The unreasonable ubiquitousness of quasi-polynomials[†]

Kevin Woods

Oberlin College, Oberlin, Ohio, USA

Abstract. A function g, with domain the natural numbers, is a quasi-polynomial if there exists a period m and polynomials $p_0, p_1, \dots, p_{m-1}$ such that $g(t) = p_i(t)$ for $t \equiv i \bmod m$. Quasi-polynomials classically – and "reasonably" – appear in Ehrhart theory and in other contexts where one examines a family of polyhedra, parametrized by a variable t, and defined by linear inequalities of the form $a_1x_1 + \cdots + a_dx_d \leq b(t)$.

Recent results of Chen, Li, Sam; Calegari, Walker; and Roune, Woods show a quasi-polynomial structure in several problems where the a_i are also allowed to vary with t. We discuss these "unreasonable" results and conjecture a general class of sets that exhibit various (eventual) quasi-polynomial behaviors: sets S_t that are defined with quantifiers ($\forall$, $\exists$), boolean operations (and, or, not), and statements of the form $a_1(t)x_1 + \cdots + a_d(t)x_d \leq b(t)$, where $a_i(t)$ and $b(t)$ are polynomials in t. These sets are a generalization of sets defined in the Presburger arithmetic. We prove several relationships between our conjectures, and we prove several special cases of the conjectures.

Résumé. Une fonction g, ayant les entiers naturels pour domaine, est un quasi-polynôme si il existe un entier m et des ploynômes $p_0, p_1, \dots, p_{m-1}$ tels que $g(t) = p_i(t)$ pour $t \equiv i \bmod m$. Les quasi-polynômes apparaissent dans la théorie d'Erhart, ainsi que dans d'autres contextes où l'on s'intéresse à des familles de polyhèdres paramétrisées par une variable t, et définies par des inégalités linéaires de la forme $a_1x_1 + \cdots + a_dx_d \leq b(t)$.

Des résultats récents de Chen, Li, Sam; Calegari, Walker; et Roune, Woods exhibent une structure de quasi-polynôme dans plusieurs problèmes où les a_i peuvent aussi varier en fonction de t. Nous nous intéressons à ces cas "non-raisonnables" et nous conjecturons l'existence d'une classe générale d'ensembles qui exhibent divers (possiblement) comportement de type quasi-polynômes : il s'agit des ensembles S_t qui sont définis en termes de quantifieurs ($\forall$, $\exists$), d'opérateurs booléens (conjonction, disjonction, négation), et d'énoncés de la forme $a_1(t)x_1 + \cdots + a_d(t)x_d \leq b(t)$, où $a_i(t)$ et $b(t)$ sont des polynômes en la variable t. Ces ensembles généralisent des ensembles définis dans l'arithmétique de Presburger. Nous démontrons plusieurs relations entre nos conjectures, ainsi que plusieurs cas spéciaux de ces mêmes conjectures.

Keywords: Quasi-polynomials, Ehrhart theory, Presburger arithmetic, rational generating functions

[†]With apologies to Wigner (1960) and Hamming (1980). A full version of this paper is available at `http://www.oberlin.edu/faculty/kwoods/papers.html`.

1 Reasonable Ubiquitousness

In this section, we survey classical appearances of quasi-polynomials (though Section 1.3 might be new even to readers already familiar with Ehrhart theory). In Section 2, we survey some recent results where the appearance of quasi-polynomials is more surprising. In Section 3, we make several conjectures generalizing these "unreasonable" results. We state theorems relating these conjectures and state theorems proving certain cases. In particular, we conjecture that any family of sets S_t – defined with quantifiers ($\forall$, $\exists$), boolean operations (and, or, not), and statements of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$ (where $\mathbf{a}(t) \in \mathbb{Q}[t]^d, b(t) \in \mathbb{Q}[t]$, and $\cdot$ is the standard dot product) – exhibits eventual quasi-polynomial behavior, as well as rational generating function behavior. Of course, reasonable people may disagree on what is unreasonable; the title is a play on "The unreasonable effectiveness of mathematics in the natural sciences" Wigner (1960).

For reasons of space, proofs are omitted here; they are in the full version of this paper, available on the author's website. We use bold letters such as $\mathbf{x}$ to indicate multi-dimensional vectors.

Definition 1 *A function $g : \mathbb{N} \to \mathbb{Q}$ is a* quasi-polynomial *if there exists a period m and polynomials $p_0, p_1, \ldots, p_{m-1} \in \mathbb{Q}[t]$ such that*

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

Example 2

$$g(t) = \left\lfloor \frac{t+1}{2} \right\rfloor = \begin{cases} \frac{t}{2} & \text{if } t \text{ even,} \\ \frac{t+1}{2} & \text{if } t \text{ odd,} \end{cases}$$

is a quasi-polynomial with period 2.

This example makes it clear that the ubiquitousness of quasi-polynomials shouldn't be too surprising: anywhere there are floor functions, quasi-polynomials are likely to appear. We will generally be concerned with *integer-valued* quasi-polynomials, those quasi-polynomials whose range lies in $\mathbb{Z}$. Note that Example 2 demonstrates that such quasi-polynomials may still require rational coefficients.

