Gröbner Bases and Tilings

Amir Hashemi

Isfahan University of Technology & IPM

CIMPA-IRAN school on Tilings and Tessellations, Isfahan, Iran, 2015

Abu Abdallah Muhammed Ibn Mussa Al-Khwarizmi, Persian mathematician, was born in Khwarizm (Kheva) around the year 770, in a village south of the Oxus River in a region that is now named the Uzbekistan (Persian empire, the former Iran). He died around the year 840. He is known for having introduced the concept of mathematical algorithm. *The word algorithm derives from his name*. His algebra treatise "Hisab al-jabr w'al-muqabala" gives us the word algebra and can be considered as the first book to be written on algebra.

Al−Khwarizmi

Outline of talk

Notations

- K; a field e.g. $K = \mathbb{R}, \mathbb{Q}, \ldots$
- $x_1, \ldots, x_n$; a sequence of variables
- A polynomial is a sum of products of numbers and variables, e.g.

$$f = x_1 x_2 + 12 x_1 - x_2^3$$

- $R = K[x_1, \ldots, x_n]$; set of all polynomials
- $f_1, \ldots, f_k \in R$ and $F = \{f_1, \ldots, f_k\}$
- $I = \langle F \rangle = \{p_1 f_1 + \cdots + p_k f_k \mid p_i \in R\}$

Notations (cont.)

The variety of a system: Consider $F = \{f_1, \ldots, f_k\}$

- $\begin{cases} f_1 & = & 0 \\ & \vdots & \\ f_k & = & 0. \end{cases}$
- $\mathbf{V}(f_1, \ldots, f_k) = \mathbf{V}(F)$: The solutions of the system
- E.g. $\begin{cases} x^2 + y^2 + z^2 & = & 4 \\ x^2 + 2y^2 & = & 5 \\ xz & = & 1 \end{cases}$
- $\mathbf{V}(f_1, f_2, f_3) = \{(1, \sqrt{2}, 1), \ldots\}$ where $f_1 = x^2 + y^2 + z^2 - 4, \cdots$

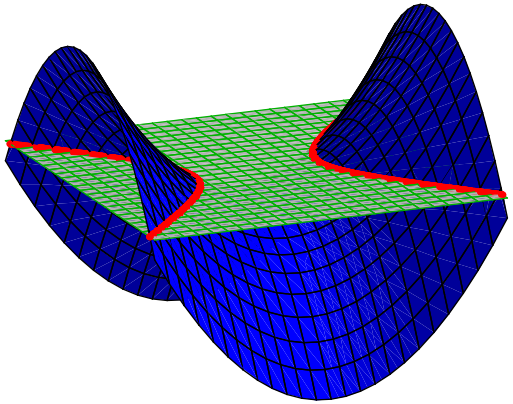
What is Algebraic Geometry?

- Studying the solutions of a polynomial system
  i.e. computing $\mathbf{V}(F)$ using algebraic tools:
  - ▷ Algebra
  - ▷ Geometry
  - ▷ Computer Science (Computational Algebraic Geometry)

What is Algebraic Geometry?

- Studying the solutions of a polynomial system
  i.e. computing $\mathbf{V}(F)$ using algebraic tools:
  - ▷ Algebra
  - ▷ Geometry
  - ▷ Computer Science (Computational Algebraic Geometry)

- Example: $I = \langle x^2 - y^2 - z, z - 2 \rangle \subset \mathbb{R}[x, y, z]$



Variables versus Unknowns

- If we consider the *equation* $x^2 - x + 1 = 0$; i.e. we look for its zeros then x is called an *unknown*

Variables versus Unknowns

- If we consider the *equation* $x^2 - x + 1 = 0$; i.e. we look for its zeros then x is called an *unknown*
- If we consider the *polynomial* $x^2 - x + 1$ then x is called a *variable*

Variables versus Unknowns

- If we consider the *equation* $x^2 - x + 1 = 0$; i.e. we look for its zeros then x is called an *unknown*
- If we consider the *polynomial* $x^2 - x + 1$ then x is called a *variable*
- So, the polynomial $x^2 - x + 1$ is never 0.

Variables versus Unknowns

- If we consider the *equation* $x^2 - x + 1 = 0$; i.e. we look for its zeros then x is called an *unknown*
- If we consider the *polynomial* $x^2 - x + 1$ then x is called a *variable*
- So, the polynomial $x^2 - x + 1$ is never 0.
- For example if we consider the polynomial $ax^2 - bx + c = 0$ in x then $a = b = c = 0$.

Variables versus Unknowns

- If we consider the *equation* $x^2 - x + 1 = 0$; i.e. we look for its zeros then x is called an *unknown*
- If we consider the *polynomial* $x^2 - x + 1$ then x is called a *variable*
- So, the polynomial $x^2 - x + 1$ is never 0.
- For example if we consider the polynomial $ax^2 - bx + c = 0$ in x then $a = b = c = 0$.
- $$\begin{array}{ccc} Equation & \rightsquigarrow & Unknown \\ Polynomial & \rightsquigarrow & Variable \end{array}$$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$

$$g := x^3 - 10x^2 + 29x - 20$$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$

$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f, g) = x - 1$ then $\mathbf{V}(f, g) = \mathbf{V}(\langle f, g \rangle) = \mathbf{V}(x-1)$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$

$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f, g) = x - 1$ then $\mathbf{V}(f, g) = \mathbf{V}(\langle f, g \rangle) = \mathbf{V}(x-1)$
- The only solution of the system $f = g = 0$ is $x = 1$

Univariate Polynomial Ring

- Let K be a field and $K[x]$ the ring of polynomials in x
- If $f_1, \ldots, f_k \in K[x]$ then $\langle f_1, \ldots, f_k \rangle = \langle gcd(f_1, \ldots, f_k) \rangle$
- $K[x]$ is a PID, e.g. $\langle x-1, x^2-1 \rangle = \langle x-1 \rangle$
- Thus, gcd computations (using Euclid algorithm) can solve many problems in $K[x]$
- Suppose that

$$f := x^3 - 6x^2 + 11x - 6$$

$$g := x^3 - 10x^2 + 29x - 20$$

- Since $gcd(f, g) = x - 1$ then $\mathbf{V}(f, g) = \mathbf{V}(\langle f, g \rangle) = \mathbf{V}(x-1)$
- The only solution of the system $f = g = 0$ is $x = 1$
- Membership Problem: $x^2 - 1 \in \langle f, g \rangle$ because $x - 1 \mid x^2 - 1$.

Two Questions

- ☞ $R = K[x_1, \ldots, x_n]$; a multivariate polynomial ring
- ☞ $F \subset R$; a finite set of polynomials
- ☞ $I \subset R$; an ideal
  - Membership problem: $h \in I$?
  - Solving polynomial systems: $\mathbf{V}(F)$?
  - In practice, the answer to these questions is not easy!

Two Questions

- ☞ $R = K[x_1, \ldots, x_n]$; a multivariate polynomial ring
- ☞ $F \subset R$; a finite set of polynomials
- ☞ $I \subset R$; an ideal
  - Membership problem: $h \in I$?
  - Solving polynomial systems: $\mathbf{V}(F)$?
  - In practice, the answer to these questions is not easy!
  - Gröbner bases can answer them!

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$
- $f := 2x^2 + 3y^2 - 11, g := x^2 - y^2 - 3$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$
- $f := 2x^2 + 3y^2 - 11, g := x^2 - y^2 - 3$
- Since $\langle f, g \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ then $V(f, g) = \{(\pm 2, \pm 1)\}$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$
- $f := 2x^2 + 3y^2 - 11, g := x^2 - y^2 - 3$
- Since $\langle f, g \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ then $V(f, g) = \{(\pm 2, \pm 1)\}$
- So we look for a more convenient generating set for $\langle F \rangle$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$
- $f := 2x^2 + 3y^2 - 11, g := x^2 - y^2 - 3$
- Since $\langle f, g \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ then $V(f, g) = \{(\pm 2, \pm 1)\}$
- So we look for a more convenient generating set for $\langle F \rangle$
- To bring it into computer, we need $|F| < \infty$

Multivariate Polynomial Ring

- $F \subset K[x_1, \ldots, x_n]$
- $\mathbf{V}(F)$ doesn't depend on the generators of $\langle F \rangle$
- $f := 2x^2 + 3y^2 - 11, g := x^2 - y^2 - 3$
- Since $\langle f, g \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ then $V(f, g) = \{(\pm 2, \pm 1)\}$
- So we look for a more convenient generating set for $\langle F \rangle$
- To bring it into computer, we need $|F| < \infty$
- By Hilbert Basis Theorem there exist $f_1, \ldots, f_m \in F$ so that

$$\langle F \rangle = \langle f_1, \ldots, f_m \rangle$$

Polynomial Ring

☞ K a field

- ▷ We denote the *monomial* $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by X^α with $\alpha = (\alpha_1, \ldots, \alpha_n)$
- ▷ $\{$monomials in $R\} \leftrightarrow \mathbb{Z}^n_{\geq 0}$
- ▷ If X^α is a monomial and $a \in K$, then aX^α is a *term*
- ▷ A polynomial is a finite sum of terms.

☞ $R = K[x_1, \ldots, x_n]$; the ring of all polynomials.

Definition

A monomial ordering is a total ordering $\prec$ on the set of monomials $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$,$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ such that,

- $X^\alpha \prec X^\beta \Rightarrow X^{\alpha+\gamma} \prec X^{\beta+\gamma}$ and
- $1 \prec X^\alpha$ for all α

Convention

For a monomial $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, We call $|\alpha| := \alpha_1 + \cdots + \alpha_n$, the total degree of X^α

Some important monomial orderings

Lex(Lexicographic) Ordering

$X^\alpha \prec_{lex} X^\beta$ if leftmost nonzero of $\alpha - \beta$ is < 0

Degree Reverse Lex Ordering

$X^\alpha \prec_{drl} X^\beta$ if

$$\begin{cases} |\alpha| < |\beta| \\ \quad \text{or} \\ |\alpha| = |\beta| \quad \text{and rightmost nonzero of } \alpha - \beta \text{ is} > 0 \end{cases}$$

- Example

  $x \prec x^3 \qquad x^2y^3 \prec_{lex(x,y)} x^3y^2 \qquad x^3y \prec_{drl(x,y)} xy^5$

Notations

- ☞ $R = K[x_1, \ldots, x_n], f \in R$
- ☞ $\prec$ a monomial ordering on R
- ☞ $I \subset R$ an ideal

$\mathrm{LM}(f)$: The greatest monomial (with respect to $\prec$) in f
$5x^3y^2 + 4x^2y^3 + xy + 1$

$\mathrm{LC}(f)$: The coefficient of $\mathrm{LM}(f)$ in f
$5x^3y^2 + 4x^2y^3 + xy + 1$

$\mathrm{LT}(f)$: $\mathrm{LC}(f)\mathrm{LM}(f)$
$5x^3y^2 + 4x^2y^3 + xy + 1$

$\mathrm{LT}(I)$: $\langle \mathrm{LT}(f) \mid f \in I \rangle$

Definition

- $I \subset K[x_1, \ldots, x_n]$
- $\prec$ A monomial ordering
- A finite set $G \subset I$ is a Gröbner Basis for I w.r.t. $\prec$, if

$$\mathrm{LT}(I) = \langle \mathrm{LT}(g) \mid g \in G \rangle$$

Existence of Gröbner bases

Each ideal has a Gröbner basis

Example

$I = \langle xy - x, x^2 - y \rangle$, $y \prec_{lex} x$
$\mathrm{LT}(I) = \langle x^2, xy, y^2 \rangle$
A Gröbner basis is: $\{xy - x, x^2 - y, y^2 - y\}$.

