Lecture 2-13-1 - Polynomial systems, computer algebra and applications

Jean-Charles Faugère

Solving Algebraic Systems with Symmetries

2022 - 2023 – MPRI

Symmetries

System invariant by the action of an Abelian group

Definition

Let I be an ideal. I is said to be *stable* under the action of G (G-*stable*) if: $\forall f \in I, \forall A \in G \quad f^A \in I$

Action of $GL_n(k)$ on polynomials.
G is a finite subgroup of $GL_n(k)$.
Let X be the column vector whose entries are $x_1, \ldots, x_n$.

For f a polynomial and $A \in G$, let f^A be the polynomial obtained by substituting the components of $A.X$ to $x_1, \ldots, x_n$.
Since $(f^A)^B = f^{AB}$, we obtain an action of G on the ring of polynomials

Remark

The action of G preserves the homogeneous components.

Main focus: G is an Abelian Group

System invariant by the action of an Abelian group

Consider the following system: 5 degree 3 equations in 5 variables: invariant by the action of $G = C_5$ (ground field is $\mathbb{F}_{65521}$):

$f_1 =$
$y_1^3 + y_2^3 + y_3^3 + y_4^3 + y_5^3 + 52524\, y_1\, y_5{}^2 + 52524\, y_1{}^2 y_2 + 52524\, y_2{}^2 y_3 + 52524\, y_3{}^2 y_4 + 52524\, y_4{}^2 y_5 +$
$19910\, y_2{}^2 y_4 + 19910\, y_1{}^2 y_3 + 37058\, y_1{}^2 y_4 + 30323\, y_1{}^2 y_5 + 30323\, y_1\, y_2{}^2 + 12774\, y_1\, y_2\, y_3 +$
$2708\, y_1\, y_2\, y_4 + 12774\, y_1\, y_2\, y_5 + 37058\, y_1\, y_3{}^2 + 2708\, y_1\, y_3\, y_4 + 2708\, y_1\, y_3\, y_5 + 19910\, y_1\, y_4{}^2 +$
$12774\, y_1\, y_4\, y_5 + y_2{}^3 + 37058\, y_2{}^2 y_5 + 30323\, y_2\, y_3{}^2 + 12774\, y_2\, y_3\, y_4 + 2708\, y_2\, y_3\, y_5 + 37058\, y_2\, y_4{}^2 +$
$2708\, y_2\, y_4\, y_5 + 19910\, y_2\, y_5{}^2 + y_3{}^3 + 19910\, y_3{}^2 y_5 + 30323\, y_3\, y_4{}^2 + 12774\, y_3\, y_4\, y_5 + 37058\, y_3\, y_5{}^2 +$
$y_4{}^3 + 30323\, y_4\, y_5{}^2 + y_5{}^3 + 19604\, y_1{}^2 + 42627\, y_1\, y_2 + 4321\, y_1\, y_3 + 4321\, y_1\, y_4 + 42627\, y_1\, y_5 +$
$19604\, y_2{}^2 + 42627\, y_2\, y_3 + 4321\, y_2\, y_4 + 4321\, y_2\, y_5 + 19604\, y_3{}^2 + 42627\, y_3\, y_4 + 4321\, y_3\, y_5 +$
$19604\, y_4{}^2 + 42627\, y_4\, y_5 + 19604\, y_5{}^2 + 1032\, y_1 + 1032\, y_2 + 1032\, y_3 + 1032\, y_4 + 1032\, y_5 + 9254$

$f_2, f_3, f_4, f_5 =$ same shape $\cdots$

System invariant by the action of an Abelian group

Consider the following system: 5 degree 3 equations in 5 variables: invariant by the action of $G = C_5$ (ground field is $\mathbb{F}_{65521}$):

