Toric ideals and Gröbner bases

Apostolos Thoma

Department of Mathematics
University of Ioannina

EMS Summer School on Multigraded Algebra and Applications
Moieciu, Romania
Let \( A = \{a_1, \ldots, a_n\} \subseteq \mathbb{Z}^m \) be a set of vectors in \( \mathbb{Q}^m \).
Let \( A = [a_1 \ldots a_n] \in \mathbb{Z}^{m \times n} \) be an integer matrix with columns \( a_i \). For a vector \( u \in \text{Ker}_\mathbb{Z}(A) \) we let \( u^+, u^- \) be the unique vectors in \( \mathbb{N}^n \) with disjoint support such that \( u = u^+ - u^- \).

**Definition**

The toric ideal \( I_A \) of \( A \) is the ideal in \( K[x_1, \ldots, x_n] \) generated by all binomials of the form \( x^{u^+} - x^{u^-} \) where \( u \in \text{Ker}_\mathbb{Z}(A) \).

A toric ideal is a binomial ideal.
Toric ideals are binomial ideals. There are certain sets of binomials that are important:

- Graver basis
- Circuits
- Markov bases
- Indispensable binomials
- reduced Gröbner basis
- universal Gröbner basis
Theorem (Diaconis-Sturmfels 1998)

\[ M \text{ is a minimal Markov basis of } A \text{ if and only if the set } \{x^{u^+} - x^{u^-} : u \in M\} \text{ is a minimal generating set of } I_A.\]

Definition

We call a minimal Markov basis of \( I_A \) any minimal generating set of \( I_A \).
In the toric ideal of the complete graph on 10 vertices there are \(3^{210}\) different minimal Markov bases. Every minimal Markov basis contains 420 elements.
A toric ideal $I_A$ is called generic if it is minimally generated by binomials with full support.

**Example**

$$A = (20 \ 24 \ 25 \ 31)$$

$$I_A = \langle x_3^3 - x_1x_2x_4, x_1^4 - x_2x_3x_4, x_4^3 - x_1x_2^2x_3, x_2^4 - x_1^2x_3x_4, x_3^2x_2^2 - x_2^2x_4^2, x_1x_2^3 - x_3^2x_4^2, x_1^3x_4^2 - x_2^3x_3^2 \rangle.$$

- Every generic toric ideal has a unique minimal Markov basis.
- If the generic toric ideal is not a principal ideal then none of the generators is a circuit.
How many Markov bases exist?

There are two main cases:
1st case. The semigroup $\mathbb{N}A$ is positive, that means $\ker_{\mathbb{Z}}(A) \cap \mathbb{N}^n = \{0\}$.
   - Every fiber is finite.
   - Every minimal Markov basis has the same number of elements.
   - There are finitely many different minimal Markov bases.
   - The multiset of fibers for which the elements of a minimal Markov basis belong to is an invariant of the toric ideal.
   - All minimal Markov bases are subsets of the Graver basis.

2nd case. The semigroup $\mathbb{N}A$ is not positive, that means $\ker_{\mathbb{Z}}(A) \cap \mathbb{N}^n \neq \{0\}$.
   - Every fiber is infinite.
   - Different minimal Markov bases may have different number of elements.
   - There are infinitely many different minimal Markov bases.
   - The multiset of fibers that the elements of a minimal Markov basis belong to is not invariant of the toric ideal.
   - There is at least one minimal Markov basis which is a subset of the Graver basis.

Apostolos Thoma

Toric ideals and Gröbner bases
Let $A = \begin{bmatrix} 1 & -1 \end{bmatrix}$, the simplest example of a matrix such that the semigroup $\mathbb{N}A$ is not positive, since $(1, 1) \in \text{Ker}_\mathbb{Z}(A) \cap \mathbb{N}^2$.

The Graver basis of $A$ is $\{1 - xy\}$.

The following sets are some of the infinitely many minimal Markov bases:

- $\{1 - xy\}$
- $\{1 - x^2y^2, 1 - x^3y^3\}$
- $\{1 - x^6y^6, 1 - x^{10}y^{10}, 1 - x^{15}y^{15}\}$
- $\{1 - x^2y^2, x - x^2y\}$
- $\{1 - x^5y^5, xy^3 - x^{2014}y^{2016}\}$

H. Charalambous, A. Thoma, M. Vladoiu, *Markov Bases of Lattice Ideals*
Let $A = \begin{bmatrix} 1 & -1 \end{bmatrix}$, the simplest example of a matrix such that the semigroup $\mathbb{N}A$ is not positive, since $(1, 1) \in \text{Ker}_\mathbb{Z}(A) \cap \mathbb{N}^2$. The Graver basis of $A$ is $\{1 - xy\}$. The following sets are some of the infinitely many minimal Markov bases:

- $\{1 - xy\}$
- $\{1 - x^2 y^2, 1 - x^3 y^3\}$
- $\{1 - x^6 y^6, 1 - x^{10} y^{10}, 1 - x^{15} y^{15}\}$
- $\{1 - x^2 y^2, x - x^2 y\}$
- $\{1 - x^5 y^5, xy^3 - x^{2014} y^{2016}\}$

H. Charalambous, A. Thoma, M. Vladoiu, *Markov Bases of Lattice Ideals*
Indispensable binomials

Definition

A binomial that belongs (up to sign) to every binomial generating set of the toric ideal $I_A$ is called indispensable.

- All elements in a minimal Markov basis of a generic toric ideal are indispensable.
- None of the elements in any minimal Markov basis of the toric ideal of the complete graph on 10 vertices is indispensable.
A Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ is a set of generators of the ideal $I$, not necessarily minimal, with good computational properties.
Let $k$ be a field and let $k[x_1, \ldots, x_n]$ be the polynomial ring in $n$ variables over $k$.

