Counting with Quasi-polynomials

Kevin Woods
Oberlin College

Quasi-polynomials

Definition: $g : \mathbb{N} \to \mathbb{N}$ is a quasi-polynomial of period m if there exist polynomials $g_0, g_1, \ldots, g_{m-1}$ such that

$$g(t) = g_{t \bmod m}(t), \forall t \in \mathbb{N}.$$

Example: For $t \in \mathbb{N}$, let

$$S_t = \{x \in \mathbb{N} : \ 1 \leq 2x \leq t\} = \{1, 2, \ldots, \lfloor t/2 \rfloor\}.$$

Then

$$|S_t| = \left\lfloor \frac{t}{2} \right\rfloor = \begin{cases} t/2 & \text{if } t \bmod 2 = 0, \\ (t-1)/2 & \text{if } t \bmod 2 = 1. \end{cases}$$

Quasi-polynomials

Definition: $g : \mathbb{N} \to \mathbb{N}$ is a quasi-polynomial of period m if there exist polynomials $g_0, g_1, \ldots, g_{m-1}$ such that

$$g(t) = g_{t \bmod m}(t), \forall t \in \mathbb{N}.$$

Example: For $t \in \mathbb{N}$, let

$$S_t = \{x \in \mathbb{N} : \ 1 \leq 2x \leq t\} = \{1, 2, \ldots, \lfloor t/2 \rfloor\}.$$

Then

$$|S_t| = \left\lfloor \frac{t}{2} \right\rfloor = \begin{cases} t/2 & \text{if } t \bmod 2 = 0, \\ (t-1)/2 & \text{if } t \bmod 2 = 1. \end{cases}$$

Quasi-polynomials

Definition: $g : \mathbb{N} \to \mathbb{N}$ is a quasi-polynomial of period m if there exist polynomials $g_0, g_1, \ldots, g_{m-1}$ such that

$$g(t) = g_{t \bmod m}(t), \forall t \in \mathbb{N}.$$

Example: For $t \in \mathbb{N}$, let

$$S_t = \{x \in \mathbb{N} : \ 1 \leq 2x \leq t\} = \{1, 2, \ldots, \lfloor t/2 \rfloor\}.$$

Then

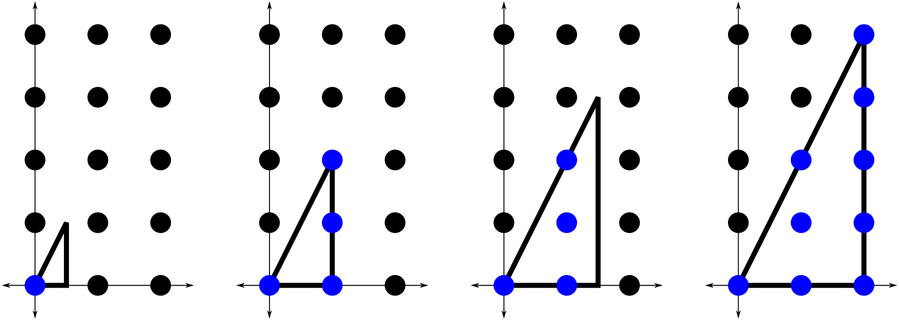
$$|S_t| = \left\lfloor \frac{t}{2} \right\rfloor = \begin{cases} t/2 & \text{if } t \bmod 2 = 0, \\ (t-1)/2 & \text{if } t \bmod 2 = 1. \end{cases}$$

Example 1: Parametric Polyhedron

Let P be the triangle with vertices $(0,0)$, $(1/2,0)$, and $(1/2,1)$.

Let $S_t = tP \cap \mathbb{Z}^2$, for $t \in \mathbb{N}$.
What is $|S_t|$, as a function of t?

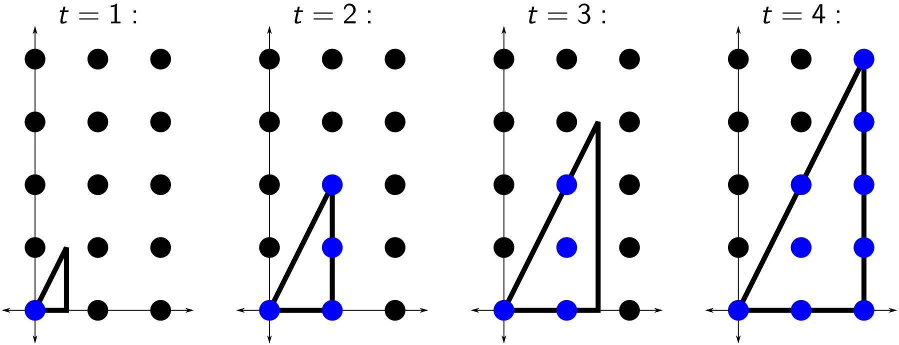
$t = 1:$ $t = 2:$ $t = 3:$ $t = 4:$



Example 1: Parametric Polyhedron

Let P be the triangle with vertices $(0, 0)$, $(1/2, 0)$, and $(1/2, 1)$.

Let $S_t = tP \cap \mathbb{Z}^2$, for $t \in \mathbb{N}$.
What is $|S_t|$, as a function of t?

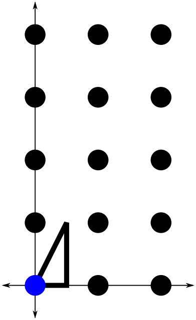


Example 1: Parametric Polyhedron

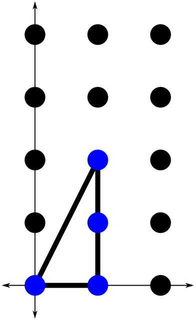
Let P be the triangle with vertices $(0,0)$, $(1/2,0)$, and $(1/2,1)$.

Let $S_t = tP \cap \mathbb{Z}^2$, for $t \in \mathbb{N}$.
What is $|S_t|$, as a function of t?

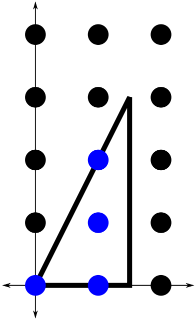
$t = 1:$



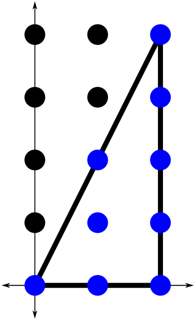
$t = 2:$



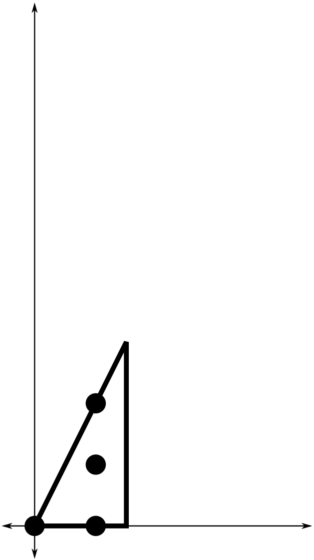
$t = 3:$



$t = 4:$



Example 1: Parametric Polyhedron



The hard (but insightful) way to calculate $|S_t|$:

Definition: The generating function for $S \subseteq \mathbb{Z}^2$ is given by

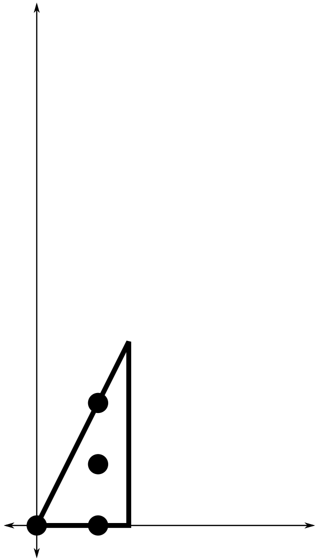
$$f(S; x, y) = \sum_{(c,d)\in S} x^c y^d.$$

Example:

$$f(S_3; x, y) = x^0 y^0 + x^1 y^0 + x^1 y^1 + x^1 y^2.$$

Let's find $f(S_t; x, y)$.

