
A Plethora of Polynomials: A Toolbox for Counting Problems

Tristram Bogart and Kevin Woods

Abstract. A wide variety of problems in combinatorics and discrete optimization depend on counting the set S of integer points in a polytope, or in some more general object constructed via discrete geometry and first-order logic. We take a tour through numerous problems of this type. In particular, we consider families of such sets S_t depending on one or more integer parameters t , and analyze the behavior of the function $f(t) = |S_t|$. In the examples that we investigate, this function exhibits surprising polynomial-like behavior. We end with two broad theorems detailing settings where this polynomial-like behavior must hold. The plethora of examples illustrates the framework in which this behavior occurs and also gives an intuition for many of the proofs, helping us create a toolbox for counting problems like these.

1. INTRODUCTION. It's no surprise that geometry is a fertile source of polynomial functions. For example, if we take a bounded d -dimensional object, B , and dilate by a factor of t , then $\text{vol}(tB) = \text{vol}(B)t^d$ is a degree d polynomial in t . It's more surprising that we can add considerable complication to these sets, taking us into the worlds of *discrete geometry* and *first-order logic*, and we still see the persistent appearance of polynomial-like functions. The framework that we will describe is broad, and it includes many problems that, at first glance, seem unrelated to geometry and logic. We will examine a number of these problems as we build intuition and a toolbox. As a teaser that we will return to later, consider the *Frobenius problem*:

Definition 1 (Frobenius problem). Given positive integers a_1, \dots, a_n , let S be the semigroup generated by the a_i , that is, the set of integers that can be written as sums of the a_i 's:

$$S = \{m \in \mathbb{Z}_{\geq 0} : \text{there exist } \lambda_1, \dots, \lambda_n \in \mathbb{Z}_{\geq 0} \text{ with } m = \lambda_1 a_1 + \dots + \lambda_n a_n\}.$$

If the a_i are relatively prime, then all sufficiently large integers are in S , and so we can define $F(a_1, \dots, a_n)$ to be the largest integer *not* contained in S (the *Frobenius number*) and $g(a_1, \dots, a_n)$ to be the number of positive integers not contained in S (the number of *gaps*). (See [25] for a broad overview.)

Example 1. Chicken McNuggets used to be sold in packs of 6, 9, or 20. If you want to eat $m \in \mathbb{Z}_{\geq 0}$ McNuggets, can you buy some packs and get exactly m McNuggets? One can check that the only m for which you *cannot* are the 22 integers 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34, 37, and 43. That is, $F(6, 9, 20) = 43$ and $g(6, 9, 20) = 22$.

Finding formulas for $F(a_1, \dots, a_n)$ and $g(a_1, \dots, a_n)$ seems fruitless in general [24], and so people have looked at many special cases. One consequence (among many) of the machinery that we explain here is that there are polynomial-like formulas whenever the a_i are polynomial functions of a single parameter t . (This was first proved in [26], when the a_i are linear functions of t , and in [27] for general polynomials.)

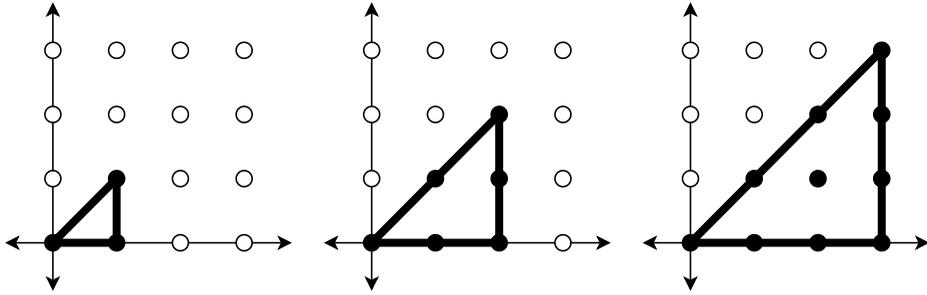


Figure 1. $T \cap \mathbb{Z}^2$, $2T \cap \mathbb{Z}^2$, and $3T \cap \mathbb{Z}^2$ from Example 4, yielding the 2nd, 3rd, and 4th triangular numbers, respectively.

Example 2. By the end of Section 6, we will have all of the tools that we need to calculate that

$$F(t, t+1, t+3) = \begin{cases} \frac{1}{3}t^2 + t - 1 & \text{if } t \equiv 0 \pmod{3}, \\ \frac{1}{3}t^2 + \frac{2}{3}t - 2 & \text{if } t \equiv 1 \pmod{3}, \\ \frac{1}{3}t^2 + \frac{1}{3}t - 1 & \text{if } t \equiv 2 \pmod{3} \end{cases}$$

and

$$g(t, t+1, t+3) = \begin{cases} \frac{1}{6}t^2 + \frac{1}{2}t & \text{if } t \equiv 0 \pmod{3}, \\ \frac{1}{6}t^2 + \frac{1}{2}t - \frac{2}{3} & \text{if } t \equiv 1 \pmod{3}, \\ \frac{1}{6}t^2 + \frac{1}{2}t - \frac{2}{3} & \text{if } t \equiv 2 \pmod{3}. \end{cases}$$

In the next sections, we build up a library of examples — starting simple and ending with ones like the above — of polynomial-like functions that describe sets in discrete geometry and logic. Many of these examples illustrate important tools in the general study of these phenomena. If the reader is itching for a spoiler at any time, Section 7 gives a precise statement of the general theorems encompassing all of these examples.

2. POLYHEDRA. We start with a classic.

Example 3. The t th triangular number, $1 + 2 + \cdots + t$, is $t(t+1)/2$.

We've seen this fact so many times that it may have lost its wonder, but it truly is wonderful! An excited student, seeing this for the first time, would want to generalize. What other wonderful results are there like this?

Example 4. Let $T \subseteq \mathbb{R}^2$ be the triangle with vertices $(0, 0)$, $(1, 0)$, and $(1, 1)$, and let tT (for $t \in \mathbb{Z}_{>0}$) be the dilation of T by a factor of t , as pictured in Figure 1. Then we see that the number of points with integer coordinates that lie in tT is the $(t+1)$ st triangular number, so this is just the same example in a geometric disguise.

Definition 2. Given a bounded set $B \subseteq \mathbb{R}^d$, define $f_B(t) = |tB \cap \mathbb{Z}^d|$, for $t \in \mathbb{Z}_{>0}$.

For our triangle, T , in Example 4, we have

$$f_T(t) = \frac{(t+1)(t+2)}{2} = \frac{1}{2}t^2 + \frac{3}{2}t + 1.$$

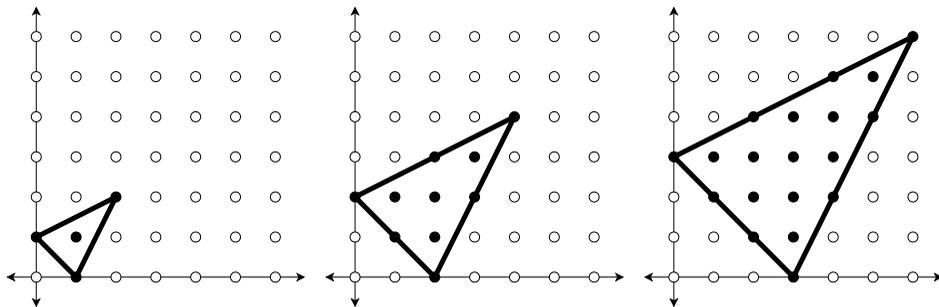


Figure 2. $Q \cap \mathbb{Z}^2$, $2Q \cap \mathbb{Z}^2$, and $3Q \cap \mathbb{Z}^2$ from Example 5.

It's not surprising that $f_T(t)$ is approximately $t^2/2$; after all, $\text{vol}(tT) = t^2 \text{vol}(T) = t^2/2$, and so for large t there should be roughly $t^2/2$ integer points contained in tT , with any discrepancy related to how the integer points interact with the boundary of tT . It is a beautiful fact that this discrepancy is so well behaved that $f_T(t)$ is still a polynomial.

How can we generalize? Let's start by examining a different triangle with integral vertices.