A monomial is a product $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, where $a = (a_1, a_2, \ldots, a_n) \in \mathbb{N}_0^n$.

**Definition**

An ideal $I \subset k[x_1, \ldots, x_n]$ is called a monomial ideal if it is generated by monomials.

**Theorem**

*Every monomial ideal has a finite unique minimal system of monomial generators.*
**Theorem**

Let $M$ be a monomial ideal in $k[x_1, \ldots, x_n]$ and let $m_1, \ldots, m_s$ be the unique minimal system of monomial generators of $M$. Then

- the monomial $m$ belongs to the monomial ideal $M$ if and only if there exists an $i \in \{1, \ldots, s\}$ such that $m = m_i q_i$, where $q_i$ is a monomial in $k[x_1, \ldots, x_n]$.

- the polynomial $f = a_1 x^{u_1} + a_2 x^{u_2} + \ldots a_r x^{u_r}$, with each $a_i \neq 0$, belongs to the monomial ideal $M$ if and only if each monomial $x^{u_i}$ belongs to $M$, where $i \in \{1, \ldots, r\}$. 
Monomial orders

By $T^n$ we denote the set of monomials $x^a$ in $k[x_1, \ldots, x_n]$.

$$T^n = \{x^a | a \in \mathbb{N}_0^n\}.$$  

Definition

By a monomial order on $T^n$ we mean a binary relation $\leq$ on $T^n$ such that

- for every $x^a \in T^n$ we have $x^a \leq x^a$ (reflexive)
- if $x^a \leq x^b$ and $x^b \leq x^a$ then $x^a = x^b$ (antisymmetric)
- if $x^a \leq x^b$ and $x^b \leq x^c$ then $x^a \leq x^c$ (transitive)
- if $x^a, x^b \in T^n$ then $x^a \leq x^b$ or $x^b \leq x^a$ (total order)
- $1 < x^a$ for all $x^a \in T^n$ with $x^a \neq 1$
- If $x^a < x^b$ then $x^a x^c < x^b x^c$ for all $x^c \in T^n$. 

Apostolos Thoma

Toric ideals and Grobner bases
Monomial orders

**Definition**

We say that $x^a < x^b$ if $x^a \leq x^b$ and $x^a \neq x^b$.

If $n = 1$ then there is a unique monomial order (on $T^1$).

$1 < x_1$ therefore $x_1 < x_1^2$ therefore $x_1^2 < x_1^3$ ...

Thus

$$1 < x_1 < x_1^2 < x_1^3 < \cdots.$$
Lexicographic monomial order

**Definition (Lexicographic order with \( x_1 > x_2 > \cdots > x_n \))**

We define \( x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x^b = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} \) if and only if there exists an \( i \in \{1, 2, \cdots, n\} \) such that

\[
\begin{align*}
a_1 &= b_1 \\
\cdots \\
a_{i-1} &= b_{i-1} \\
a_i &> b_i.
\end{align*}
\]

There are \( n! \) different Lexicographic monomial orders. We denote the Lexicographic monomial order \( > \) by

\( >_{\text{lex}} \).
We define $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x^b = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ if and only if $a_1 + a_2 + \cdots + a_n > b_1 + b_2 + \cdots + b_n$ or $a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n$ and there exists an $i \in \{1, 2, \cdots, n\}$ such that

\[
\begin{align*}
a_1 &= b_1 \\
\cdots \\
a_{i-1} &= b_{i-1} \\
a_i &= b_i.
\end{align*}
\]

There are $n!$ different Degree lexicographic monomial orders. We denote the Degree lexicographic monomial order $>$ by $>_{\text{deglex}}$. 
Definition (Degree reverse lexicographic order with \( x_1 > x_2 > \cdots > x_n \))

We define \( x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x^b = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} \) if and only if \( a_1 + a_2 + \cdots + a_n > b_1 + b_2 + \cdots + b_n \) or \( a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n \) and there exists an \( i \in \{ 1, 2, \cdots, n \} \) such that

\[
\begin{align*}
    a_n &= b_n \\
    &\vdots \\
    a_{i+1} &= b_{i+1} \\
    a_i &< b_i.
\end{align*}
\]

There are \( n! \) different Degree reverse lexicographic monomial orders. We denote the Degree reverse lexicographic monomial order \( > \) by

\[ > \text{degrevlex} \cdot \]
Example

In the polynomial ring $k[x_1, x_2, x_3]$ with $x_1 > x_2 > x_3$ for the monomials $x_1^2$, $x_1 x_2 x_3$ and $x_2^3$ we have

- $x_1^2 > \text{lex} \ x_1 x_2 x_3 > \text{lex} \ x_2^3$
- $x_1 x_2 x_3 > \text{deglex} \ x_2^3 > \text{deglex} \ x_1^2$
- $x_2^3 > \text{degrevlex} \ x_1 x_2 x_3 > \text{degrevlex} \ x_1^2$
Sometimes we can define a monomial order using a matrix $U \in \mathbb{R}^{m \times n}$. We define $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x^b = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ if and only if the first (from the top) nonzero coordinate of $U(a - b)^t$ is positive.
The lexicographic monomial order with \( x_1 > x_2 > \cdots > x_n \) can be defined by the identity \( n \times n \) matrix,

\[
I_{n \times n} = (\delta_{ij}) = \begin{pmatrix}
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & 0 \\
0 & 0 & 0 & \ldots & 0 & 1
\end{pmatrix}.
\]

while any lexicographic monomial order can be defined by a permutation matrix

\[
(\delta_{i\sigma(j)}).
\]
The degree lexicographic monomial order with $x_1 > x_2 > \cdots > x_n$ can be defined by the $n \times n$ matrix,

$$
D = \begin{pmatrix}
1 & 1 & 1 & \ldots & 1 & 1 \\
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & 0 \\
0 & 0 & 0 & \ldots & 0 & 1 \\
\end{pmatrix}
$$

