Solving Lattice Point Problems Using Rational Generating Functions

Kevin Woods
Oberlin College

\[ T(x,y,z) = x \]
An Easy Start

Question: How many even numbers are there between 100 and 250?

List them all:


and count: 76.
An Easy Start

**Question:** How many even numbers are there between 100 and 250?

List them all:


and count: **76**.
An Easy Start

This is the wrong way to answer the question.
Another Easy One

Question: How many dots are in this picture?

Count them: 76.

This is the best we can do.
Another Easy One

Question: How many dots are in this picture?

Count them: 76.
This is the best we can do.
The difference:
The difference:

The set of even numbers between 100 and 250 has a pattern that we can take advantage of.

Theme of talk: Demonstrate a nice tool to take advantage of the special structure of certain sets.

That tool is generating functions.
The Easy Problem, Redux

Given a set $S \subseteq \mathbb{N}$, define the generating function

$$f(S; x) = \sum_{a \in S} x^a.$$

In example,

$$f(S; x) = x^{100} + x^{102} + x^{104} + \cdots + x^{248} + x^{250}$$

$$= \frac{x^{100} - x^{252}}{1 - x^2}.$$

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

Use l’Hospital’s rule:

$$f(S; 1) = \frac{100 - 252}{-2} = 76.$$
The Easy Problem, Redux

Given a set $S \subseteq \mathbb{N}$, define the generating function

$$f(S; x) = \sum_{a \in S} x^a.$$  

In example,  

$$f(S; x) = x^{100} + x^{102} + x^{104} + \cdots + x^{248} + x^{250} = \frac{x^{100} - x^{252}}{1 - x^2}.$$  

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

Use l’Hospital’s rule:

$$f(S; 1) = \frac{100 - 252}{-2} = 76.$$
The Easy Problem, Redux

Given a set $S \subseteq \mathbb{N}$, define the generating function

$$f(S; x) = \sum_{a \in S} x^a.$$ 

In example,

$$f(S; x) = x^{100} + x^{102} + x^{104} + \cdots + x^{248} + x^{250}$$

$$= \frac{x^{100} - x^{252}}{1 - x^2}.$$ 

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

Use l’Hospital’s rule:

$$f(S; 1) = \frac{100 - 252}{-2} = 76.$$
The Easy Problem, Redux

Given a set $S \subseteq \mathbb{N}$, define the generating function

$$f(S; x) = \sum_{a \in S} x^a.$$

In example,

$$f(S; x) = x^{100} + x^{102} + x^{104} + \cdots + x^{248} + x^{250} = \frac{x^{100} - x^{252}}{1 - x^2}.$$

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

Use l’Hospital’s rule:

$$f(S; 1) = \frac{100 - 252}{-2} = 76.$$
The Frobenius Problem

Let $a_1, a_2, \ldots, a_d$ be nonnegative integers such that $\gcd(a_1, a_2, \ldots, a_d) = 1$. Let

$$S = \{\lambda_1 a_1 + \cdots + \lambda_d a_d : \lambda_i \in \mathbb{N}\}.$$

**Question:** What is the largest integer not in $S$?

**Question:** How many positive integers are not in $S$?
The Frobenius Problem

Example:  \( a_1 = 3, \ a_2 = 7. \)

\[
S = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}.
\]

**Question:** What is the largest integer not in \( S \)?  
**Answer:** 11.

**Question:** How many positive integers are not in \( S \)?  
**Answer:** 6.
Listing out the set is the “wrong” way to answer these questions, because there’s some structure we’re not using.

Let’s use generating functions.

\[ f(S; x) = x^0 + x^3 + x^6 + x^7 + x^9 + x^{10} + \cdots \]

As before, this can be rewritten as a nice rational function.

We will later show that

\[ f(S; x) = \frac{1 - x^{a_1a_2}}{(1 - x^{a_1})(1 - x^{a_2})}. \]
Listing out the set is the “wrong” way to answer these questions, because there’s some structure we’re not using.