Unicity

Definition

▷ $G \subset I$ is a reduced Gröbner basis w.r.t. $\prec$ if

- G is a Gröbner basis for I w.r.t. $\prec$
- $\forall g \in G$, $\mathrm{LC}(g) = 1$
- $\forall f, g \in G$, $\mathrm{LT}(f) \nmid$ any term of g

Theorem

Every ideal I has a unique reduced Gröbner basis w.r.t. $\prec$

Division Algorithm in $K[x_1, \ldots, x_n]$

Theorem

Fix a monomial ordering $\prec$ and let $F := (f_1, \ldots, f_k)$ be an ordered $s-$tuple of polynomials in $K[x_1, \ldots, x_n]$ Then, every $f \in K[x_1, \ldots, x_n]$ can be written as

$$f = q_1 f_1 + \cdots + q_k f_k + r$$

where $q_i, r \in K[x_1, \ldots, x_n]$ and either $r = 0$ or no term of r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k)$. We call r, the remainder on division of f by F.

Algorithm 1 DIVISION ALGORITHM

Require: $f, f_1, \ldots, f_k$ and $\prec$

Ensure: $q_1, \ldots, q_k, r$

$q_1 := 0; \cdots ; q_k := 0;$

$p := f;$

while $\exists f_i$ s.t. $\mathrm{LT}(f_i)$ divides a term m in p **do**

$q_i := q_i + \frac{m}{\mathrm{LT}(f_i)}$

$p := p - (\frac{m}{\mathrm{LT}(f_i)}) f_i$

end while

return $q_1, \ldots, q_k, p$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$
- So we can write $f = y(xy + 1) + (-1)(y + 1) + 2$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$
- So we can write $f = y(xy + 1) + (-1)(y + 1) + 2$

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$
- So we can write $f = y(xy + 1) + (-1)(y + 1) + 2$

Example

- ▷ $f = xy^2 + x^2y + y^2, f_1 = y^2 - 1, f_2 = xy - 1, y \prec_{lex} x$
- ▷ $f = (x + 1)f_1 + xf_2 + 2x + 1$
- ▷ $f = (x + y)f_2 + f_1 + x + y + 1$

$\Rightarrow$ The remainder is not unique.

Example

- Divide $f = xy^2 + 1$ by $f_1 = xy + 1, f_2 = y + 1$ and $y \prec_{lex} x$
- $f \to (xy^2 + 1) - y(xy + 1) = 1 - y \to (1 - y) + (y + 1) = 2$
- So we can write $f = y(xy + 1) + (-1)(y + 1) + 2$

Example

- ▷ $f = xy^2 + x^2y + y^2, f_1 = y^2 - 1, f_2 = xy - 1, y \prec_{lex} x$
- ▷ $f = (x + 1)f_1 + xf_2 + 2x + 1$
- ▷ $f = (x + y)f_2 + f_1 + x + y + 1$

$\Rightarrow$ The remainder is not unique.

Theorem

$\{g_1, \ldots, g_k\}$ is a Gröbner basis iff for each $f \in R$ the remainder of f by G is unique.

Buchberger's Criterion

Definition

S-polynomial

$$\mathrm{Spoly}(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g$$

$$x^\gamma = lcm(\mathrm{LM}(f), \mathrm{LM}(g))$$

$$\mathrm{Spoly}(x^3y^2+xy^3, xyz-z^3) = z(x^3y^2+xy^3)-x^2y(xyz-z^3) = zxy^3+x^2yz^3$$

Buchberger's Criterion

- G is a Gröbner basis for $\langle G \rangle$
- $\forall g_i, g_j \in G$, remainder$((\mathrm{Spoly}(g_i, g_j), G) = 0$

Algorithm 2 BUCHBERGER'S ALGORITHM

Require: $F := (f_1, \ldots, f_s)$ and $\prec$

Ensure: A Gröbner basis for the ideal $\langle f_1, \ldots, f_s \rangle$ w.r.t. $\prec$

```
G := F
B := {{f, g} | f, g ∈ F}
while B ≠ ∅ do
    Select and remove a pair {f, g} from B
    Let r be the remainder of Spoly(f, g) by F
    if r ≠ 0 then
        B := B ∪ {{h, r} | h ∈ G}
        G := G ∪ {r}
    end if
end while
return G
```

Example

$I = \langle f_1, f_2 \rangle = \langle xy - x, x^2 - y \rangle \quad y \prec_{lex} x$

$G := \{f_1, f_2\}$

$\mathrm{Spoly}(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{f_2} y^2 - y = f_3$

$G := \{f_1, f_2, f_3\}$

$\mathrm{Spoly}(f_i, f_j) \xrightarrow{G} 0$

$G := \{f_1, f_2, f_3\}$ is a Gröbner basis for I

Buchberger, 65 :

- Developing the theory of Gröbner bases
- Buchberger criteria

Lazard, 83 :

- Using linear algebra

Gebauer, Möller, 88 :

- Installing Buchberger criteria

Faugère, 93, 94, 02 :

- FGLM
- F_4 algorithm (intensive linear algebra)
- F_5 algorithm

Gao, Volny, 10 :

- G^2V (with Guan)
- GVW (with Wang)

- MAGMA
  University of Sydney, Australia
- MAPLE
  University of Waterloo, Canada
- SINGULAR
  University of Kaiserslautern, Germany
- MACAULAY 2
  University of cornell, USA
- COCOA
  University of Geneva, Italy

Ideal Membership

Theorem

$f \in I$ *iff* $f \rightsquigarrow_G 0$ *where* G *is a GB of* I

Example

- $I = \langle xy - x, x^2 - y \rangle$
- Is $y^2 + y \in I$?

Ideal Membership

Theorem

$f \in I$ *iff* $f \rightsquigarrow_G 0$ *where* G *is a GB of* I

Example

- $I = \langle xy - x, x^2 - y \rangle$
- Is $y^2 + y \in I$?
- $y \prec_{lex} x$
- The reduced Gröbner basis of I is $G = \{xy - x, x^2 - y, y^2 - y\}$

$\Rightarrow$ $y^2 + y \rightsquigarrow_G 2y \neq 0$, and thus $y^2 + y \notin I$.

Ideal Membership (cont.)

Theorem (Weak Hilbert's Nullstellensätz)

$$\mathbf{V}(F) = \emptyset \Leftrightarrow 1 \in \langle F \rangle \Leftrightarrow 1 \in G$$

Example

- Let F be the set $\{x^2+3y+z-1, x-3y^2-z^2, x-y, y^2-zxy-x, x^2-y\}$
- $I = \langle F \rangle$
- $z \prec_{lex} y \prec_{lex} x$
- The reduced Gröbner basis of I is $= \{1\}$

$\Rightarrow$ $\mathbf{V}(F) = \emptyset$

Elimination

Theorem

- $I \subset K[x_1, \ldots, x_n]$; *an ideal*
- $G \subset I$; *a GB of* I *for* $x_n \prec_{lex} \cdots \prec_{lex} x_1$

$\Rightarrow$ $G \cap K[x_i, \ldots, x_n]$ *generates* $I \cap K[x_i, \ldots, x_n]$.

Example

- $I = \langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1 \rangle$
- Gröbner basis of I w.r.t. $z \prec_{lex} x \prec_{lex} y$

$$\{1 - 3z^2 + 2z^4, -1 - z^2 + y^2, -3z + 2z^3 + x\}$$

$\Rightarrow$ $I \cap K[z, x] = \langle 1 - 3z^2 + 2z^4, -3z + 2z^3 + x \rangle$.

Solving Polynomial Systems

$$\begin{cases} x^2 + y^2 + z^2 & = & 4 \\ x^2 + 2y^2 & = & 5 \\ xz & = & 1 \end{cases}$$

Solving Polynomial Systems

$$\begin{cases} x^2 + y^2 + z^2 & = & 4 \\ x^2 + 2y^2 & = & 5 \\ xz & = & 1 \end{cases}$$

▷ $I = \langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1 \rangle$

Solving Polynomial Systems

$$\begin{cases} x^2+y^2+z^2 &= 4 \\ x^2+2y^2 &= 5 \\ xz &= 1 \end{cases}$$

- $I = \langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$
- Gröbner basis of I w.r.t. $z \prec_{lex} x \prec_{lex} y$

$$\{1-3z^2+2z^4, -1-z^2+y^2, -3z+2z^3+x\}$$

Solving Polynomial Systems

$$\begin{cases} x^2+y^2+z^2 &= 4 \\ x^2+2y^2 &= 5 \\ xz &= 1 \end{cases}$$

- $I = \langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$
- Gröbner basis of I w.r.t. $z \prec_{lex} x \prec_{lex} y$

$$\{1-3z^2+2z^4, -1-z^2+y^2, -3z+2z^3+x\}$$

- The zero set corresponding to G is equal to the that of the initial system.