Example 1: Parametric Polyhedron



The hard (but insightful) way to calculate $|S_t|$:

Definition: The generating function for $S \subseteq \mathbb{Z}^2$ is given by

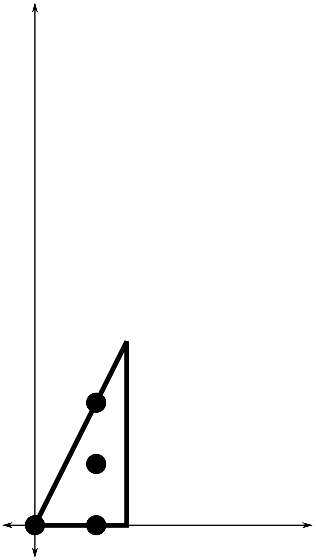
$$f(S; x, y) = \sum_{(c,d) \in S} x^c y^d.$$

Example:

$$f(S_3; x, y) = x^0 y^0 + x^1 y^0 + x^1 y^1 + x^1 y^2.$$

Let's find $f(S_t; x, y)$.

Example 1: Parametric Polyhedron



The hard (but insightful) way to calculate $|S_t|$:

Definition: The generating function for $S \subseteq \mathbb{Z}^2$ is given by

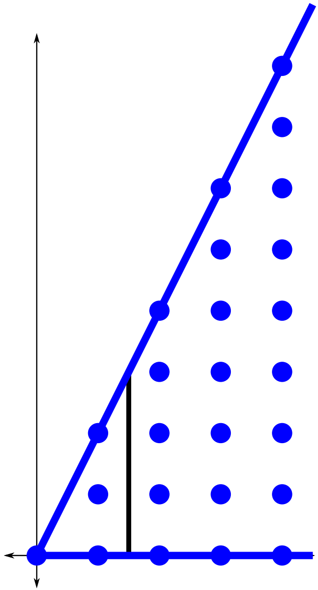
$$f(S; x, y) = \sum_{(c,d) \in S} x^c y^d.$$

Example:

$$f(S_3; x, y) = x^0 y^0 + x^1 y^0 + x^1 y^1 + x^1 y^2.$$

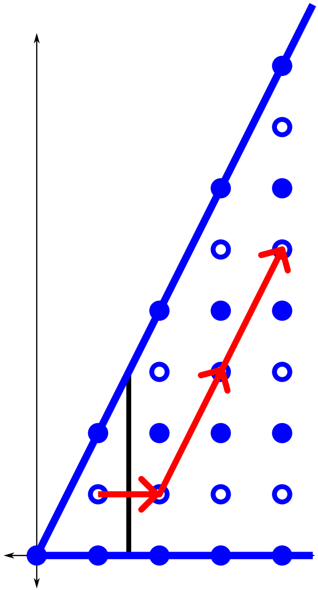
Let's find $f(S_t; x, y)$.

Example 1: Parametric Polyhedron



Let's first find $f(S; x, y)$ for this set.

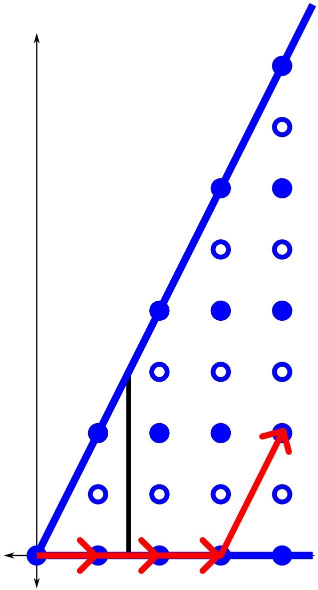
Example 1: Parametric Polyhedron



$$f(S; x, y) =$$
$$(x^0y^0 + x^1y^1)$$
$$\cdot (1 + x^1 + x^2 + x^3 + \cdots)$$
$$\cdot (1 + (x^1y^2)^1 + (x^1y^2)^2 + \cdots)$$

$$x^4y^5 = x^1y^1(x)^1(x^1y^2)^2$$

Example 1: Parametric Polyhedron



$f(S; x, y) =$

$(x^0 y^0 + x^1 y^1)$

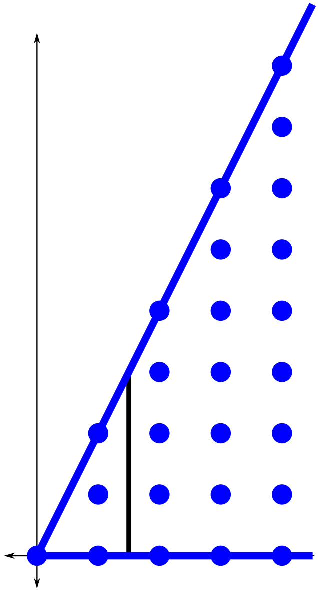
$\cdot (1 + x^1 + x^2 + x^3 + \cdots)$

$\cdot (1 + (x^1 y^2)^1 + (x^1 y^2)^2 + \cdots)$

$$x^4 y^5 = x^1 y^1 (x)^1 (x^1 y^2)^2$$

$$x^4 y^2 = x^0 y^0 (x)^3 (x^1 y^2)^1$$

Example 1: Parametric Polyhedron



$$f(S; x, y) =$$

$$(x^0y^0 + x^1y^1)$$

$$\cdot (1 + x^1 + x^2 + x^3 + \cdots)$$

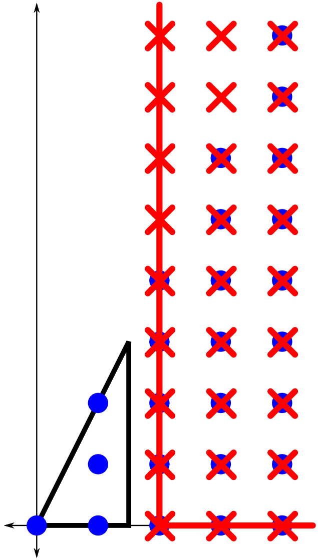
$$\cdot (1 + (x^1y^2)^1 + (x^1y^2)^2 + \cdots)$$

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

$$x^4y^5 = x^1y^1(x)^1(x^1y^2)^2$$

$$x^4y^2 = x^0y^0(x)^3(x^1y^2)^1$$

Example 1: Parametric Polyhedron

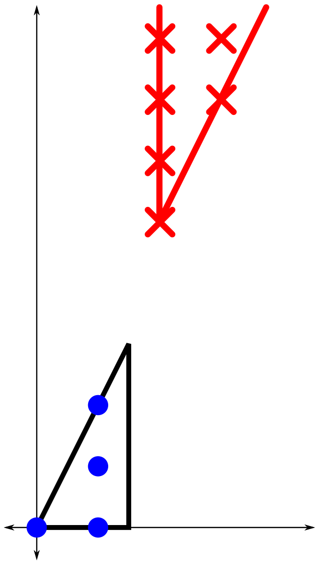


Let $k = \lfloor t/2 \rfloor$.

