Presburger Arithmetic, Rational Generating Functions, and Quasi-polynomials

Kevin Woods
Oberlin College

Examples

Theme: Generating functions encode patterns of sets, in useful ways.

Definition: Given $S \subseteq \mathbb{N}^d$, define

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

Example: $S = \left\{ a \in \mathbb{N} : \ a \leq 5000 \right\}$. Then

$$f(S; x) = 1 + x + x^2 + \cdots + x^{5000}$$

Examples

Theme: Generating functions encode patterns of sets, in useful ways.

Definition: Given $S \subseteq \mathbb{N}^d$, define

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

Example: $S = \left\{ a \in \mathbb{N} : \; a \leq 5000 \right\}$. Then

$$f(S; x) = 1 + x + x^2 + \cdots + x^{5000}$$

Examples

Theme: Generating functions encode patterns of sets, in useful ways.

Definition: Given $S \subseteq \mathbb{N}^d$, define

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

Example: $S = \left\{ a \in \mathbb{N} : \ a \leq 5000 \right\}$. Then

$$f(S; x) = 1 + x + x^2 + \cdots + x^{5000}$$

Examples

Theme: Generating functions encode patterns of sets, in useful ways.

Definition: Given $S \subseteq \mathbb{N}^d$, define

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

Example: $S = \{a \in \mathbb{N} : \ a \leq 5000\}$. Then

$$\begin{aligned} f(S; x) &= 1 + x + x^2 + \cdots + x^{5000} \\ &= \frac{1 - x^{5001}}{1 - x}. \end{aligned}$$

Examples

$$S = \left\{ a \in \mathbb{N} : \ \exists b \in \mathbb{N}, \ a = 2b+1, \ a \leq 5000 \right\}.$$

$$\begin{aligned} f(S;x) &= x + x^3 + x^5 + \cdots + x^{4999} \\ &= \frac{x - x^{5000}}{1-x^2}. \end{aligned}$$

Examples

$$S = \left\{a \in \mathbb{N} : \ \exists b \in \mathbb{N},\ a = 2b+1,\ a \leq 5000\right\}.$$

$$\begin{aligned} f(S;x) &= x + x^3 + x^5 + \cdots + x^{4999} \\ &= \frac{x - x^{5000}}{1 - x^2}. \end{aligned}$$

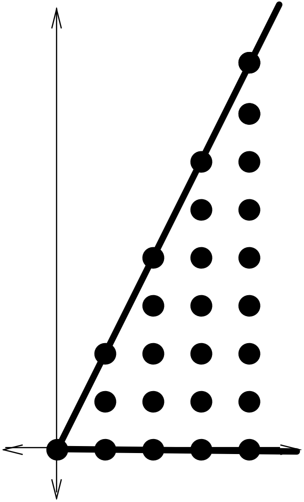
Examples

$$S = \left\{ a \in \mathbb{N} : \ \exists b \in \mathbb{N}, \ a = 2b+1, \ a \le 5000 \right\}.$$

$$\begin{aligned} f(S; x) &= x + x^3 + x^5 + \cdots + x^{4999} \\ &= \frac{x - x^{5000}}{1 - x^2}. \end{aligned}$$

Examples

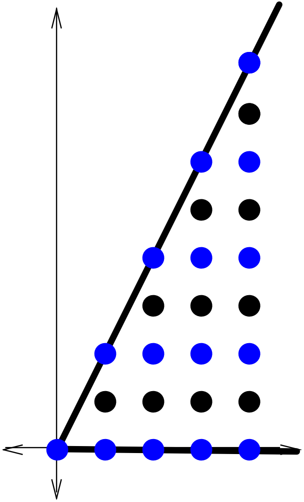
$$S = \{(a,b) \in \mathbb{N}^2 : \; b \le 2a\}$$