$f_1 =$
$y_1^3 + y_2^3 + y_3^3 + y_4^3 + y_5^3 + 52524\, y_1\, y_5^2 + 52524\, y_1^2 y_2 + 52524\, y_2^2 y_3 + 52524\, y_3^2 y_4 + 52524\, y_4^2 y_5 + 19910\, y_2^2 y_4 + 19910\, y_1^2 y_3 + 37058\, y_1^2 y_4 + 30323\, y_1^2 y_5 + 30323\, y_1\, y_2^2 + 12774\, y_1\, y_2\, y_3 + 2708\, y_1\, y_2\, y_4 + 12774\, y_1\, y_2\, y_5 + 37058\, y_1\, y_3^2 + 2708\, y_1\, y_3\, y_4 + 2708\, y_1\, y_3\, y_5 + 19910\, y_1\, y_4^2 + 12774\, y_1\, y_4\, y_5 + y_2^3 + 37058\, y_2^2 y_5 + 30323\, y_2\, y_3^2 + 12774\, y_2\, y_3\, y_4 + 2708\, y_2\, y_3\, y_5 + 37058\, y_2\, y_4^2 + 2708\, y_2\, y_4\, y_5 + 19910\, y_2\, y_5^2 + y_3^3 + 19910\, y_3^2 y_5 + 30323\, y_3\, y_4^2 + 12774\, y_3\, y_4\, y_5 + 37058\, y_3\, y_5^2 + y_4^3 + 30323\, y_4\, y_5^2 + y_5^3 + 19604\, y_1^2 + 42627\, y_1\, y_2 + 4321\, y_1\, y_3 + 4321\, y_1\, y_4 + 42627\, y_1\, y_5 + 19604\, y_2^2 + 42627\, y_2\, y_3 + 4321\, y_2\, y_4 + 4321\, y_2\, y_5 + 19604\, y_3^2 + 42627\, y_3\, y_4 + 4321\, y_3\, y_5 + 19604\, y_4^2 + 42627\, y_4\, y_5 + 19604\, y_5^2 + 1032\, y_1 + 1032\, y_2 + 1032\, y_3 + 1032\, y_4 + 1032\, y_5 + 9254$

$f_2, f_3, f_4, f_5 =$ same shape $\cdots$

Not **Generic** at all!
The system has 125 solutions.
How to use the symmetry ?

Abelian Group G

Theorem

Any finite commutative group G is uniquely isomorphic to a product $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|\ldots|q_\ell$.

Definition

Following the notations of the previous theorem, the integer $e = q_\ell$ is called the exponent of the group and is the lowest common multiple of the orders of the elements of the group.

When $\ell = 1$ and $n = q_1$ so that G is the n cyclic group.

Abelian Group G

Theorem

Any finite commutative group G is uniquely isomorphic to a product $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1 | \dots | q_\ell$.

Definition

Following the notations of the previous theorem, the integer $e = q_\ell$ is called the exponent of the group and is the lowest common multiple of the orders of the elements of the group.

When $\ell = 1$ and $n = q_1$ so that G is the n cyclic group.

Theorem

Let G be a cyclic group of order n. Let ω be a primitive e-th root of 1. The subgroup G is diagonalizable, meaning that there exists a matrix P in $GL_n(K)$, such that the group $P^{-1} G P = \{P^{-1} A P \mid A \in G\}$ is a diagonal group.

Example: cyclic Group G

Let C_n be the subgroup of $\mathfrak{S}_n$ generated by the n-cycle $\sigma = (1\ 2\ \ldots\ n)$. C_n is a cyclic group of order n, embedded in $GL_n(k)$ and generated by:

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

The cyclic group C_n is diagonalizable:
Then if we denote $K = k(\omega)$ where ω is a primitive n-root of 1, with the base-change matrix $P = (\omega^{ij})_{i,j \in \{1,\ldots,n\}}$.
The matrix associated to the cycle $(1 \ldots n)$ becomes the diagonal matrix $D_\sigma = \mathrm{diag}(\omega, \ldots, \omega^{n-1}, 1)$.

Grading induced by a diagonal matrix group

$G = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1 | \ldots | q_\ell$.

Proposition

For every monomial m and for each i, there exists a unique $\mu_i \in \{0, \ldots, q_i - 1\}$ such that $m^{D_i} = \omega^{\frac{e}{q_i}\mu_i} m$.

☞ We take μ_i in $\mathbb{Z}/q_i\mathbb{Z}$

Grading induced by a diagonal matrix group

$G = \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1 | \ldots | q_\ell$.

Proposition

For every monomial m and for each i, there exists a unique $\mu_i \in \{0, \ldots, q_i - 1\}$ such that $m^{D_i} = \omega^{\frac{e}{q_i}\mu_i} m$.

☞ We take μ_i in $\mathbb{Z}/q_i\mathbb{Z}$

Definition

The k-tuple $(\mu_1, \ldots, \mu_k) \in \prod \mathbb{Z}/q_i\mathbb{Z}$ is said to be the G-degree of m and is denoted $G\!-\!degree(m)$.

Cyclic Group G

C_3 is the matrix group generated by the diagonal matrix $D_\sigma = \mathrm{Diag}(\omega, \omega^2, 1)$ where ω is a primitive third root of 1.
Each x_i has G-degree i mod 3, so

$$G\text{-degree}\left(\prod x_j^{\alpha_j}\right) = \sum j\,\alpha_j \bmod 3$$

Hence, $x_1x_2x_3$ (resp. $x_1x_2^2$) has G-degree 0 (resp. 2).

