Parametric Presburger Arithmetic: Logic, Combinatorics, and Quasi-polynomial Behavior

Tristram Bogart*   John Goodrick†   Kevin Woods

Abstract: Parametric Presburger arithmetic concerns families of sets $S_t \subseteq \mathbb{Z}^d$, for $t \in \mathbb{N}$, that are defined using addition, inequalities, constants in $\mathbb{Z}$, Boolean operations, multiplication by t, and quantifiers on variables ranging over $\mathbb{Z}$. That is, such families are defined using quantifiers and Boolean combinations of formulas of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $\mathbf{a}(t) \in \mathbb{Z}[t]^d, b(t) \in \mathbb{Z}[t]$. A function $g : \mathbb{N} \to \mathbb{Z}$ is a quasi-polynomial if there exists a period m and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that $g(t) = f_i(t)$, for $t \equiv i \bmod m$.

Recent results of Chen, Li, Sam; Calegari, Walker; Roune, Woods; and Shen concern specific families in parametric Presburger arithmetic that exhibit quasi-polynomial behavior. For example, $|S_t|$ might be a quasi-polynomial function of t or an element $\mathbf{x}(t) \in S_t$ might be specifiable as a function with quasi-polynomial coordinates, for sufficiently large t. Woods conjectured that all parametric Presburger sets exhibit this quasi-polynomial behavior. Here, we prove this conjecture, using various tools from logic and combinatorics.

Key words and phrases: Presburger arithmetic, quasi-polynomials, lattice points, Ehrhart polynomials

1 Introduction

We examine a broad class of problems that exhibit *quasi-polynomial* behavior.

Definition 1.1. A function $g : \mathbb{N} \to \mathbb{Z}$ is a *quasi-polynomial* if there exists a period m and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that

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

A function $g : \mathbb{N} \to \mathbb{Z}$ is an *eventual quasi-polynomial*, abbreviated *EQP*, if it agrees with a quasi-polynomial for sufficiently large t. (In this paper, we take $\mathbb{N} = \{0, 1, 2, \ldots\}$.)

Example 1.2.

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

is a quasi-polynomial with period 2.

In [19], Woods noticed that several recent results concern different kinds of EQP behavior in combinatorially defined families. For example, given a family of sets $S_t \subseteq \mathbb{Z}^d$ for $t \in \mathbb{N}$, $|S_t|$ might be an EQP function of t or an element $\mathbf{x}(t) \in S_t$ might be specifiable as a function with EQP coordinates. These results are all concerned with the following types of sets [19]:

Definition 1.3. Given $d \in \mathbb{N}$, a *parametric Presburger family* is a collection $\{S_t : t \in \mathbb{N}\}$ of subsets of $\mathbb{Z}^d$ which can be defined by a formula using addition, inequalities, multiplication and addition by constants from $\mathbb{Z}$, Boolean operations (and, or, not), multiplication by t, and quantifiers ($\forall$, $\exists$) on variables ranging over $\mathbb{Z}$. That is, such families are defined using quantifiers and Boolean combinations of formulas of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $\mathbf{a}(t) \in \mathbb{Z}[t]^d, b(t) \in \mathbb{Z}[t]$.

In Section 1.1, we give a number of examples of parametric Presburger families, and discuss their previously known EQP behavior. Note that, for fixed t, a formula $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$ is simply a linear inequality; as t changes, the half-space that this linear inequality defines both shifts (as $b(t)$ changes) and rotates (as $\mathbf{a}(t)$ changes). It is important to emphasize that we do not allow quantifiers $\exists t$ or $\forall t$ applied to the parameter t.

In [19], Woods conjectured that these parametric Presburger families always have EQP behavior. In this paper, we prove this conjecture. After seeing several examples in Section 1.1, we state this theorem precisely in Section 1.2.

1.1 Examples

Example 1.4. Let S_t be the set of integer points, $\mathbf{x} \in \mathbb{Z}^d$, in a parametric polyhedron defined by a conjunction of linear inequalities of the form $\mathbf{a} \cdot \mathbf{x} \leq tb$, where $\mathbf{a} \in \mathbb{Z}^d$ and $b \in \mathbb{Z}$. That is, $S_t = tP \cap \mathbb{Z}^d$ for some rational polyhedron $P \subseteq \mathbb{R}^d$.

Ehrhart proved [5] that $|S_t|$ (if finite) is a quasi-polynomial, with a period given by the smallest m such that mP has integer vertices. This is the classic quasi-polynomial result; see the book [1] by Beck and Robins for a proof and many examples of its utility. As a concrete example:

Example 1.5. 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

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

is a quasi-polynomial with period 2.

Figure 1: The twisting square P_t from Example 1.6.

(a) P_t for $t = 1, \ldots, 5$.　　　　　(b) Integer hull of P_5.
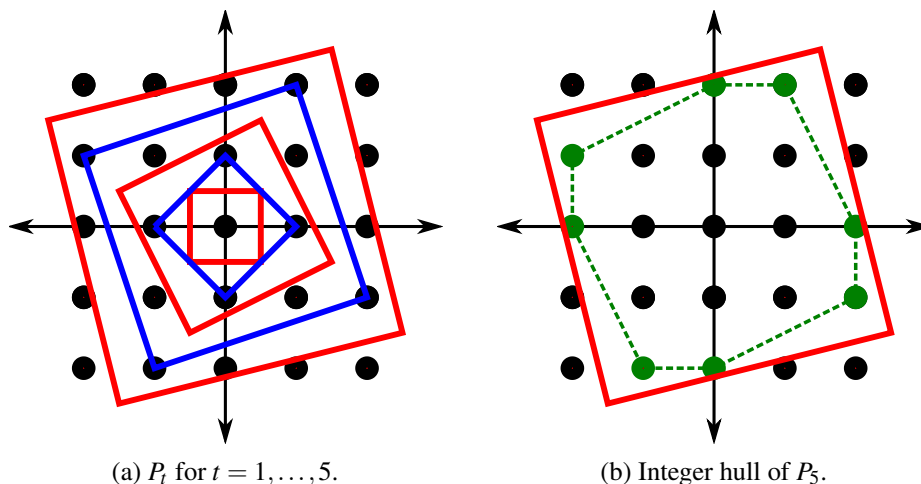
More recently, Chen, Li, and Sam proved [3] that $|S_t|$ is still an EQP, even if the normal vectors in the linear inequalities are allowed to vary with t, that is, if they are of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$, where $\mathbf{a}(t) \in \mathbb{Z}[t]^d, b(t) \in \mathbb{Z}[t]$.

For a concrete example:

Example 1.6. Let P_t be the "twisting square" in Figure 1a, defined by

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

Then $|P_t \cap \mathbb{Z}^2|$ is given by the quasi-polynomial

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

Calegari and Walker were similarly concerned [2] with the integer points in a polyhedron, P_t, defined by linear inequalities of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$. Rather than counting $|P_t \cap \mathbb{Z}^d|$, they wanted to find the vertices of the integer hull of P_t, that is, the vertices of the convex hull of $P_t \cap \mathbb{Z}^d$.

Example 1.7. Consider the twisting square, P_t, from Example 1.6. 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:

$$\left(\pm \frac{t-2}{2}, \pm \frac{t}{2} \right) \quad \text{and} \quad \left(\pm \frac{t}{2}, \mp \frac{t-2}{2} \right).$$

When t is odd, the integer hull of P_t is an octagon (pictured in Figure 1b for $t = 5$) with vertices

$$\left(0, \pm \frac{t-1}{2} \right), \left(\pm \frac{t-3}{2}, \pm \frac{t-1}{2} \right), \left(\pm \frac{t-1}{2}, 0 \right), \left(\pm \frac{t-1}{2}, \mp \frac{t-3}{2} \right).$$

Abstracting from the last example, the following turns out to be true (first proved by Calegari and Walker [2] under an additional hypothesis on P_t, later proved in general by Shen [17]):

Theorem 1.8. *Suppose that $P_t \subseteq \mathbb{R}^d$ is a family of polyhedra defined by a finite conjunction of linear inequalities $\mathbf{a}(t) \cdot \mathbf{x} \le b(t)$ where $\mathbf{a} \in \mathbb{Z}[t]^d$, $b \in \mathbb{Z}[t]$, and that every P_t is bounded. Then there exists a modulus m and functions $\mathbf{p}_{ij} : \mathbb{N} \to \mathbb{Z}^d$ with polynomial coordinates such that, for $0 \le i < m$ and for sufficiently large $t \equiv i \bmod m$, the set of vertices of the integer hull of $P_t \cap \mathbb{Z}^d$ is $\{\mathbf{p}_{i1}(t), \mathbf{p}_{i2}(t), \ldots, \mathbf{p}_{ik_i}(t)\}$.*

Another recent EQP result involves the Frobenius number:

Definition 1.9. Given $a_1, \ldots, a_d \in \mathbb{N}$, let S be the semigroup generated by the a_i, that is,

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

Note the heavy use of quantifiers in this definition, demonstrating that parametric Presburger arithmetic is a natural setting. 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. This is easily encoded in Presburger arithmetic as the (unique) element $x \in \mathbb{N}$ satisfying

$$x \notin S \wedge \forall y \in \mathbb{Z} \, (y \notin S \to y \le x).$$

Now we let $a_i = a_i(t)$ vary with t. Roune and Woods proved [14], in a few special cases, that the Frobenius number is an EQP. More recently, Shen [16] proved that this is always true for any eventually positive $a_i \in \mathbb{Z}[t]$.

Example 1.10. Let $a_1(t) = t$, $a_2(t) = t+1$, and $a_3(t) = t+2$. Then the Frobenius number is

$$\left(\left\lfloor \frac{t-2}{2} \right\rfloor + 1 \right) t - 1.$$

This is a running example in [14].

One more example (from [19]) concisely shows the sort of EQP behavior that may appear:

Example 1.11. 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

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

This set has several properties, which we will formalize in Section 1.2:

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

$$|S_t| = \begin{cases} \lfloor \frac{5t-3}{4} \rfloor - t & \text{if } t \text{ odd}, t \ge 3, \\ 0 & \text{else,} \end{cases}$$

   which is eventually a quasi-polynomial of period 4.

3. When S_t is nonempty, we can obtain an element of (indeed, 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.

Here are two examples that show that our precise definition of parametric Presburger families is important in order to get EQP behavior:

Example 1.12. The family

$$S_t = \{x \in \mathbb{Z} : \exists y [y \geq 0 \wedge xy = t]\}$$

is not a parametric Presburger family, because two variables (neither of which are the parameter, t) are multiplied together. Indeed, $|S_t|$ is the number of nonnegative divisors of t, which is not an EQP function in t.

Example 1.13. The family

$$S_{s,t} = \left\{ (x,y) \in \mathbb{Z}^2 : x \geq 0 \wedge y \geq 0 \wedge sx + ty = st \right\}$$

has two parameters, $s,t \in \mathbb{N}$. $S_{s,t}$ is an interval in $\mathbb{Z}^2$ with endpoints $(t,0)$ and $(0,s)$, and

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

For a *fixed s*, this is an EQP function of t (and vice versa), but it is not jointly an EQP function in s and t.

1.2 Statement of result

In general, let S_t, for $t \in \mathbb{N}$, be a family of subsets of $\mathbb{Z}^d$ and consider the following properties that S_t might have, *cf.* Example 1.11.

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

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

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

Property 4 (Assuming $S_t \subseteq \mathbb{N}^d$) There exists a period m such that, for sufficiently large $t \equiv i \bmod m$,

$$\sum_{\mathbf{x} \in S_t} \mathbf{z}^{\mathbf{x}} = \frac{\sum_{j=1}^{n_i} \alpha_{ij} \mathbf{z}^{\mathbf{q_{ij}}(t)}}{\left(1 - \mathbf{z}^{\mathbf{b_{i1}}(t)}\right) \cdots \left(1 - \mathbf{z}^{\mathbf{b_{ik_i}}(t)}\right)},$$

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 $\mathbf{b_{ij}}(t)$ eventually lexicographically positive. (That is, for sufficiently large t, the vector $\mathbf{b_{ij}}(t)$ is nonzero and its first nonzero coordinate is positive.)

Property 2 is about counting all solutions and Property 3 is about obtaining specific solutions, and so they seem somewhat different. Generating functions and Property 4 turn out to be the appropriate common generalization. Woods proves [19, Theorem 3.3] a web of implications among these properties; in particular:

Theorem 1.14. *Let S_t be any family of subsets of $\mathbb{N}^d$. If S_t satisfies Property 4, then it also satisfies Properties 1, 2, and 3.*

Woods conjectures [19] that these properties all hold for parametric Presburger families. The contribution of this paper is to prove this conjecture, namely:

Theorem 1.15. *Suppose $S_t \subseteq \mathbb{Z}^d$ is a parametric Presburger family. Then Properties 1, 2, and 3 all hold. Furthermore, if $S_t \subseteq \mathbb{N}^d$, then Property 4 holds.*

In general, quantifiers and Boolean operations allow us to perform many useful operations on sets. For example, if S_t is any parametric Presburger set and $\mathbf{c} \in \mathbb{Z}^d$ is constant, then the set of $\mathbf{x} \in S_t$ maximizing $\mathbf{c} \cdot \mathbf{x}$ can be defined using the parametric Presburger formula

$$\mathbf{x} \in S_t \quad \wedge \quad \forall y \in \mathbb{Z}^d \left(\mathbf{y} \in S_t \to \mathbf{c} \cdot \mathbf{y} \leq \mathbf{c} \cdot \mathbf{x} \right).$$

Likewise, if we know that Property 3 holds for all parametric Presburger families, and if $\mathbf{x} : \mathbb{N} \to \mathbb{Z}^d$ is a function with EQP coordinates picking out an element of S_t whenever this set is nonempty, then we can apply Property 3 again to the new parametric Presburger family $S_t \setminus \{\mathbf{x}(t)\}$ to obtain a function $\mathbf{x}_2 : \mathbb{N} \to \mathbb{Z}^d$ such that whenever $|S_t| \geq 2$, the pair $(\mathbf{x}(t), \mathbf{x}_2(t))$ selects two distinct elements of S_t.

