Short Rational Functions for Toric Algebra and Applications

Ruriko Yoshida
Dept. of Mathematics Duke University

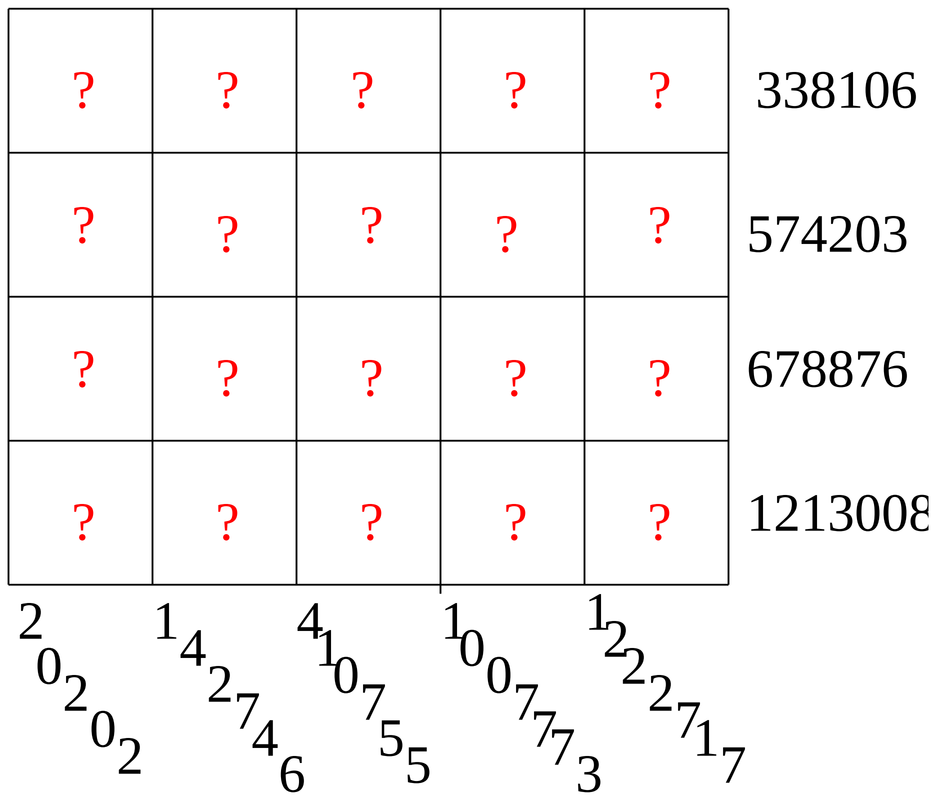
Joint work with De Loera, Haws, Hemmecke, Huggins and Sturmfels

`www.math.duke.edu/~ruriko`

September 8th, 2004

Getting started...

HOW MANY WAYS are there?



Let $P = \{x \in \Re^d | Ax = b,\ x \geq 0\}$, where $A \in \mathbb{Z}^{m \times d}$ and $b \in \mathbb{Z}^m$.

Problem: Find the multivariate generating function

$$f(P, z) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^{\alpha},$$

where $z^{\alpha} = z_1^{\alpha_1} z_2^{\alpha_2} \dots z_d^{\alpha_d}$.

This is an infinite formal power series if P is not bounded, but if P is a polytope it is a polynomial.