$$-x^{k+1}y^0 \cdot (1 + x + x^2 + \cdots) \cdot (1 + y + y^2 + \cdots)$$

$$= -\frac{x^{k+1}}{(1-x)(1-y)}$$

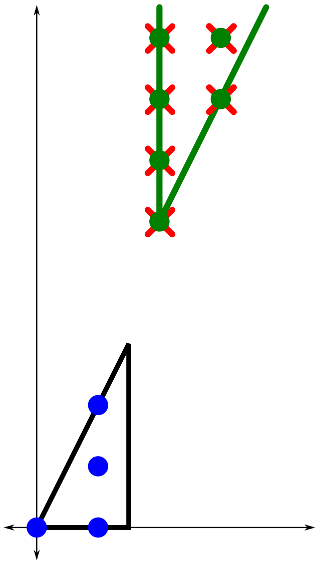
Example 1: Parametric Polyhedron



$$\frac{1+xy}{(1-x)(1-xy^2)}$$

$$-\frac{x^{k+1}}{(1-x)(1-y)}$$

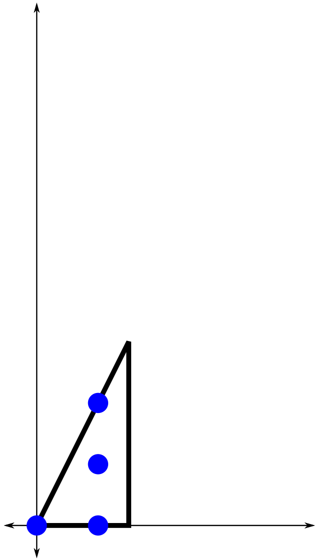
Example 1: Parametric Polyhedron



$$+x^{k+1}y^{2(k+1)+1}$$
$$\cdot\,(1 + xy^2 + (xy^2)^2 + \cdots)$$
$$\cdot\,(1 + y + y^2 + \cdots)$$

$$= \frac{x^{k+1}y^{2k+3}}{(1 - xy^2)(1 - y)}$$

Example 1: Parametric Polyhedron



$$f(S_t; x, y) =$$

$$\frac{1 + xy}{(1-x)(1-xy^2)}$$

$$-\frac{x^{k+1}}{(1-x)(1-y)}$$

$$+\frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1 + xy}{(1 - x)(1 - xy^2)} - \frac{x^{k+1}}{(1 - x)(1 - y)} + \frac{x^{k+1}y^{2k+3}}{(1 - xy^2)(1 - y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1+xy}{(1-x)(1-xy^2)} - \frac{x^{k+1}}{(1-x)(1-y)} + \frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1 + xy}{(1 - x)(1 - xy^2)} - \frac{x^{k+1}}{(1 - x)(1 - y)} + \frac{x^{k+1}y^{2k+3}}{(1 - xy^2)(1 - y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1+xy}{(1-x)(1-xy^2)} - \frac{x^{k+1}}{(1-x)(1-y)} + \frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1 + xy}{(1-x)(1-xy^2)} - \frac{x^{k+1}}{(1-x)(1-y)} + \frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Uh oh.

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1 + xy}{(1-x)(1-xy^2)} - \frac{x^{k+1}}{(1-x)(1-y)} + \frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!

Uh oh.

Take limit as $(x, y) \to (1, 1)$, e.g, get common denominator, then repeated L'Hôpital's rule, one variable at a time:

$$|S_t| = (k+1)^2 = \left(\lfloor t/2 \rfloor + 1\right)^2.$$

Example 1: Parametric Polyhedron

$$f(S_t; x, y) = \frac{1+xy}{(1-x)(1-xy^2)} - \frac{x^{k+1}}{(1-x)(1-y)} + \frac{x^{k+1}y^{2k+3}}{(1-xy^2)(1-y)}.$$

$$f(S_t; 1, 1) = \sum_{(c,d)\in S_t} 1^c 1^d = |S_t|.$$

So plug in $x = 1, y = 1$!
Uh oh.
Take limit as $(x, y) \to (1, 1)$, e.g, get common denominator, then repeated L'Hôpital's rule, one variable at a time:

$$|S_t| = (k+1)^2 = (\lfloor t/2 \rfloor + 1)^2 .$$

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1 x_1 + \cdots + a_d x_d \le bt + c.$$

Theorem (McMullen, Brion, Barvinok)
$|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1x_1 + \cdots + a_dx_d \leq bt + c.$$

Theorem (McMullen, Brion, Barvinok)

$|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1 x_1 + \cdots + a_d x_d \leq bt + c.$$

Theorem (McMullen, Brion, Barvinok)

$|P_t \cap \mathbb{Z}^d|$ *agrees with a quasi-polynomial, for sufficiently large* t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1 x_1 + \cdots + a_d x_d \leq bt + c.$$

Theorem (McMullen, Brion, Barvinok)

$|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1x_1 + \cdots + a_dx_d \leq bt + c.$$

Theorem (McMullen, Brion, Barvinok)

$|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Definition: A parametric polyhedron, $P_t \subseteq \mathbb{R}^d$, is the solution set to a system of linear inequalities of the form

$$a_1 x_1 + \cdots + a_d x_d \leq bt + c.$$

Theorem (McMullen, Brion, Barvinok)

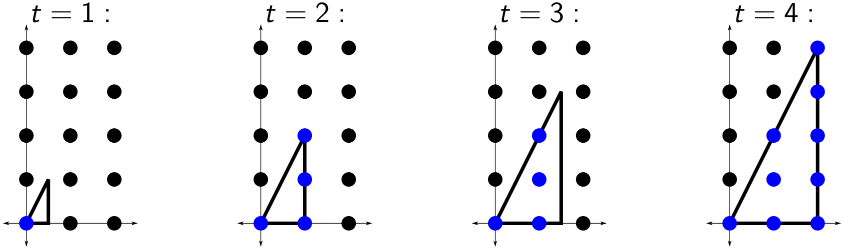
$|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

- Inclusion-exclusion on generating functions reduces to cones.
- Cones simply translate with t.
- Generating function of such a cone is easy.
- Compute $f(S; 1, \ldots, 1)$ with L'Hôpital's rule.

Generalizing Example 1

Our Example:

$$(x, y) \in \mathbb{Z}^2 : \; (y \geq 0) \wedge (2x \leq t) \wedge (y - 2x \leq 0)$$

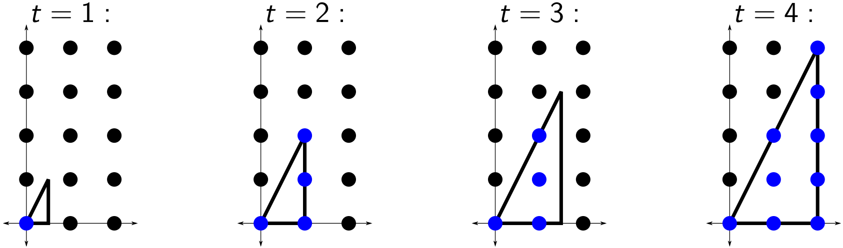


How about allowing other Boolean operations like $\vee$ (or)?

Generalizing Example 1

Our Example:

$$(x, y) \in \mathbb{Z}^2 : \ (y \geq 0) \wedge (2x \leq t) \wedge (y - 2x \leq 0)$$



How about allowing other Boolean operations like $\vee$ (or)?

No problem [Barvinok–Pommersheim].
For example, Disjunctive Normal Form yields union of parametric polyhedra:

$$A \wedge (B \vee C \vee D) \quad \text{is} \quad (A \wedge B) \vee (A \wedge C) \vee (A \wedge D).$$

Generalizing Example 1

How about adding quantifiers ($\exists, \forall$)?

Generalizing Example 1

How about adding quantifiers $(\exists, \forall)$?

No problem [W].

- Quantifiers can be eliminated [Presburger], by also using mod k operation, for constants k:

$$\{x \in \mathbb{N} : \ \exists y \in \mathbb{N}, x = 3y + 1\} = \{x \in \mathbb{N} : \ x = 1 \bmod 3\}.$$

- mod plays nicely with generating functions:

$$S = \{1, 4, 7, \dots\}, \qquad f(S; x) = x^1 + x^4 + x^7 + \cdots = \frac{x}{1 - x^3}.$$

Generalizing Example 1

How about adding quantifiers $(\exists, \forall)$?

No problem [W].

- Quantifiers can be eliminated [Presburger], by also using mod k operation, for constants k:

$$\{x \in \mathbb{N} : \ \exists y \in \mathbb{N}, x = 3y + 1\} = \{x \in \mathbb{N} : \ x = 1 \bmod 3\}.$$

- mod plays nicely with generating functions:

$$S = \{1, 4, 7, \ldots\}, \qquad f(S; x) = x^1 + x^4 + x^7 + \cdots = \frac{x}{1 - x^3}.$$

Generalizing Example 1

How about adding quantifiers ($\exists, \forall$)?

