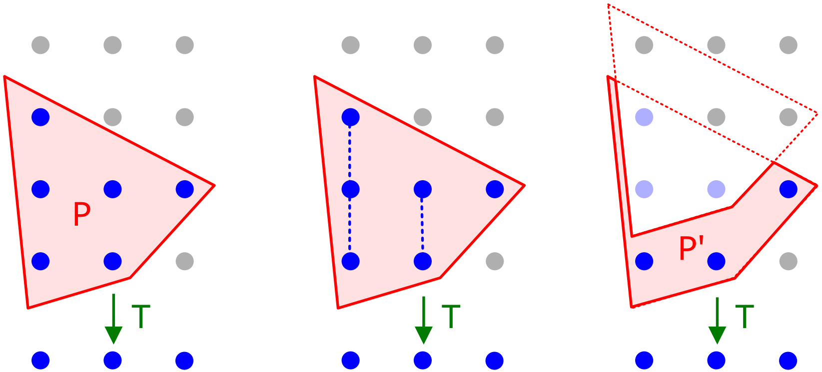
The Complexity of Presburger Arithmetic in Fixed Dimension

Kevin Woods
Oberlin College



Classic result

Theorem [Lenstra 1983]: Fix d. There is a polynomial time algorithm which, given a (rational) polyhedron $P \subseteq \mathbb{R}^d$ (input, e.g., as list of integral defining inequalities), decides if $P \cap \mathbb{Z}^d$ is nonempty.

What next? How might we generalize?

Classic result

Theorem [Lenstra 1983]: Fix d. There is a polynomial time algorithm which, given a (rational) polyhedron $P \subseteq \mathbb{R}^d$ (input, e.g., as list of integral defining inequalities), decides if $P \cap \mathbb{Z}^d$ is nonempty.

What next? How might we generalize?

Classic result

Theorem [Lenstra 1983]: Fix d. There is a polynomial time algorithm which, given a (rational) polyhedron $P \subseteq \mathbb{R}^d$ (input, e.g., as list of integral defining inequalities), decides if $P \cap \mathbb{Z}^d$ is nonempty.

What next? How might we generalize?

Theorem [Barvinok 1994]: Fix d. There is a polynomial time algorithm which, given a polyhedron $P \subseteq \mathbb{R}^d$, counts $|P \cap \mathbb{Z}^d|$.

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1, a_2, \ldots, a_d) \in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5, 50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1 - x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5 - 51}{-1} = 46.$$

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1, a_2, \ldots, a_d) \in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5, 50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1 - x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5 - 51}{-1} = 46.$$

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1,a_2,\ldots,a_d)\in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5, 50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1 - x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5 - 51}{-1} = 46.$$

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1,a_2,\ldots,a_d)\in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5, 50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1 - x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5 - 51}{-1} = 46.$$

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1,a_2,\ldots,a_d)\in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5, 50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1 - x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5 - 51}{-1} = 46.$$

A key idea

Definition: For $S \subseteq \mathbb{Z}^d$, we can define the generating function

$$\sum_{(a_1,a_2,\ldots,a_d)\in S} x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}.$$

Example: $S = [5,50] \cap \mathbb{Z}$ has generating function

$$x^5 + x^6 + \cdots + x^{50} = \frac{x^5 - x^{51}}{1-x}.$$

Limit $x \to 1$ (with L'Hôpital's Rule) yields

$$|S| = \frac{5-51}{-1} = 46.$$

A key idea

Moral:

- We can often use patterns in our sets to encode them compactly as generating functions.
- We can manipulate the generating functions to answer questions about the sets (like cardinality).

What next?

What next?

Theorem [Barvinok–W 2003]: Fix d. There is a polynomial time algorithm which, given a polyhedron $P \subseteq \mathbb{R}^d$ and a linear transformation $T : \mathbb{Z}^d \to \mathbb{Z}^k$, computes the generating function for $T(P \cap \mathbb{Z}^d)$ (and hence can compute its cardinality).

Note: Most interesting when T has nontrivial kernel, e.g., some sort of projection.

Frobenius problem

Example: Given positive integers $a_1, \ldots, a_d$, let

$$P = \mathbb{R}^d_{\geq 0} \quad \text{and} \quad T(x_1, \ldots, x_d) = a_1 x_1 + \cdots + a_d x_d.$$

Then $S = T(P \cap \mathbb{Z}^d)$ is the set of nonnegative integer combinations of $a_1, \ldots, a_d$, that is, the semigroup generated by $a_1, \ldots, a_d$ (i.e., closure under addition).