Example 5. Let Q be the triangle with vertices $(1, 0)$, $(0, 1)$, and $(2, 2)$; see Figure 2. Then

$$f_Q(t) = \frac{3}{2}t^2 + \frac{3}{2}t + 1.$$

It's fun to verify this formula by drawing dilates of Q , but we will establish it using Pick's theorem; in fact, this will prove that we get a nice polynomial formula for $f_P(t)$ when P is *any* polygon with integral vertices. Let A_t be the area of tP , b_t be the number of integer points on the boundary of tP , and i_t be the number of integer points in the interior. Pick's theorem [21] (see [3, §2] for a simple proof in English) tells us that

$$A_t = i_t + \frac{b_t}{2} - 1.$$

Rearranging, we have that

$$f_P(t) = i_t + b_t = A_t + \frac{b_t}{2} + 1.$$

But A_t and b_t are easy to calculate: $A_t = t^2 A_1$ and $b_t = t b_1$ (the latter is easiest to see for the triangle Q by dividing the boundary of tQ into three half-open intervals, including one endpoint and excluding the other, each of which has t vertices). Substituting, we have that

$$f_P(t) = A_1 t^2 + \frac{b_1}{2} t + 1$$

is a polynomial. For the triangle Q , we use $A_1 = \frac{3}{2}$ and $b_1 = 3$, but we see that it works for any polygon with integral vertices. As before, it is not surprising that the leading

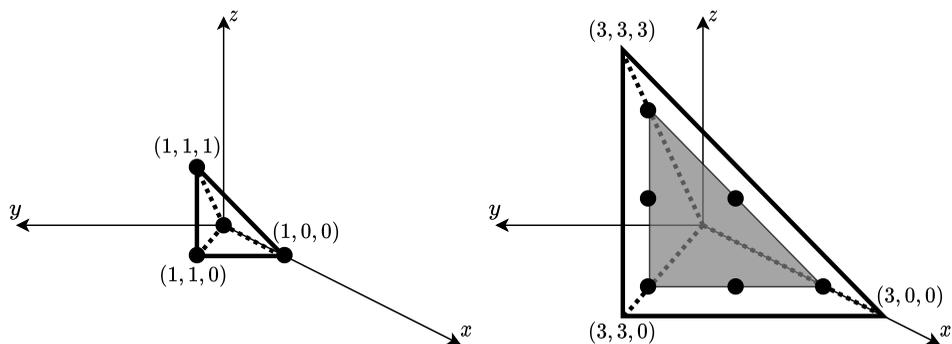


Figure 3. On the left is P from Example 6, the tetrahedron formed by the convex hull of the three labeled vertices and the origin; the $f_P(1) = |P \cap \mathbb{Z}^3| = 4$ integer points are shown. On the right is $3P$, and shaded is the cross-section of $3P$ at $x = 2$; this cross-section has 6 integer points (the third triangular number), as shown.

term is $A_t = A_1 t^2$; what is surprising is that the “correction” terms for looking at integer points are so simple.

How should we generalize next? There are two obvious ways: try dimensions higher than 2 or try polygons with nonintegral vertices. Don’t worry: we’ll try both. First let’s see an example in a higher dimension.

Example 6. Let $P \subseteq \mathbb{R}^3$ be the tetrahedron with vertices $(0, 0, 0)$, $(1, 0, 0)$, $(1, 1, 0)$, and $(1, 1, 1)$; see Figure 3. The cross-section of tP at $x = s$ is a copy of sT , where T is the triangle in Example 4. Thus the number of integer points in the cross-section is the $(s + 1)$ st triangular number, and so $f_P(t)$ is the sum of the first $t + 1$ triangular numbers, that is, the $(t + 1)$ st *tetrahedral number*. So we have

$$f_P(t) = \frac{(t + 1)(t + 2)(t + 3)}{6} = \frac{1}{6}t^3 + t^2 + \frac{11}{6}t + 1.$$

Again, our answer is a polynomial. Again the leading term is $\text{vol}(tP) = \text{vol}(P)t^3$. The first deep result in this area is that this works for *any* polytope (bounded polyhedron) in *any* dimension, as long as it has integral vertices. We’ll state this precisely after a few examples with nonintegral vertices.

Example 7. Let $P \subseteq \mathbb{R}$ be the interval $[0, 1/2]$. Then

$$f_P(t) = \lfloor t/2 \rfloor + 1 = \begin{cases} \frac{1}{2}t + 1 & \text{if } t \text{ even,} \\ \frac{1}{2}t + \frac{1}{2} & \text{if } t \text{ odd.} \end{cases}$$

This example makes it clear that, when the vertices are nonintegral, we can no longer expect to get exactly a polynomial. While $f_P(t)$ should be approximately $t/2$ (the length of tP), our formula will need to account for whether the right vertex of tP is an integer (t even) or not (t odd). The most we can hope for is to get a counting function that is polynomial-like, but includes some periodicity. Let’s combine the polynomial behavior and periodic behavior into a definition.

Definition 3 (Quasi-polynomial). A function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is a *quasi-polynomial* (which we will denote by QP) if there exist a period s and polynomial functions $f_0(t), \dots, f_{s-1}(t)$ such that $f(t) = f_i(t)$ for $t \equiv i \pmod{s}$.

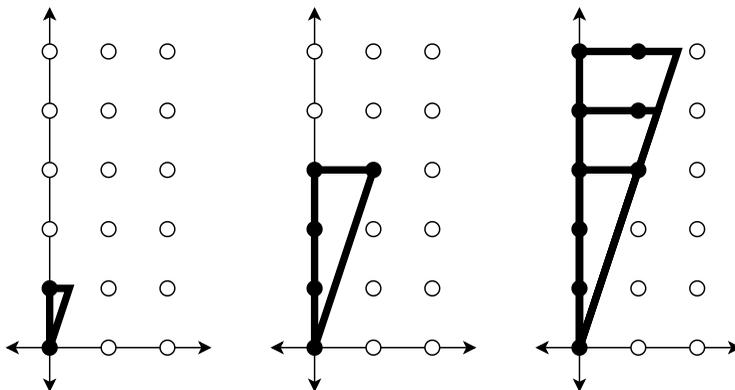


Figure 4. $T \cap \mathbb{Z}^2$, $3T \cap \mathbb{Z}^2$, and an overlay of $3T$, $4T$, $5T$, from Example 8.

Example 8. Let T be the triangle with vertices $(0, 0)$, $(0, 1)$, and $(\frac{1}{3}, 1)$; see Figure 4. How can we calculate $f(T)$? Observing that $3T$ is a polygon with integral vertices, area $3/2$, and containing five integer points on the boundary, we can use Pick's theorem to compute $f_T(t)$ when $t = 3u$ is a multiple of three:

$$f_T(t) = f_T(3u) = f_{3T}(u) = \frac{3}{2}u^2 + \frac{5}{2}u + 1 = \frac{1}{6}t^2 + \frac{5}{6}t + 1.$$

On the other hand, if $t = 3u + 1$, then we can note that $(3u + 1)T$ has exactly $u + 1$ more integer points than $3uT$ has (they are $(0, 3u + 1), \dots, (u, 3u + 1)$), to be precise; see the relationship between $3T$ and $4T$ in Figure 4). Therefore,

$$f_T(t) = f_T(3u + 1) = f_T(3u) + (u + 1) = \frac{1}{6}t^2 + \frac{5}{6}t + 1,$$

(coincidentally) the same polynomial as in the first case. We invite the reader to try this out for $t = 3u + 2$; successfully simplifying will yield

$$f_T(t) = \begin{cases} \frac{1}{6}t^2 + \frac{5}{6}t + 1 & \text{if } t \equiv 0 \pmod{3}, \\ \frac{1}{6}t^2 + \frac{5}{6}t + 1 & \text{if } t \equiv 1 \pmod{3}, \\ \frac{1}{6}t^2 + \frac{5}{6}t + \frac{2}{3} & \text{if } t \equiv 2 \pmod{3} \end{cases}$$

which is a QP of period three.

These results generalize to any polytope in any dimension, as long as it has rational vertices. This is the content of the first big theorem in this direction.

Theorem 1 (Ehrhart's Theorem). [15, 16]. Let $P \subseteq \mathbb{R}^d$ be a polytope with rational vertices, and let s be the smallest positive integer such that sP has integral vertices. Then $f_P(t) = |tP \cap \mathbb{Z}^d|$ (defined for $t \in \mathbb{Z}_{>0}$) is a quasi-polynomial with period s . In particular, if P has integral vertices, then $s = 1$ and $f_P(t)$ is a polynomial.

Proofs of Ehrhart's theorem have been explained nicely in, for example [2, §18] or [3, §3], so we do not delve into *why* this is working in dimensions larger than two; we'd rather spend our time giving an intuition for the tools that layer on top of Ehrhart theory to prove QP results for larger classes of sets.

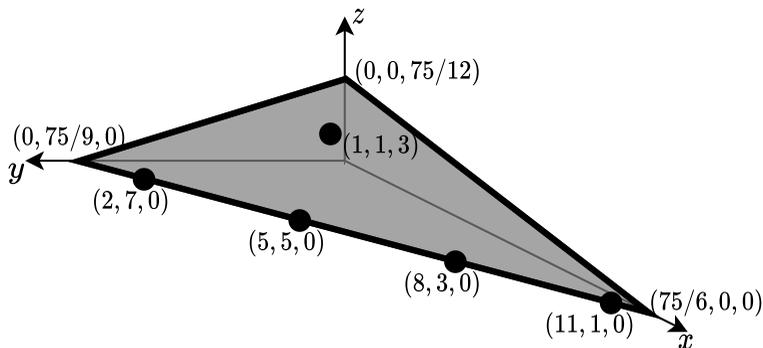


Figure 5. The triangle $75P$, from Example 9. The three vertices are labeled, as are the $f_T(75) = 5$ integer points in $75P$; for example, the point $(1, 1, 3) \in 75P$ shows that exactly 75 McNuggets can be purchased by ordering one box of 6, one box of 9, and three boxes of 20.