Solving Polynomial Systems

$$\begin{cases} x^2+y^2+z^2 &= 4 \\ x^2+2y^2 &= 5 \\ xz &= 1 \end{cases}$$

- $I = \langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$
- Gröbner basis of I w.r.t. $z \prec_{lex} x \prec_{lex} y$

$$\{1-3z^2+2z^4, -1-z^2+y^2, -3z+2z^3+x\}$$

- The zero set corresponding to G is equal to the that of the initial system.

$$\begin{cases} 3z^2-2z^4 &= 1 \\ -z^2+y^2 &= 1 \\ -3z+2z^3+x &= 0 \end{cases}$$

Solving Polynomial Systems

$$\begin{cases} x^2+y^2+z^2 &= 4 \\ x^2+2y^2 &= 5 \\ xz &= 1 \end{cases}$$

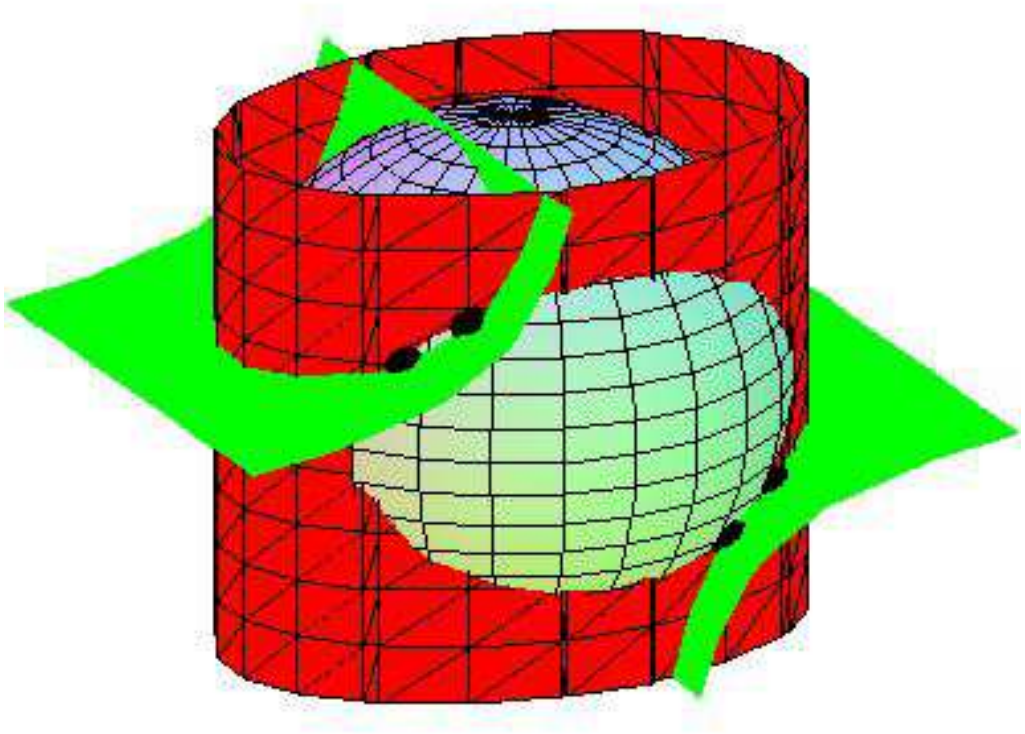
- $I = \langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$
- Gröbner basis of I w.r.t. $z \prec_{lex} x \prec_{lex} y$

$$\{1-3z^2+2z^4, -1-z^2+y^2, -3z+2z^3+x\}$$

- The zero set corresponding to G is equal to the that of the initial system.

$$\begin{cases} 3z^2-2z^4 &= 1 \\ -z^2+y^2 &= 1 \\ -3z+2z^3+x &= 0 \end{cases}$$

$$(1, \pm\sqrt{2}, 1), (-1, \pm\sqrt{2}, -1), (\sqrt{2}, \pm\sqrt{6}/2, 1/\sqrt{2}), (-\sqrt{2}, \pm\sqrt{6}/2, -1/\sqrt{2})$$



$$(1, \pm\sqrt{2}, 1), (-1, \pm\sqrt{2}, -1), (\sqrt{2}, \pm\sqrt{6}/2, 1/\sqrt{2}), (-\sqrt{2}, \pm\sqrt{6}/2, -1/\sqrt{2})$$

Implicitation

Theorem

Consider a rational parametrization: $\begin{cases} x_1 & = & \frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)} \\ & \vdots & \\ x_n & = & \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \end{cases}$

- $I = \langle x_1 g_1 - f_1, \ldots, x_n g_n - f_n, 1 - y g_1 \cdots g_n \rangle$
- *Note that* $I \subset K[x_1, \ldots, x_n, t_1, \ldots, t_m, y]$

$\Rightarrow$ $I \cap K[x_1, \ldots, x_n]$ *provides an implicitation.*

Implicitation (cont.)

Example

Consider the folium of Descartes: $\begin{cases} x_1 &= \frac{3t}{1+t^3} \\ x_2 &= \frac{3t^2}{1+t^3} \end{cases}$

- ▷ $I = \langle x_1(1+t^3) - 3t, x_2(1+t^3) - 3t^2, 1 - y(1+3t^2) \rangle$
- ▷ $G :=$ A GB of I w.r.t. $x_1 \prec_{lex} x_2 \prec_{lex} t \prec_{lex} y$
- ⇒ Since $x_1^3 + x_2^3 - 3x_1x_2 \in G$ then

$$x_1^3 + x_2^3 = 3x_1x_2$$

is an implicitation of the curve.

Computing Minimal Polynomial

Definition

Let M be a square matrix over the field K. The monic polynomial $m \in K[x]$ where

$$\langle m \rangle = \langle f \in K[x] \mid f(M) = 0 \rangle$$

is called minimal polynomial of M

Example

Minimal polynomial of $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -2 & 4 \end{pmatrix}$ is $x^3 - 7x^2 + 16x - 12$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

$I := \langle 7a_2 + a_1 + a_0, 10a_2 + 2a_1, 15a_2 + 3a_1, 22a_2 + 4a_1 + a_0 \rangle$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

$I := \langle 7a_2 + a_1 + a_0, 10a_2 + 2a_1, 15a_2 + 3a_1, 22a_2 + 4a_1 + a_0 \rangle$

$G := \{2a_1 - 5a_0, 2a_2 + a_0\}$ GB w.r.t. $a_0 \prec_{lex} a_1 \prec_{lex} a_2$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

$I := \langle 7a_2 + a_1 + a_0, 10a_2 + 2a_1, 15a_2 + 3a_1, 22a_2 + 4a_1 + a_0 \rangle$

$G := \{2a_1 - 5a_0, 2a_2 + a_0\}$ GB w.r.t. $a_0 \prec_{lex} a_1 \prec_{lex} a_2$

$m := \text{Remainder}(m, G) = -\frac{1}{2}a_0x^2 + \frac{5}{2}a_0x + a_0$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

$I := \langle 7a_2 + a_1 + a_0, 10a_2 + 2a_1, 15a_2 + 3a_1, 22a_2 + 4a_1 + a_0 \rangle$

$G := \{2a_1 - 5a_0, 2a_2 + a_0\}$ GB w.r.t. $a_0 \prec_{lex} a_1 \prec_{lex} a_2$

$m := \text{Remainder}(m, G) = -\frac{1}{2}a_0x^2 + \frac{5}{2}a_0x + a_0$

$a_0 \neq 0$, so $m := \frac{m}{-\frac{1}{2}a_0} = x^2 - 5x - 2$

Algorithm for Computing Minimal Polynomial

Input $M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$,$M^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$m := a_2x^2 + a_1x + a_0$

$a_2M^2 + a_1M + a_0I_{2\times 2} =$

$$\begin{pmatrix} 7a_2 + a_1 + a_0 & 10a_2 + 2a_1 \\ 15a_2 + 3a_1 & 22a_2 + 4a_1 + a_0 \end{pmatrix} = 0$$

$I := \langle 7a_2 + a_1 + a_0, 10a_2 + 2a_1, 15a_2 + 3a_1, 22a_2 + 4a_1 + a_0 \rangle$

$G := \{2a_1 - 5a_0, 2a_2 + a_0\}$ GB w.r.t. $a_0 \prec_{lex} a_1 \prec_{lex} a_2$

$m := \text{Remainder}(m, G) = -\frac{1}{2}a_0x^2 + \frac{5}{2}a_0x + a_0$

$a_0 \neq 0$, so $m := \frac{m}{-\frac{1}{2}a_0} = x^2 - 5x - 2$

$\Rightarrow$ Minimal polynomial of M is $x^2 - 5x - 2$

Algorithm

Algorithm 3 MinPoly

Require: $M_{n\times n}$

Ensure: Minimal polynomial m of M in x

$I := \langle \sum_{k=0}^{n} a_k M^k[i,j] \mid i,j = 1,\ldots,n\rangle$

$G :=$ A Gröbner basis for I w.r.t. $a_0 \prec_{lex} \ldots \prec_{lex} a_n$

$d :=\mid G \mid$

$m :=$ Remainder$(\sum_{i=0}^{d} a_i x^i, G|_{a_{d+1}=\cdots=a_n=0})$

$m := \frac{m}{\mathrm{LC}(m)}$

Return(m)

A Surprising Example

Timing

M : a random 90×90 matrix

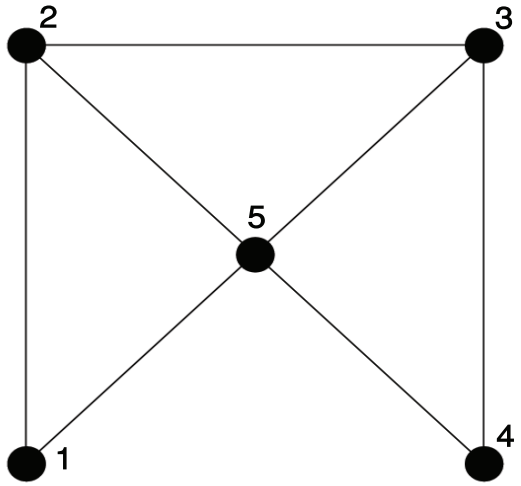
	time (sec)	memory (Gb)
MinPoly	19m39s	8.3
Maple	7h26m33s	74.6

Definition A simple graph G is proper $k-$colorable if one can assign k colors to the vertices of G such that the adjacent vertices receive different colors

Three questions:

- Is a simple graph $k-$colorable?
- If yes, how many solutions?
- If yes, how we can find all the solutions?

Example $3-$colorable?



- Assign x_i to the vertex i
- Correspond a 3-th root of unity to a color
- $I := \langle x_1^3 - 1, \ldots, x_5^3 - 1 \rangle$
- $I := I + \langle x_i^2 + x_i x_j + x_j^2 \mid (i,j) \text{ is an edge} \rangle$

Theorem

The elements of $\mathbf{V}(I)$ provide the different possible colorings and $|\mathbf{V}(I)| =$ the number of colorings

Algorithm for Graph Coloring

- ▷ Compute a Gröbner basis for I
- ▷ if $1 \in G \Rightarrow G$ is not $k-$colorable
- ▷ else, compute $\mathbf{V}(I)$ using G

The corresponsing polynomial system:

$$F := [x_1^3 - 1, \ldots, x_4^2 + x_4 x_5 + x_5^2];$$

`with(Groebner); G:=Basis(F,plex(`$x_1, \ldots, x_5$`));`

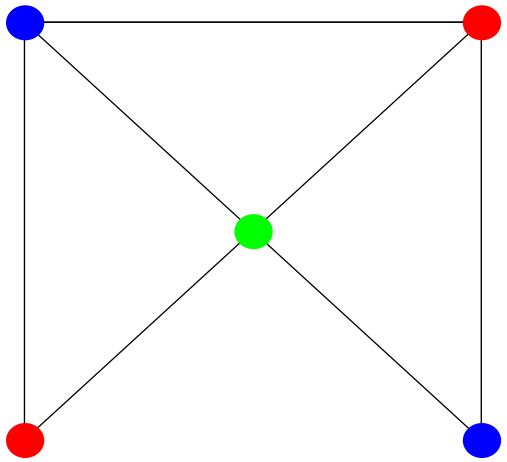
$$G = [x_5^3 - 1, x_4^2 + x_4 x_5 + x_5^2, x_5 + x_3 + x_4, x_2 - x_4, x_1 + x_4 + x_5]$$

Theorem

The set of zeros of F is equal to the one of G.