No problem [W].

- Quantifiers can be eliminated [Presburger], by also using mod k operation, for constants k:

$$\{x \in \mathbb{N} : \ \exists y \in \mathbb{N}, x = 3y + 1\} = \{x \in \mathbb{N} : \ x = 1 \bmod 3\}.$$

- mod plays nicely with generating functions:

$$S = \{1, 4, 7, \ldots\}, \qquad f(S; x) = x^1 + x^4 + x^7 + \cdots = \frac{x}{1 - x^3}.$$

Generalizing Example 1

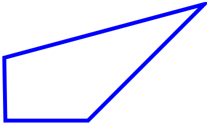
How about adding more parameter variables than simply t?

Generalizing Example 1

How about adding more parameter variables than simply t?

No problem [Barvinok–Pommersheim, W], with one new wrinkle:

$$\{a, b \in \mathbb{Z} : \ a \geq 0, \ b \geq 0, \ 2b - a \leq 2t - s, \ a - b \leq s - t\}.$$



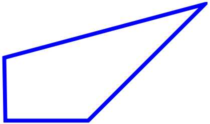
$t \leq s \leq 2t$

Generalizing Example 1

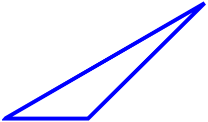
How about adding more parameter variables than simply t?

No problem [Barvinok–Pommersheim, W], with one new wrinkle:

$$\{a, b \in \mathbb{Z} : \; a \geq 0, \; b \geq 0, \; 2b - a \leq 2t - s, \; a - b \leq s - t\}.$$



$t \leq s \leq 2t$



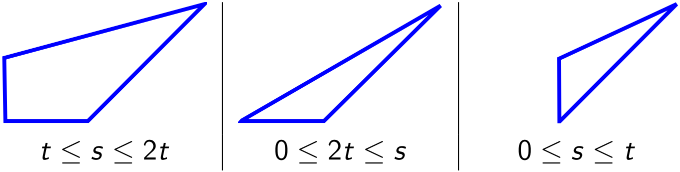
$0 \leq 2t \leq s$

Generalizing Example 1

How about adding more parameter variables than simply t?

No problem [Barvinok–Pommersheim, W], with one new wrinkle:

$$\{a, b \in \mathbb{Z} : \ a \geq 0, \ b \geq 0, \ 2b - a \leq 2t - s, \ a - b \leq s - t\}.$$



$t \leq s \leq 2t$ | $0 \leq 2t \leq s$ | $0 \leq s \leq t$

Generalizing Example 1

End up with

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

Theorem (W)

Suppose F is a first-order formula over the natural numbers, defined using linear inequalities, Boolean operations, and quantifiers (Presburger arithmetic). Suppose the free (unquantified) variables in F are $c_1, \dots c_d$ (the counted variables) and $p_1, \dots, p_n$ (the parameter variables). Then

$$g(p_1, \dots, p_n) = \#(c_1, \dots, c_d) \text{ making } F \text{ true}$$

is a piecewise quasi-polynomial, defined on polyhedral pieces.

Generalizing Example 1

End up with

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

Theorem (W)

Suppose F is a first-order formula over the natural numbers, defined using linear inequalities, Boolean operations, and quantifiers (Presburger arithmetic). Suppose the free (unquantified) variables in F are $c_1, \ldots c_d$ (the counted variables) and $p_1, \ldots, p_n$ (the parameter variables). Then

$$g(p_1, \ldots, p_n) = \#(c_1, \ldots, c_d) \text{ making } F \text{ true}$$

is a piecewise quasi-polynomial, defined on polyhedral pieces.

Generalizing Example 1

End up with

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

Theorem (W)

Suppose F is a first-order formula over the natural numbers, defined using linear inequalities, Boolean operations, and quantifiers (Presburger arithmetic). Suppose the free (unquantified) variables in F are $c_1, \ldots c_d$ (the counted variables) and $p_1, \ldots, p_n$ (the parameter variables). Then

$$g(p_1, \ldots, p_n) = \#(c_1, \ldots, c_d) \text{ making } F \text{ true}$$

is a piecewise quasi-polynomial, defined on polyhedral pieces.

Generalizing Example 1

End up with

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

Theorem (W)

Suppose F is a first-order formula over the natural numbers, defined using linear inequalities, Boolean operations, and quantifiers (Presburger arithmetic). Suppose the free (unquantified) variables in F are $c_1, \dots c_d$ (the counted variables) and $p_1, \dots, p_n$ (the parameter variables). Then

$$g(p_1, \dots, p_n) = \#(c_1, \dots, c_d) \text{ making } F \text{ true}$$

is a piecewise quasi-polynomial, defined on polyhedral pieces.

Example 2: Frobenius Problem

Definition: Let $\langle a_1, \ldots, a_n \rangle$ be the semigroup generated by $a_1, \ldots, a_n$, that is,

$$\left\{ \sum_{i=1}^{n} p_i a_i \;\middle|\; p_i \in \mathbb{Z}_{\geq 0} \right\}.$$

Example $\langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}$.

Definition: The Frobenius number, $F(a_1, \ldots, a_n)$, is the largest integer not in $\langle a_1, \ldots, a_n \rangle$ (exists when a_i are relatively prime).

So F(3,7)=11.

Example 2: Frobenius Problem

Definition: Let $\langle a_1, \ldots, a_n \rangle$ be the semigroup generated by $a_1, \ldots, a_n$, that is,

$$\left\{ \sum_{i=1}^{n} p_i a_i \;\middle|\; p_i \in \mathbb{Z}_{\geq 0} \right\}.$$

Example $\langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}$.

Definition: The Frobenius number, $F(a_1, \ldots, a_n)$, is the largest integer not in $\langle a_1, \ldots, a_n \rangle$ (exists when a_i are relatively prime).

So F(3,7)=11.

Example 2: Frobenius Problem

Definition: Let $\langle a_1, \ldots, a_n \rangle$ be the semigroup generated by $a_1, \ldots, a_n$, that is,

$$\left\{ \sum_{i=1}^{n} p_i a_i \;\middle|\; p_i \in \mathbb{Z}_{\geq 0} \right\}.$$

Example $\langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}$.

Definition: The Frobenius number, $F(a_1, \ldots, a_n)$, is the largest integer not in $\langle a_1, \ldots, a_n \rangle$ (exists when a_i are relatively prime).

So F(3,7)=11.

Example 2: Frobenius Problem

Definition: Let $\langle a_1, \ldots, a_n \rangle$ be the semigroup generated by $a_1, \ldots, a_n$, that is,

$$\left\{ \sum_{i=1}^{n} p_i a_i \;\middle|\; p_i \in \mathbb{Z}_{\geq 0} \right\}.$$

Example $\langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}$.

Definition: The Frobenius number, $F(a_1, \ldots, a_n)$, is the largest integer not in $\langle a_1, \ldots, a_n \rangle$ (exists when a_i are relatively prime).

So F(3,7)=11.

Example 2: Frobenius Problem

What is $F(t, t+1, t+2)$?

We'll work through this in a minute.

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

Simpler problem: What is $F(a, b)$, for a, b relatively prime?

Definition: The canonical form for an integer c is $c = pa + qb$ with $p, q \in \mathbb{Z}$ and $0 \leq p < b$.

Facts:

- If $c = p'a + q'b$ is any form with $p', q' \in \mathbb{Z}$, then all forms can be written as $c = (p' - kb)a + (q' + ka)b$, for $k \in \mathbb{Z}$.
- Canonical form exists and is unique. In fact, it is $ra + (q' + ka)b$, where k and r are the quotient and remainder when dividing p' by b.
- If $c = pa + qb$ is in canonical form, $c \in \langle a, b \rangle$ if and only if $q \geq 0$. ($\Leftarrow$: $p, q \geq 0$, so immediate. $\Rightarrow$: take $c = p'a + q'b$ with $p', q' \geq 0$ and use previous fact.)