Let’s use generating functions.

\[ f(S; x) = x^0 + x^3 + x^6 + x^7 + x^9 + x^{10} + \cdots \]

As before, this can be rewritten as a nice rational function.

We will later show that

\[ f(S; x) = \frac{1 - x^{a_1 a_2}}{(1 - x^{a_1})(1 - x^{a_2})}. \]
Listing out the set is the “wrong” way to answer these questions, because there’s some structure we’re not using.

Let’s use generating functions.

\[ f(S; x) = x^0 + x^3 + x^6 + x^7 + x^9 + x^{10} + \cdots \]

As before, this can be rewritten as a nice rational function.

We will later show that

\[ f(S; x) = \frac{1 - x^{a_1 a_2}}{(1 - x^{a_1})(1 - x^{a_2})}. \]
Generating Functions to the Rescue

Let $T = \mathbb{N} \setminus S$ (which is $\{1, 2, 4, 5, 8, 11\}$ in the example).

$$f(T; x) = \frac{1}{1 - x} - f(S; x)$$

$$= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1}a_2)}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.$$

The largest integer not in $S$ is the degree of the polynomial $f(T; x)$, which is

$$(1 + a_1a_2) - (1 + a_1 + a_2) = a_1a_2 - a_1 - a_2.$$

The number of positive integers not in $S$ is $f(T; 1)$, which is (taking the limit as $x \to 1$)

$$\frac{a_1a_2 - a_1 - a_2 + 1}{2}.$$
Generating Functions to the Rescue

Let $T = \mathbb{N} \setminus S$ (which is $\{1, 2, 4, 5, 8, 11\}$ in the example).

\[
f(T; x) = \frac{1}{1 - x} - f(S; x)
= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1 a_2})}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.
\]

The largest integer not in $S$ is the degree of the polynomial $f(T; x)$, which is

\[(1 + a_1 a_2) - (1 + a_1 + a_2) = a_1 a_2 - a_1 - a_2.
\]

The number of positive integers not in $S$ is $f(T; 1)$, which is (taking the limit as $x \to 1$)

\[
\frac{a_1 a_2 - a_1 - a_2 + 1}{2}.
\]
Generating Functions to the Rescue

Let \( T = \mathbb{N} \setminus S \) (which is \( \{1, 2, 4, 5, 8, 11\} \) in the example).

\[
f(T; x) = \frac{1}{1-x} - f(S; x)
= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1}a_2)}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.
\]

The largest integer not in \( S \) is the degree of the polynomial \( f(T; x) \), which is

\[
(1 + a_1 a_2) - (1 + a_1 + a_2) = a_1 a_2 - a_1 - a_2.
\]

The number of positive integers not in \( S \) is \( f(T; 1) \), which is (taking the limit as \( x \to 1 \))

\[
\frac{a_1 a_2 - a_1 - a_2 + 1}{2}.
\]
Generating Functions to the Rescue

Let \( T = \mathbb{N} \setminus S \) (which is \( \{1, 2, 4, 5, 8, 11\} \) in the example).

\[
f(T; x) = \frac{1}{1 - x} - f(S; x) \\
= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1}a_2)}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.
\]

The largest integer not in \( S \) is the degree of the polynomial \( f(T; x) \), which is

\[
(1 + a_1a_2) - (1 + a_1 + a_2) = a_1a_2 - a_1 - a_2.
\]

The number of positive integers not in \( S \) is \( f(T; 1) \), which is (taking the limit as \( x \to 1 \))

\[
\frac{a_1a_2 - a_1 - a_2 + 1}{2}.
\]
Generating Functions to the Rescue

Let $T = \mathbb{N} \setminus S$ (which is $\{1, 2, 4, 5, 8, 11\}$ in the example).

$$f(T; x) = \frac{1}{1 - x} - f(S; x)$$

$$= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1}a_2)}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.$$