Arguing as in the previous paragraph, Woods proved [19, Theorem 3.4] that the following would be an immediate corollary to Theorem 1.15:

Corollary 1.16. *Suppose $S_t \subseteq \mathbb{Z}^d$ is a parametric Presburger family. Then S_t has the following properties:*

Property 3a *Given $\mathbf{c} \in \mathbb{Z}^d \setminus \{0\}$, there exists a function $\mathbf{x} : \mathbb{N} \to \mathbb{Z}^d$ 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 EQPs. The set of t such that the maximum exists is eventually periodic.*

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

As a further illustration of the power of parametric Presburger arithmetic, note that the ability to maximize a linear functional allows us to run the beyond-and-beneath algorithm (see Grünbaum [8, Section 5.2]) on the integer points in a parametric polyhedron, P_t, defined by linear inequalities of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$. This will iteratively compute vertices of the integer hull, and they will have EQP coordinates. Given the uniform (across t) bound on the number of vertices, as proved in [2], this suffices to re-prove Theorem 1.8. All other theorems discussed in Section 1.1 are immediate consequences of Theorem 1.15.

First, in Section 2 we give an outline of the proof of Theorem 1.15, which combines ideas from logic and combinatorics. We set up the logical foundations carefully in Section 3, and then we prove Properties 1, 2, and 3 for Theorem 1.15 in Section 4. This allows us to prove them in the full generality of $\mathbb{Z}^d$, but more importantly it shows that the generating function tools are not necessary: we have enough combinatorial information about the sets S_t to prove Properties 1, 2 and 3 directly. In Section 5, we discuss generating functions in more detail and prove Property 4.

2   Outline of Proof

We are given a set S_t defined in parametric Presburger arithmetic, whose language we will denote $\mathcal{L}_{\text{EQP}}$. This language allows (repeated) multiplication by t, so that the *atomic formulas* (the basic building blocks) are of the form $\mathbf{a}(t) \cdot \mathbf{x} \leq b(t)$ or $\mathbf{a}(t) \cdot \mathbf{x} = b(t)$, where $\mathbf{a}(t) \in \mathbb{Z}[t]^d, b(t) \in \mathbb{Z}[t]$. More complicated formulas may be built up using Boolean operations and quantifiers.

By contrast, the language of *standard* Presburger arithmetic, which we denote $\mathcal{L}_{Pres}$, does not allow multiplication by t, so that its atomic formulas are of the form $\mathbf{a} \cdot \mathbf{x} \leq b$ or $\mathbf{a} \cdot x = b$, where $\mathbf{a} \in \mathbb{Z}^d, b \in \mathbb{Z}$. A standard technique to analyze formulas in $\mathcal{L}_{Pres}$ is *quantifier elimination*: obtain a *logically equivalent* formula (one defining the same set) that has no quantifiers.

Example 2.1.   The statements

$$\exists y [x + y \leq z \ \wedge \ y \geq 3] \quad \text{and} \quad x \leq z - 3$$

are logically equivalent modulo the theory of Presburger arithmetic; in the second statement, the quantified variable y has been eliminated.

Presburger originally analyzed [12] (see [13] for a translation) these formulas; Cooper [4] uses the following strategy for quantifier elimination:

Eliminate quantified variables one at a time (innermost to outermost). Since $\forall y \ \varphi(\mathbf{x}, y)$ is equivalent to $\neg \exists y \neg \varphi(\mathbf{x}, y)$, we may assume we are eliminating an existential quantifier from a formula of the form $\exists y \ \varphi(\mathbf{x}, y)$. Cooper's strategy is to find a finite set of candidate y's (each written in terms of $\mathbf{x}$) such that: there exists y making $\varphi(\mathbf{x}, y)$ true if and only if one of the candidate y's makes $\varphi(\mathbf{x}, y)$ true.

Example 2.2.   If there exists a $y \in \mathbb{Z}$ such that

$$x + 1 \leq y \leq z \ \wedge \ 2y \leq 3z - x$$

then $y = x + 1$ must be such a y (this is the smallest integer y satisfying the only lower bound on y, and therefore it is the most likely y to also satisfy the upper bounds). Substituting in $y = x + 1$ eliminates the quantifier, and we are left with

$$x + 1 \leq z \ \wedge \ 2(x + 1) \leq 3z - x.$$

In general, unfortunately, this does not quite work to guarantee that we may eliminate a quantifier. Instead, we may need to introduce some divisibility conditions:

Example 2.3. If there exists a $y \in \mathbb{Z}$ such that

$$x + 1 \leq 2y \leq z \ \wedge \ 2y \leq 3z - x$$

then our candidate for y depends on the parity of x: if x is odd, then $y = (x+1)/2$ is our candidate, and if x is even, then $y = (x+2)/2$ is our candidate. Allowing ourselves to use divisibility by 2 in the formula, we eliminate y to get:

$$\left(2\big|x \ \wedge \ x+2 \leq z \ \wedge \ x+2 \leq 3z-x\right) \ \vee \ \left(2\big|(x-1) \ \wedge \ x+1 \leq z \ \wedge \ x+1 \leq 3z-x\right).$$

To completely eliminate all quantifies in $\mathcal{L}_{Pres}$, we must *extend* our language to $\mathcal{L}^+_{Pres}$, where testing divisibility by a constant, c, is allowed. Formally, we introduce *divisibility predicates*, D_c, for constants c, into our language. For example, we write $2\big|(x-1)$ as $D_2(x-1)$.

Our proof begins by trying to apply these techniques in $\mathcal{L}_{EQP}$, where multiplication by t is allowed.

Step 1: Goodrick does exactly this in [7] (and Lasaruk and Sturm [11] independently arrived at essentially the same result using a different technique). Not surprisingly, we need to extend our language to $\mathcal{L}^+_{EQP}$, where we are also allowed to test divisibility by polynomials in t (that is, we allow divisibility predicates $D_{f(t)}$, where $f(t)$ is a polynomial in t). Even this is not quite enough to eliminate quantifiers:

Example 2.4. If there exists a $y \in \mathbb{Z}$ such that

$$x + 1 \leq ty \leq z \ \wedge \ ty \leq 3z - x$$

then our candidate for y depends on $x \bmod t$: if $x \equiv i \bmod t$, for $0 \leq i \leq t-1$, then $y = (x+t-i)/t$ is our candidate. Unfortunately, we now have t different candidates for y, and we cannot simply list them in a formula. Instead, we must write something like:

$$\exists i \left[0 \leq i \leq t-1 \ \wedge \ t\big|(x-i) \ \wedge \ \left(x+t-i \leq z\right) \ \wedge \ \left(x+t-i \leq 3z-x\right)\right]$$

We have replaced the old quantified y with a new quantified i, but we have gained something: i is *bounded* by a polynomial in t.

Goodrick proves [7] that any parametric Presburger family $\{S_t : t \in \mathbb{N}\}$ is definable by an $\mathcal{L}^+_{EQP}$-formula with *polynomially-bounded quantifiers*. Using this result, we now have that every quantified variable y is associated with a condition of the form $0 \leq y \leq f(t)$, where $f : \mathbb{N} \to \mathbb{Z}$ is a polynomial function of t.

Step 2: Next, we eliminate all occurrences of the divisibility predicates $D_{f(t)}$. We do this by replacing each variable x_i by an expression $g(t) \cdot u_i + v_i$ where u_i and v_i are new variables, g is a nonnegative common multiple of all the functions $f_1, \ldots, f_n$ which occur in divisibility predicates D_{f_i} in the formula, and with the restriction that $0 \leq v_i < g(t)$. That is, u_i and v_i represent the quotient and remainder when x_i is divided by $g(t)$.

Example 2.5. Let

$$S_t = \{(x_1, x_2) \in \mathbb{Z}^2 : D_{t+1}(x_1 + 2x_2) \wedge D_t(x_1 - x_2)\}.$$

Let $g(t) = t(t+1)$ and $x_i = g(t)u_i + v_i$. Then $D_{t+1}(x_1 + 2x_2)$ is equivalent to $D_{t+1}(v_1 + 2v_2)$, since $(t+1) \mid g(t)$. Furthermore, $0 \le v_i < t(t+1)$ implies that $v_1 + 2v_2 < 3t(t+1)$, and so $D_{t+1}(v_1 + 2v_2)$ could be replaced by the formula

$$\exists y \, [0 \le y \le 3t \, \wedge \, y \cdot (t+1) = v_1 + 2v_2].$$

Replacing both predicates, we define S_t' as the set

$$\left\{ (u_1, u_2, v_1, v_2) : \exists y \, [0 \le y \le 3t \, \wedge \, y \cdot (t+1) = v_1 + 2v_2] \wedge \exists z \, [-(t+1) \le z \le t+1 \, \wedge \, z \cdot t = v_1 - v_2] \right\}.$$

S_t' is in bijection to S_t under the map $(u_i, v_i) \mapsto x_i = g(t)u_i + v_i$.

Notice that we have eliminated the divisibility predicates, at the expense of introducing some additional polynomially-bounded quantifiers. The result of Step 2 is a new parametric Presburger family S_t' whose points are in bijection with those of S_t and such that S_t' is defined by an $\mathcal{L}_{\mathrm{EQP}}$-formula with polynomially-bounded quantifiers. Furthermore, the bijection from S_t' to S_t is an *affine reduction*; that is, it is given by an affine linear function whose coordinates are eventually quasi-polynomial in t. We will see that this preserves all the properties of S_t that we care about.

Step 3: We now apply a version of Chen–Li–Sam's "base t" method [3], in order to finally eliminate the (polynomially-bounded) quantified variables, $y_1, \ldots, y_d$. After reducing to the case that all variables are nonnegative, suppose that we have some k such that, for all i, $0 \le y_i < t^k$ are bounds on the quantified variables.

We write each y_i "base t," using new variables b_{ij}:

$$y_i = \sum_{j=0}^{k-1} b_{ij} t^j, \quad 0 \le b_{ij} < t.$$

Suppose that ℓ is the largest degree of any polynomial $f(t)$ appearing as a coefficient of some y_i. Write each free (unquantified) variable, x_i, in base t using new variables a_{ij} and z_i:

$$x_i = z_i t^{k+\ell} + \sum_{j=0}^{k+\ell-1} a_{ij} t^j, \quad 0 \le a_{ij} < t.$$

Note that we have no bound on the x_i, so we must allow an *unbounded* $t^{k+\ell}$ coefficient. The resulting S_t' will be in bijection with the original S_t, with the above formulas for x_i and y_i yielding the bijection. As in Step 2, the bijection is an affine reduction.

We now follow the Chen–Li–Sam method [3], and iteratively look at the t^0 coefficients of each term, the t^1 coefficients, etc.

Example 2.6. Suppose we have the formula[1]

$$0 \leq x_1, x_2 \wedge \exists y_1, y_2 \left[(0 \leq y_i < t^2) \wedge (x_1 - tx_2 \leq (t+1)y_1 + (t+2)y_2) \right].$$

Replace y_i by $b_{i1}t + b_{i0}$ and x_i by $z_i t^3 + a_{i2}t^2 + \cdots + a_{i0}$, with $0 \leq b_{ij} < t$ and with $0 \leq a_{ij} < t$. That is, z_1 and z_2 are the only variables not bounded by t. The main inequality is now equivalent to

$$t^4(-z_2) + t^3(z_1 - a_{22}) + t^2(a_{12} - a_{21} - b_{11} - b_{21})$$
$$+ t(a_{11} - a_{20} - b_{11} - b_{10} - 2b_{21} - b_{20}) + (a_{10} - b_{10} - 2b_{20}) \leq 0.$$

Write this inequality as

$$tu + f_0 \leq 0 \tag{1}$$

where $f_0 := a_{10} - b_{10} - 2b_{20}$. Since the a- and b-variables are all bounded between 0 and $t-1$, we see that

$$-3t + 3 \leq f_0 \leq t - 1.$$

This implies that we are in one of four exclusive cases:

$$(-3t + 3 \leq f_0 \leq -2t) \vee (-2t + 1 \leq f_0 \leq -t) \vee (-t + 1 \leq f_0 \leq 0) \vee (1 \leq f_0 \leq t - 1).$$

Let's look at the case where $-3t + 3 \leq f_0 \leq -2t$ (we will handle each of the finite number of other cases separately.) Dividing inequality (1) by t and taking integer parts, we obtain the equivalent inequality

$$u + \left\lceil \frac{f_0}{t} \right\rceil \leq 0.$$

By the hypothesis on f_0, $\left\lceil \frac{f_0}{t} \right\rceil = -2$, so we have reduced to the inequality $u - 2 \leq 0$, that is,

$$t^3(-z_2) + t^2(z_1 - a_{22}) + t(a_{12} - a_{21} - b_{11} - b_{21}) + (a_{11} - a_{20} - b_{11} - b_{10} - 2b_{21} - b_{20} - 2) \leq 0.$$

Consider the new constant term $f_1 := a_{11} - a_{20} - b_{11} - b_{10} - 2b_{21} - b_{20} - 2$. Again using the bounds on a_{ij}, b_{ij} we have

$$-6t + 4 \leq f_1 \leq t - 3.$$

The relevant seven cases are now

$$(-6t + 4 \leq f_1 \leq -5t) \vee (-5t + 1 \leq f_1 \leq -4t) \vee \cdots \vee (1 \leq f_1 \leq t - 3)$$

and we can again look at them separately. For example, if $-4t + 1 \leq f_1 \leq -3t$, then by again dividing by t, the original inequality becomes

$$t^2(-z_2) + t(z_1 - a_{22}) + (a_{12} - a_{21} - b_{11} - b_{21} - 3) \leq 0.$$

---

[1]The reader may notice that this formula is equivalent to a quantifier-free formula in which we replace the variables y_i by their maximum values $t^2 - 1$. However, such a replacement will not generally work with more complex formulas, whereas the technique of this example can be applied separately to each of the atomic inequalities.

