Parametric Presburger Arithmetic

Tristram Bogart

Universidad de los Andes

13 March 2018

Quasi-polynomials

A function $g : \mathbb{N} \to \mathbb{Z}$ is:

- quasi-polynomial (QP) if there exists a period m and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that

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

- eventually quasi-polynomial (EQP) if it agrees with a quasi-polynomial for all sufficiently large t.

Quasi-polynomials

A function $g : \mathbb{N} \to \mathbb{Z}$ is:

- quasi-polynomial (QP) if there exists a period m and polynomials $f_0, \ldots, f_{m-1} \in \mathbb{Q}[t]$ such that

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

- eventually quasi-polynomial (EQP) if it agrees with a quasi-polynomial for all sufficiently large t.

Example

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

Ehrhart's Theorem

Theorem (Ehrhart, 1962)

Let $A \in \mathbb{Z}^{m\times d}$, $\mathbf{b} \in \mathbb{Z}^m$, *and suppose the rational polyhedron* $P = \{\mathbf{x} \in \mathbb{R}^d : \; A\mathbf{x} \le b\}$ *is a polytope (i.e., that* P *is bounded.)*
For each $t \in \mathbb{N}$, *let*

$$S_t = tP \cap \mathbb{Z}^d = \{\mathbf{x} \in \mathbb{Z}^d : \; A\mathbf{x} \le \mathbf{b}t\}.$$

Then the function $L_P(t) = |S_t|$ *is quasi-polynomial.*

Ehrhart's Theorem

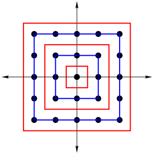
Theorem (Ehrhart, 1962)

Let $A \in \mathbb{Z}^{m \times d}$, $\mathbf{b} \in \mathbb{Z}^m$, and suppose the rational polyhedron $P = \{\mathbf{x} \in \mathbb{R}^d : A\mathbf{x} \leq b\}$ is a polytope (i.e., that P is bounded.) For each $t \in \mathbb{N}$, let

$$S_t = tP \cap \mathbb{Z}^d = \{\mathbf{x} \in \mathbb{Z}^d : A\mathbf{x} \leq \mathbf{b}t\}.$$

Then the function $L_P(t) = |S_t|$ is quasi-polynomial.

Example $P = \left\{ (x, y) \in \mathbb{R}^2 : \begin{bmatrix} -2 & 0 \\ 0 & -2 \\ 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \leq \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\}$



$$L_P(t) = \begin{cases} (t+1)^2 & \text{if } t \text{ is even;} \\ t^2 & \text{if } t \text{ is odd.} \end{cases}$$

Parametric Polytopes

Theorem (Chen-Li-Sam, 2012)

Let $A(t) \in \mathbb{Z}[t]^{m\times d}$, $\mathbf{b}(t) \in \mathbb{Z}[t]^m$. *For each* $t \in \mathbb{N}$, *let*

$$S_t = \{\mathbf{x} \in \mathbb{Z}^d : \ A(t)\mathbf{x} \le \mathbf{b}(t)\}.$$

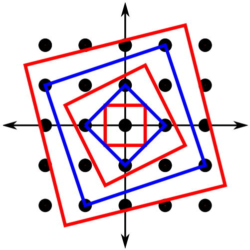
Then the function $g(t) = |S_t|$ *(if finite) is eventually quasi-polynomial.*

Ehrhart's Theorem is the case where A is constant and $\mathbf{b}$ is linear of the form $\mathbf{b}(t) = \mathbf{b}t$.

An Example of the Chen-Li-Sam Theorem

Example (Kevin Woods):

$$S_t = \left\{ (x, y) \in \mathbb{Z}^2 : \begin{cases} |2x + (2t-2)y| & \leq t^2 - 2t + 2 \\ |(2-2t)x_1 + 2x_2| & \leq t^2 - 2t + 2 \end{cases} \right\}$$



$$|S_t| = \begin{cases} t^2 - 2t + 2 & \text{for t odd} \\ t^2 - 2t + 5 & \text{for t even} \end{cases}$$

The Frobenius problem

Suppose $a_1, \ldots, a_s \in \mathbb{N}$ and $\gcd(a_1, \ldots, a_s) = 1$. Find the maximum element of

$$S = \{x \in \mathbb{N} : \neg\exists y_1, \ldots, y_s \in \mathbb{N}\,[x = y_1 a_1 + \cdots + y_s a_s]\},$$

Example: $a_1 = 3, a_2 = 8$.
$S^C = \{0, 3, 6, 8, 9, 11, 12, 14, 15, 16, \ldots\}$. $g(3, 8) = 13$.

