Applications of Short Rational Functions to Solving Integer Programming Problems

Ruriko Yoshida
Dept. of Mathematics Duke University

Joint work with J. De Loera, D. Haws, R. Hemmecke, and P. Huggins

www.math.duke.edu/~ruriko

Jan 25th, 2006

Getting started...

HOW MANY WAYS are there?

?	?	?	?	?	338106
?	?	?	?	?	574203
?	?	?	?	?	678876
?	?	?	?	?	1213008
20202	142746	410755	1007773	1222717	

One more puzzle....

What is the optimal value and an optimal solution for the following problem?

Maximize

$$213x_1 - 1928x_2 - 11111x_3 - 2345x_4 + 9123x_5 - 12834x_6 - 123x_7 + 122331x_8$$

subject to

$$11948x_1 + 23330x_2 + 30635x_3 + 44197x_4 + 92754x_5 + 123389x_6 + 136951x_7 + 140745x_8 = 14215207,$$

$x_i \in \mathbb{Z}_+$ for $i = 1, 2, \ldots, 8$.

Note: Branch-and-bound method (`CPLEX` v.6.6) failed to solve this problem.

How to solve

Let $P = \{x \in \mathbb{R}^d | Ax = a,\ Bx \leq b\}$, where A, B are integral matrices and a, b are integral vectors.

Tool: The multivariate generating function

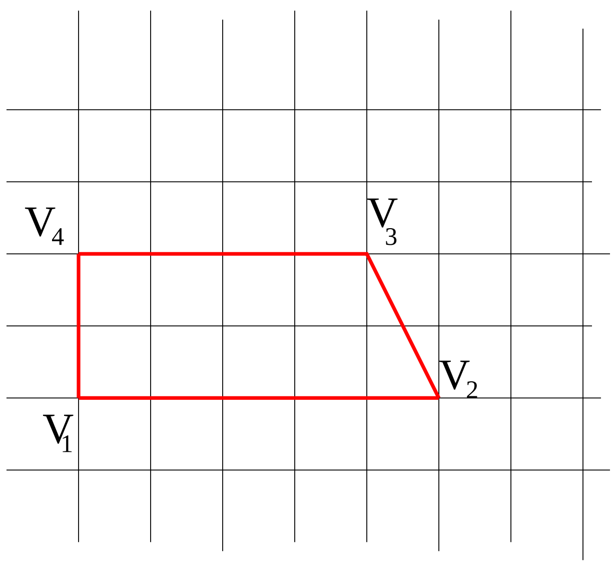
$$f(P, z) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^{\alpha},$$

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.

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:

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

However...

The multivariate generating function $f(P, z)$ has exponentially many monomials even in 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.

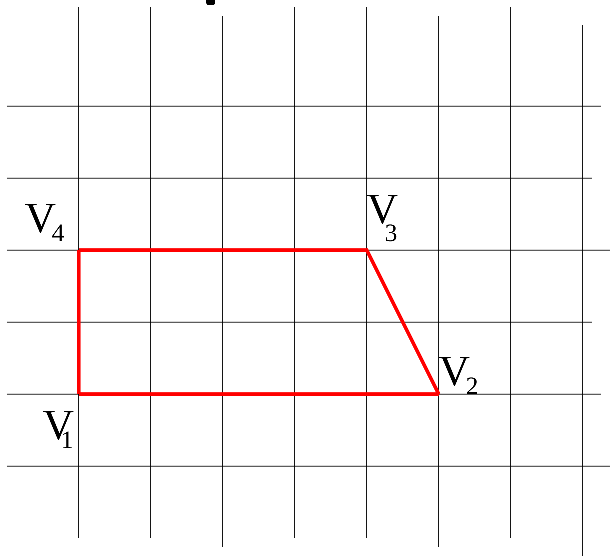
Theorem: [Barvinok (1993)]

Assume that we fix the dimension d and suppose we have a rational convex polyhedron $P = \{ u \in \mathbb{R}^d : Au \leq b \}$, 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 following form of:

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

where u_i, v_{1i}, $\ldots$ $v_{di} \in \mathbb{Z}^d$ for all $i \in I$.

From the previous example



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

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

LattE

- **INPUT**: Integral matrices A, B and integral vectors a, b for the polytope P.

