows that $d_4 = d_1 = q_{k_{i-1}}$ and that i is odd. Since $e_1, e_2 \in \mathrm{Ost}_\beta(Z_2)$ and

$$d_1 = q_{k_{i-1}} \leq e_1 < d_2 = q_{k_i} \leq e_2 \leq d_3 = q_{k_{i+1}},$$

we get from (3) that $e_1 = q'_{l_i}$ and $e_2 = q'_{l_{i+1}}$. Thus by (8.47)

$$\mathbf{Best}(q_{k_{i-1}}, q'_{l_i}, Z_4\big|^\alpha_{q_{k_{i-1}}}, Z_4, s)\ \wedge\ \mathbf{Best}(q_{k_i}, q'_{l_{i+1}}, Z_4\big|^\alpha_{q_{k_i}}, Z_4, t).$$

By (4) we get that $s = c_i$ and $t = c_{i+1}$. Since i is odd, $(s,t) = (c_i, c_{i+1}) \in S$. □

8.6.C. $\exists\forall$-Definability of Admissible and Member. For **Admissible** (Definition 8.29), we replace each variable d_i, which earlier represented some convergent $q_n \in \mathrm{Ost}_\alpha$, by a 6-tuple $\overline{d}_i = (u_i^-, v_i^-, u_i, v_i, u_i^+, v_i^+)$ such that:

$$(u_i^-, v_i^-, u_i, v_i, u_i^+, v_i^+) = (p_{n-1}, q_{n-1}, p_n, q_n, p_{n+1}, q_{n+1})\ \text{ for some } n. \tag{8.48}$$

We require $\mathbf{C}_{\forall,\alpha}(u_i^-, v_i^-, u_i, v_i, u_i^+, v_i^+) = \text{true}$ to guarantee (8.48). Here v_i takes the earlier role of d_i. Similarly, we replace each e_i in **Admissible** by a 6-tuple $\overline{e}_i$ and also require that $\mathbf{C}_{\forall,\beta}(\overline{e}_i) = \text{true}$. Here $\mathbf{C}_{\forall,\alpha}$ and $\mathbf{C}_{\forall,\beta}$ are from (8.15), with the extra subscript α or β indicating which irrational is being considered. These $\mathbf{C}_{\forall,\alpha}$ and $\mathbf{C}_{\forall,\beta}$ conditions can be combined into a $\forall^2$-part. Altogether, the new **Admissible** has 42 variables.

Recall that **Best** is $\exists^5\forall^4$-definable (Lemma 8.26). The relation $Y = X\big|^\alpha_{\overline{d}}$ from (8.44) is $\exists^2$-definable:

$$Y = X\big|^\alpha_{\overline{d}}\ \coloneqq\ Y < v^+\ \wedge\ \exists Z, Z'\ \mathbf{Compatible}(u, v, u^+, v^+, Y, Z, Z')\ \wedge\ Y + Z = X.$$

Here **Compatible** is from (8.20).

The relation $\overline{d} \in \mathrm{Ost}_\alpha(X)$, meaning v appears in $\mathrm{Ost}_\alpha(X)$, is $\exists^3$-definable (see (8.18)). The same holds for $\overline{e} \in \mathrm{Ost}_\beta(X)$ (just replace α by β).

The relation

$$\mathbf{Consec}_{\exists}(\overline{d}_1, \overline{d}_2, X) \;\coloneqq\; v_1 < v_2 \;\wedge\; \overline{d}_1 \in \mathrm{Ost}_\alpha(X) \;\wedge\; \overline{d}_2 \in \mathrm{Ost}_\alpha(X) \wedge$$
$$\exists Y_1, Y_2 \;\; Y_1 = X\big|^{\alpha}_{\overline{d}_1} \;\wedge\; Y_2 = X\big|^{\alpha}_{\overline{d}_2} \;\wedge\; \mathbf{After}(u_2^-, v_2^-, u_i, v_i, Y_2 - Y_1)$$

means $v_1 < v_2$ appear consecutively in $\mathrm{Ost}_\alpha(X)$. This is $\exists^{12}$-definable.

It is now easy to see that **Admissible** $\exists\forall$-definable, and so is **Member**. A direct count reveals that **Admissible** is at most $\exists^{50}\forall^{10}$, and **Member** is at most $\exists^{100}\forall^{10}$.

8.6.D. Undecidability.

Theorem 8.31. *The $\exists\forall\exists\forall$-fragment is undecidable.*

Proof. Here we follow an argument given in the proof of Thomas [Tho12, Th. 16.5]. Consider $U = (\mathbf{Q}, \mathbf{\Sigma}, \sigma_1, \delta, q_1, q_2)$ a universal 1-tape Turing machine with 8 states and 4 symbols, as given in [NW06]. Here $\mathbf{Q} = \{q_1, \ldots, q_8\}$ are the states, $\mathbf{\Sigma} = \{\sigma_1, \ldots, \sigma_4\}$ are the tape symbols, σ_1 is the blank symbol, q_1 is the start state and q_2 is the unique halt state. Also, $\delta : [8] \times [4] \to [8] \times [4] \times \{\pm 1\}$ is the transition function. In other words, we have $\delta(i, j) = (i', j', d)$ if upon state q_i and symbol σ_j, the machine changes to state $q_{i'}$, writes symbol $\sigma_{j'}$ and moves left ($d = -1$) or right ($d = 1$). Given an input $x \in \mathbf{\Sigma}^*$, we will now produce an $\exists\forall\exists\forall$-sentence φ_x such that φ_x holds if and only if $U(x)$ halts.

We will now use sets $A_1, \ldots, A_8 \subseteq \mathbb{N}^2$ and $B_1, \ldots B_4 \subseteq \mathbb{N}^2$ to code the computation on $U(x)$. The A_i's code the current state of the Turing machine. That is, for $(s, t) \in \mathbb{N}^2$, we have $(s, t) \in A_i$ if and only if at step s-th of the computation, U is in state q_i and its head over the t-th cell of the tape. The B_j's code which symbols are written on the tape at a given step of the computation. We have $(s, t) \in B_j$ if and only if at step s-th of the computation, the symbol σ_j is written on t-th cell of the tape. The computation $U(x)$ then halts if and only if there are $A_1, \ldots, A_8 \subseteq \mathbb{N}^2$ and $B_1, \ldots B_4 \subseteq \mathbb{N}^2$ such that:

a) A_i's are pairwise disjoint; B_j's are pairwise disjoint.

b) $(0, 0) \in A_1$, i.e., the computation starts in the initial state.

c) There exists some $(u, v) \in A_2$, i.e., the computation eventually halts.

d) For each $s \in \mathbb{N}$, there is at most one $t \in \mathbb{N}$ such that $(s, t) \in \cup_i A_i$, i.e., at each step of the computation, U can only be in exactly one state.

e) If $x = x_0 \dots x_n \in \mathbf{\Sigma}^*$, then for every $0 \leq t \leq n$, we have $x_t = \sigma_j \iff (0, t) \in B_j$, i.e., the first rows of the B_j's code the input string x.

f) Whenever $(s, t) \in B_j$,

   f1) if $(s, t) \notin A_i$ for all $i \in [8]$, then $(s + 1, t) \in B_j$. That is, if the current head position is not at t, then the t-th symbol does not change.

   f2) if $(s, t) \in A_i$ for some $i \in [8]$ and $\delta(i, j) = (\delta^1_{ij}, \delta^2_{ij}, \delta^3_{ij}) \in [8] \times [4] \times \{\pm 1\}$, then $(s + 1, t) \in B_{\delta^2_{ij}}$ and $(s + 1, t + \delta^3_{ij}) \in A_{\delta^1_{ij}}$. That is, if the head position is at t, and the state is i, then a transition rule is applied.