A final example shows that polyhedra can be hidden in seemingly nongeometric problems.

Example 9. Given that McNuggets come in boxes of 6, 9, and 20, let $f(t)$ be the number of different ways to order exactly t McNuggets. For example, $f(18) = 2$, since you can order three boxes of 6 or two boxes of 9. What is $f(t)$ as a function of t ?

Let T be the triangle, lying in three dimensions, with vertices $(1/6, 0, 0)$, $(0, 1/9, 0)$, and $(0, 0, 1/20)$. This triangle consists of the nonnegative real points lying in the hyperplane $6x + 9y + 20z = 1$. So tT is the triangle of nonnegative real points lying in the hyperplane $6x + 9y + 20z = t$, and an integer point in tT is exactly a triplet of three nonnegative integers (x, y, z) with $6x + 9y + 20z = t$; in other words, an integer point in tT corresponds to a way to order exactly t McNuggets. See Figure 5 for a depiction of $75P$ and its 5 integer points. Ehrhart's theorem tells us that $f(t) = f_T(t)$ is a QP of period $\text{lcm}(6, 9, 20) = 180$ (since the vertices of $180T$ are integral). Calculating it is best done on a computer; for example, if $t \equiv 18 \pmod{180}$, then $f(t) = \frac{1}{2160}t^2 + \frac{7}{180}t + \frac{23}{20}$, and if $t \equiv 75 \pmod{180}$, then $f(t) = \frac{1}{2160}t^2 + \frac{11}{360}t + \frac{5}{48}$.

3. MULTIPLE PARAMETERS. Where to next? One direction to take is to think of a polytope, $P \subseteq \mathbb{R}^d$, as the solution set to a *conjunction of linear inequalities*. The dilate tP can also be written as a conjunction of this sort, and it will have a very nice form: if $a_1x_1 + \cdots + a_dx_d \leq b$ is one of the defining inequalities of P , then $a_1x_1 + \cdots + a_dx_d \leq tb$ will be a defining inequality for tP . The facet of tP that this inequality defines has a normal vector, (a_1, \dots, a_d) , that is independent of t . However, the right-hand side of the inequality, tb , is changing, so the facets are shifting (but not twisting) as t changes. The particular form of the right-hand side, tb , means that the facets shift in “lockstep” with each other, as linear functions of t . This suggests another way to generalize: allow the facets to shift separately from one another (but still with constant normal vectors), perhaps — if we may be so bold — by allowing additional parameters.

Example 10. Given $s, t \in \mathbb{Z}_{>0}$, define

$$P_{s,t} = \{(x, y) \in \mathbb{R}^2 : y \geq 0, y \leq s, y \leq x, x + y \leq t\}.$$

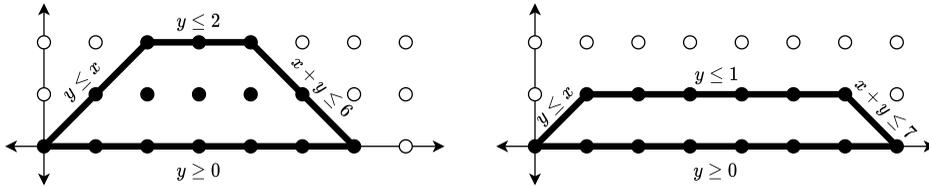


Figure 6. $P_{2,6} \cap \mathbb{Z}^2$ and $P_{1,7} \cap \mathbb{Z}^2$ from Example 10.

What is $f(s, t) = |P_{s,t} \cap \mathbb{Z}^2|$?

Examining Figure 6, it looks like $P_{s,t}$ is a trapezoid, for fixed s and t ; as s and t change, two of the sides of this trapezoid shift. Counting the number of integer points isn't too bad: this trapezoid can be divided into two triangles and a rectangle, yielding total number of integer points

$$2 \left(\frac{s(s+1)}{2} \right) + (t - 2s + 1)(s + 1) = ts - s^2 + t + 1.$$

A polynomial! As before, if the vertices of $P_{s,t}$ were not integral, our answer would also depend periodically on s and t . Perhaps you're shouting that we've missed something: if s gets large but t stays relatively small (to be precise, if $2s \geq t$), then the top edge of the trapezoid disappears, and we are left with a triangle with vertices $(0, 0)$, $(t, 0)$, and $(t/2, t/2)$. Therefore our final answer must be defined *piecewise*, depending on whether $P_{s,t}$ is a trapezoid or a triangle. Putting it all together,

$$f(s, t) = \begin{cases} ts - s^2 + t + 1 & \text{if } 2s < t, \\ \frac{1}{4}t^2 + t + 1 & \text{if } 2s \geq t, t \text{ even,} \\ \frac{1}{4}t^2 + t + \frac{3}{4} & \text{if } 2s \geq t, t \text{ odd.} \end{cases}$$

Functions like this are the final deviation from a nice, simple polynomial that we will need, made precise in the next two definitions.

Definition 4 (Multivariate Quasi-polynomials). A function $f : \mathbb{Z}^k \rightarrow \mathbb{Z}$ is a (multivariate) *quasi-polynomial* (which we will still denote by QP) if there exist a k -dimensional lattice $\Lambda \subseteq \mathbb{Z}^k$ and polynomial functions $f_C(t_1, \dots, t_k)$, one for each coset C of \mathbb{Z}^k modulo Λ , such that $f(t_1, \dots, t_k) = f_C(t_1, \dots, t_k)$ if $(t_1, \dots, t_k) \in C$.

Remark. In the $2s \geq t$ cases of the function $f(s, t)$ above, the lattice Λ is $\mathbb{Z} \times 2\mathbb{Z}$ with cosets $(0, 0) + \Lambda$ (s any integer, t even) and $(0, 1) + \Lambda$ (s any integer, t odd). In general, Λ might be a more complicated sublattice of \mathbb{Z}^k , but one could always define the quasi-polynomials on cosets of some rectangular lattice $m_1\mathbb{Z} \times \dots \times m_k\mathbb{Z} \subseteq \Lambda$ so that $f(t_1, \dots, t_k)$ is defined by polynomials on residue classes of $t_i \bmod m_i$ for each $i = 1, \dots, k$.

Definition 5 (Piecewise Quasi-polynomials). A function $f : \mathbb{Z}^k \rightarrow \mathbb{Z}$ is a *piecewise quasi-polynomial* (PQP) if there is a partition of \mathbb{R}^k into finitely many pieces S_1, \dots, S_q , each defined by a conjunction of linear inequalities, such that for each i , f agrees with a multivariate quasi-polynomial on S_i .

Remark. Depending on the application, we often restrict the domain of our PQP to be, for example, $\mathbb{Z}_{\geq 0}^k$.

Remark. Geometrically, each piece S_i is either a bounded polytope or an unbounded polyhedron. If $k = 1$, the partition of $\mathbb{R}_{\geq 0}$ in the definition of a PQP $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}$ must contain exactly one unbounded polyhedron, and so f must agree with a quasi-polynomial for all sufficiently large t ; therefore, we call f an *eventual quasi-polynomial* (EQP).

Example 11. McDonald's burger options are a little confusing. You can buy a Double Cheeseburger, which has two patties and two slices of cheese. Or you can buy a McDouble, which is identical except it has only one slice of cheese. The difference in price is completely unpredictable. Of course, you could buy a Triple Cheeseburger, which has three patties and (obviously?) two slices of cheese. Feeling particularly peckish, you want to consume 14 patties and 9 slices of cheese. Can you order exactly this (ignoring the buns), using these three types of sandwiches? In how many ways? We leave it to the reader to find the 3 different ways this can be done and to compute the number of ways to order s patties and t slices of cheese, in general. The answer is a PQP! For example, if $s \leq 2t$, $2s \geq 3t$, and s is even, then there are $(2t - s + 2)/2$ ways.

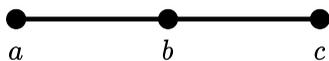
Again, this problem can be written as a conjunction of linear inequalities: if $x, y, z \in \mathbb{Z}$ are the number of Double Cheeseburgers, McDoubles, and Triple Cheeseburgers, respectively, then we must have $x, y, z \geq 0$, $2x + 2y + 3z = s$, and $2x + 1y + 2z = t$ (noting that an equality $=$ is just the conjunction of two inequalities \geq and \leq).

