State of the art Seminar

State Polytopes of Toric Ideals

Deepanjan Kesh
Thesis Supervisor: Prof. Shashank K. Mehta

August 10, 2007
Flowchart of the presentation

- Gröbner Basis
- Convex Polytope
  - State Polytope
  - Factorization
  - Problems
Gröbner Bases
Term Order

A total order $\preceq$ on $\mathbb{N}^n$ is a **term order** if the zero vector $0$ is the unique minimal element, and $a \preceq b$ implies $a + c \preceq b + c$ for all $a, b, c \in \mathbb{N}^n$.

Examples - *purely lexicographic order*, *degree lexicographic order* and *degree reverse lexicographic order*.

Initial Monomial

Given a term order $\preceq$, every non-zero polynomial $f \in k[x]$ has a unique **initial monomial**, denoted $in_{\preceq}(f)$. 
Example

\[ x^5 + 2x^3yz^2 + 3x^3y^3 + y^2z^4 \]

purely lexicographic order \( - x^5 \)
degree lexicographic order \( - 3x^3y^3 \)
degree reverse lexicographic order \( - y^2z^4 \)
A subset $I \subset k[x_1, \ldots, x_n]$ is an ideal if it satisfies:

(i) $0 \in I$.

(ii) If $f, g \in I$, then $f + g \in I$.

(iii) If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$. 
Initial Ideal

If $I$ is an ideal in $k[x]$, then its **initial ideal** is the monomial ideal

$$\text{in}_<(I) := \langle \text{in}_<(f) : f \in I \rangle$$

The monomials which do not lie in $\text{in}_<(I)$ are called **standard monomials**.
Example

\[ I = \langle x^5 + 2x^3yz^2 + 3x^3y^3 + y^2z^4, 2xy^2 + 5z^6 + x^3z \rangle \]

In general,
\[ in_{\prec}(I) \neq \langle in_{\prec}(x^5 + 2x^3yz^2 + 3x^3y^3 + y^2z^4), in_{\prec}(2xy^2 + 5z^6 + x^3z) \rangle \]

For example, in this case \( x^3y^2 \in in_{\text{lex}}(I) \), but does not belong to RHS.
Gröbner Basis

A finite subset $G \subset I$ is a Gröbner Basis for $I$ with respect to $\prec$ if $\text{in}_\prec(I)$ is generated by $\{\text{in}_\prec(g) : g \in G\}$.

If no monomial in this set is redundant, then the Gröbner Basis $G$ is minimal.

It is called reduced if, for any two distinct elements $g, g' \in G$, no term of $g'$ is divisible by $\text{in}_\prec(g)$. 
Universal Gröbner Basis

A finite subset $U \subset I$ is called a universal Gröbner Basis if $U$ is a Gröbner Basis of $I$ with respect to all term orders $\prec$ simultaneously.

It is called minimal if every element of $U$ belongs to some reduced Gröbner Basis of $I$. 
Gröbner Bases exists

**Theorem (Hilbert Basis Theorem).** Every Ideal has a finite generating set.

\[ \Downarrow \]

**Theorem.** \( I \subset k[x] \) has a Gröbner Basis .

\[ \Updownarrow \]

**Theorem.** Every ideal \( I \subset k[x] \) has only finitely many distinct initial ideals

\[ \Downarrow \]

**Theorem.** Every ideal \( I \subset k[x] \) possesses a universal Gröbner Basis .
Weight Vectors

Fix $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{R}^n$. For any polynomial $f = \sum c_i \cdot x^{a_i}$ we define the initial form $in_\omega(f)$ to be sum of all terms $c_i \cdot x^{a_i}$ such that the inner product $\omega \cdot a_i$ is maximal.