- $x_5 \in \{1, \omega, \omega^2\}$, we let $x_5 = 1$
- by second equation $x_4 \neq x_5$, so $x_4 \in \{\omega, \omega^2\}$, we set $x_4 = \omega$
- $x_3 = \omega^2, x_2 = \omega, x_1 = \omega^2$.

$$\mathbf{V}(I) = \begin{cases} (\omega & \omega^2 & \omega & \omega^2 & 1 \;) \\ (\omega^2 & \omega & \omega^2 & \omega & 1 \;) \\ (\omega & 1 & \omega & 1 & \omega^2) \\ (1 & \omega & 1 & \omega & \omega^2) \\ (\omega^2 & 1 & \omega^2 & 1 & \omega \;) \\ (1 & \omega^2 & 1 & \omega^2 & \omega \;) \end{cases}$$



Jacobian Conjecture

Theorem (Inverse function theorem)

- *Consider* $F : K^n \mapsto K^n$ *with* $F(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$
- *Suppose that* $J(F) = \det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \ldots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$

$\Rightarrow$ *If* $J(F)(p) \neq 0$ *then* F *has a local inverse at* $p \in K^n$.

Jacobian Conjecture

Theorem (Inverse function theorem)

- *Consider* $F : K^n \mapsto K^n$ *with* $F(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$
- *Suppose that* $J(F) = \det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \ldots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$

$\Rightarrow$ *If* $J(F)(p) \neq 0$ *then* F *has a local inverse at* $p \in K^n$.

Example

- We consider $F(x, y) = (e^x cos(y), e^x sin(y))$ then
- $J(F) = e^{2x}$ and therefore

$\Rightarrow$ F has a local inverse at each point (no global).

Jacobian Conjecture (cont.)

Jacobian conjecture

- ▷ If $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n]$ and $J(F) \in \mathbb{C} \setminus \{0\}$
- $\Rightarrow$ F has a global inverse.

History

- ▷ It was first posed in 1939 by Ott-Heinrich Keller,
- ▷ Wang in 1980 proved it for polynomials of degree 2,
- ▷ It is still open for degree ≥ 3.

Jacobian Conjecture (cont.)

Theorem

- ▷ *Let* $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle$.
- ▷ $G = Basis(I, plex(x_1, \ldots, x_n, y_1, \ldots, y_n))$.

⇒ *Then* F *has a global inverse iff* $G = \{x_1 - g_1, \ldots, x_n - g_n\}$ *with* $g_i \in K[y_1, \ldots, y_n]$.

Jacobian Conjecture (cont.)

Theorem

- ▷ *Let* $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle$.
- ▷ $G = Basis(I, plex(x_1, \ldots, x_n, y_1, \ldots, y_n))$.

⇒ *Then* F *has a global inverse iff* $G = \{x_1 - g_1, \ldots, x_n - g_n\}$ *with* $g_i \in K[y_1, \ldots, y_n]$.

Example

- ▷ $F(x_1, x_2) = (x_1 + (x_1 + x_2)^3, x_2 - (x_1 + x_2)^3)$
- ▷ $G = \{x_1 - y_1 + (y_1 + y_2)^3, x_2 - y_1 - (y_1 + y_2)^3\}$.

Jacobian Conjecture (cont.)

Theorem

- ▷ *Let* $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle$.
- ▷ $G = Basis(I, plex(x_1, \ldots, x_n, y_1, \ldots, y_n))$.
- ⇒ *Then* F *has a global inverse iff* $G = \{x_1 - g_1, \ldots, x_n - g_n\}$ *with* $g_i \in K[y_1, \ldots, y_n]$.

Example

- ▷ $F(x_1, x_2) = (x_1 + (x_1 + x_2)^3, x_2 - (x_1 + x_2)^3)$
- ▷ $G = \{x_1 - y_1 + (y_1 + y_2)^3, x_2 - y_1 - (y_1 + y_2)^3\}$.
- ⇒ Thus F has a global local inverse ($J(F) = 1$),

Jacobian Conjecture (cont.)

Theorem

- ▷ *Let* $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle$.
- ▷ $G = Basis(I, plex(x_1, \ldots, x_n, y_1, \ldots, y_n))$.
- ⇒ *Then* F *has a global inverse iff* $G = \{x_1 - g_1, \ldots, x_n - g_n\}$ *with* $g_i \in K[y_1, \ldots, y_n]$.

Example

- ▷ $F(x_1, x_2) = (x_1 + (x_1 + x_2)^3, x_2 - (x_1 + x_2)^3)$
- ▷ $G = \{x_1 - y_1 + (y_1 + y_2)^3, x_2 - y_1 - (y_1 + y_2)^3\}$.
- ⇒ Thus F has a global local inverse ($J(F) = 1$),
- ⇒ $F^{-1}(y_1, y_2) = (y_1 - (y_1 + y_2)^3, y_1 + (y_1 + y_2)^3)$.

Lattice

Definition: Orderly Lattice

A poset $(L, \leq)$ is called a Lattice, if

$$\forall a, b \in L, \quad \sup\{a, b\}, \inf\{a, b\} \in L$$

Lattice

Definition: Orderly Lattice

A poset $(L, \leq)$ is called a Lattice, if

$$\forall a, b \in L, \quad \sup\{a, b\}, \inf\{a, b\} \in L$$

Definition: Algebraic Lattice

- L : a set;
- $\vee, \wedge$: two binary operations on L;
- $(L, \vee, \wedge)$ is a Lattice, if for all $a, b, c \in L$:

Commutative $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$

Associative $a \vee (b \vee c) = (a \vee b) \vee c, \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$

Absorptance $a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$

$(L, \leq) = (L, \vee, \wedge)$

Orderly $\Leftrightarrow$ Algebraic

Orderly $\Rightarrow$ Algebraic Let: $a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}$

Algebraic $\Rightarrow$ Orderly Define: $a \leq b \Leftrightarrow a \vee b = b \ (or \ a \wedge b = a)$

$(L, \leq) = (L, \vee, \wedge)$

Orderly $\Leftrightarrow$ Algebraic

Orderly $\Rightarrow$ Algebraic Let: $a \vee b = \sup\{a, b\}, \quad a \wedge b = \inf\{a, b\}$

Algebraic $\Rightarrow$ Orderly Define: $a \leq b \Leftrightarrow a \vee b = b \ (or \ a \wedge b = a)$

Example

Let A be a set;

$$(P(A), \subseteq) = (P(A), \cup, \cap)$$

Distributive Lattice

Definition

A lattice L is distributive, if for each $a, b, c \in L$

$$\begin{aligned} a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \quad \text{and} \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \end{aligned}$$

Distributive Lattice

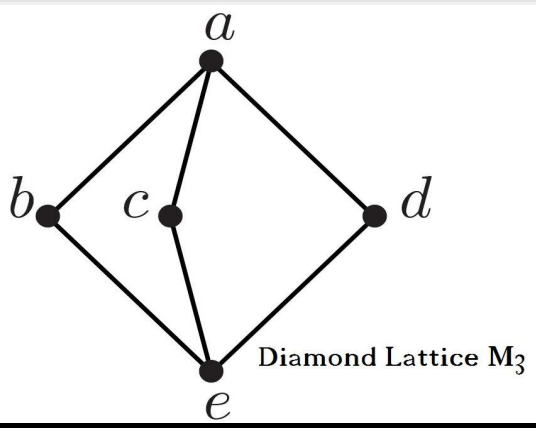
Definition

A lattice L is distributive, if for each $a, b, c \in L$

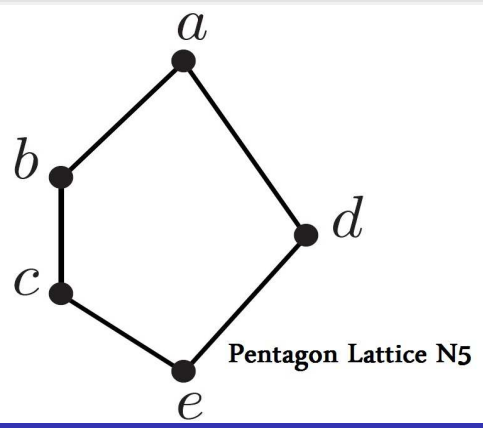
$$\begin{aligned} a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \quad \text{and} \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \end{aligned}$$

Theorem

L is distributive if and only if none of its sublattices is isomorphic to M_3 or N_5.



Diamond Lattice M_3



Pentagon Lattice N5

Problem

Lattice Distributivity Problem

▷ How can we determine whether a finite lattice is distributive?

- L: a finite lattice
- $I_L := \langle z_a z_b - z_{a \wedge b} z_{a \vee b} \mid a, b \in L \rangle \subset K[z_a \mid a \in L]$

- L: a finite lattice
- $I_L := \langle z_a z_b - z_{a\wedge b} z_{a\vee b} \mid a, b \in L \rangle \subset K[z_a \mid a \in L]$

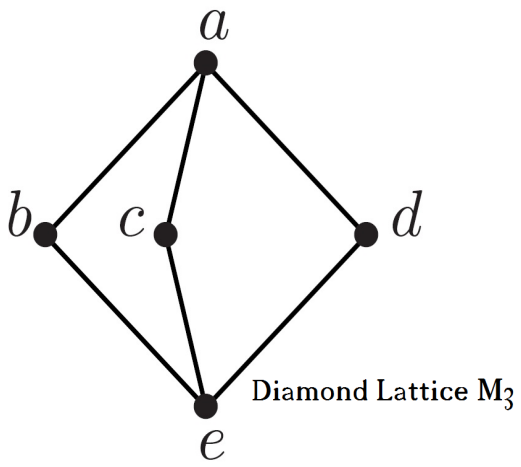
Theorem: (a)⇒ (b): Hibi, 1987, (b)⇒ (a): Qureshi, 2012

The following are equivalent:

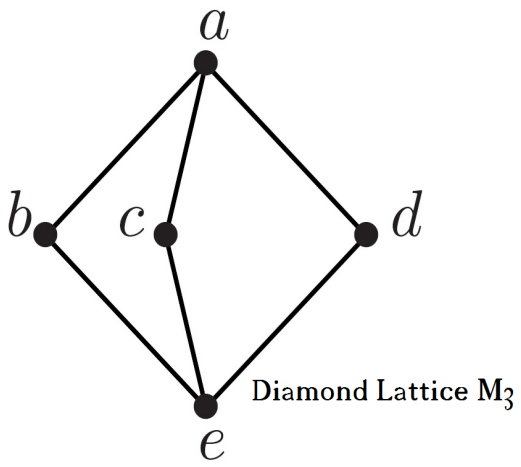
(a) L is distributive,

(b) $G_L := \{z_a z_b - z_{a\wedge b} z_{a\vee b} \mid a, b \in L \text{ are incomparable}\}$ is a Gröbner basis for I_L w.r.t. each rank reverse lexicographic ordering.

