Presburger Arithmetic, Rational Generating Functions, and Quasi-polynomials[⋆]

Kevin Woods

Oberlin College, Oberlin, Ohio, USA, Kevin.Woods@oberlin.edu

Abstract. A Presburger formula is a Boolean formula with variables in $\mathbb{N}$ that can be written using addition, comparison ($\leq$, $=$, etc.), Boolean operations (and, or, not), and quantifiers ($\forall$ and $\exists$). We characterize sets that can be defined by a Presburger formula as exactly the sets whose characteristic functions can be represented by rational generating functions; a geometric characterization of such sets is also given. In addition, if $\mathbf{p} = (p_1, \ldots, p_n)$ are a subset of the free variables in a Presburger formula, we can define a counting function $g(\mathbf{p})$ to be the number of solutions to the formula, for a given $\mathbf{p}$. We show that every counting function obtained in this way may be represented as, equivalently, either a piecewise quasi-polynomial or a rational generating function. In the full version of this paper, we also translate known computational complexity results into this setting and discuss open directions.

1 Introduction

A broad and interesting class of sets are those that can be defined over $\mathbb{N} = \{0, 1, 2, \ldots\}$ with first order logic and addition.

Definition 1. *A* Presburger formula *is a Boolean formula with variables in* $\mathbb{N}$ *that can be written using addition, comparison ($\leq$, $=$, etc.), Boolean operations (and, or, not), and quantifiers ($\forall$ and $\exists$). We will denote a generic Presburger formula as $F(\mathbf{u})$, where $\mathbf{u}$ are the free variables (those not associated with a quantifier); we use bold notation like $\mathbf{u}$ to indicate vectors of variables.*

We say that a set $S \subseteq \mathbb{N}^d$ is a Presburger set *if there exists a Presburger formula $F(\mathbf{u})$ such that $S = \{\mathbf{u} \in \mathbb{N}^d : \ F(\mathbf{u})\}$.*

Example 1. The Presburger formula

$$F(u) = \big(u > 1 \text{ and } \exists b \in \mathbb{N} : \ b + b + 1 = u\big)$$

defines the Presburger set $\{3, 5, 7, \ldots\}$. Since multiplication by an integer is the same as repeated addition, we can conceive of a Presburger formula as a Boolean combination of integral linear (in)equalities, appropriately quantified: $\exists b \ \big(u > 1$ and $2b + 1 = u\big)$.

[⋆] Full version available at http://www.oberlin.edu/faculty/kwoods/papers.html.

Presburger proved [35] that the truth of a Presburger *sentence* (a formula with no free variables) is decidable. In contrast, a broader class of sentences, where multiplication of variables is allowed, is undecidable; this is a consequence of the negative solution to Hilbert's 10th problem, given by Davis, Putnam, Robinson, and Matiyasevich (see, for example, [19]).

We would like to understand more clearly the *structure* of a given Presburger set. One way to attempt to do this is to encode the elements of the set into a generating function.

Definition 2. *Given a set $S \subseteq \mathbb{N}^d$, its associated* generating function *is*

$$f(S;\mathbf{x}) = \sum_{\boldsymbol{s}\in S} \mathbf{x}^{\boldsymbol{s}} = \sum_{(s_1,\ldots,s_d)\in S} x_1^{s_1} x_2^{s_2} \cdots x_d^{s_d}.$$

For example, if S is the set defined by Example 1, then

$$f(S;x) = x^3 + x^5 + x^7 + \cdots = \frac{x^3}{1-x^2}.$$

We see that, in this instance, the generating function has a nice form; this is not a coincidence.

Definition 3. *A* rational generating function *is a function that can be written in the form*

$$\frac{q(\mathbf{x})}{(1-\mathbf{x}^{\boldsymbol{b}_1})\cdots(1-\mathbf{x}^{\boldsymbol{b}_k})},$$

where $q(\mathbf{x})$ is a polynomial in $\mathbb{Q}[\mathbf{x}]$ and $\boldsymbol{b}_i \in \mathbb{N}^d \setminus \{\mathbf{0}\}$.

We will prove that $S \subseteq \mathbb{N}^d$ is a Presburger set if and only if $f(S;\boldsymbol{x})$ is a rational generating function. These are Properties 1 and 3 in the following theorem:

Theorem 1. *Given a set $S \subseteq \mathbb{N}^d$, the following are equivalent:*

1. *S is a Presburger set,*
2. *S is a finite union of sets of the form $P \cap (\lambda + \varLambda)$, where P is a polyhedron, $\lambda \in \mathbb{Z}^d$, and $\varLambda \subseteq \mathbb{Z}^d$ is a lattice.*
3. *$f(S;\boldsymbol{x})$ is a rational generating function.*

Property 2 gives a nice geometric characterization of Presburger sets; the set in Example 1 can be written as $[3,\infty) \cap (1+2\mathbb{Z})$.