For an ideal, we define initial ideal to be the ideal generated by all initial forms:

$$in_\omega(I) := \langle in_\omega(f) : f \in I \rangle$$
Example

\[ x^5 + 2x^3yz^2 + 3x^3y^3 + y^2z^4 \]

\[ \omega = (2, 2, 2) \]

\[ \text{in}_{\omega}(\cdot) = 2x^3yz^2 + 3x^3y^3 + y^2z^4 \]
**Theorem.** For any term order $\prec$ and any ideal $I \subset k[x]$, there exists a non-negative integer vector $\omega \in \mathbb{N}^n$ such that $\text{in}_\omega(I) = \text{in}_\prec(I)$. 
Gröbner Region

We define the **Gröbner region** of an ideal $I$, $\text{GR}(I)$, to be the set of all $\omega \in \mathbb{R}^n$ such that $\text{in}_\omega(I) = \text{in}_{\omega'}(I)$ for some $\omega' \geq 0$.

**Theorem.** Suppose that $I \subset k[x]$ is a homogeneous ideal with respect to some positive grading $\text{deg}(x_i) = d_i > 0$. Then $\text{GR}(I) = \mathbb{R}^n$. 
Faces and cones of a polytope
Faces and cones of a polytope
Faces and cones of a polytope
Faces and cones of a polytope
Faces and cones of a polytope
A *polyhedron* is a finite intersection of closed half-spaces in $\mathbb{R}^n$. Thus a polyhedron $P$ can be written as -

$$P = \{ x \in \mathbb{R}^n : A \cdot x \leq b \}$$

where $A$ is a matrix with $n$ columns.

A polyhedron $Q$ which is bounded is called a *polytope*.

If $b = 0$, then the polyhedron is called a *(polyhedral) cone*.
Theorem. Every polytope $Q$ can be written as the convex hull of finite set of points, called the **vertices** of the polytope.
Face of a Polyhedron

Let $P$ be any polyhedron in $\mathbb{R}^n$ and $\omega \in \mathbb{R}^n$. We define

$$\text{face}_\omega(P) := \{ u \in P : \omega \cdot u \geq \omega \cdot v, \forall v \in P \}.$$ 

Every subset $F$ of $P$ which has this form is called a face of $P$.

The dimension of a face $F$ of a polyhedron $P$ is the dimension of its affine span, and its codimension is $\text{codim}_P(F) := \dim(P) - \dim(F)$.

A face of codimension 1 is a facet. Faces of dimension 0 and 1 are called vertices and edges respectively.
Relating Gröbner Basis and Convex Polytopes
Minkowski Sum and Newton Polytope

Minkowski addition of polyhedra

\[ P_1 \text{ and } P_2 \text{ is defined as} \]

\[ P_1 + P_2 := \{ p_1 + p_2 : p_1 \in P_1, p_2 \in P_2 \} \]

With every polynomial \( f = \sum_{i=1}^{m} c_i \cdot x^{a_i} \in k[x] \) we associate the
Newton Polytope

\[ \text{New}(f) := \text{conv}\{ a_i : i = 1, \ldots, m \} \text{ in } \mathbb{R}^n. \]

\[ \downarrow \]

**Theorem.** \( \text{New}(f \cdot g) = \text{New}(f) + \text{New}(g) \).
Geometry of weight vectors

Two weight vectors $\omega, \omega' \in \mathbb{R}^n$ are called equivalent (with respect to $I$) if and only if $\text{in}_\omega(I) = \text{in}_{\omega'}(I)$. The equivalence class of $\omega$ is denoted by $C[\omega]$.

**Theorem.** Each equivalence class of weight vectors is a relatively open convex polyhedral cone.

We define the Gröbner fan $\text{GF}(I)$ to be the set of closed cones $C[\omega]$ for all $\omega \in \mathbb{R}^n$. 
State Polytope: Geometry of Ideals

**Theorem.** Let $I$ be a homogeneous ideal in $k[x]$. There exists a polytope $State(I) \subset \mathbb{R}^n$ whose normal fan $N(State(I))$ coincides with the Gröbner fan $GF(I)$.

\[ \Downarrow \]

There is a **bijection** between the various initial ideals of $I$ and the faces of $State(I)$.
Computability

• Given the generators of an ideal, there exists an algorithm to compute its Gröbner Basis (*Buchberger’s Algorithm*).