Once again we break into a finite list of cases for the constant term f_2. For example, in the case

$$-2t + 1 \leq a_{12} - a_{21} - b_{11} - b_{21} - 3 \leq -t,$$

the original inequality becomes equivalent to

$$t(-z_2) + (z_1 - a_{22} - 1) \leq 0. \tag{2}$$

Since z_1 is unbounded, we cannot continue with this method. But notice that the case-defining inequalities $-3t + 3 \leq f_0 \leq -2t$, $-4t + 1 \leq f_1 \leq -3t$, and $-2t + 1 \leq f_2 \leq 1$ do not involve multiplication by t, and the inequality (2) involves no quantified variables.

This strategy works in general. Our new formula has two types of atomic subformulas: those that involve quantified variables, which are in classical Presburger arithmetic (do not involve multiplication by t), and those that use only unquantified variables.

Step 4: We may now apply the classical quantifier elimination procedure to get a logically equivalent quantifier-free formula. Theorem 1.5 from [7] says that this works, because the parameter t does not occur in any of the atomic subformulas involving quantified variables. As discussed before Step 1, we must extend our language to allow D_c, divisibility predicates for constants c. To summarize, we now have a quantifier-free formula in parametric Presburger arithmetic, with the addition of D_c predicates.

Step 5: Now that we have a quantifier-free formula, we are ready to understand the geometry of these sets $S_t \subseteq \mathbb{Z}^d$. Our formula consists of atomic formulas of the form

- $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and

- $D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t)\big)$.

If our formula were simply a *conjunction* of such atomic formulas, then we would have that

$$S_t = P_t \cap (\lambda_t + \Lambda_t),$$

where $P_t \subseteq \mathbb{R}^d$ is a polyhedron (which changes as t changes) defined by the linear inequalities, $\Lambda_t \subseteq \mathbb{Z}^d$ a lattice, and $\lambda_t \in \mathbb{Z}^d$ a translation vector, with the latter two defined by the divisibility conditions.

Example 2.7. If S_t is the set of $x \in \mathbb{Z}$ such that

$$-x \leq 0 \ \wedge \ tx \leq t^2 + 1 \ \wedge \ D_2(x + t)$$

then

$$P_t = [0, (t^2 + 1)/t] \subseteq \mathbb{R}, \quad \Lambda_t = 2\mathbb{Z}, \quad \lambda_t = (t \bmod 2).$$

Of course our S_t may not be simply a conjunction of these atomic formulas, so we first show that S_t can be written as a disjoint union of such sets, using a variant of Disjunctive Normal Form. Then we may concentrate on each piece individually; $|S_t|$, for example, will simply be the sum of the cardinalities of each piece.

So we may assume that S_t is a conjunction of these atomic formulas. Note that a conjunction of formulas of the form $D_c\big(\mathbf{f}(t)\cdot\mathbf{x}-g(t)\big)$ is an "external" representation of a translation of a lattice, i.e., defined via constraints, using the language of [15]. We'd like an "internal" representation, i.e., defined parametrically; in this case, this would be a collection of basis vectors for the lattice, together with a translation vector.

Example 2.8. In Example 2.7, we converted the external representation $D_2(x+t)$ into the internal representation: lattice $\Lambda_t \subseteq \mathbb{Z}$ with basis $\{2\}$ and translate $\lambda_t = (t \bmod 2)$.

By examining Hermite Normal Forms, we prove that this can be accomplished while preserving EQP properties, and then this basis allows us to apply an affine reduction to eliminate any D_c terms.

Example 2.9. Continuing Example 2.7, our internal representation of $\Lambda_t + \lambda_t$ implies the following: for odd t, any x satisfying $D_2(x+t)$ is of the form $x = 2u+1$, for some $u \in \mathbb{Z}$. Applying the affine reduction given by $x = 2u+1$ yields (for odd t)

$$S'_t = \big\{u \in \mathbb{Z}:\ -(2u+1) \le 0 \wedge t(2u+1) \le t^2+1\big\}.$$

That is, we have eliminated all divisibility terms from the formula.

In other words, we now simply have that S_t is the set of integer points in a parametric polyhedron, defined with linear inequalities of the form $\mathbf{f}(t)\cdot\mathbf{x} \le g(t)$. This is again an "external" representation. We show that we can convert to an "internal" representation and preserve EQP properties, using row reduction over $\mathbb{Q}(t)$. In this case, an internal representation is a list of vertices (given as ratios of EQPs), of extreme rays of the recession cone (encoding directions, $\mathbf{y}$, in which the polyhedron is infinite in the $\mathbf{y}$ direction but not in the $-\mathbf{y}$ direction), and of a basis for the lineality space (encoding directions $\mathbf{z}$ in which it is infinite in both the $\mathbf{z}$ and $-\mathbf{z}$ directions).

Example 2.10. Continuing Example 2.7, the external representation $-(2u+1) \le 0 \wedge t(2u+1) \le t^2+1$ defines the polyhedron with vertices 0 and $(t^2-t+1)/2t$. Since this is a bounded polyhedron, the recession cone and the lineality space are trivial.

Step 6: We are now ready to prove Properties 1, 2, and 3. Property 1 will follow from Property 3 trivially. Property 2 follows directly from the Chen, Li, Sam result [3], as long as our polyhedron is bounded. Since we know whether our polyhedron has non-trivial recession cone and lineality space, we know whether it is bounded. If it is unbounded, then $|S_t|$ is either 0 or infinite, and we will show how to figure out which is correct. Property 3 similarly follows from Shen [17]. We delay discussion of generating functions until Section 5, but Property 4 follows from Woods [19].

2.1 Summary of Outline of Proof.

Suppose that we are given any parametric Presburger family $S_t \subseteq \mathbb{Z}^d$ defined by an $\mathcal{L}_{\mathrm{EQP}}$-formula φ. Then we will apply a series of logical equivalences and affine reductions as follows:

$$\varphi \xleftarrow[\text{(Step 1)}]{\text{logic}} \varphi_1 \xleftarrow[\text{(Step 2)}]{\text{affine}} \varphi_2 \xleftarrow[\text{(Step 3)}]{\text{affine}} \varphi_3 \xleftarrow[\text{(Step 4)}]{\text{logic}} \varphi_4 \xleftarrow[\text{(Step 5)}]{\text{logic + affine}} \varphi_5$$

where:

1. φ_1 is an $\mathcal{L}_{\text{EQP}}^+$-formula with polynomially-bounded quantifiers,

2. φ_2 is an $\mathcal{L}_{\text{EQP}}$-formula with polynomially-bounded quantifiers,

3. φ_3 is an $\mathcal{L}_{\text{EQP}}$-formula in which no variable within the scope of a quantifier is multiplied by the parameter t,

4. φ_4 is a *quantifier-free* $\mathcal{L}_{\text{EQP}}^+$-formula whose only divisibility predicates are D_c for constant functions c, and

5. φ_5 is a disjoint union of conjunctions of atomic $\mathcal{L}_{\text{EQP}}$-formulas (and hence quantifier-free).

At each stage, the reductions preserve all the properties we are interested in, until we finally reduce to the case of the parametric polyhedra defined by φ_5. In Step 6, we deal with these polyhedra by applying previously-established combinatorial techniques from Chen-Li-Sam [3], Woods [19], and Shen [17].

The sequence of reductions is a little complicated, so one might well wonder whether there is a more direct proof. For instance, one might try to show that any $\mathcal{L}_{\text{EQP}}$-formula is logically equivalent to a quantifier-free formula in a slightly larger language with additional "well-behaved" function and relation symbols (the method of *quantifier elimination* from logic), then prove a generalization of the main theorem from [19] that quantifier-free parametric Presburger formulas have the EQP behavior we seek. But we already know that quantifier elimination in the original language $\mathcal{L}_{\text{EQP}}$ is impossible (see [7]), and finding a reasonable language for quantifier elimination seems difficult. For example, Krajíček [10] gave the name "two-sorted Presburger arithmetic" to the complete first-order theory of $\mathbb{Z}$ as an ordered $\mathbb{Z}$-module in a language with two sorts of variables (one for the ring, one for the module). Two-sorted Presburger arithmetic is very similar to the logical system studied in this paper, and Krajíček noted "it is an interesting open question whether a form of quantifier elimination holds." Two-sorted Presburger arithmetic without a relation symbol for $\leq$ was studied by van den Dries and Holly [18], who gave a quantifier elimination theorem for this weaker system in a language including a relation symbol for divisibility and function symbols for gcd and a few other closely related arithmetic functions.

3   Parametric Presburger families and polynomially-bounded quantifiers

In this section, we set notation and definitions and review the result on bounding quantifiers in parametric Presburger families proved in [7]. We also define affine reductions and note that they preserve Properties 1 through 3.

3.1   Parametric Presburger arithmetic

We will use standard notation and terminology from first-order logic, for which any modern textbook on the subject could serve as a reference (for instance, [6] or [9]). In particular, a *language* is a set of finitary relational, functional, and constant symbols, usually denoted by $\mathcal{L}$ with decorations. Given a language $\mathcal{L}$, an $\mathcal{L}$-*formula* means a first-order formula in $\mathcal{L}$: we allow basic symbols in $\mathcal{L}$ plus equality, symbols for variables, Boolean operations, and quantifiers.

We let $\mathcal{L}_{Pres}$ be the first-order language with symbols for 0 and 1 (constants), $<$ (binary relation for the ordering), $-$ (a unary operation symbol for negation), and $+$ (binary function symbol for addition).

We will always work in the standard model of Presburger arithmetic with universe $\mathbb{Z}$, so whenever we write "$\models \varphi$" or "φ holds" we are referring to the standard interpretation of the language.

$\mathcal{L}_{Pres}^{+} \supseteq \mathcal{L}_{Pres}$ is the expansion which includes unary predicates D_c for each $c \in \mathbb{Z}$, to be interpreted as divisibility by c. By convention, if $c = 0$, then "$D_0(x)$" is false for every $x \in \mathbb{Z}$, even if $x = 0$.

Now we come to the main definition:

Definition 3.1. A *parametric Presburger formula* is a first-order formula in the language $\mathcal{L}_{EQP} := \mathcal{L}_{Pres} \cup \{\lambda_t\}$. The intended interpretation of $\lambda_t(x)$ is that we are multiplying x by the parameter t which takes some value from $\mathbb{N}$.

Given $t \in \mathbb{N}$ and an $\mathcal{L}_{EQP}$-formula φ, we define the $\mathcal{L}_{Pres}$-formula φ_t to be the translation of φ defined recursively so that each term of the form $\lambda_t(s)$ occurring in φ (where s is a term) is replaced by one of the following:

1. If $t > 0$, then $\lambda_t(s)$ is replaced in φ_t by $s + s + \ldots + s$ with t repetitions of s;

2. if $t = 0$, then $\lambda_t(s)$ is replaced in φ_t by the constant symbol 0.

Remark 3.2. Here and below, we will adopt the notational convention of writing "$f(t) \cdot s$" for the $\mathcal{L}_{EQP}$-term formed from the term s and $f(t) \in \mathbb{Z}[t]$ by repeated applications of the function λ_t. For instance, the expression $(t^2 + 2) \cdot x_1$ stands for the term $\lambda_t(\lambda_t(x_1)) + x_1 + x_1$.

When we write $\varphi(\mathbf{x})$, we mean that all of the free variables occurring in φ are listed in the tuple $\mathbf{x} = (x_1, \ldots, x_d)$. (Throughout, boldface letters such as $\mathbf{a}$ and $\mathbf{x}$ will always denote finite tuples.)

The definition of φ_t above allows us to talk about the *truth* of $\mathcal{L}_{EQP}$-formulas relative to a parameter $t \in \mathbb{N}$: given an $\mathcal{L}_{EQP}$-formula $\varphi(x_1, \ldots, x_d)$ whose free variables are contained in $\{x_1, \ldots, x_d\}$ and $(k_1, \ldots, k_d) \in \mathbb{Z}^d$, we will write

$$\models \varphi_t(k_1, \ldots, k_d)$$

just in case the $\mathcal{L}_{Pres}$-formula φ_t is true with the variable x_i evaluated as k_i.

Definition 3.3. A *parametric Presburger family* is a family of sets $\{S_t : t \in \mathbb{N}\}$ such that

$$S_t = \{(k_1, \ldots, k_d) \in \mathbb{Z}^d : \models \varphi_t(k_1, \ldots, k_d)\}$$

for some fixed d and some $\mathcal{L}_{EQP}$-formula $\varphi(x_1, \ldots, x_d)$.

From a logical standpoint, the idea behind parametric Presburger definability is that we are essentially expanding classical Presburger arithmetic by a restricted multiplication function: we allow multiplication of any variable or term by the special parameter variable t, but we do not allow multiplication between any of the other variables, and we do not allow quantification over t, thus avoiding the complications of sets definable in the full first-order theory of $(\mathbb{Z}; <, +, \cdot)$.

Definition 3.4. $\mathcal{L}_{EQP}^{+} := \mathcal{L}_{EQP} \cup \{D_{f(t)} : f(t) \in \mathbb{Z}[t]\}$, where $D_{f(t)}$ is a unary relation symbol denoting divisibility by the value of $f(t)$.

Given an $\mathcal{L}_{EQP}^{+}$-formula $\varphi(x_1, \ldots, x_d)$, for any $t \in \mathbb{N}$ and $a_1, \ldots, a_d \in \mathbb{Z}$, we can define the truth value of $\varphi_t(a_1, \ldots, a_d)$ as before, recalling the convention that $D_0(x)$ is always false.

Definition 3.5. Two $\mathcal{L}_{EQP}^+$-formulas $\varphi(x_1,\ldots,x_d)$ and $\psi(x_1,\ldots,x_d)$ are *logically equivalent* just in case for *every* $t \in \mathbb{N}$, the $\mathcal{L}_{Pres}^+$-formulas φ_t and ψ_t are logically equivalent; in other words, for every $t \in \mathbb{N}$ and every $(k_1,\ldots,k_d) \in \mathbb{Z}^d$,

$$\models \varphi_t(k_1,\ldots,k_d) \Leftrightarrow \models \psi_t(k_1,\ldots,k_d).$$

It is clear that every $\mathcal{L}_{EQP}^+$-formula is logically equivalent to some $\mathcal{L}_{EQP}$-formula.