Example 2: Frobenius Problem

So $c \in \mathbb{Z}$ are in bijection to canonical forms (p, q) with $0 \leq p < b$.

$c \in \langle a, b \rangle$ are in bijection to canonical forms with $q \geq 0$.

Largest $c \notin \langle a, b \rangle$ corresponds to $p = b - 1, q = -1$.

$$F(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

Example 2: Frobenius Problem

So $c \in \mathbb{Z}$ are in bijection to canonical forms (p, q) with $0 \leq p < b$.

$c \in \langle a, b \rangle$ are in bijection to canonical forms with $q \geq 0$.

Largest $c \notin \langle a, b \rangle$ corresponds to $p = b - 1, q = -1$.

$$F(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

Example 2: Frobenius Problem

So $c \in \mathbb{Z}$ are in bijection to canonical forms (p, q) with $0 \leq p < b$.

$c \in \langle a, b \rangle$ are in bijection to canonical forms with $q \geq 0$.

Largest $c \notin \langle a, b \rangle$ corresponds to $p = b - 1, q = -1$.

$$F(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

Example 2: Frobenius Problem

So $c \in \mathbb{Z}$ are in bijection to canonical forms (p, q) with $0 \leq p < b$.

$c \in \langle a, b \rangle$ are in bijection to canonical forms with $q \geq 0$.

Largest $c \notin \langle a, b \rangle$ corresponds to $p = b - 1, q = -1$.

$$F(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

Example 2: Frobenius Problem

So $c \in \mathbb{Z}$ are in bijection to canonical forms (p, q) with $0 \leq p < b$.

$c \in \langle a, b \rangle$ are in bijection to canonical forms with $q \geq 0$.

Largest $c \notin \langle a, b \rangle$ corresponds to $p = b - 1, q = -1$.

$$F(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

$F(3, 7) = 3 \cdot 7 - 3 - 7 = 11$.

Example 2: Frobenius Problem

How about $F(t, t+1, t+2)$?

Let

- $a = t$, $b = t+1$, $c = t+2$,
- $S = \langle a, b, c \rangle$,
- $T = \langle a, c \rangle$.

Note: $2b = a + c$.

So if $u = pa + qb + rc$, with $p, q, r \geq 0$ is a representation of $u \in S$, and if $q \geq 2$, then so is

$$(p+1)a + (q-2)b + (r+1)c.$$

$$S = T \cup (b + T).$$

Example 2: Frobenius Problem

How about $F(t, t+1, t+2)$?

Let

- $a = t$, $b = t+1$, $c = t+2$,
- $S = \langle a, b, c \rangle$,
- $T = \langle a, c \rangle$.

Note: $2b = a + c$.

So if $u = pa + qb + rc$, with $p, q, r \geq 0$ is a representation of $u \in S$, and if $q \geq 2$, then so is

$$(p+1)a + (q-2)b + (r+1)c.$$

$$S = T \cup (b + T).$$

Example 2: Frobenius Problem

How about $F(t, t+1, t+2)$?

Let

- $a = t$, $b = t + 1$, $c = t + 2$,
- $S = \langle a, b, c \rangle$,
- $T = \langle a, c \rangle$.

Note: $2b = a + c$.

So if $u = pa + qb + rc$, with $p, q, r \geq 0$ is a representation of $u \in S$, and if $q \geq 2$, then so is

$$(p+1)a + (q-2)b + (r+1)c.$$

$$S = T \cup (b + T).$$

Example 2: Frobenius Problem

How about $F(t, t+1, t+2)$?

Let

- $a = t,\ b = t+1,\ c = t+2$,
- $S = \langle a, b, c \rangle$,
- $T = \langle a, c \rangle$.

Note: $2b = a + c$.

So if $u = pa + qb + rc$, with $p, q, r \geq 0$ is a representation of $u \in S$, and if $q \geq 2$, then so is

$$(p+1)a + (q-2)b + (r+1)c.$$

$$S = T \cup (b + T).$$

Example 2: Frobenius Problem

How about $F(t, t+1, t+2)$?

Let

- $a = t$, $b = t+1$, $c = t+2$,
- $S = \langle a, b, c \rangle$,
- $T = \langle a, c \rangle$.

Note: $2b = a + c$.

So if $u = pa + qb + rc$, with $p, q, r \geq 0$ is a representation of $u \in S$, and if $q \geq 2$, then so is

$$(p+1)a + (q-2)b + (r+1)c.$$

$$S = T \cup (b + T).$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t + 2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s+1, 2s+3) = \gcd(2, 2s+1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s+1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t + 2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s+1, 2s+3) = \gcd(2, 2s+1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s+1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s+1, 2s+3) = \gcd(2, 2s+1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s+1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s+1, 2s+3) = \gcd(2, 2s+1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s+1)a - sc.$$

Example 2: Frobenius Problem

$$\gcd(a, c) = \gcd(t, t+2) = \gcd(2, t).$$

Case: t is odd. Let $t = 2s + 1$.
So $a = t = 2s + 1, \quad b = t + 1 = 2s + 2, \quad c = t + 2 = 2s + 3.$

$$\gcd(a, c) = \gcd(2s + 1, 2s + 3) = \gcd(2, 2s + 1) = \gcd(1, 2) = 1.$$

Extended Euclidean algorithm yields

$$1 = (s + 1)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2+4s+2)a - (2s^2+2s)c.$$

To get canonical form, divide $(2s^2+4s+2)$ by $c = 2s+3$.

Quotient is s, with remainder $s+2$, so the canonical form for b is

$$\big((2s^2+4s+2) - sc\big)a + \big(-(2s^2+2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2 + 4s + 2)a - (2s^2 + 2s)c.$$

To get canonical form, divide $(2s^2 + 4s + 2)$ by $c = 2s + 3$.

Quotient is s, with remainder $s + 2$, so the canonical form for b is

$$\big((2s^2 + 4s + 2) - sc\big)a + \big(-(2s^2 + 2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s + 1)a - sc.$$

So one form for b is

$$b = b(s + 1)a - bsc = (2s^2 + 4s + 2)a - (2s^2 + 2s)c.$$

To get canonical form, divide $(2s^2 + 4s + 2)$ by $c = 2s + 3$.

Quotient is s, with remainder $s + 2$, so the canonical form for b is

$$\big((2s^2 + 4s + 2) - sc\big)a + \big(-(2s^2 + 2s) + sa\big)c = (s + 2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2+4s+2)a - (2s^2+2s)c.$$

To get canonical form, divide $(2s^2+4s+2)$ by $c = 2s+3$.

Quotient is s, with remainder $s+2$, so the canonical form for b is

$$\big((2s^2+4s+2) - sc\big)a + \big(-(2s^2+2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2 + 4s + 2)a - (2s^2 + 2s)c.$$

To get canonical form, divide $(2s^2 + 4s + 2)$ by $c = 2s + 3$.

Quotient is s, with remainder $s + 2$, so the canonical form for b is

$$\big((2s^2 + 4s + 2) - sc\big)a + \big(-(2s^2 + 2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2+4s+2)a - (2s^2+2s)c.$$

To get canonical form, divide $(2s^2+4s+2)$ by $c = 2s+3$.

Quotient is s, with remainder $s+2$, so the canonical form for b is

$$\big((2s^2+4s+2) - sc\big)a + \big(-(2s^2+2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

$$1 = (s+1)a - sc.$$

So one form for b is

$$b = b(s+1)a - bsc = (2s^2+4s+2)a - (2s^2+2s)c.$$

To get canonical form, divide $(2s^2+4s+2)$ by $c = 2s+3$.