Why we care

We can apply $f(P, z)$ to the followings:

(A) Counting Problem,

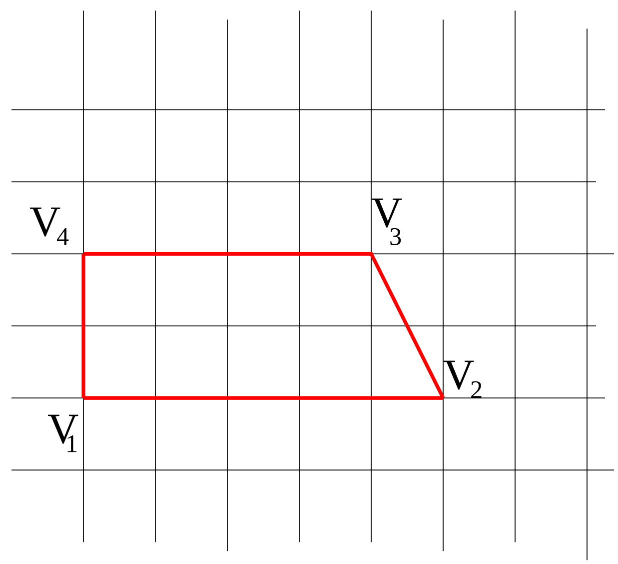
(B) Integer Programming,

(C) Integer Feasibility Problem,

(D) Computing the reduced Gröbner basis of a given integral matrix A.

Example for $f(P, z)$

Let $V_1 = (0, 0)$, $V_2 = (5, 0)$, $V_3 = (4, 2)$, and $V_4 = (0, 2)$.



Each vertex is represented by the following monomials:

For $V_1 = (0, 0)$, $z^{V_1} = z_1^0 z_2^0 = 1$.

For $V_2 = (5, 0)$, $z^{V_2} = z_1^5 z_2^0 = z_1^5$.

For $V_3 = (4, 2)$, $z^{V_3} = z_1^4 z_2^2$.

For $V_4 = (0, 2)$, $z^{V_4} = z_1^0 z_2^2 = z_2^2$.

In this manner, we have $f(P, z)$ as the following:

$$f(P, z) = {z_1}^5 + {z_1}^4 z_2 + {z_1}^4 + {z_1}^4 {z_2}^2 + z_2 {z_1}^3 + {z_1}^3 + {z_1}^3 {z_2}^2 + z_2 {z_1}^2 + {z_1}^2 + {z_1}^2 {z_2}^2 + z_1 z_2 + z_1 + z_1 {z_2}^2 + {z_2}^2 + z_2 + 1.$$

If we send $z_1 \to 1$ and $z_2 \to 1$, then we have $f(P, (1, 1)) =$ the number of lattice points in P.

However...

The multivariate generating function $f(P, z)$ has exponentially many monomials even though we fixed the dimension.

Question: How can we encode $f(P, z)$ in polynomial size if we fix the dimension??

Answer: We can encode $f(P, z)$ as a short sum of rational functions.

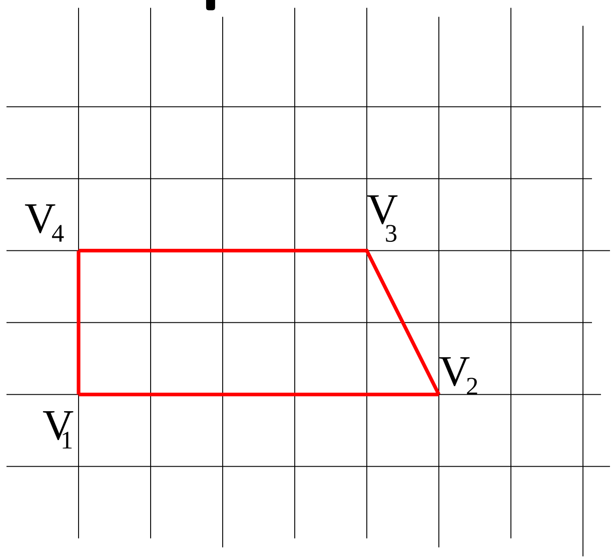
Theorem: [Barvinok (1993)]

Assume that we fix the dimension d and suppose we have a rational convex polyhedron $P = \{ u \in \mathbb{R}^d \; : \; A \cdot u = b \text{ and } u \geq 0 \}$, where $A \in \mathbb{Z}^{m \times d}$ and $b \in \mathbb{Z}^m$. Then there exists a polynomial time algorithm to compute $f(P, z)$ in the form of:

$$f(P, z) \quad = \quad \sum_{i \in I} \pm \frac{x^{u_i}}{(1 - x^{c_{1,i}})(1 - x^{c_{2,i}}) \ldots (1 - x^{c_{m-d,i}})}$$

where u_i, $c_{1,i}$, $\ldots$ $c_{m-d,i} \in \mathbb{Z}^d$ for all $i \in I$.

