GRÖBNER BASES AND APPLICATIONS

Manuel Kauers · Institute for Algebra · JKU

Finite sets of numbers can be viewed as solutions of polynomial equations:

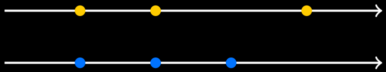
Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

$q = (x-1)(x-2)(x-3) = 0$

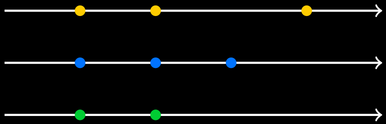


Finite sets of numbers can be viewed as solutions of polynomial equations:

$$p = (x-1)(x-2)(x-4) = 0$$

$$q = (x-1)(x-2)(x-3) = 0$$

Intersection: $\gcd(p, q) = 0$



Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

$q = (x-1)(x-2)(x-3) = 0$

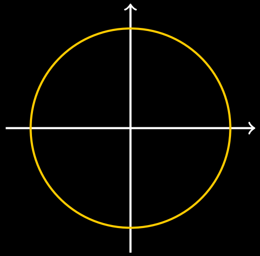
Intersection: $\gcd(p, q) = 0$

Union: $\operatorname{lcm}(p, q) = 0$

In the case of two variables, the solution set of a single polynomial is a curve.

In the case of two variables, the solution set of a single polynomial is a curve.

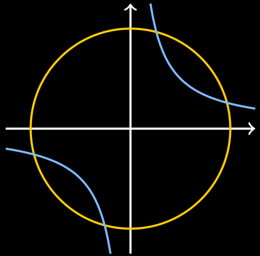
$$x^2 + y^2 - 4 = 0$$



In the case of two variables, the solution set of a single polynomial is a curve.

$$x^2 + y^2 - 4 = 0$$

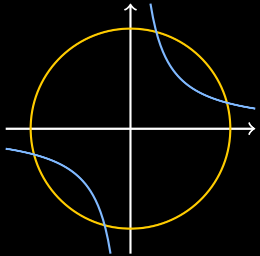
$$xy - 1 = 0$$



In the case of two variables, the solution set of a single polynomial is a curve.

$$x^2 + y^2 - 4 = 0$$

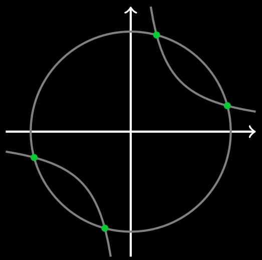
$$xy - 1 = 0$$



Any finite set of points can be viewed as the intersection of such curves.

In the case of two variables, the solution set of a single polynomial is a curve.

$$\begin{gathered} x^2 + y^2 - 4 = 0 \\ \wedge \\ xy - 1 = 0 \end{gathered}$$



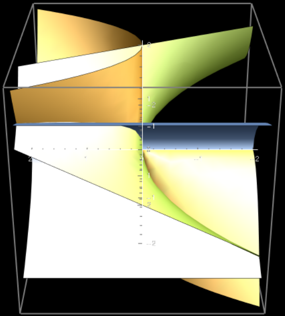
Any finite set of points can be viewed as the intersection of such curves.

A polynomial in three variables describes a surface.

$$xz - y^2 = 0$$

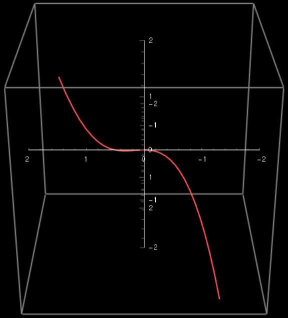
$$y - z^2 = 0$$

$$x - yz = 0$$



A polynomial in three variables describes a surface.

$$xz - y^2 = 0$$
$$\wedge$$
$$y - z^2 = 0$$
$$\wedge$$
$$x - yz = 0$$



Curves and finite sets of points can be viewed as intersections of such surfaces.

Let K be a field (e.g., $\mathsf{K} = \mathbb{Q}$), and let $\mathsf{K}[X] = \mathsf{K}[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Let K be a field (e.g., $\mathsf{K} = \mathbb{Q}$), and let $\mathsf{K}[X] = \mathsf{K}[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Polynomial equations have implications:

1. $u = 0$ and $v = 0 \Rightarrow u + v = 0$
2. $u = 0$ and v arbitrary $\Rightarrow uv = 0$.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Definition A set $I \subseteq K[X]$ is called an ideal iff

1. $u, v \in I \Rightarrow u + v \in I$
2. $u \in I, v \in K[X] \Rightarrow uv \in I$.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Definition A set $I \subseteq K[X]$ is called an ideal iff

1. $u, v \in I \Rightarrow u + v \in I$
2. $u \in I, v \in K[X] \Rightarrow uv \in I$.

If I is the smallest ideal containing $p_1, \ldots, p_k$, we write

$$I = \langle p_1, \ldots, p_k \rangle$$

and call $\{p_1, \ldots, p_k\}$ a basis for I.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \dots, x_n]$ be the set of polynomials in $x_1, \dots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Definition A set $I \subseteq K[X]$ is called an ideal iff

1. $u, v \in I \Rightarrow u + v \in I$
2. $u \in I, v \in K[X] \Rightarrow uv \in I$.

If I is the smallest ideal containing $p_1, \dots, p_k$, we write

$$\boxed{I = \langle p_1, \dots, p_k \rangle} \text{ — “theory”}$$

and call $\{p_1, \dots, p_k\}$ a basis for I.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Definition A set $I \subseteq K[X]$ is called an ideal iff

1. $u, v \in I \Rightarrow u + v \in I$
2. $u \in I, v \in K[X] \Rightarrow uv \in I$.

If I is the smallest ideal containing $p_1, \ldots, p_k$, we write

$$\boxed{I = \langle p_1, \ldots, p_k \rangle} \text{ — “theory”}$$

and call $\underbrace{\boxed{\{p_1, \ldots, p_k\}}}_{\text{“axioms”}}$ a basis for I.

Let K be a field (e.g., $K = \mathbb{Q}$), and let $K[X] = K[x_1, \ldots, x_n]$ be the set of polynomials in $x_1, \ldots, x_n$ with coefficients in K.

Example: $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \in \mathbb{Q}[x, y]$.

Definition A set $I \subseteq K[X]$ is called an ideal iff

1. $u, v \in I \Rightarrow u + v \in I$
2. $u \in I, v \in K[X] \Rightarrow uv \in I$.

"deduction rules"

If I is the smallest ideal containing $p_1, \ldots, p_k$, we write

$$\boxed{I = \langle p_1, \ldots, p_k \rangle}$$

"theory"

and call $\boxed{\{p_1, \ldots, p_k\}}$ a basis for I.

"axioms"

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \notin I$

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \notin I$
- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \in I$

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \notin I$
- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \in I$

Note:

$$p \in \langle p_1, \ldots, p_k \rangle \iff \exists\ q_1, \ldots, q_k : p = q_1p_1 + \cdots + q_kp_k$$

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \notin I$
- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \in I$

Note:

$$p \in \langle p_1, \ldots, p_k \rangle \iff \exists\, q_1, \ldots, q_k : p = q_1p_1 + \cdots + q_kp_k$$

Example:

$$\begin{aligned} &3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \\ &= \left(3x^2y^2 + 8xy\right)x + \left(7x^2y^2 - 4x + 8y^2\right)y \end{aligned}$$

Example: For $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$ we have

- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17 \notin I$
- $3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \in I$

Note:

$$p \in \langle p_1, \dots, p_k \rangle \iff \exists\, q_1, \dots, q_k : p = q_1p_1 + \cdots + q_kp_k$$

Example:

$$\begin{aligned} &3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 \\ &= \left(3x^2y^2 + 8xy\right)x + \left(7x^2y^2 - 4x + 8y^2\right)y \\ &= \left(7xy^3 - 4y\right)x + \left(3x^3y + 8x^2 + 8y^2\right)y \end{aligned}$$

Note: Also the basis of an ideal is not unique.