1.1 Ehrhart theory

Perhaps the most well-studied quasi-polynomials are the *Ehrhart quasi-polynomials*:

Theorem 3 (Ehrhart, 1962) *Suppose P is a polytope (bounded polyhedron) whose vertices have rational coordinates. Let $g(t)$ be the number of integer points in tP, the dilation of P by a factor of t. Then $g(t)$ is a quasi-polynomial, with period the smallest m such that mP has integer coordinates.*

Example 4 *Let P be the triangle with vertices $(0,0)$, $\left(\frac{1}{2}, 0\right)$, and $\left(\frac{1}{2}, \frac{1}{2}\right)$. Then*

$$g(t) = \#(tP \cap \mathbb{Z}^2) = \frac{\big(\lfloor t/2 \rfloor + 1\big)\big(\lfloor t/2 \rfloor + 2\big)}{2} = \begin{cases} (t+2)(t+4)/8 & \text{if } t \text{ even,} \\ (t+1)(t+3)/8 & \text{if } t \text{ odd,} \end{cases} \tag{1}$$

is a quasi-polynomial with period 2.

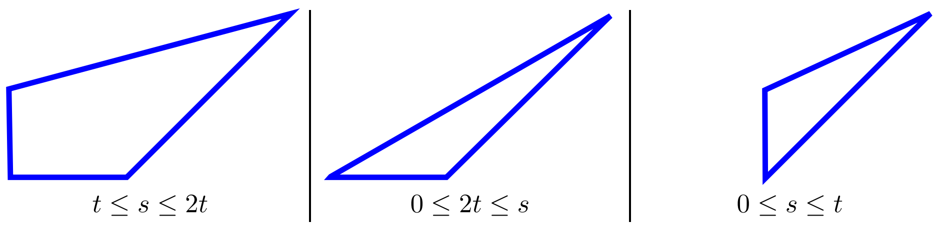

Fig. 1: Polyhedra defined in Example 5 for various $(s,t) \in \mathbb{N}^2$.

Writing tP from this example as

$$\{(x,y) \in \mathbb{R}^2 : \ 2x \le t, \ y - x \le 0, \ -y \le 0\}$$

suggests a way to generalize this result: for $\mathbf{t} \in \mathbb{N}^n$, let $S_{\mathbf{t}}$ be the set of integer points, $\mathbf{x} \in \mathbb{Z}^d$, in a polyhedron defined with linear inequalities of the form $\mathbf{a} \cdot \mathbf{x} \le b(\mathbf{t})$, where $\mathbf{a} \in \mathbb{Z}^d$ and $b(\mathbf{t})$ is a degree 1 polynomial in $\mathbf{t}$.

Example 5 *Let*

$$S_{s,t} = \big\{(x,y) \in \mathbb{Z}^2 : \ 2y - x \le 2t - s, \ x - y \le s - t, \ x, y \ge 0\big\}.$$

For a fixed (s,t), $S_{s,t}$ is the set of integer points in a polyhedron in $\mathbb{R}^2$. As (s,t) varies, the "constant" term of these inequalities change, but the coefficients of x and y do not; in other words, the normal vectors to the facets of the polyhedron do not change, but the facets move "in and out". In fact, they can move in and out so much that the combinatorial structure of the polyhedron changes. Figure 1 shows the combinatorial structure for different $(s,t) \in \mathbb{N}^2$. Using various methods, Beck (2004) and Verdoolaege and Woods (2008) compute that

$$g(s,t) = |S_{s,t}| = \begin{cases} \frac{s^2}{2} - \lfloor \frac{s}{2} \rfloor s + \frac{s}{2} + \lfloor \frac{s}{2} \rfloor^2 + \lfloor \frac{s}{2} \rfloor + 1 & \text{if } t \le s \le 2t, \\ st - \lfloor \frac{s}{2} \rfloor s - \frac{t^2}{2} + \frac{t}{2} + \lfloor \frac{s}{2} \rfloor^2 + \lfloor \frac{s}{2} \rfloor + 1 & \text{if } 0 \le 2t \le s, \\ \frac{t^2}{2} + \frac{3t}{2} + 1 & \text{if } 0 \le s \le t. \end{cases}$$

In this example, the function $g(s,t)$ is a quasi-polynomial (in this multivariate case, one must consider both s and t modulo some periods), at least *piecewise*. Sturmfels (1995) effectively proved this generalization of Ehrhart theory:

Theorem 6 *Let $S_{\mathbf{t}}$ be the set of integer points, $\mathbf{x} \in \mathbb{Z}^d$, in a polyhedron defined with linear inequalities $\mathbf{a} \cdot \mathbf{x} \le b(\mathbf{t})$, where $\mathbf{a} \in \mathbb{Z}^d$ and $b(\mathbf{t})$ is a degree 1 polynomial in $\mathbb{Z}[\mathbf{t}]$. Then $g(\mathbf{t}) = |S_{\mathbf{t}}|$ is a piecewise-defined quasi-polynomial, where the finite number of pieces are polyhedral regions of parameter space.*

Sections 2 and further will predominantly be concerned with *univariate* functions. Being a univariate piecewise quasi-polynomial $g : \mathbb{N} \to \mathbb{Q}$ is equivalent to *eventually* being a quasi-polynomial; that is, there exists a T such that for all $t \ge T$, $g(t)$ agrees with a quasi-polynomial.