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

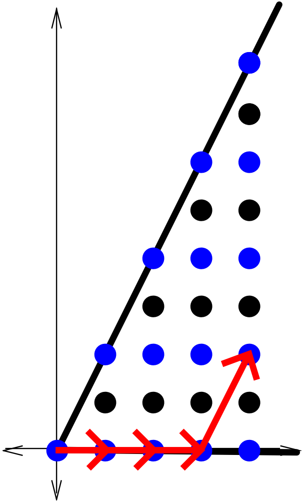
Examples

$$S = \left\{(a, b) \in \mathbb{N}^2 : \ b \leq 2a\right\}$$



Examples

$$S = \{(a, b) \in \mathbb{N}^2 : \ b \leq 2a\}$$

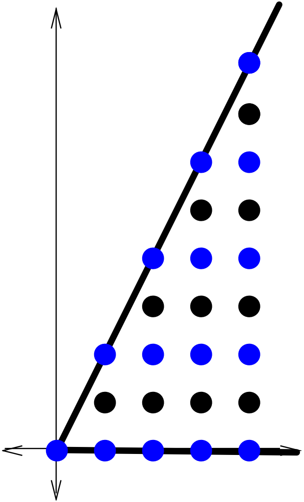


$$x^4 y^2 = (x)^3 (xy^2)^1$$

$$\begin{aligned} &(1 + x + x^2 + x^3 + \cdots) \\ &\cdot (1 + (xy^2)^1 + (xy^2)^2 + \cdots) \\ &= \frac{1}{(1-x)(1-xy^2)} \end{aligned}$$

Examples

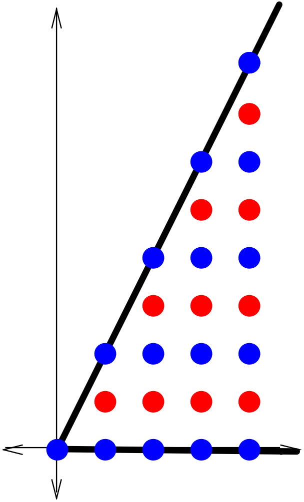
$$S = \left\{(a,b) \in \mathbb{N}^2 : \ b \leq 2a\right\}$$



$$\begin{gathered}(1 + x + x^2 + x^3 + \cdots) \\ \cdot(1 + (xy^2)^1 + (xy^2)^2 + \cdots) \\ = \frac{1}{(1-x)(1-xy^2)}\end{gathered}$$

Examples

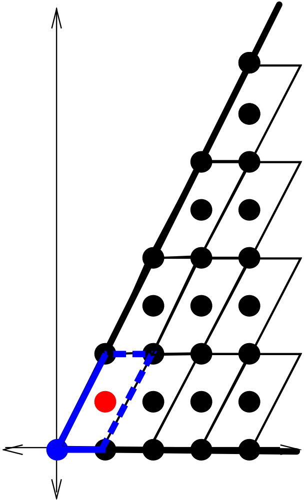
$$S = \{(a,b) \in \mathbb{N}^2 : \; b \leq 2a\}$$



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

Examples

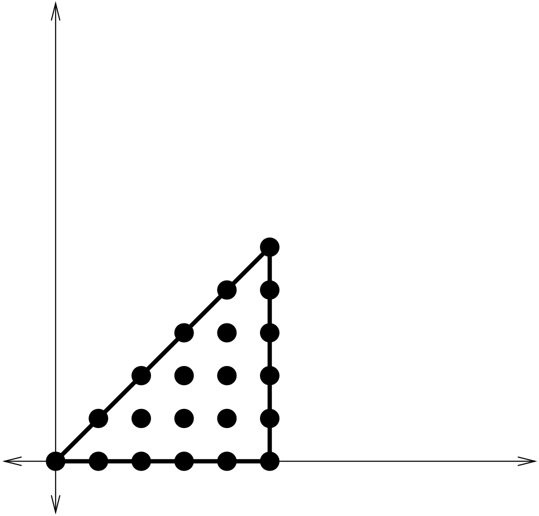
$$S = \left\{(a, b) \in \mathbb{N}^2 : \; b \leq 2a\right\}$$