Example:

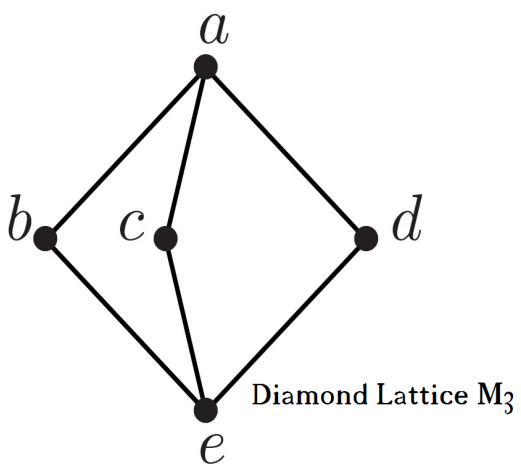


Example:



$G_{M_3} = \{z_b z_c - z_a z_e, z_b z_d - z_a z_e, z_c z_d - z_a z_e\}$ is not a Gröbner basis w.r.t. $z_e \prec z_b \prec z_c \prec z_d \prec z_a$, because:

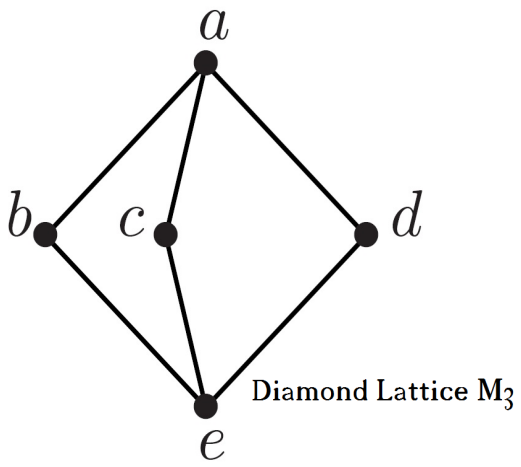
Example:



$G_{M_3} = \{z_b z_c - z_a z_e, z_b z_d - z_a z_e, z_c z_d - z_a z_e\}$ is not a Gröbner basis w.r.t. $z_e \prec z_b \prec z_c \prec z_d \prec z_a$, because:

$$\mathrm{LM}(\mathrm{Spoly}(z_b z_c - z_a z_e, z_b z_d - z_a z_e)) = z_d z_a z_e \notin \mathrm{LM}(G_{M_3})$$

Example:



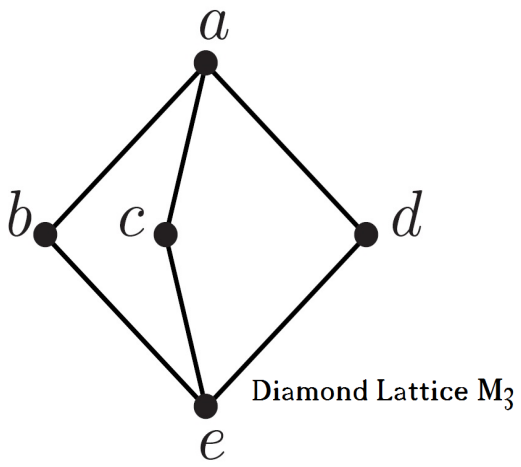
$G_{M_3} = \{z_b z_c - z_a z_e, z_b z_d - z_a z_e, z_c z_d - z_a z_e\}$ is not a Gröbner basis w.r.t. $z_e \prec z_b \prec z_c \prec z_d \prec z_a$, because:

$$\mathrm{LM}(\mathrm{Spoly}(z_b z_c - z_a z_e, z_b z_d - z_a z_e)) = z_d z_a z_e \notin \mathrm{LM}(G_{M_3})$$

Result

M_3 is not distributive.

Example:



$G_{M_3} = \{z_b z_c - z_a z_e, z_b z_d - z_a z_e, z_c z_d - z_a z_e\}$ is not a Gröbner basis w.r.t. $z_e \prec z_b \prec z_c \prec z_d \prec z_a$, because:

$$\mathrm{LM}(\mathrm{Spoly}(z_b z_c - z_a z_e, z_b z_d - z_a z_e)) = z_d z_a z_e \notin \mathrm{LM}(G_{M_3})$$

Result

M_3 is not distributive.

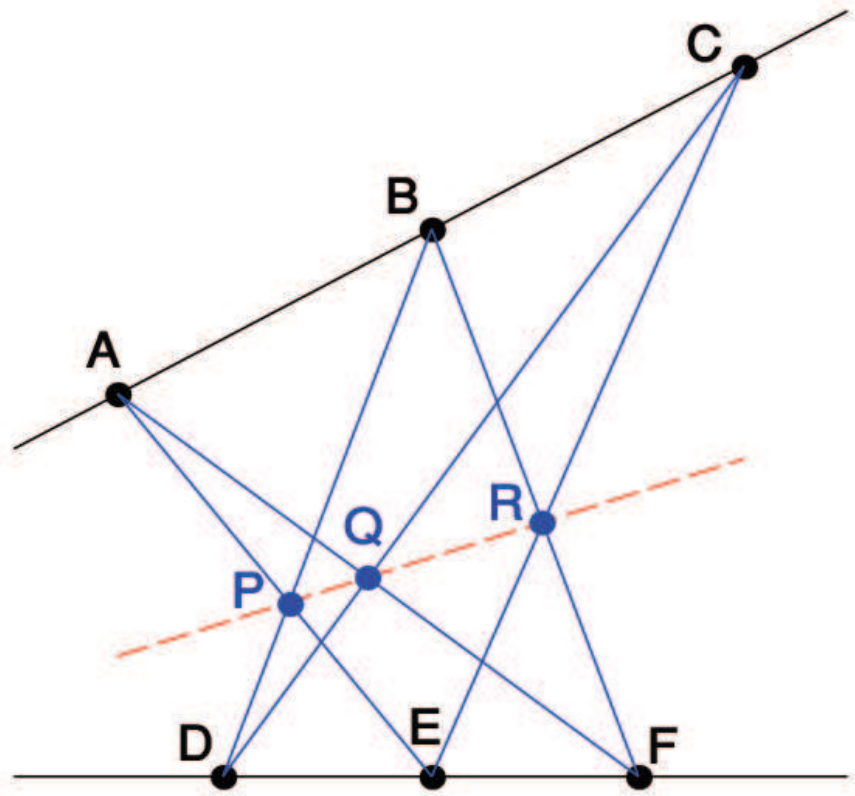
Note

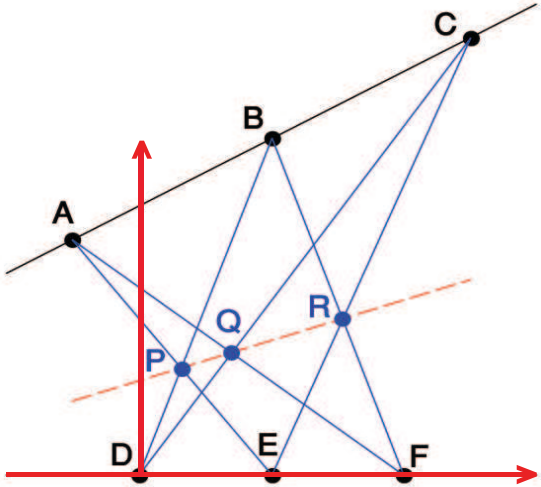
$$b = b \wedge (c \vee d) \neq (b \wedge c) \vee (b \wedge d) = e$$

Automatic Geometry Theorem Proving

Example

Pappus theorem: P, Q and R are collinear





Coordinate of points:

$D := (0,0) \quad E := (u_1, 0) \quad F := (u_2, 0)$

$A := (u_3, u_4) \; B := (u_5, u_6) \; C := (u_7, x_1)$

$P := (x_2, x_3) \; Q := (x_4, x_5) \; R := (x_6, x_7)$

- Since A, B, C are colinear, we have $\frac{u_5 - u_3}{u_6 - u_4} = \frac{u_7 - u_3}{x_1 - u_4}$, and so from the collinearity of points we obtain:

- Since A, B, C are colinear, we have $\frac{u_5-u_3}{u_6-u_4} = \frac{u_7-u_3}{x_1-u_4}$, and so from the collinearity of points we obtain:
- Hypothesis polynomials

$$
\begin{aligned}
h_1 &:= x_1u_3 + u_6u_7 - u_6u_3 - x_1u_5 - u_4u_7 + u_4u_5 \\
h_2 &:= u_4u_1 + x_3u_3 - x_3u_1 - u_4x_2 \\
h_3 &:= u_5x_3 - u_6x_2 \\
h_4 &:= u_4u_2 + x_5u_3 - x_5u_2 - u_4x_4 \\
h_5 &:= u_7x_5 - x_1x_4 \\
h_6 &:= u_6u_2 + x_7u_5 - x_7u_2 - u_6x_6 \\
h_7 &:= x_1u_1 + x_7u_7 - x_7u_1 - x_1x_6
\end{aligned}
$$

- Since A, B, C are colinear, we have $\frac{u_5-u_3}{u_6-u_4} = \frac{u_7-u_3}{x_1-u_4}$, and so from the collinearity of points we obtain:
- Hypothesis polynomials

$$
\begin{aligned}
h_1 &:= x_1u_3 + u_6u_7 - u_6u_3 - x_1u_5 - u_4u_7 + u_4u_5 \\
h_2 &:= u_4u_1 + x_3u_3 - x_3u_1 - u_4x_2 \\
h_3 &:= u_5x_3 - u_6x_2 \\
h_4 &:= u_4u_2 + x_5u_3 - x_5u_2 - u_4x_4 \\
h_5 &:= u_7x_5 - x_1x_4 \\
h_6 &:= u_6u_2 + x_7u_5 - x_7u_2 - u_6x_6 \\
h_7 &:= x_1u_1 + x_7u_7 - x_7u_1 - x_1x_6
\end{aligned}
$$

- Conclusion polynomial

$$g := x_7x_2 + x_5x_6 - x_5x_2 - x_7x_4 - x_3x_6 + x_3x_4$$

- $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

- $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

- $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

Theorem

Conclusion is true iff the reduced Gröbner basis of

$$\langle h_1, \ldots, h_r, 1 - yg \rangle \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n, y]$$

equals to $\{1\}$

▷ $I := \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}[x_1, \ldots, x_n, u_1, \ldots, u_m]$

Theorem

Conclusion is true iff the reduced Gröbner basis of

$$\langle h_1, \ldots, h_r, 1 - yg \rangle \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n, y]$$

equals to $\{1\}$

The reduced Gröbner basis of

$$\langle h_1, \ldots, h_7, 1 - yg \rangle \subset \mathbb{R}(u_1, \ldots, u_7)[x_1, \ldots, x_7, y]$$

is $\{1\}$, so the Pappus theorem is proved.