1.2 Generating functions

Classic proofs of Ehrhart's Theorem (Theorem 3) use generating functions. To prove that a function $g(t)$ is a quasi-polynomial of period m, it suffices (see Section 4.4 of Stanley, 2012) to prove that the Hilbert series $\sum_{t\in\mathbb{N}} g(t)y^t$ can be written as a rational function of the form

$$\frac{p(y)}{(1-y^m)^d},$$

where $p(y)$ is a polynomial of degree less than md. For $g(t)=|tP|$ with P the triangle in Example 4, we can see that

$$\sum_{t\in\mathbb{N}} g(t)y^t = 1+y+3y^2+3y^3+6y^4+\cdots = \frac{1+y}{(1-y^2)^3}. \tag{2}$$

Indeed, these proofs of Ehrhart's Theorem start by considering the generating function $\sum_{t\in\mathbb{N},\mathbf{s}\in tP\cap\mathbb{Z}^d} \mathbf{x}^{\mathbf{s}}y^t$ (where $\mathbf{x}^{\mathbf{s}} = x_1^{s_1}\cdots x_d^{s_d}$) and substituting in $\mathbf{x}=(1,\ldots,1)$ to get the Hilbert series. For P in Example 4,

$$\begin{aligned}\sum_{t\in\mathbb{N},\mathbf{s}\in tP\cap\mathbb{Z}^d} \mathbf{x}^{\mathbf{s}}y^t &= 1+y+(1+x_1+x_1x_2)y^2+(1+x_1+x_1x_2)y^3+(1+\cdots+x_1^2x_2^2)y^4+\cdots\\ &= \frac{1+y}{(1-y^2)(1-x_1y^2)(1-x_1x_2y^2)},\end{aligned}$$

as can be checked by expanding as a product of infinite geometric series. Substituting $x_1=x_2=1$ yields the Hilbert series in Equation 2.

Definition 7 *We call any generating function or Hilbert series a* rational generating function *if it can be written in the form*

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

where p is a Laurent polynomial over $\mathbb{Q}$ and $\mathbf{b}_i\in\mathbb{Z}^d$ are lexicographically positive (first nonzero entry is positive), .

While we will generally be assuming that the generating functions are for subsets of $\mathbb{N}^d$, we need $\mathbf{b}_i$ to be lexicographically positive rather than simply in $\mathbb{N}^d\setminus\{0\}$ for examples like the following:

Example 8 *Let $S=\big\{(x,y)\in\mathbb{N}^2:\ x+y=1000\big\}$. While $y^{1000}+xy^{999}+\cdots+x^{1000}$ is a legitimate generating function, it makes more sense to write it as*

$$\frac{y^{1000}-x^{1001}y^{-1}}{1-xy^{-1}}.$$

If $\mathbf{b}$ is lexicographically negative, then

$$\frac{1}{1-\mathbf{x}^{\mathbf{b}}} = \frac{-\mathbf{x}^{-\mathbf{b}}}{1-\mathbf{x}^{-\mathbf{b}}}$$

with $-\mathbf{b}$ is lexicographically positive. Having $\mathbf{b}$ lexicographically positive guarantees that $1/(1-\mathbf{x}^{\mathbf{b}}) = 1+\mathbf{x}^{\mathbf{b}}+\mathbf{x}^{2\mathbf{b}}+\cdots$ is the Laurent series convergent in a neighborhood of $\mathbf{x}=(e^{-\varepsilon},e^{-\varepsilon^2},\ldots,e^{-\varepsilon^d})$ for sufficiently small ε.

In Section 3, we will use a different generating function: for *fixed* t, examine the generating function $\sum_{\mathbf{s}\in tP\cap\mathbb{Z}^d}\mathbf{x}^{\mathbf{s}}$. In the triangle from Example 4, this gives us

$$\left(1+x_1+x_1^2+\cdots+x_1^{\lfloor t/2\rfloor}\right)+\left(x_1+x_1^2+\cdot+x_1^{\lfloor t/2\rfloor}\right)x_2+\cdots+\left(x_1^{\lfloor t/2\rfloor}\right)x_2^{\lfloor t/2\rfloor}.$$

In general, powerful tools such as Brion's Theorem (Brion, 1988) help us compute a compact form for this generating function; see Verdoolaege and Woods (2008) for more details. In this example, we can verify directly, by expanding the fractions as products of geometric series, that

$$\sum_{\mathbf{s}\in tP\cap\mathbb{Z}^d}\mathbf{x}^{\mathbf{s}}=\frac{1}{(1-x_1)(1-x_1x_2)}-\frac{x_1^{\lfloor t/2\rfloor+1}}{(1-x_1)(1-x_2)}+\frac{x_1^{\lfloor t/2\rfloor+1}x_2^{\lfloor t/2\rfloor+2}}{(1-x_2)(1-x_1x_2)}. \tag{3}$$

Given this generating function, we can count the number of integer points in tP by substituting in $\mathbf{x}=(1,\ldots,1)$. Substituting $x_1=x_2=1$ into Equation 3, we see that $(1,1)$ is a pole of these fractions. Fortunately, getting a common denominator and applying L'Hôpital's rule to find the limit as x_1 and x_2 approach 1 will work, and it is evident that the differentiation involved in L'Hôpital's rule will yield a quasi-polynomial in t as the result; careful calculation will show that it matches Equation 1.