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

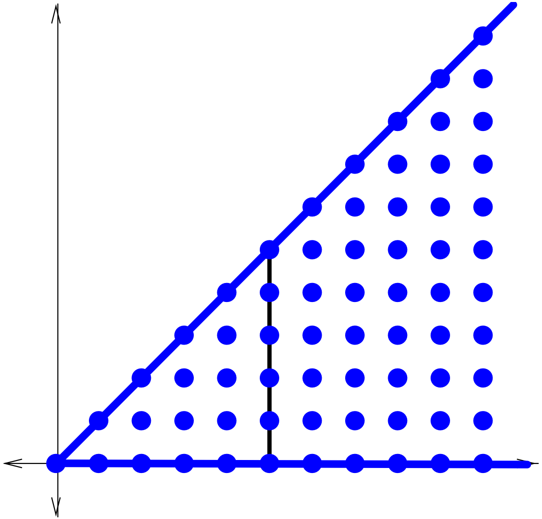
Examples

$$S = \left\{(a, b) \in \mathbb{N}^2 : \ b \leq a, \ a \leq 5\right\}$$



Examples

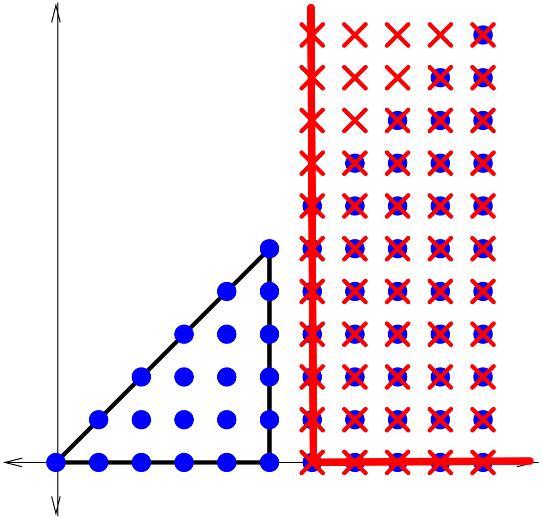
$$S = \left\{(a,b) \in \mathbb{N}^2 : \; b \leq a, \; a \leq 5\right\}$$



$$\frac{1}{(1-x)(1-xy)}$$

Examples

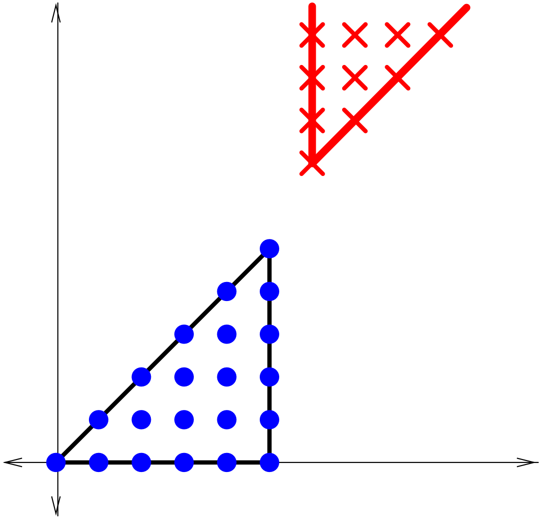
$$S = \left\{(a,b) \in \mathbb{N}^2 : \; b \le a, \; a \le 5\right\}$$