- What is the largest integer not in S, assuming a_i relatively prime? (Frobenius problem)
- How many positive integers are not in S?
- What is the generating function for S?

Frobenius problem

Example: Given positive integers $a_1, \ldots, a_d$, let

$$P = \mathbb{R}^d_{\geq 0} \quad \text{and} \quad T(x_1, \ldots, x_d) = a_1 x_1 + \cdots + a_d x_d.$$

Then $S = T(P \cap \mathbb{Z}^d)$ is the set of nonnegative integer combinations of $a_1, \ldots, a_d$, that is, the semigroup generated by $a_1, \ldots, a_d$ (i.e., closure under addition).

- What is the largest integer not in S, assuming a_i relatively prime? (Frobenius problem)
- How many positive integers are not in S?
- What is the generating function for S?

Frobenius problem

Example: Given positive integers $a_1, \dots, a_d$, let

$$P = \mathbb{R}^d_{\geq 0} \quad \text{and} \quad T(x_1, \dots, x_d) = a_1 x_1 + \cdots + a_d x_d.$$

Then $S = T(P \cap \mathbb{Z}^d)$ is the set of nonnegative integer combinations of $a_1, \dots, a_d$, that is, the semigroup generated by $a_1, \dots, a_d$ (i.e., closure under addition).

- What is the largest integer not in S, assuming a_i relatively prime? (Frobenius problem)
- How many positive integers are not in S?
- What is the generating function for S?

Frobenius problem

Example: Given positive integers $a_1, \ldots, a_d$, let

$$P = \mathbb{R}^d_{\geq 0} \quad \text{and} \quad T(x_1, \ldots, x_d) = a_1 x_1 + \cdots + a_d x_d.$$

Then $S = T(P \cap \mathbb{Z}^d)$ is the set of nonnegative integer combinations of $a_1, \ldots, a_d$, that is, the semigroup generated by $a_1, \ldots, a_d$ (i.e., closure under addition).

- What is the largest integer not in S, assuming a_i relatively prime? (Frobenius problem)
- How many positive integers are not in S?
- What is the generating function for S?

Frobenius problem

Example: When $d = 2$ and a_1, a_2 relatively prime,

- The largest integer not in S is $a_1 a_2 - a_1 - a_2$ [Sylvester 1884].
- The number of positive integers not in S is $(a_1 a_2 - a_1 - a_2 + 1)/2$.
- The generating function for S is

$$\sum_{n \in S} x^n = \frac{1 - x^{a_1 a_2}}{(1 - x^{a_1})(1 - x^{a_2})}.$$

For $d > 3$, no known nice formulas; we need these algorithmic results.

Frobenius problem

Example: When $d = 2$ and a_1, a_2 relatively prime,

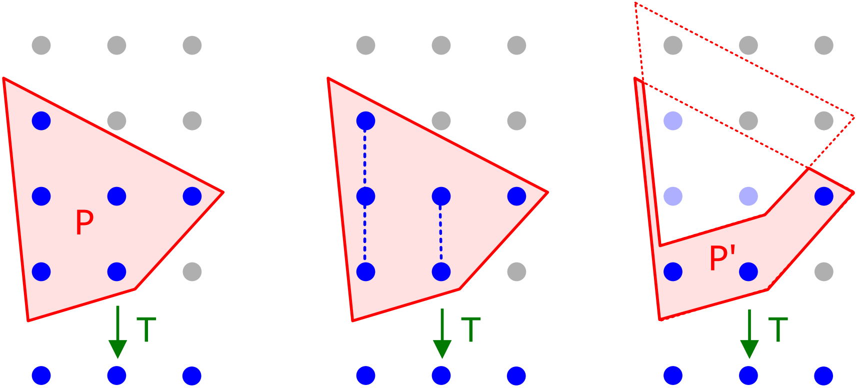
- The largest integer not in S is $a_1 a_2 - a_1 - a_2$ [Sylvester 1884].
- The number of positive integers not in S is $(a_1 a_2 - a_1 - a_2 + 1)/2$.
- The generating function for S is

$$\sum_{n \in S} x^n = \frac{1 - x^{a_1 a_2}}{(1 - x^{a_1})(1 - x^{a_2})}.$$

For $d > 3$, no known nice formulas; we need these algorithmic results.

