ENUMERATION OF INTEGER POINTS IN PROJECTIONS OF UNBOUNDED POLYHEDRA

DANNY NGUYEN AND IGOR PAK

Abstract. 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-Frobenius problem*.

1. Introduction

1.1. **The results.** The *integer linear programming* is a classical subject with many advances and applications to other areas. The pioneer result by Lenstra [Len83] shows that the *feasibility* of integer linear programming in fixed dimension can be decided in polynomial time:

$$(\circ) \qquad \exists \mathbf{x} \,:\, A\mathbf{x} \,\le\, \overline{b}.$$

This result was extended by Kannan [Kan90], who showed that *parametric integer linear programming* in fixed dimension can be decided in polynomial time:

$$(\circ\circ) \qquad \forall \mathbf{y} \in (P \cap \mathbb{Z}^n)\, \exists \mathbf{x} \in \mathbb{Z}^m \,:\, A\mathbf{x} \,+\, B\mathbf{y} \,\le\, \overline{b}.$$

Both results rely on difficult results in geometry of numbers and can be viewed geometrically: $(\circ)$ asks whether a polyhedron $Q = \{A\mathbf{x} \le \overline{b}\} \subseteq \mathbb{R}^n$ has an integer point. Similarly, $(\circ\circ)$ asks whether every integer point in polyhedron P is a projection of an integer point in polyhedron $Q = \{A\mathbf{x} + B\mathbf{y} \le \overline{b}\} \subseteq \mathbb{R}^{m+n}$.

Barvinok [Bar93] famously showed that the number of integer points in polytopes in fixed dimension can be computed in polynomial time. He used a technology of *short generating functions* (GF) to enumerate the integer points in general (possibly unbounded) rational polyhedra in $\mathbb{R}^n$ in the following form:

$$(\circledast) \qquad f(\mathbf{t}) \,=\, \sum_{i=1}^{N} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1-\mathbf{t}^{\overline{b}_{i1}})\cdots(1-\mathbf{t}^{\overline{b}_{ik_i}})}\,,$$

where $\mathbf{t}^{\overline{a}} = t_1^{a_1} \cdots t_n^{a_n}$ for $\overline{a} = (a_1, \ldots, a_n)$. This technology allows to compute the number of integer points in the bounded case, but also take intersections, unions and complements for general (possibly unbounded) polyhedra [Bar08, BP99].

Barvinok's algorithm was extended to projections of polytopes by Barvinok and Woods [BW03], see Theorem 4.1. The result has a major technical drawback: while it does generalize Kannan's result for bounded P and Q as in $(\circ\circ)$, it does not apply for unbounded polyhedra. The main result of this paper is an extension of Barvinok's algorithm to the unbounded case.

---

*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {ldnguyen,pak}@math.ucla.edu.
December 1, 2016.

Theorem 1.1. *Let $m, n \in \mathbb{N}$ be fixed. Given a (possibly unbounded) polyhedron $Q = \{\mathbf{x} \in \mathbb{R}^m : A\mathbf{x} \le \bar{b}\}$, and a linear transformation $T : \mathbb{Z}^m \to \mathbb{Z}^n$ satisfying $T(\mathbb{Z}^m) \subseteq \mathbb{Z}^n$, let $g(\mathbf{t})$ be the GF for $T(Q \cap \mathbb{Z}^m)$:*

$$g(\mathbf{t}) = \sum_{\mathbf{y} \in T(Q \cap \mathbb{Z}^m)} \mathbf{t}^{\mathbf{y}}.$$

Then there is a polynomial time algorithm to compute $g(\mathbf{t})$ in the form of a short GF ($\circledast$).

Our main tool is a structural result describing projections of *semilinear sets*, which are defined as disjoint union of intersections of polyhedra and lattice cosets. More precisely, we prove that such projections are also semilinear and give bound on (combinatorial) complexity of the projections (Theorem 3.4). In combination with the Barvinok–Woods theorem this gives the extension to unbounded polyhedra.

We then present a far-reaching generalization of our results to all formulas in *Presburger Arithmetic*: we first prove a the structural result (Theorem 5.2) and then a generalization of Theorem 1.1 (Theorem 5.3). We illustrate the power of our generalization in the case of the *k-Frobenius Problem.*

1.2. **Connections and applications.** Lenstra's original algorithm was further improved in [Eis03, FT87]. Kannan's algorithm was generalized in [ES08] by removing the condition that P has a bounded affine dimension. Barvinok's algorithm has been simplified and improved in [DK97, KV08]. Both Barvinok's and Barvinok–Woods' algorithms have been implemented and used for practical computation [D+04, Köp07, V+07].

Let us emphasize that in the context of parametric integer programming, there are 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) For a fixed unbounded polyhedron Q and a varying polytope P in ($\circ\circ$), one can count the number of points in the projection of Q within P, by intersecting Q with a box of growing size and then projecting it. The Barvinok–Woods algorithm is called multiple times for different boxes. Our approach allows to call the Barvinok–Woods algorithm only once to project Q (unbounded), and then call a more economical Barvinok's algorithm to compute the intersection with P. See Section 6 for an explicit example.

2. Standard definitions and notations

We use $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, \ldots\}$.
All constant vectors are denoted $\overline{a}, \overline{b}, \overline{c}, \overline{d}, \overline{n}, \overline{v}$, etc.
Matrices are denoted A, B, C, etc.
Variables are denoted x, y, z, etc.; vectors of variables are denoted $\mathbf{x}, \mathbf{y}, \mathbf{z}$, etc.
We write $\mathbf{x} \le \mathbf{y}$ if $x_j \le y_j$ for coordinate in vectors $\mathbf{x}$ and $\mathbf{y}$.
We also write $\mathbf{x} \le N$ to mean that each coordinate is $\le N$.
GF is an abbreviation for "*generating function.*"
Multivariate GFs are denoted by $f(\mathbf{t}), g(\mathbf{t}), h(\mathbf{t})$, etc.
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.
The *affine dimension* of P is denoted by $\dim(P)$.