- **OUTPUT**: $f(P, z)$ written as a short sum of rational functions.

- **APPLICATIONS**:

  (A) Counting Problem,

  (B) Integer Programming,

  (C) Integer Feasibility Problem,

  (D) Computing a universal test set of a given integral matrix A.

Answer to the puzzle

?	?	?	?	?	338106
?	?	?	?	?	574203
?	?	?	?	?	678876
?	?	?	?	?	1213008
20202	142746	410755	1007773	1222717	

3160528209301169094598220490521497877480049630580229972623997.

Answer to the puzzle

Maximize

$$213x_1 - 1928x_2 - 11111x_3 - 2345x_4 + 9123x_5 - 12834x_6 - 123x_7 + 122331x_8$$

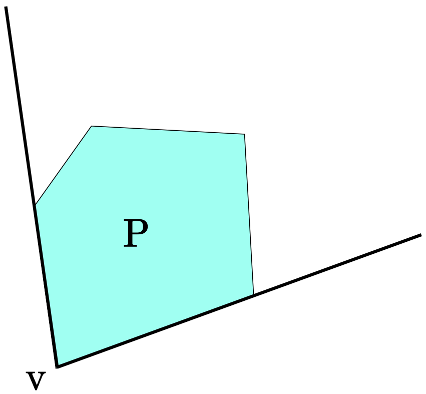
subject to

$$11948x_1 + 23330x_2 + 30635x_3 + 44197x_4 + 92754x_5 + 123389x_6 + 136951x_7 + 140745x_8 = 14,215,207,$$

$x_i \in \mathbb{Z}_+$ for $i = 1, 2, \ldots, 8$.

The optimal value is 3471390.
An optimal solution is $(853,\ 2,\ 0,\ 4,\ 0,\ 0,\ 0,\ 27)$.
The number of feasible integer points is 2047107.
CPU Time: about 12 sec.

Theory behind the implementation



Theorem[Brion, Lawrence]

Let P be a convex polyhedron and let $V(P)$ be the vertex set of P. Let K_v be the tangent cone at $v \in V(P)$. Then

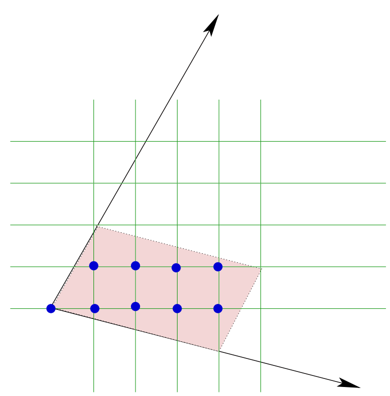
$$f(P, z) = \sum_{v \in V(P)} f(K_v, z).$$

If we have a simple cone...

For a simple cone $K \subset \mathbb{R}^d$,

$$f(K, z) = \frac{\sum_{u \in \Pi \cap \mathbb{Z}^d} z^u}{(1 - z^{c_1})(1 - z^{c_2}) \ldots (1 - z^{c_d})}$$

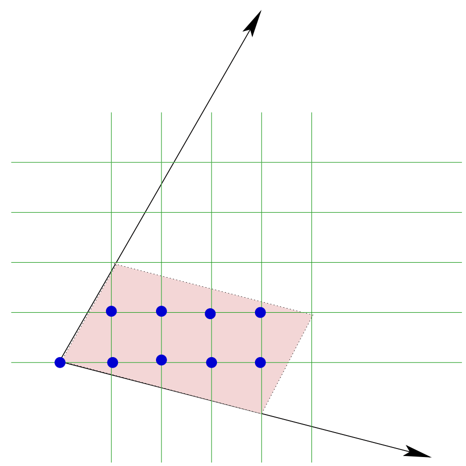
where Π is the half open parallelepiped spanned by the rays of the cone K, $c_1, \ldots, c_d \in \mathbb{Z}^d$.