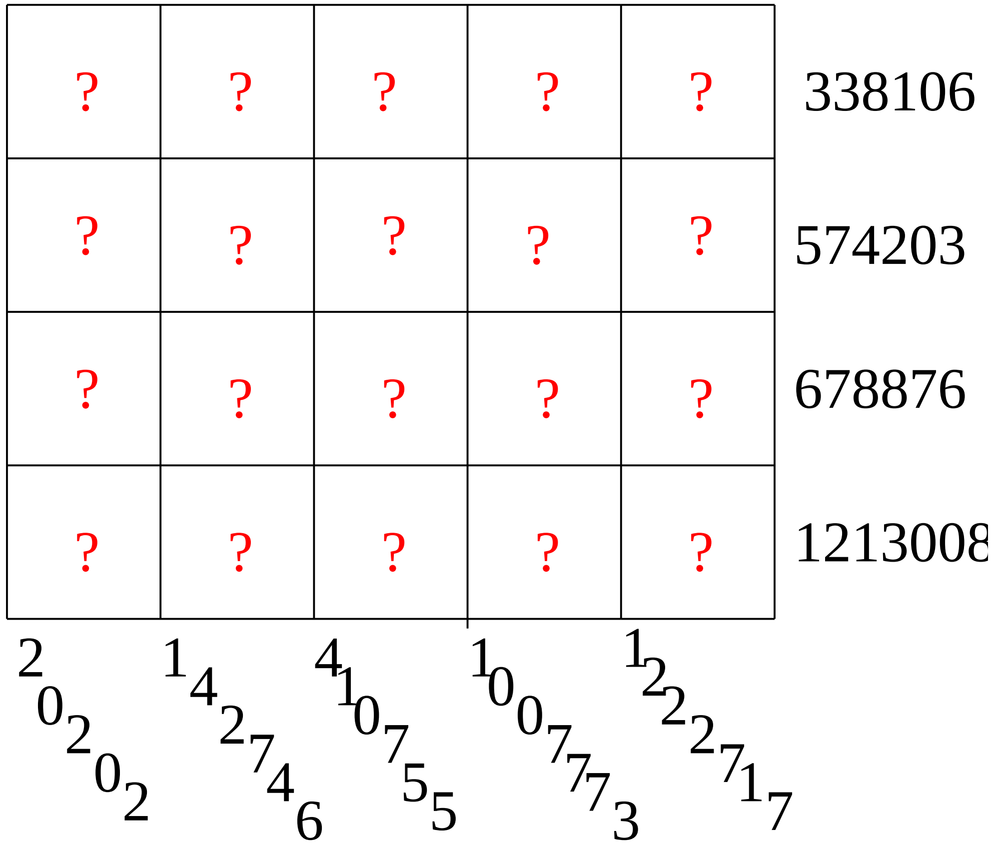
From the previous example



$$f(P,z) = {z_1}^5 + {z_1}^4 z_2 + {z_1}^4 + {z_1}^4 {z_2}^2 + z_2 {z_1}^3 + {z_1}^3 + {z_1}^3 {z_2}^2 + z_2 {z_1}^2 + {z_1}^2 + {z_1}^2 {z_2}^2 + z_1 z_2 + z_1 + z_1 {z_2}^2 + {z_2}^2 + z_2 + 1$$

$$= \frac{1}{(1-z_1)(1-z_2)} + \frac{{z_1}^5}{(1-{z_1}^{-1})(1-z_2)} + \frac{z_1^2}{(1-z_1)(1-z_2^{-1})} + \frac{z_1^5}{(1-z_1^{-1}z_2)(1-z_2^{-1})} + \frac{{z_1}^4 {z_2}^2}{(1-{z_2}^{-1})(1-z_1)} - \frac{z_1^4 z_2^2}{(1-z_1^{-1}{z_2}^2)(1-z_1^{-1})}.$$