The Frobenius problem

Suppose $a_1, \ldots, a_s \in \mathbb{N}$ and $\gcd(a_1, \ldots, a_s) = 1$. Find the maximum element of

$$S = \{x \in \mathbb{N} : \neg\exists y_1, \ldots, y_s \in \mathbb{N}\,[x = y_1 a_1 + \cdots + y_s a_s]\},$$

Example: $a_1 = 3, a_2 = 8$.
$S^C = \{0, 3, 6, 8, 9, 11, 12, 14, 15, 16, \ldots\}$. $g(3, 8) = 13$.
Parametric version: for each $t \in \mathbb{N}$, find the maximum of

$$S_t = \{x \in \mathbb{N} : \neg\exists y_1, \ldots, y_s \in \mathbb{N}\,[x = y_1 a_1(t) + \cdots + y_s a_s(t)]\},$$

the complement of the projection of the integer points in a parametric polyhedron.

The Frobenius problem

Suppose $a_1, \ldots, a_s \in \mathbb{N}$ and $\gcd(a_1, \ldots, a_s) = 1$. Find the maximum element of

$$S = \{x \in \mathbb{N} : \neg \exists y_1, \ldots, y_s \in \mathbb{N}\, [x = y_1 a_1 + \cdots + y_s a_s]\},$$

Example: $a_1 = 3, a_2 = 8$.
$S^C = \{0, 3, 6, 8, 9, 11, 12, 14, 15, 16, \ldots\}$. $g(3, 8) = 13$.
Parametric version: for each $t \in \mathbb{N}$, find the maximum of

$$S_t = \{x \in \mathbb{N} : \neg \exists y_1, \ldots, y_s \in \mathbb{N}\, [x = y_1 a_1(t) + \cdots + y_s a_s(t)]\},$$

the complement of the projection of the integer points in a parametric polyhedron.

Theorem (Bobby Shen, 2015)

Let $a_1(t), \ldots, a_s(t) \in \mathbb{Z}[t]$ be such that for $t \gg 0$, $a_i(t) > 0$ and $\gcd(a_1(t), \ldots, a_s(t)) = 1$. Then $g(a_1(t), \ldots, a_s(t))$ is eventually quasi-polynomial.

A Common Framework

A parametric Presburger set (as defined by Woods) is a family of sets $S_t \subseteq \mathbb{Z}^d$, one for each natural number t, defined using a Boolean combination of linear inequalities of the form

$$\mathbf{a}(t) \cdot \mathbf{x} \leq \mathbf{b}(t)$$

where $\mathbf{a}(t) \in \mathbb{Z}[t]^d, b(t) \in \mathbb{Z}[t]$,

plus quantifiers $\forall x_i, \exists x_j$ over variables other than t.

All sets S_t covered by the Chen-Li-Theorem as well as parametric Frobenius sets (i.e. subsemigroups of $\mathbb{N}$, or even of $\mathbb{N}^k$) are parametric Presburger sets.

Properties of integer point set families

Let S_t, for $t \in \mathbb{N}$, be a family of subsets of $\mathbb{Z}^d$. Consider the following properties that S_t might or might not have.

Properties of integer point set families

Let S_t, for $t \in \mathbb{N}$, be a family of subsets of $\mathbb{Z}^d$. Consider the following properties that S_t might or might not have.

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

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

(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 $\mathbf{x}(t) \in S_t$.

Properties of integer point set families

Let S_t, for $t \in \mathbb{N}$, be a family of subsets of $\mathbb{Z}^d$. Consider the following properties that S_t might or might not have.

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

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

(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 $\mathbf{x}(t) \in S_t$.

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

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

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.