Integer lattices are denoted by $\mathcal{L}, \mathcal{T}, \mathcal{U}, \mathcal{W}$, etc.
Let $\operatorname{rank}(\mathcal{L})$ denotes the *rank* of lattice $\mathcal{L}$.
Patterns are denoted by $\boldsymbol{L}, \boldsymbol{T}, \boldsymbol{S}, \boldsymbol{U}, \boldsymbol{W}$, etc.
Let $\phi(\cdot)$ denotes the *binary length* of a number, vector, matrix, GF, or a logical formula.
For a polyhedron Q described by a linear system $A\mathbf{x} \le \bar{b}$, let $\phi(Q)$ denote the total length $\phi(A) + \phi(\bar{b})$.
For a lattice $\mathcal{L}$ generated by a matrix A, we use $\phi(\mathcal{L})$ to denote $\phi(A)$.

3. Structure of a projection

3.1. **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 3.1. Given a set $X \subseteq \mathbb{R}^{n+1}$, the *projection* of X, 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 $\mathbf{y} \in \operatorname{proj}(Q)$, denote by $\operatorname{proj}^{-1}(\mathbf{y}) \subseteq X$ the preimage of $\mathbf{y}$ in X.

Definition 3.2. 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 3.3. A *semilinear* set X is a set of the form

$$X = \bigsqcup_{i=1}^{k} Q_i \cap \boldsymbol{L}_i\,, \tag{3.1}$$

where each $Q_i \cap \boldsymbol{L}_i$ is a patterned polyhedron with period $\mathcal{L}_i$, and the polyhedra Q_i are a pairwise disjoint.[1] The *period length* $\psi(X)$ of X is defined as

$$\psi(X) = \sum_{i=1}^{k} \phi(Q_i) + \phi(\mathcal{L}_i).$$

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.

Our main structural result is the following theorem.

[1] In Theoretical CS literature, the semilinear sets are often given in a more explicit presentation which makes some operations like projections easy to compute, while structural properties harder to establish (see e.g. [CH16] and references therein).

Theorem 3.4. *Let $m, n \in \mathbb{N}$ be fixed. Let $X \subseteq \mathbb{Z}^m$ be a semilinear set of the form (3.1). 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*

$$T(X) = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j \,, \tag{3.2}$$

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 $\operatorname{poly}(\psi(X))$*. Moreover,*

$$r = \eta(X)^{O(m!)} \quad \text{and} \quad \eta(R_j) = \eta(X)^{O(m!)},\ 1 \leq j \leq r.$$

Remark 3.5. 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 (3.2) 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 3.4 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 3.4, we need a technical lemma:

Lemma 3.6. *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*

$$\operatorname{proj}(Q \cap \boldsymbol{L}) = \bigsqcup_{j=0}^{r} R_j \cap \boldsymbol{T}_j \,, \tag{3.3}$$

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 $\operatorname{poly}(\phi(Q) + \phi(\mathcal{L}))$*. Moreover,*

$$r = O\big(\eta(Q)^2\big) \quad \text{and} \quad \eta(R_j) = O\big(\eta(Q)^2\big), \quad \text{for all } \ 0 \leq j \leq r\,.$$

We postpone the proof of the lemma until Subsection 3.3.

3.2. **Proof of Theorem 3.4.**

We begin with the following standard definitions and notation.

Definition 3.7. A *copolyhedron* $P \subseteq \mathbb{R}^n$ 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 ($\overline{a}\,\mathbf{x} \leq b-1$), after scaling $\overline{a}$ and b to integers. Clearly, we have $P \cap \mathbb{Z}^n = \lfloor P \rfloor \cap \mathbb{Z}^n$.

Recall that X has the form (3.1) with each $Q_i \cap \boldsymbol{L}_i$ having period $\mathcal{L}_i$. Define a polyhedron

$$\widehat{Q}_i \coloneqq \big\{(\mathbf{x}, \mathbf{y}) : \mathbf{y} = T(\mathbf{x}) \text{ and } \mathbf{x} \in Q_i\big\} \subseteq \mathbb{R}^{m+n}. \tag{3.4}$$

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 $\mathcal{U}_i$. By (3.4), we have:

$$T(Q_i \cap \boldsymbol{L}_i) = S(\widehat{Q}_i \cap \boldsymbol{U}_i) \quad \text{and} \quad T(X) = \bigcup_{i=1}^{r} S(\widehat{Q}_i \cap \boldsymbol{U}_i),$$

where S is a vertical projection mapping $(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{m+n}$ to $\mathbf{y} \in \mathbb{R}^n$. We can write $S = S_1 \circ \cdots \circ S_m$, where each $S_i : \mathbb{R}^{i+n} \to \mathbb{R}^{i+n-1}$ is a projection along the x_{i+n} coordinate. We repeatedly apply Lemma 3.6 on $S_m, \ldots, S_1$.

Start by applying Lemma 3.6 on S_m. We have:

$$S_m(\widehat{Q}_i \cap \boldsymbol{U}_i) \;=\; \bigsqcup_{j=1}^{r_i} R_{ij} \cap \boldsymbol{T}_{ij} \quad \text{for all} \;\; 1 \le i \le k, \tag{3.5}$$

where each $R_{ij} \cap \boldsymbol{T}_{ij}$ is a patterned polyhedron in $\mathbb{Z}^{m+n-1}$ with period $\mathcal{T}_{ij}$. Note that two pieces R_{ij} and $R_{i'j'}$ can be overlapping for some $i \neq i'$. However, we can refine all R_{ij} into polynomially many disjoint copolyhedra $P_1, \dots, P_e$, so that

$$\bigcup_{i=1}^{k} \bigcup_{j=1}^{r_i} R_{ij} \;=\; \bigsqcup_{d=1}^{e} P_d\,. \tag{3.6}$$

For each P_d we can also find a pattern $\boldsymbol{W}_d$ with period $\mathcal{W}_d \subseteq \mathbb{Z}^{m+n-1}$. The (full-rank) period $\mathcal{W}_d$ can be taken as the intersection of polynomially many (full-rank) periods $\mathcal{T}_{ij}$ for which $P_d \subseteq R_{ij}$. We then round each P_d to $\lfloor P_d \rfloor$, see Definition 3.7. From (3.5) and (3.6) we have:

$$\bigcup_{i=1}^{k} S_m(\widehat{Q}_i \cap \boldsymbol{U}_i) \;=\; \bigsqcup_{d=1}^{e} \lfloor P_d \rfloor + \boldsymbol{W}_d\,.$$

The above RHS is a semilinear set in $\mathbb{R}^{m+n-1}$. A similar argument applies to $S_{m-1}, \dots, S_1$. In the end, we have (3.2).