A key idea

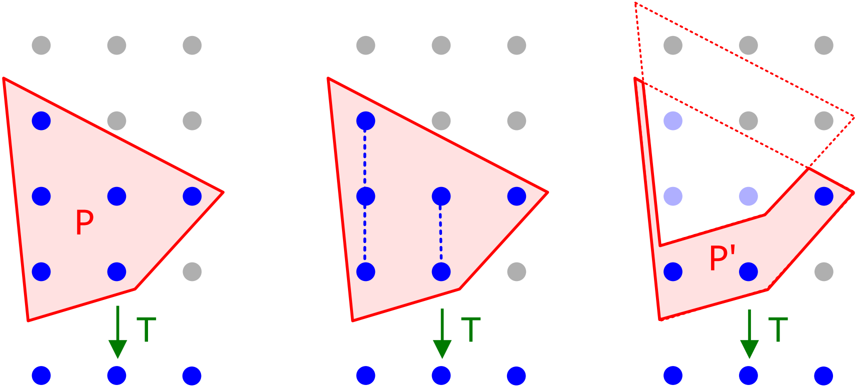
A 1-dimensional kernel is pretty easy. E.g, $T(x, y) = x$:



The fibers of $T(P \cap \mathbb{Z}^2)$ have no gaps.
Let $P' = P \setminus \big(P + (0, 1)\big)$. Then T is one-to-one on $P' \cap \mathbb{Z}^2$.

A key idea

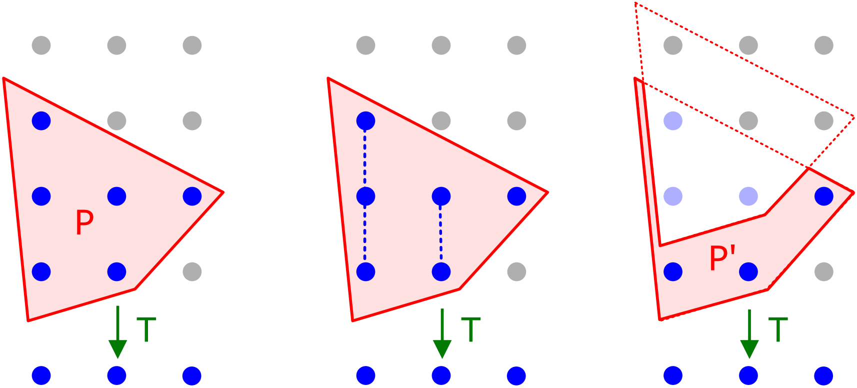
A 1-dimensional kernel is pretty easy. E.g, $T(x, y) = x$:



The fibers of $T(P \cap \mathbb{Z}^2)$ have no gaps.
Let $P' = P \setminus \big(P + (0, 1)\big)$. Then T is one-to-one on $P' \cap \mathbb{Z}^2$.

A key idea

A 1-dimensional kernel is pretty easy. E.g, $T(x, y) = x$:

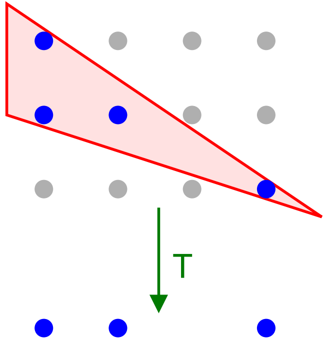


The fibers of $T(P \cap \mathbb{Z}^2)$ have no gaps.

Let $P' = P \setminus \big(P + (0,1)\big)$. Then T is one-to-one on $P' \cap \mathbb{Z}^2$.

A key idea

With a higher dimensional kernel, inductively project out one dimension at a time. But this may create gaps.



Key: Carefully control the gaps.

What next?

What next?