Main Theorems

Theorem (Woods, 2014)

1. *Let S_t be any family of subsets of $\mathbb{N}^d$. If S_t satisfies (4), then it also satisfies (1), (2), and (3).*
2. *If $S_t \subseteq \mathbb{N}^d$ is defined by a quantifier-free parametric Presburger formula, then S_t satisfies all four of the properties.*

Main Theorems

Theorem (Woods, 2014)

1. *Let S_t be any family of subsets of $\mathbb{N}^d$. If S_t satisfies (4), then it also satisfies (1), (2), and (3).*
2. *If $S_t \subseteq \mathbb{N}^d$ is defined by a quantifier-free parametric Presburger formula, then S_t satisfies all four of the properties.*

Theorem (B-Goodrick-Woods, 2017)

Let $S_t \subseteq \mathbb{Z}^d$ be any parametric Presburger family. Then Properties (1), (2), and (3) all hold. Furthermore, if $S_t \subseteq \mathbb{N}^d$, then (4) holds.

Quantifier elimination?

Theorem (Presburger, 1929)

The language $(\mathbb{Z}, +, 0, \leq)$ of ordinary Presburger arithmetic, extended by divisibility predicates D_c for each positive integer c, admits quantifier elimination.

That is, every Presburger set S can be defined by a quantifier-free formula, possibly involving divisibility predicates.

Quantifier elimination?

Theorem (Presburger, 1929)

The language $(\mathbb{Z}, +, 0, \leq)$ of ordinary Presburger arithmetic, extended by divisibility predicates D_c for each positive integer c, admits quantifier elimination.

That is, every Presburger set S can be defined by a quantifier-free formula, possibly involving divisibility predicates.

If the same were to hold for parametric Presburger arithmetic, then our theorem would immediately follow from Woods' result.

Quantifier elimination?

Theorem (Presburger, 1929)

The language $(\mathbb{Z}, +, 0, \leq)$ of ordinary Presburger arithmetic, extended by divisibility predicates D_c for each positive integer c, admits quantifier elimination.

That is, every Presburger set S can be defined by a quantifier-free formula, possibly involving divisibility predicates.

If the same were to hold for parametric Presburger arithmetic, then our theorem would immediately follow from Woods' result.

However, we do not know of any reasonable language for PPA that admits quantifier elimination.

Affine reduction

Let $S_t \subseteq \mathbb{Z}^d$ and $S'_t \subseteq \mathbb{Z}^{d'}$ be parametric Presburger families. An affine reduction from S'_t to S_t is an EQP-affine-linear function $F : \mathbb{Z}^{d'} \times \mathbb{N} \to \mathbb{Z}^d$ such that for every $t \in \mathbb{Z}$, F restricts to a bijection from S'_t to S_t.

Affine reduction

Let $S_t \subseteq \mathbb{Z}^d$ and $S'_t \subseteq \mathbb{Z}^{d'}$ be parametric Presburger families. An affine reduction from S'_t to S_t is an EQP-affine-linear function $F : \mathbb{Z}^{d'} \times \mathbb{N} \to \mathbb{Z}^d$ such that for every $t \in \mathbb{Z}$, F restricts to a bijection from S'_t to S_t.

Proposition

Affine reductions preserve Properties (1), (2), (3), and (4).

Proof of the Main Theorem: Step 1

Using logical equivalence, S_t can be defined by a parametric Presburger formula with only polynomially-bounded quantifiers and possibly predicates for divisibility by EQP functions.

Proof of the Main Theorem: Step 1

Using logical equivalence, S_t can be defined by a parametric Presburger formula with only polynomially-bounded quantifiers and possibly predicates for divisibility by EQP functions.

Example

$$S_t = \{(x, z) : \exists y \, [x + 1 \leq ty \leq z \ \wedge \ ty \leq 3z - x]\}$$

Proof of the Main Theorem: Step 1

Using logical equivalence, S_t can be defined by a parametric Presburger formula with only polynomially-bounded quantifiers and possibly predicates for divisibility by EQP functions.

Example

$$S_t = \{(x, z) : \ \exists y \, [x + 1 \le ty \le z \ \wedge \ ty \le 3z - x]\}$$

The candidate for y depends on x mod t: for $0 \le i \le t - 1$, $y = (x + t - i)/t$ is our candidate.

So we can write

$$S_t = \{(x, z) : \exists i \left[0 \le i \le t - 1 \ \wedge \ t \middle| (x - i) \ \wedge \ (x + t - i \le z) \right.$$
$$\left. \wedge \ (x + t - i \le 3z - x)\right]\}$$

Step 2

Using an affine reduction, eliminate the divisibility predicates.

Step 2

Using an affine reduction, eliminate the divisibility predicates.