We use the predicate **Member** to code membership $(s, t) \in A_i, B_j$. By Theorem 8.30, there should exist tuples $\boldsymbol{X}_i = (X_{i1}, \dots, X_{i4})$, $\boldsymbol{Y}_j = (Y_{j1}, \dots, Y_{j4}) \in \mathbb{N}^4$ that represent A_i and B_j. In other words, we have

$$(s, t) \in A_i \iff \mathbf{Member}(\boldsymbol{X}_i, s, t)\ , \quad (s, t) \in B_j \iff \mathbf{Member}(\boldsymbol{Y}_j, s, t).$$

For the input condition e), there exist $\boldsymbol{Z}_j = (Z_{j1}, \dots, Z_{j4}) \in \mathbb{N}^4$ so that

$$x_t = \sigma_j \iff \mathbf{Member}(\boldsymbol{Z}_j, 0, t) \quad \forall\ 0 \leq t \leq n.$$

Note that $\boldsymbol{Z}_j$ can be explicitly constructed from the input x (see Theorem 8.30's proof). Now the sentence ϕ_x that encodes halting of $U(x)$ is:

$$
\begin{aligned}
\varphi_x \;\coloneqq\; & \exists \boldsymbol{X}_1, \dots, \boldsymbol{X}_8,\, \boldsymbol{Y}_1, \dots, \boldsymbol{Y}_4 \in \mathbb{N}^4,\, u, v \in \mathbb{N} \quad \forall s, t, t' \in \mathbb{N} \\
& \bigwedge_{i \neq i'} \neg\big(\mathbf{Member}(\boldsymbol{X}_i, s, t) \;\wedge\; \mathbf{Member}(\boldsymbol{X}_{i'}, s, t)\big) \\
& \wedge \bigwedge_{j \neq j'} \neg\big(\mathbf{Member}(\boldsymbol{Y}_j, s, t) \;\wedge\; \mathbf{Member}(\boldsymbol{Y}_{j'}, s, t)\big) \\
& \wedge \mathbf{Member}(\boldsymbol{X}_1, 0, 0) \;\;\wedge\;\; \mathbf{Member}(\boldsymbol{X}_2, u, v) \\
& \wedge \Big[\big(\bigvee_i \mathbf{Member}(\boldsymbol{X}_i, s, t)\big) \;\wedge\; \big(\bigvee_i \mathbf{Member}(\boldsymbol{X}_i, s, t')\big) \;\to\; t = t'\Big] \\
& \wedge \bigwedge_j \big(\mathbf{Member}(\boldsymbol{Z}_j, 0, t) \to \mathbf{Member}(\boldsymbol{Y}_j, 0, t)\big) \\
& \wedge \bigwedge_j \Big(\mathbf{Member}(\boldsymbol{Y}_j, s, t) \to \big[\, \bigwedge_i \neg\mathbf{Member}(\boldsymbol{X}_i, s, t) \;\wedge\; \mathbf{Member}(\boldsymbol{Y}_j, s+1, t) \,\big] \\
\vee & \bigvee_i \big[\, \mathbf{Member}(\boldsymbol{X}_i, s, t) \;\wedge\; \mathbf{Member}(\boldsymbol{Y}_{\delta^2_{ij}}, s+1, t) \;\wedge\; \mathbf{Member}(\boldsymbol{X}_{\delta^1_{ij}}, s+1, t+\delta^3_{ij}) \,\big] \,\Big).
\end{aligned}
$$

Since **Member** is $\exists\forall$-definable, the sentence ϕ_x is $\exists\forall\exists\forall$. Whether $U(x)$ halts or not is undecidable, so is ϕ_x. A direct count shows that **Member** appears at most 200 times in ϕ_x. From the last estimate in §8.6.C, we see that ϕ_x is at most a $\exists^k\forall^k\exists^k\forall^k$ sentence, where $k = 20000$. This completes the proof. □

8.7. Final remarks and open problems

8.7.A. Comparing theorems 8.34 and 8.3, we see a big complexity jump by going from one to three alternating quantifier blocks, even the field is quadratic. The interesting open questions are the complexity of deciding (8.1) when $k = 2, 3$ with α non-quadratic. We make the following conjecture:

Conjecture 8.32. *For α non-quadratic and $k = 3$, integer sentences* (8.1) *are undecidable.*

Similarly, when α is quadratic we make the following conjecture:

Conjecture 8.33. *For α quadratic and $k = 2$, deciding integer sentences* (8.1) *with and a fixed number of variables and inequalities is* NP*-hard.*

We note that for $\alpha = \sqrt{5}$, $\exists\forall$-sentences in $\mathcal{S}_\alpha$ can already express non-trivial questions, such as the following: *Given $a, b \in \mathbb{Z}$, decide whether there is a Fibonacci number F_n congruent to a modulo b?* Note that the sequence $\{F_n \bmod b\}$ is periodic with period $O(b)$, called the *Pisano period*. These periods were introduced by Lagrange and heavily studied in number theory (see e.g. [Sil11, §29]), but the question above is likely computationally hard.

8.7.B. Khachiyan and Porkolab proved in [KP00] the following positive result on Integer Programming with irrational polyhedra:

Theorem 8.34 ([KP00])**.** *Let $\mathbb{K} = \overline{\mathbb{Q}}$ be the field of algebraic numbers. For every fixed n, sentences of the form $\exists \mathbf{y} \in \mathbb{Z}^n : A\mathbf{y} \leq \overline{b}$ with $A \in \mathbb{K}^{m\times n}, \overline{b} \in \mathbb{K}^m$ can be decided in polynomial time. Here the system $A\mathbf{y} \leq \overline{b}$ in the theorem can involve arbitrary algebraic irrationals.*

Note that the system $A\mathbf{y} \leq \overline{b}$ in the theorem can involve arbitrary algebraic irrationals. This is a rare positive result on irrational polyhedra. In fact, for a non-quadratic α, this gives the only positive result on $\mathcal{S}_\alpha$ that we know of (cf. §8.7.B). This result very much contrasts Theorem 8.6. The reason for polynomial decidability here is that it only considers $\exists$-sentences. More generally, Khachiyan and Porkolab showed that Integer Programming is polynomial time for convex semialgebraic sets in fixed dimension:

Theorem 8.35 ([KP00])**.** *Let $k, m, n_1, \ldots, n_m$ be fixed. Consider a first order formula $F(\mathbf{y})$ over the reals of the form:*

$$\mathbf{y} \in \mathbb{R}^k : Q_1 \mathbf{x}_1 \in \mathbb{R}^{n_1} \ \ldots \ Q_m \mathbf{x}_m \in \mathbb{R}^{n_m} \ P(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_m),$$

where $P(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_w)$ is a Boolean combination of equalities/inequalities of the form

$$g_i(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_w) \ *_i \ 0$$

with $*_i \in \{>, <, =\}$ and $g_i \in \mathbb{Z}[\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_w]$. Suppose that $S_F := \{\mathbf{y} \in \mathbb{R}^n : F(\mathbf{y}) = \text{true}\}$ is a convex set. Then we can either decide in polynomial time that $S_F \cap \mathbb{Z}^k = \varnothing$, or produce in polynomial time some $\mathbf{y} \in S_F \cap \mathbb{Z}^k$.