We are particularly interested in generating functions because of their powerful flexibility: we can use algebraic manipulations to answer questions about the set. For example, $f(S;1,1,\ldots,1)$ is exactly the cardinality of S (if finite). More generally, we may want to count solutions to a Presburger formula as a function of several parameter variables:

Definition 4. *The* Presburger counting function *for a given Presburger formula $F(\boldsymbol{c},\boldsymbol{p})$ is*

$$g_F(\boldsymbol{p}) = \#\{\boldsymbol{c} \in \mathbb{N}^d : \; F(\boldsymbol{c},\boldsymbol{p})\}.$$

Note that $\boldsymbol{c}$ (the *counted* variables) and $\boldsymbol{p}$ (the *parameter* variables) are free variables. We will restrict ourselves to counting functions such that $g_F(\boldsymbol{p})$ is finite for all $\boldsymbol{p} \in \mathbb{N}^n$. One could instead either include ∞ in the codomain of g_F or restrict the domain of g_F to where $g_F(\boldsymbol{p})$ is finite (this domain would itself be a Presburger set).

A classic example is to take $F(\mathbf{c}, p)$ to be the conjunction of linear inequalities of the form $a_1c_1 + \cdots + a_dc_d \leq a_0p$, where $a_i \in \mathbb{Z}$. Then $g_F(p)$ counts the number of integer points in the p^{th} dilate of a polyhedron.

Example 2. If $F(c_1, c_2, p)$ is $2c_1 + 2c_2 \leq p$, then the set of solutions $(c_1, c_2) \in \mathbb{N}^2$ lies in the triangle with vertices $(0, 0)$, $(0, p/2)$, $(p/2, 0)$, and

$$\begin{aligned} g_F(p) &= \frac{1}{2}\left(\left\lfloor \frac{p}{2} \right\rfloor + 1\right)\left(\left\lfloor \frac{p}{2} \right\rfloor + 2\right) \\ &= \begin{cases} \frac{1}{8}p^2 + \frac{3}{4}p + 1 & \text{if } p \text{ is even,} \\ \frac{1}{8}p^2 + \frac{1}{2}p + \frac{3}{8} & \text{if } p \text{ is odd.} \end{cases} \end{aligned}$$

The nice form of this function is also not a coincidence. For this particular type of Presburger formula (dilates of a polyhedron), Ehrhart proved [21] that the counting functions are *quasi-polynomials*:

Definition 5. *A* quasi-polynomial *(over $\mathbb{Q}$) is a function $g : \mathbb{N}^n \to \mathbb{Q}$ such that there exists an n-dimensional lattice $\Lambda \subseteq \mathbb{Z}^n$ together with polynomials $q_{\bar{\lambda}}(\boldsymbol{p}) \in \mathbb{Q}[\boldsymbol{p}]$, one for each $\bar{\lambda} \in \mathbb{Z}^n/\Lambda$, such that*

$$g(\boldsymbol{p}) = q_{\bar{\lambda}}(\boldsymbol{p}), \text{ for } \boldsymbol{p} \in \bar{\lambda}.$$

In Example 2, we can take the lattice $\Lambda = 2\mathbb{Z}$ and each coset (the evens and the odds) has its associated polynomial. We need something slightly more general to account for all Presburger counting functions:

Definition 6. *A* piecewise quasi-polynomial *is a function $g : \mathbb{N}^n \to \mathbb{Q}$ such that there exists a finite partition $\bigcup_i (P_i \cap \mathbb{N}^n)$ of $\mathbb{N}^n$ with P_i polyhedra (which may not all be full-dimensional) and there exist quasi-polynomials g_i such that*

$$g(\boldsymbol{p}) = g_i(\boldsymbol{p}) \text{ for } \boldsymbol{p} \in P_i \cap \mathbb{N}^n.$$

One last thing that is not a coincidence: For the triangle in Example 2, we can compute

$$\begin{aligned} \sum_{p \in \mathbb{N}} g_F(p)x^p &= 1 + x + 3x^2 + 3x^3 + 6x^4 + \cdots \\ &= \frac{1}{(1-x)(1-x^2)^2}, \end{aligned}$$

a rational generating function! The following theorem says that these ideas are – almost – equivalent.

Theorem 2. *Given a function $g : \mathbb{N}^n \to \mathbb{Q}$ and the following three possible properties:*

A. g is a Presburger counting function,
B. g is a piecewise quasi-polynomial, and
C. $\sum_{\boldsymbol{p}\in\mathbb{N}^n} g(\boldsymbol{p})\boldsymbol{x}^{\boldsymbol{p}}$ is a rational generating function,

we have the implications

$$A \Rightarrow B \Leftrightarrow C.$$

Remark 1. Proving Theorem 2 will give us much of Theorem 1, using the following idea. A set $S \subseteq \mathbb{Z}^d$ corresponds exactly to its characteristic function

$$\chi_S(\mathbf{u}) = \begin{cases} 1 & \text{if } \mathbf{u} \in S, \\ 0 & \text{if } \mathbf{u} \notin S. \end{cases}$$

If S is a Presburger set defined by $F(\mathbf{u})$, then

$$\chi_S(\mathbf{u}) = \#\{c \in \mathbb{N} : \ F(\mathbf{u}) \text{ and } c = 0\}$$

is a Presburger counting function.