Note: Also the basis of an ideal is not unique.

Example: $\langle x^2 + y^2 - 4,\ \ xy - 1\rangle = \langle y^4 - 4y^2 + 1,\ \ y^3 - 4y + x\rangle$.

Note: Also the basis of an ideal is not unique.

Example: $\langle x^2 + y^2 - 4,\ \ xy - 1\rangle = \langle y^4 - 4y^2 + 1,\ \ y^3 - 4y + x\rangle$.

Proof:

Note: Also the basis of an ideal is not unique.

Example: $\langle \underbrace{x^2+y^2-4}_{p_1},\ \underbrace{xy-1}_{p_2} \rangle = \langle \underbrace{y^4-4y^2+1}_{q_1},\ \underbrace{y^3-4y+x}_{q_2} \rangle$.

Proof:

Note: Also the basis of an ideal is not unique.

Example: $\langle \underbrace{x^2+y^2-4}_{p_1},\ \underbrace{xy-1}_{p_2} \rangle = \langle \underbrace{y^4-4y^2+1}_{q_1},\ \underbrace{y^3-4y+x}_{q_2} \rangle.$

Proof:

"$\subseteq$" $\quad p_1 = (y^2-4)\, q_1 + (x+4y-y^3)\, q_2,$

$p_2 = -q_1 + y\, q_2.$

Note: Also the basis of an ideal is not unique.

Example: $\langle \underbrace{x^2 + y^2 - 4}_{p_1}, \ \underbrace{xy - 1}_{p_2} \rangle = \langle \underbrace{y^4 - 4y^2 + 1}_{q_1}, \ \underbrace{y^3 - 4y + x}_{q_2} \rangle$.

Proof:

"$\subseteq$" $\quad p_1 = (y^2 - 4)\, q_1 + (x + 4y - y^3)\, q_2,$
$\quad p_2 = -q_1 + y\, q_2.$

"$\supseteq$" $\quad q_1 = y^2\, p_1 - (xy + 1)\, p_2,$
$\quad q_2 = y\, p_1 - x\, p_2.$ ∎

Note: Also the basis of an ideal is not unique.

Example: $\langle \underbrace{x^2+y^2-4}_{p_1},\ \underbrace{xy-1}_{p_2} \rangle = \langle \underbrace{y^4-4y^2+1}_{q_1},\ \underbrace{y^3-4y+x}_{q_2} \rangle.$

Proof:

"$\subseteq$" $\quad p_1 = (y^2-4)\,q_1 + (x+4y-y^3)\,q_2,$

$\qquad p_2 = -q_1 + y\,q_2.$

"$\supseteq$" $\quad q_1 = y^2\,p_1 - (xy+1)\,p_2,$

$\qquad q_2 = y\,p_1 - x\,p_2.$ $\blacksquare$

Among all the bases of a given ideal, the Gröbner basis is one that satisfies a certain minimality condition.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., $x^2 y$ and $x y^2$ are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., $x^2 y$ and xy^2 are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

Example: $\boxed{3x^3y^2} + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17.$

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

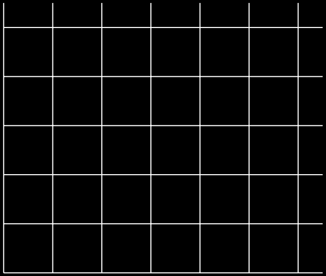
Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

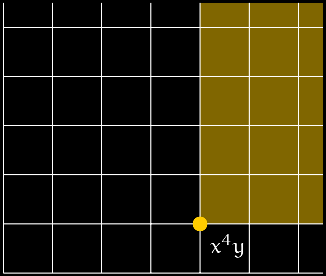
Example: $\boxed{3x^3y^2} + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17$.

Among all the bases of an ideal, the Gröbner basis is such that the leading terms of its elements are as small as possible.

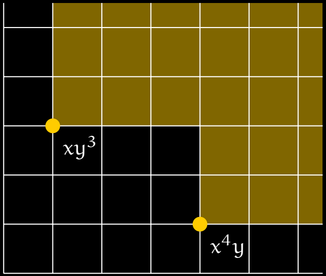
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



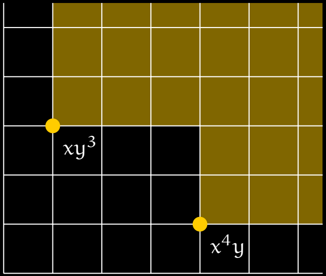
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.

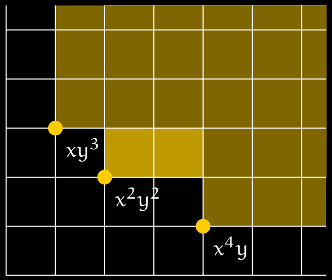


If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



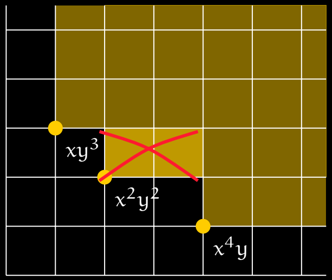
In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

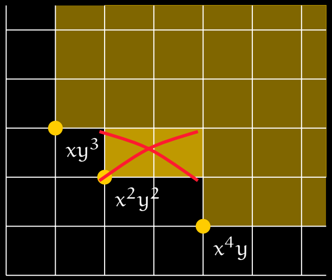
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

The basis is called a Gröbner basis if this does not happen.

If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



$\{g_1, \ldots, g_k\}$ is a Gröbner basis
$\iff \forall\, p \in \langle g_1, \ldots, g_k \rangle \setminus \{0\}\ \exists\, i \in \{1, \ldots, k\} : \mathrm{Head}(g_i) \mid \mathrm{Head}(p).$

Fact 1: Every ideal $\mathrm{I} \subseteq \mathrm{K}[\mathrm{X}]$ has a finite Gröbner basis

Fact 1: Every ideal $\mathrm{I} \subseteq \mathrm{K}[\mathrm{X}]$ has a finite Gröbner basis

Fact 2: The Gröbner basis is essentially unique

Fact 1: Every ideal $I \subseteq K[X]$ has a finite Gröbner basis

Fact 2: The Gröbner basis is essentially unique

Fact 3: Given an arbitrary basis, a Gröbner basis can be computed

Fact 1: Every ideal $I \subseteq K[X]$ has a finite Gröbner basis

Fact 2: The Gröbner basis is essentially unique

Fact 3: Given an arbitrary basis, a Gröbner basis can be computed

Fact 4: The computation of a Gröbner basis is a hard problem

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim \, = K[X]/I$ is a ring.

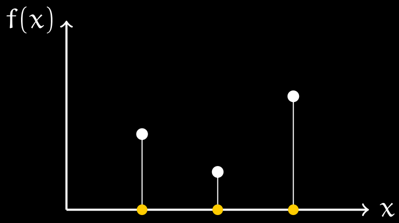
Its elements can be interpreted as polynomial functions restricted to the zero set of I.

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

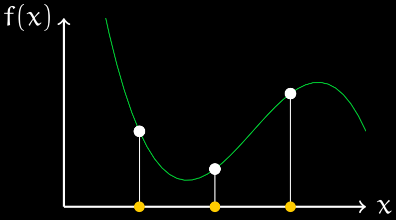


Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/{\sim} = K[X]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

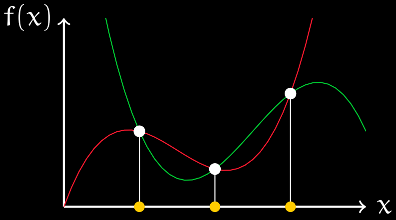


Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim \; = K[X]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

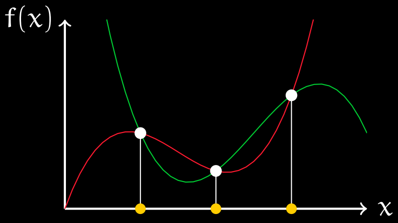


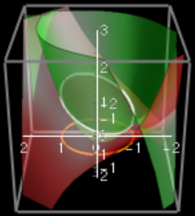
Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\!\sim\, = K[X]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.