This immediately implies Theorem 8.34. Here there is no restriction on the number of g_i's and their degrees. The coefficients of g_i's are encoded in binary.

Note that convexity is crucially important in the theorem. In [MA78], it is shown that given $a, b, c \in \mathbb{Z}$, deciding $\exists \mathbf{y} \in \mathbb{N}^2 \ : \ ay_1^2 + by_2 + c = 0$ is NP-complete. Here the semialgebraic set

$$\left\{ \mathbf{y} \in \mathbb{R}^2 \ : \ 0 \leq ay_1^2 + by_2 + c < 1 \right\}$$

is not necessarily convex.

CHAPTER 9

Integer points in translated and expanded polyhedra

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 also consider the *Ehrhart quasi-polynomial* of a rational polytope, which counts the number of integer points in its expansions, and show that it can have arbitrarily bad fluctuations. This chapter is a version of the preprint [NP18].

9.1. Introduction

9.1.A. Translation of polytopes. We first state a more general problem, which was considered by Eisenbrand and Hähnle in [EH12].

Integer Point Minimization (IPM)

Input: $A \in \mathbb{Q}^{m\times n}$, a rational polyhedron $W \subseteq \mathbb{R}^m$, $k \in \mathbb{N}$.

Decide: $\exists \overline{b} \in W$ s.t. $\#\{\mathbf{x} \in \mathbb{Z}^n : A\mathbf{x} \leq \overline{b}\} \leq k$?

Here, the polytope $P_{\overline{b}} := \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \overline{b}\}$ is called a *parametric polytope* with $\overline{b}$ being the parameters varying over W. The problem asks whether we can find such a $\overline{b} \in W$ so that $|P_{\overline{b}}|$, its number of integer points, is at most k. Such polytopes were introduced by Kannan [Kan90], who gave a polynomial time algorithm for IPM with $k = 0$ and n bounded (Theorem 3.18). 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 Chapter 7). The following problem is an especially

attractive special case:

Polytope Translation

Input: $A \in \mathbb{Q}^{m\times n}$, $\overline{b} \in \mathbb{Q}^m$, $\vec{v} \in \mathbb{Q}^n$, and $k \in \mathbb{N}$.

Decide: $\exists \lambda,\ 0 \le \lambda \le 1$ s.t. $\#\{\mathbf{x} \in \mathbb{Z}^n : A(\mathbf{x} - \lambda\vec{v}) \le \overline{b}\} \le k$?

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

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

Theorem 9.1 ([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 9.2. *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 9.3. *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 9.3 is implied by Theorem 9.2 by a simple argument on rationality, its proof is simpler and will be presented first (cf. Section 9.3). The technique differs from that in [EH12].

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

To prove Theorem 9.3, 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. Let us mention that positivity and convexity are major obstacles here, and occupy much of the proof.

9.1.B. 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. For a rational polytope $P \subset \mathbb{R}^n$, consider the following function:

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

Ehrhart famously proved that $f_P(t)$ is a quasi-polynomial, called the *Ehrhart quasi-polynomial*, see e.g. [Bar08, §18]. It is well known and easy to see that $f_P(t) \sim \mathrm{vol}_n(P)t^n$.

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: $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}$, $\gcd(\alpha_1, \ldots, \alpha_n) = 1$.

Output: $g(\overline{a}) \coloneqq \max\big\{t \in \mathbb{N} \,:\, \nexists\, c_1, \ldots, c_n \in \mathbb{N} \;\text{ s.t. }\; t = c_1\alpha_1 + \ldots + c_n\alpha_n\big\}$.

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

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

Then $f_{\overline{\alpha}}(t)$ counts the number of ways to write $t \ge 0$ 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: $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}$, $\gcd(\alpha_1, \ldots, \alpha_n) = 1$, $k \in \mathbb{N}$.

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 (see Theorem 6.21). 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 $P \in \mathbb{R}^n$ 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 9.4. *The* k-ETP *is* NP*-hard for rational polytopes* $P \in \mathbb{R}^6$ *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 §9.6.A).

9.1.C. 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:

$$p(t) \ = \ \sum_{i=1}^{r} \gamma_i \prod_{j=1}^{n} \big\lfloor \alpha_{ij} t + \beta_{ij} \big\rfloor, \tag{9.1}$$

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 (9.1) efficiently when n is

fixed (see e.g. [VW08]).

Not all quasi-polynomials arise from polytopes. 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 terms 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 9.5. *Let $N \in \mathbb{N}$ and $p : \mathbb{Z} \to \mathbb{Z}$ be a quasi-polynomial of the form (9.1), 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 $Q \in \mathbb{R}^d$ 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 9.6. *For every sequence $c_0, \ldots, c_{r-1} \in \mathbb{N}$, there exists a polytope $Q \in \mathbb{R}^d$ 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 9.5 to $f(t)$ with $N = r$. □

9.1.D. Brief historical overview. 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 9.5. 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, Woo05]. It seems that fluctuations of Ehrhart quasi-polynomials have not been considered until now.

9.2. Proof of Theorem 9.3

9.2.A. General setup. We start with the following classical QDE problem:

Quadratic Diophantine Equations

Input: $\alpha, \beta, \gamma \in \mathbb{N}$.

Decide: $\exists u \in \mathbb{N},\ 0 \le u < \gamma \ \ \text{s.t.}\ \ u^2 \equiv \alpha \,(\text{mod}\ \beta)$?

Manders and Adleman [MA78] proved that this problem[2] 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

$$f(u,v) \coloneqq (u^2 - \alpha - \beta v)^2 \quad \text{over} \quad (u,v) \in \mathrm{B} \cap \mathbb{Z}^2. \tag{9.2}$$

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:

$$u = \lfloor t/\beta \rfloor \quad \text{and} \quad v = t \,(\text{mod}\ \beta) = t - \beta \lfloor t/\beta \rfloor.$$

[2] We already used this in Theorem 7.58.