If $T(x, y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \quad (x, y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x, y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \ldots, x_m$, $y_1, \ldots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \exists y \in \mathbb{Z}^n \; \Phi(x, y).$$

Similarly for $x \in \mathbb{Z}^m : \forall y \in \mathbb{Z}^n \; \Phi(x, y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x, y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \ \exists y \in \mathbb{Z} \quad (x, y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x, y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \dots, x_m$, $y_1, \dots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \ \exists y \in \mathbb{Z}^n \ \Phi(x, y).$$

Similarly for $x \in \mathbb{Z}^m : \ \forall y \in \mathbb{Z}^n \ \Phi(x, y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x,y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \quad (x,y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x,y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \dots, x_m$, $y_1, \dots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \exists y \in \mathbb{Z}^n \; \Phi(x,y).$$

Similarly for $x \in \mathbb{Z}^m : \forall y \in \mathbb{Z}^n \; \Phi(x,y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x,y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \ \exists y \in \mathbb{Z} \quad (x,y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x,y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \ldots, x_m$, $y_1, \ldots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \ \exists y \in \mathbb{Z}^n \ \Phi(x,y).$$

Similarly for $x \in \mathbb{Z}^m : \ \forall y \in \mathbb{Z}^n \ \Phi(x,y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x, y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \quad (x, y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x, y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \ldots, x_m$, $y_1, \ldots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \exists y \in \mathbb{Z}^n \ \Phi(x, y).$$

Similarly for $x \in \mathbb{Z}^m : \forall y \in \mathbb{Z}^n \ \Phi(x, y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x,y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \ \exists y \in \mathbb{Z} \quad (x,y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x,y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \ldots, x_m$, $y_1, \ldots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \ \exists y \in \mathbb{Z}^n \ \Phi(x,y).$$

Similarly for $x \in \mathbb{Z}^m : \ \forall y \in \mathbb{Z}^n \ \Phi(x,y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

What next?

If $T(x,y) = x$, then $T(P \cap \mathbb{Z}^2) = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \quad (x,y) \in P\}$.

Presburger Arithmetic: Sets defined over the integers using quantifiers and Boolean combinations ($\wedge$, $\vee$, $\neg$) of linear inequalities. So far, we've been using only conjunctions.

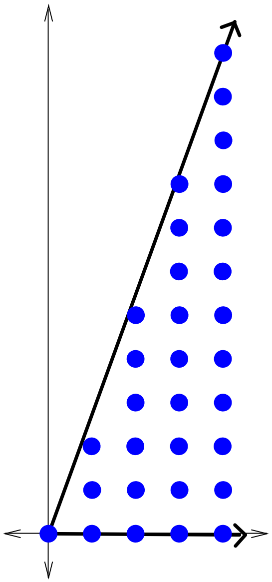
Theorem [Barvinok-W 2003]: Fix m, n, s. There is a polynomial time algorithm which, given a formula $\Phi(x, y)$ that is a Boolean combination of at most s linear inequalities in $x_1, \ldots, x_m$, $y_1, \ldots, y_n$, computes the generating function for

$$x \in \mathbb{Z}^m : \exists y \in \mathbb{Z}^n \ \Phi(x, y).$$

Similarly for $x \in \mathbb{Z}^m : \forall y \in \mathbb{Z}^n \ \Phi(x, y)$.

Note: If s is not fixed above, then the problem is NP-hard [Schöning 1997].

Hilbert bases



Given a (rational) cone $C \subseteq \mathbb{Z}^d$, $C \cap \mathbb{Z}^d$ is a semigroup (closed under addition).

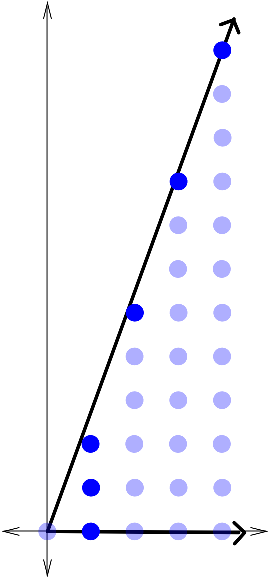
Let S be the minimal set of generators (Hilbert Basis). In example, S is

$$(1,0),(1,1),(1,2),(2,5),(3,8),(4,11)$$

S is the set of $x \in \mathbb{Z}^d$ such that

$$\forall y,z \in \mathbb{Z}^d \ \big(y \in C \setminus \{0\} \ \wedge \ z \in C \setminus \{0\}\big) \Rightarrow x \neq y + z$$

Hilbert bases



Given a (rational) cone $C \subseteq \mathbb{Z}^d$, $C \cap \mathbb{Z}^d$ is a semigroup (closed under addition).