Definition 3.6. Given an $\mathcal{L}_{EQP}^+$-formula $\varphi(x_1,\ldots,x_d,y)$ whose free variables are among $\{x_1,\ldots,x_d,y\}$ and $f \in \mathbb{Z}[t]$, a *polynomially-bounded universal quantifier* applied to φ yields

$$\forall y \, [0 \leq y \leq f(t) \rightarrow \varphi(x_1,\ldots,x_d,y)]$$

for some $f \in \mathbb{Z}[t]$. Similarly, a *polynomially-bounded existential quantifier* applied to φ yields

$$\exists y \, [0 \leq y \leq f(t) \, \wedge \, \varphi(x_1,\ldots,x_d,y)] \, .$$

An $\mathcal{L}_{EQP}^+$-*formula with polynomially-bounded quantifiers* is a member of the smallest class of $\mathcal{L}_{EQP}^+$-formulas containing all atomic formulas and closed under Boolean combinations and the formation of polynomially-bounded quantifiers.

We recall the following theorem, which was proved in [7]:

Theorem 3.7. *Every $\mathcal{L}_{EQP}^+$-formula is logically equivalent to an $\mathcal{L}_{EQP}^+$-formula with polynomially-bounded quantifiers.*

Also see [7] for a discussion on how this relates to similar previously-known results of Weispfenning and Lasaruk-Sturm [11].

Assumption 3.8. *In any first-order formula φ, we always assume that no variable occurs in φ both as a free variable and as a quantified variable: that is, formulas such as*

$$(x > 0) \wedge (y > 0) \wedge \exists x \, [x + x = y]$$

are not allowed (we have to rename the quantified variable and replace the last conjunct by "$\exists z \, [z + z = y]$").

3.2 Eventual quasi-polynomials and affine reductions

Recall that EQPs were defined in Definition 1.1.

Definition 3.9. Given any $d' \times d$ matrix $A(t) = (f_{i,j}(t))$ of EQP functions and any d'-tuple $(g_1(t),\ldots,g_{d'}(t))$ of EQP functions, we call the function $F : \mathbb{Z}^d \times \mathbb{N} \rightarrow \mathbb{Z}^{d'}$ given by the rule

$$F(x_1,\ldots,x_d,t) = A(t) \cdot (x_1,\ldots,x_d)^T + (g_1(t),\ldots,g_{d'}(t))^T$$

an *EQP-affine function.*

Definition 3.10. Suppose that $S_t \subseteq \mathbb{Z}^d$ and $S'_t \subseteq \mathbb{Z}^{d'}$ are parametric Presburger families, defined by $\mathcal{L}^+_{\text{EQP}}$-formulas $\varphi(\mathbf{x})$ and $\varphi'(\mathbf{z})$ respectively. We say that S'_t is *affine reducible to S_t* if there is an EQP-affine function $F : \mathbb{Z}^{d'} \times \mathbb{N} \to \mathbb{Z}^d$ such that for every $t \in \mathbb{Z}$, if F_t is the function obtained from F by fixing the value of t for the $(d'+1)$-th coordinate, then $F_t \upharpoonright S'_t$ is a bijection from S'_t onto S_t.

Abusing notation, we will not always distinguish carefully between an $\mathcal{L}^+_{\text{EQP}}$-definable family and the parametric Presburger set that it defines, and we may say "φ' is affine reducible to φ" with the obvious meaning.

The key property of affine reductions for our approach is that they preserve Properties 1, 2, and 3:

Remark 3.11. If $S_t \subseteq \mathbb{Z}^d$ and $S'_t \subseteq \mathbb{Z}^{d'}$ are families parametrized by $t \in \mathbb{N}$ and S'_t is affine reducible to S_t, then if S'_t has any of the Properties 1, 2, or 3, then S_t has the same Properties.

Proof. The preservation of Properties 1 and 2 is trivial, since F induces bijections from the sets S'_t onto the S_t. For Property 3, if $F : \mathbb{Z}^{d'} \times \mathbb{N} \to \mathbb{Z}^d$ gives an affine reduction from S'_t to S_t and $\mathbf{x} : \mathbb{N} \to \mathbb{Z}^{d'}$ is an EQP-affine function such that $\mathbf{x}(t) \in S'_t$ (whenever $S'_t \neq \emptyset$), then the composition $F \circ \mathbf{x} : \mathbb{N} \to \mathbb{Z}^d$ is an EQP function yielding points in S_t whenever this is nonempty. $\square$

4 A sequence of reductions

In this section we give the details of the six steps of our procedure as outlined in Section 2. This will prove Properties 1, 2, and 3 in Theorem 1.15.

4.1 Step 1

This is the content of Theorem 3.7, proved in [7].

4.2 Step 2

Next we describe an affine reduction which eliminates the divisibility predicates $D_{f(t)}$ from an $\mathcal{L}^+_{\text{EQP}}$ formula, but at the cost of adding additional bounded quantifiers and new variables, cf. Example 2.5:

Lemma 4.1. *Let $S_t \subseteq \mathbb{Z}^d$ be a parametric Presburger family defined by an $\mathcal{L}^+_{\text{EQP}}$-formula with polynomially-bounded quantifiers. Then there is a parametric Presburger family $S'_t \subseteq \mathbb{Z}^{d'}$ which is definable by an $\mathcal{L}_{\text{EQP}}$-formula with polynomially-bounded quantifiers and such that S'_t is affine reducible to S_t.*

Proof. Fix some $\mathcal{L}^+_{\text{EQP}}$ formula $\varphi(\mathbf{x})$ with polynomially-bounded quantification which defines the family S_t. Let $f_1, \ldots, f_r$ be all the functions in $\mathbb{Z}[t]$ which occur in divisibility predicates $D_{f_i(t)}$ in φ. Without loss of generality, none of the f_i's is the zero polynomial (since formulas $D_0(s)$ are trivially false), so $f_i(t)$ is nonzero for sufficiently large t. Since D_f and D_{-f} are logically equivalent, we may assume that $f_i(t)$ is eventually positive. Let $g \in \mathbb{Z}[t]$ be the product $f_1 f_2 \cdots f_r$. Then for sufficiently large $t \in \mathbb{N}$, the value $g(t)$ is a positive common multiple of $f_1(t), \ldots, f_r(t)$; there are only finitely many values of t at which one of $f_1(t), \ldots, f_r(t)$ is nonpositive, and an EQP-affine reduction can handle these cases separately.

Let $z_1, \ldots, z_m$ list all variables occurring in φ, both free and quantified. Let $u_1, \ldots, u_m$ and $v_1, \ldots, v_m$ be a set of new variables. Let $F : \mathbb{Z}^{2m} \times \mathbb{N} \to \mathbb{Z}^m$ be the EQP-affine function

$$F(u_1, \ldots, u_m, v_1, \ldots, v_m, t) = (g(t) \cdot u_1 + v_1, \ldots, g(t) \cdot u_m + v_m).$$

We will now define a formula φ' whose free variables are among $u_1, \ldots, u_m, v_1, \ldots, v_m$ and show that this is affine reducible to φ "via F": this means that the restriction of F to the set defined by φ', ignoring any u_i or v_i which does not occur free, yields a bijection onto the set S_t defined by φ.

In fact, we will recursively construct $\mathcal{L}_{\mathrm{EQP}}$-formulas ψ' for every subformula ψ of φ, starting with the atomic subformulas, such that every ψ' has polynomially-bounded quantification and the parametric Presburger family defined by ψ is affine reducible to that defined by ψ' via the map F, and the family S'_t that we seek will be that defined by φ'.

The formula ψ' will be defined as $\theta \wedge \psi''$ where θ is the conjunction

$$\bigwedge_{i=1}^{m} [0 \le v_i < g(t)]$$

and the formula ψ'' is defined by recursion. As we define the formula ψ'', we will also show inductively that the following holds:

($*$) For any sequence of values $(\mathbf{a}, \mathbf{b}) = (a_1, \ldots, a_m, b_1, \ldots, b_m)$ which satisfies θ, we have $\models (\psi'')_t(\mathbf{a}, \mathbf{b})$ if and only if $\models \psi_t(F(\mathbf{a}, \mathbf{b}, t))$.

Note that ($*$) immediately implies that ψ' is affine reducible to ψ via F.

- For any term s in the variables $z_1, \ldots, z_m$, let $s(g \cdot \mathbf{u} + \mathbf{v}/\mathbf{z})$ be the result of replacing each instance of the variable z_i by $g \cdot u_i + v_i$. Then if ψ is an atomic formula of the form $s_1 = s_2$, we let ψ'' be the atomic formula

$$s_1(g \cdot \mathbf{u} + \mathbf{v}/\mathbf{z}) = s_2(g \cdot \mathbf{u} + \mathbf{v}/\mathbf{z}).$$

If ψ is an atomic formula of the form $s_1 \le s_2$, then ψ'' is

$$s_1(g \cdot \mathbf{u} + \mathbf{v}/\mathbf{z}) \le s_2(g \cdot \mathbf{u} + \mathbf{v}/\mathbf{z}).$$

It is clear that in this case that ($*$) holds.

- For any atomic formula ψ of the form $D_{f_j(t)}(s)$ (where s is a term), let $h_s(t) \in \mathbb{Z}[t]$ be such that $|s^t(a_1, \ldots, a_m)| \le h_s(t)$, for all $t \in \mathbb{N}$ and all $a_1, \ldots, a_m$ with $0 \le a_i < g(t)$ (since, for fixed t, s is linear in $a_1, \ldots, a_m$, we only need check the bound on the finite set of 2^d EQPs obtained by setting each a_i to 0 or to $g(t)$, in the term $s(a_1, \ldots, a_m)$). Let $s(\mathbf{v}/\mathbf{z})$ be the result of replacing each instance of each variable z_i by v_i. Now let ψ'' be the formula

$$\exists y \left[0 \le y \le h_s(t) \wedge \left(f_j(t) \cdot y = s(\mathbf{v}/\mathbf{z}) \vee f_j(t) \cdot (-y) = s(\mathbf{v}/\mathbf{z}) \right) \right],$$

where y is a new variable. Note that ψ'' has polynomially-bounded quantification. The hypothesis ($*$) asserts that checking that the term s applied to the $g(t) \cdot u_i + v_i$ is divisible by $f_j(t)$ is equivalent to checking the divisibility of s applied to the v_i: this is true because $g(t)$ is divisible by $f_j(t)$.

- $(\psi_1 \wedge \psi_2)'' = \psi_1'' \wedge \psi_2''$, $(\neg \psi)'' = \neg(\psi'')$, $(\psi_1 \vee \psi_2)'' = \psi_1'' \vee \psi_2''$, and $(\psi_1 \to \psi_2)'' = \psi_1'' \to \psi_2''$. It is routine to check that if $(*)$ holds for the formulas ψ_i and ψ_i'', then they continue to hold for the Boolean combinations above. Furthermore, if the formulas ψ_i'' have bounded quantification, then so do all of these Boolean combinations.

- If ψ is a formula of the form $\exists z_i [0 \leq z_i \leq h(t) \wedge \theta]$ (with polynomially-bounded quantification on the outside), then we define ψ'' as

$$\exists u_i [0 \leq u_i \leq h(t) \wedge$$

$$\exists v_i \left[(0 \leq v_i < g(t)) \wedge (0 \leq g(t) \cdot u_i + v_i \leq h(t)) \wedge \theta''(g(t) \cdot u_i + v_i / z_i) \right]],$$

where "$\theta''(g \cdot u_i + v_i / z_i)$" means the result of substituting each instance of the free variable z_i in the formula θ with the term $g \cdot u_i + v_i$. Again, the new formula ψ'' has polynomially-bounded quantification under the inductive hypothesis that θ'' does, and $(*)$ is also immediate by induction. □

Remark 4.2. We note in passing that the same argument can be applied to $\mathcal{L}_R$-definable families (in the language of [7]) for any ring R of $\mathbb{Z}$-valued functions, with only minor modifications. This gives us the following: for any R-parametric Presburger family $S_t \subseteq \mathbb{Z}^d$, there is an R-parametric Presburger family $S_t' \subseteq \mathbb{Z}^{d'}$ which is definable by an $\mathcal{L}_R$-formula with R-bounded quantifiers and such that S_t' is R-affine reducible to S_t.

4.3 Step 3

This next step involves writing the variables of our formula in "base t," cf. Example 2.6. To do this, it is most convenient to show that we can reduce to the case where the free variables are nonnegative (by Definition 3.6 for polynomially-bounded quantifiers, the quantified variables are already nonnegative). Indeed, if our free variables are among $(x_1, \ldots, x_d)$, we partition $\mathbb{Z}^d$ into 2^d pairwise disjoint regions $X_1, \ldots, X_{2^d}$ according whether each free variable x_i is negative or nonnegative. Now let $S_t^k := X_k \cap S_t$ for each $k \in \{1, \ldots, 2^d\}$, and note that S_t^k is a parametric Presburger family which is EQP-affine reducible to a parametric Presburger family living in $\mathbb{N}^d$ (by inverting the values of negative coordinates). Then S_t is the disjoint union of these S_t^k, and the following remark shows that we may examine each S_t^k separately.

Remark 4.3. If we can write S_t as a union $S_t^1 \cup \cdots \cup S_t^k$ of pairwise disjoint parametric Presburger families, then to prove that S_t satisfies Properties 1, 2, and 3 (as in Theorem 1.15), it is sufficient to prove these for each S_t^i separately. In particular, Property 1 follows because the union of eventually periodic sets is eventually periodic, Property 2 follows because the sum of EQP's is an EQP, and Property 3 follows because we may specify an $\mathbf{x}(t)$ from any of the (nonempty) sets in the disjoint union.