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:

$$\begin{aligned} f\big(\lfloor t/\beta \rfloor, t - \beta\lfloor t/\beta \rfloor\big) &= \Big(\lfloor t/\beta \rfloor^2 - \alpha - \beta\big(t - \beta\lfloor t/\beta \rfloor\big)\Big)^2 \\ &= \Big(\lfloor t/\beta \rfloor\big(\lfloor t/\beta \rfloor + \beta^2\big) - \big(\alpha + \beta t\big)\Big)^2 \qquad (9.3) \\ &= \underbrace{\lfloor t/\beta \rfloor^2\big(\beta^2 + \lfloor t/\beta \rfloor\big)^2}_{T_1(t)} + \underbrace{\big(\alpha + \beta t\big)^2}_{T_2(t)} - \underbrace{2\lfloor t/\beta \rfloor\big(\beta^2 + \lfloor t/\beta \rfloor\big)\big(\alpha + \beta t\big)}_{S(t)}. \end{aligned}$$

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:

$$\begin{aligned} -S(t) &= -S(t) \,+\, 2\beta(\beta^2 + \beta)(\alpha + \beta t) \,-\, 2\beta(\beta^2 + \beta)(\alpha + \beta t) \,+\, \sigma \,-\, \sigma \qquad (9.4) \\ &= \Big[\beta(\beta^2 + \beta) - \lfloor t/\beta \rfloor\big(\beta^2 + \lfloor t/\beta \rfloor\big)\Big]2(\alpha + \beta t) \,+\, \sigma \,-\, 2\beta(\beta^2 + \beta)(\alpha + \beta t) - \sigma \\ &= \underbrace{\big(\beta - \lfloor t/\beta \rfloor\big)\big(\beta^2 + \beta + \lfloor t/\beta \rfloor\big)(2\alpha + 2\beta t)}_{T_3(t)} + \underbrace{\big[\sigma \,-\, 2\beta(\beta^2 + \beta)(\alpha + \beta t)\big]}_{T_4(t)} - \sigma. \end{aligned}$$

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:

$$\min_{0 \le t < N} g(t) \;=\; \min_{0 \le t < N} T_1(t) \,+\, \ldots \,+\, T_4(t). \qquad (9.5)$$

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.

9.2.B. 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:

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

(see Figure 9.1). 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 9.1). Formally, let:

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

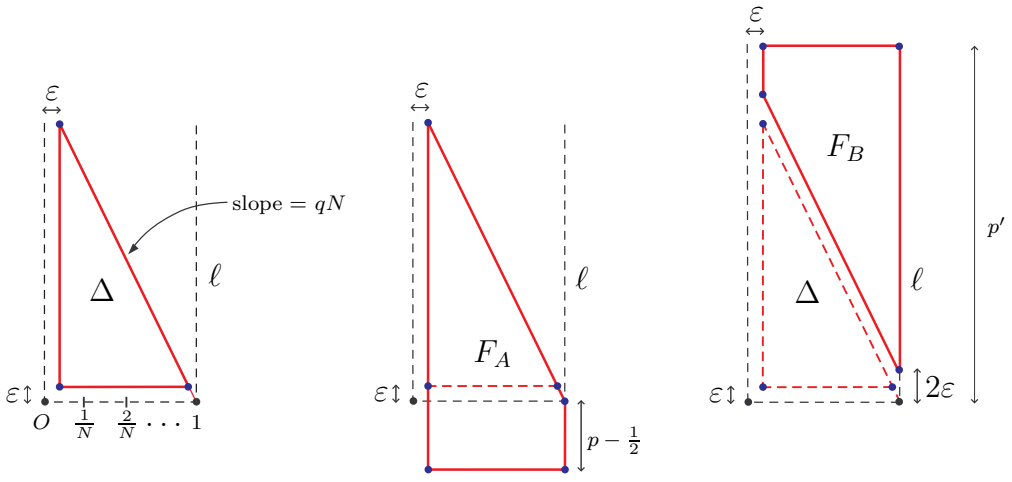


Figure 9.1: The triangle Δ and trapezoids F_A, F_B.

Let us show that these trapezoids encode the function as stated above. For F_A, we have $(F_A + t\vec{v}) \cap \ell = \big[\frac{1}{2} - p,\, qt\big]$, and thus $|F_A + t\vec{v}| = p + qt$. For F_B, the hypotenuse of $F_B + t\vec{v}$ intersects ℓ at $qt + 2\varepsilon$. Thus, we have $(F_B + t\vec{v}) \cap \ell = \big[qt + 2\varepsilon,\, p'\big]$, 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 9.2). 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:

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

respectively (see Figure 9.2).

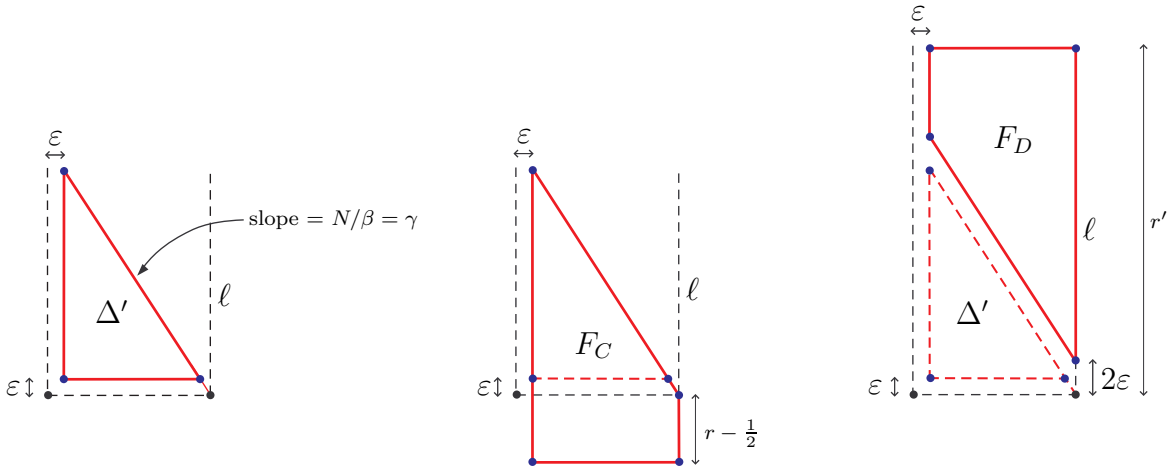


Figure 9.2: The triangle Δ' and trapezoids F_C, F_D.

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 $t \in [0, N)$.

9.2.C. 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:

$$P \;=\; \big\{(x, y_1, \ldots, y_d) \in \mathbb{R}^{d+1} \;:\; \max_{1\le i\le d} \mu_i \le x \le \min_{1\le i\le d} \nu_i,\; \rho_i + \tau_i x \le y_i \le \rho_i' + \tau_i' x\big\}. \tag{9.6}$$

It is clear that for every t and every vertical hyperplane $H = \{x = x_0\}$ in $\mathbb{R}^{d+1}$, we have $(P + t\vec{v}) \cap H = \big((F_1 + t\vec{v}) \cap H\big) \times \cdots \times \big((F_d + t\vec{v}) \cap H\big)$.[3] 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.