$$-\frac{x^6}{(1-x)(1-y)}$$

Examples

$$S = \left\{(a, b) \in \mathbb{N}^2 : \; b \leq a, \; a \leq 5\right\}$$

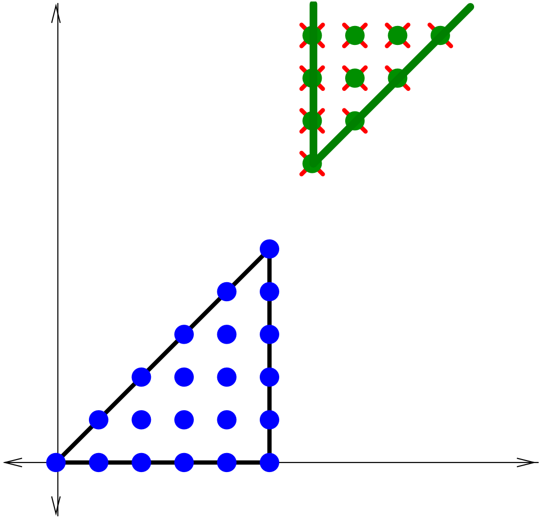


$$\frac{1}{(1-x)(1-xy)}$$

$$-\frac{x^6}{(1-x)(1-y)}$$

Examples

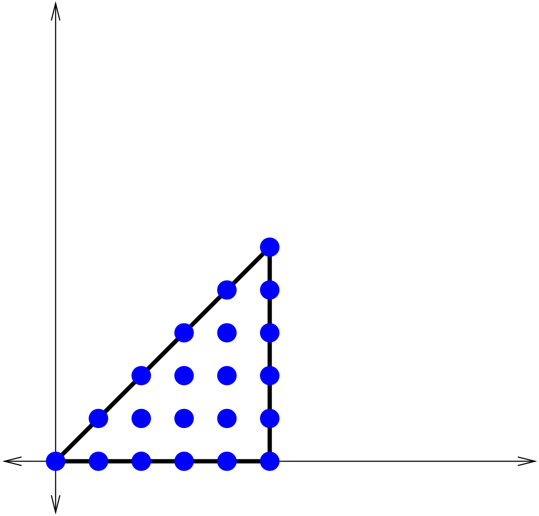
$$S = \{(a,b) \in \mathbb{N}^2 : \; b \le a, \; a \le 5\}$$



$$+\frac{x^6 y^7}{(1-xy)(1-y)}$$

Examples

$$S = \left\{(a,b) \in \mathbb{N}^2 : \ b \leq a, \ a \leq 5\right\}$$



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

$$\frac{1}{(1-x)(1-xy)}$$

$$-\frac{x^6}{(1-x)(1-y)}$$

$$+\frac{x^6y^7}{(1-xy)(1-y)}.$$

Presburger Sets

Definition: A Presburger set is defined over $\mathbb{N}^d$ using quantifiers ($\exists$ and $\forall$), boolean operations (and, or, not), and linear (in)equalities ($\leq$, $=$, $>$).

Examples

$$S = \left\{a \in \mathbb{N} : \; a \leq 5000\right\}$$
$$S = \left\{a \in \mathbb{N} : \; \exists b \in \mathbb{N}, \; a = 2b + 1, \; a \leq 5000\right\}$$
$$S = \left\{(a, b) \in \mathbb{N}^2 : \; b \leq 2a\right\}$$
$$S = \left\{(a, b) \in \mathbb{N}^2 : \; b \leq a, \; a \leq 5\right\}$$

Presburger Sets

The generating function of a Presburger set is a rational function:

- Cones: see example (triangulate if not simplicial).
- Polyhedra: by inclusion-exclusion [Brion].
- Quantifier-free formulas: unions of polyhedra (DNF).
- All Presburger sets: quantifier elimination [Presburger].

Presburger Sets

The generating function of a Presburger set is a rational function:

- Cones: see example (triangulate if not simplicial).
- Polyhedra: by inclusion-exclusion [Brion].
- Quantifier-free formulas: unions of polyhedra (DNF).
- All Presburger sets: quantifier elimination [Presburger].

Presburger Sets

The generating function of a Presburger set is a rational function:

- Cones: see example (triangulate if not simplicial).
- Polyhedra: by inclusion-exclusion [Brion].
- Quantifier-free formulas: unions of polyhedra (DNF).
- All Presburger sets: quantifier elimination [Presburger].

Presburger Sets

The generating function of a Presburger set is a rational function:

- Cones: see example (triangulate if not simplicial).
- Polyhedra: by inclusion-exclusion [Brion].
- Quantifier-free formulas: unions of polyhedra (DNF).
- All Presburger sets: quantifier elimination [Presburger].

Presburger Sets

The generating function of a Presburger set is a rational function:

- Cones: see example (triangulate if not simplicial).
- Polyhedra: by inclusion-exclusion [Brion].
- Quantifier-free formulas: unions of polyhedra (DNF).
- All Presburger sets: quantifier elimination [Presburger].