Using Lemma 3.6, we can bound the number of polyhedra r_i in (3.5), 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 (3.6). By a careful analysis, after m projections, the total number r of pieces in the final decomposition (3.2) is at most $\eta(X)^{O(m!)}$. Each piece R_j also has at most $\eta(X)^{O(m!)}$ facets. $\square$

3.3. **Proof of Lemma 3.6.** The proof is by induction on n. The case $n = 0$ is trivial. For the rest of the proof, assume $n \ge 1$.

Let $\boldsymbol{L} \subseteq \mathbb{Z}^{n+1}$ be a pattern full-rank 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 $\mathcal{L}' = \operatorname{proj}(\mathcal{L})$. Since $\mathcal{L}$ is of full rank, we can define

$$\ell = \min\{t \in \mathbb{Z}_+ : (t, 0, \dots, 0) \in \mathcal{L}\}. \tag{3.7}$$

Let $R = \operatorname{proj}(Q)$. Assume Q is described by the system $A\mathbf{x} \le \overline{b}$. 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 $A\mathbf{x} \le \overline{b}$ into

$$A_1\mathbf{y} + \overline{b}_1 \le x_1, \quad x_1 \le A_2\mathbf{y} + \overline{b}_2 \quad \text{and} \quad A_3\mathbf{y} \le \overline{b}_3, \tag{3.8}$$

where $\mathbf{y} = (x_2, \dots, x_{n+1}) \in \mathbb{R}^n$. Then R is described by a system $C\mathbf{y} \le \overline{d}$, which consists of $(A_3\mathbf{y} \le \overline{b}_3)$ and $(\overline{a}_1\mathbf{y} + b_1 \le \overline{a}_2\mathbf{y} + b_2)$ for every possible pair of rows $\overline{a}_1\mathbf{y} + b_1$ and $\overline{a}_2\mathbf{y} + b_2$ from the first two systems in (3.8). Moreover, we can decompose

$$R \;=\; \bigsqcup_{j=1}^{r} P_j, \tag{3.9}$$

where each P_j is a copolyhedron, so that over each P_j, the largest row in $A_1\mathbf{y} + \overline{b}_1$ is $\overline{a}_{j1}\mathbf{y} + b_{j1}$ and the smallest row in $A_2\mathbf{y} + \overline{b}_2$ is $\overline{a}_{j2}\mathbf{y} + b_{j2}$. Thus, for every $\mathbf{y} \in P_j$, we have $\operatorname{proj}^{-1}(\mathbf{y}) = [\alpha_j(\mathbf{y}), \beta_j(\mathbf{y})]$, 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 $C\mathbf{y} \le \overline{d}$ 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 $1 \le j \le r$.

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 length of this segment. Now we refine the decomposition in (3.9) to

$$R \,=\, R_0 \sqcup R_1 \sqcup \cdots \sqcup R_r\,, \qquad \text{where} \tag{3.10}$$

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 $|\mathrm{proj}^{-1}(\mathbf{y})| \ge \ell$.
c) For every $\mathbf{y} \in R_j$ $(1 \le j \le r)$, we have the length $|\mathrm{proj}^{-1}(\mathbf{y})| < \ell$. 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

$$R_0 = \mathrm{proj}[Q \cap (Q + \ell\overline{v}_1)] \subseteq R,$$

where $\overline{v}_1 = (1, 0, \ldots, 0)$. The facets of R_0 can be found from those of $Q \cap (Q + \ell\overline{v}_1)$ again by Fourier–Motzkin elimination, and also $\eta(R_0) = O(m^2)$. Observe that $|\mathrm{proj}^{-1}(\mathbf{y})| \ge \ell$ 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 $\mathrm{proj}^{-1}(\mathbf{y}) = [\alpha_j(\mathbf{y}), \beta_j(\mathbf{y})]$. Therefore,

$$R_j \,=\, P_j \backslash R_0 \,=\, \{\mathbf{y} \in P_j : |\mathrm{proj}^{-1}(\mathbf{y})| < \ell\} \,=\, \{\mathbf{y} \in P_j : \alpha_j(\mathbf{y}) + \ell > \beta_j(\mathbf{y})\}.$$

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 (3.9), we can decompose:

$$R \,=\, R_0 \sqcup (R \backslash R_0) \,=\, R_0 \bigsqcup_{j=1}^{r} (P_j \backslash R_0) \,=\, \bigsqcup_{j=0}^{r} R_j\,.$$

This decomposition satisfies all conditions a)–c) and proves (3.10). 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 $\mathrm{proj}(Q \cap \boldsymbol{L})$ within R_0 has a simple pattern:

Lemma 3.8. $\mathrm{proj}(Q \cap \boldsymbol{L}) \cap R_0 \,=\, R_0 \cap \boldsymbol{L}'$.

Proof. Recall that $\mathrm{proj}(\boldsymbol{L}) = \boldsymbol{L}'$, 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 $\mathbf{y} = \mathrm{proj}(\mathbf{x})$. If $\mathbf{y} \in R_0 \cap \boldsymbol{L}'$, we also have $|\mathrm{proj}^{-1}(\mathbf{y})| \ge \ell$ by condition b), with ℓ defined in (3.7). The point $\mathbf{x}$ and the segment $\mathrm{proj}^{-1}(\mathbf{y})$ lie on the same vertical line. Therefore, since $|\mathrm{proj}^{-1}(\mathbf{y})| \ge \ell$, we can find another $\mathbf{x}'$ such that $\mathbf{x}' \in \mathrm{proj}^{-1}(\mathbf{y}) \subseteq Q$ 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 $\mathbf{y} \in \mathrm{proj}(Q \cap \boldsymbol{L})$. Therefore we have RHS $\subseteq$ LHS, and the lemma holds. □