while any other degree lexicographic monomial order can be defined by a matrix obtained by a permutation of the last $n$ rows of $D$. 
The degree reverse lexicographic monomial order with $x_1 > x_2 > \cdots > x_n$ can be defined by the $n \times n$ matrix,

$$
R = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 & 1 \\
0 & 0 & 0 & \cdots & 0 & -1 \\
0 & 1 & 0 & \cdots & -1 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & -1 & \cdots & 0 & 0 \\
0 & -1 & 0 & \cdots & 0 & 0 \\
-1 & 0 & 0 & \cdots & 0 & 0 \\
\end{pmatrix}
$$

while any other degree reverse lexicographic monomial order can be defined by a matrix obtained by a permutation of the last $n$ rows of $R$. 
If $n \geq 2$ then there are infinitely many monomial orders on $T^n$. For example for $n = 2$ there are infinitely many monomial orders on $T^2$ defined by the matrices

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

or

$$B = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix}$$

where $a, b \in \mathbb{R}_{\geq 0}$. Note that all are distinct except if $ab = 1$ and $a \notin \mathbb{Q}_{\geq 0}$. 
Monomial orders defined by matrices

**Theorem (Robbiano)**

A matrix $U \in \mathbb{R}^{m \times n}$ defines a monomial order if

- $\ker(U) \cap \mathbb{N}_0^n = \{(0, 0, \cdots, 0)\}$
- the first nonzero coordinate in every column of $U$ is positive.

Every monomial order can be defined by an appropriate matrix.
Let $>$ be a monomial order on $T^n$. Let $f$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$. We may write

$$f = a_1 x^{u_1} + a_2 x^{u_2} + \cdots + a_r x^{u_r},$$

where $a_i \neq 0$ and $x^{u_1} > x^{u_2} > \cdots > x^{u_r}$.

**Definition**

For $f \neq 0$ in $k[x_1, \ldots, x_n]$, we define the initial monomial of $f$ to be $in_<(f) = x^{u_1}$. The coefficient $a_1$ is called the initial coefficient of $f$ and is denoted by $c_f$. For a subset $S$ of $k[x_1, \ldots, x_n]$ we define the initial monomial ideal of $S$ to be the monomial ideal $in_<(S) = \langle in_<(f) | f \in S \rangle$. 
Gröbner bases

Definition
A set of non-zero polynomials \( G = \{g_1, \ldots, g_t\} \) contained in an ideal \( I \) is called Gröbner basis for \( I \) if and only if for all nonzero \( f \in I \) there exists \( i \in \{1, \ldots, t\} \) such that \( \text{in}_<(g_i) \) divides \( \text{in}_<(f) \).

Theorem
A set of non-zero polynomials \( G = \{g_1, \ldots, g_t\} \) contained in an ideal \( I \) is a Gröbner basis for \( I \) if and only if
\[
\text{in}_<(G) = \text{in}_<(I).
\]
Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$ and let $I \subset k[x_1, \ldots, x_n]$ be an ideal.

**Definition**

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

**Example**

Let $I$ be the ideal $< x_1^2 - x_2^3, x_2^2 - x_3^3, x_3^2 - x_4^3 >$ of the polynomial ring $k[x_1, x_2, x_3, x_4]$ with the lexicographic monomial order with $x_1 > x_2 > x_3 > x_4$. Then $\text{in}_{\text{lex}}(I) = < x_1^2, x_2^2, x_3^2 >$ therefore the ideal $I$ has the Gröbner basis 

$$\{x_1^2 - x_2^3, x_2^2 - x_3^3, x_3^2 - x_4^3\}$$

The standard monomials are of the form $x_4^i, x_1x_4^i, x_2x_4^i, x_3x_4^i, x_1x_2x_4^i, x_1x_3x_4^i, x_2x_3x_4^i, x_1x_2x_3x_4^i$ for some $i \in \mathbb{N}_0$. 
Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$. 

**Definition**

Given polynomials $f, g, h$ in $k[x_1, \ldots, x_n]$ with $g \neq 0$, we say that $f$ reduces to $h$ modulo $g$, and we write $f \rightarrow_g h$, if and only if $\text{in}_<(g)$ divides a nonzero term $X$ of $f$ and

$$h = f - \frac{X}{c_g \text{in}_<(g)} g.$$ 

**Example**

Let $f = x_1^4 x_3 + 2x_1^2 x_2^2 - x_3^5$ and $g = x_1^2 x_2 - x_3$ in $\mathbb{Q}[x_1, x_2, x_3]$ with the lexicographic monomial order with $x_1 > x_2 > x_3$. Then $\text{in}_<(g) = x_1^2 x_2$ divides the term $X = 2x_1^2 x_2^2$ and $h =$

$$f - \frac{X}{c_g \text{in}_<(g)} g = x_1^4 x_3 + 2x_1^2 x_2^2 - x_3^5 - \frac{2x_1^2 x_2^2}{x_1^2 x_2} (x_1^2 x_2 - x_3) = x_1^4 x_3 + 2x_2 x_3 - x_3^5.$$
Let $> \in k[x_1, \ldots, x_n]$.

**Definition**

Given polynomials $f, f_1, \ldots, f_s, h$ in $k[x_1, \ldots, x_n]$ with $f_i \neq 0$. We say that $f$ reduces to $h$ modulo $F = \{f_1, f_2, \ldots, f_s\}$, and we write

$$f \rightarrow_F h$$

if and only if there exists a sequence of indices $i_1, \ldots, i_t$ such that

$$f \rightarrow_{f_{i_1}} h_1 \rightarrow_{f_{i_2}} h_2 \rightarrow \cdots \rightarrow_{f_{i_t}} h.$$
Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$.