Presburger Sets

The following are equivalent:

- S is a Presburger set.
- $f(S; \mathbf{x})$ is a rational generating function.
- S is a finite union of sets of the form $P \cap (\lambda + \Lambda)$, where P is a polyhedron, $\lambda \in \mathbb{N}^d$, and $\Lambda \subseteq \mathbb{Z}^d$ is a lattice.
  [cf. semi-linear sets of Ginsburg, Spanier]

The Power of Generating Functions

So What?

So What?

The generating function contains all of the information of the set, in a way that can be exploited.

$$
\begin{aligned}
f(S;1) &= |S|. \\
\frac{\partial}{\partial x_1} f(S;\mathbf{x})\Big|_{\mathbf{x}=1} &= \sum_{\mathbf{a}\in S} a_1. \\
\text{degree } f\left(S; z^{c_1},\ldots,z^{c_d}\right) &= \max_{\mathbf{a}\in S} \mathbf{c}\cdot\mathbf{a}.
\end{aligned}
$$

So What?

The generating function contains all of the information of the set, in a way that can be exploited.

$$f(S; 1) = |S|.$$

$$\frac{\partial}{\partial x_1} f(S; \mathbf{x})\Big|_{\mathbf{x}=1} = \sum_{\mathbf{a} \in S} a_1.$$

$$\text{degree } f\left(S; z^{c_1}, \ldots, z^{c_d}\right) = \max_{\mathbf{a} \in S} \mathbf{c} \cdot \mathbf{a}.$$

So What?

The generating function contains all of the information of the set, in a way that can be exploited.

$$
\begin{aligned}
f(S;1) &= |S|. \\
\frac{\partial}{\partial x_1} f(S;\mathbf{x})\Big|_{\mathbf{x}=1} &= \sum_{\mathbf{a}\in S} a_1. \\
\text{degree } f\left(S; z^{c_1}, \ldots, z^{c_d}\right) &= \max_{\mathbf{a}\in S} \mathbf{c}\cdot\mathbf{a}.
\end{aligned}
$$

So What?

The generating function contains all of the information of the set, in a way that can be exploited.

$$f(S;1) = |S|.$$

$$\frac{\partial}{\partial x_1} f(S;\mathbf{x})\Big|_{\mathbf{x}=1} = \sum_{\mathbf{a}\in S} a_1.$$

$$\text{degree } f\left(S; z^{c_1}, \ldots, z^{c_d}\right) = \max_{\mathbf{a}\in S} \mathbf{c}\cdot\mathbf{a}.$$

The Power of Generating Functions

For fixed dimension, given rational generating functions $f(S;\mathbf{x})$ and $f(T;\mathbf{x})$, there are polynomial time algorithms to compute

- $f(S;1)$
- $\frac{\partial}{\partial x_1} f(S;\mathbf{x})$
- degree $f\left(S; z^{c_1}, \ldots, z^{c_d}\right)$
- $f(S \cap T);\mathbf{x})$

[Barvinok, W],

though it is NP-hard to compute, given a projection π,

- $f(\pi(S);\mathbf{x})$.

[W].

The Power of Generating Functions

For fixed dimension, given rational generating functions $f(S;\mathbf{x})$ and $f(T;\mathbf{x})$, there are polynomial time algorithms to compute

- $f(S;1)$
- $\frac{\partial}{\partial x_1} f(S;\mathbf{x})$
- degree $f\left(S; z^{c_1}, \dots, z^{c_d}\right)$
- $f(S \cap T); \mathbf{x})$

[Barvinok, W],

though it is NP-hard to compute, given a projection π,

- $f(\pi(S);\mathbf{x})$.

[W].