1.3 Presburger arithmetic

So far, our examples have been integer points in polyhedra. A key property of such sets is that they can be defined without quantifiers. However, even for sets defined with quantifiers, we end up with reasonable appearances of quasi-polynomials.

Definition 9 *A* Presburger formula *is a boolean formula with variables in $\mathbb{N}$ that can be written using quantifiers ($\exists,\forall$), boolean operations (and, or, not), and linear (in)equalities in the variables. We write a Presburger formula as $F(\mathbf{u})$ to indicate the the free variables $\mathbf{u}$ (those not associated with a quantifier).*

Presburger (1929) (see Presburger, 1991, for a translation) examined this first order theory and proved it is decidable.

Example 10 *Given $t\in\mathbb{N}$, let*

$$S_t=\left\{x\in\mathbb{N}:\ \exists y\in\mathbb{N}, 2x+2y+3=5t \text{ and } t<x\le y\right\}.$$

We can compute that

$$S_t=\begin{cases}\left\{t+1,t+2,\ldots,\left\lfloor\frac{5t-3}{4}\right\rfloor\right\} & \text{if } t \text{ odd, } t\ge 3,\\ \emptyset & \text{else.}\end{cases}$$

This set has several properties, *cf.* Section 3:

1. The set of t such that S_t is nonempty is $\{3,5,7,\ldots\}$. This set is eventually periodic.
2. The cardinality of S_t is
$$S_t=\begin{cases}\left\lfloor\frac{5t-3}{4}\right\rfloor-t & \text{if } t \text{ odd, } t\ge 3,\\ 0 & \text{else,}\end{cases}$$
which is eventually a quasi-polynomial of period 4.

3. When S_t is nonempty, we can obtain an element of S_t with the function $x(t) = t + 1$, and $x(t)$ is eventually a quasi-polynomial.

3a. More strongly, when S_t is nonempty, we can obtain the maximum element of S_t with the function $x(t) = \lfloor (5t-3)/4 \rfloor$, and $x(t)$ is eventually a quasi-polynomial.

4. We can compute the generating function

$$\sum_{s \in S_t} x^s = \begin{cases} x^{t+1} + x^{t+2} + \cdots + x^{\lfloor (5t-3)/4 \rfloor} & \text{if } t \text{ odd, } t \geq 3, \\ 0 & \text{else,} \end{cases}$$
$$= \begin{cases} \dfrac{x^{t+1} - x^{\lfloor (5t-3)/4) \rfloor + 1}}{1-x} & \text{if } t \text{ odd, } t \geq 3, \\ 0 & \text{else.} \end{cases}$$

We see that, for fixed t, this generating function is a rational function. Considering each residue class of $t \bmod 4$ separately, the exponents in the rational function can eventually be written as polynomials in t.

Versions of these properties always hold for sets defined in Presburger arithmetic. For example, Woods (2012) gave several properties of Presburger formulas that hold even for sets defined with multivariate parameters, $\mathbf{t} \in \mathbb{N}^n$:

Theorem 11 (from Theorems 1 and 2 of Woods, 2012) *Suppose $F(\mathbf{s}, \mathbf{t})$ is a Presburger formula, with $\mathbf{s}$ and $\mathbf{t}$ collections of free variables. Then*

- $g(\mathbf{t}) = \#\{\mathbf{s} \in \mathbb{N}^d : \ F(\mathbf{s}, \mathbf{t})\}$ *is a piecewise quasi-polynomial,*
- $\sum_{\mathbf{s},\mathbf{t}: F(\mathbf{s},\mathbf{t})} \mathbf{x}^{\mathbf{s}} \mathbf{y}^{\mathbf{t}}$ *is a rational generating function, and*
- $\sum_{\mathbf{t} \in \mathbb{N}^n} g(\mathbf{t}) \mathbf{y}^{\mathbf{t}}$ *is a rational generating function.*

Property 4 from Example 10 can be proved in general by using Theorem 11 to write $\sum_{\mathbf{s},\mathbf{t}: F(\mathbf{s},\mathbf{t})} \mathbf{x}^{\mathbf{s}} \mathbf{y}^{\mathbf{t}}$ as a rational generating function and applying Theorem 29. The proof of Theorem 26 then shows that all of the other properties follow, though the exact definitions of these properties are only stated in Section 3 for a univariate parameter, $t \in \mathbb{N}$.

2 Unreasonable Ubiquitousness

We now turn to the inspiration for this paper. Three recent results exhibit quasi-polynomial behavior, in situations that seem "unreasonable". In particular, all three involve sets S_t defined by inequalities $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $\mathbf{a}(t)$ is a polynomial in t; that is, the normal vectors to the facets change as t changes. First we give an example showing that, unlike in Section 1, it is now important that we restrict to only one parameter, t.