The largest integer not in $S$ is the degree of the polynomial $f(T; x)$, which is

$$(1 + a_1 a_2) - (1 + a_1 + a_2) = a_1 a_2 - a_1 - a_2.$$

The number of positive integers not in $S$ is $f(T; 1)$, which is (taking the limit as $x \to 1$)

$$\frac{a_1 a_2 - a_1 - a_2 + 1}{2}.$$
Generating Functions to the Rescue

Let \( T = \mathbb{N} \setminus S \) (which is \( \{1, 2, 4, 5, 8, 11\} \) in the example).

\[
f(T; x) = \frac{1}{1 - x} - f(S; x)
\]

\[
= \frac{(1 - x^{a_1})(1 - x^{a_2}) - (1 - x)(1 - x^{a_1 a_2})}{(1 - x)(1 - x^{a_1})(1 - x^{a_2})}.
\]

The largest integer not in \( S \) is the degree of the polynomial \( f(T; x) \), which is

\[
(1 + a_1 a_2) - (1 + a_1 + a_2) = a_1 a_2 - a_1 - a_2.
\]

The number of positive integers not in \( S \) is \( f(T; 1) \), which is (taking the limit as \( x \to 1 \))

\[
\frac{a_1 a_2 - a_1 - a_2 + 1}{2}.
\]
What else?

Questions:

▷ What types of sets can be encoded as rational generating functions?

▷ What types of sets can be encoded as short rational generating functions, quickly?

If $S \subseteq \mathbb{N}^n$, then let

$$f(S; x) = \sum_{s=(s_1, \ldots, s_n) \in S} x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n}.$$
What else?

**Question:** When can a set be encoded as a rational generating function?

**Answer [W]:** If and only if it can be written like

\[ S = \{ x \in \mathbb{N} \mid \forall y_1 \in \mathbb{N}, \exists y_2 \in \mathbb{N} : (3y_1 + 5y_2 - x \geq 0) \text{ and } (5y_1 + 2y_2 + 3x < 5 \text{ or } 3y_1 - x = 7)\} \]

using quantifiers (\(\exists\) and \(\forall\)), boolean operations (and, or, not), and linear (in)equalities (\(\leq, =, >\)).

These are sentences in the **Presburger arithmetic**.
What else?

Examples:

\[ S = \{ x \in \mathbb{N} \mid \exists y \in \mathbb{N} : 2y = x \text{ and } 100 \leq x \leq 250 \} \].

\[ S = \{ x \in \mathbb{N} \mid \exists \lambda_1 \in \mathbb{N}, \ldots, \exists \lambda_d \in \mathbb{N} : \\
    x = a_1 \lambda_1 + \cdots + a_d \lambda_d \} \].
A Computer Example

\[
\text{for } i=0 \text{ to } 5 \\
\text{ for } j=0 \text{ to } i \\
\quad \text{Do something that requires } i \cdot j \text{ units of storage} \\
\text{end} \\
\text{end}
\]

Want to compute

\[
\sum_{i=0}^{5} \sum_{j=0}^{i} ij.
\]

Let

\[S = \{(i,j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\}.\]

We want

\[
\sum_{(i,j) \in S} ij.
\]
for i=0 to 5
   for j=0 to i
       Do something that requires $i \cdot j$ units of storage
   end
end

Want to compute

$$\sum_{i=0}^{5} \sum_{j=0}^{i} ij.$$ 

Let

$$S = \{(i,j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\}.$$ 

We want

$$\sum_{(i,j) \in S} ij.$$
A Computer Example

Let’s find $f(S; x, y)$

$$= 1 + x + \cdots + x^5 y^5$$
A Computer Example
A Computer Example

\[ x^5 y^2 = (x)^3(xy)^2 \]

\[(1 + x + x^2 + x^3 + \cdots) \cdot (1 + xy + (xy)^2 + \cdots) = \frac{1}{(1 - x)(1 - xy)}\]
A Computer Example