Frobenius Problem

- $a_1 \leq a_2 \leq \cdots \leq a_r$ natural numbers
- $\gcd(a_1, \ldots, a_r) = 1$
- $N(a_1, \ldots, a_r) := \max\{n \in \mathbb{N} \mid n \neq \lambda_1 a_1 + \cdots + \lambda_r a_r\}$
- Frobenius problem : Find $N(a_1, \ldots, a_r)$

Example

- $N(5, 7) = 23$
- $N(11, 13, 17) = 53$
- $N(238, 569, 791) = 18205$

- $I := \langle x_1 - t^{a_1}, \ldots, x_r - t^{a_r} \rangle \subset \mathbb{Q}[x_1, \ldots, x_r, t]$

- $I := \langle x_1 - t^{a_1}, \ldots, x_r - t^{a_r} \rangle \subset \mathbb{Q}[x_1, \ldots, x_r, t]$
- G:= A Gröbner basis for I w.r.t. $x_i \prec_{lex} t$

- $I := \langle x_1 - t^{a_1}, \ldots, x_r - t^{a_r} \rangle \subset \mathbb{Q}[x_1, \ldots, x_r, t]$
- G:= A Gröbner basis for I w.r.t. $x_i \prec_{lex} t$

- $I := \langle x_1 - t^{a_1}, \ldots, x_r - t^{a_r} \rangle \subset \mathbb{Q}[x_1, \ldots, x_r, t]$
- G:= A Gröbner basis for I w.r.t. $x_i \prec_{lex} t$

Theorem

$N = \lambda_1 a_1 + \cdots + \lambda_r a_r$ *iff* *remainder*$(t^N, G) = x_1^{\lambda_1} \cdots x_r^{\lambda_r}$

Example

McNugget numbers $N(6, 9, 20) = 43$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=$\mathrm{Basis}(J, plex(t, x_1, x_2, x_3));$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=$\mathrm{Basis}(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

$$t x_1 x_2^4$$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

$$t x_1 x_2^4$$

NormalForm$(t^{44}, G, plex(t, x_1, x_2, x_3));$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

$$t x_1 x_2^4$$

NormalForm$(t^{44}, G, plex(t, x_1, x_2, x_3));$

$$x_1 x_2^2 x_3 \Rightarrow 44 = 1 \times 6 + 2 \times 9 + 1 \times 20$$

...

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

$$t x_1 x_2^4$$

NormalForm$(t^{44}, G, plex(t, x_1, x_2, x_3));$

$$x_1 x_2^2 x_3 \Rightarrow 44 = 1 \times 6 + 2 \times 9 + 1 \times 20$$

...

NormalForm$(t^{50}, G, plex(t, x_1, x_2, x_3));$

Example

McNugget numbers $N(6,9,20) = 43$

$J := \langle x_1 - t^6, x_2 - t^9, x_3 - t^{20} \rangle :$

G:=Basis$(J, plex(t, x_1, x_2, x_3));$

NormalForm$(t^{41}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2 x_3 \Rightarrow 41 = 2 \times 6 + 1 \times 9 + 1 \times 20$$

NormalForm$(t^{43}, G, plex(t, x_1, x_2, x_3));$

$$t x_1 x_2^4$$

NormalForm$(t^{44}, G, plex(t, x_1, x_2, x_3));$

$$x_1 x_2^2 x_3 \Rightarrow 44 = 1 \times 6 + 2 \times 9 + 1 \times 20$$

...

NormalForm$(t^{50}, G, plex(t, x_1, x_2, x_3));$

$$x_1^2 x_2^2 x_3 \Rightarrow 50 = 2 \times 6 + 2 \times 9 + 1 \times 20$$

N	Remainder	λ_i's
53	$x_2^4 t$	$-$
54	$x_1 x_2^2 x_3$	$[1,2,1]$
55	x_1^5	$[5,0,0]$
56	$x_2^3 x_3$	$[0,3,1]$
57	$x_1^4 x_2$	$[4,1,0]$
58	$x_1 x_2 x_3^2$	$[1,1,2]$
59	$x_1^3 x_2^2$	$[3,2,0]$
60	$x_2^2 x_3^2$	$[0,2,2]$
61	$x_1^2 x_2^3$	$[2,3,0]$
62	$x_1 x_3^3$	$[1,0,3]$
63	$x_1 x_2^4$	$[1,4,0]$
64	$x_2 x_3^3$	$[0,1,3]$

$\Rightarrow \quad N(11,13,17) = 53$

Solving Linear Diophantine Systems [Conti-Traverso, 1991]

Consider $a_{ij}, b_i \in \mathbb{N}$ and the following Diophantine systems:

$$\begin{cases} a_{11}\sigma_1 & + & \cdots & + & a_{1n}\sigma_n & = & b_1 \\ & & \vdots & & & & \\ a_{m1}\sigma_1 & + & \cdots & + & a_{mn}\sigma_n & = & b_m. \end{cases}$$

- $I := \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}} \rangle$

Solving Linear Diophantine Systems [Conti-Traverso, 1991]

Consider $a_{ij}, b_i \in \mathbb{N}$ and the following Diophantine systems:

$$\begin{cases} a_{11}\sigma_1 & + & \cdots & + & a_{1n}\sigma_n & = & b_1 \\ & & \vdots & & & & \\ a_{m1}\sigma_1 & + & \cdots & + & a_{mn}\sigma_n & = & b_m. \end{cases}$$

- $I := \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}} \rangle$
- $G =$ Gröbner basis of I w.r.t $y_i \prec_{lex} x_j$

Solving Linear Diophantine Systems [Conti-Traverso, 1991]

Consider $a_{ij}, b_i \in \mathbb{N}$ and the following Diophantine systems:

$$\begin{cases} a_{11}\sigma_1 & + & \cdots & + & a_{1n}\sigma_n & = & b_1 \\ & & \vdots & & & & \\ a_{m1}\sigma_1 & + & \cdots & + & a_{mn}\sigma_n & = & b_m. \end{cases}$$

- $I := \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}} \rangle$
- $G =$ Gröbner basis of I w.r.t $y_i \prec_{lex} x_j$
- $x_1^{b_1} \cdots x_m^{b_m} \rightsquigarrow_G h$

Solving Linear Diophantine Systems [Conti-Traverso, 1991]

Consider $a_{ij}, b_i \in \mathbb{N}$ and the following Diophantine systems:

$$\begin{cases} a_{11}\sigma_1 & + & \cdots & + & a_{1n}\sigma_n & = & b_1 \\ & & \vdots & & & & \\ a_{m1}\sigma_1 & + & \cdots & + & a_{mn}\sigma_n & = & b_m. \end{cases}$$

- $I := \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}} \rangle$
- $G =$ Gröbner basis of I w.r.t $y_i \prec_{lex} x_j$
- $x_1^{b_1} \cdots x_m^{b_m} \rightsquigarrow_G h$
- $h = y_1^{\sigma_1} \cdots y_n^{\sigma_n} \Leftrightarrow (\sigma_1, \ldots, \sigma_n)$ is a natural solution.

Solving Linear Diophantine Systems (cont.)

Example

$$\triangleright \begin{cases} 3\sigma_1 & +2\sigma_2 & +\sigma_3 & + & \sigma_4 & = & 10 \\ 4\sigma_1 & +\sigma_2 & +\sigma_3 & + & & = & 5. \end{cases}$$

Solving Linear Diophantine Systems (cont.)

Example

- $\begin{cases} 3\sigma_1 & +2\sigma_2 & +\sigma_3 & + & \sigma_4 & = & 10 \\ 4\sigma_1 & +\sigma_2 & +\sigma_3 & + & & = & 5. \end{cases}$
- $I := \langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \rangle,$

Solving Linear Diophantine Systems (cont.)

Example

- $\begin{cases} 3\sigma_1 & +2\sigma_2 & +\sigma_3 & + & \sigma_4 & = & 10 \\ 4\sigma_1 & +\sigma_2 & +\sigma_3 & + & & = & 5. \end{cases}$
- $I := \langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \rangle$,
- Gröbner basis of I w.r.t $y_i \prec_{lex} x_j$ is:

$$\{y_2 - y_3 y_4, y_1 y_4 - y_3^4, x_2 y_4 - y_3, x_2 y_3^3 - y_1, x_1 - y_4\}$$

Solving Linear Diophantine Systems (cont.)

Example

- $\begin{cases} 3\sigma_1 & +2\sigma_2 & +\sigma_3 & + & \sigma_4 & = & 10 \\ 4\sigma_1 & +\sigma_2 & +\sigma_3 & + & & = & 5. \end{cases}$
- $I := \langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \rangle$,
- Gröbner basis of I w.r.t $y_i \prec_{lex} x_j$ is:

$$\{y_2 - y_3 y_4, y_1 y_4 - y_3^4, x_2 y_4 - y_3, x_2 y_3^3 - y_1, x_1 - y_4\}$$

$\Rightarrow$ $x_1^{10} x_2^5 \rightsquigarrow_G y_3^5 y_4^5$ and $(0, 0, 5, 5)$ is a solution.

Integer Solutions

- z; a new variable
- $I := \langle y_1 - x_1^{a_{11}} \cdots x_m^{a_{m1}}, \ldots, y_n - x_1^{a_{1n}} \cdots x_m^{a_{mn}}, y_1 \cdots y_n z - 1 \rangle$
- $G =$ Gröbner basis of I w.r.t $z \prec_{lex} y_i \prec_{lex} x_j$
- $x_1^{b_1} \cdots x_m^{b_m} \rightsquigarrow_G h$

Theorem (Hashemi, 2013)

The has an integer solution iff $h \in K[y_1, \ldots, y_n, z]$. Moreover, if the remainder is $y_1^{\alpha_1} \cdots y_n^{\alpha_n} z^{\alpha}$, then $(\alpha_1 - \alpha, \ldots, \alpha_n - \alpha)$ is a solution of the system.