It remains to show that $\mathrm{proj}(Q \cap \boldsymbol{L}) \cap R_j$ also has a pattern for every $j > 0$. By condition c), every such R_j has a "thin" preimage. Let $Q_j = \mathrm{proj}^{-1}(R_j) \subseteq Q$. 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 $\mathbf{y} \in R$, $\overline{v} \in D$ and $\lambda > 0$. Since $\mathbf{y} + \lambda\overline{v} \in R$, from c) we have $\mathrm{proj}^{-1}(\mathbf{y} + \lambda\overline{v}) = [\alpha(\mathbf{y} + \lambda\overline{v}), \beta(\mathbf{y} + \lambda\overline{v})]$. Denote by $\widetilde{\alpha}$ and $\widetilde{\beta}$ the linear parts of the affine maps α and β. By property of affine maps, we have:

$$\mathrm{proj}^{-1}(\mathbf{y} + \lambda\overline{v}) = [\alpha(\mathbf{y} + \lambda\overline{v}), \beta(\mathbf{y} + \lambda\overline{v})] = [\alpha(\mathbf{y}) + \lambda\widetilde{\alpha}(\overline{v}),\ \beta(\mathbf{y}) + \lambda\widetilde{\beta}(\overline{v})]. \tag{3.11}$$

Therefore,

$$|\mathrm{proj}^{-1}(\mathbf{y} + \lambda\overline{v})| = \beta(\mathbf{y}) - \alpha(\mathbf{y}) + \lambda\big[\widetilde{\beta} - \widetilde{\alpha}\big](\overline{v}).$$

Since $(\mathbf{y} + \lambda \overline{v}) \in R$, by c) we have:

$$0 \le |\mathrm{proj}^{-1}(\mathbf{y} + \lambda \overline{v})| = \beta(\mathbf{y}) - \alpha(\mathbf{y}) + \lambda\big[\widetilde{\beta} - \widetilde{\alpha}\big](\overline{v}) < \ell.$$

Because $\lambda > 0$ is arbitrary, we must have $\big[\widetilde{\beta} - \widetilde{\alpha}\big](\overline{v}) = 0$. This holds for all $\overline{v} \in D$. We conclude that $\big[\widetilde{\beta} - \widetilde{\alpha}\big]$ vanishes on the whole subspace $H \coloneqq \mathrm{span}(D)$, i.e., for any $\overline{v} \in H$ we have $\widetilde{\alpha}(\overline{v}) = \widetilde{\beta}(\overline{v})$. Thus, we can rewrite (3.11) as

$$\mathrm{proj}^{-1}(\mathbf{y} + \lambda \overline{v}) = [\alpha(\mathbf{y}), \beta(\mathbf{y})] + \lambda \widetilde{\alpha}(\overline{v}) = \mathrm{proj}^{-1}(\mathbf{y}) + \lambda \widetilde{\alpha}(\overline{v}). \tag{3.12}$$

Define $C \coloneqq \widetilde{\alpha}(D)$ and $G \coloneqq \widetilde{\alpha}(H)$. Note that $\mathrm{span}(C) = G$, because $\mathrm{span}(D) = H$. Recall that $R = R' + D$ with R' a polytope. In (3.12), we let $\mathbf{y}$ vary over R', λ vary over $\mathbb{R}_+$ and $\overline{v}$ vary over D. The LHS becomes $Q = \mathrm{proj}^{-1}(R)$. The RHS becomes $\mathrm{proj}^{-1}(R') + C$. Therefore, we have $Q = \mathrm{proj}^{-1}(R') + C$. Since $\mathrm{proj}^{-1}(R')$ is a polytope, we conclude that C is the recession cone for Q.

Because $\mathrm{proj}^{-1}(\mathbf{y}) = [\alpha(\mathbf{y}), \beta(\mathbf{y})]$ 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., $\mathrm{proj}(\widetilde{\alpha}(\mathbf{y})) = \mathrm{proj}(\widetilde{\alpha}(\mathbf{y})) = \mathbf{y}$. This implies $\mathrm{proj}(G) = H$, because $G = \widetilde{\alpha}(H)$. In other words, $\widetilde{\alpha}$ is the inverse map for proj on G (see Fig. 1).

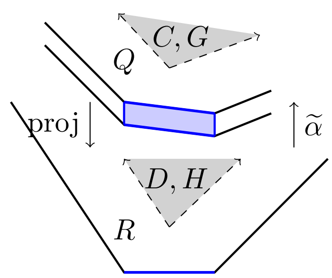

FIGURE 1. R and $Q = \mathrm{proj}^{-1}(R)$, with R' and $\mathrm{proj}^{-1}(R')$ shown in blue. The cones C and D span G and H, respectively.

Recall that $Q \cap \boldsymbol{L}$ is a patterned polyhedron with period $\mathcal{L}$, and $\mathrm{proj}(Q) = R$. Define

$$\mathcal{S} \coloneqq \mathcal{L} \cap G \quad \text{and} \quad \mathcal{T} \coloneqq \mathrm{proj}(\mathcal{S}) \subset \mathrm{proj}(G) = H.$$

Since $\mathcal{L}$ is full-rank, we have $\mathrm{rank}(\mathcal{S}) = \dim(G)$. Since $\widetilde{\alpha}$ and proj are inverse maps, we have $\mathcal{S} = \widetilde{\alpha}(\mathcal{T})$. We claim that $\mathrm{proj}(Q \cap \boldsymbol{L}) \subset R$ 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 $\mathbf{y}_1 \in \mathrm{proj}(Q \cap \boldsymbol{L})$, i.e., there exists $\mathbf{x}_1 \in Q \cap \boldsymbol{L}$ with $\mathrm{proj}(\mathbf{x}_1) = \mathbf{y}_1$. We show that $\mathbf{y}_2 \in \mathrm{proj}(Q \cap \boldsymbol{L})$. First, we have $\mathrm{proj}^{-1}(\mathbf{y}_1) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)]$ and $\mathrm{proj}^{-1}(\mathbf{y}_2) = [\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)]$. Let $\overline{v} = \mathbf{y}_2 - \mathbf{y}_1 \in \mathcal{T} \subset H$. By (3.12), we have:

$$[\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)] = \mathrm{proj}^{-1}(\mathbf{y}_2) = \mathrm{proj}^{-1}(\mathbf{y}_1 + \overline{v}) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)] + \widetilde{\alpha}(\overline{v}). \tag{3.13}$$

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 $\mathrm{proj}(\mathbf{x}_1) = \mathbf{y}_1$, we have:

$$\mathbf{x}_1 \in \mathrm{proj}^{-1}(\mathbf{y}_1) = [\alpha(\mathbf{y}_1), \beta(\mathbf{y}_1)] \subseteq Q.$$

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 $[\alpha(\mathbf{y}_2), \beta(\mathbf{y}_2)] = \mathrm{proj}^{-1}(\mathbf{y}_2)$ with

$$\mathbf{x}_2 - \mathbf{x}_1 = \alpha(\mathbf{y}_2) - \alpha(\mathbf{y}_1) = \widetilde{\alpha}(\mathbf{y}_2 - \mathbf{y}_1) = \widetilde{\alpha}(\overline{v}) \in \widetilde{\alpha}(\mathcal{T}) = \mathcal{S}.$$

This $\mathbf{x}_2$ satisfies $\mathrm{proj}(\mathbf{x}_2) = \mathbf{y}_2$. 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 $\mathbf{y}_2 \in \mathrm{proj}(Q \cap \boldsymbol{L})$.