\[(1 + x + x^2 + x^3 + \cdots) \cdot (1 + xy + (xy)^2 + \cdots) = \frac{1}{(1 - x)(1 - xy)}\]
A Computer Example

\[-x^6 \cdot (1 + x + x^2 + \cdots) \cdot (1 + y + y^2 + \cdots) = -\frac{x^6}{(1-x)(1-y)}\]
A Computer Example

\[
\frac{1}{(1-x)(1-xy)} - \frac{x^6}{(1-x)(1-y)}
\]
A Computer Example

\begin{align*}
+ x^6 y^7 \\
\cdot (1 + xy + (xy)^2 + \cdots ) \\
\cdot (1 + y + y^2 + \cdots ) \\
= \frac{x^6 y^7}{(1 - xy)(1 - y)}
\end{align*}
A Computer Example

\[
f(S; x, y) = \frac{1}{(1 - x)(1 - xy)} - \frac{x^6}{(1 - x)(1 - y)} + \frac{x^6y^7}{(1 - xy)(1 - y)}.\]
A Computer Example

We have

\[ f(S; x, y) = \sum_{(i,j) \in S} x^i y^j. \]

We want

\[ \sum_{(i,j) \in S} ij. \]
A Computer Example

We have

\[ f(S; x, y) = \sum_{(i,j) \in S} x^i y^j. \]

We want

\[ \sum_{(i,j) \in S} ij. \]

\[ \frac{\partial^2}{\partial x \partial y} f(S; x, y) = \sum_{(i,j) \in S} ij x^{i-1} y^{j-1}. \]

Therefore we want

\[ \frac{\partial^2}{\partial x \partial y} f(S; x, y) \bigg|_{x=1, y=1} = 140. \]
Summary

- We can often use patterns in seemingly complicated sets to encode them compactly as generating functions.
- We can manipulate the generating functions to answer questions about the sets.
Quick now!

**Question:** When can we find $f(S; x)$ quickly?

We want an algorithm that inputs a Presburger sentence and outputs $f(S; x)$.

The input size is the number of bits needed to encode the input for the algorithm.

The input size of a number $a$ is approximately

$$\log_2(a).$$

An algorithm is polynomial time if there is a polynomial $p$ such that the algorithm runs in at most $p(\text{input size})$ steps.

polynomial time $=$ quick
Question: When can we find $f(S; x)$ quickly?

We want an algorithm that inputs a Presburger sentence and outputs $f(S; x)$.

The input size is the number of bits needed to encode the input for the algorithm.

The input size of a number $a$ is approximately

$$\log_2(a).$$

An algorithm is polynomial time if there is a polynomial $p$ such that the algorithm runs in at most $p($input size$)$ steps.

polynomial time = quick
Quick now!

**Question:** When can we find $f(S; x)$ quickly?

We want an algorithm that inputs a Presburger sentence and outputs $f(S; x)$.

The input size is the number of bits needed to encode the input for the algorithm.

The input size of a number $a$ is approximately

$$\log_2(a).$$

An algorithm is **polynomial time** if there is a polynomial $p$ such that the algorithm runs in at most $p(\text{input size})$ steps.

polynomial time $=$ quick
Good Algorithms

- If there are no quantifiers, there is a polynomial time algorithm (if we fix the number of variables) [Barvinok].