9.2.D. Putting it all together. We apply this product construction to each of the four terms T_1, T_2 in (9.3), T_3, T_4 in (9.4) 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

$$|P_i + t\vec{v}| \;=\; T_i(t \bmod N) \quad \text{for every } t \in \mathbb{Z}. \tag{9.7}$$

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

$$\begin{aligned}
Q_1 \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1, \ldots, x_5) \in P_1,\; x_6 = 1\},\\
Q_3 \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1, \ldots, x_4) \in P_3,\; x_5 = 1,\; x_6 = 0\},\\
Q_2 \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1, \ldots, x_3) \in P_2,\; x_4 = 1,\; x_5 = 0,\; x_6 = 0\},\\
Q_4 \;&=\; \{\mathbf{x} \in \mathbb{R}^6 \;:\; (x_1, x_2) \in P_4,\; x_3 = 1,\; x_4 = 0,\; x_5 = 0,\; x_6 = 0\}.
\end{aligned} \tag{9.8}$$

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

Note that $Q_1, \ldots, Q_4$ are all disjoint. Define the polytope

$$W = \operatorname{conv}(Q_1, \ldots, Q_4). \tag{9.9}$$

Because of the way $P_1, \ldots, P_4$ are embedded in $\mathbb{R}^4$, for every $t \in \mathbb{Z}$ we have:

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

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 (9.5), 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, polytope W has in total 60 vertices, as desired. □

9.3. Proof of Theorem 9.2

We modify the construction in the proof of Theorem 9.3 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 (9.3) and (9.4), 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.[4] 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:

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

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

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 9.3. Define the real set

$$Z_\delta \;=\; \Big\{ \frac{t}{N} + \tau \;:\; t \in \mathbb{Z},\; -\delta/4 \le \tau \le \delta/4 \Big\}. \tag{9.10}$$

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 (9.6)). Note that $P'_i = P_i + \delta \vec{e}_1$ and by (9.7), for every $\lambda \in Z_\delta$ we have:

$$|P'_i + \lambda \vec{e}_1| \;=\; |P_i + t(\lambda)\vec{v}| \;=\; T_i(t(\lambda) \bmod N) \quad (1 \le i \le 4). \tag{9.11}$$

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

$$Y_\delta \;=\; \Big\{ \frac{t}{N} + \tau \;:\; t \in \mathbb{Z},\; \frac{\delta}{8} \le \tau \le \frac{1}{N} - \frac{\delta}{8} \Big\}. \tag{9.12}$$

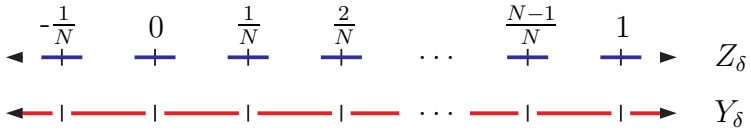


Figure 9.3: The sets Z_δ and Y_δ consisting of bold segments.

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 (9.3)–(9.5). 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 9.4).

Lemma 9.7. *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.

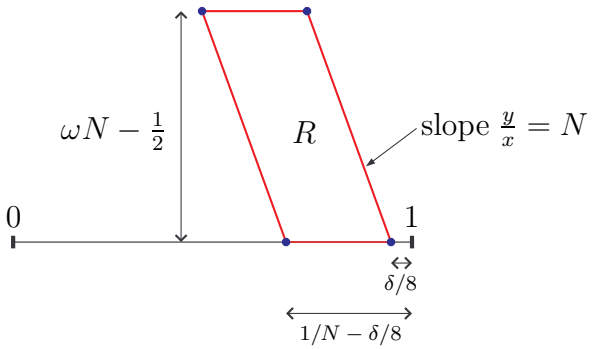


Figure 9.4: The parallelogram R.

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 (9.11). We embed them into $\mathbb{R}^5$ similarly to (9.8):

$$\begin{aligned}
Q'_1 &= \{\mathbf{x} \in \mathbb{R}^6 \,:\, (x_1, \ldots, x_5) \in P'_1,\ x_6 = 1\},\\
Q'_3 &= \{\mathbf{x} \in \mathbb{R}^6 \,:\, (x_1, \ldots, x_4) \in P'_3,\ x_5 = 1,\ x_6 = 0\},\\
Q'_2 &= \{\mathbf{x} \in \mathbb{R}^6 \,:\, (x_1, \ldots, x_3) \in P'_2,\ x_4 = 1,\ x_5 = 0,\ x_6 = 0\},\\
Q'_4 &= \{\mathbf{x} \in \mathbb{R}^6 \,:\, (x_1, x_2) \in P'_4,\ x_3 = 1,\ x_4 = 0,\ x_5 = 0,\ x_6 = 0\}.
\end{aligned} \tag{9.13}$$

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

$$Q'_5 = \{\mathbf{x} \in \mathbb{R}^6 \,:\, (x_1, x_2) \in R, \quad x_3 = 0,\ x_4 = 0,\ x_5 = 0,\ x_6 = 0\}.$$

Now let $W' = \operatorname{conv}(Q'_1, \ldots, Q'_5)$. By the above embeddings, we have:

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

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 (9.10) and (9.12). In this case, by (9.11) and Lemma 9.7, 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:

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

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 9.2. □

9.4. Applications

9.4.A. Proof of Theorem 9.4. Recall the polytope $P \subset \mathbb{R}^6$ from Theorem 9.3 with 60 vertices and the translation vector $\vec{v} = \vec{e}_1/N$. From the construction in Section 9.2, it is clear that P has at least one integer point, which we call $\vec{p}$. We translate P by $-\vec{p}$ so that $(0,0) \in P$, 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). Then for every $0 \le t < N$, the two polytopes

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

satisfy $R_t \subset R'_t$, even though R'_t is just slightly larger. Since both polytopes are closed, if they differ by very little, we should have $|R_t| = |R'_t|$. To ensure this for all $0 \le t < N$, it is enough to pick M so that $N/M < d_1/D_2$, where:

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

Here $\delta(\cdot,\cdot)$ denotes the shortest distance between two 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 $0 \le t < N$. Let $Q = \frac{1}{M}P + \vec{v}$, then $R'_t = (t+M)Q$. Thus, $|R_t| = |(t+M)Q|$ for every $0 \le t < N$. 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

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

Thus, computing $\min_{0\le t<N} |(t+M)Q| = \min_{0\le t<N} |P + t\vec{v}|$ 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. □

9.4.B. Proof of Theorem 9.5. The constants K, M will be later quantified. Recall that

$$p(t) \;=\; \sum_{i=1}^{r} \gamma_i \prod_{j=1}^{n} \big\lfloor \alpha_{ij} t + \beta_{ij} \big\rfloor \tag{9.14}$$

with $\gamma_i \in \mathbb{Z}$. By increasing d 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 9.8. *For every $n \ge 2$, we have the identity:*

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

where

$$\sigma_j(S) = \begin{cases} 1 & \text{if } \; j-1 \in S \\ -1 & \text{if } \; j-1 \notin S \end{cases}, \;\; \tau_j(S) = \begin{cases} 1 & \text{if } \; s_{\max} > j \\ -1 & \text{if } \; s_{\max} \le j \end{cases}, \;\; \sigma(S) = \max(0, n - s_{\max} - 1),$$

and $s_{\max} = \max(S)$.