The Power of Generating Functions

Proofs using generating functions:

- For fixed dimension, the number of solutions to a quantifier-free Presburger formula (e.g., a polyhedron) is computable in polynomial time. [Barvinok]
- For fixed dimension and number of linear inequalities, the number of solutions to Presburger formula with no quantifier alternation (using only $\exists$ or only $\forall$) is computable in polynomial time. [Barvinok, W]

The Power of Generating Functions

Proofs using generating functions:

- For fixed dimension, the number of solutions to a quantifier-free Presburger formula (e.g., a polyhedron) is computable in polynomial time. [Barvinok]
- For fixed dimension and number of linear inequalities, the number of solutions to Presburger formula with no quantifier alternation (using only $\exists$ or only $\forall$) is computable in polynomial time. [Barvinok, W]

The Power of Generating Functions?

Proofs using generating functions:

- For fixed dimension, the number of solutions to a quantifier-free Presburger formula (e.g., a polyhedron) is computable in polynomial time. [Barvinok]
- For fixed dimension and number of linear inequalities, the number of solutions to Presburger formula with no quantifier alternation (using only $\exists$ or only $\forall$) is computable in polynomial time. [Barvinok, W]

Open Problem: What if there is quantifier alternation? Don't even know that the existence of solutions can be decided in polynomial time.

Parametric Counting

$$S_t = \{a \in \mathbb{N} : \ 2a \le t\}$$

Then

$$\begin{aligned} g(t) &\doteq |S_t| \\ &= \left\lfloor \frac{t}{2} \right\rfloor + 1 \\ &= \begin{cases} \frac{t+2}{2} & \text{if } t \equiv 0 \bmod 2, \\ \frac{t+1}{2} & \text{if } t \equiv 1 \bmod 2 \end{cases} \end{aligned}$$

is a quasi-polynomial.

Parametric Counting

$$S_t = \{a \in \mathbb{N} : \ 2a \le t\}$$

Then

$$\begin{aligned} g(t) &\doteq \ |S_t| \\ &= \left\lfloor \frac{t}{2} \right\rfloor + 1 \\ &= \begin{cases} \frac{t+2}{2} & \text{if } t \equiv 0 \bmod 2, \\ \frac{t+1}{2} & \text{if } t \equiv 1 \bmod 2 \end{cases} \end{aligned}$$

is a quasi-polynomial.

Parametric Counting

$$S_t = \{a \in \mathbb{N} : \ 2a \leq t\}$$

Then

$$\begin{aligned} g(t) &\doteq |S_t| \\ &= \left\lfloor \frac{t}{2} \right\rfloor + 1 \\ &= \begin{cases} \frac{t+2}{2} & \text{if } t \equiv 0 \bmod 2, \\ \frac{t+1}{2} & \text{if } t \equiv 1 \bmod 2 \end{cases} \end{aligned}$$

is a quasi-polynomial.

Parametric Counting

$$S_t = \{a \in \mathbb{N} : \ 2a \leq t\}$$

Then

$$\begin{aligned} g(t) &\doteq |S_t| \\ &= \left\lfloor \frac{t}{2} \right\rfloor + 1 \\ &= \begin{cases} \frac{t+2}{2} & \text{if } t \equiv 0 \bmod 2, \\ \frac{t+1}{2} & \text{if } t \equiv 1 \bmod 2 \end{cases} \end{aligned}$$

is a quasi-polynomial.

Parametric Counting

$$
\begin{aligned}
\sum_t g(t)x^t &= \sum_t \left(\left\lfloor \frac{t}{2} \right\rfloor + 1 \right) x^t \\
&= 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots \\
&= (1 + x)(1 + 2x^2 + 3x^4 + \cdots) \\
&= \frac{1 + x}{(1 - x^2)^2},
\end{aligned}
$$

Parametric Counting

$$\begin{aligned}\sum_t g(t)x^t &= \sum_t \left(\left\lfloor \frac{t}{2} \right\rfloor + 1\right) x^t \\ &= 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots \\ &= (1+x)(1 + 2x^2 + 3x^4 + \cdots) \\ &= \frac{1+x}{(1-x^2)^2},\end{aligned}$$

Parametric Counting

$$\begin{aligned}\sum_t g(t)x^t &= \sum_t \left(\left\lfloor \frac{t}{2} \right\rfloor + 1\right) x^t \\ &= 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots \\ &= {\color{red}(1+x)(1+2x^2+3x^4+\cdots)} \\ &= \frac{1+x}{(1-x^2)^2},\end{aligned}$$

