The 22nd National School on Algebra:
Algebraic and Combinatorial Applications of Toric Ideals
Romania, September 1-5, 2014

Toric and Lattice Ideals: Generating Sets

Hara Charalambous

Department of Mathematics
Aristotle University of Thessaloniki

Toric ideals

Let $A = \{\mathbf{a}_1, \dots, \mathbf{a}_n\} \subseteq \mathbb{Z}^m \setminus \{0\}$, so that the corresponding matrix with columns the vectors of A has rank m. Let $\mathbb{N}A := \{l_1\mathbf{a}_1 + \cdots + l_n\mathbf{a}_n \mid l_i \in \mathbb{N}_0\}$, $\Bbbk$ a field, $L = \ker_{\mathbb{Z}}(A) \subset \mathbb{Z}^n$. Note that L is a lattice. We grade $R = \Bbbk[x_1, \dots, x_n]$ by the semigroup $\mathbb{N}A$:

$$\deg_A(x_i) = \mathbf{a}_i \ , \quad i = 1, \dots, m \ .$$

For $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{N}^n$ and $\mathbf{x}^{\mathbf{u}} := x_1^{u_1} \cdots x_n^{u_n}$ we let

$$\deg_A(\mathbf{x}^{\mathbf{u}}) := u_1\mathbf{a}_1 + \cdots + u_n\mathbf{a}_n \in \mathbb{N}A.$$

Definition

The **toric ideal** *of A is the ideal $I_A := \langle \mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} : \ \deg_A(\mathbf{x}^{\mathbf{u}}) = \deg_A(\mathbf{x}^{\mathbf{v}})\rangle$. I_A is also called the lattice ideal I_L.*

Properties of toric ideals

- toric ideals are prime ideals
- toric ideals are generated by binomials
- $I_A = I_L = < \mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}}$ such that $\mathbf{u} - \mathbf{v} \in L >$.
- The ring R/I_A has Krull dimension m.
- For every term order, the corresponding Gröbner basis of I_A consists of binomials.

How do we compute toric ideals?

Example I

Example

Let $A = \{2, 1, 1\}$. In $\phi : \ K[x_1, x_2, x_3]$ we set $\deg_A(x_1) = 2$, $\deg_A(x_2) = \deg_A(x_1) = 1$. Note that $L = \ker_{\mathbb{Z}} A = \langle (1, -2, 0), (0, -1, 1) \rangle$.

$$I_A = (x_1 - x_2^2, x_2 - x_3)$$

Let $\mathbf{u} = (1, -2, 0) \in \ker \pi$. Then

$$\mathbf{u} = (1, 0, 0) - (0, 2, 0) = (3, 1, 2) - (2, 3, 2)$$

The corresponding binomials are

$$x_1 - x_2^2 \text{ and } x_1^3 x_2 x_3^2 - x_1^2 x_2^3 x_3^2 \in I_A \ .$$

We let $\mathbf{u}^+ = (1, 0, 0)$, $\mathbf{u}^- = (0, 2, 0)$.

Example II

Example

Let $A = \{1, -1, 1\}$. In $R = \Bbbk[x_1, x_2, x_3]$ we set $\deg_A(x_1) = 1$, $\deg_A(x_2) = -1$, $\deg_A(x_3) = 1$. Note that $L = \ker_{\mathbb{Z}} A$ $= \langle (1,1,0), (0,1,1), (1,0,-1) \rangle = \langle (1,1,0), (0,1,1) \rangle$.

$$I_L = (1 - x_1x_2, 1 - x_2x_3, x_1 - x_3) = (1 - x_1x_2, x_1 - x_3)$$
$$= (1 - x_1x_2, 1 - x_2x_3)$$

There are infinitely many monomials in R of degree 0: $\deg_A(x_1^t x_2^t) = 0$ for $t \in \mathbb{N}$. Thus $1 - x_1^t x_2^t \in I_L$.

Lattice ideals

Let $L \subset \mathbb{Z}^n$ be a lattice.