Proof. Straightforward by induction, starting with the base case $n = 2$:

$$3g_1g_2 + h_1h_2 = (g_1 - h_1)(g_2 - h_2) + g_1(g_2 + h_2) + (g_1 + h_1)g_2.$$

The inductive step from $n-1$ to n is:

$$\begin{aligned} 3^{n-1} g_1 \ldots g_n + h_1 \ldots h_n \;\; = \;\; & 3(g_1 - h_1)(3^{n-2} g_2 \ldots g_n - h_2 \ldots h_n) + \\ & g_1(3^{n-2} g_2 \ldots g_n + h_2 \ldots h_n) + (g_1 + h_1) 3^{n-2} g_2 \ldots g_n. \end{aligned}$$

Now replace $-h_2$ by h_2' in the first term and apply the $(n-1)$-st step. □

The point of this lemma 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:

$$q_i(t) + 3^{n-1}g^n = h_{i1}(t) \ldots h_{in}(t) + 3^{n-1}g^n = \sum_{S \subseteq [n],\, S \neq \varnothing} 3^{\delta(S)} g^{n-|S|} \prod_{j \in S} \big(g \,\pm\, h_{ij}(t)\big). \quad (9.15)$$

Now the trapezoid construction from Section 9.2 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 (9.15), we take the product of the trapezoids for the terms $g \pm h_{ij}(t)$ with the construction from §9.2.C. 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 (there are $2^n - 1$ of them), we pad in another extra n dimensions, and augment each P_S with the coordinates of a distinct point in $\{0,1\}^n$ (see (9.8)). Taking the convex hull of the resulting polytopes, we get some 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 $t \in \mathbb{Z}$. 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 (9.14). 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 the proof of Theorem 9.4 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 9.5. □

9.5. Integer polytopes

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

Proposition 9.9. *For integer polytopes, the* k-ETP *problem is polynomial time solvable.*

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, BR04]. 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 9.2 continues to hold for integer polytopes. However, it is not difficult to see that Theorem 9.3 extends to this setting:

Theorem 9.10. *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 §9.2.B can be reused, with the ε's removed to make all their vertices integer.[5] A small complication arises for trapezoids of type F_D in Figure 9.2, 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 $t \in [0, N)$

[5] Those ε's only mattered in Section 9.3, where we say that small perturbation does not change the number of integer points in the trapezoids.

with $\beta | t$ can be ignored because they correspond to $v = 0$ in (9.2), 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 9.11. *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 Chapter 7). Here $1/N$ is a small enough refinement of the unit interval. Then the short GF technique of taking intersections (see Theorem 7.14) 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 9.6. We refer to [Bra16] for a recent survey article and references therein.

9.6. Final remarks and open problems

9.6.A. 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 Proposition 7.49). From this point of view, our Theorem 9.2 is unsurprising, since it uses a counting oracle in a restricted setting.

9.6.B. 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 9.2 is not sharp.

Conjecture 9.12. *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 intermediate between P and NP.

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

Conjecture 9.13. *For some fixed* n*, the* Polytope Translation *problem for rational simplices* $\Delta \subset \mathbb{R}^n$ *is* NP*-hard.*

By analogy, we believe that Theorem 9.4 also holds for simplices:

Conjecture 9.14. 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 9.15. *The k-*Frobenius Problem *is* NP*-hard for some fixed n.*

9.6.C. Corollary 9.6 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.

[Aa16] S. Aaronson, $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$, in *Open problems in mathematics*, Springer, New York, 2016, 1–122.

[AOW14] D. Adjiashvili, T. Oertel and R. Weismantel, A polyhedral Frobenius theorem with applications to integer optimization, *SIAM J. Discrete Math.* **29** (2015), 1287–1302.

[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 structureand the k-Frobenius problem, in *Recent Trends in Combinatorics*, Springer, 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, 2009.

[A+16] M. Aschenbrenner, A. Dolich, D. Haskell, D. Macpherson and S. Starchenko, Vapnik-Chervonenkis density in some theories without the independence property, I, *Trans. AMS* **368** (2016), 5889–5949.

[BMS86] E. Bach, G. Miller and J. Shallit, Sum of divisors, perfect numbers and factoring, *SIAM J. Comput.* **15** (1986), 1143–1154.

[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.

[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.

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

[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.

[Bar94] A. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed, *Math. Oper. Res.* **19** (1994), 769–779.

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

[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, UK, 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.

[BV07] N. Berline and M. Vergne, Local Euler–Maclaurin formula for polytopes, *Mosc. Math. J.* **7** (2007), 355–386.

[BWG17] T. Bogart, J. Goodrick and K. Woods, Parametric Presburger Arithmetic: logic, combinatorics, and quasi-polynomial behavior, *Discrete Anal.*, 2017:4, 34 pp.

[BGNW18] T. Bogart, J. Goodrick, D. Nguyen and K. Woods, Parametric Presburger Arithmetic: Complexity of Counting and Quantifier Elimination, preprint; `arxiv:1802.00974`.

[BGP92] E. Bombieri, A. Granville and J. Pintz, Squares in arithmetic progressions, *Duke Math. J.* **66** (1992), 369–385.

[BT76] I. Borosh, L. B. Treybig, Bounds on positive integral solutions of linear Diophantine equations, Proc. Amer. Math. Soc. 55 (1976), no. 2, 299–304.

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

[Cai07] J-Y. Cai, $\mathsf{S}_2^{\mathsf{P}} \subseteq \mathsf{ZPP}^{\mathsf{NP}}$, *J. Comput. System Sci.* **73** (2007), 25–35.

[CH16] D. Chistikov and C. Haase, The taming of the semi-linear set, in *Proc. ICALP 2016*, 127:1–127:13.

[Che16] A. Chernikov, *Models theory and combinatorics*, course notes, UCLA; available electronically at `https://tinyurl.com/y8ob6uyv`.

[Chu36] A. Church, An Unsolvable Problem of Elementary Number Theory, *Amer. J. Math.* **58** (1936), no. 2, 345–363.

[CL98] P. Clauss and V. Loechner, Parametric analysis of polyhedral iteration spaces, *J. VLSI Signal Process.* **19** (1998), 179–194.

[Coo72] D. C. Cooper, Theorem proving in arithmetic without multiplication, in *Machine Intelligence* (B. Meltzer and D. Michie, eds.), Edinburgh Univ. Press, 1972, 91–99.

[Dav73] M. Davis, Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly* **80** (1973), 233–269.

[DHK09] J. A. De Loera, R. Hemmecke, M. Köppe, Pareto optima of multicriteria integer linear programs, *INFORMS J. Comput.* **21** (2009), 39–48.

[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.