Parametric Counting

$$
\begin{aligned}
\sum_t g(t)x^t &= \sum_t \left(\left\lfloor \frac{t}{2} \right\rfloor + 1 \right) x^t \\
&= 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots \\
&= (1+x)(1 + 2x^2 + 3x^4 + \cdots) \\
&= \frac{1+x}{(1-x^2)^2},
\end{aligned}
$$

by substituting $y = x^2$ into

$$
1+2y+3y^2+\cdots = \frac{\partial}{\partial y}(1+y+y^2+\cdots) = \frac{\partial}{\partial y}\left(\frac{1}{1-y}\right) = \frac{1}{(1-y)^2}.
$$

Parametric Counting

$$\begin{aligned}
\sum_t g(t)x^t &= \sum_t \left(\left\lfloor \frac{t}{2} \right\rfloor + 1 \right) x^t \\
&= 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \cdots \\
&= (1 + x)(1 + 2x^2 + 3x^4 + \cdots) \\
&= \frac{1 + x}{(1 - x^2)^2},
\end{aligned}$$

by substituting $y = x^2$ into

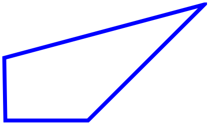
$$1+2y+3y^2+\cdots = \frac{\partial}{\partial y}(1+y+y^2+\cdots) = \frac{\partial}{\partial y}\left(\frac{1}{1-y}\right) = \frac{1}{(1-y)^2}.$$

This is a rational generating function!!!

Parametric Counting

With more than 1 parameter, need piecewise quasi-polynomials.

Example: $S_{s,t} = \{a, b \in \mathbb{N} : \ 2b - a \leq 2t - s, \ a - b \leq s - t\}$

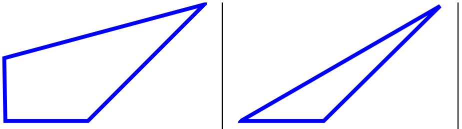


$t \leq s \leq 2t$

Parametric Counting

With more than 1 parameter, need piecewise quasi-polynomials.

Example: $S_{s,t} = \{a, b \in \mathbb{N} : \ 2b - a \leq 2t - s, \ a - b \leq s - t\}$

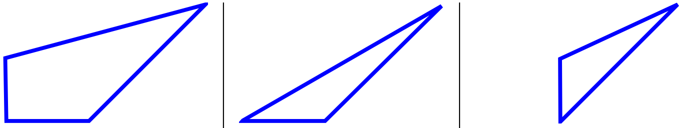


$t \leq s \leq 2t$ | $0 \leq 2t \leq s$

Parametric Counting

With more than 1 parameter, need piecewise quasi-polynomials.

Example: $S_{s,t} = \{a, b \in \mathbb{N} : \ 2b - a \leq 2t - s, \ a - b \leq s - t\}$

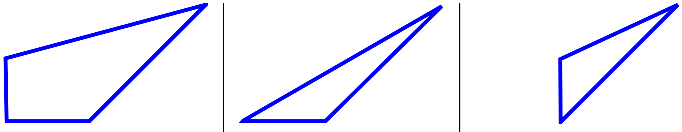


$t \leq s \leq 2t$ | $0 \leq 2t \leq s$ | $0 \leq s \leq t$

Parametric Counting

With more than 1 parameter, need piecewise quasi-polynomials.

Example: $S_{s,t} = \{a, b \in \mathbb{N} :\ 2b - a \leq 2t - s,\ a - b \leq s - t\}$



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

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

Parametric Counting

Given a function $g : \mathbb{N}^n \to \mathbb{Q}$ and the following three possible properties:

A. g parametrically counts solutions to a Presburger formula,

B. g is a piecewise quasi-polynomial, and

C. $\sum_{\mathbf{p} \in \mathbb{N}^n} g(\mathbf{p}) \mathbf{x}^{\mathbf{p}}$ is a rational function,

we have the implications

$$A \Rightarrow B \Leftrightarrow C.$$

Thank You!