Definition

The lattice ideal I_L is

$$I_L := \langle x^u - x^v : \; u - v \in L \rangle = \langle x^{w^+} - x^{w^-} : \; w \in L \rangle$$

where $w = w^+ - w^-$ and $gcd(x^{w^+}, x^{w^-}) = 1$.

Let $\mathbf{a_i} = \mathbf{e_i} + \mathbf{L} \in \mathbb{Z}^\mathbf{n}/\mathbf{L}$ for $i = 1, \ldots, n$, $A = \{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$. For $u \in \mathbb{N}^n$, we let

$$\deg_A(x^u) := \sum u_i \mathbf{a}_i \; .$$

Theorem

I_L is generated by all binomials $\mathbf{x^u} - \mathbf{x^v}$ such that $\deg_A(\mathbf{x^u}) = \deg_A(\mathbf{x^v})$.

Example: lattice ideals

Example

Let $L = 3\mathbb{Z}$. Then $u - v \in L$ iff $u \equiv v \mod 3$.

$$I_L = \langle 1 - x^3 \rangle \ = \langle 1 - x^6, x^5 - x^8 \rangle.$$

$$1 - x^3 = (1 - x^6) + x(x^5 - x^8) - x^3(1 - x^6)\ .$$

Note that in this case $\mathbb{Z}/L$ has torsion.

Finding generating sets: $L = \ker A$ where $A \subset \mathbb{Z}^m$

I_L is a toric Ideal. Let the columns of A be $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ and $S = R[t_0, \ldots, t_m]$.

Algorithm

1. Let

$$J = \langle 1 - t_0 t_1 \ldots t_m, x_1 t^{\mathbf{a}_1^-} - t^{\mathbf{a}_1^+}, \ldots, x_n t^{\mathbf{a}_n^-} - t^{\mathbf{a}_n}\rangle$$

It can be proved that $I_L = J \cap R$.
2. Compute a reduced Gröbner basis G for J according to a proper (eliminating) order: $\{t_j\} > \{x_i\}$. (Use of computer). It can be proved that the elements of G are binomials
3. Choose the elements of G that do not involve $t_0, \ldots, t_m$, $(G \cap R)$. They form a generating set of I_L since they are a Gröbner basis of I_L.
4. Minimize $G \cap R$.

Finding generating sets when a $\mathbb{Z}$-basis of L is known.

If J is any ideal of R and $f \in R$, we let

$$(J : f^\infty) = \{g \in R : \; gf^r \in J, \; r \in \mathbb{N}\} \; .$$

Theorem

Let E be a $\mathbb{Z}$-basis of L. For all $w \in E$ consider the ideal $I(E) = \langle x^{w^+} - x^{w^-} : \; w \in E\rangle$. Then $I_L = (I(E) : \; (x_1 \cdots x_m)^\infty)$

The computations involve computational tricks and techniques and heavy Gröbner bases usage

Important binomial subsets of I_A and corresponding subsets of $L = \ker_{\mathbb{Z}}(A)$

To each binomial $x^u - x^v \in I_A$ we correspond $u - v \in L$.

- The set consisting of all **primitive** binomials of I_A. The corresponding vectors form the Graver basis of A
- The universal Gröbner basis of I_A is the union of all reduced Gröbner basis of I_A. The corresponding vectors form the universal Gröbner basis of A.
- A Markov basis of I_A i.e. a minimal generating set of binomials of I_A. The corresponding vectors form a **Markov** basis of A.
- The universal Markov basis of I_A is the union of all Markov bases of I_A. The corresponding vectors form the universal Markov basis of A.
- The indispensable binomials that belong to all Markov bases of I_A. The corresponding vectors form the set of indispensables of A.

Graver basis

An irreducible binomial $x^{\mathbf{u}^+} - x^{\mathbf{u}^-} \in I_A$ is called *primitive* if there exists no other binomial $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} \in I_A$ such that $x^{\mathbf{v}^+}$ divides $x^{\mathbf{u}^+}$ and $x^{\mathbf{v}^-}$ divides $x^{\mathbf{u}^-}$. The set of all primitive binomials of a toric ideal I_A is the Graver basis of I_A.