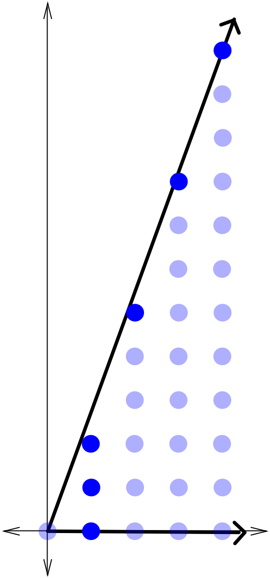
Let S be the minimal set of generators (Hilbert Basis). In example, S is

$$(1,0),(1,1),(1,2),(2,5),(3,8),(4,11)$$

S is the set of $x \in \mathbb{Z}^d$ such that

$$\forall y,z \in \mathbb{Z}^d \ \big(y \in C \setminus \{0\} \ \wedge \ z \in C \setminus \{0\}\big) \Rightarrow x \neq y+z$$

Hilbert bases



Given a (rational) cone $C \subseteq \mathbb{Z}^d$, $C \cap \mathbb{Z}^d$ is a semigroup (closed under addition).

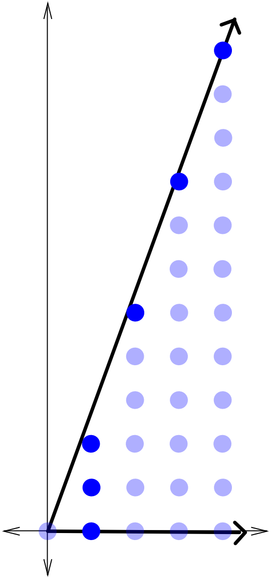
Let S be the minimal set of generators (Hilbert Basis). In example, S is

$$(1,0),(1,1),(1,2),(2,5),(3,8),(4,11)$$

S is the set of $x \in \mathbb{Z}^d$ such that

$$\forall y, z \in \mathbb{Z}^d \ \big(y \in C \setminus \{0\} \ \wedge \ z \in C \setminus \{0\}\big) \Rightarrow x \neq y + z$$

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

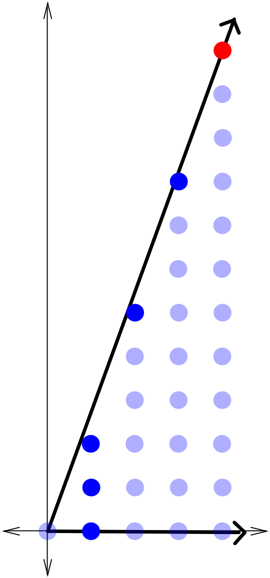
$$\frac{11}{4} = 2 + \frac{1}{1 + \frac{1}{3}}, \quad \frac{8}{3} = 2 + \frac{1}{1 + \frac{1}{2}}, \quad \frac{5}{2} = 2 + \frac{1}{1 + \frac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

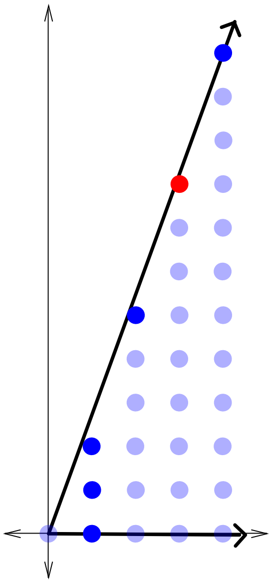
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

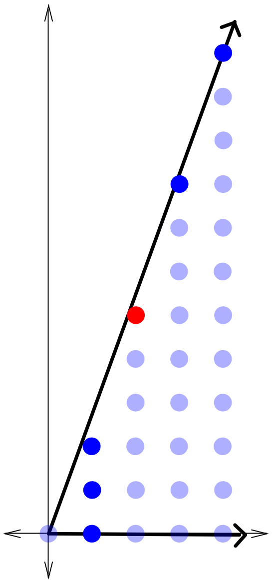
$$\frac{11}{4} = 2+\cfrac{1}{1+\cfrac{1}{3}}, \quad \frac{8}{3} = 2+\cfrac{1}{1+\cfrac{1}{2}}, \quad \frac{5}{2} = 2+\cfrac{1}{1+\cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1,3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