Example

$$\begin{cases} 12\sigma_1 + 7\sigma_2 + 9\sigma_3 = 12 \\ 5\sigma_2 + 8\sigma_3 + 10\sigma_4 = 0 \\ 15\sigma_1 + 21\sigma_3 + 69\sigma_4 = 3. \end{cases}$$

$$I = \langle y_1 - x_1^{12}x_3^{15}, y_2 - x_1^7x_2^5, y_3 - x_1^9x_2^8x_3^{21}, y_4 - x_2^{10}x_3^{69}, y_1y_2y_3y_4z - 1\rangle$$

$G =$ Gröbner basis of I w.r.t $z \prec_{lex} y_i \prec_{lex} x_j$

$x_1^{12}x_3^3 \rightsquigarrow_G z^{336}y_1^{293}y_3^{656}y_4^{248}$

$(293, 0, 656, 248) - (336, 336, 336, 336) = (-43, -336, 320, -88)$
an integer solution

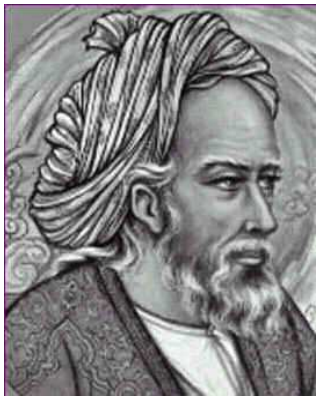
Since $z^{2056}y_1^{1819}y_2^{238}y_3^{3786}y_4^{1581} - 1 \in I$, we have the general solution $(-237k - 43, -1818k - 336, 1730k + 320, -475k - 88)$

Gröbner Bases and Tilings

Amir Hashemi

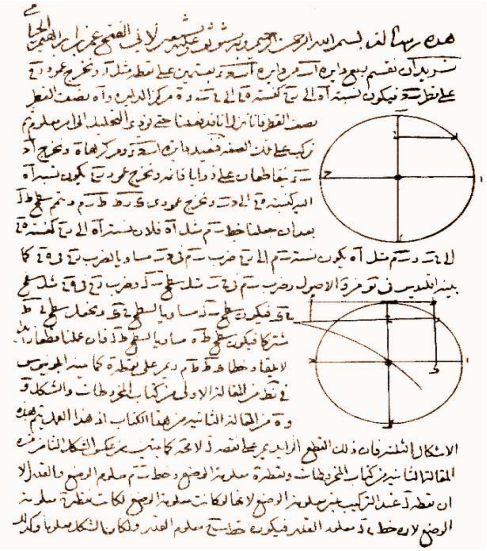
Isfahan University of Technology & IPM

CIMPA-IRAN school on Tilings and Tessellations, Isfahan, Iran, 2015



Hakim Abolfath Omar ebn Ibrahim Khayyám Nieshapuri (18 May 1048 -4 December 1131), born in Nishapur in North Eastern Iran, was a great Persian polymath, philosopher, mathematician, astronomer and poet, who wrote treatises on mechanics, geography, mineralogy, music, and Islamic theology.

Khayyám was famous during his times as a mathematician. He wrote the influential treatise on *demonstration of problems of algebra (1070)*, which laid down the principles of algebra, part of the body of Persian Mathematics that was eventually transmitted to Europe. In particular, he derived general methods for *solving cubic equations and even some higher orders*.



He wrote on *the triangular array of binomial coefficients* known as Khayyám-Pascal's triangle. In 1077, Khayyám also wrote a book published in English as "On the Difficulties of Euclid's Definitions". An important part of the book is concerned with Euclid's famous parallel postulate and his approach made their way to Europe, and may have contributed to the eventual development of non-Euclidean geometry.

Notations

- So far, we have considered $R = K[x_1, \ldots, x_n]$
- and discussed Gröbner bases over fields + applications
- In this part, we consider $A = \mathbb{Z}[x_1, \ldots, x_n]$
- We discuss Gröbner bases over integers
- and review its application in tilings.

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$
- i.e. $2x \nmid 3x$

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$
- i.e. $2x \nmid 3x$
- Further, in A we have $3x \nmid x$ and $2x \nmid x$ however $x \in \langle 2x, 3x \rangle$

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$
- i.e. $2x \nmid 3x$
- Further, in A we have $3x \nmid x$ and $2x \nmid x$ however $x \in \langle 2x, 3x \rangle$
- Thus $f = x + 1$ is reducible by $\{f_1 = 2x + 3, f_2 = 3x - 5\}$, i.e. $f \rightsquigarrow f - (f_2 - f_1) = (x + 1) - (3x - 5 - 2x - 3) = 9$.

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$
- i.e. $2x \nmid 3x$
- Further, in A we have $3x \nmid x$ and $2x \nmid x$ however $x \in \langle 2x, 3x \rangle$
- Thus $f = x + 1$ is reducible by $\{f_1 = 2x + 3, f_2 = 3x - 5\}$, i.e. $f \rightsquigarrow f - (f_2 - f_1) = (x + 1) - (3x - 5 - 2x - 3) = 9$.

Main Problem

☞ Main obstacle in theory of Gröbner bases over $\mathbb{Z}$ is division. Let us consider the polynomial ring $R = K[x_1, \ldots, x_n]$. In this ring we have $2x \mid 3x$. However that does not hold in

- $A = \mathbb{Z}[x_1, \ldots, x_n]$
- i.e. $2x \nmid 3x$
- Further, in A we have $3x \nmid x$ and $2x \nmid x$ however $x \in \langle 2x, 3x \rangle$
- Thus $f = x + 1$ is reducible by $\{f_1 = 2x + 3, f_2 = 3x - 5\}$, i.e. $f \rightsquigarrow f - (f_2 - f_1) = (x + 1) - (3x - 5 - 2x - 3) = 9$.

Thus, $\mathrm{LT}(f)$ is divisible by none of $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ however, it is reducible by a combination of $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$

Example

Example

- $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$
- $f = xy - 1, f_1 = 7x + 3, f_2 = 3y - 5$
- We note that $\mathrm{LT}(f_1) \nmid \mathrm{LT}(f)$ and $\mathrm{LT}(f_2) \nmid \mathrm{LT}(f)$
- however, $xy \in \langle 7x, 3y \rangle_{\mathbb{Z}[x,y]} \rightsquigarrow xy = y(7x) - 2x(3y)$
- $f - (yf_1 - 2xf_2) = -3y - 10x - 1.$

Gröbner Bases

Definition

- $I \subset A$
- $\prec$ a monomial ordering
- A finite set $G \subset I$ is a Gröbner Basis for I w.r.t. $\prec$, if

$$\forall f \in I \; \exists g \in G \text{ s.t. } \mathrm{LT}(g) \mid \mathrm{LT}(f)$$

Existence of Gröbner bases

Each ideal has a Gröbner basis

Membership problem

$f \in I$ iff $f \rightsquigarrow_G 0$

Example

☞ $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$

- $f_1 = 4x + 1, f_2 = 6y + 1$ and $I = \langle f_1, f_2 \rangle$

Example

☞ $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$

- $f_1 = 4x + 1, f_2 = 6y + 1$ and $I = \langle f_1, f_2 \rangle$
- $f := 3yf_1 - 2xf_2 = 3y - 2x$ and $\mathrm{LT}(f) = -2x \notin \langle 4x, 6y \rangle$

Example

☞ $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$

- $f_1 = 4x + 1, f_2 = 6y + 1$ and $I = \langle f_1, f_2 \rangle$
- $f := 3yf_1 - 2xf_2 = 3y - 2x$ and $\mathrm{LT}(f) = -2x \notin \langle 4x, 6y \rangle$

Example

☞ $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$

- $f_1 = 4x + 1, f_2 = 6y + 1$ and $I = \langle f_1, f_2 \rangle$
- $f := 3yf_1 - 2xf_2 = 3y - 2x$ and $\mathrm{LT}(f) = -2x \notin \langle 4x, 6y \rangle$

$\{f_1, f_2\}$ is not a Gröbner basis for I

Gröbner Bases Calculation over Integers

- The process is the same as Buchberger's algorithm over fields
- The only difference is the division algorithm

Gröbner Bases Calculation over Integers

- The process is the same as Buchberger's algorithm over fields
- The only difference is the division algorithm

Example

▷ $A = \mathbb{Z}[x, y]$ and $y \prec_{lex} x$

▷ $f_1 = 2x + 1, f_2 = 3y + 1$ and $I = \langle f_1, f_2 \rangle$

$$\mathrm{Spoly}(f_1, f_2) = \frac{lcm(\mathrm{LT}(f_1),\mathrm{LT}(f_2))}{\mathrm{LT}(f_1)} f_1 - \frac{lcm(\mathrm{LT}(f_1),\mathrm{LT}(f_2))}{\mathrm{LT}(f_2)} f_2$$

$$\mathrm{Spoly}(f_1, f_2) = \frac{6xy}{2x} f_1 - \frac{6xy}{3y} f_2 = 3y f_1 - 2x f_2 = 3y - 2x$$

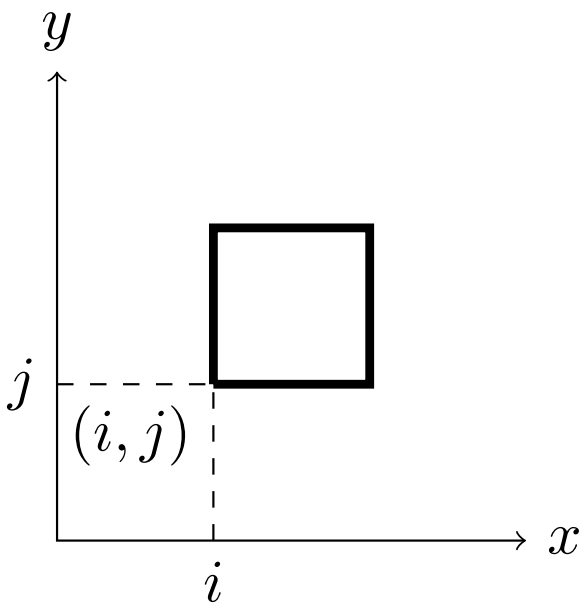
▷ $\mathrm{Spoly}(f_1, f_2) \rightsquigarrow \mathrm{Spoly}(f_1, f_2) + f_1 = 3y + 1 \rightsquigarrow_{f_2} 0$.

So, $\{f_1, f_2\}$ is a Gröbner basis for I

Polynomial Model

Definition

- A *celle* is the square
  $c(i,j) = \{(x,y) \mid i \leq x < i+1, j \leq y < j+1\}$
- To a celle $c(i,j)$ we associate the polynomial $\mathcal{P}_{c(i,j)} = x^i y^j$



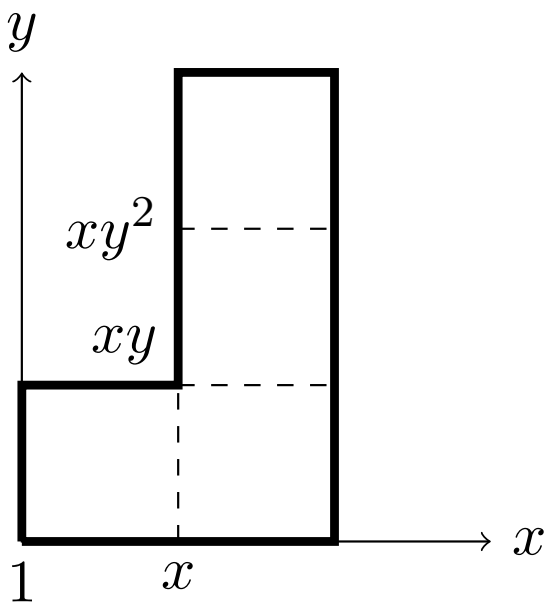
Polynomial Model (cont.)

- A *polyomino* is a finite union of celles

Definition

$T = \cup_{(i,j)\in\Lambda} c(i,j)$ then define $\mathcal{P}_T = \sum_{(i,j)\in\Lambda} \mathcal{P}_{c(i,j)}$.