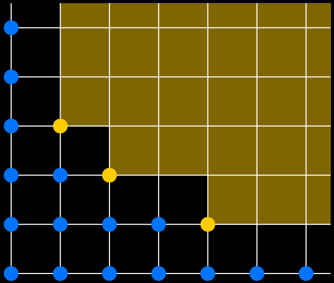


Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\!\sim\; = K[X]/I$ is a ring.

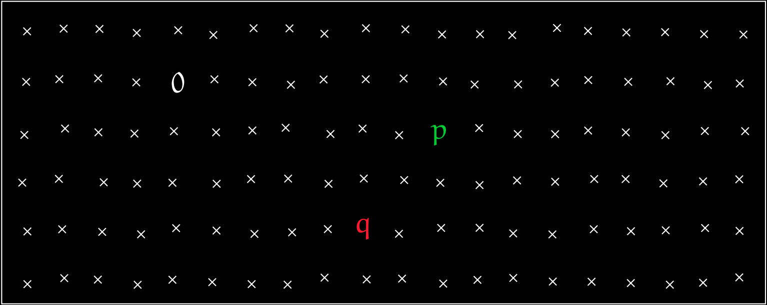
The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.



Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim \, = K[X]/I$ is a ring.

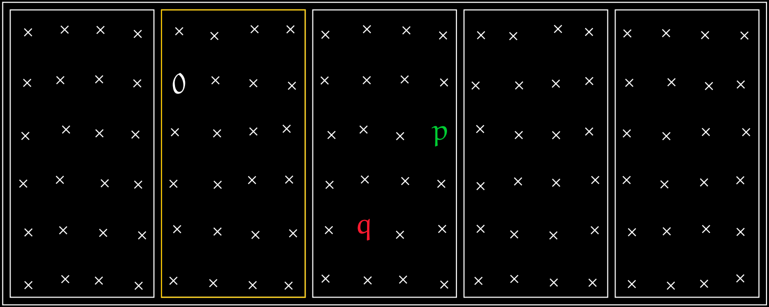


$K[X]$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

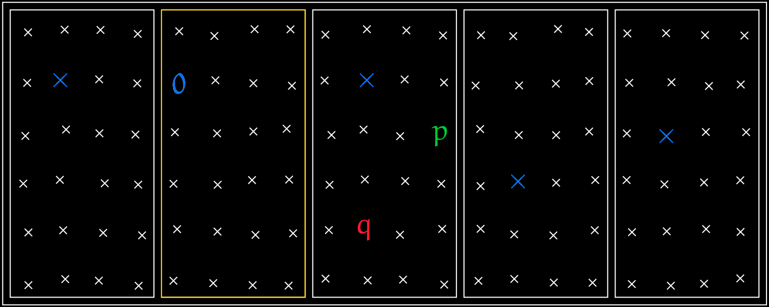


$K[X]/I$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\!\sim\, = K[X]/I$ is a ring.

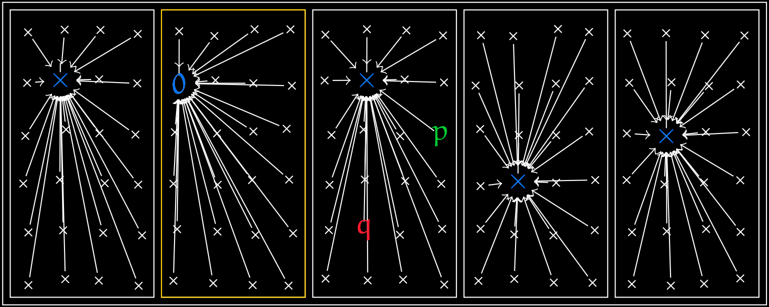


$K[X]/I$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.



$K[X]/I$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/{\sim} = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim \; = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

We write $\mathrm{red}(p, I)$ for the unique representative of the equivalence class $p \bmod I$ which only contains blue terms.

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/{\sim} = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

We write $\mathrm{red}(p, I)$ for the unique representative of the equivalence class p mod I which only contains blue terms.

Examples:

- $\mathrm{red}(3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17, \langle x, y\rangle) = -17$
- $\mathrm{red}(3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3, \langle x, y\rangle) = 0$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

We write $\mathrm{red}(p, I)$ for the unique representative of the equivalence class p mod I which only contains blue terms.

Examples:

- $\mathrm{red}(3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17, \langle x, y\rangle) = -17$
- $\mathrm{red}(3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3, \langle x, y\rangle) = 0$
- $\mathrm{red}(3x^3y^2 + 7x^2y^3 + 8x^2y - 4xy + 8y^3, \langle x^2 + y^2 - 1, y^7 - 3\rangle)$ $= 3xy^2 - 13xy - 21y^2 + 8y + 21$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\!\sim\; = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

We write $\mathsf{red}(p, I)$ for the unique representative of the equivalence class p mod I which only contains blue terms.

Fact 5: $p \sim q \iff \mathsf{red}(p, I) = \mathsf{red}(q, I)$.
In particular, $p \in I \iff \mathsf{red}(p, I) = 0$

Fix an ideal $I \subseteq K[X]$ and define

$$p \sim q \iff p - q \in I.$$

Then $K[X]/\sim = K[X]/I$ is a ring.

The ideal basis is a Gröbner basis iff each equivalence class contains exactly one polynomial with only blue terms.

We write $\text{red}(p, I)$ for the unique representative of the equivalence class p mod I which only contains blue terms.

Fact 5: $p \sim q \iff \text{red}(p, I) = \text{red}(q, I)$.
In particular, $p \in I \iff \text{red}(p, I) = 0$

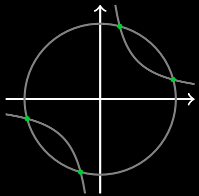
Fact 6: The function $\text{red}(\cdot, I)$ is computable

Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Example:

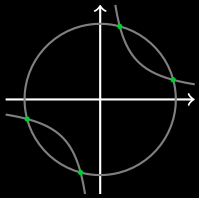
$$\langle x^2 + y^2 - 4, xy - 1\rangle \cap \mathbb{Q}[x]$$



Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Example:

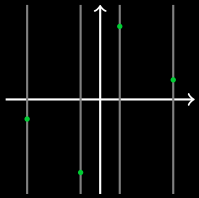
$$\langle x^2 + y^2 - 4, xy - 1 \rangle \cap \mathbb{Q}[x]$$
$$= \langle x^4 - 4x^2 + 1 \rangle \subseteq \mathbb{Q}[x]$$



Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Example:

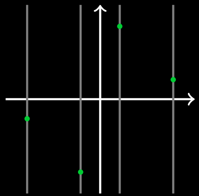
$$\langle x^2 + y^2 - 4, xy - 1\rangle \cap \mathbb{Q}[x]$$
$$= \langle x^4 - 4x^2 + 1\rangle \subseteq \mathbb{Q}[x]$$



Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Example:

$$\langle x^2 + y^2 - 4, xy - 1 \rangle \cap \mathbb{Q}[x]$$
$$= \langle x^4 - 4x^2 + 1 \rangle \subseteq \mathbb{Q}[x]$$



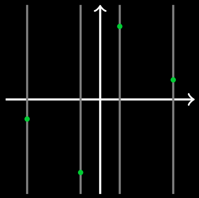
Fact 7*: If G is a Gröbner basis of I, then $G \cap K[X_*]$ is a Gröbner basis of $I \cap K[X_*]$, where $X_* \subseteq \{x_1, \ldots, x_n\}$

* only works for suitably chosen term orders.