- If only \( \exists \)'s are needed to define \( S \), there is a polynomial time algorithm (if we fix the number of variables and linear inequalities) [W].
No Quantifiers

This is like the previous example:

\[ S = \{(i, j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\}. \]

- Inclusion-Exclusion of cones [Brion]
- Not all cones are “nice” (unimodular):
No Quantifiers

This is like the previous example:

\[ S = \{(i, j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\}. \]

- Inclusion-Exclusion of cones [Brion]
- Not all cones are “nice” (unimodular):

unimodular decomposition [Barvinok]
No Quantifiers

This is like the previous example:

\[ S = \{(i, j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\}. \]

- Inclusion-Exclusion of cones [Brion]
- Not all cones are “nice” (unimodular):

unimodular decomposition [Barvinok]
No Quantifiers

This is like the previous example:

\[ S = \{(i, j) \in \mathbb{N}^2 \mid i \leq 5 \text{ and } j \leq i\} . \]

- Inclusion-Exclusion of cones [Brion]
- Not all cones are “nice” (unimodular):

unimodular decomposition [Barvinok]
Existential Quantifiers

Projections

\[ S = \{ i \in \mathbb{N} \mid \exists j \in \mathbb{N} : (i, j) \in P \} . \]

We need to compute generating functions for projections of \( P \cap \mathbb{Z}^n \), where \( P \) is a polyhedron.

\[ T(i, j) = i, \quad \text{and} \quad S = T(P \cap \mathbb{Z}^2) . \]
Example: Frobenius Problem with \( a_1 = 2 \), \( a_2 = 5 \).

\[
P = \{(i, j) : i, j \geq 0\}
\]

\[
T(i, j) = 2i + 5j. \quad (1\text{-d Kernel})
\]

Then \( S = T(P \cap \mathbb{Z}^2) \).
Compute \( f(P \cap \mathbb{Z}^2; x, y) = \frac{1}{(1-x)(1-y)} \). [Barvinok]

Compute \( f(P \cap \mathbb{Z}^2; t^2, t^5) \). Then \( x^i y^j \mapsto t^{2i+5j} \).
Existential Quantifiers

1-d Kernel

\[
f(P \cap \mathbb{Z}^2; t^2, t^5) = \frac{1}{(1 - t^2)(1 - t^5)} = (1 + t^2 + t^4 + \cdots)(1 + t^5 + \cdots)
= 1 + t^2 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + \cdots.
\]
Existential Quantifiers

1-d Kernel

\[ f(P \cap \mathbb{Z}^2; t^2, t^5) = \frac{1}{(1 - t^2)(1 - t^5)} = (1 + t^2 + t^4 + \cdots)(1 + t^5 + \cdots) \]
\[ = 1 + t^2 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + 2t^{10} + \cdots \]

Problem: \( T \) is not 1-1 on \( P \cap \mathbb{Z}^2 \).
Existential Quantifiers

1-d Kernel

\[ f(P \cap \mathbb{Z}^2; t^2, t^5) = \frac{1}{(1 - t^2)(1 - t^5)} = (1 + t^2 + t^4 + \cdots)(1 + t^5 + \cdots) \]
\[ = 1 + t^2 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + 2t^{10} + \cdots \]

Problem: \( T \) is not 1-1 on \( P \cap \mathbb{Z}^2 \).
Let \( Q = \{(i,j) : i \geq 5, j \geq 0\} \).

\[
f(Q \cap \mathbb{Z}^2; x, y) = \frac{x^5}{(1-x)(1-y)}.
\]

\[
f(Q \cap \mathbb{Z}^2; t^2, t^5) = \frac{t^{10}}{(1-t^2)(1-t^5)}.
\]
Existential Quantifiers

$T$ is $1$-$1$ on $(P - Q) \cap \mathbb{Z}^2$.

$$f(S; t) = f(P \cap \mathbb{Z}^2; t^2, t^5) - f(Q \cap \mathbb{Z}^2; t^2, t^5) = \frac{1 - t^{10}}{(1 - t^2)(1 - t^5)}.$$
$T$ is 1-1 on $(P - Q) \cap \mathbb{Z}^2$.

$$f(S; t) = f(P \cap \mathbb{Z}^2; t^2, t^5) - f(Q \cap \mathbb{Z}^2; t^2, t^5) = \frac{1 - t^{10}}{(1 - t^2)(1 - t^5)}.$$
Existential Quantifiers

Why This Works: There are no gaps in the fibers of $T$.