The following is the main Proposition encompassing Step 3:

Proposition 4.4. *Let $S_t \subseteq \mathbb{N}^d$ be a parametric Presburger family which is definable by an $\mathcal{L}_{\mathrm{EQP}}$-formula with polynomially-bounded variables $y_1, \ldots, y_m$. Then there is an EQP-parametric Presburger family S_t' that is EQP-affine reducible to S_t and such that S_t' is definable by a $\mathcal{L}_{\mathrm{EQP}}$-formula $\varphi(\mathbf{a}, \mathbf{z})$ whose free variables are among the variables $\mathbf{a}$ and $\mathbf{z}$ and whose quantified variables are listed in the finite tuple $\mathbf{b}$ (which is assumed to be disjoint from $\mathbf{a}$ and $\mathbf{z}$), and satisfying the following conditions:*

1. *The atomic subformulas of φ are all of one of two types:*

    *(a) Type 1, which are inequalities involving only variables in **a**, **b**, and t, and which do not involve any multiplication by t;*

    *(b) Type 2, which are inequalities involving only t and the free variables (from **a** or from **z**);*

2. *Any free variable from **a** is explicitly bounded between 0 and $t - 1$ (inclusive) by an atomic subformula of φ which is outside the scope of any quantifier or disjunction; and*

3. *Any quantified variable from **b** is bounded between 0 and $t - 1$ (inclusive).*

In order to prove Proposition 4.4, we adapt the approach of Chen, Li, and Sam in [3] of writing each variable "base *t*." We cannot directly apply their results because of the interaction between the potential unboundedness of the free variables and the existence of (bounded) quantified variables. Specifically, their key Lemma 3.2 uses sets defined only by equalities and nonnegativity constraints. We need to work with general linear inequalities and cannot apply the usual procedure of introducing slack variables to convert them into equalities because of the presence of quantifiers.

For example, consider the set S given by

$$S = \{x \in \mathbb{Z} : x \geq 0 \wedge \exists y\, [(y \geq 0) \wedge (x + y \leq 2)]\} \;=\; \{0, 1, 2\}.$$

Since x and y are nonnegative, we could introduce a slack variable w to obtain the set $S' \subset \mathbb{Z}^2$ given by

$$S' = \{(x, w) : x \geq 0 \wedge w \geq 0 \wedge \exists y\, [(y \geq 0) \wedge (x + y + w = 2)]\}$$

$$= (0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (2, 0)\},$$

but obviously S and S' are not in bijection.

Lemma 4.5. *For every parametric Presburger family S'_t defined by an $\mathcal{L}_{\mathrm{EQP}}$-formula φ' with polynomially-bounded quantifiers, there is an $M \geq 0$ and a parametric Presburger family S''_t which is affine reducible to S_t and is definable by an $\mathcal{L}_{\mathrm{EQP}}$-formula φ'' that has the following properties:*

1. *The quantified variables $\{b_{ij}\}$ in φ'' all satisfy $0 \leq b_{ij} \leq t - 1$.*

2. *The free variables in φ'' are of two types: $\{a_{ij}\}$ with $0 \leq a_{ij} \leq t - 1$ and $\{z_i\}$ with no a priori bound.*

3. *φ'' has no equalities and every inequality (other than the bounds on the variables) takes the form*

$$\sum_{s \geq 0} f_s t^s \leq 0 \tag{3}$$

    where no f_s contains t, f_s does not contain any unbounded free variables if $s < M$, and f_s does not contain any quantified variables if $s \geq M$.

Proof. Let $\{x_1, \ldots, x_d\}$ be the free variables and $\{y_1, \ldots, y_m\}$ the quantified variables in φ'. Let $k \in \mathbb{N}$ be such that $0 \leq y_i \leq t^k - 1$ for every i and sufficiently large t (such a k is obtainable, because each y_i is polynomially-bounded; the finite set of t for which the bound doesn't hold may be handled individually).

Also let ℓ be the highest power of t that is multiplied by any y_i in φ'. Define a $\mathbb{Z}[t]$-affine (hence EQP-affine) function $G : \mathbb{Z}^{d \times (k+\ell+1)} \to \mathbb{Z}^d$ by

$$
\begin{bmatrix} x_1 \\ \vdots \\ x_d \end{bmatrix} = G \left(\begin{bmatrix} a_{1,0} & \cdots & a_{1,k+\ell-1} & z_1 \\ \vdots & & \vdots & \vdots \\ a_{d,0} & \cdots & a_{d,k+\ell-1} & z_d \end{bmatrix} \right) = \begin{bmatrix} \sum_{j=0}^{k+\ell-1} t^j a_{1,j} + t^{k+\ell} z_1 \\ \vdots \\ \sum_{j=0}^{k+\ell-1} a_{d,j} t^j + t^{k+\ell} z_d \end{bmatrix}
$$

That is, we write each x_i base t (in the sense of [3]) up to the power $t^{k+\ell-1}$ and write the remaining part of x_i as $t^{k+\ell} z_i$. So there is a unique inverse image of any point $(x_1, \ldots x_d)$ that satisfies the inequalities $0 \le a_{i,j} \le t - 1, 0 \le z_i$ for $i = 1, \ldots, d$. We define S_t'' to be the set of these preimages, so that G is an affine reduction of S_t'' to S_t'.

Next, in the formula defining S_t'', replace each y_i by $\sum_{j=0}^{k-1} b_{i,j} t^j$ and the bounded quantifier $\exists y_i : 0 \le y_i \le t^k - 1$ by the series of bounded quantifiers $\exists b_{i,0}, \ldots, b_{i,k-1} : 0 \le b_{i,0}, \ldots, b_{i,k-1} \le t - 1$. Let φ'' be the resulting formula.

Since each unbounded free variable z_i is multiplied by $t^{k+\ell}$ each time it is introduced, the condition on terms of t-degree lower than $k + \ell$ is immediate. Also each bounded variable $b_{i,j}$ appears by replacing y_i by $b_{i,j} t^j$; thus the powers of t that are multiplied by $b_{i,j}$ in φ'' are j more than the powers of t that are multiplied by y_i in φ'. By the choice of k and ℓ, if we let $M = k + \ell$ then the final condition is also satisfied. □

Lemma 4.6. *Suppose $\sum_s f_s t^s \le 0$ is an atomic subformula of an $\mathcal{L}_{\text{EQP}}$-formula φ'' as in the conclusion of Lemma 4.5, and further assume that f_0 does not contain any of the unbounded free variables $z_1, \ldots, z_d$. Then for $t \gg 0$, $\sum_s f_s t^s \le 0$ is logically equivalent to a Boolean combination of:*

- *inequalities in Presburger arithmetic (allowing t as an ordinary Presburger variable), and*

- *parametric Presburger inequalities of the form $\sum_s f_s' t^s \le 0$ such that $f_s' = f_{s+1}$ for $s \ge 1$ and $f_0' = f_1 + h$ where h is constant.*

Proof. Since f_0 does not contain any of the variables $z_1, \ldots z_d$, write

$$
f_0 = c_0 + \sum_{i=1}^{d} \sum_{j=o}^{k+\ell-1} c_{i,j} a_{i,j} + \sum_{i=1}^{m} \sum_{j=0}^{k-1} c_{i,j}' b_{i,j} \tag{4}
$$

where all of the coefficients c_0, c_{ij} and c_{ij}' are in $\mathbb{Z}$. Let c be the maximum among the absolute values of all of these coefficients and let Q be the total number of terms in f_0. Since each variable in f_0 is bounded between 0 and $t - 1$, we have for $t \gg 0$ that

$$
-Qc(t-1) \le f_0 \le Qc(t-1). \tag{5}
$$

We can loosen (5) to obtain

$$
-Qct < f_0 \le Qct \tag{6}
$$

which is equivalent to the finite disjunction

$$
\bigvee_{h=-Qc+1}^{Qc} (h-1)t < f_0 \le ht. \tag{7}
$$

Now fix a particular value of h. With $(h-1)t < f_0 \leq ht$, the inequality $\sum_{s \geq 0} f_s t^s \leq 0$ is equivalent to $\sum_{s \geq 1} f_s t^s \leq -ht$. Adding ht to both sides and dividing by t, we obtain $\sum_{s \geq 0} f'_s t_s \leq 0$, where indeed $f'_s = f_{s+1}$ for $s \geq 1$ and $f'_0 = f_1 + h$. $\qquad \square$

Proof of Proposition 4.4. Given a parametric Presburger family S_t, consider the affine equivalent family S''_t and its defining formula φ'' that are obtained from Lemma 4.5. Let $\sum_{s \geq 0} f_s t^s \leq 0$ be one of the inequalities occurring in φ'', and k and ℓ be defined as in the proof of Lemma 4.5. If $k = 0$, then there are no quantified variables and we do not need to modify the inequality.

If $k \geq 1$, then in particular $k + \ell \geq 1$, so f_0 does not contain any of the unbounded free variables. Thus we can apply Lemma 4.6. Consider one of the resulting inequalities $\sum_{s \geq 0} f'_s t^s \leq 0$ that is not in Presburger arithmetic. If $k + \ell = 1$, then by Lemma 4.5, f_s does not contain any quantified variables for $s \geq 1$, and then by Lemma 4.6, f'_s does not contain quantified variables for any value of s whatsoever. That is, the inequality $\sum_{s \geq 0} f'_s t^s \leq 0$ is free of quantified variables. On the other hand, if $k + \ell > 1$, then $f'_0 = f_1 + h$ does not contain any unbounded free variables and so we can apply Lemma 4.5 again. In fact we can repeat this process $k + \ell$ times. For the same reason as in the case of $k + \ell = 1$, the resulting inequalities are of two types: those that contain only Presburger arithmetic and those that are free of quantified variables. $\qquad \square$

4.4 Step 4

Now we apply a quantifier elimination algorithm for "classical" Presburger arithmetic to the output of Step 3. The algorithm we will use is that described in [4].

Say that an $\mathcal{L}_{\text{EQP}}^+$-formula *has no division by t* if it involves only divisibility relations D_c where c is a constant (with no dependence on t).

A term or formula in $\mathcal{L}_{\text{EQP}}^+$ *has no multiplication by t* if it contains no terms involving multiplication by any $f(t) \in \text{EQP}$ of degree ≥ 1.

Proposition 4.7. *Suppose that $\varphi(\mathbf{a}, \mathbf{z})$ is an $\mathcal{L}_{\text{EQP}}^+$-formula with no division by t whose free variables are among the variables $\mathbf{a}$ and $\mathbf{z}$ and whose quantified variables are listed in the finite tuple $\mathbf{b}$ (which is assumed to be disjoint from $\mathbf{a}$ and $\mathbf{z}$). We further assume:*

1. *The atomic subformulas of φ are all of one of three types:*

    (a) *Type 1, which are inequalities involving only variables in $\mathbf{a}$, $\mathbf{b}$, and t, and which do not involve any multiplication by t;*

    (b) *Type 2, which are inequalities involving only t and the free variables (from $\mathbf{a}$ or from $\mathbf{z}$); and*

    (c) *Type 3, which are divisibility conditions $D_c(s)$ where c is a constant and s is a term which does not involve any multiplication by t;*

2. *Any free variable from $\mathbf{a}$ is explicitly bounded between 0 and $t-1$ (inclusive) by an atomic subformula of φ which is outside the scope of any quantifier or disjunction; and*

3. *Any quantified variable from $\mathbf{b}$ is bounded between 0 and $t-1$ (inclusive).*

   ***THEN** φ is logically equivalent to a quantifier-free formula in $\mathcal{L}_{\text{EQP}}^+$ which has no division by t.*

Proof. This follows from Theorem 1.5 of [7]. □

Example 4.8. A typically complex formula satisfying the hypotheses of Proposition 4.7 is

$$\varphi(a_0, a_1) = (0 \le a_0 < t) \land (0 \le a_1 < t)$$

$$\land \exists b_0 \exists b_1 \left[(0 \le b_0, b_1 < t) \land (t < 2a_0 + 3b_0 + 7b_1 \le 2t) \land (2t < a_1 + 2b_1 \le 3t) \right].$$

This contains no atomic subformulas of Type 2 involving z_i variables, but adding such a subformula would not make the quantifier elimination process any more difficult. Also, the bounds on a_0 and a_1 outside the quantifiers will have no effect on the procedure.

We work outwards starting from the inner quantifier $\exists b_1$. Using the notation of the procedure, the least common multiple M of the b_1 coefficients is 14, so we first multiply substitute b_1' for $14b_1$ and get that the subformula of φ bounded by the scope of $\exists b_1 \ldots$ is equivalent to

$$\exists b_1' \, (0 \le b_0 < t) \land (0 \le b_1' < 14t)$$

$$\land (2t < 4a_0 + 6b_0 + b_1' \le 4t) \land (14t < 7a_1 + b_1' \le 21t) \land D_{14}(b_1').$$

Now as in the proof, within the quantifier $\exists b_1'$ we have atomic subformulas of the three types:

(A'): $b_1' < 14t$, $b_1' < 4t - 4a_0 - 6b_0 + 1$, and $b_1' < 21t - 7a_1 + 1$;
(B'): $-1 < b_1'$, $2t - 4a_0 - 6b_0 < b_1'$, and $14t - 7a_1 < b_1'$; and
(C'): $D_{14}(b_1')$.

The procedure replaces the entire quantified subformula bounded by the scope of $\exists b_1'$ by a disjunction ψ' of 42 quantifier-free formulas, one for each choice of a constant $j \in \{1, \ldots, 14\}$ and one of the three expressions B' listed above. For example, fixing the second subformula of type B' yields the following disjunction, which forms a part of ψ':

$$\bigvee_{j=1}^{14} (0 \le b_0 < t) \land (0 \le 2t - 4a_0 - 6b_0 + j \le 14t) \land (2t < 4a_0 + 2t - 4a_0 + j \le 4t)$$

$$\land (14t < 7a_1 + 2t - 4a_0 - 6b_0 + j \le 21t) \land D_{14}(2t - 4a_0 - 6b_0 + j).$$

(Note that for any fixed values of t, a_0, and b_0, exactly one of the 14 values of j will make the last conjunct with D_{14} true, so in practice one does not need to evaluate all of the inequalities for every possible value of j.)