**Definition**

A polynomial $r$ is called reduced with respect to a set of non-zero polynomials $F = \{f_1, f_2, \ldots, f_s\}$ if

- $r = 0$ or
- no term of $r$ is a multiple of any $\text{in}_<(f_i)$.

**Definition**

If $f \rightarrow_F r$ and $r$ is reduced with respect to $F$ then $r$ is called a remainder for $f$ modulo $F$. 
The remainder of a polynomial $f$ modulo a set of non-zero polynomials may not be unique.

Example

Let $f = x_1 x_2 x_3 + 2x_1$ and $F = \{f_1 = x_1 x_2 - 1, f_2 = x_2 x_3 - x_1\}$ in $\mathbb{Q}[x_1, x_2, x_3]$ with the degree lexicographic monomial order with $x_1 > x_2 > x_3$. Then $f \rightarrow_{f_1} 2x_1 + x_3$ and $f \rightarrow_{f_2} x_1^2 + 2x_1$.

Note that both $2x_1 + x_3$ and $x_1^2 + 2x_1$ are reduced with respect to $F$, thus both are remainders for $f$ modulo $F$. 
Theorem

Let $I$ be a non-zero ideal in $k[x_1, \ldots, x_n]$. The set of non-zero polynomials $G = \{g_1, g_2, \cdots, g_t\} \subseteq I$ is a Gröbner basis for $I$ if and only if the remainder of any polynomial $f \in k[x_1, \ldots, x_n]$ by $G$ is unique.

Theorem

Let $I$ be a non-zero ideal in $k[x_1, \ldots, x_n]$. The set of non-zero polynomials $G = \{g_1, g_2, \cdots, g_t\} \subseteq I$ is a Gröbner basis for $I$ if and only if the remainder of any polynomial $f \in I$ by $G$ is zero.

The remainder of any polynomial modulo a Gröbner basis is a linear combination of standard monomials.
S-polynomials

**Definition (Buchberger)**

Let \( f, g \) be two non-zero polynomials in \( k[x_1, \ldots, x_n] \). Let 
\[
L = \text{LCM}(\text{in}_{<}(f), \text{in}_{<}(g)).
\]

The polynomial
\[
S(f, g) = \frac{L}{c_f \text{in}_{<}(f)} f - \frac{L}{c_g \text{in}_{<}(g)} g
\]
is called the S-polynomial of \( f \) and \( g \).

**Example**

Let \( f = 3x^2yz - y^3z^3, g = xy^2 + z^2 \) in the polynomial ring \( \mathbb{Q}[x, y, z] \) with the lexicographic monomial order with \( x > y > z \). Then 
\[
L = \text{LCM}(\text{in}_{<}(f), \text{in}_{<}(g)) = \text{LCM}(x^2yz, xy^2) = x^2y^2z
\]
and
\[
S(f, g) = \frac{x^2y^2z}{3x^2yz} f - \frac{x^2y^2z}{xy^2} g = -xz^3 - \frac{y^4z^3}{3}.
\]
Remark

The S-polynomial of $f$ and $g$ belongs to the ideal generated by $f$, $g$.

Theorem

Let $I$ be a non-zero ideal in $k[x_1, \ldots, x_n]$. The set of non-zero polynomials $G = \{g_1, g_2, \ldots, g_t\} \subset I$ is a Gröbner basis for $I$ if and only if the remainder of any polynomial $f \in I$ by $G$ is zero.

Theorem (Buchberger)

Let $I$ be a non-zero ideal in $K[x_1, \ldots, x_n]$. The set of non-zero polynomials $G = \{g_1, g_2, \ldots, g_t\} \subset I$ is a Gröbner basis for $I = \langle g_1, g_2, \ldots, g_t \rangle$ if and only if $S(f, g) \rightarrow_G 0$. 
Buchberger’s Algorithm

- INPUT: $F = \{f_1, f_2, \cdots, f_t\}$ a set of non-zero polynomials of $K[x_1, \ldots, x_n]$
- OUTPUT: $G = \{g_1, g_2, \cdots, g_s\}$ a Gröbner basis for $I = \langle f_1, f_2, \cdots, f_t \rangle$.
- SET: $G := F$, $S = \{S(f_i, f_j)|f_i \neq f_j \in G\}$
- WHILE $S \neq \emptyset$ DO
  - Choose any $S(f, g) \in S$
  - set $S : S := S \setminus \{S(f, g)\}$
  - $S(f, g) \rightarrow_G h$, where $h$ is the remainder modulo $G$
- IF $h \neq 0$ THEN
  - $S := S \cup \{S(u, h)|\text{for all } u \in G\}$
  - $G := G \cup \{h\}$. 

Apostolos Thoma  Toric ideals and Gröbner bases
Buchberger’s Algorithm

Let \( I = \langle x^2y + z, xz + y \rangle \) be an ideal in \( \mathbb{R}[x, y, z] \). Let \( \langle \text{deglex} \rangle \) be the degree lexicographic monomial order in \( \mathbb{R}[x, y, z] \) with \( x > y > z \).