This example is a special case of the *vector partition function*, a multi-dimensional generalization of a Frobenius-style problem: for fixed vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{Z}_{\geq 0}^k$, given $\mathbf{t} \in \mathbb{Z}_{\geq 0}^k$, define $f(\mathbf{t})$ to be the number of nonnegative integer vectors $(\lambda_1, \dots, \lambda_n)$ such that $\sum_i \lambda_i \mathbf{v}_i = \mathbf{t}$ (we use bold notation to signify a vector). Then $f(\mathbf{t})$ will be a PQP [29]. In the example, we have $\mathbf{v}_1 = (2, 2)$, $\mathbf{v}_2 = (2, 1)$, and $\mathbf{v}_3 = (3, 2)$.

Where we stand. The sets we are defining have two types of variables, the *parameter* variables $\mathbf{t} \in \mathbb{Z}^k$ and the *counted* variables $\mathbf{x} \in \mathbb{Z}^n$. We define a parametric family of sets $S_{\mathbf{t}}$, and examine $f(\mathbf{t}) = |S_{\mathbf{t}}|$. In the examples so far, $S_{\mathbf{t}}$ is the set of $\mathbf{x} \in \mathbb{Z}^n$ such that the variables \mathbf{t}, \mathbf{x} satisfy a conjunction of linear inequalities (interestingly, \mathbf{t} and \mathbf{x} are indistinguishable in the linear inequalities; they are only distinguished when we decide to fix \mathbf{t} and look at the set, $S_{\mathbf{t}}$, of \mathbf{x} that these inequalities define). In this setup, we have seen examples where $f(\mathbf{t}) = |S_{\mathbf{t}}|$ is a PQP. This will always be true! See [2, §18], for example, where this is proved alongside Ehrhart's theorem.

4. BOOLEAN COMBINATIONS. Where to next? Once we start thinking of a polyhedron as a *conjunction* of linear inequalities, it seems natural to allow arbitrary boolean combinations. That is, we allow our linear inequalities to be joined together with any combination of logical operators: \wedge 's (and's), \vee 's (or's), and \neg 's (not's). This gives us some great examples of QP counting functions, many of which are not obviously geometric in nature.

Example 12. Let G be the graph with vertices a, b, c and two edges $\{a, b\}$ and $\{b, c\}$; see Figure 7a. The *chromatic polynomial*, $\chi_G(t)$, is the number of ways to color the vertices of G with t possible colors, so that no adjacent vertices have the same color. For this particular graph G , calculating that $\chi_G(t) = t(t - 1)^2$ is a standard exercise. (Hint: how many ways can you color a ? Now b ? Now c ?) But it also fits our current setup of boolean combinations of linear inequalities: if (x_a, x_b, x_c) are the colors of a, b , and c , respectively, with colors corresponding to the integers $1, 2, \dots, t$, then a



(a) The graph, G , in Example 12.

12	1	11
7	8	9
5	15	4

(b) A 24-magic square; see Example 13.

Figure 7.

coloring of G satisfies

$$(1 \leq x_a, x_b, x_c \leq t) \wedge \neg(x_a = x_b) \wedge \neg(x_b = x_c).$$

Chromatic polynomials, along with many other interesting examples, were first conceived in this way in [4] as the counting functions of *inside-out polytopes*.

Example 13. Define a t -magic square to be a way to fill a 3×3 grid with nine distinct positive integers such that the sum of every row, every column, and the two diagonals are all exactly t ; see Figure 7b for a 24-magic square. The number of t -magic squares depends on $t \pmod{18}$ (see [5] for this and many similar calculations); if t is not a multiple of 3, then there are no t -magic squares (can you prove it?). On the other hand, for example, if $t \equiv 6 \pmod{18}$, then there are $\frac{2}{9}(t-6)(t-10)$ such t -magic squares. Again a quasi-polynomial!

If x_{ij} is the number in the i th row and j th column, then we see that the set of t -magic squares can be defined as a boolean combination of linear inequalities. For example, we require $x_{11} \neq x_{12}$ and so on (all entries distinct), and $x_{11} + x_{12} + x_{13} = t$ and so on (all rows, columns, diagonals sum to t).

Example 14. How many ways are there to place three queens on an $t \times t$ board such that no two queens are attacking each other? This and many other formulas are calculated in [11]: there are

$$\frac{t^6}{6} - \frac{5t^5}{3} + \frac{79t^4}{12} - \frac{25t^3}{2} + 11t^2 - \frac{43t}{12} + \frac{1}{8} + (-1)^t \left(\frac{t}{4} - \frac{1}{8} \right)$$

ways, a QP of period 2. This problem falls into our setting! Let's momentarily label the queens 1, 2, 3 and count labeled ways to place them (and then divide by 6 since all permutations of the three queens are equivalent). Suppose we place Queen i at position $(x_i, y_i) \in \mathbb{Z}^2$ where $1 \leq x_i, y_i \leq t$. The nonattacking conditions are given by boolean combinations of linear inequalities; for example, $x_1 \neq x_2$ says that the first two queens can't be in the same row, and $x_1 - y_1 \neq x_2 - y_2$ says they cannot be along one of the same diagonals.

Where we stand. We can define our sets $S_{\mathbf{t}}$ using boolean combinations of linear inequalities in the parameters \mathbf{t} and counted variables \mathbf{x} . If $f(\mathbf{t})$ is the number of $\mathbf{x} \in S_{\mathbf{t}}$, then $f(\mathbf{t})$ will be PQP. Allowing boolean combinations opens up a wide variety of possible applications of these methods. Mathematically, however, there is not much new: boolean combinations may be converted into *disjunctive normal form*, that

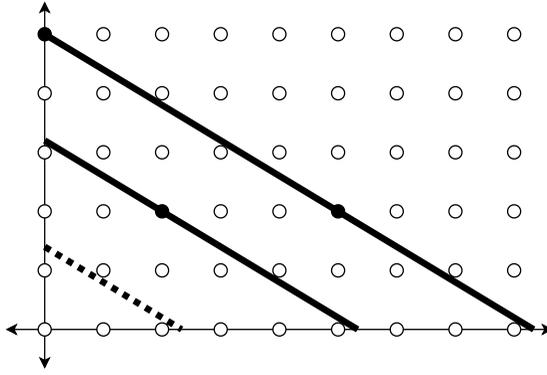


Figure 8. Diagonal line segments are $3x + 5y = n$, for $n = 7, 16, 25$, constrained by $x, y \geq 0$. We see that $7 \notin S$, because there are no integer points on the line segment. On the other hand $16 \in S$ and $25 \in S$; in fact, the two integer points for $n = 25$ correspond to two ways to write 25 using 3's and 5's: $25 = 0 \cdot 3 + 5 \cdot 5 = 5 \cdot 3 + 2 \cdot 5$. Furthermore, we can see the second quantifier elimination step used in Example 16: if there are some $x, y \in \mathbb{Z}_{\geq 0}$ with $3x + 5y = n$, then we may take y to be 0, 1, or 2; indeed, if (x, y) is on the line segment with $y \geq 3$, then $(x + 5, y - 3)$ is also on the line segment, e.g., $(0, 5)$ and $(5, 2)$ are on the line segment corresponding to $n = 25$.

is, written as a disjunction of conjunctions of linear inequalities, that is, a union of polyhedra. With a little care on the overlaps, we can rewrite such a set as a *disjoint* union of polyhedra, and therefore apply the old methods.

5. QUANTIFIERS. Where to next? Having allowed boolean combinations, we've set our list of allowed operations firmly in a logical realm. Adding quantifiers ($\exists x \in \mathbb{Z}$ and $\forall x \in \mathbb{Z}$) gives us a full first-order logic, such an important one that it has a name: *Presburger arithmetic* [22] (see [23] for a translation). The most obvious thing that allowing quantifiers buys us is that we may now define sets with regular gaps in them, such as the set of odd numbers:

Example 15. Given $t \in \mathbb{Z}_{\geq 0}$ define

$$S_t = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z}, x = 2y + 1 \wedge 0 \leq x \leq t\},$$

the set of odd integers between 0 and t . Happily, we still get quasi-polynomial behavior: $|S_t| = \lfloor (t + 1)/2 \rfloor$.

Allowing quantifiers definitely gives us a robust collection of sets we can now describe, and the good news is that we will still get quasi-polynomial behavior. The key is a process called *quantifier elimination*, explained nicely in [13]. For simplicity, we illustrate this method with an example that doesn't have any parameters.

Example 16. Suppose we want to understand the semigroup generated by 3 and 5,

$$\begin{aligned} S &= \{n \in \mathbb{Z} : \exists x, y \in \mathbb{Z}, (x \geq 0) \wedge (y \geq 0) \wedge (3x + 5y = n)\} \\ &= \{0, 3, 5, 6, 8, 9, 10, \dots\}; \end{aligned}$$

see Figure 8.