Answer of puzzle



$316052820930116909459822049052149787748004963058022997262397.$

Computing Gröbner bases via Barvinok's Rational Functions

Some Definitions

Definition Let $\prec$ be a total order on $\mathbb{Z}_+^d$. We call $\prec$ a *term order* if it satisfies the following:

- For any α, β, $\delta \in \mathbb{Z}_+^d$, $\alpha \prec \beta \rightarrow \alpha + \delta \prec \beta + \delta$.
- For any $\alpha \in \mathbb{Z}_+^d \backslash \{0\}$, $0 \prec \alpha$.

Definition Fix a subset $A = \{a_1, a_2, \ldots, a_d\}$ of $\mathbb{Z}^n$. Each vector a_i is identified with a monomial in the Laurent polynomial ring $K[\pm t] := K[t, t^2, \ldots, t^d, t^{-1}, t^{-2}, \ldots, t^{-d}]$. Consider the homomorphism induced by the monomial map

$$\hat{\pi} : K[x] \rightarrow K[\pm t],\ x_i \rightarrow t^{a_i}.$$

Then the kernel of the homomorphism $\hat{\pi}$ is called the *toric ideal* I_A of A.

Example

Let $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$.

Then the toric ideal of A is:

$$I_A = \{x^z : z \in \ker(A) \cap \mathbb{Z}^3\},$$

where $\ker(A) = \{z \in \mathbb{R}^3 : z = \lambda \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix},\ \lambda \in \mathbb{R}\}$.

What is a Gröbner basis??

Let K be any field and let $K[x] = K[x_1, x_2, \ldots, x_d]$ be the polynomial ring in d indeterminates. Given a term order $\prec$, let $in_{\prec}(f)$ $f \in K[x]$ be an intial monomial of f. If I is an ideal in $K[x]$, then its *initial ideal* is the monomial ideal

$$in_{\prec}(I) :=< in_{\prec}(f) : f \in I > .$$

A finite subset $G \subset I$ is called a *Gröbner basis* for I with respect to $\prec$ if $in_{\prec}(I)$ is generated by $\{in_{\prec}(g) : g \in G\}$.

A Gröbner basis is called *reduced* if for any two distinct elements $g, \bar{g} \in G$, no terms of $\bar{g}$ is divisible by $in_{\prec}(g)$.

Example

Let $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$.

The reduced Gröbner basis accosiated to the matrix A is:

$G := \{x^{g_1},\, x^{g_2}, x^{g_3}\}$,

where $g_1 = (-1, 2, -1, 0)$, $g_2 = (1, -1, -1, 1)$, and $g_3 = (0, -1, 2, -1)$.

Let $G := \{g_1, g_2, \ldots, g_k\}$ be a Gröbner basis for an ideal $I \subset K[x]$ and let $f \in K[x]$. Then there exists a unique $r \in K[x]$ such that:

- No term of r is divisible by any of leading term of g_i, for all $i = 1, 2, \ldots, k$.
- There is $g \in I$ such that $f = g + r$.

r is the remainder on division of f by G and The remainder r for $f \in K[x]$ is called the *normal form* of f.

Want. We want to compute the reduced Gröbner basis associated to the matrix A efficiently.

Problem. There are exponencially many elements in the reduced Gröbner basis even though we fix the dimension.

Solution. Use a short sum of rational functions!

Theorem [De Loera, Haws, Hemmecke, Huggins, Sturmfels, Y.]