- Set \( G_0 = \{ g_1 = x^2y + z, g_2 = xz + y \} \) and \( S_0 = \{ S(g_1, g_2) \} \)
- \( S_0 \neq \emptyset \). Reduce \( S(g_1, g_2) \) with respect to \( G_0 \): 
  \[ S(g_1, g_2) = \frac{x^2yz}{x^2y} (x^2y + z) - \frac{x^2yz}{xz} (xz + y) = -xy^2 + z^2 \rightarrow G_0 - xy^2 + z^2 \neq 0 \]
- Set \( G_1 = \{ g_1, g_2, g_3 = -xy^2 + z^2 \} \) and 
  \( S_1 = (S_0 - \{ S(g_1, g_2) \}) \cup \{ S(g_1, g_3), S(g_2, g_3) \} \).
- \( S_1 \neq \emptyset \). Reduce \( S(g_1, g_3) \) with respect to \( G_1 \): 
  \[ S(g_1, g_3) = \frac{x^2y^2}{x^2y} (x^2y + z) - \frac{x^2y^2}{-xy^2} (-xy^2 + z^2) = xz^2 + yz \rightarrow G_1 0 \]
- Set \( G_2 = G_1 \) and \( S_2 = S_1 - \{ S(g_1, g_2) \} = \{ S(g_2, g_3) \} \).
- \( S_2 \neq \emptyset \). Reduce \( S(g_2, g_3) \) with respect to \( G_2 \): 
  \[ S(g_2, g_3) = \frac{x^2yz}{xz} (xz + y) - \frac{x^2yz}{-xy^2} (-xy^2 + z^2) = y^3 + z^3 \rightarrow G_2 y^3 + z^3 \neq 0 \]
- Set \( G_3 = \{ g_1, g_2, g_3, g_4 = y^3 + z^3 \} \) and 
  \( S_3 = (S_2 - \{ S(g_2, g_3) \}) \cup \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} = \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} \).
Buchberger’s Algorithm

Let $I = \langle x^2 y + z, xz + y \rangle$ be an ideal in $\mathbb{R}[x, y, z]$. Let $<_{\text{deglex}}$ be the degree lexicographic monomial order in $\mathbb{R}[x, y, z]$ with $x > y > z$.

Set $G_0 = \{g_1 = x^2 y + z, g_2 = xz + y\}$ and $S_0 = \{S(g_1, g_2)\}$

$S_0 \neq \emptyset$. Reduce $S(g_1, g_2)$ with respect to $G_0$: $S(g_1, g_2) = \frac{x^2 yz}{x^2 y} (x^2 y + z) - \frac{x^2 yz}{xz} (xz + y) = -xy^2 + z^2 \rightarrow_{G_0} -xy^2 + z^2 \neq 0$

Set $G_1 = \{g_1, g_2, g_3 = -xy^2 + z^2\}$ and $S_1 = (S_0 - \{S(g_1, g_2)\}) \cup \{S(g_1, g_3), S(g_2, g_3)\}$.

$S_1 \neq \emptyset$. Reduce $S(g_1, g_3)$ with respect to $G_1$: $S(g_1, g_3) = \frac{x^2 y^2}{x^2 y} (x^2 y + z) - \frac{x^2 y^2}{-xy^2} (-xy^2 + z^2) = xz^2 + yz \rightarrow_{G_1} 0$

Set $G_2 = G_1$ and $S_2 = S_1 - \{S(g_1, g_2)\} = \{S(g_2, g_3)\}$.

$S_2 \neq \emptyset$. Reduce $S(g_2, g_3)$ with respect to $G_2$: $S(g_2, g_3) = \frac{xy^2 z}{xz} (xz + y) - \frac{xy^2 z}{-xy^2} (-xy^2 + z^2) = y^3 + z^3 \rightarrow_{G_2} y^3 + z^3 \neq 0$

Set $G_3 = \{g_1, g_2, g_3, g_4 = y^3 + z^3\}$ and $S_3 = (S_2 - \{S(g_2, g_3)\}) \cup \{S(g_1, g_4), S(g_2, g_4), S(g_3, g_4)\} = \{S(g_1, g_4), S(g_2, g_4), S(g_3, g_4)\}$.
Buchberger’s Algorithm

Let \( I = \langle x^2y + z, xz + y \rangle \) be an ideal in \( \mathbb{R}[x, y, z] \). Let \(<_{\text{deglex}}\) be the degree lexicographic monomial order in \( \mathbb{R}[x, y, z] \) with \( x > y > z \).

- Set \( G_0 = \{ g_1 = x^2y + z, g_2 = xz + y \} \) and \( S_0 = \{ S(g_1, g_2) \} \)
- \( S_0 \neq \emptyset \). Reduce \( S(g_1, g_2) \) with respect to \( G_0 \): \( S(g_1, g_2) = \frac{x^2yz}{x^2y}(x^2y + z) - \frac{x^2yz}{xz}(xz + y) = -xy^2 + z^2 \rightarrow G_0 \) \( -xy^2 + z^2 \neq 0 \)
- Set \( G_1 = \{ g_1, g_2, g_3 = -xy^2 + z^2 \} \) and \( S_1 = (S_0 - \{ S(g_1, g_2) \}) \cup \{ S(g_1, g_3), S(g_2, g_3) \} \).
- \( S_1 \neq \emptyset \). Reduce \( S(g_1, g_3) \) with respect to \( G_1 \): \( S(g_1, g_3) = \frac{x^2y^2}{x^2y}(x^2y + z) - \frac{x^2y^2}{xy^2}(-xy^2 + z^2) = xz^2 + yz \rightarrow G_1 \) \( 0 \)
- Set \( G_2 = G_1 \) and \( S_2 = S_1 - \{ S(g_1, g_2) \} = \{ S(g_2, g_3) \} \).
- \( S_2 \neq \emptyset \). Reduce \( S(g_2, g_3) \) with respect to \( G_2 \): \( S(g_2, g_3) = \frac{xy^2z}{xz}(xz + y) - \frac{xy^2z}{-xy^2}(-xy^2 + z^2) = y^3 + z^3 \rightarrow G_2 \) \( y^3 + z^3 \neq 0 \)
- Set \( G_3 = \{ g_1, g_2, g_3, g_4 = y^3 + z^3 \} \) and \( S_3 = (S_2 - \{ S(g_2, g_3) \}) \cup \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} = \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} \).
Let $I = \langle x^2 y + z, xz + y \rangle$ be an ideal in $\mathbb{R}[x, y, z]$. Let $<_{\text{deglex}}$ be the degree lexicographic monomial order in $\mathbb{R}[x, y, z]$ with $x > y > z$.