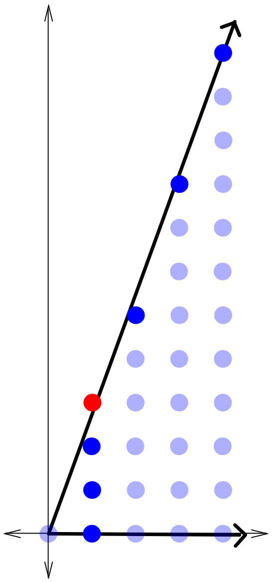
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

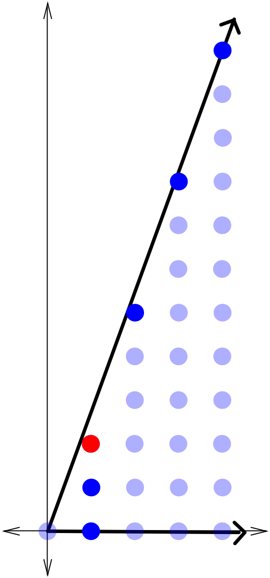
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1,3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

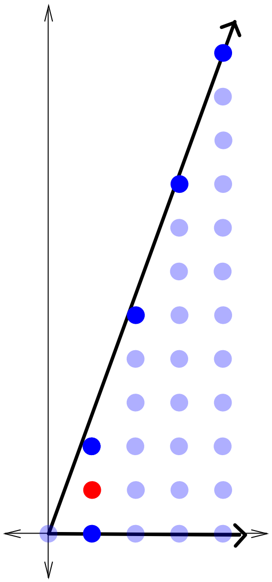
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

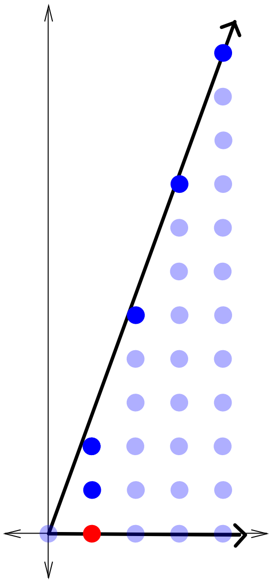
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

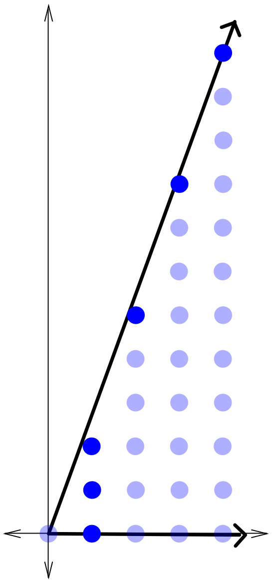
$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

Hilbert bases



When $d = 2$ and cone has extreme rays (q, p) and $(1, 0)$, Hilbert basis is related to continued fraction expansion of p/q.

$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}}, \quad \frac{8}{3} = 2 + \cfrac{1}{1 + \cfrac{1}{2}}, \quad \frac{5}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{1}},$$

$$\frac{3}{1} = 2 + \frac{1}{1} \text{ but } (1, 3) \notin C,$$

$$\frac{2}{1} = 2, \quad \frac{1}{1} = 1, \quad \frac{0}{1} = 0.$$

Note: the y-coordinates form non-overlapping arithmetic progressions: (0,1,2), (5,8,11).

What next?

What next?

What if we allow quantifier alternation: $\exists x \forall y$ or $\forall x \exists y$?

What next?

What if we allow quantifier alternation: $\exists x \forall y$ or $\forall x \exists y$?

NO!

Theorem [Nguyen–Pak 2017]: Even with at most 10 inequalities and at most 5 variables, deciding if the set

$$S = \left\{ z \in \mathbb{Z} : \ \forall y \in \mathbb{Z}^2 \ \exists x \in \mathbb{Z}^2 \ \Phi(x, y, z) \right\}$$

is nonempty is NP-complete (and counting $|S|$ is #P-complete).

What next?

What if we allow quantifier alternation: $\exists x \forall y$ or $\forall x \exists y$?

NO!

Theorem [Nguyen–Pak 2017]: Even with at most 10 inequalities and at most 5 variables, deciding if the set

$$S = \left\{ z \in \mathbb{Z} : \ \forall y \in \mathbb{Z}^2 \ \exists x \in \mathbb{Z}^2 \ \Phi(x, y, z) \right\}$$

is nonempty is NP-complete (and counting $|S|$ is #P-complete).