So we have established that $\mathrm{proj}(Q \cap \boldsymbol{L}) \subset R$ is a patterned polyhedron with period $\mathcal{T}$. Note that

$$\mathrm{rank}(\mathcal{T}) = \mathrm{rank}(\mathcal{S}) = \dim(G) = \dim(H) = \dim(D).$$

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 $\mathrm{span}(D) = H$. 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 $\mathrm{proj}(Q \cap \boldsymbol{L})$.

To summarize, for every piece R_j and $Q_j = \mathrm{proj}^{-1}(R_j)$, $1 \leq j \leq r$, the projection $\mathrm{proj}(Q_j \cap \boldsymbol{L}) \subset R_j$ has period $\mathcal{T}_j$. Thus $\mathrm{proj}(Q_j \cap \boldsymbol{L})$ is a patterned polyhedron. This completes the proof. $\square$

4. Finding short GF for unbounded projection

4.1. **Barvinok–Woods algorithm.** In this section, we are again assuming that dimensions m and n are fixed. We recall the Barvinok–Woods algorithm, which finds in polynomial time a short GF for the projection of integer points in a polytope:

Theorem 4.1 ([BW03])**.** *Let $m, n \in \mathbb{N}$ be fixed. Given a rational polytope $Q = \{\mathbf{x} \in \mathbb{R}^m : A\mathbf{x} \leq \overline{b}\}$, and a linear transformation $T : \mathbb{Z}^m \to \mathbb{Z}^n$ satisfying $T(\mathbb{Z}^m) \subseteq \mathbb{Z}^n$, there is a polynomial time algorithm to compute a short GF for $T(Q \cap \mathbb{Z}^m)$ as:*

$$g(\mathbf{t}) \; = \sum_{\mathbf{y} \,\in\, T(Q \cap \mathbb{Z}^m)} \mathbf{t}^{\mathbf{y}} \; = \; \sum_{i=1}^{M} \frac{c_i \, \mathbf{t}^{\overline{a}_i}}{(1 - \mathbf{t}^{\overline{b}_{i1}}) \ldots (1 - \mathbf{t}^{\overline{b}_{is}})}, \tag{4.1}$$

where $c_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$, $\overline{b}_{ij} \neq 0$ for all i, j, and s is a constant depending only on m. Furthermore, the short GF $g(\mathbf{t})$ has length $\phi(g) = \mathrm{poly}(\phi(Q) + \phi(T))$, where

$$\phi(g) \; = \; \sum_{i} \lceil \log_2 |c_i| + 1 \rceil \; + \; \sum_{i,j} \lceil \log_2 a_{ij} + 1 \rceil \; + \; \sum_{i,j,k} \lceil \log_2 b_{ijk} + 1 \rceil . \tag{4.2}$$

Clearly, extend our main result Theorem 1.1 is an extension of Theorem 4.1. The proof of Theorem 1.1 is based on Theorem 3.4 and uses the following standard result:

Proposition 4.2 (see e.g. [Mei93])**.** *Let $n \in \mathbb{N}$ be fixed. Let $R = \{\mathbf{x} \in \mathbb{R}^n : C\mathbf{x} \leq \overline{d}\}$ be a possibly unbounded polyhedron. There is a decomposition*

$$R = \bigsqcup_{k=1}^{t} R_k \oplus D_k \,, \tag{4.3}$$

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 $\mathrm{poly}(\phi(R))$.

4.2. **Proof of Theorem 1.1.** Without loss of generality, we can assume $\dim(Q) = m$ and $\dim(T(Q)) = n$. Clearly, the set $X = Q \cap \mathbb{Z}^m$ is a semilinear, 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 $\operatorname{poly}(\phi(Q) + \phi(P))$. Assume P is given by a system $C\mathbf{y} \le \bar{d}$. For any $\overline{v} \in P$, we have $\overline{v} \in T(X)$ if and only if the following system has a solution $\mathbf{x} \in \mathbb{Z}^m$:

$$S_{\overline{v}} \;\coloneqq\; \begin{cases} A\mathbf{x} & \le \;\; \bar{b} \\ T(\mathbf{x}) & = \;\; \overline{v} \end{cases}. \tag{4.4}$$

By bound on integer programming solutions (see [Sch86, Cor. 17.1b]), $S_{\overline{v}}$ has a solution $\mathbf{x} \in \mathbb{Z}^m$ if and only if it has a solution $\mathbf{x} \in \mathbb{Z}^m$ with binary length at most $\operatorname{poly}(\phi(S_{\overline{v}}))$. Since $\overline{v} \in P$, and P is bounded, we have $\phi(\overline{v}) = \operatorname{poly}(\phi(P))$. Because $S_{\overline{v}}$ involves only $\overline{v}, Q$ and T, we have $\phi(S_{\overline{v}}) = \operatorname{poly}(\phi(P) + \phi(Q) + \phi(T))$. Thus, we can find $N \in \mathbb{N}$ of length $\log(N) = \operatorname{poly}(\phi(P) + \phi(Q) + \phi(T))$, such that (4.4) remains equivalent with the extra condition $-N \le \mathbf{x} \le N$. Define a polytope $\widehat{Q} \subset \mathbb{R}^m$ by:

$$\begin{cases} A\mathbf{x} & \le \;\; \bar{b} \\ C\,T(\mathbf{x}) & \le \;\; \bar{d} \\ -N \le \mathbf{x} & \le \;\; N \end{cases}.$$