Now if we were to continue the quantifier elimination procedure for φ (which we will not), the next step would be to eliminate the quantifier $\exists b_0$. We only note that this time we have a subformula of Type 3, $D_{14}(2t - 4a_0 - 6b_0 + j)$, in the input formula, even though the original input formula φ contained no such divisibility predicates. The important thing is that it has the correct form for a Type 3 subformula: we are dividing only by the constant 14 and there is no multiplication of t with another variable.

4.5   Step 5

Lemma 4.9. *Let $S_t \subseteq \mathbb{Z}^d$ be defined by an $\mathcal{L}_{EQP}^+$ formula, $\varphi(\mathbf{x})$, which is quantifier-free and has no division by t (the only divisibility relations are of the form D_c, where c is a constant). Then S_t can be written as a finite disjoint union,*

$$S_t = \bigsqcup_{i=1}^{n} S_{i,t},$$

where $S_{i,t}$ is defined by an $\mathcal{L}_{EQP}^+$ formula, $\varphi_i(\mathbf{x})$, that is a conjunction of atomic formulas, each of the form:

- $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ *or*

- $D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t)\big),$

where $\mathbf{f} : \mathbb{N} \to \mathbb{Z}^d$ has EQP coordinates, $g : \mathbb{N} \to \mathbb{Z}$ is in EQP, and $c \in \mathbb{Z}$ is constant.

Proof. Using that

$$\neg(\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)) \quad \text{logically equivalent to} \quad -\mathbf{f}(t) \cdot \mathbf{x} \leq -g(t) - 1$$

and that

$$\neg\big(D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))\big) \quad \text{logically equivalent to} \quad \bigvee_{k=1}^{c-1} D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t) + k\big),$$

we may assume that every atomic formula in $\varphi(\mathbf{x})$ is of the form $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ or $D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t)\big)$.

Enumerate the atomic formulas in $\varphi(\mathbf{x})$ by $r_1, \ldots, r_m$. For $1 \leq j \leq m$, define R_j, a set of atomic formulas, as follows:

- If r_j is of the form $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$, then

$$R_j = \{\mathbf{f}(t) \cdot \mathbf{x} < g(t),\ \mathbf{f}(t) \cdot \mathbf{x} > g(t),\ \mathbf{f}(t) \cdot \mathbf{x} = g(t)\}$$

- If r_j is of the form $D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t)\big)$, then

$$R_j = \{D_c\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t) + k\big) : 0 \leq k \leq c - 1\}.$$

For a given j, every element of $\mathbb{Z}^d$ satisfies exactly one $s_j \in R_j$. Also, for a given $s_j \in R_j$, either every element of $\mathbb{Z}^d$ satisfying s_j also satisfies r_j, or every element of $\mathbb{Z}^d$ satisfying s_j fails to satisfy r_j. For any choice $(s_1, \ldots, s_m) \in R_1 \times \cdots \times R_m$, define $S_{(s_1,\ldots,s_m),t} \subseteq \mathbb{Z}^d$ with the formula $s_1 \wedge \cdots \wedge s_m$. These $S_{(s_1,\ldots,s_m),t}$ partition $\mathbb{Z}^d$. Furthermore, for a given $S_{(s_1,\ldots,s_m),t}$ either every $\mathbf{x} \in S_{(s_1,\ldots,s_m),t}$ satisfies $\varphi(\mathbf{x})$ or every $\mathbf{x} \in S_{(s_1,\ldots,s_m),t}$ fails to satisfy $\varphi(\mathbf{x})$. Therefore S_t is the disjoint union of those $S_{(s_1,\ldots,s_m),t}$ that do satisfy $\varphi(\mathbf{x})$. Using that $<, >$, and $=$ may be rewritten with $\leq$, these sets are of the required form. $\square$

Since S_t has now been written as a disjoint union, we may examine each piece separately; see Remark 4.3 above.

Our next task is to eliminate the $D_c(\cdot)$ atomic formulas with an affine reduction. To do this, let's look at a conjunction of formulas, each of the form $D_c\big(\mathbf{f}(t)\cdot\mathbf{x}-g(t)\big)$. For each t, this will be a translate of a lattice. Using the language of [15], this could be called an "external" representation of this lattice translate, i.e., defined via constraints. We'd like an "internal" representation, i.e., defined parametrically; in this case, this would be a collection of basis vectors for the lattice, together with a translation vector. The content of the following proposition is that we can achieve this in an EQP way, cf. Example 2.8. Note that the proposition even applies when the divisibility relations are of the form $D_{h(t)}$, where $h(t) \in$ EQP.

Proposition 4.10. *Let $S_t \subseteq \mathbb{Z}^d$ be defined by*

$$\bigwedge_{j=1}^{n} D_{h_j(t)}\big(\mathbf{f}_j(t)\cdot\mathbf{x}-g_j(t)\big),$$

where $\mathbf{f}_j : \mathbb{N} \to \mathbb{Z}^d$ has EQP coordinates, $g_j, h_j : \mathbb{N} \to \mathbb{Z}$ in EQP, and $h_j(t)$ is eventually nonzero. Then there exist N and a period m, such that, for fixed i with $0 \le i \le m-1$, either

- *S_t is empty for all $t \in \mathbb{N}$ with $t \ge N$ and $t \equiv i \bmod m$, or*

- *there exist $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_r : \mathbb{N} \to \mathbb{Z}^d$ whose coordinate functions are polynomials in $\mathbb{Z}[t]$, such that, for all $t \in \mathbb{N}$ with $t \ge N$ and $t \equiv i \bmod m$, we have that*

$$S_t = \mathbf{u}_0(t) + \mathbb{Z}\mathbf{u}_1(t) + \cdots + \mathbb{Z}\mathbf{u}_r(t),$$

  where $\mathbf{u}_1(t), \ldots, \mathbf{u}_r(t)$ are linearly independent.

Proof. Note that S_t is the set of $\mathbf{x} \in \mathbb{Z}^d$ such that there exist $\mathbf{y} \in \mathbb{Z}^n$, such that

$$\mathbf{f}_j(t)\cdot\mathbf{x} + h_j(t)y_j = g_j(t),$$

for all $1 \le j \le n$. We create an $n \times (d+n)$ matrix A, with entries in EQP, as follows: let $A = [F\ D]$, where F is the $n \times d$ matrix whose j^{th} row is the coordinates of $\mathbf{f}_j(t)$, and D is the diagonal matrix whose (j, j) entry is $h_j(t)$. Let $\mathbf{g}$ be the $n \times 1$ column vector whose j^{th} entry is $g_j(t)$. Regarding $\mathbf{x}$ and $\mathbf{y}$ as column vectors, we have that S_t is the set of $\mathbf{x} \in \mathbb{Z}^d$ such that there exists $\mathbf{y} \in \mathbb{Z}^n$, such that

$$A\begin{bmatrix}\mathbf{x}\\\mathbf{y}\end{bmatrix} = \mathbf{g}.$$

Using Corollary 2.8 of [2], A may be put into *Hermite normal form*. That is, letting r be the rank of A (we actually have $r = n$ here, because the matrix D ensures that A is full row rank), there exist an $n \times r$ matrix B and a $(d+n) \times (d+n)$ matrix U such that

- *$AU = [B\ 0]$,*

- all entries above the main diagonal of B are 0,

- all entries along the main diagonal of B are positive,

- all entries below the main diagonal of B are nonnegative, and each row achieves its maximum uniquely on the main diagonal,

- U is unimodular, i.e., determinant ± 1 (U encodes the elementary column operations transforming A into B), and

- all entries are in EQP.

Corollary 5.3b of [15] shows that the set of integer solutions to $A \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix} = \mathbf{g}$ is nonempty if and only if $B^{-1}\mathbf{g}$ is an integer. The entries of B^{-1} may be ratios of EQPs; the set of t for which $B^{-1}\mathbf{g}$ is integral will be eventually periodic. Therefore we may assume we are looking at a residue class i mod m such that $B^{-1}\mathbf{g}$ is integral. Then Corollary 5.3c of [15] shows that the set of integer solutions to $A \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix} = \mathbf{g}$ can be written in the form

$$\mathbf{v}_0(t) + \mathbb{Z}\mathbf{v}_1(t) + \cdots + \mathbb{Z}\mathbf{v}_d(t),$$

where $\mathbf{v}_1(t), \ldots, \mathbf{v}_d(t)$ are linearly independent; in particular,

$$\mathbf{v}_0 = U \begin{bmatrix} B^{-1}\mathbf{g} \\ 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{v}_j = (n+j)^{\text{th}} \text{ column of } U,$$

for $1 \leq j \leq d$, and so the entries of $\mathbf{v}_j : \mathbb{N} \to \mathbb{Z}^{d+n}$ are in EQP. For $0 \leq j \leq d$, let $\mathbf{w}_j$ be the first d coordinates of $\mathbf{v}_j$. Then

$$S_t = \mathbf{w}_0(t) + \mathbb{Z}\mathbf{w}_1(t) + \cdots + \mathbb{Z}\mathbf{w}_d(t).$$

We are almost finished; the only problem is that the $\mathbf{w}_1, \ldots, \mathbf{w}_d$ may not be linearly independent. Let A' be the $d \times d$ matrix whose columns are $\mathbf{w}_1, \ldots, \mathbf{w}_d$, and let r be the rank of A'. Putting A' in Hermite normal form, we have a $d \times d$ unimodular matrix U' and a $d \times r$ matrix B', such that $A'U' = [B' \ 0]$ with restrictions on the entries of B' as above. Let $\mathbf{u}_1 \ldots, \mathbf{u}_r$ be the columns of B', which are linearly independent. Since elementary column operations don't affect the $\mathbb{Z}$-span of the columns,

$$\mathbb{Z}\mathbf{w}_1(t) + \cdots + \mathbb{Z}\mathbf{w}_d(t) = \mathbb{Z}\mathbf{u}_1(t) + \cdots + \mathbb{Z}\mathbf{u}_r(t).$$

Taking $\mathbf{u}_0 = \mathbf{w}_0$, we have the desired property:

$$S_t = \mathbf{u}_0(t) + \mathbb{Z}\mathbf{u}_1(t) + \cdots + \mathbb{Z}\mathbf{u}_r(t),$$

where $\mathbf{u}_1(t), \ldots, \mathbf{u}_r(t)$ are linearly independent. $\qquad \square$

To recall, we have written the set we are interested in as a disjoint union of sets, each defined by a conjunction of atomic formulas of the form $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and $D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))$. We now show that we can eliminate the $D_c(\cdot)$ formulas, with an affine reduction, cf. Example 2.9. In fact, this would work even for divisibility by non-constant $h(t)$:

Lemma 4.11. *Let $S_t \subseteq \mathbb{Z}^d$ be defined by an $\mathcal{L}_{\mathrm{EQP}}^+$ formula, $\varphi(\mathbf{x})$, that is a conjunction of atomic formulas, each of the form*

- $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ *or*

- $D_{h(t)}\big(\mathbf{f}(t) \cdot \mathbf{x} - g(t)\big),$

where $\mathbf{f} : \mathbb{N} \to \mathbb{Z}^d$ has EQP coordinates, $g, h : \mathbb{N} \to \mathbb{Z} \in \mathrm{EQP}$, and h is eventually nonzero.

Then there is some $S_t' \subseteq \mathbb{Z}^{d'}$, affine reducible to S_t, such that $S_t' \subseteq \mathbb{Z}^{d'}$ is defined by an $\mathcal{L}_{\mathrm{EQP}}$ formula that is a conjunction of atomic formulas of the form $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$, where $\mathbf{f} : \mathbb{N} \to \mathbb{Z}^d$ has EQP coordinates and $g(t) : \mathbb{N} \to \mathbb{Z}$ is in EQP.

Proof. Let $R_t \subseteq \mathbb{Z}^d$ be the set satisfying the conjunction of the $D_{h(t)}$ terms. R_t can be represented by:

$$\{\mathbf{u}_0(t) + \lambda_1 \mathbf{u}_1(t) + \cdots + \lambda_r \mathbf{u}_r(t) : \ \lambda_j \in \mathbb{Z}\},$$

where $\mathbf{u}_1(t), \ldots, \mathbf{u}_r(t)$ are linearly independent, by Proposition 4.10. We take as our affine reduction $F : \mathbb{Z}^r \to \mathbb{Z}^d$, given by $F(\lambda) = \mathbf{u}_0(t) + \lambda_1 \mathbf{u}_1(t) + \cdots + \lambda_r \mathbf{u}_r(t)$. Since the $\mathbf{u}_j$ are linearly independent, this defines a bijection $\mathbb{Z}^r \to R_t$. An element $\mathbf{x} \in S_t$ satisfying a linear inequality $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ is equivalent to $\lambda = F^{-1}(\mathbf{x})$ satisfying

$$\mathbf{f}(t) \cdot \big(\mathbf{u}_0(t) + \lambda_1 \mathbf{u}_1(t) + \cdots + \lambda_r \mathbf{u}_r(t)\big) \leq g(t),$$

which simplifies to a linear inequality of the desired form. $\qquad\square$

Now we have S_t written as the set of integer points in a "parametric polyhedron", that is, defined by linear inequalities that depend on t, as above. If this polyhedron is bounded, then it immediately follows from [3] that $|S_t| \in \mathrm{EQP}$. We must detect when S_t is unbounded. To do this, it is helpful to switch to an "internal" representation of the parametric polyhedron, as opposed to this "external" representation as a solution set to linear inequalities, cf. Example 2.10. That is, we want to write the polyhedron as

$$\mathrm{conv}\{\mathbf{x}_1, \ldots, \mathbf{x}_q\} + \mathrm{cone}\{\mathbf{y}_1, \ldots, \mathbf{y}_r\} + \mathrm{span}\{\mathbf{z}_1, \ldots, \mathbf{z}_s\},$$

where

$$\mathbf{x}_i \in \mathbb{Q}^d, \ \mathbf{y}_j, \mathbf{z}_k \in \mathbb{Z}^d - \{0\},$$
$$A + B = \{a + b : \ a \in A, \ b \in B\},$$
$$\mathrm{conv}\{\mathbf{x}_1, \ldots, \mathbf{x}_q\} = \{\lambda_1 \mathbf{x}_1 + \cdots + \lambda_q \mathbf{x}_q : \ \lambda_i \in \mathbb{R}, \ \lambda_i \geq 0, \ \lambda_1 + \cdots + \lambda_r = 1\},$$
$$\mathrm{cone}\{\mathbf{y}_1, \ldots, \mathbf{y}_r\} = \{\lambda_1 \mathbf{y}_1 + \cdots + \lambda_r \mathbf{y}_r : \ \lambda_i \in \mathbb{R}, \ \lambda_i \geq 0\},$$
$$\mathrm{span}\{\mathbf{z}_1, \ldots, \mathbf{z}_s\} = \{\lambda_1 \mathbf{z}_1 + \cdots + \lambda_s \mathbf{z}_s : \ \lambda_i \in \mathbb{R}\},$$

and $\mathrm{cone}\{\mathbf{y}_1, \ldots, \mathbf{y}_r\}$ contains no lines. We follow the convention that $\mathrm{conv}\{\emptyset\} = \emptyset$, $\mathrm{cone}\{\emptyset\} = \{\mathbf{0}\}$, and $\mathrm{span}\{\emptyset\} = \{\mathbf{0}\}$, so that this representation may include the empty polyhedron. Also note that the polyhedron is bounded exactly when $r = s = 0$. We have the following proposition:

Proposition 4.12. *Suppose $S_t \subseteq \mathbb{Z}^d$ is defined by*

$$\bigwedge_{j=1}^{n} \mathbf{f}_j(t) \cdot \mathbf{x} \leq g_j(t),$$

where $\mathbf{f}_j : \mathbb{N} \to \mathbb{Z}^d$ has EQP coordinates and $g_j : \mathbb{N} \to \mathbb{Z}$ in EQP. Then there exists N and a period m such that, for fixed i with $0 \leq i \leq m$, there exist $\mathbf{x}_1, \ldots, \mathbf{x}_q : \mathbb{N} \to \mathbb{Q}^d$ and $\mathbf{y}_1, \ldots, \mathbf{y}_r, \mathbf{z}_1 \ldots, \mathbf{z}_s : \mathbb{N} \to \mathbb{Z}^d$, with $\mathbf{x}_j$ rational functions in $\mathbb{Q}(t)$ and $\mathbf{y}_j, \mathbf{z}_k$ nonzero polynomials in $\mathbb{Z}[t]$, such that, for all $t \in \mathbb{N}$ with $t \geq N$ and $t \equiv i \bmod m$, we have that S_t is the set of integer points in

$$\mathrm{conv}\{\mathbf{x}_1(t), \ldots, \mathbf{x}_q(t)\} + \mathrm{cone}\{\mathbf{y}_1(t), \ldots, \mathbf{y}_r(t)\} + \mathrm{span}\{\mathbf{z}_1(t), \ldots, \mathbf{z}_s(t)\},$$

where $\mathrm{cone}\{\mathbf{y}_1(t), \ldots, \mathbf{y}_r(t)\}$ contains no lines.

Proof. We may assume we are looking at a residue class $i \bmod m$ such that g_j and the coordinates of $\mathbf{f}_j$ are in $\mathbb{Q}[t]$. Let F be the $n \times d$ matrix whose j^{th} row is f_j, and let $\mathbf{g}$ be the $n \times 1$ column vector whose j^{th} entry is g_j. Regarding $\mathbf{x} \in \mathbb{Z}^d$ as a column vector, S_t is the set integer solutions to $F \cdot \mathbf{x} \leq \mathbf{g}$. Note that we may perform standard row reduction on F, in the field of rational functions $\mathbb{Q}(t)$. This suffices to compute the desired representation, using Theorem 8.5 of [15], as follows:

- For the convex hull, take any maximally linear independent subset of rows, F', of F and their corresponding $\mathbf{g}'$. (Note that any given subset of rows of F is either eventually always linearly dependent or eventually always linearly independent, since this can be tested by computing determinants of minors of F, which are polynomial functions in t.) Take any solution $\mathbf{x}(t)$ to $F' \cdot \mathbf{x} = \mathbf{g}'$; $\mathbf{x}$ may be computed using row reduction and will have entries in $\mathbb{Q}(t)$. If $\mathbf{x}(t)$ eventually satisfies $F \cdot \mathbf{x} \leq \mathbf{g}$, then include it as one of the $\mathbf{x}_j(t)$. Doing this for all maximally linearly independent set of rows of F yields $\mathrm{conv}\{\mathbf{x}_1(t), \ldots, \mathbf{x}_q(t)\}$.

- For the cone, take any subset of rows, F', and a distinct row, $\mathbf{f}$, such that F' and $\mathbf{f}$ together are a maximally linear independent subset of rows of F. Take any solution $\mathbf{y}(t)$ to

$$\begin{bmatrix} F' \\ \mathbf{f} \end{bmatrix} \mathbf{y} = \begin{bmatrix} \mathbf{0} \\ -1 \end{bmatrix}.$$

  This may again be computed using row reduction and will have entries in $\mathbb{Q}(t)$. If $\mathbf{y}(t)$ eventually satisfies $F \cdot \mathbf{y} \leq \mathbf{0}$, then include $p(t)\mathbf{y}(t)$ as one of the $\mathbf{y}_j(t)$, where $p \in \mathbb{Z}[t]$ is eventually positive and makes $p\mathbf{y} \in \mathbb{Z}[t]$. Doing this for all such F' and $\mathbf{f}$ yields $\mathrm{cone}\{\mathbf{y}_1(t), \ldots, \mathbf{y}_r(t)\}$.

- Use row reduction to find a basis for $F \cdot \mathbf{z} = \mathbf{0}$. Clearing fractions to make each $\mathbf{z}_j(t) \in \mathbb{Z}[t]$, this yields $\mathrm{span}\{\mathbf{z}_1(t), \ldots, \mathbf{z}_s(t)\}$. $\qquad\square$

4.6 Step 6

In the output of Proposition 4.12, any polyhedron P with $r = s = 0$ is bounded, and we may apply the results from [3] and from [17]. The following lemma helps us deal with unbounded polyhedra.

Lemma 4.13. *Suppose we have a polyhedron, $P \subseteq \mathbb{R}^d$, given by*

$$P = \mathrm{conv}\{\mathbf{x}_1,\ldots,\mathbf{x}_q\} + \mathrm{cone}\{\mathbf{y}_1,\ldots,\mathbf{y}_r\} + \mathrm{span}\{\mathbf{z}_1,\ldots,\mathbf{z}_s\},$$

with $\mathbf{x}_i \in \mathbb{Q}^d$, $\mathbf{y}_j, \mathbf{z}_k \in \mathbb{Z}^d - \{0\}$. Let

$$Q = \mathrm{conv}\{\mathbf{x}_1,\ldots,\mathbf{x}_q\} + \mathrm{zono}\{\mathbf{y}_1,\ldots,\mathbf{y}_r,\mathbf{z}_1,\ldots,\mathbf{z}_s\},$$

where $\mathrm{zono}\{\mathbf{w}_1,\ldots,\mathbf{w}_u\} = \{\lambda_1\mathbf{w}_1 + \cdots + \lambda_u\mathbf{w}_u : \lambda_i \in \mathbb{R}, 0 \le \lambda_i \le 1\}$ is the zonotope (Minkowski sum of line segments) generated by the $\mathbf{w}_i$.

Assume either $r \ge 1$ or $s \ge 1$. Then

- *if Q contains an integer point, then P contains an infinite number of integer points, and*

- *if Q contains no integer points, then P contains no integer points.*

Furthermore, Q is a bounded polyhedron, given by the convex hull of the following points: for each $W \subseteq \{\mathbf{y}_1,\ldots,\mathbf{y}_s,\mathbf{z}_1,\ldots,\mathbf{z}_t\}$ and i with $1 \le i \le q$, take the point

$$\mathbf{x}_i + \sum_{\mathbf{w}\in W} \mathbf{w}.$$

Proof. Without loss of generality, $r \ge 1$. If Q contains an integer point, $\mathbf{x}$, then certainly $\mathbf{x} \in P$, since $Q \subseteq P$. But also $\mathbf{x} + k\mathbf{y}_1 \in P$, for all $k \in \mathbb{N}$, so P contains an infinite number of integer points.

We prove the contrapositive of the second bullet point. Suppose P contains an integer point

$$\sum_i \lambda_i\mathbf{x}_i + \sum_j \mu_j\mathbf{y}_j + \sum_k \nu_k\mathbf{z}_k,$$

with $\lambda_i, \mu_k \ge 0$, $\sum_i \lambda_i = 1$. Then Q contains the integer point

$$\sum_i \lambda_i\mathbf{x}_i + \sum_j [\mu_j]\mathbf{y}_j + \sum_k [\nu_k]\mathbf{z}_k,$$

where $[\eta]$ is the unique real number in $[0,1)$ such that $\eta - [\eta]$ is an integer.

The representation of Q as a convex hull follows from the fact that Q is the Minkowski sum of $\mathrm{conv}\{\mathbf{x}_1,\ldots,\mathbf{x}_q\}$, the line segments $[0,\mathbf{y}_i]$, and the line segments $[0,\mathbf{z}_i]$, and the standard observation that each vertex of a Minkowski sum can be written as the sum of vertices of the summand polytopes. $\square$

We now have all the ingredients necessary to prove Properties 1, 2, and 3. Using all of the results of this section up to Proposition 4.12, and noting that all of the properties only need to be shown for all sufficiently large t congruent to some i modulo a fixed number m, it suffices to show the following.

Proposition 4.14. *Suppose S_t is the set of integer points in*

$$\mathrm{conv}\{\mathbf{x}_1(t),\ldots,\mathbf{x}_q(t)\} + \mathrm{cone}\{\mathbf{y}_1(t),\ldots,\mathbf{y}_r(t)\} + \mathrm{span}\{\mathbf{z}_1(t),\ldots,\mathbf{z}_s(t)\},$$

as in Proposition 4.12. Then

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

2. *The set of t such that S_t has finite cardinality is eventually periodic.*

3. *There exists an EQP $g : \mathbb{N} \to \mathbb{N}$ such that, if S_t has finite cardinality, then $g(t) = |S_t|$.*

4. *There exists a function $\mathbf{x} : \mathbb{N} \to \mathbb{Z}^d$, whose coordinate functions are EQPs, such that, if S_t is nonempty, then $\mathbf{x}(t) \in S_t$.*

Proof. Note that Woods [19] shows that these follow from the EQP behavior of the generating function, which we discuss and prove in Section 5 (at least for $S \subseteq \mathbb{N}^d$, a case we could reduce to). We therefore only present a brief proof here, to demonstrate that generating functions are unnecessary.

First consider the case that $r = s = 0$; i.e. S_t is the set of integer points in the parametric polytope

$$\text{conv}\{\mathbf{x}_1(t), \dots, \mathbf{x}_q(t)\}.$$

Then S_t is finite for all t so (2) is immediate. Furthermore, (3) is the main result of Chen-Li-Sam [3, Theorem 2.1]: the idea of the proof is that writing each variable "base t" (as in Step 3) reduces this to a problem in classic Ehrhart Theory (see Example 1.4).

Next, (4) is effectively the main result of Shen [17, Corollary 3.2.2], which proves that, for any $\mathbf{c} \in \mathbb{Z}^d$, the maximum value of $\mathbf{c} \cdot \mathbf{x}$ is EQP (in fact, it proves a slightly more general statement). To prove (4), we might demonstrate that an *argmax* (an $\mathbf{x}$ maximizing this linear function $\mathbf{c} \cdot \mathbf{x}$) has EQP coordinates. While [17] demonstrates only that the *max* value of $\mathbf{c} \cdot \mathbf{x}$ is an EQP, it is clear that the proof also works for the argmax. The key idea is that, after performing the "base t" reduction, such an $\mathbf{x}$ must be within a fixed distance to one of the facets of the parametric polytope [17, Proposition 4.1]; therefore, by searching all parallel hyperplanes within that fixed distance of a facet, we reduce the dimension of the problem inductively.

To instead derive (4) directly from the statement of Shen [17, Corollary 3.2.2], we may do the following: First take, $c = e_1$ to get a maximum value for the x_1 coordinate, say a_1. Then, substitute the value a_1 in for x_1 into the definition of our polyhedron, reducing the dimension by one; we now have the cross-section of the original polyhedron at $x_1 = a_1$. Then take $c = e_2$ to get the maximum in the x_2 coordinate, and repeat.

Finally, (1) follows from the other properties as proved in [19]. For example, (3) yields that $|S_t|$ is an EQP, and the only way to have an infinite number of zeros in this EQP is for a constituent polynomial to be identically zero. Alternatively, (1) also follows from the proofs in [17].

Now suppose that either $r \geq 1$ or $s \geq 1$. Again let

$$Q = \text{conv}\{\mathbf{x}_1, \dots, \mathbf{x}_q\} + \text{zono}\{\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_s\}.$$

By Lemma 4.13, Q is a parametric polytope so we can apply the previous case to the set $S_t' := Q \cap \mathbb{Z}^d$. In particular, the set of t for which S_t' is nonempty is eventually periodic. But since (again by Lemma 4.13) S_t is finite iff S_t is empty iff S_t' is empty, (1), (2), and (3) immediately follow. Also, (4) holds for S_t' by the previous case. Since $Q \subseteq P$ and S_t is empty iff S_t' is empty, we see that (4) also holds for S_t by simply choosing a point in S_t'. $\square$

5 Generating Functions

Given a set $S \subseteq \mathbb{N}^d$, we define its generating function to be

$$\sum_{\mathbf{s} \in S} \mathbf{x}^{\mathbf{s}} = \sum_{\mathbf{s} \in S} x_1^{s_1} x_2^{s_2} \cdots x_d^{s_d}.$$

These generating functions can often be simplified to a rational function.