In light of Theorem 1, we might wonder if there is a sense in which $B \Rightarrow A$. Of course we would have to restrict g, for example requiring that its range be in $\mathbb{N}$ (Theorem 1 essentially restricts the range of g to $\{0, 1\}$, as it must be a characteristic function). The implication still does not hold, however. For example, suppose the polynomial

$$g(s,t) = (t - s^2)^2$$

were a Presburger counting function given by a Presburger formula $F(\boldsymbol{c}, s, t)$, that is,

$$g(s,t) = \#\{\boldsymbol{c} \in \mathbb{N}^d : \ F(\boldsymbol{c}, s, t)\}.$$

Then the set

$$\begin{aligned} \big\{(s,t) \in \mathbb{N}^2 : \ \nexists \boldsymbol{c}\ F(\boldsymbol{c}, s, t)\big\} &= \{(s,t) \in \mathbb{N}^2 : \ g(s,t) = 0\} \\ &= \{(s, s^2) : \ s \in \mathbb{N}\} \end{aligned}$$

would be a Presburger set. This is not the case, however, as it does not satisfy Property 2 in Theorem 1. If the parameter is univariate, however, the following proposition shows that we do have the implication $B \Rightarrow A$.

Proposition 1. *Given a function $g : \mathbb{N} \to \mathbb{Q}$, if g is a piecewise quasi-polynomial whose range is in $\mathbb{N}$, then g is a Presburger counting function.*

In Section 4, we prove Theorems 1 and 2 (the proof of Proposition 1 appears in the full version of this paper). In Section 2, we survey related work. In Section 3, we present the primary tools we need for the proofs. In the full version of this paper, we also turn to computational questions; we survey known results, but restate them in terms of Presburger arithmetic.

2 Related Work

Presburger arithmetic is a classical first order theory of logic, proven decidable by Presburger [35]. Various upper and lower bounds on the complexity of decision algorithms for the general theory have occupied the theoretical computer science community, see [8,17,22,24,26,33].

A finite automata approach to Presburger arithmetic was pioneered in [12,15], and continues to be an active area of research (see, for example, [10,16,30,47]). This approach is quite different from the present paper's, but it can attack similar questions: for example, see [34] for results on counting solutions to Presburger formulas (non-parametrically).

The importance of understanding Presburger Arithmetic is highlighted by the fact that many problems in computer science and mathematics can be phrased in this language: for example, integer programming [31,40], geometry of numbers [13,29], Gröbner bases and algebraic integer programming [43,45], neighborhood complexes and test sets [38,44], the Frobenius problem [37], Ehrhart theory [7,21], monomial ideals [32], and toric varieties [23]. Several of the above references analyze the computational complexity of their specific problem. In most of the above references, the connection to Presburger arithmetic is only implicit.

The algorithmic complexity of specific rational generating function problems has been addressed in, for example, [1,5,9,20,27,28]. Several of these results are summarized in the full version of this current paper.

Connections between subclasses of Presburger arithmetic and generating functions are made explicit in [3,4,5]. Connections between rational generating functions and quasi-polynomials have been made in [21,41,42], and the algorithmic complexity of their relationship was examined in [46]. Counting solutions to Presburger formulas has been examined in [36], though the exact scope of the results is not made explicit, and rational generating functions are not used. Similar counting algorithms appear in [14], and [18] proves that the counting functions for a special class of Presburger formuals (those whose parameters $\boldsymbol{p}$ only appear in terms $c_i \leq p_i$) are piecewise quasi-polynomials. This current paper is the first to state and prove a general connection between Presburger arithmetic, quasi-polynomials, and rational generating functions.

Theorem 1 was originally proved in the author's thesis [48]; in this paper, it is put into context as a consequence of the more general Theorem 2. A simpler geometric characterization of Presburger sets (equivalent to Property 2 of Theorem 1) was given in [25]: they are the *semi-linear* sets, those sets that can be written as a finite union of sets of the form $S = \{\boldsymbol{a}_0 + \sum_{i=1}^{k} n_i \boldsymbol{a}_i : \ n_i \in \mathbb{N}\}$, where $\boldsymbol{a}_i \in \mathbb{N}^d$. Furthermore, if one takes these S to be disjoint and requires the $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ to be linearly independent, for each S (as [25] implicitly prove can be done, made explicit in [18] as *semi-simple* sets), then each S can be encoded with the rational generating function

$$\frac{\boldsymbol{x}^{\boldsymbol{a}_0}}{(1-\boldsymbol{x}_1^{\boldsymbol{a}_1})\cdots(1-\boldsymbol{x}_k^{\boldsymbol{a}_k})}$$

and we obtain a slightly different version of 2 ⇒ 3 in Theorem 1. There seems to be no previous result analogous to 3 ⇒ 2.