Applying Theorem 4.1 to $\widehat{Q}$, we get 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 3.4 to X, we have a decomposition:

$$T(X) = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j\,. \tag{4.5}$$

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 4.2, we can decompose

$$R = \bigsqcup_{i=1}^{t_j} R_i \oplus D_i \quad \text{and} \quad R \cap \boldsymbol{T} = \bigsqcup_{i=1}^{t_j} (R_i \oplus D_i) \cap \boldsymbol{T}. \tag{4.6}$$

Recall from Theorem 3.4 that $\mathcal{T}$ has full rank. Let $d_i = \dim(D_i)$ and $\overline{v}_i^1, \dots, \overline{v}_i^{d_i}$ be the generating rays of the (simple) cone D_i. For each $\overline{v}_i^t$, we can find $n_t \in \mathbb{Z}_+$ such that $\overline{w}_i^t = n_t \overline{v}_i^t \in \mathcal{T}$. Let P_i and $\mathcal{T}_i$ be the parallelepiped and lattice spanned by $\overline{w}_i^1, \dots, \overline{w}_i^{d_i}$, respectively. We have $D_i = P_i + \mathcal{T}_i$ and therefore

$$R_i \oplus D_i = R_i \oplus (P_i + \mathcal{T}_i) = (R_i \oplus P_i) + \mathcal{T}_i. \tag{4.7}$$

Each $R_i \oplus P_i$ is a copolytope. Note that Theorem 4.1 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 3.7 (Section 3.2). 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 (4.7), we can get the short GF $f_i(\mathbf{t})$ for $(R_i \oplus D_i) \cap \boldsymbol{T}$ as

$$f_i(\mathbf{t}) = \sum_{\mathbf{y} \in (R_i \oplus D_i) \cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} = \sum_{\mathbf{y} \in (R_i \oplus P_i) \cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} . \sum_{\mathbf{y} \in \mathcal{T}_i} \mathbf{t}^{\mathbf{y}} = h_i(\mathbf{t}) \prod_{t=1}^{d_i} \frac{1}{1 - \mathbf{t}^{\overline{w}_i^t}}. \tag{4.8}$$

By (4.6), we obtain

$$g(\mathbf{t}) = \sum_{\mathbf{y}\in R\cap \boldsymbol{T}} \mathbf{t}^{\mathbf{y}} \;=\; \sum_{1\,\le\, i\,\le\, t_j} f_i(\mathbf{t}). \tag{4.9}$$

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 (4.5), we get a short GF for $T(X)$, as desired. ☐

Remark 4.3. Throughout the paper we sidestep the convergence of GFs issue by working with formal power series. When valuation is taken into account, any formal GF with infinite line will vanish. We refer to [Bar08, BP99] for a careful explanation.

5. Sets defined by Presburger formulas

In this section, all variables $x, y, z, \mathbf{x}, \mathbf{y}, \mathbf{z}$, etc., are over $\mathbb{Z}$. *Presburger Arithmetic* (PA) is the first order theory on the integers that allows only additions and inequalities. In other words, each *atom* (quantifier and Boolean free term) in PA is an integer inequality of the form

$$a_1x_1 + \ldots + a_nx_n \le b,$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ are integer variables, and $a_1, \ldots, a_n, b \in \mathbb{Z}$ are integer constants. A general PA formula is formed by taking negations, conjunctions, disjunctions of such inequalities, and also quantifiers $\forall/\exists$ over different variables. A sentence in PA is a formula with all variables quantified. Every integer programming problem can be expressed as an existential PA sentence of the form

$$\exists \mathbf{x} : A\mathbf{x} \le b.$$

This is because rational half-spaces describing a polyhedron Q can be rescaled to integer inequalities.

Fix $k \in \mathbb{Z}_+$ and a vector of dimensions $\overline{n} = (n_1, \ldots, n_k) \in \mathbb{Z}_+^k$. Let $\mathbf{x}_1 \in \mathbb{Z}^{n_1}, \ldots, \mathbf{x}_k \in \mathbb{Z}^{n_k}$ be vectors of integer variables. We consider the class $\mathrm{PA}_{k,\overline{n}}$ consisting of Presburger formulas F of the form

$$F \;=\; \big\{\mathbf{x}_1 : Q_2\mathbf{x}_2 \ldots Q_k\mathbf{x}_k \; \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)\big\}.$$

Here $Q_2, \ldots, Q_k \in \{\forall, \exists\}$ are any k quantifiers, and $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ is a Boolean combination of linear inequalities in $\mathbf{x}_1, \ldots, \mathbf{x}_k$. For a specific value of $\mathbf{x}_1 \in \mathbb{Z}^{n_1}$, the *substituted formula* $F(\mathbf{x}_1)$ is a Presburger sentence in variables $\mathbf{x}_2, \ldots, \mathbf{x}_k$. We say that $\mathbf{x}_1$ *satisfies* F if $F(\mathbf{x}_1)$ is a true Presburger sentence. To simplify the notation, we identify a formula F with the set of integer points $\mathbf{x}_1$ that satisfy F. The length $\phi(F)$ is the total length of all symbols and constants in F written in binary.

Example 5.1. The formula $F = \{x : \forall y \; (5y \ge x+1) \vee (5y \le x-1)\} \in \mathrm{PA}_{2,(1,1)}$ determines the set of non-multiples of 5.

Below is our main result for this section, which generalizes Theorem 3.4.

Theorem 5.2. *Fix k and $\overline{n}$. Given a Presburger 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 $\mathrm{poly}(\phi(F))$.

Proof. Consider any $F \in \mathrm{PA}_{k,\overline{n}}$ of the form:

$$F = \{\mathbf{x}_1 : Q_2\mathbf{x}_2 \dots Q_k\mathbf{x}_k \; \Phi(\mathbf{x}_1, \dots, \mathbf{x}_k)\}.$$

Let $\overline{\mathbf{x}} = (\mathbf{x}_1, \dots, \mathbf{x}_k)$ and $n = n_1 + \dots + n_k$. Let us show directly that

$$X = \{\overline{\mathbf{x}} \in \mathbb{Z}^n : \Phi(\overline{\mathbf{x}})\}$$

is semilinear. Recall that Φ is a Boolean combination of linear inequalities. Using Proposition 5.2.2 in [Woo04], we can rewrite Φ into a disjunctive normal form of polynomial length:

$$\Phi = (A_1\overline{\mathbf{x}} \leq \overline{b}_1) \vee \dots \vee (A_t\overline{\mathbf{x}} \leq \overline{b}_t).$$

Here, each $A_i\overline{\mathbf{x}} \leq \overline{b}_i$ is a system of inequalities, describing a polyhedron $P_i \subseteq \mathbb{R}^n$. Moreover, all polyhedra $P_1, \dots, P_t$ are pairwise disjoint, and $\sum_{i=1}^{t} \phi(P_i) = \mathrm{poly}(\phi(F))$. In other words, the set X consists of integer points in a disjoint union of t polyhedra. Thus, X is a semilinear set with $\psi(X) = \mathrm{poly}(\phi(F))$, in the notation of Definition 3.3.