Example 12 *Define $S_{s,t} = \{(x, y) \in \mathbb{N}^2 : \ sx + ty = st\}$. Then $S_{s,t}$ is an interval in $\mathbb{Z}^2$ with endpoints $(t, 0)$ and $(0, s)$, and*

$$|S_{s,t}| = \gcd(s, t) + 1.$$

There is no hope for simple quasi-polynomial behavior here, as the cardinality depends on the arithmetic relationship of s and t.

2.1 Three results

This first result most directly generalizes Ehrhart Theory. Chen, Li, and Sam (2012) prove that, if S_t is the set of integer points in a polytope defined by inequalities of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, then $|S_t|$ is eventually a quasi-polynomial.

Theorem 13 (Theorem 2.1 of Chen et al., 2012) *Let $A(t)$ be an $r \times d$ matrix, and $b(t)$ be a column vector of length r, all of whose entries are in $\mathbb{Z}[t]$. Assume $P_t = \{\mathbf{x} \in \mathbb{R}^d : \ A(t)\mathbf{x} \leq b(t)\}$ is eventually a bounded set (a polytope). Then $|P_t \cap \mathbb{Z}^d|$ is eventually a quasi-polynomial.*

Note that this can be equivalently phrased (Theorem 1.1 of Chen et al., 2012) using equalities $A(t)\mathbf{x} = b(t)$, where $\mathbf{x}$ is constrained to be nonnegative, or it can be phrased (Theorem 1.4 of Chen et al., 2012) by listing the vertices of P_t as rational functions of t.

Calegari and Walker (2011) were similarly concerned with the integer points in polyhedra defined by $A(t)\mathbf{x} \leq b(t)$. Rather than counting $|P_t \cap \mathbb{Z}^d|$, they wanted to find the integer hull of P_t, that is, the set of vertices of the convex hull of $P_t \cap \mathbb{Z}^d$.

Theorem 14 (Theorem 3.5 of Calegari and Walker, 2011) *Let $\mathbf{v}_i(t)$ be vectors in $\mathbb{Q}^d$ whose coordinates are rational functions of size $O(t)$, and let P_t be the convex hull of the $\mathbf{v}_i(t)$. Then there exists a modulus m and functions $\mathbf{p}_{ij} : \mathbb{N} \to \mathbb{Z}^d$ with polynomial coordinates such that, for $0 \leq i < m$ and for sufficiently large $t \equiv i \bmod m$, the integer hull of P_t is $\{\mathbf{p}_{i1}(t), \mathbf{p}_{i2}(t), \ldots, \mathbf{p}_{ik_i}(t)\}$.*

This theorem could be similarly phrased using facet definitions of the polyhedra, rather than vertex definitions. That the vertices are $\mathrm{O}(t)$ (grow no faster that ct for some constant c) is important for the proof, though Calegari and Walker conjecture that the theorem still holds without this restriction.

A third recent result concerns the Frobenius number.

Definition 15 *Given $a_1, \ldots, a_d \in \mathbb{N}$, let S be the semigroup generated by the a_i, that is,*

$$S = \{a \in \mathbb{N} : \ \exists \lambda_1, \ldots, \lambda_d \in \mathbb{N}, a = \lambda_1 a_1 + \cdots + \lambda_d a_d\}.$$

If the a_i are relatively prime, then S contains all sufficiently large integers, and the Frobenius number *is defined to be the largest integer not in S.*

Now we let $a_i = a_i(t)$ vary with t. Roune and Woods (2012) prove that, if the $a_i(t)$ are linear functions of t, then the Frobenius number is eventually a quasi-polynomial, and they conjecture that this is true if the $a_i(t)$ are any polynomial functions of t:

Theorem 16 *Let $a_i(t) \in \mathbb{Z}[t]$ have degree at most one and be eventually positive. Then the set of t such that the $a_i(t)$ are relatively prime is eventually periodic, and, for such t, the Frobenius number is eventually given by a quasi-polynomial.*

Example 17 *Consider $a_1(t) = t$, $a_2(t) = t + 3$. These are relatively prime exactly when $t \equiv 1, 2 \bmod 3$. Since there are only two generators, a well-known formula (seemingly due to Sylvester, 1884) gives that the Frobenius number is*

$$a_1 a_2 - a_1 - a_2 = t^2 + t - 3.$$

Note that Theorem 16 utilizes sets defined with quantifiers; Presburger arithmetic seems a good place to look for generalizations encompassing these three results.

2.2 Common tools

Each of these three results has their own method for proving quasi-polynomial behavior, but there are several common tools needed. Chen et al. (2012) and Calegari and Walker (2011) independently prove Theorems 18 through 22, and Calegari and Walker (2011) prove Theorem 23.

Theorem 18 (Division Algorithm) *Given $f(t), g(t)$ integer-valued polynomials,*

1. *if $\deg g > 0$, there exist integer-valued quasi-polynomials $q_1(t)$ and $r_1(t)$ such that $f(t) = q_1(t)g(t) + r_1(t)$, with $\deg r_1 < \deg g$, and*
2. *if $g \neq 0$, there exist integer-valued quasi-polynomials $q_2(t)$ and $r_2(t)$ such that $f(t) = q_2(t)g(t) + r_2(t)$, with eventually $0 \leq r_2(t) < |g(t)|$.*

These are both useful results, and only slightly different. For example, suppose $f(t) = 2t - 3$ and $g(t) = t$. Then Statement 1 is a traditional polynomial division algorithm: $f = 2g + -3$. Statement 2, however, is a numerical division algorithm: $f = 1g + (t - 3)$, and the remainder $t - 3$ is between 0 and g as long as $t \geq 3$. In other words, if we have found q_1 and r_1, but we eventually have $r_1(t) < 0$, then we should use quotient $q_2 = q_1 - \operatorname{sgn}(g)$ and remainder $r_2 = |g| + r_1$ instead, as eventually $0 \leq |g(t)| + r_1(t) < |g(t)|$.