3 Primary Background Theorems

Here we detail several tools we will use. The first tool we need is a way to simplify Presburger formulas. As originally proved [35] by Presburger (see [33] for a nice exposition), we can completely eliminate the quantifiers if we are allowed to also use modular arithmetic.

Definition 7. *An* extended Presburger formula *is a Boolean formula with variables in $\mathbb{N}$ expressible in the elementary language of Presburger Arithmetic extended by the* $\bmod k$ *operations, for constants $k > 1$.*

Theorem 3. *Given a formula $F(\mathbf{u})$ in extended Presburger arithmetic (and hence any formula in Presburger arithmetic), there exists an equivalent* quantifier free *formula $G(\mathbf{u})$ such that*

$$\{\mathbf{u} \in \mathbb{N}^d : \ F(\mathbf{u})\} = \{\mathbf{u} \in \mathbb{N}^d : \ G(\mathbf{u})\}.$$

For instance, the set from Example 1 can be written as ($u > 1$ and $u \bmod 2 = 1$).

Next, we give two theorems that tie in generating functions. The first gives us a way to convert from a specific type of Presburger set to a generating function.

Theorem 4. *Given a point $\lambda \in \mathbb{Z}^d$, a lattice $\Lambda \subseteq \mathbb{Z}^d$, and a rational polyhedron $P \subseteq \mathbb{R}^d_{\geq 0}$, $f\big(P \cap (\lambda + \Lambda); \boldsymbol{x}\big)$ (as given in Definition 2) is a rational generating function.*

The first step to proving this is to use Brion's Theorem [11], which says that the generating function can be decomposed into functions of the form $f\big(K \cap (\lambda + \Lambda); \mathbf{x}\big)$, where K is a cone. Then, one can notice that integer points in cones have a natural structure that can be encoded as geometric series.

Example 3. Let $K \subseteq \mathbb{R}^2$ be the cone with vertex at the origin and extreme rays $\mathbf{u} = (1, 0)$ and $\boldsymbol{v} = (1, 2)$. Using the fact that the lattice $(u\mathbb{Z} + v\mathbb{Z})$ has index 2 in $\mathbb{Z}^2$, with coset representatives $(0, 0)$ and $(1, 1)$, every integer point in K can be written as either $(0, 0) + \lambda_1 \mathbf{u} + \lambda_2 \boldsymbol{v}$ or $(1, 1) + \lambda_1 \mathbf{u} + \lambda_2 \boldsymbol{v}$, where $\lambda_1, \lambda_2 \in \mathbb{N}$. Therefore

$$\begin{aligned} f(K \cap \mathbb{Z}^2; \mathbf{x}) &= (\mathbf{x}^{(0,0)} + \mathbf{x}^{(1,1)})(1 + \mathbf{x}^{\mathbf{u}} + \mathbf{x}^{2\mathbf{u}} + \cdots)(1 + \mathbf{x}^{\boldsymbol{v}} + \mathbf{x}^{2\boldsymbol{v}} + \cdots) \\ &= \frac{\mathbf{x}^{(0,0)} + \mathbf{x}^{(1,1)}}{(1 - \mathbf{x}^{\mathbf{u}})(1 - \mathbf{x}^{\boldsymbol{v}})}. \end{aligned}$$

See [2, Chapter VIII], for example, for more details.

Next, we would like to be able to perform substitutions on the variables in a rational generating function and still retain a rational generating function; particularly, we would like to substitute in 1's for several of the variables.

Theorem 5. *Given a rational generating function $f(\boldsymbol{x})$, then*

$$g(\boldsymbol{z}) = f(\boldsymbol{z}^{\boldsymbol{l}_1}, \boldsymbol{z}^{\boldsymbol{l}_2}, \dots, \boldsymbol{z}^{\boldsymbol{l}_d}),$$

with $\boldsymbol{l}_i \in \mathbb{N}^k$, is also a rational generating function, assuming the substituted values do not lie entirely in the poles of f. In particular, substituting in $x_i = \boldsymbol{z}^{\boldsymbol{0}} = 1$ yields a rational function, if $\mathbf{1}$ is not a pole of f.

The proof is immediate: if substituting in $x_i = \boldsymbol{z}^{\boldsymbol{l}_i}$ would make any of the binomials in the denominator of f zero (when f is written in the form from Definition 3), then that binomial must be a factor of the numerator (or else such $\mathbf{z}^{\boldsymbol{l}_i}$ would lie entirely in the poles of f); therefore, substituting in $x_i = \boldsymbol{z}^{\boldsymbol{l}_i}$ yields a new rational generating function.