- Set $G_0 = \{g_1 = x^2 y + z, g_2 = xz + y\}$ and $S_0 = \{S(g_1, g_2)\}$
- $S_0 \neq \emptyset$. Reduce $S(g_1, g_2)$ with respect to $G_0$: $S(g_1, g_2) = \frac{x^2 y z}{x^2 y} (x^2 y + z) - \frac{x^2 y z}{xz} (xz + y) = -xy^2 + z^2 \rightarrow G_0 - xy^2 + z^2 \neq 0$
- Set $G_1 = \{g_1, g_2, g_3 = -xy^2 + z^2\}$ and $S_1 = (S_0 - \{S(g_1, g_2)\}) \cup \{S(g_1, g_3), S(g_2, g_3)\}$.
- $S_1 \neq \emptyset$. Reduce $S(g_1, g_3)$ with respect to $G_1$: $S(g_1, g_3) = \frac{x^2 y^2}{x^2 y} (x^2 y + z) - \frac{x^2 y^2}{-xy^2} (-xy^2 + z^2) = xz^2 + yz \rightarrow G_1 0$
- Set $G_2 = G_1$ and $S_2 = S_1 - \{S(g_1, g_2)\} = \{S(g_2, g_3)\}$.
- $S_2 \neq \emptyset$. Reduce $S(g_2, g_3)$ with respect to $G_2$: $S(g_2, g_3) = \frac{xy^2 z}{xz} (xz + y) - \frac{xy^2 z}{-xy^2} (-xy^2 + z^2) = y^3 + z^3 \rightarrow G_2 y^3 + z^3 \neq 0$
- Set $G_3 = \{g_1, g_2, g_3, g_4 = y^3 + z^3\}$ and $S_3 = (S_2 - \{S(g_2, g_3)\}) \cup \{S(g_1, g_4), S(g_2, g_4), S(g_3, g_4)\} = \{S(g_1, g_4), S(g_2, g_4), S(g_3, g_4)\}$. 
Buchberger’s Algorithm

Let \( I = \langle x^2y + z, xz + y \rangle \) be an ideal in \( \mathbb{R}[x, y, z] \). Let \( <_{\text{deglex}} \) be the degree lexicographic monomial order in \( \mathbb{R}[x, y, z] \) with \( x > y > z \).

- Set \( G_0 = \{ g_1 = x^2y + z, g_2 = xz + y \} \) and \( S_0 = \{ S(g_1, g_2) \} \)
- \( S_0 \neq \emptyset \). Reduce \( S(g_1, g_2) \) with respect to \( G_0 \): \( S(g_1, g_2) = \frac{x^2yz}{x^2y} (x^2y + z) - \frac{x^2yz}{xz} (xz + y) = -xy^2 + z^2 \rightarrow_{G_0} -xy^2 + z^2 \neq 0 \)
- Set \( G_1 = \{ g_1, g_2, g_3 = -xy^2 + z^2 \} \) and \( S_1 = (S_0 - \{ S(g_1, g_2) \}) \cup \{ S(g_1, g_3), S(g_2, g_3) \} \).
- \( S_1 \neq \emptyset \). Reduce \( S(g_1, g_3) \) with respect to \( G_1 \):
  \[ S(g_1, g_3) = \frac{x^2y^2}{x^2y} (x^2y + z) - \frac{x^2y^2}{-xy} (-xy^2 + z^2) = xz^2 + yz \rightarrow_{G_1} 0 \]
- Set \( G_2 = G_1 \) and \( S_2 = S_1 - \{ S(g_1, g_2) \} = \{ S(g_2, g_3) \} \).
- \( S_2 \neq \emptyset \). Reduce \( S(g_2, g_3) \) with respect to \( G_2 \): \( S(g_2, g_3) = \frac{xy^2z}{xz} (xz + y) - \frac{xy^2z}{-xy} (-xy^2 + z^2) = y^3 + z^3 \rightarrow_{G_2} y^3 + z^3 \neq 0 \)
- Set \( G_3 = \{ g_1, g_2, g_3, g_4 = y^3 + z^3 \} \) and \( S_3 = (S_2 - \{ S(g_2, g_3) \}) \cup \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} = \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} \).
Let \( I = \langle x^2 y + z, xz + y \rangle \) be an ideal in \( \mathbb{R}[x, y, z] \). Let \( \text{deglex} \) be the degree lexicographic monomial order in \( \mathbb{R}[x, y, z] \) with \( x > y > z \).

- Set \( G_0 = \{ g_1 = x^2 y + z, g_2 = xz + y \} \) and \( S_0 = \{ S(g_1, g_2) \} \)
- \( S_0 \neq \emptyset \). Reduce \( S(g_1, g_2) \) with respect to \( G_0 \): \( S(g_1, g_2) = \frac{x^2 y z}{x^2 y} (x^2 y + z) - \frac{x^2 y z}{xz} (xz + y) = -xy^2 + z^2 \rightarrow G_0 -xy^2 + z^2 \neq 0 \)
- Set \( G_1 = \{ g_1, g_2, g_3 = -xy^2 + z^2 \} \) and \( S_1 = (S_0 - \{ S(g_1, g_2) \}) \cup \{ S(g_1, g_3), S(g_2, g_3) \} \).
- \( S_1 \neq \emptyset \). Reduce \( S(g_1, g_3) \) with respect to \( G_1 \):
  \[
  S(g_1, g_3) = \frac{x^2 y^2}{x^2 y} (x^2 y + z) - \frac{x^2 y^2}{-xy^2} (-xy^2 + z^2) = xz^2 + yz \rightarrow G_1 0
  \]
- Set \( G_2 = G_1 \) and \( S_2 = S_1 - \{ S(g_1, g_2) \} = \{ S(g_2, g_3) \} \).
- \( S_2 \neq \emptyset \). Reduce \( S(g_2, g_3) \) with respect to \( G_2 \):
  \[
  S(g_2, g_3) = \frac{xy^2 z}{xz} (xz + y) - \frac{xy^2 z}{-xy^2} (-xy^2 + z^2) = y^3 + z^3 \rightarrow G_2 y^3 + z^3 \neq 0
  \]
- Set \( G_3 = \{ g_1, g_2, g_3, g_4 = y^3 + z^3 \} \) and \( S_3 = (S_2 - \{ S(g_2, g_3) \}) \cup \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} = \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} \).
Let \( I = \langle x^2y + z, xz + y \rangle \) be an ideal in \( \mathbb{R}[x, y, z] \). Let \( \langle \text{deglex} \rangle \) be the degree lexicographic monomial order in \( \mathbb{R}[x, y, z] \) with \( x > y > z \).