The main subtlety in proving Statement 1 of this theorem is the following: Suppose $f(t) = t^2 + 3t$ and $g(t) = 2t + 1$. Then the leading coefficient of g does not divide the leading coefficient of f, and the traditional polynomial division algorithm would produce quotients that are not integer-valued. Instead, we look at t modulo the leading coefficient of g; for example, if $t = 2s+1$, substituting gives $f(2s+1) = 4s^2 + 10s + 3$ and $g(2s + 1) = 4s + 3$, and now the leading term does divide evenly.

The division algorithm in hand, one can prove some stronger results:

Theorem 19 (Euclidean Algorithm and gcds) *Let f and g be integer-valued quasi-polynomials. Then there exists integer-valued quasi-polynomials $p(t)$, $q(t)$, and $d(t)$ such that $\gcd\big(f(t), g(t)\big) = d(t)$ and $d(t) = p(t)f(t) + q(t)g(t)$.*

This is obtained by repeated applications of the division algorithm.

Example 20

$$\gcd(2t + 1, 5t + 6) = \gcd(t + 4, 2t + 1) = \gcd(7, t + 4) = \begin{cases} 7 & \textit{if } t \equiv 3 \bmod 7, \\ 1 & \textit{else.} \end{cases}$$

Similarly, repeated application of the Euclidean algorithm can produce the Hermite or Smith normal forms of matrices. We won't define those here, but they are important, for example, in producing a basis for lower-dimensional sublattices of $\mathbb{Z}^d$ (see Newman, 1972).

Theorem 21 (Hermite/Smith Normal Forms) *Given a matrix $A(t)$ with integer-valued quasi-polynomial entries, the Hermite and the Smith Normal forms, as well as their associated change-of-basis matrices, also have quasi-polynomial entries.*

The following theorem is obvious, but is repeatedly used.

Theorem 22 (Dominance) *Suppose $f, g \in \mathbb{Q}[t]$ with $f \neq g$. Then either eventually $f(t) > g(t)$ or eventually $g(t) > f(t)$.*

Repeated use of this property, for example, shows that the combinatorial structure of a polyhedron P_t eventually stabilizes, when P_t is defined by $A(t)\mathbf{x} \le b(t)$.

Rational functions commonly appear in these results. For example, if a polyhedron is defined by $A(t)\mathbf{x} \le b(t)$, a vertex will be a point where several of these inequalities are equalities, i.e., the solution to some $A'(t)\mathbf{x} = b'(t)$, where $A'(t)$ is a full-rank $d \times d$ matrix of polynomials in t. Solving for $\mathbf{x}$ using the adjunct matrix of A' will result in $\mathbf{x}(t)$ given as a rational function of t. For large t, the behavior of a rational function is predictable:

Theorem 23 (Rounding) *Let $f(t), g(t) \in \mathbb{Z}[t]$. Then $f(t)/g(t)$ converges to a polynomial, and $\lfloor f(t)/g(t) \rfloor$ is eventually a quasi-polynomial.*

3 Conjectures

Let $S_t \subseteq \mathbb{N}^d$ be a family of subsets of natural numbers. We now discuss some properties that it would be nice (though unreasonable!) for such sets to have; *cf.* Example 10.

Property 1: The set of t such that S_t is nonempty is eventually periodic.

This is the weakest of the properties we will discuss, but an important one, as it is related to the decision problem – “Is there a solution?”

Property 2: There exists a function $g : \mathbb{N} \to \mathbb{N}$ such that, if S_t has finite cardinality, then $g(t) = |S_t|$, and $g(t)$ is eventually a quasi-polynomial. The set of t such that S_t has finite cardinality is eventually periodic.

This is the property found in Theorem 13, where S_t is the set of integer points in a polytope defined by inequalities $\mathbf{a}(t) \cdot \mathbf{x} \le b(t)$. Theorems 14 and 16, on the other hand, are not about counting points but about finding points:

Property 3: There exists a function $\mathbf{x} : \mathbb{N} \to \mathbb{N}^d$ such that, if S_t is nonempty, then $\mathbf{x}(t) \in S_t$, and the coordinate functions of $\mathbf{x}$ are eventually quasi-polynomials. The set of t such that S_t is nonempty is eventually periodic.

This function $\mathbf{x}(t)$ acts as a certificate that the set is nonempty. But we may want to go further and pick out particular elements of S_t:

Property 3a: Given $\mathbf{c} \in \mathbb{Z}^d$, there exists a function $\mathbf{x} : \mathbb{N} \to \mathbb{N}^d$ such that, if $\max_{\mathbf{y} \in S_t} \mathbf{c} \cdot \mathbf{y}$ exists, then it is attained at $\mathbf{x}(t) \in S_t$, and the coordinate functions of $\mathbf{x}$ are eventually quasi-polynomials. The set of t such that the maximum exists is eventually periodic.