Using the elimination property, we can find elements of an ideal which only contain some of the variables.

Example:

$$\langle x^2 + y^2 - 4, xy - 1 \rangle \cap \mathbb{Q}[x]$$
$$= \langle x^4 - 4x^2 + 1 \rangle \subseteq \mathbb{Q}[x]$$



Fact 7*: If G is a Gröbner basis of I, then $G \cap K[X_*]$ is a Gröbner basis of $I \cap K[X_*]$, where $X_* \subseteq \{x_1, \ldots, x_n\}$

In particular, we can "triangularize" (and thus solve) a system of polynomial equations.

---

* only works for suitably chosen term orders.

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

$\alpha \in \mathbb{C}$ is called algebraic iff $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x] \setminus \{0\}$.

$\alpha \in \mathbb{C}$ is called algebraic iff $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x] \setminus \{0\}$.

Example: $\sqrt{2}$ is algebraic but π is not.

$\alpha \in \mathbb{C}$ is called algebraic iff $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x] \setminus \{0\}$.

Example: $\sqrt{2}$ is algebraic but π is not.

Theorem: If α, β are algebraic, then so is $\alpha + \beta$.

$\alpha \in \mathbb{C}$ is called algebraic iff $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x] \setminus \{0\}$.

Example: $\sqrt{2}$ is algebraic but π is not.

Theorem: If α, β are algebraic, then so is $\alpha + \beta$.

Question: How to compute a polynomial for $\alpha + \beta$ from given polynomials for α and β?

$\alpha \in \mathbb{C}$ is called algebraic iff $p(\alpha) = 0$ for some $p \in \mathbb{Q}[x] \setminus \{0\}$.

Example: $\sqrt{2}$ is algebraic but π is not.

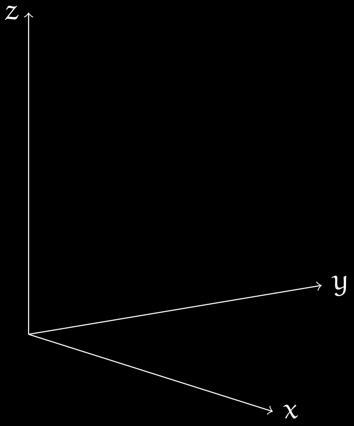
Theorem: If α, β are algebraic, then so is $\alpha + \beta$.

Question: How to compute a polynomial for $\alpha + \beta$ from given polynomials for α and β?

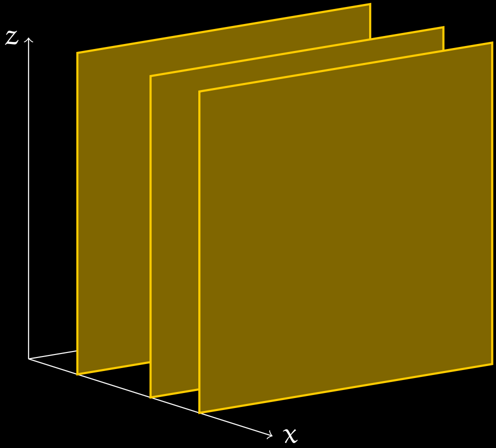
Answer: If $p(\alpha) = q(\beta) = 0$, then we can take a basis element of

$$\langle p(x), q(y), z - (x + y) \rangle \cap \mathbb{Q}[z].$$

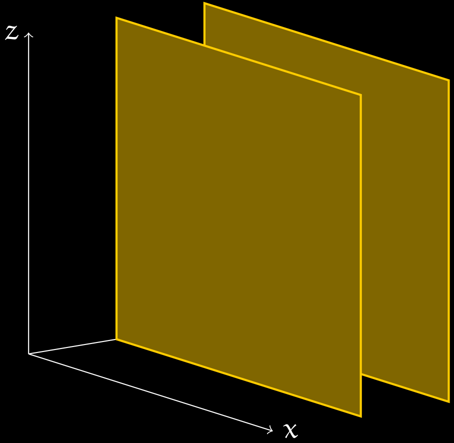
$$\langle p(x), q(y), z - (x + y) \rangle \cap \mathbb{Q}[z] = \langle u(z) \rangle$$



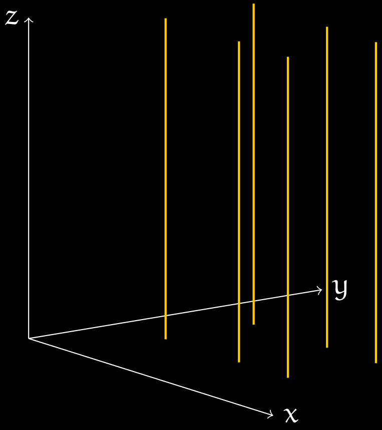
$$\langle p(x), q(y), z - (x + y) \rangle \cap \mathbb{Q}[z] = \langle u(z) \rangle$$



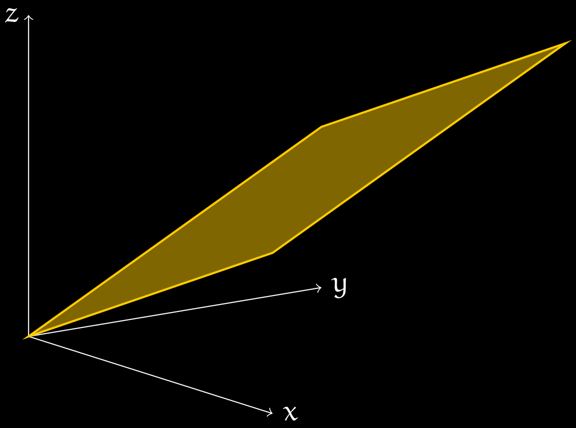
$$\langle p(x), q(y), z - (x + y)\rangle \cap \mathbb{Q}[z] = \langle u(z)\rangle$$



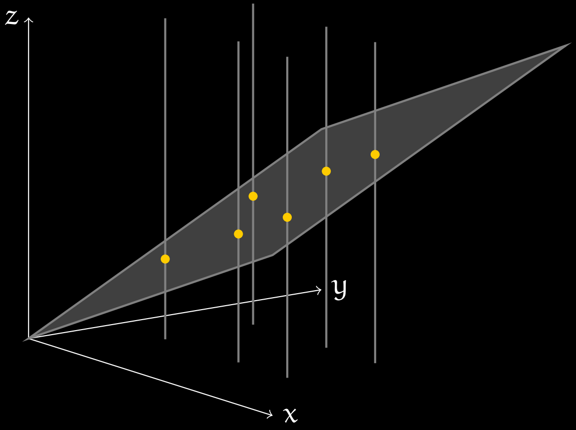
$$\langle p(x), q(y), z - (x + y) \rangle \cap \mathbb{Q}[z] = \langle u(z) \rangle$$



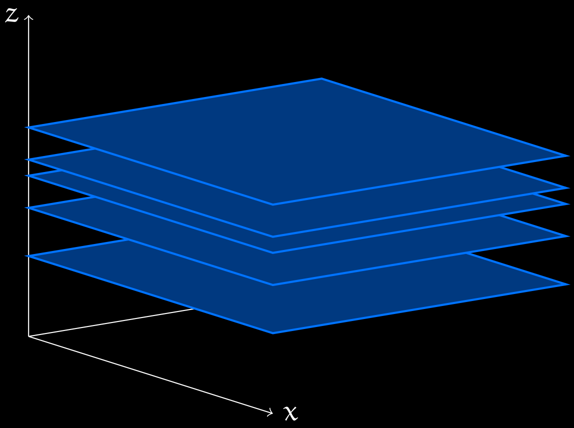
$$\langle p(x), q(y), z - (x + y)\rangle \cap \mathbb{Q}[z] = \langle u(z)\rangle$$



$$\langle p(x), q(y), z - (x+y) \rangle \cap \mathbb{Q}[z] = \langle u(z) \rangle$$



$$\langle p(x), q(y), z - (x+y) \rangle \cap \mathbb{Q}[z] = \langle u(z) \rangle$$



Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$p(\alpha x, \beta y) = ax^2 + bxy + cy^2 \quad ?$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha x)^2 + 2(\alpha x)(\beta y) + 3(\beta y)^2 = ax^2 + bxy + cy^2 \quad ?$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha^2 - a)x^2 + (2\alpha\beta - b)xy + (3\beta^2 - c)y^2 = 0 \quad ?$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha^2 - a)x^2 + (2\alpha\beta - b)xy + (3\beta^2 - c)y^2 = 0 \quad ?$$

Coefficient comparison yields:

$$\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \subseteq \mathbb{Q}[\alpha, \beta, a, b, c]$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha^2 - a)x^2 + (2\alpha\beta - b)xy + (3\beta^2 - c)y^2 = 0 \quad ?$$

Coefficient comparison yields:

$$\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \cap \mathbb{Q}[a, b, c]$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha^2 - a)x^2 + (2\alpha\beta - b)xy + (3\beta^2 - c)y^2 = 0 \quad ?$$

Coefficient comparison yields:

$$\begin{aligned}&\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c\rangle \cap \mathbb{Q}[a, b, c]\\ &= \langle 3b^2 - 4ac\rangle\end{aligned}$$

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$(\alpha^2 - a)x^2 + (2\alpha\beta - b)xy + (3\beta^2 - c)y^2 = 0 \quad ?$$

Coefficient comparison yields:

$$\begin{aligned} &\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \cap \mathbb{Q}[a, b, c] \\ &= \langle 3b^2 - 4ac \rangle \end{aligned}$$

Answer: Suitable α, β exist if and only if $3b^2 = 4ac$.

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Example: $9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2 \overset{?}{\in} \mathbb{Q}[x + 2y,\ 3xy + 1]$

Example: Is there a polynomial $p(u, v) \in \mathbb{Q}[u, v]$ such that

$$9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2 = p\big(\, x + 2y,\ 3xy + 1\,\big) \quad ?$$

Example: Is there a polynomial $p(u,v) \in \mathbb{Q}[u,v]$ such that

$$9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2 = p\big(\, x + 2y,\ 3xy + 1\, \big) \quad ?$$

Set $I = \langle\, u - (x + 2y),\ v - (3xy + 1)\rangle \subseteq \mathbb{Q}[x, y, u, v]$ and choose a term order for eliminating x and y.

Example: Is there a polynomial $p(u, v) \in \mathbb{Q}[u, v]$ such that

$$9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2 = p\big(\, x + 2y,\; 3xy + 1 \,\big) \quad ?$$

Set $I = \langle\, u - (x + 2y),\, v - (3xy + 1)\rangle \subseteq \mathbb{Q}[x, y, u, v]$ and choose a term order for eliminating x and y. Then compute

$$\begin{aligned} &\text{red}(9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2, I) \\ &= u^2 + uv - u + v^2 - \tfrac{10}{3}v + \tfrac{7}{3} \end{aligned}$$

Example: Is there a polynomial $p(u, v) \in \mathbb{Q}[u, v]$ such that

$$9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2 = p\big(\, x + 2y,\ 3xy + 1 \,\big) \quad ?$$

Set $I = \langle\, u - (x + 2y),\ v - (3xy + 1)\rangle \subseteq \mathbb{Q}[x, y, u, v]$ and choose a term order for eliminating x and y. Then compute

$$\begin{aligned} &\mathrm{red}(9x^2y^2 + 3x^2y + x^2 + 6xy^2 + 4y^2, I) \\ &= u^2 + uv - u + v^2 - \tfrac{10}{3}v + \tfrac{7}{3} \end{aligned}$$

Fact 8:

- If the result is free of x and y, it is a suitable p
- If the result still contains x and y, no suitable p exists.

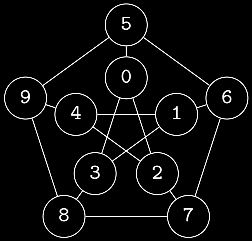
Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Example: Is the following graph 3-colorable?



Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.

Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.
- Take one variable for each vertex: $x_0, x_1, \ldots, x_9$.

Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.
- Take one variable for each vertex: $x_0, x_1, \ldots, x_9$.
- Specify the equations $x_i^3 - 1 = 0$ for all i.
  ("Every vertex gets one color")

Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.
- Take one variable for each vertex: $x_0, x_1, \dots, x_9$.
- Specify the equations $x_i^3 - 1 = 0$ for all i.
  ("Every vertex gets one color")
- For each edge (i, j), specify the restriction $x_i \neq x_j$.
  ("Adjacent vertices get different colors")

Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.
- Take one variable for each vertex: $x_0, x_1, \ldots, x_9$.
- Specify the equations $x_i^3 - 1 = 0$ for all i.
  ("Every vertex gets one color")
- For each edge (i, j), specify the restriction $x_i \neq x_j$.
  ("Adjacent vertices get different colors")
- Note: $x_i \neq x_j \iff x_i - x_j \neq 0 \iff$ The equation $(x_i - x_j)z = 1$, for a new variable z, has a solution.

Example: Is the following graph 3-colorable?

Idea:

- Let's use the 3rd roots of unity $\omega^0, \omega^1, \omega^2$ as colors.
- Take one variable for each vertex: $x_0, x_1, \dots, x_9$.
- Specify the equations $x_i^3 - 1 = 0$ for all i.
  ("Every vertex gets one color")
- For each edge (i, j), specify the restriction $x_i \neq x_j$.
  ("Adjacent vertices get different colors")
- Note: $x_i \neq x_j \iff x_i - x_j \neq 0 \iff$ The equation $(x_i - x_j)z = 1$, for a new variable z, has a solution.
- Note also: $A \neq 0 \wedge B \neq 0 \iff AB \neq 0$

Example: Is the following graph 3-colorable?

Compute a Gröbner basis of the ideal

$$\langle x_0^3 - 1, x_1^3 - 1, \ldots, x_9^3 - 1,$$
$$(x_5 - x_9)(x_5 - x_0)(x_5 - x_6) \cdots (x_8 - x_7)z - 1\rangle \subseteq \mathbb{Q}[x_0, \ldots, x_9, z].$$

Example: Is the following graph 3-colorable?

Compute a Gröbner basis of the ideal

$$\langle x_0^3 - 1, x_1^3 - 1, \ldots, x_9^3 - 1, \\ (x_5 - x_9)(x_5 - x_0)(x_5 - x_6) \cdots (x_8 - x_7)z - 1\rangle \subseteq \mathbb{Q}[x_0, \ldots, x_9, z].$$

Fact: The number of distinct colorings of the graph is exactly the number of blue terms for this Gröbner basis.

Example: Is the following graph 3-colorable?

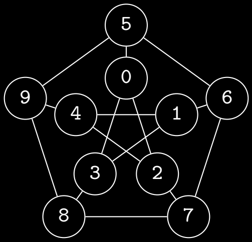
Compute a Gröbner basis of the ideal

$$\langle x_0^3 - 1, x_1^3 - 1, \ldots, x_9^3 - 1,\\ (x_5 - x_9)(x_5 - x_0)(x_5 - x_6) \cdots (x_8 - x_7)z - 1\rangle \subseteq \mathbb{Q}[x_0, \ldots, x_9, z].$$

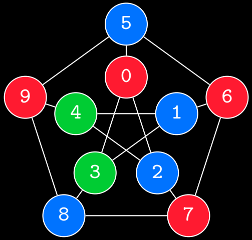
Fact: The number of distinct colorings of the graph is exactly the number of blue terms for this Gröbner basis.