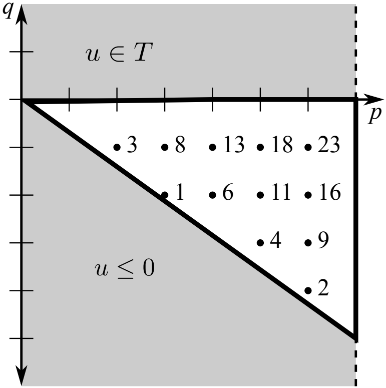
Quotient is s, with remainder $s+2$, so the canonical form for b is

$$\big((2s^2+4s+2) - sc\big)a + \big(-(2s^2+2s) + sa\big)c = (s+2)a - sc.$$

Example 2: Frobenius Problem

Reminder: $T = \langle a, c\rangle$ and $S = \langle a, b, c\rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \le p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5,\ b = 6,\ c = 7$.

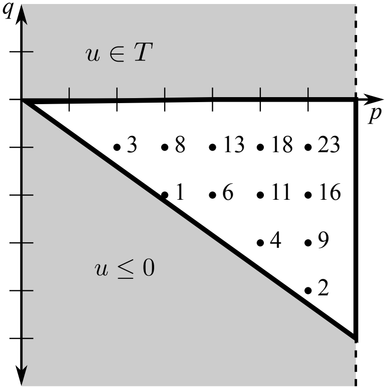
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c \rangle$ and $S = \langle a, b, c \rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \leq p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

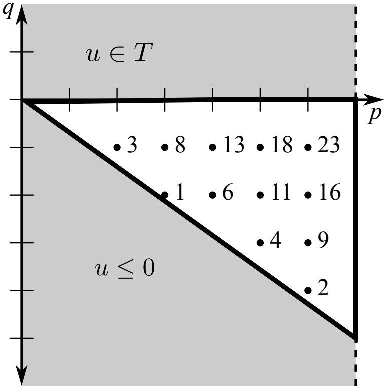
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c \rangle$ and $S = \langle a, b, c \rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \leq p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

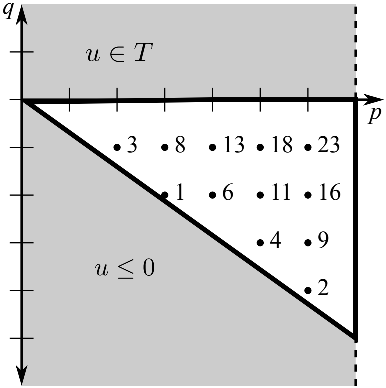
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c \rangle$ and $S = \langle a, b, c \rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \le p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5,\ b = 6,\ c = 7$.

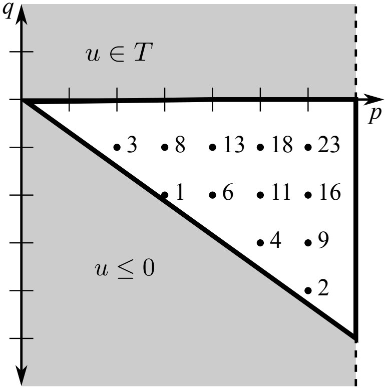
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c \rangle$ and $S = \langle a, b, c \rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \leq p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

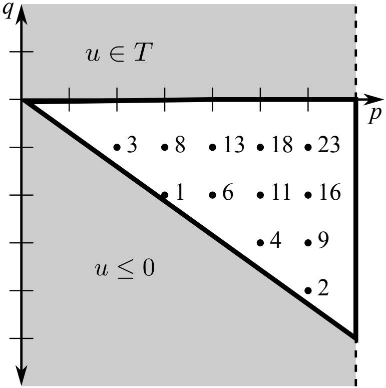
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c\rangle$ and $S = \langle a, b, c\rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \le p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

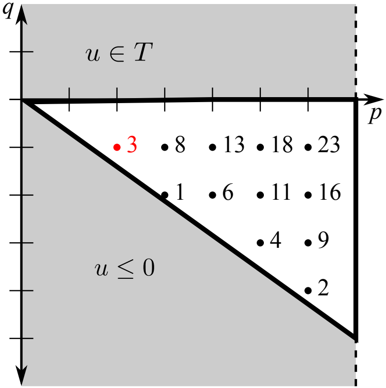
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c \rangle$ and $S = \langle a, b, c \rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \leq p < c$.
$u \notin T$ means $q < 0$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

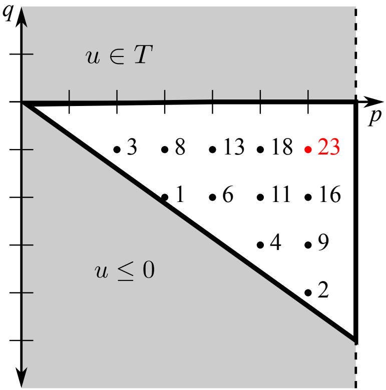
$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

Example 2: Frobenius Problem

Reminder: $T = \langle a, c\rangle$ and $S = \langle a, b, c\rangle = T \cup (b + T)$.
Want: Largest integer $u \notin S$. That is, $u \notin T$ and $u \notin b + T$.

Let $u = pa + qc$ be canonical form for u, $0 \le p < c$.
$u \notin T$ means $q < 0$.



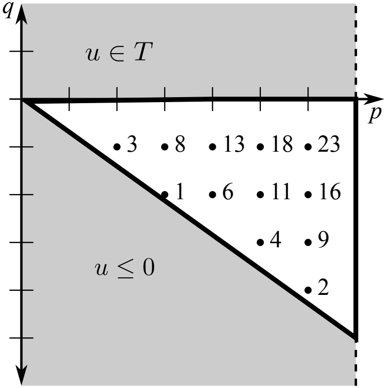
$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

$3 = 2 \cdot 5 - 1 \cdot 7$ is in canonical form. $3 \notin T$.

$F(5, 7) = 6 \cdot 5 - 1 \cdot 7 = 23$.

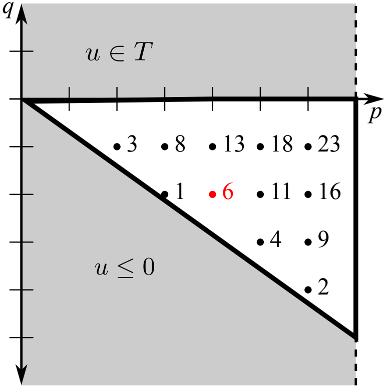
Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.



Example 2: Frobenius Problem

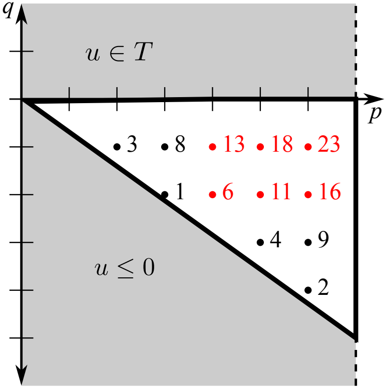
Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.



$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s + 2)a - sc$.

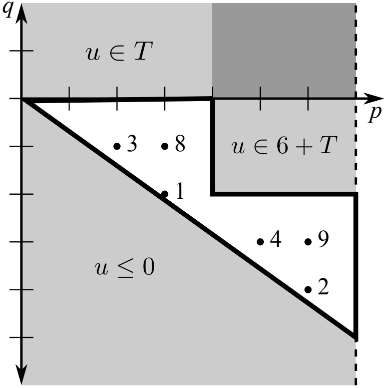


$t = 5$.
$a = 5$, $b = 6$, $c = 7$.

$b + T$ shown in red.

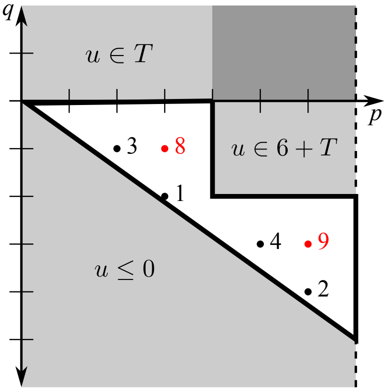
Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s + 2)a - sc$.



Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

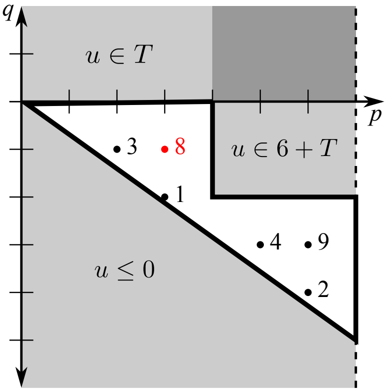


Candidates for $F(a, b, c)$ are the "corners".

$F(5, 6, 7) = \max\{8, 9\} = 9$.

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

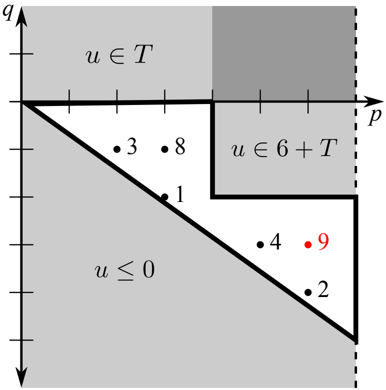


General corners:
$p = s+1, q = -1$ and
$p = 2s+2, q = -s-1$.

$$
\begin{aligned}
F(t, t+1, t+2) &= \max\{(s+1)a - 1c, \\
&\qquad (2s+2)a + (-s-1)c\} \\
&= 2s^2 + s - 1 \\
&= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}).
\end{aligned}
$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

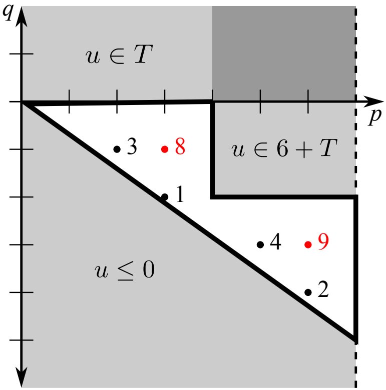


General corners:
$p = s+1, q = -1$ and
$p = 2s+2, q = -s-1$.

$$\begin{aligned} F(t, t+1, t+2) &= \max\{(s+1)a - 1c, \\ &\qquad (2s+2)a + (-s-1)c\} \\ &= 2s^2 + s - 1 \\ &= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}). \end{aligned}$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

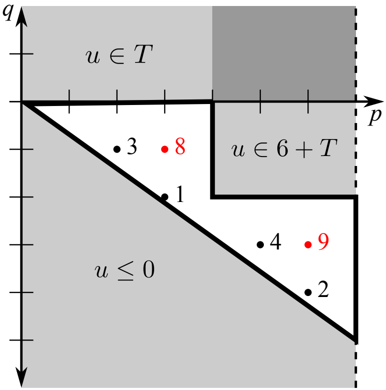


General corners:
$p = s+1, q = -1$ and
$p = 2s+2, q = -s-1$.

$$F(t, t+1, t+2)$$
$$= \max\{(s+1)a - 1c,\ (2s+2)a + (-s-1)c\}$$
$$= 2s^2 + s - 1$$
$$= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}).$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

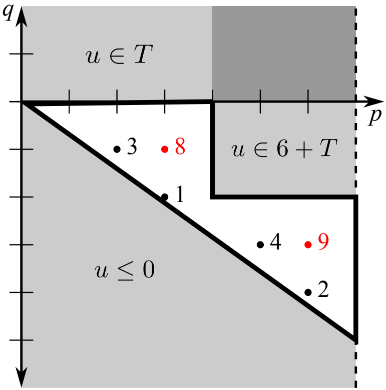


General corners:
$p = s+1, q = -1$ and
$p = 2s+2, q = -s-1$.

$$
\begin{aligned}
F(t, t+1, t+2) \\
&= \max\{(s+1)a - 1c, \\
&\quad (2s+2)a + (-s-1)c\} \\
&= 2s^2 + s - 1 \\
&= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}).
\end{aligned}
$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

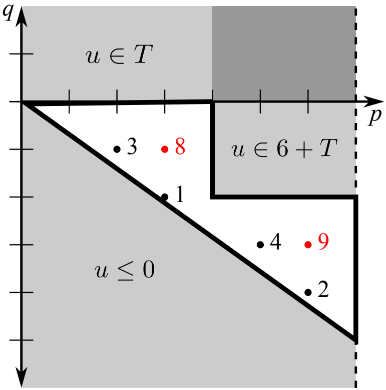


General corners:
$p = s + 1, q = -1$ and
$p = 2s + 2, q = -s - 1$.

$$
\begin{aligned}
F(t, t+1, t+2) \\
&= \max\{(s+1)a - 1c, \\
&\qquad (2s+2)a + (-s-1)c\} \\
&= 2s^2 + s - 1 \\
&= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}).
\end{aligned}
$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.

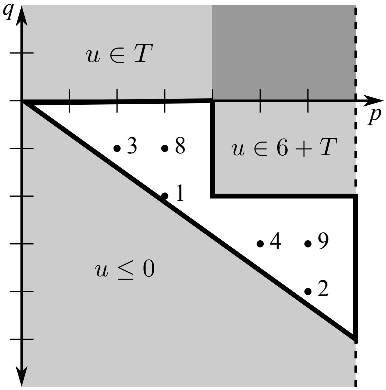


General corners:
$p = s+1, q = -1$ and
$p = 2s+2, q = -s-1$.

$$
\begin{aligned}
F(t, t+1, t+2) \\
&= \max\{(s+1)a - 1c, \\
&\qquad (2s+2)a + (-s-1)c\} \\
&= 2s^2 + s - 1 \\
&= \frac{t^2}{2} - \frac{t}{2} - 1 \quad (t \text{ odd}).
\end{aligned}
$$

Example 2: Frobenius Problem

Want: $u \notin T$ and $u \notin b + T$.
Reminder: $b = (s+2)a - sc$.



Similarly,

$$F(t, t+1, t+2) = \frac{t^2}{2} \quad (t \text{ even}).$$

What's Different?

$$\langle t, t+1, t+2 \rangle = \left\{ x \in \mathbb{N} : \exists y_1, y_2, y_3 \in \mathbb{N},\ x = t y_1 + (t+1) y_2 + (t+2) y_3 \right\}.$$

What's Different?

$$\langle t, t+1, t+2\rangle = \left\{x \in \mathbb{N} : \ \exists y_1, y_2, y_3 \in \mathbb{N},\ x = ty_1 + (t+1)y_2 + (t+2)y_3\right\}.$$

Coefficients of the variables depend on t.
As t changes, the normal vectors of (in)equalities change.

Still seems to be quasi-polynomial behavior in this situation, for sufficiently large t.

What's Different?

$$\langle t, t+1, t+2\rangle = \left\{x \in \mathbb{N} : \exists y_1, y_2, y_3 \in \mathbb{N},\ x = ty_1 + (t+1)y_2 + (t+2)y_3\right\}.$$

Coefficients of the variables depend on t.
As t changes, the normal vectors of (in)equalities change.

Still seems to be quasi-polynomial behavior in this situation, for sufficiently large t.

What's Different?

$$\langle t, t+1, t+2 \rangle = \left\{ x \in \mathbb{N} : \ \exists y_1, y_2, y_3 \in \mathbb{N}, \ x = ty_1 + (t+1)y_2 + (t+2)y_3 \right\}.$$

Coefficients of the variables depend on t.
As t changes, the normal vectors of (in)equalities change.

Still seems to be quasi-polynomial behavior in this situation, for sufficiently large t.

What's Different?

Theorem (Roune–W)

If $a_1(t), \ldots, a_n(t)$ are linear functions of t, then $F\big(a_1(t), \ldots, a_n(t)\big)$ agrees with a quasi-polynomial, for sufficiently large t.