This corresponds to Theorem 16, where we want to find the Frobenius number, the maximum element of the complement of the semigroup. On the other hand, we may want to list *multiple* elements of the set:

Property 3b: Fix $k \in \mathbb{N}$. There exist functions $\mathbf{x}_1, \dots, \mathbf{x}_k : \mathbb{N} \to \mathbb{N}^d$ such that, if $|S_t| \ge k$, then $\mathbf{x}_1(t), \dots, \mathbf{x}_k(t)$ are distinct elements of S_t, and the coordinate functions of $\mathbf{x}_i$ are eventually quasi-polynomials. The set of t such that $|S_t| \ge k$ is eventually periodic.

If there is a uniform bound on $|S_t|$, then this property can be used to enumerate all elements of S_t, for all t. This is the content of Theorem 14. Property 2 is about counting all solutions and Properties 3/3a/3b are about obtaining specific solutions, and so they seem somewhat orthogonal to each other. The following property, we shall see, unifies them:

Property 4: There exists a period m such that, for $t \equiv i \bmod m$,

$$\sum_{\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} = \frac{\sum_{j=1}^{n_i} \alpha_{ij}\mathbf{x}^{\mathbf{q}_{ij}(t)}}{\left(1-\mathbf{x}^{\mathbf{b}_{i1}(t)}\right)\cdots\left(1-\mathbf{x}^{\mathbf{b}_{ik_i}(t)}\right)},$$

where $\alpha_{ij} \in \mathbb{Q}$, and the coordinate functions of $\mathbf{q}_{ij}, \mathbf{b}_{ij} : \mathbb{N} \to \mathbb{Z}^d$ are polynomials with the $\mathbf{b}_{ij}(t)$ lexicographically positive.

For what sets S_t can we hope for these properties to hold? Here is a candidate:

Definition 24 *A family of sets S_t is a* parametric Presburger family *if they can be defined over the natural numbers using quantifiers, boolean operations, and inequalities of the form $\mathbf{a}(t)\cdot\mathbf{x} \le b(t)$, where $b \in \mathbb{Z}[t]$ and $\mathbf{a} \in \mathbb{Z}[t]^d$.*

We conjecture that these properties do, in fact, hold for any parametric Presburger family:

Conjecture 25 *Let S_t be a parametric Presburger family. Then Properties 1, 2, 3, 3a, 3b, and 4 all hold.*

Note that one can define a family S_t of subsets of $\mathbb{Z}^d$ rather than of $\mathbb{N}^d$, though one must be more careful when talking about generating functions. For example, the set $\mathbb{Z}$ has generating function

$$\cdots + x^{-1} + 1 + x^1 + x^2 + \cdots = \frac{x^{-1}}{1-x^{-1}} + \frac{1}{1-x} = -\frac{1}{1-x} + \frac{1}{1-x} = 0.$$

See, for example, Barvinok (2008) for more details.

As evidence that Property 4 is interesting, we will show that it generalizes both 2 and 3/3a/3b:

Theorem 26 *Let S_t be any family of subsets of $\mathbb{N}^d$. We have the following implications among possible properties of S_t.*

$$\begin{tikzcd}
 & & 2 \arrow[dr, Rightarrow, bend left] & \\
4 \arrow[urr, Rightarrow, bend left] \arrow[r, Rightarrow] \arrow[dr, Rightarrow, bend right] & 3a \arrow[r, Rightarrow] & 3 \arrow[r, Rightarrow] & 1 \\
 & 3b \arrow[ur, Rightarrow, bend right] & &
\end{tikzcd}$$

As a final relationship between these properties, we note that, for the class of parametric Presburger families, 3, 3a, and 3b are equivalent:

Theorem 27 *Suppose all parametric Presburger families have Property 3. Then all parametric Presburger families have Properties 3a and 3b.*

Theorem 27 is a weaker implication than Theorem 26, which holds for a single family S_t in isolation. To prove that 3 "implies" 3a and 3b, on the other hand, we will need to create new families S_t' using additional quantifiers or boolean operators, and we need to know that these new families still have Property 3.

Finally, we give evidence that these properties might actually hold. We can show that they all hold for two broad classes of parametric Presburger families:

Theorem 28 *Suppose S_t is a parametric Presburger family such that either*

(a) *S_t is defined without using any quantifiers,* or

(b) *S_t is defined using only inequalities of the form $\mathbf{a}\cdot\mathbf{x} \le b(t)$, where $b(t)$ is a polynomial (that is, the normal vector, $\mathbf{a}$, to the hyperplane must be fixed).*

Then Properties 1, 2, 3, 3a, 3b, and 4 all hold.

We isolate a piece of the proof of Part (b), in order to point out that Property 4 is a weaker property than we might hope for, but seems to be as strong a property as we can get. Indeed, we might hope that $\sum_{t\in\mathbb{N},\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} y^t$ is a rational generating function. Theorem 11 shows that this is true for sets defined in the normal Presburger arithmetic, and the following theorem shows that this implies Property 4.