Finally, we need a connection between Presburger formulas and quasi-polynomials. This is given by Sturmfels [42]:

Definition 8. *Given $\boldsymbol{a}_1, \dots, \boldsymbol{a}_d \in \mathbb{N}^n$, the* vector partition function $g : \mathbb{N}^n \to \mathbb{N}$ *is defined by*

$$g(\boldsymbol{p}) = \#\{(\lambda_1, \dots, \lambda_d) \in \mathbb{N}^d : \ \boldsymbol{p} = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_d \boldsymbol{a}_d\},$$

that is, the number of ways to partition the vector $\boldsymbol{p}$ into parts taken from $\{\boldsymbol{a}_i\}$.

Theorem 6. *Any vector partition function is a piecewise quasi-polynomial.*

See [6] for a self-contained explanation utilizing the partial fraction expansion of the generating function

$$\sum_{\mathbf{p} \in \mathbb{N}^n} g(\mathbf{p}) \mathbf{x}^{\mathbf{p}} = \frac{1}{(1 - \mathbf{x}^{\boldsymbol{a}_1}) \cdots (1 - \mathbf{x}^{\boldsymbol{a}_d})};$$

this equality can be obtained by rewriting the rational function as a product of infinite geometric series:

$$(1 + \mathbf{x}^{\boldsymbol{a}_1} + \mathbf{x}^{2\boldsymbol{a}_1} + \cdots) \cdots (1 + \mathbf{x}^{\boldsymbol{a}_d} + \mathbf{x}^{2\boldsymbol{a}_d} + \cdots).$$

4 Proofs

4.1 Proof of Theorem 2

A $\Rightarrow$ C.

Given a Presburger counting function, $g(\boldsymbol{p}) = \#\{\boldsymbol{c} \in \mathbb{N}^d : \ F(\boldsymbol{c}, \boldsymbol{p})\}$, we first apply Presburger Elimination (Theorem 3) to F to obtain a quantifier free formula, $G(\boldsymbol{c}, \boldsymbol{p})$, in extended Presburger arithmetic such that $g(\boldsymbol{p}) = \#\{\boldsymbol{c} \in \mathbb{N}^d : \ G(\boldsymbol{c}, \boldsymbol{p})\}$. Integers which satisfy a statement of the form

$$a_1 p_1 + \cdots + a_n p_n + a_{n+1} c_1 + \cdots + a_{n+d} c_d \equiv a_0 \pmod{m}$$

are exactly sets $\lambda + \varLambda$, where $\lambda \in \mathbb{Z}^{n+d}$ and $\varLambda$ is a lattice in $\mathbb{Z}^{n+d}$. Since $G(\boldsymbol{c}, \boldsymbol{p})$ is a Boolean combination of linear inequalities and these linear congruences, we may write the set, S, of points $(\boldsymbol{c}, \boldsymbol{p})$ which satisfy $G(\boldsymbol{c}, \boldsymbol{p})$ as a *disjoint* union

$$S = \bigcup_{i=1}^{k} P_i \cap (\lambda_i + \varLambda_i),$$

where, for $1 \le i \le k$, $P_i \subseteq \mathbb{R}^{n+d}_{\ge 0}$ is a polyhedron, $\varLambda_i$ is a sublattice of $\mathbb{Z}^{n+d}$, and λ_i is in $\mathbb{Z}^{n+d}$. (To see this, convert the formula into disjunctive normal form; each conjunction will be of this form $P_i \cap (\lambda_i + \varLambda_i)$; these sets may overlap, but their overlap will also be of this form.)

Let $S_i = P_i \cap (\lambda_i + \varLambda_i)$. By Theorem 4, we know we can write $f(S_i; \mathbf{y}, \mathbf{x})$ as a rational generating function, and so

$$f(S; \mathbf{y}, \mathbf{x}) = \sum_i f(S_i; \mathbf{y}, \mathbf{x}) = \sum_{(\boldsymbol{c},\boldsymbol{p}):\ G(\boldsymbol{c},\boldsymbol{p})} \mathbf{y}^{\boldsymbol{c}} \mathbf{x}^{\boldsymbol{p}}$$

can be written as a rational generating function. Finally, we substitute $\mathbf{y} = (1, 1, \dots, 1)$, using Theorem 5, to obtain the rational generating function

$$\sum_{\boldsymbol{p}} \#\{\boldsymbol{c} \in \mathbb{N}^d :\ G(\boldsymbol{c}, \boldsymbol{p})\} \mathbf{x}^{\boldsymbol{p}} = \sum_{\boldsymbol{p}} g(\boldsymbol{p}) \mathbf{x}^{\boldsymbol{p}}.$$

C $\Rightarrow$ **B**.