Set \( G_0 = \{ g_1 = x^2y + z, g_2 = xz + y \} \) and \( S_0 = \{ S(g_1, g_2) \} \)

\( S_0 \neq \emptyset \). Reduce \( S(g_1, g_2) \) with respect to \( G_0 \): \( S(g_1, g_2) = \frac{x^2yz}{x^2y}(x^2y + z) - \frac{x^2yz}{xz}(xz + y) = -xy^2 + z^2 \rightarrow_{G_0} -xy^2 + z^2 \neq 0 \)

Set \( G_1 = \{ g_1, g_2, g_3 = -xy^2 + z^2 \} \) and \( S_1 = (S_0 - \{ S(g_1, g_2) \}) \cup \{ S(g_1, g_3), S(g_2, g_3) \} \).

\( S_1 \neq \emptyset \). Reduce \( S(g_1, g_3) \) with respect to \( G_1 \):
\[
S(g_1, g_3) = \frac{x^2y^2}{x^2y}(x^2y + z) - \frac{x^2y^2}{-xy^2}(-xy^2 + z^2) = xz^2 + yz \rightarrow_{G_1} 0
\]

Set \( G_2 = G_1 \) and \( S_2 = S_1 - \{ S(g_1, g_2) \} = \{ S(g_2, g_3) \} \).

\( S_2 \neq \emptyset \). Reduce \( S(g_2, g_3) \) with respect to \( G_2 \): \( S(g_2, g_3) = \frac{xy^2z}{xz}(xz + y) - \frac{xy^2z}{-xy^2}(-xy^2 + z^2) = y^3 + z^3 \rightarrow_{G_2} y^3 + z^3 \neq 0 \)

Set \( G_3 = \{ g_1, g_2, g_3, g_4 = y^3 + z^3 \} \) and \( S_3 = (S_2 - \{ S(g_2, g_3) \}) \cup \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} = \{ S(g_1, g_4), S(g_2, g_4), S(g_3, g_4) \} \).
Buchberger’s Algorithm

\[ S(g_1, g_4) \rightarrow_{G_3} G_3 0, \]
\[ S(g_2, g_4) \rightarrow_{G_3} G_3 0, \]
\[ S(g_3, g_4) \rightarrow_{G_3} G_3 0. \]

So after three more steps \( S = \emptyset \) and therefore

\[ \{ g_1, g_2, g_3, g_4 \} \]

is a Gröbner basis for \( I \).
For any nonzero ideal $I$ and for any monomial order there exist Gröbner bases for $I$. Actually there exist infinitely many.

**Definition**

A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is called a reduced Gröbner basis for $I$ if
- the initial coefficient of $g_i$ is equal to 1 for all $i \in \{1, \ldots, t\}$ and
- no monomial in $g_i$ is divisible by any $in_<(g_j)$ for any $j \neq i$.

**Theorem**

Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$ and $I_A$ a toric ideal. Then $\{x_1^{u_1^+} - x_1^{u_1^-}, x_2^{u_2^+} - x_2^{u_2^-}, \ldots, x_s^{u_s^+} - x_s^{u_s^-}\}$ is reduced Gröbner basis with respect to the monomial order $<$ if and only if $x_1^{u_1^+}, x_2^{u_2^+}, \ldots, x_s^{u_s^+}$ are the minimal monomial generators of $in_<(I_A)$ and $x_1^{u_1^-}, x_2^{u_2^-}, \ldots, x_s^{u_s^-}$ are standard monomials.
Theorem

(Buchberger) Let $<$ be a monomial order on $k[x_1, \ldots, x_n]$ and $I$ a nonzero ideal. Then $I$ has a unique reduced Gröbner basis with respect to the monomial order $<$. 
Elimination order

We consider two sets of variables $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$. Let $<_x$ be any monomial order on the $x$ variables and let $<_y$ any monomial order on the $y$ variables. We can define a new monomial order:

**Definition**

Let $x^a, x^b$ be monomials in the $x$ variables and $y^c, y^d$ be monomials in the $y$ variables. We define

\[ x^a y^c < x^b y^d \]

if and only if $x^a <_x x^b$ or $x^a = x^b$ and $y^c <_y y^d$.

The new monomial order is called an elimination order with the $x$ variables larger than the $y$ variables.

If the $<_x$ monomial order is defined by a matrix $A$ and the $<_y$ monomial order is defined by a matrix $B$ then the elimination order is defined by the matrix

\[
\begin{pmatrix}
A & 0 \\
0 & B
\end{pmatrix}.
\]
Theorem

Let $I$ be a nonzero ideal of $K[x_1, \cdots, x_n, y_1, \cdots, y_m]$ and let $<$ be an elimination order with the $x$ variables larger than the $y$ variables. Let $G = \{g_1, g_2, \cdots, g_t\}$ be a Gröbner basis for $I$. Then $G \cap K[y_1, \cdots, y_m]$ is a Gröbner basis for the ideal $I \cap K[y_1, \cdots, y_m]$. 
Although $k[x_1, \ldots, x_n]$, for $n \geq 2$ has infinitely many different monomial orders for a fixed nonzero ideal $I$ there exist finitely many different reduced Gröbner bases for $I$.