Theorem (Chen–Li–Sam)

If P_t is a polyhedron defined by linear inequalities of the form

$$a_1(t)x_1 + \cdots + a_d(t)x_d \leq a_0(t),$$

where $a_i(t)$ are polynomials in t, then $|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

Similar phenomenon for integer hulls of such polyhedra [Calegari–Walker].

What's Different?

Theorem (Roune–W)

If $a_1(t), \ldots, a_n(t)$ *are linear functions of* t*, then* $F\big(a_1(t), \ldots, a_n(t)\big)$ *agrees with a quasi-polynomial, for sufficiently large* t*.*

Theorem (Chen–Li–Sam)

If P_t *is a polyhedron defined by linear inequalities of the form*

$$a_1(t)x_1 + \cdots + a_d(t)x_d \leq a_0(t),$$

where $a_i(t)$ *are polynomials in* t*, then* $|P_t \cap \mathbb{Z}^d|$ *agrees with a quasi-polynomial, for sufficiently large* t*.*

Similar phenomenon for integer hulls of such polyhedra [Calegari–Walker].

What's Different?

Theorem (Roune–W)

If $a_1(t), \ldots, a_n(t)$ are linear functions of t, then $F\big(a_1(t), \ldots, a_n(t)\big)$ agrees with a quasi-polynomial, for sufficiently large t.

Theorem (Chen–Li–Sam)

If P_t is a polyhedron defined by linear inequalities of the form

$$a_1(t)x_1 + \cdots + a_d(t)x_d \leq a_0(t),$$

where $a_i(t)$ are polynomials in t, then $|P_t \cap \mathbb{Z}^d|$ agrees with a quasi-polynomial, for sufficiently large t.

Similar phenomenon for integer hulls of such polyhedra [Calegari–Walker].

What's Different?

Conjecture: This works in general, for formulas in Presburger arithmetic, extended to allow coefficients of the linear inequalities to be polynomials in t.

Caution: Only works with one parameter. For example

$$S_{s,t} = \{(x, y) \in \mathbb{N}^2 : \ sx + ty = st\}$$

is the line segment between $(t, 0)$ and $(0, s)$, so

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

is not a quasi-polynomial.

What's Different?

Conjecture: This works in general, for formulas in Presburger arithmetic, extended to allow coefficients of the linear inequalities to be polynomials in t.

Caution: Only works with one parameter. For example

$$S_{s,t} = \{(x, y) \in \mathbb{N}^2 : \ sx + ty = st\}$$

is the line segment between $(t, 0)$ and $(0, s)$, so

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

is not a quasi-polynomial.

What's Different?

Conjecture: This works in general, for formulas in Presburger arithmetic, extended to allow coefficients of the linear inequalities to be polynomials in t.

Caution: Only works with one parameter. For example

$$S_{s,t} = \{(x,y) \in \mathbb{N}^2 : \; sx + ty = st\}$$

is the line segment between $(t,0)$ and $(0,s)$, so

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

is not a quasi-polynomial.

What's Different?

Conjecture: This works in general, for formulas in Presburger arithmetic, extended to allow coefficients of the linear inequalities to be polynomials in t.

Caution: Only works with one parameter. For example

$$S_{s,t} = \{(x, y) \in \mathbb{N}^2 : \; sx + ty = st\}$$

is the line segment between $(t, 0)$ and $(0, s)$, so

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

is not a quasi-polynomial.

What's Different?

Key Tool: Division algorithm – and hence gcd – yields quasi-polynomial behavior.

Example: Divide $a = t^2 - t + 3$ by $b = 2t$.

Usual division algorithm in $\mathbb{Q}[t]$:

$$a = \left(\frac{t}{2} - \frac{1}{2}\right) \cdot b + 3.$$

What's Different?

Key Tool: Division algorithm – and hence gcd – yields quasi-polynomial behavior.

Example: Divide $a = t^2 - t + 3$ by $b = 2t$.

Usual division algorithm in $\mathbb{Q}[t]$:

$$a = \left(\frac{t}{2} - \frac{1}{2}\right) \cdot b + 3.$$

What's Different?

Key Tool: Division algorithm – and hence gcd – yields quasi-polynomial behavior.

Example: Divide $a = t^2 - t + 3$ by $b = 2t$.

Usual division algorithm in $\mathbb{Q}[t]$:

$$a = \left(\frac{t}{2} - \frac{1}{2}\right) \cdot b + 3.$$

What's Different?

Key Tool: Division algorithm – and hence gcd – yields quasi-polynomial behavior.

Example: Divide $a = t^2 - t + 3$ by $b = 2t$.

Usual division algorithm in $\mathbb{Q}[t]$:

$$a = \left(\frac{t}{2} - \frac{1}{2}\right) \cdot b + 3.$$

But quotient may not be integral!

What's Different?

Break into cases based on parity of t. If $t = 2s$ is even:

$$\begin{aligned} a &= t^2 - t + 3 = 4s^2 - 2s + 3, \\ b &= 2t = 4s, \end{aligned}$$

$$\begin{aligned} a &= s \cdot b + (-2s + 3) \\ &= (s-1) \cdot b + (b - 2s + 3) \\ &= (s-1) \cdot b + (2s + 3), \end{aligned}$$

with $0 \leq 2s + 3 < b$ for sufficiently large s.

What's Different?

Break into cases based on parity of t. If $t = 2s$ is even:

$$a = t^2 - t + 3 = 4s^2 - 2s + 3,$$
$$b = 2t = 4s,$$

$$\begin{aligned} a &= s \cdot b + (-2s + 3) \\ &= (s-1) \cdot b + (b - 2s + 3) \\ &= (s-1) \cdot b + (2s + 3), \end{aligned}$$

with $0 \leq 2s + 3 < b$ for sufficiently large s.

What's Different?

Break into cases based on parity of t. If $t = 2s$ is even:

$$\begin{aligned} a &= t^2 - t + 3 = 4s^2 - 2s + 3, \\ b &= 2t = 4s, \end{aligned}$$

$$\begin{aligned} a &= s \cdot b + (-2s + 3) \\ &= (s-1) \cdot b + (b - 2s + 3) \\ &= (s-1) \cdot b + (2s + 3), \end{aligned}$$

with $0 \leq 2s + 3 < b$ for sufficiently large s.

What's Different?

Break into cases based on parity of t. If $t = 2s$ is even:

$$\begin{aligned} a &= t^2 - t + 3 = 4s^2 - 2s + 3, \\ b &= 2t = 4s, \end{aligned}$$

$$\begin{aligned} a &= s \cdot b + (-2s + 3) \\ &= (s - 1) \cdot b + (b - 2s + 3) \\ &= (s - 1) \cdot b + (2s + 3), \end{aligned}$$

with $0 \leq 2s + 3 < b$ for sufficiently large s.

What's Different?

Break into cases based on parity of t. If $t = 2s$ is even:

$$a = t^2 - t + 3 = 4s^2 - 2s + 3,$$
$$b = 2t = 4s,$$

$$\begin{aligned} a &= s \cdot b + (-2s + 3) \\ &= (s-1) \cdot b + (b - 2s + 3) \\ &= (s-1) \cdot b + (2s+3), \end{aligned}$$

with $0 \leq 2s + 3 < b$ for sufficiently large s.

What's Different?

- [Roune–W], [Chen–Li–Sam], [Calegari–Walker] all use division algoirthm heavily.
- But all have their own tricks on top of that.
- An algorithm like quantifier elimination would be desirable.

What's Different?

- [Roune–W], [Chen–Li–Sam], [Calegari–Walker] all use division algoirthm heavily.
- But all have their own tricks on top of that.
- An algorithm like quantifier elimination would be desirable.

What's Different?

- [Roune–W], [Chen–Li–Sam], [Calegari–Walker] all use division algoirthm heavily.
- But all have their own tricks on top of that.
- An algorithm like quantifier elimination would be desirable.

Thank You!