It suffices to prove this for functions g such that $\sum_{\boldsymbol{p}} g(\boldsymbol{p}) \mathbf{x}^{\boldsymbol{p}}$ is a rational generating function of the form

$$\frac{\mathbf{x}^{\boldsymbol{q}}}{(1 - \mathbf{x}^{\boldsymbol{a}_1})(1 - \mathbf{x}^{\boldsymbol{a}_2}) \cdots (1 - \mathbf{x}^{\boldsymbol{a}_k})},$$

where $\boldsymbol{q} \in \mathbb{N}^n, \boldsymbol{a}_i \in \mathbb{N}^n \setminus \{0\}$, because the property of being a piecewise quasi-polynomial is preserved under linear combinations. Furthermore, we may take $\boldsymbol{q} = (0, 0, \dots, 0)$, because multiplying by $\mathbf{x}^{\boldsymbol{q}}$ only shifts the domain of the function g. Expanding this rational generating function as a product of infinite geometric series,

$$\sum_{\boldsymbol{p}} g(\boldsymbol{p}) \mathbf{x}^{\boldsymbol{p}} = (1 + \mathbf{x}^{\boldsymbol{a}_1} + \mathbf{x}^{2\boldsymbol{a}_1} + \cdots) \cdots (1 + \mathbf{x}^{\boldsymbol{a}_k} + \mathbf{x}^{2\boldsymbol{a}_k} + \cdots),$$

and we see that

$$g(\boldsymbol{p}) = \#\{(\lambda_1, \dots, \lambda_k) \in \mathbb{N}^k :\ \boldsymbol{p} = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_k \boldsymbol{a}_k\}.$$

This is exactly a vector partition function, which Theorem 6 tells us is a piecewise quasi-polynomial.

B $\Rightarrow$ **C**.

Any piecewise quasi-polynomial can be written as a linear combination of functions of the form

$$g(\boldsymbol{p}) = \begin{cases} \boldsymbol{p}^{\boldsymbol{a}} & \text{if } \boldsymbol{p} \in P \cap (\lambda + \Lambda), \\ 0 & \text{otherwise,} \end{cases}$$

where $\boldsymbol{a} \in \mathbb{N}^n$, $P \subseteq \mathbb{R}^n_{\geq 0}$ is a polyhedron, $\lambda \in \mathbb{Z}^n$, and Λ is a sublattice of $\mathbb{Z}^n$. Since linear combinations of rational generating functions are rational generating functions, it suffices to prove it for such a g. Let c_{ij}, for $1 \leq i \leq n$ and $1 \leq j \leq a_i$, be variables, and define the polyhedron

$$Q = \{(\boldsymbol{p}, \boldsymbol{c}) \in \mathbb{N}^{n+a_1+\cdots+a_n} : \\ \boldsymbol{p} \in P \text{ and } 1 \leq c_{ij} \leq p_i \text{ for all } c_{ij}\}.$$

This Q is defined so that $\#\{\boldsymbol{c} :\ (\boldsymbol{p}, \boldsymbol{c}) \in Q\}$ is $p_1^{a_1} \cdots p_n^{a_n} = \mathbf{p}^{\boldsymbol{a}}$ for $\boldsymbol{p} \in P$ (and 0 otherwise). Using Theorem 4, we can find the generating function for the set $Q \cap (\lambda + \Lambda)$ as a rational generating function. Substituting $\boldsymbol{c} = (1, 1, \ldots, 1)$, using Theorem 5, gives us $\sum_{\boldsymbol{p}} g(\boldsymbol{p})\mathbf{x}^{\boldsymbol{p}}$ as a rational generating function.

4.2 Proof of Theorem 1

Given a set $S \subseteq \mathbb{Z}^d$, define the characteristic function, $\chi_S : \mathbb{N}^d \to \{0, 1\}$, as in Remark 1. Define a new property:

$2'$. χ_S is a piecewise quasi-polynomial.

Translating Theorem 2 into properties of S and χ_S, we have

$$1 \Rightarrow (2' \Leftrightarrow 3).$$

So we need to prove $2 \Rightarrow 1$ and $2' \Rightarrow 2$.

$\mathbf{2} \Rightarrow \mathbf{1}$.

This is straightforward: the property of being an element of $\lambda + \Lambda$ can be written using linear congruences and existential quantifiers, and the property of being an element of P can be written as a set of linear inequalities.

$\mathbf{2'} \Rightarrow \mathbf{2}$.

Since χ_S is a piecewise quasi-polynomial, it is constituted from associated polynomials. Let us examine such a polynomial $q(\mathbf{p})$ that agrees with χ_S on some $P \cap (\lambda + \Lambda)$, where $P \subseteq \mathbb{R}^n_{\geq 0}$ is a polyhedron, $\lambda \in \mathbb{Z}^n$, and Λ a sublattice of $\mathbb{Z}^n$. It suffices to prove that 2 holds for $S \cap P \cap (\lambda + \Lambda)$, since S is the disjoint union of such pieces.