Example

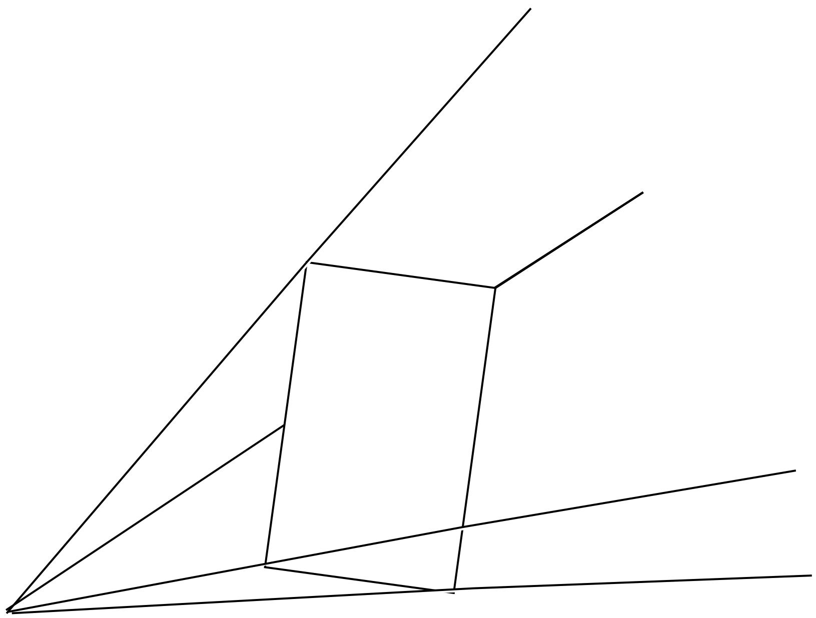
In this case, we have $d = 2$ and $c_1 = (1, 2)$, $c_2 = (4, -1)$. We have:

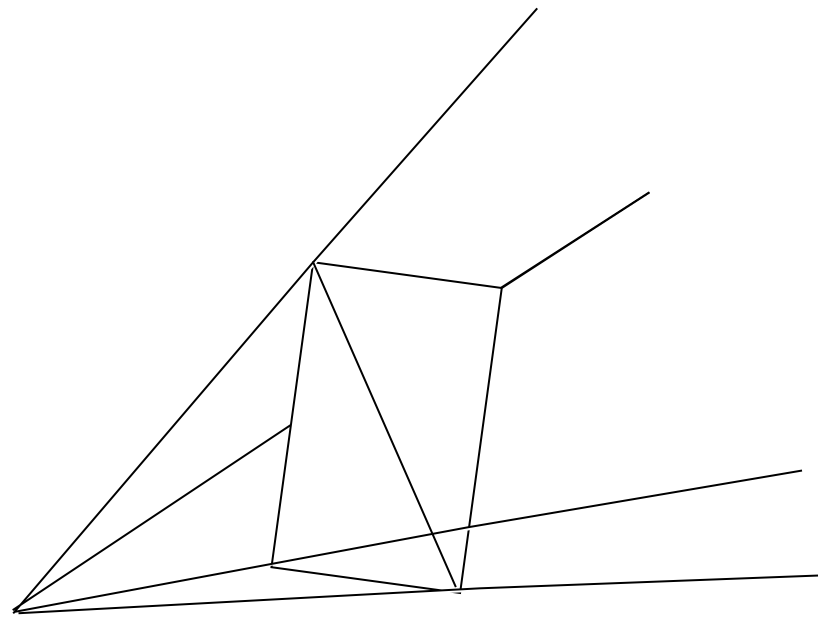
$$f(K, z) = \frac{z_1^4 z_2 + z_1^3 z_2 + z_1^2 z_2 + z_1 z_2 + z_1^4 + z_1^3 + z_1^2 + z_1 + 1}{(1 - z_1 z_2^2)(1 - z_1^4 z_2^{-1})}.$$



If a cone K is not simple....

We triangulate the cone into simple cones.





Fact: If the parallelepiped Π for a simple cone K has only one integral point u, then

$$f(K,z) = \frac{z^u}{\prod_{i=1}^{d}(1 - z^{c_i})}.$$

Goal: Want to decompose K into simple cones whose parallelepipeds Π have ONLY one integral point.