The colorings correspond to the solutions of the equation system.

Example: Is the following graph 3-colorable?



Example: Is the following graph 3-colorable? Yes!



Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

If so, what is the minimal number of boxes we have to buy?

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

If so, what is the minimal number of boxes we have to buy?

Idea: Consider the ideal

$$I = \langle x_4 - x_1^4, x_6 - x_1^6, x_9 - x_1^9, x_{20} - x_1^{20} \rangle \subseteq \mathbb{Q}[x_1, x_4, x_6, x_9, x_{20}].$$

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

If so, what is the minimal number of boxes we have to buy?

Idea: Consider the ideal

$$I = \langle x_4 - x_1^4, x_6 - x_1^6, x_9 - x_1^9, x_{20} - x_1^{20} \rangle \subseteq \mathbb{Q}[x_1, x_4, x_6, x_9, x_{20}].$$

Choose a term order which eliminates x_1 and minimizes total degree for the remaining variables.

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

If so, what is the minimal number of boxes we have to buy?

Idea: Consider the ideal

$$I = \langle x_4 - x_1^4, x_6 - x_1^6, x_9 - x_1^9, x_{20} - x_1^{20} \rangle \subseteq \mathbb{Q}[x_1, x_4, x_6, x_9, x_{20}].$$

Choose a term order which eliminates x_1 and minimizes total degree for the remaining variables.

Then $\mathrm{red}(x_1^{123}, I)$ is a monomial which tells us what to buy. If it contains x_1, there is no way.

Example: If there are Chicken McNuggets of sizes 4, 6, 9, and 20, is there a way to buy exactly 123 nuggets?

If so, what is the minimal number of boxes we have to buy?

Idea: Consider the ideal

$$I = \langle x_4 - x_1^4, x_6 - x_1^6, x_9 - x_1^9, x_{20} - x_1^{20} \rangle \subseteq \mathbb{Q}[x_1, x_4, x_6, x_9, x_{20}].$$

Choose a term order which eliminates x_1 and minimizes total degree for the remaining variables.

Then $\mathrm{red}(x_1^{123}, I)$ is a monomial which tells us what to buy. If it contains x_1, there is no way.

For the example, we find $\mathrm{red}(x_1^{123}, I) = x_4^2 x_6 x_9 x_{20}^5$

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification

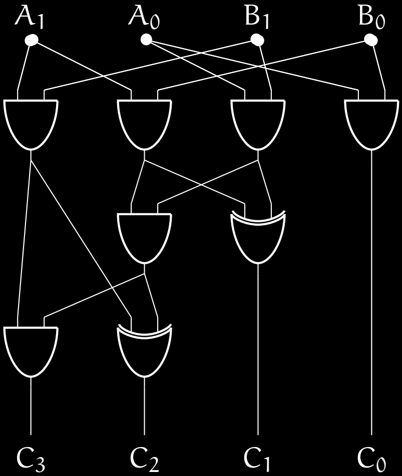
Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification*

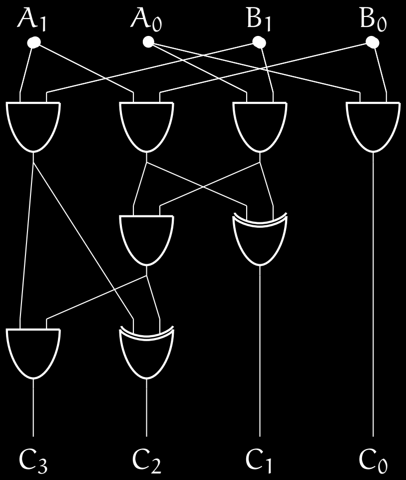
* Joint work with Armin Biere and Daniela Ritirc

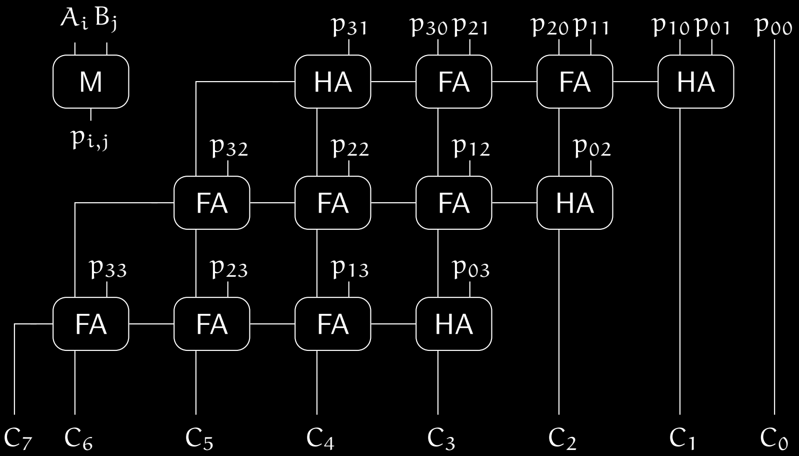
$$10001011001 \times 11011000001$$

$$1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1 \times 1\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1$$

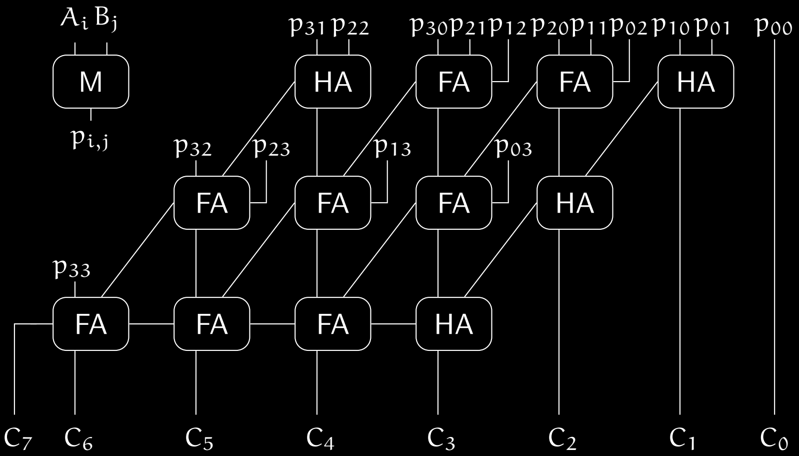


A_1
A_0
B_1
B_0
C_3
C_2
C_1
C_0


A_1
A_0
B_1
B_0
C_3
C_2
C_1
C_0



A_i B_j
M
$p_{i,j}$
p_{31}
p_{30} p_{21}
p_{20} p_{11}
p_{10} p_{01}
p_{00}
HA
FA
FA
HA
p_{32}
p_{22}
p_{12}
p_{02}
FA
FA
FA
HA
p_{33}
p_{23}
p_{13}
p_{03}
FA
FA
FA
HA
C_7
C_6
C_5
C_4
C_3
C_2
C_1
C_0



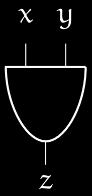
A_i B_j
M
$p_{i,j}$
p_{31} p_{22}
p_{30} p_{21} p_{12} p_{20} p_{11} p_{02} p_{10} p_{01} p_{00}
HA
FA
FA
HA
p_{32} p_{23} p_{13} p_{03}
FA
FA
FA
HA
p_{33}
FA
FA
FA
HA
C_7 C_6 C_5 C_4 C_3 C_2 C_1 C_0

- Every circuit implements a certain function $\{0,1\}^n \to \{0,1\}^m$

- Every circuit implements a certain function $\{0,1\}^n \rightarrow \{0,1\}^m$
- A circuit is "correct" if it corresponds the right function

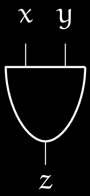
- Every circuit implements a certain function $\{0,1\}^n \rightarrow \{0,1\}^m$
- A circuit is "correct" if it corresponds the right function
- The behaviour of a gate is described by a polynomial equation