Continuation of Example

Given

$$S_t = \{(x, z) : \exists i \left[0 \leq i \leq t - 1 \ \wedge \ t \middle| (x - i) \wedge \ (x + t - i \leq z) \wedge \ \cdots \right]$$

take

$$\begin{aligned} S'_t = \{(u, v, z) : \exists i\, [0 \leq i \leq t - 1 \ \wedge \ v - i = 0 \\ \wedge \ (u + tv + t - i \leq z) \wedge \ \cdots] \end{aligned}$$

Step 3

Using an affine reduction based on expressing the variables in base t (a la Chen-Li-Sam), separate the quantifiers from all multiplications by t.

Step 3

Using an affine reduction based on expressing the variables in base t (a la Chen-Li-Sam), separate the quantifiers from all multiplications by t.

Example

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

Step 3

Using an affine reduction based on expressing the variables in base t (a la Chen-Li-Sam), separate the quantifiers from all multiplications by t.

Example

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

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 $0 \le b_{ij} < t$ and with $0 \le a_{ij} < t$. That is, z_1 and z_2 are the only unbounded variables. The last inequality becomes

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

Step 3

Using an affine reduction based on expressing the variables in base t (a la Chen-Li-Sam), separate the quantifiers from all multiplications by t.

Example

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

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 unbounded variables. The last inequality becomes

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

Equivalently, divide by t to obtain:

Step 3, continued

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

Step 3, continued

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

Now $f_0 := a_{10} - b_{10} - 2b_{20}$ satisfies $-3t + 3 \leq f_0 \leq t - 1$.

Step 3, continued

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

Now $f_0 := a_{10} - b_{10} - 2b_{20}$ satisfies $-3t + 3 \leq f_0 \leq t - 1$.
If $-3t + 3 \leq f_0 \leq -2t$ (one of four cases), then

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

now of degree three rather than four.

Step 3, continued

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

Now $f_0 := a_{10} - b_{10} - 2b_{20}$ satisfies $-3t + 3 \leq f_0 \leq t - 1$.
If $-3t + 3 \leq f_0 \leq -2t$ (one of four cases), then

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

now of degree three rather than four.
Iterating this process, we obtain a Boolean combination of:

- Case-defining inequalities such as $-3t + 3 \leq f_0 \leq -2t$ that do not involve multiplication by t, and
- Inequalities such as $t(-z_2) + (z_1 - a_{22} - 1) \leq 0$ that do not involve any of the quantified variables b_{ij}.

Sketch of the Remaining Steps

- The quantifiers now appear only in clauses free of multiplication by t. So we can eliminate them, using Cooper's standard algorithm. We now have a set S_t defined by a Boolean combination of atomic formulas of the form
  - $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and
  - $D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))$.

Sketch of the Remaining Steps

- The quantifiers now appear only in clauses free of multiplication by t. So we can eliminate them, using Cooper's standard algorithm. We now have a set S_t defined by a Boolean combination of atomic formulas of the form
  - $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and
  - $D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))$.
- Again eliminate the divisibility predicates by an affine reduction.

Sketch of the Remaining Steps

- The quantifiers now appear only in clauses free of multiplication by t. So we can eliminate them, using Cooper's standard algorithm. We now have a set S_t defined by a Boolean combination of atomic formulas of the form
  - $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and
  - $D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))$.
- Again eliminate the divisibility predicates by an affine reduction.
- If $S_t \subseteq \mathbb{N}^d$, apply Woods' result that Property (4) holds in the quantifier-free case and that (1), (2), and (3) are consequences of (4).

Sketch of the Remaining Steps

- The quantifiers now appear only in clauses free of multiplication by t. So we can eliminate them, using Cooper's standard algorithm. We now have a set S_t defined by a Boolean combination of atomic formulas of the form
  - $\mathbf{f}(t) \cdot \mathbf{x} \leq g(t)$ and
  - $D_c(\mathbf{f}(t) \cdot \mathbf{x} - g(t))$.
- Again eliminate the divisibility predicates by an affine reduction.
- If $S_t \subseteq \mathbb{N}^d$, apply Woods' result that Property (4) holds in the quantifier-free case and that (1), (2), and (3) are consequences of (4).

If we only have $S_t \subseteq \mathbb{Z}^d$, we can prove (1), (2), and (3) directly with more work.