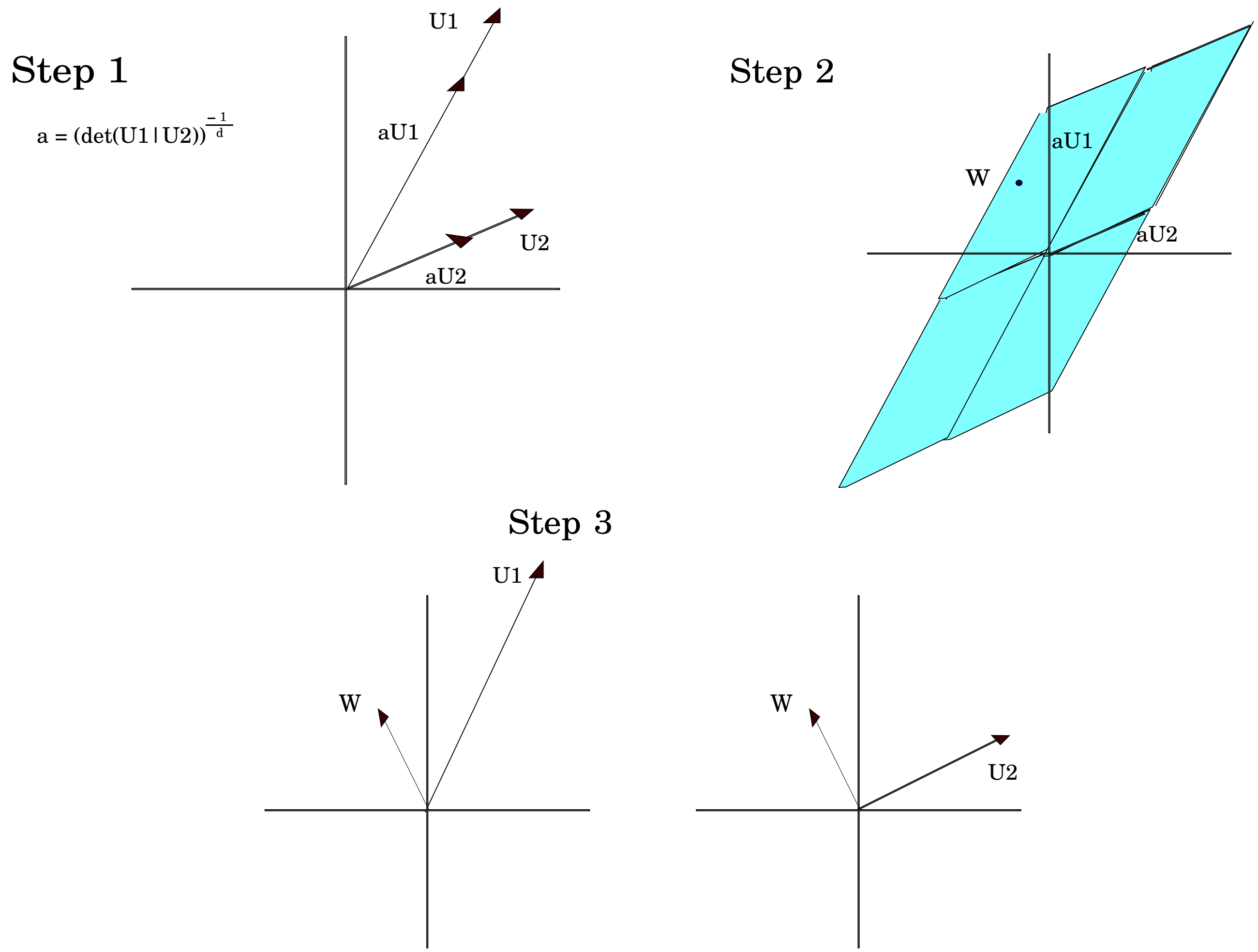
Definition: A *unimodular cone* K is a simple cone such that the half open parallelepiped generated by the rays of K contains only one lattice point

Barvinok's cone decomposition

Theorem [Barvinok] Fix the dimension d. Then there exists a polynomial time algorithm which decomposes a rational polyhedral cone $K \subset \mathbb{R}^d$ into unimodular cones K_i with numbers $\epsilon_i \in \{-1, 1\}$ such that

$$f(K, z) = \sum_{i \in I} \epsilon_i f(K_i, z), \quad |I| < \infty.$$

We do this process until all cones become unimodular.



We have so far...

1. Find the vertices of the given polytope and their defining tangent cones.

2. Triangulate and apply Barvinok's cone decomposition to each of the cones.

3. Obtain the signed rational function of each cone and sum them up.

We need to include lower dimensional cones and also apply the inclusion-exclusion principle, to get the multivariate generating function $f(P, z)$.