The quantifiers are the new complication here; we'd like to get rid of them, that is, describe S *without* needing to use quantifiers at all. Quantifier elimination is a

tool for doing this. We first get rid of the existential quantifier on x . This is pretty straightforward: if there is any integer x that works, it must be $x = (n - 5y)/3$, to make the equation $3x + 5y = n$ true. We need to be a little careful here: x must be an integer, so we must have $3|(n - 5y)$. In that case, we can simply substitute $x = (n - 5y)/3$ into the constraints: $x \geq 0$ becomes $(n - 5y)/3 \geq 0$, $y \geq 0$ stays the same, and $3x + 5y = n$ becomes the tautology $n = n$. After simplifying slightly, we have found a new way to express the semigroup:

$$S = \left\{ n \in \mathbb{Z} : \exists y \in \mathbb{Z}, 3|(n - 5y) \wedge (5y \leq n) \wedge (y \geq 0) \right\}.$$

At the minor cost of introducing the *divisibility predicate* $3|(n - 5y)$, the quantified variable x has been eliminated!

Let's try to eliminate y next. This is not quite as easy, since there is no equality that would say exactly what y must be. We instead ask ourselves, "If there exists *some* y that makes this true, what is the smallest y that works?" We claim that the smallest y must be 0, 1, or 2: indeed, exactly one of these will make $3|(n - 5y)$ true, these are the smallest y 's that might make $y \geq 0$ true, and to make $5y \leq n$ we actually *want* to choose y as small as possible (this is, if $y = i$ satisfies $5y \leq n$, then so does $i - 3$, $i - 6$, etc., and so either $y = 0$, $y = 1$, or $y = 2$ will satisfy it). In other words, we may replace this expression for S with one that has three cases (separated with or's), substituting $y = 0$, $y = 1$, and $y = 2$, respectively:

$$\begin{aligned} & \left(3|n \wedge (0 \leq n) \wedge (0 \geq 0) \right) \vee \left(3|(n - 5) \wedge (5 \leq n) \wedge (1 \geq 0) \right) \\ & \vee \left(3|(n - 10) \wedge (10 \leq n) \wedge (2 \geq 0) \right). \end{aligned}$$

The quantifiers are gone, leaving only the variable n . Wow! We can now apply all of the machinery that we had already built up for quantifier-free formulas. In this particular example, we have divided into three disjoint cases based on whether n is 0, 2, or 1 modulo 3, respectively:

$$S = \{0, 3, 6, \dots\} \sqcup \{5, 8, 11, \dots\} \sqcup \{10, 13, 16, \dots\},$$

and the set of nonnegative integers *not* in S is

$$\emptyset \sqcup \{2\} \sqcup \{1, 4, 7\}.$$

Thus $F(3, 5) = 7$ and $g(3, 5) = 4$ (see Definition 1). In fact, the pattern of quantifier elimination is fairly clear if we replace 3 and 5 by any relatively prime a and b : it will give us the decomposition of S based on its so-called *Apéry sets* [1] (and see [24] for much more):

$$S = \bigsqcup_{i=0}^{a-1} (bi + a\mathbb{Z}_{\geq 0}) \quad \text{and} \quad S^c = \bigsqcup_{i=0}^{a-1} \{bi - aj : 1 \leq j \leq \lfloor bi/a \rfloor\}.$$

The maximum element of S^c occurs when $i = a - 1$ and $j = 1$, and so $F(a, b) = b \cdot (a - 1) - a \cdot 1 = ab - a - b$. Less obviously, we also get $g(a, b) = (ab - a - b + 1)/2$. (Hint: pair the i and $a - i$ terms in this union together.) These formulas were first proved in [30].

Remark. The number of gaps $g(a, b)$ is a counting function as in all of our other examples, but the Frobenius number $F(a, b)$ has a slightly different character: it *specifies* the maximal element of the set of gaps. In general, we might want to do something like specify the maximal element of any of our families of one-dimensional sets S_t , or in higher dimensions specify an element that maximizes a given linear functional. The general results for specification problems are similar to those for counting problems, as we will see in Section 7.

Now we give an example that does have a parameter (three parameters!), for which we get a PQP counting function. This example could be analyzed with the same quantifier elimination tools as above (we will leave the reader to have fun with it).

Example 17. A particular McDonald’s location will have only a finite number of boxes of McNuggets available to buy. Suppose they have r boxes of 6, s boxes of 9, and t boxes of 20 available. How many different numbers of McNuggets could you buy? The answer will be PQP, since the set of possibilities can be defined with quantifiers, boolean combinations, and linear inequalities:

$$S_{r,s,t} = \{n \in \mathbb{Z} : \exists x, y, z \in \mathbb{Z}, \\ (0 \leq x \leq r) \wedge (0 \leq y \leq s) \wedge (0 \leq z \leq t) \wedge (n = 6x + 9y + 20z)\}.$$

Indeed, for r , s , and t sufficiently large, one can verify that there will be $6r + 9s + 20t - 43$ possibilities.

For an algebraic perspective that interprets functions like this as Hilbert polynomials, see [20].

Where we stand. We can define our sets S_t using quantifiers and boolean combinations of linear inequalities; there will now be three types of variables: the parameters \mathbf{t} , the counted variables \mathbf{x} , and the *bound* variables \mathbf{y} (those associated with a quantifier). If $f(\mathbf{t})$ is the number of $\mathbf{x} \in S_t$, then $f(\mathbf{t})$ will be PQP. The main tool is quantifier elimination, which reduces the problem to the previously understood quantifier-free case; see [32].

6. NONLINEARITY, WITH ONE PARAMETER VARIABLE. Where to next? For our last twist (pun intended), we must restrict ourselves to only one parameter t . Recalling prior polyhedral examples, changing t only caused a parallel shift of the facets of the polyhedra. Now we will allow the facets to “twist” by allowing the normal vectors to also depend on t .

Example 18. [31] Let P_t be the “twisting square” defined by

$$P_t = \left\{ (x, y) \in \mathbb{R}^2 : - (t^2 - 2t + 2) \leq 2x + (2t - 2)y \leq t^2 - 2t + 2, \right. \\ \left. - (t^2 - 2t + 2) \leq (2 - 2t)x + 2y \leq t^2 - 2t + 2 \right\};$$

see Figure 9. Then $|P_t \cap \mathbb{Z}^2|$ is given by the QP

$$|P_t \cap \mathbb{Z}^2| = \begin{cases} t^2 - 2t + 2 & \text{if } t \text{ odd,} \\ t^2 - 2t + 5 & \text{if } t \text{ even.} \end{cases}$$

We leave the proof that this formula for $|P_t \cap \mathbb{Z}^2|$ is correct as an exercise.

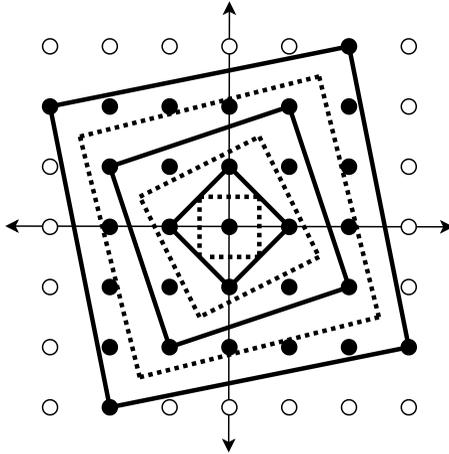


Figure 9. The twisting square P_t in Example 18, for $t = 1, 2, 3, 4, 5, 6$. Even t are in solid lines and odd t in dotted lines.

Remarkably, lattice-point counting functions are EQP (eventual quasi-polynomials, that is, quasi-polynomial for sufficiently large t) for all such families of twisting polytopes [12]. To be precise, this result applies to polytopes that can be written as conjunctions of inequalities of the form

$$a_1(t)x_1 + \cdots + a_d(t)x_d \leq b(t)$$

where $a_1(t), \dots, a_d(t), b(t)$ are polynomials in t with integer coefficients. That is, we no longer require our defining inequalities to be linear; we may now multiply by t with impunity. Indeed, we can do this, not only with polytopes, but with any formula built from quantifiers, boolean operations, and inequalities of the above form. This was conjectured in [31], proved in [7], and will be stated precisely in the next section. We first proceed with some examples.

For these first two examples, note that two very natural functions, integer division and gcd, can be expressed in this new language: if $f(t)$ and $g(t)$ are polynomials with integer coefficients, then $\lfloor f(t)/g(t) \rfloor$ is the largest $x \in \mathbb{Z}$ such that $g(t)x \leq f(t)$, and $\gcd(f(t), g(t))$ is the smallest $y \in \mathbb{Z}_{>0}$ such that

$$\exists a, b \in \mathbb{Z}, af(t) + bg(t) = y.$$

The next two examples illustrate how to see that $\lfloor f(t)/g(t) \rfloor$ and $\gcd(f(t), g(t))$ are indeed EQP functions.