A key idea

Define the set of y coordinates of a particular Hilbert Basis, creating non-overlapping arithmetic progressions. Needs a $\forall$ quantifier.

Take these y's modulo M (for a well chosen M), creating overlapping arithmetic progressions. Needs an $\exists$ quantifier:

$$\exists k \in \mathbb{Z} : \; 0 \leq y - kM < M \ldots \forall \ldots$$

This looks like a known NP-complete problem: Given a set of arithmetic progressions and an interval, do the arithmetic progressions cover the interval?

A key idea

Define the set of y coordinates of a particular Hilbert Basis, creating non-overlapping arithmetic progressions. Needs a $\forall$ quantifier.

Take these y's modulo M (for a well chosen M), creating overlapping arithmetic progressions. Needs an $\exists$ quantifier:

$$\exists k \in \mathbb{Z} : \ 0 \leq y - kM < M \ldots \forall \ldots$$

This looks like a known NP-complete problem: Given a set of arithmetic progressions and an interval, do the arithmetic progressions cover the interval?

A key idea

Define the set of y coordinates of a particular Hilbert Basis, creating non-overlapping arithmetic progressions. Needs a $\forall$ quantifier.

Take these y's modulo M (for a well chosen M), creating overlapping arithmetic progressions. Needs an $\exists$ quantifier:

$$\exists k \in \mathbb{Z}: \; 0 \leq y - kM < M \ldots \forall \ldots$$

This looks like a known NP-complete problem: Given a set of arithmetic progressions and an interval, do the arithmetic progressions cover the interval?

A key idea

Define the set of y coordinates of a particular Hilbert Basis, creating non-overlapping arithmetic progressions. Needs a $\forall$ quantifier.

Take these y's modulo M (for a well chosen M), creating overlapping arithmetic progressions. Needs an $\exists$ quantifier:

$$\exists k \in \mathbb{Z}: \ 0 \leq y - kM < M \ldots \forall \ldots$$

This looks like a known NP-complete problem: Given a set of arithmetic progressions and an interval, do the arithmetic progressions cover the interval?

A key idea

Define the set of y coordinates of a particular Hilbert Basis, creating non-overlapping arithmetic progressions. Needs a $\forall$ quantifier.

Take these y's modulo M (for a well chosen M), creating overlapping arithmetic progressions. Needs an $\exists$ quantifier:

$$\exists k \in \mathbb{Z} : \; 0 \leq y - kM < M \ldots \forall \ldots$$

This looks like a known NP-complete problem: Given a set of arithmetic progressions and an interval, do the arithmetic progressions cover the interval?

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.

  Decidable [Presburger 1930].

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.
  Decidable [Presburger 1930].
  But requires doubly exponential time [Fischer–Rabin 1974].

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.
  Decidable [Presburger 1930].
  But requires doubly exponential time [Fischer–Rabin 1974].
- Fix number of variables, no quantifiers.
  Polynomial time [Lenstra 1983, Barvinok 1994].

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.
  Decidable [Presburger 1930].
  But requires doubly exponential time [Fischer–Rabin 1974].
- Fix number of variables, no quantifiers.
  Polynomial time [Lenstra 1983, Barvinok 1994].
- Fixed number of variables, quantifiers allowed.
  NP-hard [Schöning 1997].

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.
  Decidable [Presburger 1930].
  But requires doubly exponential time [Fischer–Rabin 1974].
- Fix number of variables, no quantifiers.
  Polynomial time [Lenstra 1983, Barvinok 1994].
- Fixed number of variables, quantifiers allowed.
  NP-hard [Schöning 1997].
- Fixed number of variables and inequalities, no quantifier alternation.
  Polynomial time [Kannan 1990, Barvinok–W 2003].

Summary

Presburger sentences from an algorithmic perspective:

- General sentences.
  Decidable [Presburger 1930].
  But requires doubly exponential time [Fischer–Rabin 1974].
- Fix number of variables, no quantifiers.
  Polynomial time [Lenstra 1983, Barvinok 1994].
- Fixed number of variables, quantifiers allowed.
  NP-hard [Schöning 1997].
- Fixed number of variables and inequalities, no quantifier alternation.
  Polynomial time [Kannan 1990, Barvinok–W 2003].
- Fixed number of variables and inequalities, mixed quantifiers.
  NP-hard [Nguyen–Pak 2017].

Thank You!