Multiple Parameters

A k-parametric Presburger set is a family of sets $S_{\mathbf{t}} \subseteq \mathbb{Z}^d$, one for each $\mathbf{t} = (t_1, \ldots, t_k) \in \mathbb{N}^k$, defined using a Boolean combination of inequalities of the form

$$\mathbf{a}(t) \cdot \mathbf{x} \leq \mathbf{b}(\mathbf{t})$$

where $\mathbf{a}(\mathbf{t}) \in \mathbb{Z}[\mathbf{t}]^d, b(t) \in \mathbb{Z}[\mathbf{t}]$,
plus quantifiers $\forall x_i, \exists x_j$ over variables other than $t_1, \ldots, t_k$.

Farewell to Polynomials

Example

$$S_{t_1,t_2} = \{(x_1, x_2) \in \mathbb{N}^2 \,:\, t_1 x_1 + t_2 x_2 = t_1 t_2\}$$

consists of the lattice points on the line segment from $(t_2, 0)$ to $(0, t_1)$ and so $|S_{t_1,t_2}| = \gcd(t_1, t_2) + 1$.

Farewell to Polynomials

Example

$$S_{t_1,t_2} = \{(x_1, x_2) \in \mathbb{N}^2 \,:\, t_1x_1 + t_2x_2 = t_1t_2\}$$

consists of the lattice points on the line segment from $(t_2, 0)$ to $(0, t_1)$ and so $|S_{t_1,t_2}| = \text{gcd}(t_1, t_2) + 1$.

The gcd function is not piecewise quasi-polynomial, which would be the most obvious analogue of EQP for multiple parameters.

Negative Results for Multiple Parameters

A Σ_2 formula is one that is of the form $\exists y_1 \ldots \exists y_m \forall z_1 \ldots \forall z_n \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ where Φ is quantifier-free.

Negative Results for Multiple Parameters

A Σ_2 formula is one that is of the form $\exists y_1 \ldots \exists y_m \forall z_1 \ldots \forall z_n \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ where Φ is quantifier-free.

Theorem (Nguyen–Pak, consequence of 2017 preprint)

Assume P $\neq$ NP. *There exists a 3-parametric* Σ_2 *PA family* $S_{p,q,M}$ *such that* $|S_{p,q,M}|$ *is always finite but cannot be expressed as a polynomial-time evaluable function in* p, q, *and* M.

Negative Results for Multiple Parameters

A Σ_2 formula is one that is of the form $\exists y_1 \ldots \exists y_m \forall z_1 \ldots \forall z_n \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ where Φ is quantifier-free.

Theorem (Nguyen–Pak, consequence of 2017 preprint)

Assume $\mathrm{P} \neq \mathrm{NP}$. *There exists a 3-parametric Σ_2 PA family $S_{p,q,M}$ such that $|S_{p,q,M}|$ is always finite but cannot be expressed as a polynomial-time evaluable function in p, q, and M.*

Theorem (B-Goodrick-Nguyen-Woods, 2018 preprint)

Assume $P = NP$. There exists a 2-parametric Σ_2 PA family S_{t_1,t_2} for which $|S_{t_1,t_2}|$ is always finite but cannot be expressed as a polynomial time evaluable function in t_1 and t_2.

Negative Results for Multiple Parameters

A Σ_2 formula is one that is of the form
$\exists y_1 \ldots \exists y_m \forall z_1 \ldots \forall z_n \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ where Φ is quantifier-free.

Theorem (Nguyen–Pak, consequence of 2017 preprint)

Assume $\mathrm{P} \neq \mathrm{NP}$. *There exists a 3-parametric Σ_2 PA family $S_{p,q,M}$ such that $|S_{p,q,M}|$ is always finite but cannot be expressed as a polynomial-time evaluable function in p, q, and M.*

Theorem (B-Goodrick-Nguyen-Woods, 2018 preprint)

Assume $P = NP$. There exists a 2-parametric Σ_2 PA family S_{t_1,t_2} for which $|S_{t_1,t_2}|$ is always finite but cannot be expressed as a polynomial time evaluable function in t_1 and t_2.

This result is optimal: polynomial evaluability follows from:

- our previous theorem, for just one parameter,
- Barvinok's algorithm (1994) for quantifier-free formulas with any number of parameters, or
- Barvinok and Woods (2003) for Σ_1 sentences (no quantifier alternation) with any number of parameters.