[DHTY04] J. A. De Loera, R. Hemmecke, J. Tauzer and R. Yoshida, Effective lattice point counting in rational convex polytopes, *J. Symbolic Comput.* **38** (2004), 1273–1302.

[DRS10] J. A. De Loera, J. Rambau and F. Santos, *Triangulations*, Springer, Berlin, 2010.

[DHWZ16] A. Del Pia, R. Hildebrand, R. Weismantel and K. Zemmer, Minimizing cubic and homogeneous polynomials over integers in the plane, *Math. Oper. Res.* **41** (2016), 511–530.

[DW14] A. Del Pia and R. Weismantel, Integer quadratic programming in the plane, in *Proc. 25th SODA*, ACM, New York, 2014, 840–846.

[DK97] M. Dyer and R. Kannan, On Barvinok's algorithm for counting lattice points in fixed dimension, *Math. Oper. Res.* **22** (1997), 545–549.

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

[Eis03] F. Eisenbrand, Fast integer programming in fixed dimension, in *Proc. 11th ESA*, Springer, Berlin, 2003, 196–207.

[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.

[ER09] F. Eisenbrand and T. Rothvoß, New hardness results for Diophantine approximation, in*Lecture Notes Comput. Sci.* **5687**, Springer, Berlin, 2009, 98–110.

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

[FR74] M. J. Fischer and M. O. Rabin, Super-Exponential Complexity of Presburger Arithmetic, in*Proc. SIAM-AMS Symposium in Applied Mathematics*, AMS, Providence, RI, 1974, 27–41.

[FT87] A. Frank and É. Tardos, An application of simultaneous Diophantine approximation in combinatorial optimization, *Combinatorica* **7** (1987), 49–65.

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

[Fü82] M. Fürer, The complexity of Presburger Arithmetic with bounded quantifier alternation depth, *Theoret. Comput. Sci.* **18** (1982), 105–111.

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

[Gi66] S. Ginsburg, *The mathematical theory of context free languages*, McGraw-Hill, 1966.

[GS64] S. Ginsburg, E. Spanier, Bounded ALGOL-like languages, *Trans. Amer. Math. Soc.* **113** (1964), 333–368.

[GP17] P. Glivický and P. Pudlák, Wild models of linear arithmetics, to appear in *Mathematical Logic Quarterly*, 2017; `arXiv:1602.03083`.

[Grä88] E. Grädel, Subclasses of Presburger Arithmetic and the polynomial-time hierarchy, *Theoret. Comput. Sci.* **56** (1988), no. 3, 289–301.

[Grä87] E. Grädel, *The complexity of subclasses of logical theories*, Dissertation, Universität Basel, 1987.

[GTW] E. Grädel, W. Thomas and T. Wilke (Eds.), *Automata, Logics, and Infinite Games. A Guide to Current Research*, Springer, Berlin, 2002.

[GLS89] M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer, Berlin, 1988.

[Guy04] R. K. Guy, *Unsolved problems in number theory* (Third edition), Springer, New York, 2004.

[Haa14] C. Haase, Subclasses of Presburger Arithmetic and the weak EXP hierarchy, in *Proc. joint 23rd EACSL and 29th LICS*, Article No. 47, 10 pp., ACM, New York, 2014.

[HW] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, UK, 2008.

[Hie16] P. Hieronymi, Expansions of the ordered additive group of real numbers by two discrete subgroups, *J. Symb. Log.* **81** (2016), no. 3, 1007–1027.

[Hie15] P. Hieronymi, When is scalar multiplication decidable, preprint; arXiv:1409.6701.

[HNP18] P. Hieronymi, D. Nguyen and I. Pak, Presburger Arithmetic with algebraic scalar multiplications, preprint; arXiv:1805.03624.

[HTe18] P. Hieronymi and A. Terry Jr., Ostrowski Numeration Systems, Addition, and Finite Automata, *Notre Dame J. Form. Log.* **59** (2018), 215–232.

[HTy14] P. Hieronymi and M. Tychonievich, Interpreting the projective hierarchy in expansions of the real line, *Proc. AMS* **142** (2014), 3259–3267.

[HWZ17] R. Hildebrand, R. Weismantel and K. Zemmer, An FPTAS for minimizing indefinite quadratic forms over integers in polyhedra, in *Proc. 27th SODA*, ACM, New York, 2016, 1715–1723.

[Hou15] B. Hough, Solution of the minimum modulus problem for covering systems, *Ann. of Math.* **181** (2015), 361–382.

[HUM06] J. E. Hopcroft, J. Ullman and R. Motwani, *Introduction to automata theory, languages, and computation* (3rd ed.), Addison-Wesley, 2006.

[HS07] S. Hosten, B. Sturmfels, Computing the integer programming gap, *Combinatorica* **27** (2007), 367–382.

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

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

[KB79] R. Kannan, A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **8** (1979), 499–507.

[Kar13] O. Karpenkov, *Geometry of continued fractions*, Springer, Heidelberg, 2013.

[KM00] M. Karpinski and A. Macintyre, Approximating volumes and integrals in o-minimal and p-minimal theories, in *Connections between model theory and algebraic and analytic geometry*, Seconda Univ. Napoli, Caserta, 2000, 149–177.

[KM97] M. Karpinski and A. Macintyre, Polynomial bounds for VC dimension of sigmoidal and general Pfaffian neural networks, *J. Comput. System Sci.* **54** (1997), 169–176.

[KP00] L. Khachiyan and L. Porkolab, Integer optimization on convex semialgebraic sets, *Discrete Comput. Geom.* **23** (2000), no. 2, 207–224

[Khi64] A. Ya. Khinchin, *Continued fractions*, Univ. of Chicago Press, Chicago, IL, 1964.

[KS01] A. Klivans and D. Spielman, Randomness efficient identity testing of multivariate polynomials, in *Proc. 33rd FOCS*, ACM, New York, 2001, 216–223.

[Köp12] M. Köppe, On the complexity of nonlinear mixed-integer optimization, *Mixed integer nonlinear programming*, 533–557, IMA Vol. Math. Appl., 154, Springer, New York, 2012.

[Köp07] M. Köppe, A primal Barvinok algorithm based on irrational decompositions, *SIAM J. Discrete Math.* **21** (2007), 220–236.

[KV08] M. Köppe and S. Verdoolaege, Computing parametric rational generating functions with a primal Barvinok algorithm, *Electron. J. Combin.* **15** (2008), no. 1, RP 16, 19 pp.

[Lag85] J. Lagarias, The computational complexity of simultaneous Diophantine approximation problems, *SIAM J. Comput.* **14** (1985), 196–209.

[LO87] J. Lagarias and A. Odlyzko, Computing $\pi(x)$: an analytic method, *J. Algorithms* **8** (1987), 173–191.

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

[Ler05] J. Leroux, A Polynomial Time Presburger Criterion and Synthesis for Number Decision Diagrams, in *Proc. 20th LICS*, IEEE, Chicago, IL, 2005, 147–156.

[Lov89] L. Lovász, Geometry of numbers and integer programming, in*Mathematical programming*, SCIPRESS, Tokyo, 1989, 177–201.