• Given the generators of a homogeneous ideal, there exists an algorithm to compute its state polytope.

• Given the state polytope of a homogeneous ideal, there exists an algorithm to compute its universal Gröbner Basis.

• Given the universal Gröbner Basis of a homogeneous ideal, there exists an algorithm to compute its state polytope.
Problem: Characterization of Polytopes

Given a polytope \( \in \mathbb{R}^n \), can we answer the following questions

- Does there exist an ideal, for which the given polytope is the state polytope?
- If yes, what is the corresponding ideal?
A special class of ideals: 
Toric ideals
Toric Ideals

Fix a subset $\mathcal{A} = \{a_1, \ldots, a_n\}$ of $\mathbb{Z}^d$. Each vector $a_i$ is identified with a monomial $t^{a_i}$ in the Laurent polynomial ring $k[t^\pm] := k[t_1, \ldots, t_d, t_1^{-1}, \ldots, t_d^{-1}]$. Consider the semigroup homomorphism

$\pi : \mathbb{N}^n \to \mathbb{Z}^d, \mathbf{u} = (u_1, \ldots, u_n) \mapsto u_1a_1 + \ldots + u_na_n$

The map $\pi$ lifts to a homomorphism of semigroup algebras:

$\hat{\pi} : k[\mathbf{x}] \to k[t^\pm], x_i \mapsto t^{a_i}$.

The kernel of $\hat{\pi}$ is denoted $I_{\mathcal{A}}$ and called the toric ideal of $\mathcal{A}$. 
Let $u \in \mathbb{Z}^n$ be written as $u^+ - u^-$ such that all the components in $u^+, u^-$ are in $\mathbb{N}^n$.

Then, toric ideals can also be defined as

$$\{x^{u^+} - x^{u^-} | A \cdot u = 0\}$$
Computing Gröbner Basis of Toric Ideals

1. Introduce $n + d + 1$ indeterminates $t_0, t_1, \ldots, t_d, x_1, x_2, \ldots, x_n$.
   Let $\prec$ be any elimination term order with $\{t_i\} \succ \{x_j\}$.

2. Compute the reduced Gröbner Basis $\mathcal{G}$ for the ideal
   $$\langle t_0 t_1 \cdots t_d - 1, x_1 \cdot t_1^a - t_1^a, \ldots, x_n \cdot t_n^a - t_n^a \rangle.$$  

3. Output : The set $\mathcal{G} \cap k[x]$ is the reduced Gröbner Basis for $I_A$ with respect to $\prec$. 

33
Complexity of Gröbner Basis Algorithm

Given a basis \( \{f_1, \ldots, f_t\} \) of an ideal \( I \subset k[x_1, \ldots, x_n] \), the worst-case time complexity of the Buchberger’s Algorithm is \( d^{2^{O(n)}} \), where \( d = \text{maxdeg}(f_i) \).

Fortunately, for Toric Ideals there exists exponential time algorithm for computing its Gröbner Basis.
Fiber

Let us restrict the codomain of the previously mentioned map \( \pi \) to \( \mathbb{N}^d \). We call \( \pi^{-1}(b) \) the \textit{fiber} of \( A \) over \( b \).

We can also define \textit{fiber} as

\[
\{ u \in \mathbb{N}^n | A \cdot u = b \}
\]
Applications of Toric Ideals

There are three natural families of problems associated with these fibres:

- **Enumeration**: Determine the cardinality of $\pi^{-1}(b)$. If this number is "not too big", then list all elements in the fiber $\pi^{-1}(b)$ explicitly.
If complete enumeration is infeasible, then the following questions are of interest.