**Definition**

The universal Gröbner basis of an ideal $I$ is the union of all reduced Gröbner bases $G_<$ of the ideal $I$ as $<$ runs over all monomial orders and is denoted by $UGB(I)$.

The universal Gröbner basis is a finite subset of $I$ and it is a Gröbner basis for $I$ with respect to all monomial orders simultaneously.

**Theorem**

(V. Weispfenning and N. Schwartz) *Universal Gröbner basis exists for every ideal in $k[x_1, \ldots, x_n]$.***
Gröbner bases of toric ideals

- Toric ideals are binomial ideals
- Let \( f = x^{u^+} - x^{u^-}, g = x^{v^+} - x^{v^-} \) be two non-zero binomials in \( k[x_1, \ldots, x_n] \) with \( x^{v^+} > x^{v^-} \) and such that \( x^{v^+} | x^{u^+} \). Then the remainder of the division is zero or a binomial.

\[
(f \rightarrow g) h = (x^{u^+} - x^{u^-}) - \frac{x^{u^+}}{x^{v^+}}(x^{v^+} - x^{v^-}) = \frac{x^{u^+}}{x^{v^+}}x^{v^-} - x^{u^-}.
\]

- Let \( f = x^{u^+} - x^{u^-}, g = x^{v^+} - x^{v^-} \) be two non-zero binomials in \( k[x_1, \ldots, x_n] \) with \( x^{u^+} > x^{u^-}, x^{v^+} > x^{v^-} \). Let \( L = \text{LCM}(x^{u^+}, x^{v^+}) \). The polynomial

\[
S(f, g) = \frac{L}{x^{u^+}}(x^{u^+} - x^{u^-}) - \frac{L}{x^{v^+}}(x^{v^+} - x^{v^-}) = \frac{L}{x^{v^+}}x^{v^-} - \frac{L}{x^{u^+}}x^{u^-}
\]

is the S-polynomial of \( f \) and \( g \) and it is binomial.

- Any reduced Gröbner basis of a toric ideal consists of binomials.
Any reduced Gröbner basis of a toric ideal consists of binomials. What kind of binomials?

**Theorem (B. Sturmfels)**

*For any toric ideal $I_A$ we have that the Universal Gröbner basis is a subset of the Graver basis.*
Any reduced Gröbner basis of a toric ideal consists of binomials. What kind of binomials?

**Theorem (B. Sturmfels)**

*For any toric ideal $I_A$ we have that the Universal Gröbner basis is a subset of the Graver basis.*
Proof.

Suppose that there exists a binomial $x^{u+} - x^{u-}$ in the Universal Gröbner basis which does not belong to the Graver. Then

1. there exists a monomial order $<$ such that $x^{u+} - x^{u-}$ is in the reduced Gröbner basis with respect to the monomial order $>$ and
2. there exists a non-zero $x^{v+} - x^{v-} \in I_A$, with $x^{v+} - x^{v-} \neq x^{u+} - x^{u-}$ such that $x^{v+} \mid x^{u+}$ and $x^{v-} \mid x^{u-}$.

The first condition means that $x^{u+}$ is a minimal generator of $\text{in}_<(I_A)$ and $x^{u-}$ is a standard monomial.

For $x^{v+} - x^{v-} \in I_A$ there are two cases:

1. $x^{v+} > x^{v-}$ implies $x^{v+} \in \text{in}_<(I_A)$ and divides one of the minimal generators of $\text{in}_<(I_A)$, the $x^{u+}$. Therefore $x^{v+} = x^{u+}$. But then $(x^{v+} - x^{v-}) - (x^{u+} - x^{u-}) = x^{u-} - x^{v-} \in I_A$ is non-zero and $x^{u-} > x^{v-}$ (since $x^{v-} \mid x^{u-}$). Therefore $x^{u-} \in \text{in}_<(I_A)$. A contradiction since $x^{u-}$ is a standard monomial.

2. $x^{v-} > x^{v+}$ then $x^{v-} \in \text{in}_<(I_A)$ and divides a standard monomial, the $x^{u-}$. Contradiction.
Proof.

Suppose that there exists a binomial $x^{u^+} - x^{u^-}$ in the Universal Gröbner basis which does not belong to the Graver. Then

1. there exists a monomial order $<$ such that $x^{u^+} - x^{u^-}$ is in the reduced Gröbner basis with respect to the monomial order $>$ and
2. there exists a non-zero $x^{v^+} - x^{v^-} \in I_A$, with $x^{v^+} - x^{v^-} \neq x^{u^+} - x^{u^-}$ such that $x^{v^+} | x^{u^+}$ and $x^{v^-} | x^{u^-}$.

The first condition means that $x^{u^+}$ is a minimal generator of $in_<(I_A)$ and $x^{u^-}$ is a standard monomial.

For $x^{v^+} - x^{v^-} \in I_A$ there are two cases:

1. $x^{v^+} > x^{v^-}$ implies $x^{v^+} \in in_<(I_A)$ and divides one of the minimal generators of $in_<(I_A)$, the $x^{u^+}$. Therefore $x^{v^+} = x^{u^+}$. But then $(x^{v^+} - x^{v^-}) - (x^{u^+} - x^{u^-}) = x^{u^-} - x^{v^-} \in I_A$ is non-zero and $x^{u^-} > x^{v^-}$ (since $x^{v^-} | x^{u^-}$). Therefore $x^{u^-} \in in_<(I_A)$. A contradiction since $x^{u^-}$ is a standard monomial.
2. $x^{v^-} > x^{v^+}$ then $x^{v^-} \in in_<(I_A)$ and divides a standard monomial, the $x^{u^-}$. Contradiction.