The proof goes by recursive construction of sets $X^{(k)}, X^{(k-1)}, \dots, X^{(1)}$. Let $X^{(k)} := X$. If $Q_k = \exists$, we consider the set

$$X^{(k-1)} \;:=\; \big\{(\mathbf{x}_1, \dots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; \Phi(\overline{\mathbf{x}})\big\} \;=\; \big\{(\mathbf{x}_1, \dots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; [\overline{\mathbf{x}} \in X^{(k)}]\big\}.$$

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 3.4, we can find in polynomial time a decomposition of the form (3.2) for $X^{(k-1)}$. Moreover, we have $\psi(X^{(k-1)}) = \mathrm{poly}(\psi(X^{(k)}))$.

Similarly, if $Q_k = \forall$, we consider

$$X^{(k-1)} \;:=\; \big\{(\mathbf{x}_1, \dots, \mathbf{x}_{k-1}) : \forall \mathbf{x}_k \; \Phi(\overline{\mathbf{x}})\big\} \;=\; \neg\big\{(\mathbf{x}_1, \dots, \mathbf{x}_{k-1}) : \exists \mathbf{x}_k \; [\overline{\mathbf{x}} \in \neg X^{(k)}]\big\}.$$

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 $\big(\mathbb{R}^n \setminus \sqcup_{i=1}^{p} P_i\big)$ can also be partitioned into polynomially many pairwise disjoint polyhedra. Indeed, we can represent $\sqcup_{i=1}^{p} P_i$ by a Boolean expression of linear inequalities in $\mathbf{x}$. Therefore, the complement can also be represented by a Boolean expression. By Proposition 5.2.2 in [Woo04] mentioned above, we can rewrite the complement as a disjoint union of polynomially many polyhedra $P'_1, \dots, P'_q$. From here, we obtain the decomposition:

$$\neg X = \bigsqcup_{i=1}^{p} P_i \cap \boldsymbol{L}'_i \;\; \bigsqcup_{j=1}^{q} P'_j \cap \mathbb{Z}^n\,,$$

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 3.4, we can obtain $X^{(k-1)}$ by projecting $\neg X^{(k)}$.

Applying the above argument recursively for quantifers $Q_{k-1}, \dots, Q_2$, we obtain a polynomial length decomposition for the semilinear set

$$X^{(1)} = \{\mathbf{x}_1 \in \mathbb{Z}^{n_1} : Q_2\mathbf{x}_2 \dots Q_k\mathbf{x}_k \; \Phi(\mathbf{x})\} = F.$$

This completes the proof. □

Theorem 5.3. *Fix k and $\overline{n}$. Let $F \in \mathrm{PA}_{k,\overline{n}}$ be a Presburger formula and M be a positive integer. Denote by $f_M(\mathbf{t})$ the partial GF*

$$f_M(\mathbf{t}) \coloneqq \sum_{\mathbf{x} \in F,\, |\mathbf{x}| \le M} \mathbf{t}^{\mathbf{x}}. \tag{5.1}$$

Suppose there is an oracle computing $f_M(\mathbf{t})$ as a short GF ($\circledast$) in time $\mu(F, M)$. Then there is an integer $N = N(F)$ with $\log(N) = \mathrm{poly}(\phi(F))$, 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 $\mathrm{poly}(\phi(F))$.

In other words, Theorem 5.3 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 5.2, we have a decomposition

$$F = \bigsqcup_{j=1}^{r} R_j \cap \boldsymbol{T}_j\,.$$

We proceed similarly to the proof of Theorem 1.1. Denote R_j and $\boldsymbol{T}_j$ by R and $\boldsymbol{T}$ respectively, for convenience. We have the decomposition (4.6) for R and $R \cap \boldsymbol{T}$, which leads to (4.7). Eventually, we can compute a short GF $g(\mathbf{t})$ for $R \cap \boldsymbol{T}$ using (4.8) and (4.9). 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 (4.8), cannot be obtained from Theorem 4.1, since F is no longer the result of a single projection.

Recall that each $R_i \oplus P_i$ is a polytope, with facets of total length $\mathrm{poly}(\phi(F))$. 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

$$\log(N) = \mathrm{poly}(\phi(F)) \quad \text{and} \quad R_i \oplus P_i \subseteq [-N, N]^n \quad \text{for all } 1 \le i \le t_j.$$

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.

Barvinok's theorem [Bar93] (see also Theorem 4.4 in [BP99]) allows us to compute in polynomial time a short GF

$$f_i(\mathbf{t}) = \sum_{\mathbf{x} \in (R_i \oplus P_i) \cap \mathbb{Z}^n} \mathbf{t}^{\mathbf{x}}$$

for each polytope $R_i \oplus P_i$. Theorem 10.2 in [BP99] 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

$$h_i(\mathbf{t}) \;=\; \sum_{\mathbf{x} \in (R_i \oplus P_i) \cap F} \mathbf{t}^{\mathbf{x}} \;=\; \left(\sum_{\mathbf{x} \in (R_i \oplus P_i) \cap \mathbb{Z}^n} \mathbf{t}^{\mathbf{x}} \right) \star \left(\sum_{\mathbf{x} \in F \cap [-N,N]^n} \mathbf{t}^{\mathbf{x}} \right) \;=\; f_i(\mathbf{t}) \star f_N(\mathbf{t}).$$

in time $\mathrm{poly}(\mu(F, N))$. Here $\star$ is the *Hadamard product* of two power series (see [BP99]). 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. $\square$

Remark 5.4. We emphasize that Theorem 5.3 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 $F \in \mathrm{PA}_{2,(1,1)}$. This result is proved in [Woo04, Prop. 5.3.2], and is ultimately derived from a result by Schöning [Sch97], which says that deciding the truth of Presburger sentences of the form $\exists x \forall y\ \Phi(x, y)$ is an NP-complete problem.