Brion's polarization trick

Lemma: Let $K \subset \mathbb{R}^d$ be a cone. If K contains a straight line then $f(K, z) \equiv 0$.

By this lemma we can avoid using the inclusion-and-exclusion principle and save time and memory. The trick is the following:

1. Polarize the tangent cone.

2. Decompose the polar into unimodular cones.

3. Polarize back each of the unimodular cones.

If we do this process, the multivariate function $f(K, z)$ for each lower dimensional cone K becomes zero.

Example

$d = 2$ and $K = \text{cone}\{(1,\, 0),\ (1,\, k)\}$ for some large $k \in \mathbb{Z}$.

The dual cone $K^* = \text{cone}\{(-k,\, 1),\ (0,\, -1)\}$.

Applying Barvinok's cone decomposition, we have

$$f(K^*, z) = f(K_1^*, z) + f(K_2^*, z) + f(K_3^*, z),$$

where $K_1^* = \text{cone}\{(-k,\, 1),\ (-1,\, 0)\}$, $K_2^* = \text{cone}\{(0,\, -1),\ (-1,\, 0)\}$, and $K_3^* = \text{cone}\{(-1,\, 0)\}$.

Applying Brion's trick, we have

$$f(K, z) = f(K_1, z) + f(K_2, z),$$

where $K_1 = \text{cone}\{(0,\, -1), (1,\, k)\}$ and $K_2 = \text{cone}\{(0,\, 1), (1,\, 0)\}$.

Outline of the implementation

1. Find the vertices of the given polytope and their defining tangent cones.
2. Compute the polar cone to each of the cones.
3. Triangulate and apply Barvinok's cone decomposition to each of the polar cones.
4. Polarize back each of the full dimensional unimodular cones.
5. Obtain the signed rational function of each cone and sum them up.

Integer Programming

via Short Rational Functions

Integer programming

Problem: Given $A \in \mathbb{Z}^{m \times d}$, $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^d$,

$$\max\ c \cdot x \ \text{ subject to } Ax \leq b,\ x \in \mathbb{Z}^d.$$

There are several algorithms to solve the integer programming problem using short rational functions, such as:

1. Barvinok's binary search (BBS) algorithm

2. The digging algorithm

3. The test-set (Gröbner bases, Graver bases, etc) algorithm

Barvinok's binary search (BBS) algorithm and the digging algorithm are implemented in `LattE`.

Digging algorithm

Problem: Find the optimal value $M \in \mathbb{Z}$ and an optimal solution $x^* \in Z^d$ for $\max\{c \cdot x : x \in P \cap \mathbb{Z}^d\}$, where P is a rational convex polyhedron.

If we make the substitutions $\Phi : \mathbb{C}^d \to \mathbb{C}$ such that $\Phi(z_i) = t^{c_i}$, then we will have that $\Phi(z^\alpha) = t^{c \cdot \alpha}$,

and we will thereby obtain

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

$$= kt^M + \text{(lower degree terms)}.$$

Note: With the substitutions $z_i \to y_i t^{c_i}$ instead, we can obtain an optimal solution as well.

Suppose we have a sum of short rational functions for P:

$$f(P,z) \quad = \quad \sum_{i \in I} \pm \frac{z^{u_i}}{(1-z^{v_{1i}})(1-z^{v_{2i}})\dots(1-z^{v_{di}})}.$$

With the monomial substitutions $z_i \to y_i t^{c_i}$, we get:

$$g(P;y,t) = \sum_{i \in I} \pm \frac{y^{u_i} t^{c \cdot u_i}}{\prod_{j=1}^{d}(1-y^{v_{ij}} t^{c \cdot v_{ij}})}.$$