Only works for 1-d kernel.
General situation: Use induction on the dimension of the kernel.

Must control the gaps.
Existential Quantifiers

A Tool:

Flatness Theorem (Khinchin): Convex objects that contain no integer points are thin in some direction.
Looking at a fiber of the desired projection, suppose we project onto the thinnest direction.

If there are large gaps,
Looking at a fiber of the desired projection, suppose we project onto the thinnest direction.

If there are large gaps,
Then there is a lattice-free polytope that is wide.
Contradiction.
Look at a fiber of $T(P)$, and pick the **thinnest** direction. That direction gets projected out last (inductively).
Existential Quantifiers

Higher-d Kernel

Complication: Different fibers have different thin directions.
Solution: Break things up into pieces [Kannan].
Applications

- Frobenius problem [Barvinok-W]
- Minimal Hilbert Bases [Barvinok-W]
- Hilbert series of rings generated by monomials [Barvinok-W]
- Test sets for integer programming [Barvinok-W]
- Integer programming gaps [Hoşten-Sturmfels]
- Reduced Gröbner bases for toric ideals, and some related computations [De Loera, et al.]
- Standard pairs and arithmetic degree of order ideals in integer programming [Thomas-W]
- Ehrhart quasi-polynomials (and their period) [W]
Summary

- We can often use hidden **structure** in seemingly complicated sets to encode them compactly as generating functions.
- We can **manipulate** the generating functions to answer questions about the sets.
Summary

- We can often use hidden structure in seemingly complicated sets to encode them compactly as generating functions.
- We can manipulate the generating functions to answer questions about the sets.
- We can do many of these things quickly.
Thank You!

T(x,y,z) = x
The Good, the Bad, and the ____

Presburger sentences from an algorithmic perspective:
  ▶ General sentences.
The Good, the Bad, and the _____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad
The Good, the Bad, and the ____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad

- Fix number of variables, no quantifiers.
The Good, the Bad, and the ____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad

- Fix number of variables, no quantifiers.
  - Good [Barvinok]
Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad
- Fix number of variables, no quantifiers.
  - Good [Barvinok]
- Fix number of variables, quantifiers allowed.
The Good, the Bad, and the ____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - **Bad**
- Fix number of variables, no quantifiers.
  - **Good** [Barvinok]
- Fix number of variables, quantifiers allowed.
  - **Bad**, even with a single quantifier [W; Schöning]
Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad

- Fix number of variables, no quantifiers.
  - Good [Barvinok]

- Fix number of variables, quantifiers allowed.
  - Bad, even with a single quantifier [W; Schöning]

- Fix number of variables and inequalities, only $\exists$ quantifiers.
The Good, the Bad, and the ____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad

- Fix number of variables, no quantifiers.
  - Good [Barvinok]

- Fix number of variables, quantifiers allowed.
  - Bad, even with a single quantifier [W; Schöning]

- Fix number of variables and inequalities, only $\exists$ quantifiers.
  - Good [W]
The Good, the Bad, and the _____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad

- Fix number of variables, no quantifiers.
  - Good [Barvinok]

- Fix number of variables, quantifiers allowed.
  - Bad, even with a single quantifier [W; Schöning]

- Fix number of variables and inequalities, only $\exists$ quantifiers.
  - Good [W]

- Fix number of variables and inequalities, mixed quantifiers.
The Good, the Bad, and the _____

Presburger sentences from an algorithmic perspective:

- General sentences.
  - Bad
- Fix number of variables, no quantifiers.
  - Good [Barvinok]
- Fix number of variables, quantifiers allowed.
  - Bad, even with a single quantifier [W; Schöning]
- Fix number of variables and inequalities, only $\exists$ quantifiers.
  - Good [W]
- Fix number of variables and inequalities, mixed quantifiers.
  - ?????
Thank You!

\[ T(x, y, z) = x \]