Example

We have seen that $I = (x_1 - x_2^2, x_2 - x_3)$ is the toric ideal corresponding to $A = \{2, 1, 1\}$.

All elements of the minimal generating set of I are primitive.

$x_2^5 - x_1^2 x_3 \in I$ is not primitive since $x_2^2 - x_1 \in I$.

Markov basis

Theorem

(Diaconis, Sturmfels 1998) $A \subseteq \mathbb{Z}^m \setminus \{0\}$. *Let* $C \subset L = \ker_{\mathbb{Z}}(A)$. *Then*

$$\{x^{\mathbf{u}^-} - x^{\mathbf{u}^+} : \ \mathbf{u} \in C\}$$

is a minimal generating set of I_A *iff* C *is minimal with respect to the following property:*

whenever $\mathbf{w}, \mathbf{u} \in \mathbb{N}^n$ *and* $\mathbf{w} - \mathbf{u} \in L$ *(i.e.* $A\mathbf{w} = A\mathbf{u}$*), there exists a subset* $\{\mathbf{v}_i : i = 1, \ldots, s\}$ *of* C *that connects* $\mathbf{w}$ *to* $\mathbf{u}$*. This means that for* $1 \leq p \leq s$,

$$\mathbf{w} + \sum_{i=1}^{p} \mathbf{v}_i \in \mathbb{N}^n, \ \ and \ \mathbf{w} + \sum_{i=1}^{s} \mathbf{v}_i = \mathbf{u} \ .$$

Graver basis

Let $\mathbf{u}, \mathbf{v}, \mathbf{w}$ be nonzero integer vectors. We say that $\mathbf{u} = \mathbf{v} +_c \mathbf{w}$ is a **conformal decomposition** of $\mathbf{u}$ if $\mathbf{u}^+ = \mathbf{v}^+ + \mathbf{w}^+$ and $\mathbf{u}^- = \mathbf{v}^- + \mathbf{w}^-$.

It is immediate that the Graver basis of A consists of all elements of L which have no conformal decomposition.

What is the relation between the previously defined sets (Graver, universal Gröbner, universal Markov)? Of course the universal Gröbner basis **contains** a Markov basis, but is it also true that the universal Markov basis is inside the universal Gröbner basis?

Universal Gröbner bases and Primitive polynomials

Theorem

(Sturmfels 95) For any lattice ideal I_A the following containments hold:

$$\text{Universal Gröbner basis of } A \subset \text{Graver basis of } A$$

What is the relation between the universal Gröbner basis of A and the universal Markov basis of A? What is the relation between the universal Markov basis of A and the Graver basis of A?

Example

Let $I = (x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8)$. This generating set is not part of any reduced Gröbner basis of I.

Example

Let

$$A = \begin{pmatrix} 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\ 4 & 0 & 4 & 0 & 3 & 3 & 3 & 3 \\ 4 & 0 & 0 & 4 & 3 & 3 & 3 & 3 \\ 2 & 2 & 2 & 2 & 6 & 0 & 6 & 0 \\ 2 & 2 & 2 & 2 & 6 & 0 & 0 & 6 \end{pmatrix}.$$

It can be shown that

$$I_A = (x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8).$$

The binomial $x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8$ does not belong to a reduced Gröbner basis of I_A since for any monomial order, the initial term of $x_1x_2 - x_3x_4$ divides $x_1^2x_2^2x_3x_4$ while the initial term of $x_5x_6 - x_7x_8$ divides $x_5x_6x_7x_8$.

Markov Polytopes

Let $A \subset \mathbb{N}^m$. For $u \in L$, let $\mathcal{F}_{\mathbf{u}} = \mathcal{F}_{\mathbf{u}^+} := \{\mathbf{t} \in \mathbb{N}^n : \mathbf{u}^+ - \mathbf{t} \in L\}$.