- Every circuit implements a certain function $\{0,1\}^n \to \{0,1\}^m$
- A circuit is “correct” if it corresponds the right function
- The behaviour of a gate is described by a polynomial equation

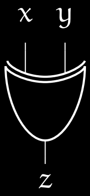


$$z = xy$$

- Every circuit implements a certain function $\{0,1\}^n \to \{0,1\}^m$
- A circuit is "correct" if it corresponds the right function
- The behaviour of a gate is described by a polynomial equation

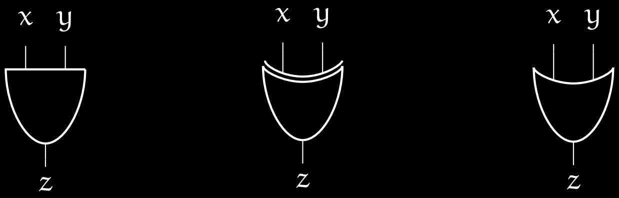


$z = xy$



$z = x + y - 2xy$

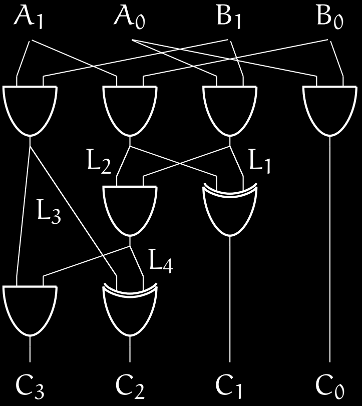
- Every circuit implements a certain function $\{0,1\}^n \to \{0,1\}^m$
- A circuit is "correct" if it corresponds the right function
- The behaviour of a gate is described by a polynomial equation



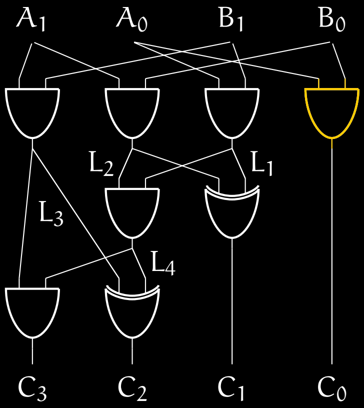
$z = xy$ $\qquad$ $z = x + y - 2xy$ $\qquad$ $z = x + y - xy$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.

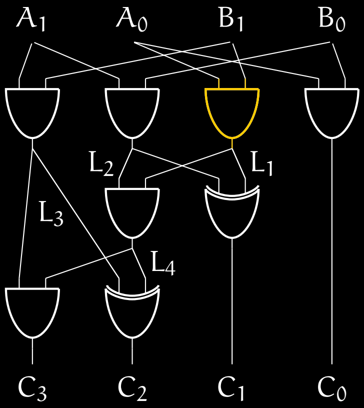


- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



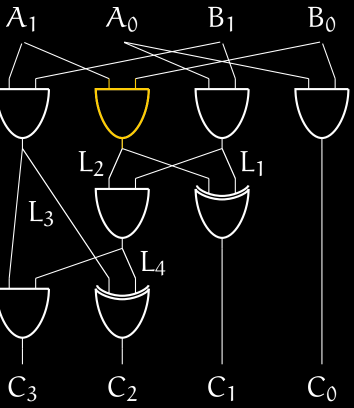
  - $C_0 = A_0 B_0$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



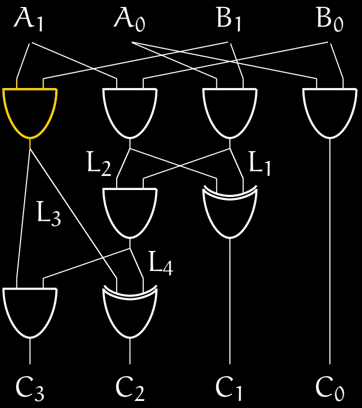
- $C_0 = A_0 B_0$
- $L_1 = A_0 B_1$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



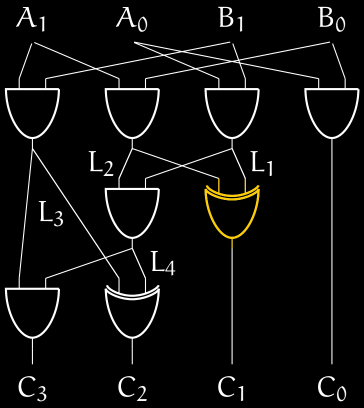
  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



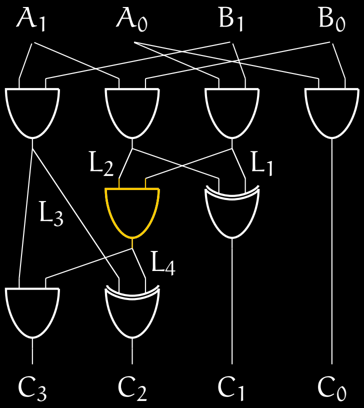
  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$
  - $L_3 = A_1 B_1$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



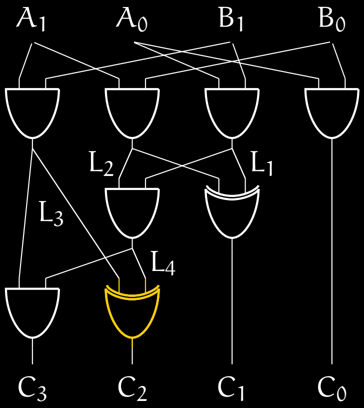
- $C_0 = A_0 B_0$
- $L_1 = A_0 B_1$
- $L_2 = A_1 B_0$
- $L_3 = A_1 B_1$
- $C_1 = L_1 + L_2 - 2L_1 L_2$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



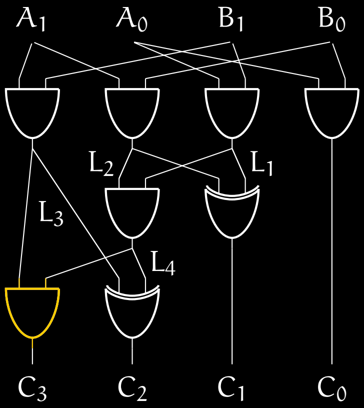
  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$
  - $L_3 = A_1 B_1$
  - $C_1 = L_1 + L_2 - 2L_1 L_2$
  - $L_4 = L_1 L_2$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



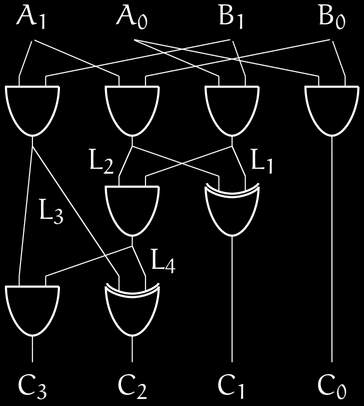
  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$
  - $L_3 = A_1 B_1$
  - $C_1 = L_1 + L_2 - 2L_1 L_2$
  - $L_4 = L_1 L_2$
  - $C_2 = L_3 + L_4 - 2L_3 L_4$

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



- $C_0 = A_0 B_0$
- $L_1 = A_0 B_1$
- $L_2 = A_1 B_0$
- $L_3 = A_1 B_1$
- $C_1 = L_1 + L_2 - 2L_1 L_2$
- $L_4 = L_1 L_2$
- $C_2 = L_3 + L_4 - 2L_3 L_4$
- $C_3 = L_3 L_4$

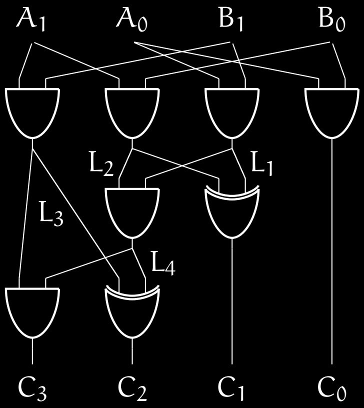
- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$
  - $L_3 = A_1 B_1$
  - $C_1 = L_1 + L_2 - 2L_1 L_2$
  - $L_4 = L_1 L_2$
  - $C_2 = L_3 + L_4 - 2L_3 L_4$
  - $C_3 = L_3 L_4$

- We also have polynomials for restricting the range of the variables to $\{0, 1\}$.