- **Sampling:** Choose a point at random from $\pi^{-1}(b)$. For our purposes it suffices to assume that "at random" refers to the uniform distribution on $\pi^{-1}(b)$.

- **Integer Programming:** Given any "cost vector" $\omega \in \mathbb{R}^n$, find a point $u$ in $\pi^{-1}(b)$ which minimizes the value of the linear functional $u \mapsto u \cdot \omega$

These standard problems can be handled with toric ideals model.
Comments

Developing algorithms for computing Gröbner Basis of toric ideals have lots of practical applications and we intend to address this problem as a part of our thesis.

The **TiGERS** (Toric Gröbner Bases Enumeration by Reverse Search) is the current state of the art system employed to compute the Gröbner fan of toric ideals.
A benchmark application for Gröbner Basis computation of Toric Ideals
A **partition identity** is any identity of the form

\[ a_1 + a_2 + a_3 + \ldots + a_k = b_1 + b_2 + b_3 + \ldots + b_l \]

where \( 0 < a_i, b_j \leq n \) and all parts are integers (generally not distinct). The number \( k + l \) is called its **degree**.

We call a partition identity as **primitive** if there is no proper subidentity

\[ a_{i_1} + a_{i_2} + \ldots + a_{i_r} = b_{j_1} + b_{j_2} + \ldots + b_{j_r} \]

where \( 1 \leq r + s \leq k + l - 1 \).
Example

\[4 + 4 = 1 + 1 + 1 + 5\]
\[3 + 4 + 4 + 4 = 5 + 5 + 5\]
The problem

We want to compute the number of primitive partition identities that can be formed for a given $n$. The number is known upto $n = 20$ using toric ideals methods. It is known for much higher $n(=27)$ using optimization techniques. Yet, to compute for $n > 20$ is a nice benchmark problem for implementations of the Buchberger Algorithm for toric ideals.
Multivariate Polynomial factorization via Integral Polytopes
Definitions

Let $k$ be any arbitrary field and $f \in k[x_1, \ldots, x_n]$ be a polynomial, where

$$f = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

We call $f$ absolutely irreducible over $k$ if it has no non-trivial factors over the algebraic closure of $k$.

The integral polytope

$$\text{conv}\{(i_1, \ldots, i_n) | a_{i_1 \ldots i_n} \neq 0\}$$

in $\mathbb{R}^n$ is called the Newton Polytope of $f$.

We say that an integral polytope is integrally decomposable, or simply decomposable, if it can be written as a Minkowski sum of two integral polytopes, each of which has more than one point.
The Irreducibility Criterion

Let \( f \in k[x_1, \ldots, x_n] \) with \( f \) not divisible by any \( x_i \) for \( 1 \leq i \leq n \). If the Newton polytope of \( f \) is integrally indecomposable, then \( f \) is absolutely irreducible.
Polygon Decomposability (PolyDecomp). Given an integral polytope, say as its list of vertices, decide whether it is integrally indecomposable.

Theorem. PolyDecomp is NP-complete.
$n = 2$: Polygons

There exists an algorithm whose running time is polynomial in the length of the sides of the polygon rather than the logarithm of the lengths.

This is an example of a pseudopolynomial-time algorithm.
Higher dimensional Integral Polytopes

There exists a randomized pseudo-polynomial time algorithm for testing the decomposibility of integral polytopes

**Note:** This problem is NP-complete
Open Problems

- Is PolyDecomp **strongly NP-complete** in the sense that the problem remains \(NP-complete\) when one bounds running time by the lengths, instead of logarithm of the lengths, of the edge vectors?

- To develop a psuedo-polynomial time algorithm for testing the decomposibility of integral polytopes.
References


• Shashank K Mehta (2003), *A New Algorithm for Universal Gröbner Basis for Toric Ideals*, 6th International Conference of the Association of Asia Pacific Operational Research Societies, New Delhi.

Thank You for your patience!