Example 19. Let's evaluate $\lfloor \frac{t^2}{2t+3} \rfloor$. By polynomial division, we obtain

$$\frac{t^2}{2t+3} = \frac{t}{2} - \frac{3}{4} + \frac{9/4}{2t+3} = \frac{t-2}{2} + \left(\frac{1}{4} + \frac{9/4}{2t+3} \right).$$

For sufficiently large t , the term in parentheses is strictly between 0 and $\frac{1}{2}$, and thus

$$\left\lfloor \frac{t^2}{2t+3} \right\rfloor = \left\lfloor \frac{t-2}{2} \right\rfloor = \begin{cases} \frac{t-2}{2} & \text{if } t \equiv 0 \pmod{2}, \\ \frac{t-3}{2} & \text{if } t \equiv 1 \pmod{2} \end{cases}$$

for all $t \geq 4$ (but not for $t = 1$ or $t = 3$).

Example 20. Let's calculate $\gcd(t^2 + 1, 2t - 1)$. A natural way to do this is to use the Euclidean algorithm, and the previous example shows that the quotients and remainders are all EQPs, so this algorithm must work to calculate the gcd as an EQP. In this example, we divide $2t - 1$ into $t^2 + 1$ and immediately see that our answer must depend on $t \pmod 2$. Let's look at even t , so $t = 2u$ for some $u \in \mathbb{Z}$, $t^2 + 1 = 4u^2 + 1$, and $2t - 1 = 4u - 1$. The Euclidean algorithm yields

$$\begin{aligned} 4u^2 + 1 &= u(4u - 1) + (u + 1) \\ 4u - 1 &= 4(u + 1) - 5, \end{aligned}$$

and so

$$\gcd(4u^2 + 1, 4u - 1) = \gcd(u + 1, 5) = \begin{cases} 5 & \text{if } u \equiv 4 \pmod{5}, \\ 1 & \text{otherwise.} \end{cases}$$

Note that $u \equiv 4 \pmod{5}$ corresponds to $t \equiv 2 \cdot 4 \equiv 3 \pmod{5}$. We leave the reader to try the case where t is odd, which turns out to give the same answer: regardless of parity, we have

$$\gcd(t^2 + 1, 2t - 1) = \begin{cases} 5 & \text{if } t \equiv 3 \pmod{5}, \\ 1 & \text{otherwise.} \end{cases}$$

Let's finally tackle our teaser problem from Section 1, to compute $F(t, t + 1, t + 3)$ and $g(t, t + 1, t + 3)$, the Frobenius number and number of gaps for the semigroup generated by t , $t + 1$, and $t + 3$, as defined in Definition 1. These problems involve most of the twists we have introduced; in particular, they require both quantifiers and multiplication of the parameter variable t by other variables.

Example 21. Define the semigroup S_t to be the set of integers n such that

$$\exists x, y, z \in \mathbb{Z}_{\geq 0}, tx + (t + 1)y + (t + 3)z = n.$$

We'll just do the first step for calculating $F(t, t + 1, t + 3)$ and $g(t, t + 1, t + 3)$, which requires a new technique, the "base t " method from [12]. The remainder of the computation will be doable with techniques from previous sections, but it would be calculation intensive. Note that for all $n \geq t^2$, we have $n \in S_t$ (indeed $F(t, t + 1) = t(t + 1) - t - (t + 1) = t^2 - t - 1$ already, so everything larger than $t^2 - t - 1$ must be in S_t). So we concentrate on $n < t^2$, and we write n in "base t ," that is, $n = at + b$ with $0 \leq a, b < t$. Also note that $0 \leq x, y, z < t$ must be true in our defining equation, $tx + (t + 1)y + (t + 3)z = n$ (or else $n \geq t^2$). We rearrange our defining equation:

$$t(x + y + z) + (y + 3z) = n = at + b.$$

Note that if $y + 3z < t$, then the left-hand side must be a "base t expression" (a polynomial in t with coefficients between 0 and $t - 1$); this would mean that our expression simplifies to

$$(x + y + z = a) \wedge (y + 3z = b).$$

Of course, $y + 3z$ need not be less than t , but we do know it is less than $t + 3t = 4t$ (since $y < t$ and $z < t$); this suggests breaking into four cases: $0 \leq y + 3z < t$, $t \leq y + 3z < 2t$, $2t \leq y + 3z < 3t$, and $3t \leq y + 3z < 4t$. These cases can be analyzed one by one; for example, if $2t \leq y + 3z < 3t$, then

$$t(x + y + z + 2) + (y + 3z - 2t) = at + b$$

is a base t expression, meaning $a = x + y + z + 2$ and $b = y + 3z - 2t$. Combining all of this together, the set $S_t \cap [0, t^2)$ is in bijection with the set of (a, b) (under the map $(a, b) \mapsto at + b$) such that

$$\begin{aligned} \exists x, y, z \in \mathbb{Z}, (0 \leq a, b, x, y, z < t) \\ \wedge \bigvee_{i=0}^3 \left((a = x + y + z + i) \wedge (b = y + 3z - it) \right). \end{aligned}$$

This is getting too ugly to want to continue analyzing, but we could. No variables in this expression are multiplied by $t!$ (Remember that i is just one of the constants $0, 1, 2, 3$.) The next step would be to eliminate the quantifiers, and we will find $F(t, t + 1, t + 3)$ and $g(t, t + 1, t + 3)$ as EQP functions. See the teaser in Section 1 for the final answer.

In addition to the Frobenius number and the number of gaps, many other invariants of parametric semigroups have recently been studied; see [17, 18, 19], for example. The connection of these *parametric semigroups* to the methods we are describing here was explored in [9].

7. STATEMENT OF THEOREMS. In this section, we state everything precisely. Recall the definitions of quasi-polynomial (QP) and piecewise quasi-polynomial (PQP) functions of several parameters (Definitions 4 and 5). Recall that, with a single parameter t , PQP is more conveniently conceived of as *eventually quasi-polynomial* (EQP): that is, agreeing with a quasi-polynomial for sufficiently large values of t .

Definition 6. We say that a subset $T \subseteq \mathbb{Z}^k$ is *piecewise periodic* if

$$\chi_T(\mathbf{t}) = \begin{cases} 1 & \text{if } \mathbf{t} \in T, \\ 0 & \text{else} \end{cases}$$

is PQP, that is, if T is a finite union of intersections of lattice cosets and polyhedra. With $k = 1$, this simply means that the set T is eventually periodic.

In general, let $S_{\mathbf{t}}$, for $\mathbf{t} \in \mathbb{Z}^k$, be a family of subsets of \mathbb{Z}^d and consider the following properties (of a quasi-polynomial nature) that $S_{\mathbf{t}}$ might have.

Property 1. The set of \mathbf{t} such that $S_{\mathbf{t}} \neq \emptyset$ is piecewise periodic.

Property 2. There exists a PQP $g : \mathbb{Z}^k \rightarrow \mathbb{Z}$ such that, if $S_{\mathbf{t}}$ has finite cardinality, then $g(\mathbf{t}) = |S_{\mathbf{t}}|$. The set of \mathbf{t} such that $S_{\mathbf{t}}$ has finite cardinality is piecewise periodic.

Property 3. There exists a function $\mathbf{x} : \mathbb{Z}^k \rightarrow \mathbb{Z}^d$, whose coordinate functions are PQPs, such that, if $S_{\mathbf{t}}$ is nonempty, then $\mathbf{x}(\mathbf{t}) \in S_{\mathbf{t}}$. The set of \mathbf{t} such that $S_{\mathbf{t}}$ is nonempty is piecewise periodic.

Property 3a. Given $\mathbf{c} \in \mathbb{Z}^d \setminus \{0\}$, there exists a function $\mathbf{x} : \mathbb{Z}^k \rightarrow \mathbb{Z}^d$, whose coordinate functions are PQPs, such that if $\max_{\mathbf{y} \in S_{\mathbf{t}}} \mathbf{c} \cdot \mathbf{y}$ exists, then it is attained at $\mathbf{x}(\mathbf{t}) \in S_{\mathbf{t}}$. The set of \mathbf{t} such that the maximum exists is piecewise periodic.

Property 3b. Fix $n \in \mathbb{Z}_{>0}$. There exist functions $\mathbf{x}_1, \dots, \mathbf{x}_n : \mathbb{Z}^k \rightarrow \mathbb{Z}^d$, whose coordinate functions are PQPs, such that if $|S_{\mathbf{t}}| \geq n$, then $\mathbf{x}_1(\mathbf{t}), \dots, \mathbf{x}_n(\mathbf{t})$ are distinct elements of $S_{\mathbf{t}}$. The set of \mathbf{t} such that $|S_{\mathbf{t}}| \geq n$ is piecewise periodic.