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

[Mei93] S. Meiser, Point location in arrangement of hyperplanes, *Inform. and Comput.* **106** (1993), 286–303.

[Mey75] A. Meyer, Weak monadic second order theory of succesor is not elementary-recursive, in *Proc. Logic Colloquium* (Boston, Mass., 1972–1973), pp. 132–154. Lecture Notes in Math., Vol. 453, Springer, Berlin, 1975.

[Mil01] C. Miller, Expansions of dense linear orders with the intermediate value property, *J. Symbolic Logic* **66** (2001), 1783–1790.

[MM11] C. Moore and S. Mertens, *The nature of computation*, Oxford Univ. Press, Oxford, 2011.

[NW06] T. Neary, D. Woods, Small fast universal Turing machines, *Theoret. Comput. Sci.* **362** (2006), 171–195.

[NP18] D. Nguyen and I. Pak, On the number of integer points in translated and expanded polyhedra, preprint; arXiv:1805.03685.

[NP17a] VC-dimension of short Presburger formulas, preprint; arxiv:1710.04171.

[NP17b] D. Nguyen and I. Pak, Short Presburger Arithmetic is hard, in *Proc. 58th FOCS*, IEEE, Los Alamitos, CA, 2017, 37–48; arXiv:1708.08179.

[NP17c] D. Nguyen and I. Pak, The computational complexity of integer programming with alternations, in *Proc. 32nd CCC*, LIPIcs. Leibniz Int. Proc. Inform. **79**, 2017; arXiv:1702.08662.

[NP17d] D. Nguyen and I. Pak, Complexity of short generating functions, *Forum of Mathematics, Sigma* **6** (2018) E.1; arXiv:1702.08660.

[NP17e] D. Nguyen and I. Pak, Complexity of short Presburger Arithmetic, in *Proc. 49th STOC*, ACM, New York, 2017, 812–820; arXiv:1704.00249.

[NP17f] D. Nguyen and I. Pak, Enumeration of integer points in projections of unbounded polyhedra, *SIAM J. Discrete Math.* **32** (2018), 986–1002.

[Opp78] D. C. Oppen, A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger Arithmetic, *J. Comput. System Sci.* **16** (1978), 323–332.

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

[Pak09] I. Pak, *Lectures on Discrete and Polyhedral Geometry*, monograph draft, 2009; available electronically at https://tinyurl.com/y9hayto.

[Par66] R. Parikh, On context-free languages, *J. Assoc. Comput. Mach.* **13** (1966), 570–581.

[Pre29] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt (in German), in*Comptes Rendus du I congrès de Mathématiciens des Pays Slaves*, Warszawa, 1929, 92–101.

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

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

[RL78] C. R. Reddy and D. W. Loveland, Presburger Arithmetic with bounded quantifier alternation, in *Proc. 10th STOC*, ACM, 1978, 320-325.

[Rei02] K. Reinhardt, The complexity of translating logic to finite automata, in *Automata, logics, and infinite games*, 231–238, Lecture Notes in Comput. Sci., 2500, Springer, Berlin, 2002.

[Rib96] P. Ribenboim, *The new book of prime number records*, Springer, New York, 1996.

[RS92] A. M. Rockett and P. Szüsz, *Continued fractions*, World Sci., River Edge, NJ, 1992.

[Sa72] N. Sauer, On the density of families of sets, *J. Combin. Theory, Ser. A* **13** (1972), 145–147.

[Sca84] B. Scarpellini, Complexity of subcases of Presburger Arithmetic, *Trans. AMS* **284** (1984), 203–218.

[Sch97] U. Schöning, Complexity of Presburger Arithmetic with fixed quantifier dimension, *Theory Comput. Syst.* **30** (1997), 423–428.

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

[Sh72] S. Shelah, A combinatorial problem; stability and order for models and theories in infinitary languages, *Pacific J. Math.* **41** (1972), 247–261.

[Sil11] J. H. Silverman, *A Friendly Introduction to Number Theory*, Pearson, 2011.

[Sko31] T. Skolem, Über einige Satzfunktionen in der Arithmetik (in German), in *Skr. Norske Vidensk. Akad., Oslo, Math.-naturwiss. Kl.* **7**, 1931, 1–28.

[Sto74] L. Stockmeyer, *The Complexity of Decision Problems in Automata Theory and Logic*, Ph.D. thesis, Massachusetts Institute of Technology, 1974, 224 pp.

[SM73] L. J. Stockmeyer and A. R. Meyer, Word problems requiring exponential time: preliminary report, in *Proc. Fifth STOC*, ACM, New York, 1973, 1–9.

[Sze74] E. Szemerédi, The number of squares in an arithmetic progression, *Studia Sci. Math. Hungar.* **9** (1974), no. 3-4, 417.

[TCH12] T. Tao, E. Croot and H. Helfgott, Deterministic methods to find primes, *Math. Comp.* **81** (2012), 1233–1246.

[TV06] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Univ. Press, Cambridge, UK, 2006.

[Tho12] W. Thomas, Finite automata and the analysis of infinite transition systems, in *Modern applications of automata theory*, World Sci., Hackensack, NJ, 2012, 495–527.

[vdDH92] L. van den Dries, J. Holly, Quantifier elimination for modules with scalar variables, *Ann. Pure Appl. Logic* **57** (1992), no. 2, 161–179.

[vEB81] P. van Emde Boas, Another NP-complete partition problem and the complexity of computing shortvectors in a lattice, *Math. Dept. Report* **81–04**, Univ. Amsterdam, April 1981, 10 pp.

[Vap98] V. N. Vapnik, *Statistical learning theory*, John Wiley, New York, 1998.

[VC71] V. N. Vapnik and A. Ja. Chervonenkis, The uniform convergence of frequencies of the appearance of events to their probabilitie, *Theor. Probability Appl.* **16** (1971), 264–280.

[Weil84] A. Weil, *Number theory. An approach through history*, Birkhäuser, Boston, MA, 1984.

[Wei99] V. D. Weispfenning, Mixed real–integer linear quantifier elimination, in *Proc. 1999 ISSAC*, ACM, New York, 1999, 129–136.

[Wei97] V. D. Weispfenning, Complexity and uniformity of elimination in Presburger Arithmetic, in *Proc. 1997 ISSAC*, ACM, New York, 1997, 48–53.

[V+07] S. Verdoolaege, R. Seghir, K. Beyls, V. Loechner and M. Bruynooghe, Counting integer points in parametric polytopes using Barvinok's rational functions, *Algorithmica* **48** (2007), 37–66.

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

[Woo15] K. Woods, Presburger Arithmetic, rational generating functions, and quasi-polynomials, *J. Symb. Log.* **80** (2015), 433–449.

[Woo14] K. Woods, The unreasonable ubiquitousness of quasi-polynomials, *Electron. J. Combin.* **21** (2014), no. 1, Paper 1.44, 23 pp.

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

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

[Zie95] G. Ziegler, *Lectures on polytopes*, Springer, New York, 1995.