Ideally, we would like to argue that, since q only takes on the values 0 and 1, the polynomial q must be constant on $P \cap (\lambda + \Lambda)$, at least if P is unbounded. This is not quite true; for example, if

$$P = \{(x, y) \in \mathbb{R}^2 :\ x \geq 0 \text{ and } 0 \leq y \leq 1\},$$

then the polynomial $q(x, y) = y$ is 1 for $y = 1$ and 0 for $y = 0$.

What we can say is that q must be constant on any infinite ray contained in $P \cap (\lambda + \Lambda)$: if we parametrize the ray by $\mathbf{x}(t) = (x_1(t), \cdots, x_n(t))$, then $q(\mathbf{x}(t))$ is a *univariate* polynomial that is either 0 or 1 at an infinite number of points, and so must be constant. Inductively, we can similarly show that q must be constant on any cone contained in P.

Let K be the cone with vertex at the origin

$$K = \{\mathbf{y} \in \mathbb{R}^n : \ \mathbf{y} + P \subseteq P\}.$$

Then K is the largest cone such that the cones $\mathbf{x} + K$ are contained in P, for all $\mathbf{x} \in P$; K is often called the *recession cone* or *characteristic cone* of P (see Section 8.2 of [39]), and the polyhedron P can be decomposed into a Minkowski sum $K + Q$, where Q is a *bounded* polyhedron. We can write $P \cap (\lambda + \Lambda)$ as a finite union (possibly with overlap) of sets of the form

$$Q_j = (v_j + K) \cap (\lambda + \Lambda),$$

for some v_j, and on each of these pieces q must be constant. If q is the constant 1 on Q_j, then Q_j is contained in S, and if q is the constant 0, then none of Q_j is in S. Since S is a finite union of the appropriate Q_j, S has the form needed for Property 2.

5 Acknowledgements

My thanks to the referees, particularly for pointers to relevant related works.

References

1. Barvinok, A.: A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. Math. Oper. Res. **19**(4) (1994) 769–779
2. Barvinok, A.: A Course in Convexity. Volume 54 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI (2002)
3. Barvinok, A.: The complexity of generating functions for integer points in polyhedra and beyond. In: International Congress of Mathematicians. Vol. III. Eur. Math. Soc., Zürich (2006) 763–787
4. Barvinok, A., Pommersheim, J.: An algorithmic theory of lattice points in polyhedra. In: New Perspectives in Algebraic Combinatorics (Berkeley, CA, 1996–97). Volume 38 of Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge (1999) 91–147
5. Barvinok, A., Woods, K.: Short rational generating functions for lattice point problems. J. Amer. Math. Soc. **16**(4) (2003) 957–979 (electronic)
6. Beck, M.: The partial-fractions method for counting solutions to integral linear systems. Discrete Comput. Geom. **32**(4) (2004) 437–446
7. Beck, M., Robins, S.: Computing the continuous discretely. Undergraduate Texts in Mathematics. Springer, New York (2007) Integer-point enumeration in polyhedra.