Property 2 is designed for counting problems, while Properties 3, 3a, and 3b apply to various types of specification problems. Property 1 is a more fundamental property about nonemptiness, important in its own right, but also needed for the other definitions.

Now we define some families, $S_{\mathbf{t}}$, that we might hope have these properties. These families are crafted using *quantification over integers* ($\exists x \in \mathbb{Z}$ or $\forall x \in \mathbb{Z}$, where x is one of the nonparameter variables, \mathbf{x}) and *boolean combinations* (stringing together simpler formulas using the logical operations and, or, not). First, consider the sets with multiple parameters that we had defined up through Section 5:

Definition 7. A *Presburger family* is a collection $\{S_{\mathbf{t}} : \mathbf{t} \in \mathbb{Z}^k\}$ of subsets of \mathbb{Z}^d that can be defined by quantifying a boolean combination of formulas of the form $\mathbf{a} \cdot \mathbf{x} \leq b + \mathbf{c} \cdot \mathbf{t}$, where $b, \mathbf{a}, \mathbf{c}$ are constants with integer coordinates.

Next, consider the family of sets where we restricted to one parameter variable, but we allowed nonlinearity in that parameter, as in Section 6:

Definition 8. A *1-parametric Presburger family* is a collection $\{S_t : t \in \mathbb{Z}\}$ of subsets of \mathbb{Z}^d that can be defined by quantifying a boolean combination of formulas of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $b(t), \mathbf{a}(t)$ have coordinates in $\mathbb{Z}[t]$.

Our two main theorems say that these families have everything we could possibly want!

Theorem 2. A Presburger family $S_{\mathbf{t}}$ has all of the Properties 1, 2, 3, 3a, and 3b.

This is proved in [32]; Properties 3/3a/3b do not appear there, but they follow immediately from the techniques presented in [31].

Theorem 3. A 1-parametric Presburger family S_t has all of the Properties 1, 2, 3, 3a, and 3b.

This is proved in [7]. Both Presburger families and 1-parametric Presburger families also have certain generating function properties that we will not discuss here; see [7, 31, 32].

8. GOING TOO FAR. Where to next? It's not so clear. Here are two options for generalizing that lead to problems: allow a second (nonlinear) parameter or allow nonlinearity in the nonparameter variables.

Example 22. [31] Let $f(s, t)$ be the number of $(x, y) \in \mathbb{Z}_{\geq 0}^2$ such that $sx + ty = st$. This has two nonlinear parameters, s and t , and it defines the interval in \mathbb{Z}^2 with endpoints $(0, s)$ and $(t, 0)$; see Figure 10. So $f(s, t) = \gcd(s, t) + 1$, which is a very nonpolynomial function.

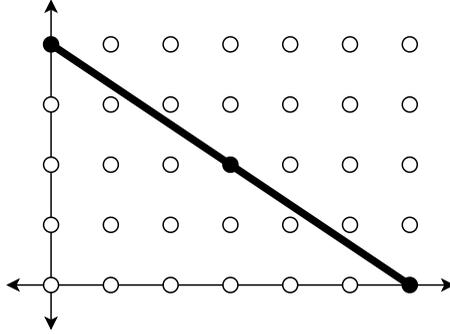


Figure 10. Taking $s = 4$ and $t = 6$ in Example 22, we examine the line segment of $x, y \geq 0$ such that $4x + 6y = 4 \cdot 6$, which has endpoints $(0, 4)$ and $(6, 0)$. Therefore $f(4, 6) = 3 = \gcd(4, 6) + 1$.

Example 23. [31] Let $f(t)$ be the number of $x \in \mathbb{Z}_{\geq 0}$ such that $\exists y \in \mathbb{Z}_{\geq 0}, xy = t$. This is nonlinear in x and y , and $f(t)$ is the number of divisors of t , which is a very nonpolynomial function.

We should step back and be thankful that nonlinearity in a parameter variable ended up so nicely (we will discuss a little bit of why we think it ended up so nicely in Section 10). Allowing nonlinearity is extremely dangerous, so be careful! Allowing such expressiveness rapidly approaches the domain of Gödel's first incompleteness theorem:

Example 24. Let $p(x_0, \dots, x_d)$ be a polynomial, and define $f_p(t)$ to be the number of $(x_1, \dots, x_d) \in \mathbb{Z}^d$ such that $p(t, x_1, \dots, x_d) = 0$. A consequence of the DPRM theorem (see [14]), which solves Hilbert's 10th problem in the negative, is that there exists a specific polynomial p such that $f_p(t)$ is not computable (and indeed, that figuring out whether $f_p(t) = 0$ is undecidable.)

9. NOT FAR ENOUGH? But we shouldn't give up so easily. One might look for other natural problems that, though they do not seem to fit into the domain of parametric Presburger arithmetic, do still yield EQP results:

Example 25. For $t \in \mathbb{Z}_{\geq 0}$, let $P_t \subseteq \mathbb{Z}^d$ be a polytope defined by linear equations of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $\mathbf{a} : \mathbb{Z} \rightarrow \mathbb{Z}^d$ and $b : \mathbb{Z} \rightarrow \mathbb{Z}$ have polynomial coordinates. It has been shown that there is an EQP function $\mathbf{v} : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}^d$ such that $\mathbf{v}(t)$ is a vertex of the convex hull of $P_t \cap \mathbb{Z}^d$ [10, 28]; see, for example, Figure 11. A natural way to specify such a \mathbf{v} would be

$$(\mathbf{v} \in P_t \cap \mathbb{Z}^d) \wedge \exists \mathbf{z} \in \mathbb{Z}^d, \forall \mathbf{x} \in P_t \cap \mathbb{Z}^d, (\mathbf{x} = \mathbf{v}) \vee (\mathbf{z} \cdot \mathbf{x} < \mathbf{z} \cdot \mathbf{v}).$$

Note that writing $\mathbf{z} \cdot \mathbf{x}$ and $\mathbf{z} \cdot \mathbf{v}$ puts us outside of the domains of Presburger arithmetic and 1-parametric Presburger arithmetic, and yet we still get an EQP specification function.

Example 26. For $t \in \mathbb{Z}_{\geq 0}$, let $\Lambda_t \subseteq \mathbb{Z}^d$ be the lattice generated by $\mathbf{b}_1(t), \dots, \mathbf{b}_d(t)$, where the \mathbf{b}_i have polynomial coordinates. Then there is an EQP function $\mathbf{v} : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}^d$ such that $\mathbf{v}(t)$ is the shortest (in the Euclidean norm) nonzero vector in Λ_t [8]. Comparing Euclidean norms of vectors seems to require nonlinearity, since $\|\mathbf{v}\|^2 =$

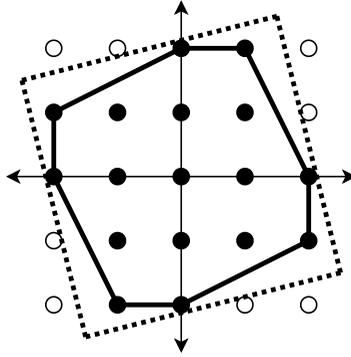


Figure 11. The integer hull (solid line) of P_5 (dotted line), in Example 18 (cf., Figure 9). When t is odd, the integer hull of P_t is an octagon with vertices $(0, \pm \frac{t-1}{2}), (\pm \frac{t-3}{2}, \pm \frac{t-1}{2}), (\pm \frac{t-1}{2}, 0), (\pm \frac{t-1}{2}, \mp \frac{t-3}{2})$. When t is even, the vertices of P_t are integers, so the vertices of the integer hull are simply the vertices of P_t : $(\pm \frac{t-2}{2}, \pm \frac{t}{2})$ and $(\pm \frac{t}{2}, \mp \frac{t-2}{2})$; see Example 25.

$\sum_i v_i^2$. So again we seem to have left the domains of Presburger arithmetic and 1-parametric Presburger arithmetic, and yet we still get an EQP function.

In both of these examples, additional tools (specific to each problem) are required to prove EQP properties.

Question. Is there a common generalization: some larger class of problems whose answer can be shown to be EQP?

Another way to generalize might be to allow two nonlinear parameters, accept that we won't get EQP functions, but still hope that our functions are "nice" somehow. For example, the lcm function pops up in some simple examples:

Example 27. Let's further define the Frobenius problem for generators that are not relatively prime. Let $F(a_1, \dots, a_d)$ be the largest element of $a_1\mathbb{Z} + \dots + a_d\mathbb{Z}$ that is not in the semigroup generated by a_1, \dots, a_d . Then

$$F(a_1, a_2) = \text{lcm}(a_1, a_2) - a_1 - a_2.$$

What a nice function!