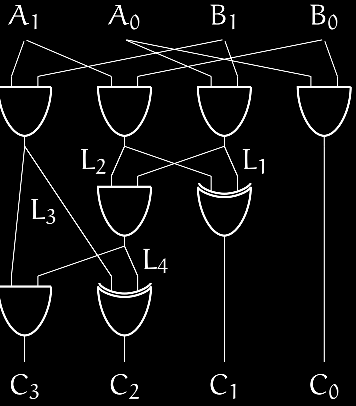
- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



  - $C_0 = A_0 B_0$
  - $L_1 = A_0 B_1$
  - $L_2 = A_1 B_0$
  - $L_3 = A_1 B_1$
  - $C_1 = L_1 + L_2 - 2L_1 L_2$
  - $L_4 = L_1 L_2$
  - $C_2 = L_3 + L_4 - 2L_3 L_4$
  - $C_3 = L_3 L_4$
  - $A_0(A_0 - 1) = 0$
  - $A_1(A_1 - 1) = 0$
  - $B_0(B_0 - 1) = 0$
  - $B_1(B_1 - 1) = 0$

- We also have polynomials for restricting the range of the variables to $\{0, 1\}$.

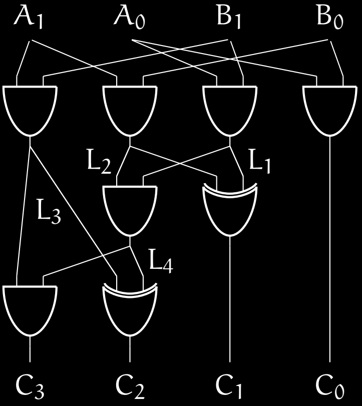
- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



  - $C_0 - A_0 B_0 = 0$
  - $L_1 - A_0 B_1 = 0$
  - $L_2 - A_1 B_0 = 0$
  - $L_3 - A_1 B_1 = 0$
  - $C_1 - L_1 - L_2 + 2L_1 L_2 = 0$
  - $L_4 - L_1 L_2 = 0$
  - $C_2 - L_3 - L_4 + 2L_3 L_4 = 0$
  - $C_3 - L_3 L_4 = 0$
  - $A_0(A_0 - 1) = 0$
  - $A_1(A_1 - 1) = 0$
  - $B_0(B_0 - 1) = 0$
  - $B_1(B_1 - 1) = 0$

- We also have polynomials for restricting the range of the variables to $\{0, 1\}$.

- For the whole circuit, we have one variable for each circuit input bit and each gate output, and one polynomial per gate.



  - $C_0 - A_0 B_0$
  - $L_1 - A_0 B_1$
  - $L_2 - A_1 B_0$
  - $L_3 - A_1 B_1$
  - $C_1 - L_1 - L_2 + 2L_1 L_2$
  - $L_4 - L_1 L_2$
  - $C_2 - L_3 - L_4 + 2L_3 L_4$
  - $C_3 - L_3 L_4$
  - $A_0(A_0 - 1)$
  - $A_1(A_1 - 1)$
  - $B_0(B_0 - 1)$
  - $B_1(B_1 - 1)$

- We also have polynomials for restricting the range of the variables to $\{0, 1\}$.

- The ideal generated by these polynomial contains all the polynomial relations implied by the circuit.

- The ideal generated by these polynomial contains all the polynomial relations implied by the circuit.
- The polynomials form a Gröbner bases for a suitably chosen order.

- The ideal generated by these polynomial contains all the polynomial relations implied by the circuit.
- The polynomials form a Gröbner bases for a suitably chosen order.
- Taking $\mathbb{Q}$ as ground field, a multiplier circuit is correct iff its ideal contains the polynomial

$$\left(\sum_{k=0}^{n-1} 2^k A_k\right)\left(\sum_{k=0}^{n-1} 2^k B_k\right) - \left(\sum_{k=0}^{2n-1} 2^k C_k\right)$$

- The ideal generated by these polynomial contains all the polynomial relations implied by the circuit.
- The polynomials form a Gröbner bases for a suitably chosen order.
- Taking $\mathbb{Q}$ as ground field, a multiplier circuit is correct iff its ideal contains the polynomial

$$\left(\sum_{k=0}^{n-1} 2^k A_k\right)\left(\sum_{k=0}^{n-1} 2^k B_k\right) - \left(\sum_{k=0}^{2n-1} 2^k C_k\right)$$

- Correctness thus reduces to ideal membership test.

- Can we trust the computer algebra system and/or the implementation of our own improvements?

- Can we trust the computer algebra system and/or the implementation of our own improvements?
- Can we construct a checkable proof object rather than a yes/no answer?

- Can we trust the computer algebra system and/or the implementation of our own improvements?
- Can we construct a checkable proof object rather than a yes/no answer?
- Recall: $p \in \langle p_1, \ldots, p_m \rangle \iff p = q_1 p_1 + \cdots + q_m p_m$ for certain polynomials q_i.

- Can we trust the computer algebra system and/or the implementation of our own improvements?
- Can we construct a checkable proof object rather than a yes/no answer?
- Recall: $p \in \langle p_1, \ldots, p_m \rangle \iff p = q_1 p_1 + \cdots + q_m p_m$ for certain polynomials q_i.
- These cofactors $q_1, \ldots, q_m$ can serve as certificate of the ideal membership.

- Can we trust the computer algebra system and/or the implementation of our own improvements?
- Can we construct a checkable proof object rather than a yes/no answer?
- Recall: $p \in \langle p_1, \ldots, p_m \rangle \iff p = q_1 p_1 + \cdots + q_m p_m$ for certain polynomials q_i.
- These cofactors $q_1, \ldots, q_m$ can serve as certificate of the ideal membership.
- This is well-known in theory, but not so easy in practice: the cofactors can be quite large.

- Translate the defining properties of ideals into a formal proof system:

- Translate the defining properties of ideals into a formal proof system:

$$\forall\, p, q \in I : p + q \in I$$

- Translate the defining properties of ideals into a formal proof system:

$$\forall\, p, q \in I : p + q \in I$$

$$\forall\, p \in K[X]\ \forall\, q \in I : pq \in I$$

- Translate the defining properties of ideals into a formal proof system:

$$\forall\ p, q \in I : p + q \in I \qquad \rightsquigarrow \qquad \frac{p \quad q}{p + q}$$

$$\forall\ p \in K[X]\ \forall\ q \in I : pq \in I \qquad \rightsquigarrow \qquad \frac{q}{pq}$$

- Translate the defining properties of ideals into a formal proof system:

$$\forall\, p, q \in I : p + q \in I \qquad \rightsquigarrow \qquad \frac{p \quad q}{p + q}$$

$$\forall\, p \in K[X]\ \forall\, q \in I : pq \in I \qquad \rightsquigarrow \qquad \frac{q}{pq}$$

- We construct a formal proof by tracing the reduction process

```
⋮
* : -b+1-a,       a,            -a*b+a-a^2;
+ : -a*b+a-a^2,   a^2-a,        -a*b;
+ : -a*b,         -c+a*b,       -c;
* : -c,           -1,           c;
⋮
```

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification*

* Joint work with Armin Biere and Daniela Ritirc

Some applications of Gröbner Bases

- Computing with Algebraic Numbers
- Quantifier Elimination
- Subring Membership
- Graph Coloring
- Integer Programming
- Circuit Verification*

* Joint work with Armin Biere and Daniela Ritirc