We can assume that $c \cdot v_{ij} < 0$. If $c \cdot v_{ij} > 0$, then we use the following identity:

$$\frac{y^v}{(1-y^u)} = -\frac{y^{v-u}}{(1-y^{-u})}.$$

We send t to ∞ in the rational function

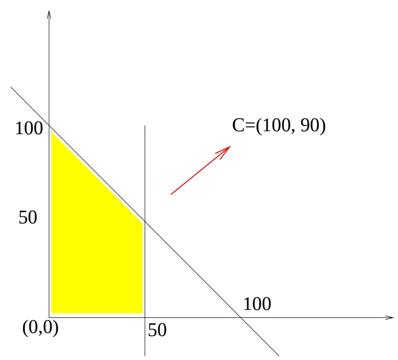
$$g(P; y, t) = \sum_{i \in I} \pm \frac{y^{u_i} t^{c \cdot u_i}}{\prod_{j=1}^{d} (1 - y^{v_{ij}} t^{c \cdot v_{ij}})}.$$

and we obtain the following power series:

$$k y^{x^*} t^{M} + \text{(terms whose degree in } t \text{ is } < M).$$

Example

maximize $100x + 90y$ subject to $x + y \leq 100,\ x \leq 50,\ x, y \geq 0,\ \ x, y \in \mathbb{Z}^d$.



The rational generating function is:

$$\frac{1}{(1-x_1)(1-x_2)} + \frac{x_1^{50}}{(1-x_1^{-1})(1-x_2)} + \frac{x_2^{100}}{(1-x_2^{-1})(1-x_1x_2^{-1})} + \frac{x_1^{50}x_2^{50}}{(1-x_2^{-1})(1-x_1^{-1}x_2)}.$$

Example cont.

We apply the monomial substitution and apply the appropriate algebraic identities and we get:

$$\frac{t^{-190}}{(1-t^{-100})(1-t^{-90})} - \frac{t^{4910}}{(1-t^{-100})(1-t^{-90})} - \frac{t^{8990}}{(1-t^{-90})(1-t^{-10})} + \frac{t^{9500}}{(1-t^{-90})(1-t^{-10})}.$$

Sending t to ∞, then this rational function approaches the power series

$$t^{9500} + \text{(lower degree terms)}.$$

Therefore, the optimal value for this problem is 9500.

IP via Gröbner basis

First we define a term order from a vector c as follows:
For all α, $\beta \in \mathbb{Z}^d_+$, $\alpha \prec_c \beta$ if

- $c \cdot \alpha < c \cdot \beta$ or
- $c\alpha = c\beta$ and $\alpha \prec_{lex} \beta$.

For example, suppose $c = (1, 0, 2)$ and if we have $(3, 2, 7)$ and $(3, 5, 2)$ in $\mathbb{R}^3$, then we have $(1, 0, 2) \cdot (3, 2, 7) = 17$ and $(1, 0, 2) \cdot (3, 5, 2) = 13$. So, since $(1, 0, 2) \cdot (3, 5, 2) < (1, 0, 2) \cdot (3, 2, 7)$, we have $(3, 5, 2) \prec_c (3, 2, 7)$ and $x_1^3 x_2^5 x_3^2 \prec_c x_1^3 x_2^2 x_3^7$.

What is a Gröbner basis??

Let $P = \{x \in \mathbb{R}^d : Ax = b, x \geq 0\} \neq \emptyset$, where $A \in \mathbb{Z}^{n \times d}$ and $b \in \mathbb{Z}^n$. Let M be a finite set such that $M \subset \{x \in \mathbb{Z}^d : Ax = 0\}$ and let $\prec$ be any term order on $\mathbb{N}^d$. Then we define the graph G_b such that:

- Nodes of G_b are lattice points inside P.
- Draw a directed edge from a node v to a node u if and only if $u \prec v$ for $u - v \in M$.

If G_b is acyclic and has a unique sink for all b with $P \neq \emptyset$, then M is a Gröbner basis for a toric ideal associate with a matrix A with respect to $\prec$.

Algorithm

Let $P := \{x \in \mathbb{R}^d : Ax = b,\ x \geq 0\}$.

Input: $c \in \mathbb{Z}^d$, $A \in \mathbb{Z}^{n \times d}$, $b \in \mathbb{Z}^n$ and a feasible solution $v_0 \in P \cap \mathbb{Z}^d$.

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 of I_A, the toric ideal associated with A with the term order $\prec_c$.

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

Theorem [De Loera, Haws, Hemmecke, Huggins, Sturmfels, Y. (04)]

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:

$$\text{maximize } c \cdot x \text{ subject to } x \in P, \; x \in \mathbb{Z}^d.$$

Questions??

Software

LattE is available from our website:

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

If you have any questions about LattE, please send me email at

ruriko@math.duke.edu.