Question. Can we generalize to other 2-parametric Presburger families?

In full generality, the answer is an emphatic "No!"; not all 2-parametric families have cardinalities that are nice functions. The proof of this acknowledges that deciding what functions are "nice" is hard, but asks us to believe that nice functions can at least be computed in polynomial time (in a theoretical computer science sense; polynomials, QPs, and lcms, for example, can be evaluated in polynomial time). Assuming $P \neq NP$, *there exists a specific 2-parametric family $S_{s,t}$ whose cardinality cannot be computed in polynomial time in the size of the input s and t* [6].

On the other hand, if we are only allowed equalities rather than inequalities, then it turns out that functions related to lcm, gcd, and the extended Euclidean algorithm do suffice to describe all counting functions, for any number of nonlinear parameters [6] (as usual, the nonparameter variables must be linear, or we would run into Gödel-like problems quickly).

10. WHY EQP? To conclude, we would like to philosophize about why piecewise/eventual quasi-polynomials show up in so many counting problems related to discrete geometry.

First of all, why not simply polynomials? Well, even a simple formula like $0 \leq 2x \leq t$ immediately requires some periodicity, with functions like $\lfloor t/2 \rfloor$, so we would expect quasi-polynomials to appear fairly often.

So why not simply QPs? Well, with one parameter, simple formulas like $0 \leq (3t + 2)x \leq t^2$ will require us to calculate floor functions, like $\lfloor t^2/(3t + 2) \rfloor$, that are only quasi-polynomial for sufficiently large t . Or we might have to decide which of two polynomials, like $t^2 + 10$ and $2t^2 - 5$, is larger, which will depend on whether t is sufficiently large. So we would expect EQPs to appear fairly often. With more than one parameter, we immediately see examples like the trapezoid/triangle phenomenon in Example 10; the combinatorial structure changes as the parameters change, and so we need piecewise quasi-polynomials.

The bigger question is why EQP functions suffice for so many counting problems. This seems to follow directly from the fact that the floor of a rational function, $\lfloor f(t)/g(t) \rfloor$, is EQP. The floor function is the basis of many operations that we might need to undertake, such as the gcd operation. Algebraically, any finitely generated ideal in the ring of EQPs is principal [12] (such a ring is called a *Bezout domain*). While the ring of integer-valued polynomials and the ring of QPs are not closed under some very natural operations, the ring of EQPs is.

This also helps us see why problems with two parameters can get rapidly hard.

Question. What kind of function is $\lfloor \frac{t^2+st+3s+7}{t-s} \rfloor$? Can it be simplified in any reasonable way, in the sense that $\lfloor f(t)/g(t) \rfloor$ can be simplified to an EQP? We invite the reader to explore!

ACKNOWLEDGMENTS. We thank John Goodrick, Danny Nguyen, and Chris O'Neill for useful discussions as we were writing this paper. We also appreciate the reviewers' careful reading and helpful comments.

REFERENCES

1. Apéry, R. (1946). Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris.* 222: 1198–1200.
2. Barvinok, A. (2008). *Integer Points in Polyhedra*. Zürich: European Mathematical Society.
3. Beck, M., Robins, S. (2007). *Computing the Continuous Discretely: Integer-point Enumeration in Polyhedra*. New York: Springer.
4. Beck, M., Zaslavsky, T. (2006). Inside-out polytopes. *Adv. Math.* 205(1): 134–162.
5. Beck, M., Zaslavsky, T. (2010). Six little squares and how their numbers grow. *J. Integer Seq.* 13(6): Article 10.3.8.
6. Bogart, T., Goodrick, J., Nguyen, D., Woods, K. (2019). Parametric Presburger arithmetic: complexity of counting and quantifier elimination. *Math. Log. Q.* 65(2): 237–250.
7. Bogart, T., Goodrick, J., Woods, K. (2017). Parametric Presburger arithmetic: logic, combinatorics, and quasi-polynomial behavior. *Discrete Anal.* 2017: Paper No. 4, 34 pp.
8. Bogart, T., Goodrick, J., Woods, K. (2020). A parametric version of LLL and some consequences: parametric shortest and closest vector problems. *SIAM J. Discrete Math.* 34(4): 2363–2387.
9. Bogart, T., Goodrick, J., Woods, K. (2020). Periodic behavior in families of numerical and affine semi-groups via parametric Presburger arithmetic. *Semigroup Forum.* to appear.
10. Calegari, D., Walker, A. (2013). Integer hulls of linear polyhedra and scl in families. *Trans. Amer. Math. Soc.* 365(10): 5085–5102.
11. Chaiken, S., Hanusa, C. R. H., Zaslavsky, T. (2020). A q -queens problem V. some of our favorite pieces: queens, bishops, rooks, and nightriders. *J. Korean Math. Soc.* 57(6): 1407–1433.
12. Chen, S., Li, N., Sam, S. V. (2012). Generalized Ehrhart polynomials. *Trans. Amer. Math. Soc.* 364(1): 551–569.

13. Cooper, D. (1972). Theorem proving in arithmetic without multiplication. *Machine Intelligence*. 7: 91–99.
14. Davis, M. (1973). Hilbert’s tenth problem is unsolvable. *Amer. Math. Monthly*. 80(3): 233–269.
15. Ehrhart, E. (1962). Sur les polyèdres homothétiques bordés à n dimensions. *C. R. Acad. Sci. Paris*. 254: 616–618.
16. Ehrhart, E. (1977). *Polynômes Arithmétiques et Méthode des Polyèdres en Combinatoire*. Basel-Stuttgart: Birkhäuser Verlag.
17. Garcia, S. R., Omar, M., O’Neill, C., Wesley, T. (2020). Factorization length distribution for affine semigroups III: modular equidistribution for numerical semigroups with arbitrarily many generators. arXiv preprint arxiv.org/abs/2006.00121.
18. Garcia, S. R., Omar, M., O’Neill, C., Yih, S. (2021). Factorization length distribution for affine semigroups II: asymptotic behavior for numerical semigroups with arbitrarily many generators. *J. Combin. Theory Ser. A*. 178: 105358.
19. Garcia, S. R., O’Neill, C., Yih, S. (2019). Factorization length distribution for affine semigroups I: numerical semigroups with three generators. *European J. Combin.* 78: 190–204.
20. Khovanskii, A. G. (1992). The Newton polyhedron, the Hilbert polynomial and sums of finite sets. *Funktsional. Anal. i Prilozhen.* 26(4): 57–63.
21. Pick, G. (1899). Geometrisches zur Zahlenlehre. *Sitzber. Lotos (Prague)*. 19: 311–319.
22. Presburger, M. (1929). 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 Mathématiciens des Pays Slaves*.
23. Presburger, M. (1991). 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. Translated from the German and with commentaries by Dale Jacquette.
24. Ramírez Alfonsín, J. L. (1996). Complexity of the Frobenius problem. *Combinatorica*. 16(1): 143–147.
25. Ramírez Alfonsín, J. L. (2005). *The Diophantine Frobenius Problem*. Oxford: Oxford UP.
26. Roune, B. H., Woods, K. (2015). The parametric Frobenius problem. *Electron. J. Combin.* 22(2): Paper 2.36, 16 pp.
27. Shen, B. (2015). The parametric Frobenius problem and parametric exclusion. arXiv preprint arxiv.org/abs/1510.01349.
28. Shen, B. (2018). Parametrizing an integer linear program by an integer. *SIAM J. Discrete Math.* 32(1): 173–190.
29. Sturmfels, B. (1995). On vector partition functions. *J. Combin. Theory Ser. A*. 72(2): 302–309.
30. Sylvester, J. J. (1884). Mathematical questions with their solutions. *Educational Times*. 41(21): 171–178.
31. Woods, K. (2014). The unreasonable ubiquitousness of quasi-polynomials. *Electron. J. Combin.* 21(1): Paper 1.44, 23 pp.
32. Woods, K. (2015). Presburger arithmetic, rational generating functions, and quasi-polynomials. *J. Symb. Log.* 80(2): 433–449.

TRISTRAM BOGART received his Ph.D. from the University of Washington in 2007. After post docs at Queen’s University and MSRI / San Francisco State University, he moved to Los Andes University in Bogotá, Colombia, where he is now an Associate Professor of Mathematics.

Departamento de Matemáticas, Universidad de los Andes, Bogotá, Colombia
tc.bogart22@uniandes.edu.co

KEVIN WOODS received his Ph.D. from the University of Michigan in 2004. After a post doc at the University of California, Berkeley, he moved to Oberlin College in 2006, and he is now a Professor of Mathematics there. He is happiest when he is with his dogs or is taking long walks, but he is sad that his dogs cannot keep up on these long walks.

Department of Mathematics, Oberlin College, Oberlin, OH 44074
Kevin.Woods@oberlin.edu