- We associate $1 + x + xy + xy^2$ to the following polyomino



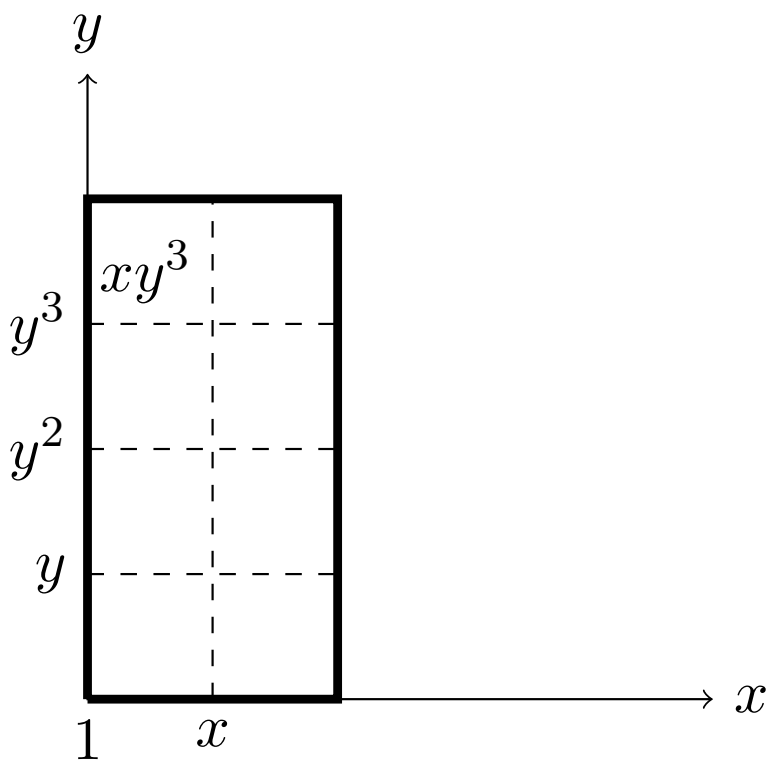
$\mathbb{Z}$-Tiling

- P: A polyomino
- F: A finite set of polyominoes

$\mathbb{Z}$-tiling problem is a finite number of translated polyominoes from F to cover P so that the sum of signs on P at each cell is $+1$.

Example

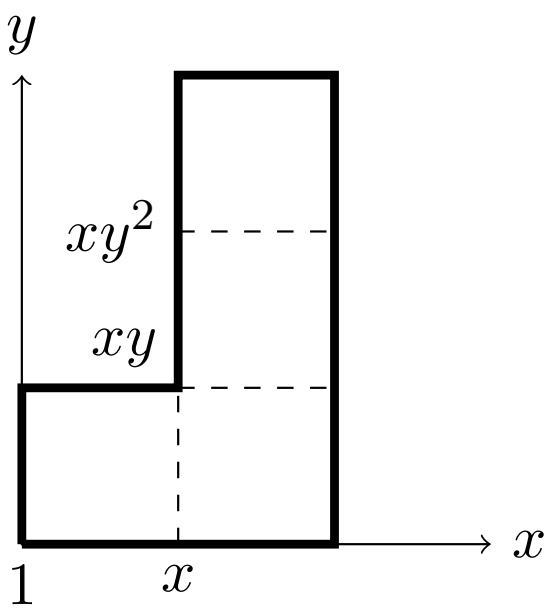
We consider the following polyomio P



☞ We associate the polynomial $f = 1 + x + y + \cdots + xy^3$.

Example (cont.)

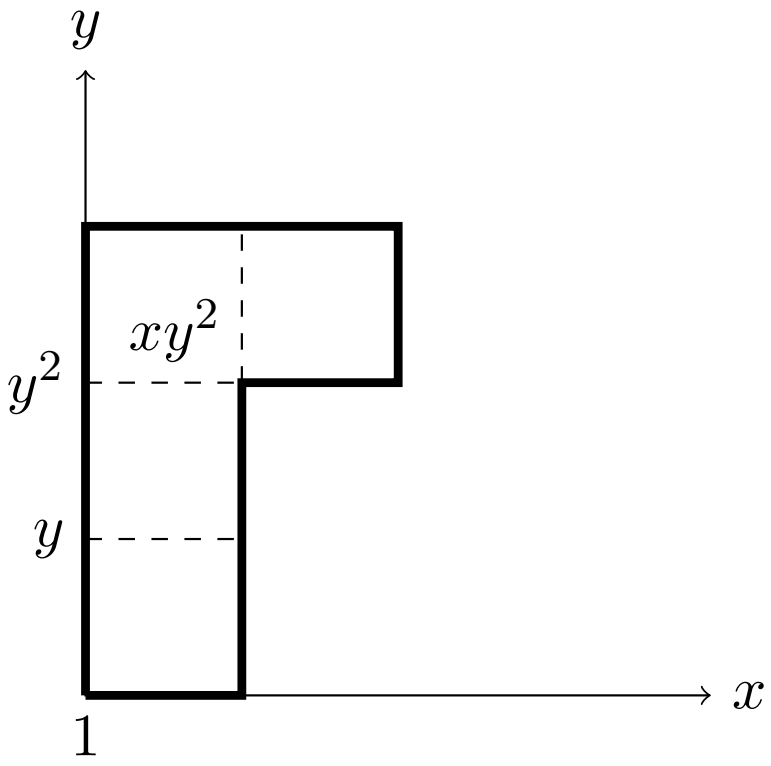
and we would like to cover it by the following polyomino T



☞ we associate the polynomial $f_1 = 1 + x + xy + xy^2$.

Example (cont.)

☞ so we shall consider all (four) rotations of T, e.g.

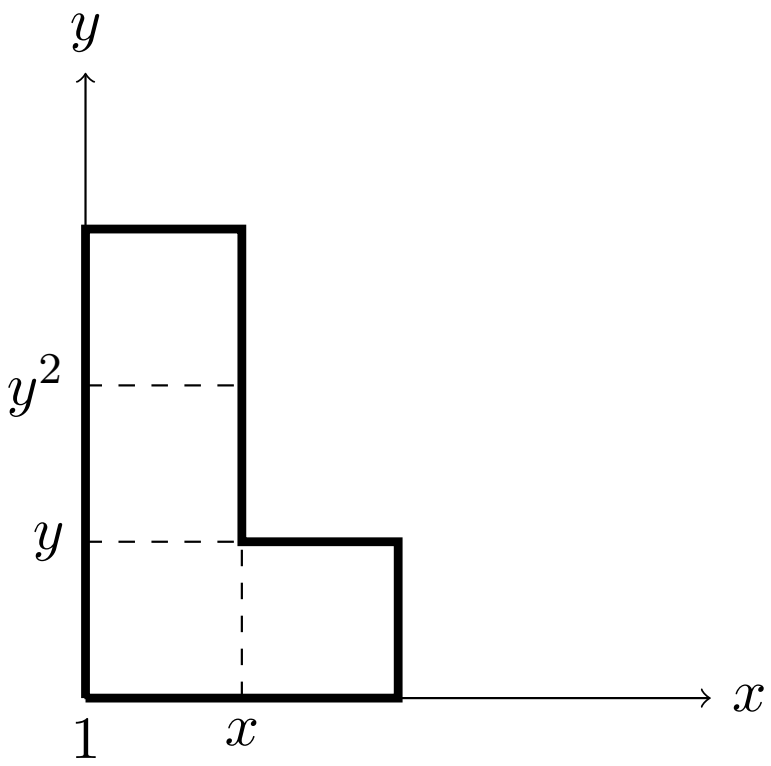


☞ we associate the polynomial $f_2 = 1 + y + y^2 + xy^2$.

☞ Let f_2, f_3, f_4 be associated poly of all rotations

Example (cont.)

- In addition, we shall consider all rotations of the reflection of T



- we associate the polynomial $g_1 = 1 + y + y^2 + x$.
- Let g_2, g_3, g_4 be associated poly of all rotations

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

- we can do this check by Gröbner bases over integers

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

- we can do this check by Gröbner bases over integers
- Let G be the Gröbner basis of this ideal

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

- we can do this check by Gröbner bases over integers
- Let G be the Gröbner basis of this ideal
- since the remainder of f by G is zero, (indeed we have $f = f_1 + y f_2$)

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

- we can do this check by Gröbner bases over integers
- Let G be the Gröbner basis of this ideal
- since the remainder of f by G is zero, (indeed we have $f = f_1 + y f_2$)

Example (cont.)

- To check whether P can be covered by T (and its rotations and reflection), one can verify whether

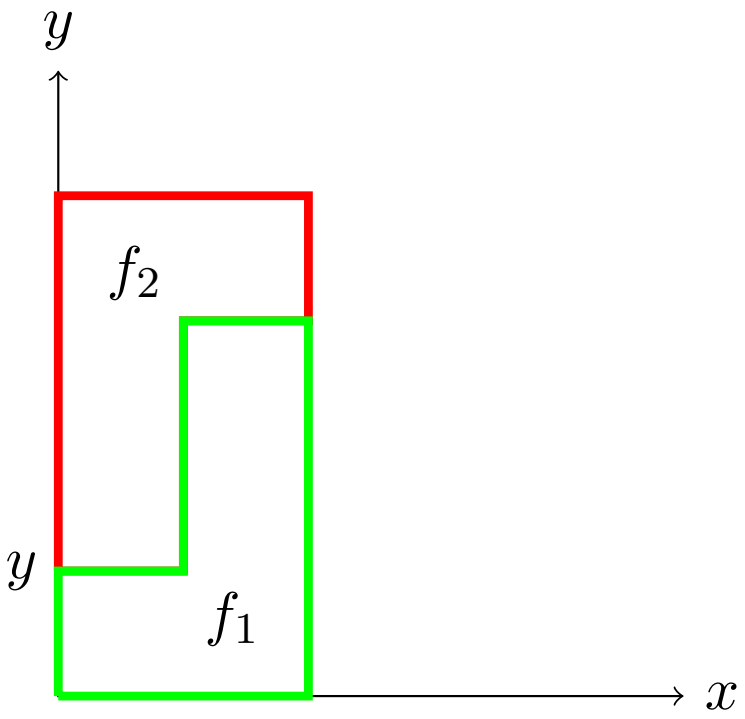
$$f \in \langle f_1, \ldots, f_4, g_1, \ldots, g_4 \rangle \subset \mathbb{Z}[x, y]$$

- we can do this check by Gröbner bases over integers
- Let G be the Gröbner basis of this ideal
- since the remainder of f by G is zero, (indeed we have $f = f_1 + y f_2$)

Thus, we can cover P by T.

Example (cont.)

Thus we have



☞ $f = f_1 + y f_2$

Thanks for your attention...

References

[1] David Cox, John Little and Donal O'Shea:
Ideals, varieties, and algorithms.
Undergraduate Texts in Mathematics, Springer-Verlag, 2006.
[2] David Cox, John Little and Donal O'Shea:
Using algebraic geometry.
Graduate Texts in Mathematics, Springer-Verlag, 2005.
[3] Thomas Becker and Volker Weispfenning:
Gröbner bases, A computational approach to commutative algebra.
Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.
[4] William W. Adams and Philippe Loustaunau:
An introduction to Gröbner bases.
American Mathematical Society, 1994.