Let $A \in \mathbb{Z}^{m \times d}$, $b \in \mathbb{Z}^m$, $W \in \mathbb{Z}^{d \times d}$, where d and m are fixed.

Suppose the term order $\prec_W$ is given. Then there is a polynomial time algorithm to compute the multivariate generating function $G(z)$ for the reduced Gröbner basis of the toric ideal associated to A with the term order $\prec_W$ as a short sum of rational functions.

Why we care?

There are many useful applications.

- Integer Programming
- Counting the number of tables via the Gröbner basis (different from the method I have shown)
- Estimating the number of tables.

Integer Programming

Suppose $A \in Z^{n \times d}$, $c \in Z^d$, and $b \in Z^n$. We assume that the rank of A is n. Given a polyhedron $P = \{x \in \mathbb{R}^d : Ax = b,\, x \geq 0\}$, we want to solve the following problem:

$$\text{(IP) minimize } c \cdot x \text{ subject to } \quad x \in P, \;\; x \in \mathbb{Z}^d.$$

These problems are called *integer programming problems* and we know that this problem is NP-hard by Karp. However, Lenstra showed that if we fixed the dimension, we can solve (IP) in polynomial time.

IP via Gröbner bases

Algorithm [Sturmfels]

Input: A cost vector $c \in \mathbb{Z}^d$, a matrix $A \in \mathbb{Z}^{n \times d}$, a vector $b \in \mathbb{Z}^n$ and a feasible solution $v_0 \in P \cap \mathbb{Z}^d$, where $P := \{x \in \mathbb{R}^d : Ax = b,\ x \geq 0\}$.

Output: An optimal solution and the optimal value of minimize $c \cdot x$ subject to $x \in P \cap \mathbb{Z}^d$.

Step 1: Compute the Gröbner basis with the term order $\prec_c$.

Step 2: Compute the normal form x^u of x^{v_0} and return u and cu, which are an optimal solution and the optimal value, respectively.

Example

Let $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 9 \\ 11 \end{pmatrix}$, and $c = \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix}$.

Let $v_0 = \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$. Then:

$G = \{x^v : v = \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}\}$ and $u = \begin{pmatrix} 0 \\ 7 \\ 2 \end{pmatrix}$.

Main Theorem

Let $A \in \mathbb{Z}^{m \times d}$. Assuming that m, d are fixed, there is a polynomial time algorithm to compute a short rational function $G(z)$ which represents the reduced Gröbner basis of the toric ideal I_A w.r.t. any given term order $\prec$. Given G and any monomial x^a, the following tasks can be performed in polynomial time:

1. Decide whether x^a is in normal form with respect to $G(z)$.
2. Compute the normal form of x^a modulo the Gröbner basis $G(z)$.
3. Let $b \in \mathbb{Z}^m$ and $c \in \mathbb{Z}^d$. Given a polyhedron $P = \{x | Ax = b, \, x \geq 0\}$, compute the integer programming problem:

$$\text{minimize } cx \text{ subject to } x \in P, \; x_i \in \mathbb{Z} \text{ for } i \in [d].$$

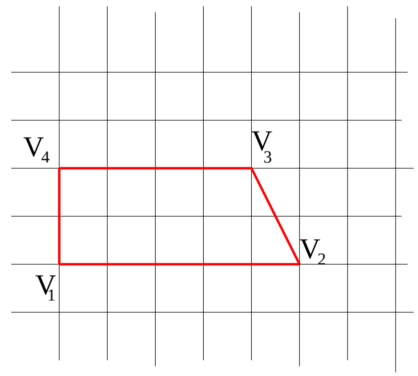
Theory behind it...

Projection Theorem

Theorem [Barvinok and Woods]

Assume the dimension d is a fixed constant. Consider a rational polytope $P \subset \mathbb{R}^d$ and a linear map $T : \mathbb{Z}^d \to \mathbb{Z}^k$. There is a polynomial time algorithm which computes the generating function $f\big(T(P \cap \mathbb{Z}^d), z\big)$ as a short sum of rational functions.