8. Berman, L.: The complexity of logical theories. Theoret. Comput. Sci. **11**(1) (1980) 57, 71–77 With an introduction “On space, time and alternation”.
9. Blanco, V., García-Sánchez, P.A., Puerto, J.: Counting numerical semigroups with short generating functions. Internat. J. Algebra Comput. **21**(7) (2011) 1217–1235
10. Boudet, A., Comon, H.: Diophantine equations, Presburger arithmetic and finite automata. In: Trees in algebra and programming—CAAP ’96 (Linköping, 1996). Volume 1059 of Lecture Notes in Comput. Sci. Springer, Berlin (1996) 30–43
11. Brion, M.: Points entiers dans les polyèdres convexes. Ann. Sci. École Norm. Sup. **4** (1988) 653–663
12. Büchi, J.R.: Weak second-order arithmetic and finite automata. Z. Math. Logik Grundlagen Math. **6** (1960) 66–92
13. Cassels, J.W.S.: An introduction to the geometry of numbers. Classics in Mathematics. Springer-Verlag, Berlin (1997) Corrected reprint of the 1971 edition.
14. Clauss, P., Loechner, V.: Parametric analysis of polyhedral iteration spaces. Journal of VLSI Signal Processing **19**(2) (July 1998) 179–194
15. Cobham, A.: On the base-dependence of sets of numbers recognizable by finite automata. Math. Systems Theory **3** (1969) 186–192
16. Comon, H., Jurski, Y.: Multiple counters automata, safety analysis and Presburger arithmetic. In: Computer aided verification (Vancouver, BC, 1998). Volume 1427 of Lecture Notes in Comput. Sci. Springer, Berlin (1998) 268–279
17. Cooper, D.: Theorem proving in arithmetic without multiplication. Machine Intelligence **7** (1972) 91–99
18. D’Alessandro, F., Intrigila, B., Varricchio, S.: On some counting problems for semi-linear sets. CoRR **abs/0907.3005** (2009)
19. Davis, M.: Hilbert’s tenth problem is unsolvable. Amer. Math. Monthly **80** (1973) 233–269
20. De Loera, J., Haws, D., Hemmecke, R., Huggins, P., Sturmfels, B., Yoshida, R.: Short rational functions for toric algebra. to appear in *Journal of Symbolic Computation* (2004)
21. Ehrhart, E.: Sur les polyèdres rationnels homothétiques à n dimensions. C. R. Acad. Sci. Paris **254** (1962) 616–618
22. Fischer, M., Rabin, M.: Super-exponential complexity of Presburger arithmetic. In: Complexity of computation (Proc. SIAM-AMS Sympos., New York, 1973). Amer. Math. Soc., Providence, R.I. (1974) 27–41. SIAM–AMS Proc., Vol. VII
23. Fulton, W.: Introduction to Toric Varieties. Volume 131 of Annals of Mathematics Studies. Princeton University Press, Princeton, NJ (1993)
24. Fürer, M.: The complexity of Presburger arithmetic with bounded quantifier alternation depth. Theoret. Comput. Sci. **18**(1) (1982) 105–111
25. Ginsburg, S., Spanier, E.: Semigroups, Presburger formulas and languages. Pacific Journal of Mathematics **16**(2) (1966) 285–296
26. Grädel, E.: Subclasses of Presburger arithmetic and the polynomial-time hierarchy. Theoret. Comput. Sci. **56**(3) (1988) 289–301
27. Guo, A., Miller, E.: Lattice point methods for combinatorial games. Adv. in Appl. Math. **46**(1-4) (2011) 363–378
28. Hoşten, S., Sturmfels, B.: Computing the integer programming gap. to appear in *Combinatorics* (2004)
29. Kannan, R.: Test sets for integer programs, ∀∃ sentences. In: Polyhedral combinatorics (Morristown, NJ, 1989). Volume 1 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci. Amer. Math. Soc., Providence, RI (1990) 39–47
30. Klaedtke, F.: Bounds on the automata size for Presburger arithmetic. ACM Trans. Comput. Log. **9**(2) (2008) Art. 11, 34

31. Lenstra, Jr., H.: Integer programming with a fixed number of variables. Math. Oper. Res. **8**(4) (1983) 538–548
32. Miller, E., Sturmfels, B.: Combinatorial commutative algebra. Volume 227 of Graduate Texts in Mathematics. Springer-Verlag, New York (2005)
33. Oppen, D.: A superexponential upper bound on the complexity of Presburger arithmetic. J. Comput. System Sci. **16**(3) (1978) 323–332
34. Parker, E., Chatterjee, S.: An automata-theoretic algorithm for counting solutions to presburger formulas. In: Compiler Construction, Springer (2004) 104–119
35. Presburger, M.: On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation. Hist. Philos. Logic **12**(2) (1991) 225–233 Translated from the German and with commentaries by Dale Jacquette.
36. Pugh, W.: Counting solutions to presburger formulas: how and why. SIGPLAN Not. **29**(6) (June 1994) 121–134
37. Ramírez Alfonsín, J.L.: The Diophantine Frobenius problem. Volume 30 of Oxford Lecture Series in Mathematics and its Applications. Oxford University Press, Oxford (2005)
38. Scarf, H.: Test sets for integer programs. Math. Programming **79**(1-3, Ser. B) (1997) 355–368
39. Schrijver, A.: Theory of Linear and Integer Programming. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Ltd., Chichester (1986)
40. Schrijver, A.: Combinatorial optimization. Polyhedra and efficiency. Volume 24 of Algorithms and Combinatorics. Springer-Verlag, Berlin (2003)
41. Stanley, R.P.: Decompositions of rational convex polytopes. Ann. Discrete Math. **6** (1980) 333–342 Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978).
42. Sturmfels, B.: On vector partition functions. J. Combin. Theory Ser. A **72**(2) (1995) 302–309
43. Sturmfels, B.: Gröbner Bases and Convex Polytopes. Volume 8 of University Lecture Series. American Mathematical Society, Providence, RI (1996)
44. Thomas, R.: A geometric Buchberger algorithm for integer programming. Math. Oper. Res. **20**(4) (1995) 864–884
45. Thomas, R.: The structure of group relaxations. to appear in Handbook of Discrete Optimization (eds: K. Aardal, G. Nemhauser, R. Weismantel) (2003)
46. Verdoolaege, S., Woods, K.: Counting with rational generating functions. J. Symbolic Comput. **43**(2) (2008) 75–91
47. Wolper, P., Boigelot, B.: An automata-theoretic approach to Presburger arithmetic constraints. In: Static Analysis, 2nd Intl. Symp. Volume 983 of Lecture Notes in Comput. Sci., Springer (1995) 21–32
48. Woods, K.: Rational Generating Functions and Lattice Point Sets. PhD thesis, University of Michigan (2004)