Example 5.1. The generating function for $S = \mathbb{N}$ is

$$\sum_{s \in \mathbb{N}} x^s = 1 + x + x^2 + \cdots = \frac{1}{1-x},$$

and the infinite sum is convergent for $|x| < 1$.

Now let S_t be a parametric Presburger family. For a fixed $t \in \mathbb{N}$, S_t has a generating function, and Property 4 examines what happens to this generating function as t changes.

Example 5.2. For the triangle P from Example 1.5 with vertices $(0,0)$, $\left(\frac{1}{2},0\right)$, and $\left(\frac{1}{2},\frac{1}{2}\right)$, we have the generating function

$$\sum_{\mathbf{s} \in tP \cap \mathbb{Z}^d} \mathbf{x}^{\mathbf{s}} = \left(1 + x_1 + x_1^2 + \cdots + x_1^{\lfloor t/2 \rfloor}\right)$$

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

$$= \frac{1}{(1-x_1)(1-x_1 x_2)} - \frac{x_1^{\lfloor t/2 \rfloor + 1}}{(1-x_1)(1-x_2)} + \frac{x_1^{\lfloor t/2 \rfloor + 1} x_2^{\lfloor t/2 \rfloor + 2}}{(1-x_2)(1-x_1 x_2)}$$

$$= \frac{1 - x_2 - (1 - x_1 x_2) x_1^{\lfloor t/2 \rfloor + 1} + (1 - x_1) x_1^{\lfloor t/2 \rfloor + 1} x_2^{\lfloor t/2 \rfloor + 2}}{(1-x_1)(1-x_2)(1-x_1 x_2)}$$

(the second equality can be verified directly by expanding the fractions as products of geometric series).

Note that the above example satisfies Property 4.

Generating functions are powerful tools for understanding the structure of S_t. For example, given the generating function, we can count the number of integer points in S_t (if finite) by substituting in $\mathbf{x} = (1, \ldots, 1)$.

Example 5.3. Substituting $x_1 = x_2 = 1$ into the generating function for Example 5.2, we see that $(1,1)$ is a zero of the numerator and denominator of this rational function. Fortunately, 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 Example 1.5.

Remark 5.4. To prove Property 4 for parametric Presburger families, we will assume from now on that $S_t \subseteq \mathbb{N}^d$. We must check that the EQP-affine reductions in Steps 2, 3, and 5 above result in a family S_t' which is still a subset of $\mathbb{N}^{d'}$ for some d' (rather than simply a subset of $\mathbb{Z}^{d'}$), but this is immediate upon inspection. Steps 1 and 4 do not cause any problems either since they give logically equivalent formulas which define the same parametric Presburger family.

While one may instead define generating functions for subsets of $\mathbb{Z}^d$, this may lose information about the sets:

Example 5.5. If $S = \mathbb{Z}$, then the generating function for S is

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

If you regard this as an infinite series, then it doesn't converge on any open neighborhood. If you regard it as a formal power series, then it simplifies to

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

which is also the generating function for the empty set.

In the statement of Property 4, we need $\mathbf{b}_{ij}(t)$ to be lexicographically positive rather than simply in $\mathbb{N}^d \setminus \{0\}$ for examples like the following:

Example 5.6. Let $S_t = \{(x,y) \in \mathbb{N}^2 : x + y = t\}$. Then the generating function for S_t is

$$y^t + xy^{t-1} + \cdots + x^t = \frac{y^t - x^{t+1}y^{-1}}{1 - xy^{-1}}.$$

Remark 5.7. If $\mathbf{b}$ is lexicographically negative, then we may instead write

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

with $-\mathbf{b}$ lexicographically positive.

Remark 5.8. 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 on a neighborhood of $\mathbf{a} \doteq (e^{-\varepsilon}, e^{-\varepsilon^2}, \ldots, e^{-\varepsilon^d})$, for sufficiently small ε, as follows: Let $b_i > 0$ be the first nonzero coordinate of $\mathbf{b}$. Then

$$\ln\left(\mathbf{a}^{\mathbf{b}}\right) = -\varepsilon b_1 - \varepsilon^2 b_2 - \cdots - \varepsilon^d b_d = -\varepsilon^i b_i - \cdots - \varepsilon^d b_d.$$

For sufficiently small ε, the $-\varepsilon^i b_i$ term dominates, and $\ln(\mathbf{a}^{\mathbf{b}}) < 0$. This implies that $|\mathbf{a}^{\mathbf{b}}| < 1$, and indeed $1 + \mathbf{x}^{\mathbf{b}} + \mathbf{x}^{2\mathbf{b}} + \cdots$ does converge on a neighborhood of $\mathbf{a}$.

Now we prove Property 4, for parametric Presburger families. The hardest work has already been done:

- At the end of Step 4, we had that S_t was affine reducible to a set S_t', described by a quantifier free formula in parametric Presburger arithmetic.

- By [19, Theorem 3.5(a)], any set described by a quantifier-free formula has Property 4.

The only remaining step is to check that Property 4 is preserved by affine reductions. First a short lemma:

Lemma 5.9. *Let $S \subseteq \mathbb{N}^d$ and $S' \subseteq \mathbb{N}^e$ be sets such that there is a $\mathbb{Z}$-affine linear function $F : \mathbb{Z}^e \to \mathbb{Z}^d$ that restricts to a bijection from S' to S. Let $F(\mathbf{x}) = A\mathbf{x} + \mathbf{c}$, where $A = (a_{ij})$. Define monomials $m_i = w_1^{a_{1i}} \cdots w_d^{a_{di}}$ for $i = 1, \ldots, e$. Let $g(z_1, \ldots, z_e) = g(\mathbf{z})$ be the generating function for S'. Then the generating function for S is $\mathbf{w}^{\mathbf{c}} g(m_1, \ldots, m_e)$, where $\mathbf{w} := (w_1, \ldots, w_d)$.*

Proof. Let $h(w_1, \ldots, w_d) =: h(\mathbf{w})$ be the generating function for S. Then

$$h(\mathbf{w}) = \sum_{\mathbf{y} \in S} \mathbf{w}^{\mathbf{y}}$$

$$= \sum_{\mathbf{x} \in S'} \mathbf{w}^{A\mathbf{x} + \mathbf{c}}$$

$$= \mathbf{w}^{\mathbf{c}} \sum_{\mathbf{x} \in S'} w_1^{a_{11}x_1 + \ldots + a_{1e}x_e} \cdots w_d^{a_{d1}x_1 + \ldots + a_{de}x_e}$$

$$= \mathbf{w}^{\mathbf{c}} \sum_{\mathbf{x} \in S'} \left(w_1^{a_{11}} \cdots w_d^{a_{d1}} \right)^{x_1} \cdots \left(w_1^{a_{1e}} \cdots w_d^{a_{de}} \right)^{x_e}$$

$$= \mathbf{w}^{\mathbf{c}} \sum_{\mathbf{x} \in S'} m_1^{x_1} \cdots m_e^{x_e}$$

$$= \mathbf{w}^{\mathbf{c}} g(m_1, \ldots, m_e)$$

where the second equality follows because F restricts to a bijection from S' to S. $\qquad \square$

Proposition 5.10. *Suppose $S'_t \subseteq \mathbb{N}^{d'}$ is EQP-affine reducible to $S_t \subseteq \mathbb{N}^d$. If S'_t has Property 4, then so does S_t.*

Proof. First consider the case that the affine reduction is defined by polynomials and that there is no periodicity in the generating function $g(\mathbf{z}, t)$ for S'_t. That is, $F(\mathbf{x}) = A(t)\mathbf{x} + \mathbf{c}(t)$ where $A(t) \in \mathbb{Z}[t]^{d \times e}$ and $\mathbf{c}(t) \in \mathbb{Z}[t]^d$, and

$$g(\mathbf{z}, t) := \sum_{\mathbf{x} \in S'_t} \mathbf{z}^{\mathbf{x}} = \frac{\sum_{j=1}^{n_i} \alpha_j \mathbf{z}^{\mathbf{q_j(t)}}}{\left(1 - \mathbf{z}^{\mathbf{b_1}(t)}\right) \cdots \left(1 - \mathbf{z}^{\mathbf{b_k}(t)}\right)},$$

where the coordinate functions of $\mathbf{q_j}$ and $\mathbf{b_j}$ are polynomials with the $\mathbf{b_j}$ lexicographically positive.

Fix notation as in Lemma 5.9 and additionally define $\mathbf{m}(t) = (m_1(t), \ldots m_e(t))$, where $m_i(t) = w_1^{a_{1i}(t)} \cdots w_d^{a_{di}(t)}$ and $w_1, \ldots, w_d$ are variables. Applying Lemma 5.9 for each value of t, we see that the generating function $h(\mathbf{w}, t)$ of S_t is given by

$$h(\mathbf{w}, t) = \mathbf{w}^{\mathbf{c}(t)} g(m_1(t), \ldots, m_e(t))$$

$$= \mathbf{w}^{\mathbf{c}(t)} \frac{\sum_{j=1}^{n_i} \alpha_j \mathbf{m}(t)^{\mathbf{q_j(t)}}}{\left(1 - \mathbf{m}(t)^{\mathbf{b_1}(t)}\right) \cdots \left(1 - \mathbf{m}(t)^{\mathbf{b_k}(t)}\right)}.$$

Writing $\mathbf{q_j}(\mathbf{t}) = (q_j^1(t), \ldots, q_j^e(t))$, we have that

$$\mathbf{m}(t)^{q_j(t)} = \left(w_1^{a_{11}(t)} \cdots w_d^{a_{d1}(t)} \right)^{q_j^1(t)} \cdots \left(w_1^{a_{1e}(t)} \cdots w_d^{a_{de}(t)} \right)^{q_j^e(t)}$$

$$= w_1^{a_{11}(t)q_j^1(t) + \ldots + a_{1e}(t)q_j^e(t)} \cdots w_d^{a_{d1}(t)q_j^1(t) + \ldots + a_{de}(t)q_j^e(t)}$$

so the exponents of $w_1, \ldots, w_d$ in the numerator are polynomial functions of t, and remain so after multiplying in the factor of $\mathbf{w}^{\mathbf{c}}(t)$ outside the sum. Similarly, the exponents of $w_1, \ldots, w_d$ in each factor in the denominator are polynomials in t. If any of these exponents are (eventually) lexicographically negative, apply Remark 5.7 to make them eventually lexicographically positive.

In the general case, let t_0 be chosen sufficiently large so that the affine reduction is defined by quasi-polynomials for all $t > t_0$ and also the function g has the desired form as a rational function for all $t > t_0$. Let D be the least common multiple of all periods occurring in either the affine reduction or the generating function g. Then the generating function h has the desired form with period D for all $t > t_0$. $\qquad\qquad\square$

References

[1] Matthias Beck and Sinai Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics, Springer, 2007. 2

[2] Danny Calegari and Alder Walker. Integer hulls of linear polyhedra and scl in families. *Transactions of the American Mathematical Society*, **365** (2013), 5085–5102. 3, 4, 7, 24

[3] Sheng Chen, Nan Li, and Steven V. Sam. Generalized Ehrhart polynomials. *Transactions of the American Mathematical Society*, **364** (2012), 551–569. 3, 9, 12, 13, 19, 20, 26, 27, 29

[4] D. C. Cooper. Theorem proving in arithmetic without multiplication. *Machine Intelligence*, **7** (1972), 91–99. 7, 21

[5] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *Comptes Rendues de l'Académie des Sciences, Paris*, **254** (1962), 616–618. 2

[6] Herbert Enderton. *A mathematical introduction to logic*. Harcourt / Academic Press, 2001. 13

[7] John Goodrick. Bounding quantification in parametric expansions of Presburger arithmetic, 2016, arXiv:1604.06166. 8, 11, 13, 15, 16, 18, 22

[8] Branko Grünbaum. *Convex polytopes*. Springer, 2003. 7

[9] Wilfrid Hodges. *Model theory*. Cambridge University Press, 1993. 13

[10] Jan Krajíček. Discretely ordered modules as a first-order extension of the cutting planes proof system. *J. Symb. Log.*, **63** (1998), no. 4, 1582–1596. 13

[11] Aless Lasaruk and Thomas Sturm. Weak quantifier elimination for the full linear theory of the integers. *Applicable Algebra in Engineering*, Communication and Computing **18** (2007), no. 6, 545–574. 8, 15

[12] Mojżesz Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen in welchen die Addition als einzige Operation hervortritt. *Comptes-Rendus du premier Congrès des Mathèmaticiens des Pays Slaves*, 1929. 7

[13] 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** (1991), no. 2, 225–233, Translated from the German and with commentaries by Dale Jacquette. 7

[14] Bjarke Hammersholt Roune and Kevin Woods. The parametric Frobenius problem. *Electronic Journal of Combinatorics*, **22** (2015). 4

[15] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1986. 12, 24, 25, 27

[16] Bobby Shen. The parametric Frobenius problem and parametric exclusion. 2015, arXiv:1510.01349. 4

[17] Bobby Shen. Parametrizing an integer linear program by an integer. 2015, arXiv:1510.01343. 4, 12, 13, 27, 29

[18] Lou van den Dries and Jan Holly. Quantifier elimination for modules with scalar variables. *Ann. Pure Appl. Logic*, **57** (1992), 161–179. 13

[19] Kevin Woods. The unreasonable ubiquitousness of quasi-polynomials. *Electronic Journal of Combinatorics*, **21** (2014). 2, 4, 6, 12, 13, 29, 31

AUTHORS

Tristram Bogart
Associate Professor
Universidad de los Andes
Bogotá, Colombia
tc.bogart22 [at] uniandes [dot] edu [dot] co
http://wwwprof.uniandes.edu.co/~tc.bogart22/

John Goodrick
Associate Professor
Universidad de los Andes
Bogotá, Colombia
jr.goodrick427 [at] uniandes [dot] edu [dot] co
http://matematicas.uniandes.edu.co/~goodrick/

Kevin Woods
Associate Professor
Oberlin College
Oberlin, Ohio, USA
Kevin.Woods [at] oberlin [dot] edu
http://www.oberlin.edu/faculty/kwoods/