6. The k-feasibility problem

We present an application of Theorem 5.3. Let n, d and k be fixed integers and $A \in \mathbb{Z}^{d\times n}$. In [ADL16], the authors defined a set $\operatorname{Sg}_{\geq k}(A) \in \mathbb{Z}^d$ of *k-feasible* vectors as

$$\operatorname{Sg}_{\geq k}(A) = \{\mathbf{y} \in \mathbb{Z}^d \,:\, \exists \mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{N}^n,\ \mathbf{y} = A\mathbf{x}_j,\ \mathbf{x}_i \neq \mathbf{x}_j \text{ if } i \neq j,\ 1 \leq i, j \leq k\}. \tag{6.1}$$

In other words, $\operatorname{Sg}_{\geq k}(A)$ 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 $\operatorname{Sg}_{\geq k}(A)$, the authors also gave an algorithm to compute a short GF for $\operatorname{Sg}_{\geq k}(A)$ within a finite box:

Theorem 6.1 (Theorem 5 in [ADL16])**.** *Fix n, d and k. Let $A \in \mathbb{Z}^{d\times n}$, and let N be a positive integer. Let*

$$f_N(\mathbf{t}) = \sum_{\mathbf{x} \,\in\, \operatorname{Sg}_{\geq k}(A) \cap [-N,N]^d} \mathbf{t}^{\mathbf{x}}$$

be the partial GF for $\operatorname{Sg}_{\geq k}(A)$ 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 5.3, we can extend Theorem 6.1 as follows:

Theorem 6.2. *Fix n, d and k. Then there is a polynomial time algorithm to compute*

$$f(\mathbf{t}) = \sum_{\mathbf{x} \,\in\, \operatorname{Sg}_{\geq k}(A)} \mathbf{t}^{\mathbf{x}}$$

for the entire set $\operatorname{Sg}_{\geq k}(A)$, as a short GF.

Proof. From the definition (6.1), we see that $\operatorname{Sg}_{\geq k}(A)$ is a Presburger formula in variables $\mathbf{y}, \mathbf{x}_1, \dots, \mathbf{x}_k$ with only an existential ($\exists$) quantifier. Indeed, each condition $\mathbf{y} = A\mathbf{x}_j$ is a system of 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 $\operatorname{Sg}_{\geq k}(A) \in \mathrm{PA}_{k+1,\overline{n}}$, where $\overline{n} = (d, n, \dots, n)$.

Applying Theorem 5.3, we can compute in polynomial time the a short GF $f(\mathbf{t})$ for $\operatorname{Sg}_{\geq k}(A)$ given the partial short GF $f_N(\mathbf{t})$. Finally, Theorem 6.1 allows us to compute $f_N(\mathbf{t})$ in polynomial time. □

Theorem 6.1 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 6.3. *Fix n and k, but let d be arbitrary. Then there is a polynomial time algorithm to compute*

$$f(\mathbf{t}) = \sum_{\mathbf{x} \,\in\, \operatorname{Sg}_{\geq k}(A)} \mathbf{t}^{\mathbf{x}}$$

for the entire set $\operatorname{Sg}_{\geq k}(A)$, 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 $\operatorname{rank}(\mathcal{L}_A) = \operatorname{rank}(A) \leq n$. 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 6.2 to get a short GF $g(\mathbf{t})$ for $\operatorname{Sg}_{\geq k}(B)$. The GF for $\operatorname{Sg}_{\geq k}(A)$ is easily obtained from $g(\mathbf{t})$ by a variable substitution via U^{-1}. □

7. Conclusion

We extend 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 prove 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.

We refer to [Gin66] for a related investigation of semilinear sets in the context of Presburger Arithmetic, and to [CH16] for most recent developments. The study of semilinear sets has important applications in other areas, such as analysis of *number decision diagrams* (see [Ler03, Ler05]), and integer optimization (see e.g. [AOW14]). Let us also mention that in a forthcoming paper [NP17+] we give a far-reaching generalization of results by Lenstra, Kannan, Barvinok and Barvinok–Woods to general Presburger Arithmetic formulas.

Finally, we refer to [RA05] for an extensive introduction to the Frobenius problem. This was an original application by Kannan of his pioneering result [Kan92], an application first suggested by Lovász [Lov89].

Acknowledgements. We are greatly indebted to Sasha Barvinok and Sinai Robins for introducing us to the subject. We are also thankful to Iskander Aliev, Matthias Aschenbrenner, Artëm Chernikov, Jesús De Loera, Lenny Fukshansky and Oleg Karpenkov for interesting conversations and helpful remarks. The second author was partially supported by the NSF.

References

[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.

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

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

[Bar93] A. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed, *Math. Oper. Res.* **19** (1994), 769–779.

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

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

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

[BV07] N. Berline and M. Vergne, Local Euler–Maclaurin formula for polytopes, *Mosc. Math. J.* **7** (2007), 355–386.

[CH16] D. Chistikov and C. Haase, The taming of the semi-linear set, in *Proc. ICALP 2016*, 127:1–127:13.

[D+04] 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.

[DK97] M. Dyer and R. Kannan, On Barvinok's algorithm for counting lattice points in fixed dimension, *Math. Oper. Res.* **22** (1997), 545–549.

[Eis03] F. Eisenbrand, Fast integer programming in fixed dimension, in *Proc. 11th ESA*, Springer, Berlin, 2003, 196–207.

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

[FT87] A. Frank and É. Tardos, An application of simultaneous Diophantine approximation in combinatorial optimization, *Combinatorica* **7** (1987), 49–65.

[Gin66] S. Ginsburg, *The mathematical theory of context free languages*, McGraw-Hill, 1966.

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

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

[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.

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

[Ler03] J. Leroux, The Affine Hull of a Binary Automaton is Computable in Polynomial Time, In *Proc. 5th INFINITY*, Marseille, France, 2003, *Electronic Notes in Theor. Comp. Sci.* **98** (2004), 89–104.

[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.

[Mei93] S. Meiser, Point location in arrangement of hyperplanes, *Inform. and Comput.* **106** (1993), 286–303.

[NP17+] D. Nguyen and I. Pak, Short Presburger Arithmetic is in P, in preparation.

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

[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.

[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.

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