Theorem 29 *Suppose $S_{\mathbf{p}}$, for $\mathbf{p} \in \mathbb{N}^n$, is a family of subsets of $\mathbb{N}^d$. If $\sum_{\mathbf{p}\in\mathbb{N}^n,\mathbf{s}\in S_{\mathbf{p}}} \mathbf{x}^{\mathbf{s}}\mathbf{y}^{\mathbf{p}}$ is a rational generating function, then there is a finite decomposition of $\mathbb{N}^n$ into pieces of the form $P \cap \mathbb{Z}^n$ (with P a polyhedron) such that, considering the $\mathbf{p}$ in each piece separately,*

$$\sum_{\mathbf{s}\in S_{\mathbf{p}}} \mathbf{x}^{\mathbf{s}} = \sum_i \epsilon_i \frac{\mathbf{x}^{\mathbf{q}_i(\mathbf{p})}}{(1-\mathbf{x}^{\mathbf{b}_{i1}})\cdots(1-\mathbf{x}^{\mathbf{b}_{ik_i}})},$$

where $\epsilon_i = \pm 1$, $\mathbf{b}_{ij} \in \mathbb{Z}^d$ are lexicographically positive, and the coordinate functions of $\mathbf{q}_i : \mathbb{N}^n \to \mathbb{Z}^d$ are degree 1 quasi-polynomials in $\mathbf{p}$.

In general, however, $\sum_{t\in\mathbb{N},\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} y^t$ will not be a rational generating function:

Example 30 *Let S_t be the set $\{(s_1,s_2) \in \mathbb{N}^2 :\ ts_1 = s_2\}$. Then*

$$\sum_{\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} = 1 + x_1x_2^t + x_1^2x_2^{2t} + \cdots = \frac{1}{1-x_1x_2^t}$$

is a rational generating function with exponents depending on t, so Property 4 is satisfied. Nevertheless,

$$\sum_{t\in\mathbb{N},\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} y^t = \frac{1}{1-x_1} + \frac{y}{1-x_1x_2} + \frac{y^2}{1-x_1x_2^2} + \cdots$$

cannot be written as a rational function.

To prove that it cannot be so written, note that the set $\big\{(s_1,s_2,t) :\ \mathbf{s} \in S_t\big\}$ cannot be written as a finite union of sets of the form $P \cap (\lambda + \Lambda)$, where P is a polyhedron, $\lambda \in \mathbb{Z}^3$ and $\Lambda \subseteq \mathbb{Z}^3$ is a lattice; Theorem 1 of Woods (2012) then implies that $\sum_{t\in\mathbb{N},\mathbf{s}\in S_t} \mathbf{x}^{\mathbf{s}} y^t$ is not a rational generating function.

References

Alexander Barvinok. *Integer points in polyhedra*. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich, 2008. URL `http://dx.doi.org/10.4171/052`.

Alexander Barvinok and James Pommersheim. 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.*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.

Matthias Beck. The partial-fractions method for counting solutions to integral linear systems. *Discrete Comput. Geom.*, 32(4):437–446, 2004. URL `http://dx.doi.org/10.1007/s00454-004-1131-5`.

Michel Brion. Points entiers dans les polyèdres convexes. *Ann. Sci. École Norm. Sup.*, 4:653–663, 1988.

Danny Calegari and Allen Walker. Integer hulls of linear polyhedra and scl in families. preprint, 2011. URL `http://arxiv.org/abs/1011.1455`.

Sheng Chen, Nan Li, and Steven V. Sam. Generalized Ehrhart polynomials. *Trans. Amer. Math. Soc.*, 364 (1):551–569, 2012. URL `http://dx.doi.org/10.1090/S0002-9947-2011-05494-2`.

Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254: 616–618, 1962.

Morris Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Math., Vol. 45.

Mojżesz Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen in welchen die Addition als einzige Operation hervortritt. In *Comptes-Rendus du premier Congrès des Mathèmaticiens des Pays Slaves*, 1929.

Mojżesz Presburger. 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):225–233, 1991. URL `http://dx.doi.org/10.1080/014453409108837187`. Translated from the German and with commentaries by Dale Jacquette.

Bjarke Roune and Kevin Woods. The parametric Frobenius problem. forthcoming, 2012.

Richard P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

Bernd Sturmfels. On vector partition functions. *J. Combin. Theory Ser. A*, 72(2):302–309, 1995. URL `http://dx.doi.org/10.1016/0097-3165(95)90067-5`.

James J. Sylvester. Mathematical questions with their solutions. *Educational Times*, 41(21), 1884.

Sven Verdoolaege and Kevin Woods. Counting with rational generating functions. *J. Symbolic Comput.*, 43(2):75–91, 2008. URL `http://dx.doi.org/10.1016/j.jsc.2007.07.007`.

Sven Verdoolaege, Rachid Seghir, Kristof Beyls, Vincent Loechner, and Maurice Bruynooghe. Counting integer points in parametric polytopes using barvinok's rational functions. *Algorithmica*, 48:37–66, 2007. URL `http://dx.doi.org/10.1007/s00453-006-1231-0`.

Kevin Woods. Presburger arithmetic, rational generating functions, and quasi-polynomials. preprint, 2012. URL `http://arxiv.org/abs/1211.0020`.