Example



$$f(P,z)=\frac{1}{(1-z_1)(1-z_2)}+\frac{{z_1}^5}{(1-{z_1}^{-1})(1-z_2)}+\frac{z_1^2}{(1-z_1)(1-z_2^{-1})}+\frac{z_1^5}{(1-z_1^{-1}z_2)(1-z_2^{-1})}+\frac{{z_1}^4{z_2}^2}{(1-{z_2}^{-1})(1-z_1)}-\frac{z_1^4z_2^2}{(1-z_1^{-1}{z_2}^2)(1-z_1^{-1})}.$$

Let T be a projection from $T:\mathbb{R}^2\to\mathbb{R}$ such that $T(x,y)=x$.

Then we have:

$$f(T(P\cap\mathbb{Z}^2),z)=\frac{1}{(1-z_1)}+\frac{z_1^5}{(1-z_1^{-1})}=1+z_1+z_1^2+z_1^3+z_1^4+z_1^5.$$

Theorem [Barvinok and Woods]

Let S_1 and S_2 be finite subsets of $\mathbb{Z}^d$. Suppose that $f(S_1, z)$ and $f(S_2, z)$ are given as short rational functions. If we fix the dimension then there exists a polynomial time algorithm to compute $f(S_1 \cap S_2, z)$.

Corollary [Barvinok and Woods]

Suppose that $f(S_1, z)$ and $f(S_2, z)$ are given as short rational functions. If we fix the dimension then there exist polynomial time algorithms to compute $f(S_1 \cup S_2, z)$ and $f(S_1 \backslash S_2, z)$.

Definition: Let g_1 and g_2 be Laurent power series in $z \in \mathbb{C}^d$ such that $g_1(z) = \sum_{\alpha \in \mathbb{Z}^d} a_\alpha z^\alpha$ and $g_2(z) = \sum_{\alpha \in \mathbb{Z}^d} b_\alpha z^\alpha$. Then the Hadamard product $g = g_1 * g_2$ is the power series such that:

$$g(z) = \sum_{\alpha \in \mathbb{Z}^d} a_\alpha b_\alpha z^\alpha.$$

Using the Hadamard product, we can obtain $f(S_1 \cap S_2, z)$ with the given $f(S_1, z)$ and $f(S_2, z)$, where S_1 and S_2 are finite subsets of $\mathbb{Z}^d$.

Example

Let $S_1 = \{x \in \mathbb{R} : -1 \leq x \leq 1\} \cap \mathbb{Z}$ and $S_2 = \{x \in \mathbb{R} : 0 \leq x \leq 2\} \cap \mathbb{Z}$.

$$f(S_1, z) = \frac{z^{-1}}{(1-z)} + \frac{z}{(1-z^{-1})} = \frac{-z^{-2}}{(1-z^{-1})} + \frac{z}{(1-z^{-1})} = g_{11} + g_{12},$$

$$f(S_2, z) = \frac{1}{(1-z)} + \frac{z^2}{(1-z^{-1})} = \frac{-z^{-1}}{(1-z^{-1})} + \frac{z^2}{(1-z^{-1})} = g_{21} + g_{22}.$$

$$f(S_1, z) * f(S_2, z) = g_{11} * g_{21} + g_{12} * g_{22} + g_{12} * g_{21} + g_{11} * g_{22}$$

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

$$= \frac{z-z^{-1}}{1-z^{-1}} = 1 + z = f(S_1 \cap S_2, z).$$

Software for Lattice point Enumeration

Source codes are available and you can download from our website:

`http://www.math.ucdavis.edu/~latte`.

If you want to try your examples, please send your example to

latte@math.ucdavis.edu.

Question??

Thanks you...