Construct the graph $G_{\mathbf{u}}$: its vertices are the elements of $\mathcal{F}_{\mathbf{u}}$. Two vertices $\mathbf{w}_1$, $\mathbf{w}_2$ are joined by an edge if $gcd(x^{w_1}, x^{w_2}) \neq 1$.

Theorem

(CKT07, DSS09) $\mathbf{u}$ *is in the universal Markov basis of A if and only if* $\mathbf{u}^+$ *and* $\mathbf{u}^-$ *belong to different connected components of* $G_{\mathbf{u}}$*.*

We consider the convex hulls of the connected components of $G_{\mathbf{u}}$.

Definition

(CTV14a) A Markov polytope is the convex hull of the elements in a connected component of this graph.

Universal Markov and universal Gröbner basis

Let $A \subset \mathbb{N}^m$, $L = \ker_{\mathbb{Z}}(A)$.

Theorem

(St 95) $\mathbf{u} \in L$ *is in the universal Gröbner basis of* A *if* $\mathbf{u}$ *is in the Graver basis of* A *and* $[\mathbf{u}^+, \mathbf{u}^-]$ *is an edge at the convex hull of all points in* $\mathcal{F}_u$.

We get the following characterization:

Theorem

(CTVl14a) Let $\mathcal{L}$ *be as above. An element* $\mathbf{u}$ *of the universal Markov basis of* A *belongs to the universal Gröbner basis of* A *if and only if* $\mathbf{u}^+$ *and* $\mathbf{u}^-$ *are vertices of two different (Markov) polytopes.*

Example of Markov polytope

Example

Let A be the matrix of the previous example. Recall that $x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8$ is in the universal Markov basis of I_A but not in the universal Gröbner basis of I_A. Let $\mathbf{u} = (2, 2, 1, 1, -1, -1, -1, -1) \in L$. Then $|\mathcal{F}_{\mathbf{u}}| = 7$ and $\mathcal{F}_{\mathbf{u}} =$

$$\{(3, 3, 0, \ldots, 0), u^+, (1, 1, 2, 2, 0, 0, 0, 0), (0, 0, 3, 3, 0, 0, 0, 0)\}$$

$$\cup \{(0, \ldots, 0, 2, 2, 0, 0), u^-, (0, \ldots, 0, 2, 2)\}$$

The graph $G_{\mathbf{u}}$ has two connected components.

The Markov polytopes are line segments: u^+ and u^- are not vertices of their Markov polytopes.

In conclusion

Let $A \subset \mathbb{Z}^m$, $L = \ker_{\mathbb{Z}}(A)$.

- If $A \subset \mathbb{N}^m$, then the universal Markov basis of A is contained in the Graver basis of A.
- The universal Gröbner basis of A is always contained in the Graver basis of A.
- The universal Markov basis of A is not necessarily a subset of the Gröbner basis of A.
- The universal Markov basis of A is part of the Graver basis of A if and only if $L \cap \mathbb{N}^n = 0$ or if $L = \langle u \rangle$ where $u \in \mathbb{N}^n$, (CTV14a).

- CKT H. Charalambous, A. Katsabekis, A. Thoma, Minimal systems of binomial generators and the indispensable complex of a toric ideal, Proc. Amer. Math. Soc. **135**, 3443–3451 (2007).
- CTV H. Charalambous, A. Thoma, M. Vladoiu, Markov bases of lattice ideals, arXiv:1303.2303v2.
- CTVa H. Charalambous, A. Thoma, M. Vladoiu, Markov complexity of monomial curves, J. Algebra, (2014)
- CTV H. Charalambous, A. Thoma, M. Vladoiu, Markov bases and generalized Lawrence liftings, Annals of Combinatorics, (2014)
- DS P. Diaconis, B. Sturmfels, Algebraic algorithms for sampling from conditional distributions, Ann. Statist. **26**, 363–397 (1998).
- DSS M.Drton, B.Sturmfels, S. Sullivant, Lectures on Algebraic Statistics, 2009
- B. Sturmfels, *Gröbner bases and Convex Polytopes, University Lecture Series, Vol 8, AMS (1995)*