The repartition into same G-degree is as follows :

G-degree	0	1	2
monomials	$1, x_3, x_3^2, x_1x_2$ $x_3^3, x_1x_2x_3, x_2^3, x_1^3$	x_1, x_1x_3, x_2^2 $x_1x_3^2, x_2^2x_3, x_1^2x_2$	x_2, x_2x_3, x_1^2 $x_2x_3^2, x_1^2x_3, x_1x_2^2$

Solving systems invariant by the action of an Abelian group

We diagonalize the group:

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ compute } Q \text{ s.t. } Q\,G\,Q^{-1} = \begin{bmatrix} w^2 & 0 & 0 & 0 & 0 \\ 0 & w^4 & 0 & 0 & 0 \\ 0 & 0 & w & 0 & 0 \\ 0 & 0 & 0 & w^3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $w^5 = 1$. ☞ New variables $Q \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$

Solving systems invariant by the action of an Abelian group

We diagonalize the group:

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ compute } Q \text{ s.t. } Q\,G\,Q^{-1} = \begin{bmatrix} w^2 & 0 & 0 & 0 & 0 \\ 0 & w^4 & 0 & 0 & 0 \\ 0 & 0 & w & 0 & 0 \\ 0 & 0 & 0 & w^3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $w^5 = 1$. ☞ New variables $Q \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$

$g_1 = 41\,x_0^3 + 9\,x_0\,x_1\,x_4 + 7\,x_0\,x_2\,x_3 - 17\,x_1^2x_3 + 28\,x_1\,x_2^2 + 15\,x_2\,x_4^2 + 44\,x_3^2x_4 - 21\,x_0^2 - 42\,x_1\,x_4 - 27\,x_2\,x_3 + 22\,x_0 - 4120$

$g_2, g_3, g_4, g_5 =$ same shape $\cdots$

- The new system is sparse: length$(g_1) = 12 \ll 56 =$ length(f_1)
- Support of the polys: monomials $x_i x_j x_k$ s.t. $i + j + k = 0 \mod n$
  $\longrightarrow$ New grading: G-degree$(x_{i_1} \cdots x_{i_k}) = i_1 + \cdots + i_k \mod n$
  $g(w^0 x_0, w^1 x_1, \ldots, w^{n-1} x_{n-1}) = w^{G-degree(g)} g(x_0, x_1, \ldots, x_{n-1})$
  $\longrightarrow$ Here all the polynomials of G-degree 0

G-homogeneity

For algorithms: the S-polynomial of two G-homogeneous polynomials is also G-homogeneous

Definition

A polynomial f is said to be G-homogeneous if all monomials of f share the same G-degree $(\mu_1, \ldots, \mu_k)$. In this case, we set G-degree$(f) = G$-degree$(\mathrm{LM}(f)) = (\mu_1, \ldots, \mu_k)$.

G-*homogeneity*

For algorithms: the S-polynomial of two G-homogeneous polynomials is also G-homogeneous

Definition

A polynomial f is said to be G-homogeneous if all monomials of f share the same G-degree $(\mu_1, \ldots, \mu_k)$. In this case, we set $G\text{-degree}(f) = G\text{-degree}(\mathrm{LM}(f)) = (\mu_1, \ldots, \mu_k)$.

Proposition

If f is G-homogeneous and m is a monomial, then $m\,f$ is also G-homogeneous. Moreover, $G\text{-degree}(m\,f) = G\text{-degree}(m) + G\text{-degree}(f)$.

G-homogeneity

The cornerstone of the new Abelian-F5 algorithm is that the S-polynomial of two G-homogeneous polynomials is G-homogeneous:

Theorem

Let f, g be two G-homogeneous polynomials. The S-polynomial of f and g is also G-homogeneous of G-degree: G-degree$(LM(f) \vee LM(g))$. Where $LM(f) \vee LM(g) =$ lowest common multiple of $LM(f)$ and $LM(g)$.

Test in a CAS

We consider the cyclic group C_n:

Home Work

- write the matrix M_G of G
- Compute P such that

$$P^{-1}\ M_G\ P = D \text{ a diagonal matrix}$$

- write a function to change the variables
- Apply the change of variables to some interesting polynomial, for instance:

$$x_1 + x_2 + \cdots + x_n$$

Test 1

We will use the well known *Cyclic-n problem*. The ideal I generated by:

$$(I)\begin{cases} f_1 = x_1 + \cdots + x_n \\ f_2 = x_1x_2 + x_2x_3 + \cdots + x_nx_1 \\ \vdots \\ f_{n-1} = x_1x_2\ldots x_{n-1} + x_2\ldots x_nx_1 + \cdots + x_nx_1\ldots x_{n-2} \\ f_n = x_1x_2\ldots x_{n-1}x_n - 1 \end{cases}$$

The ideal I is invariant under the cyclic group C_n, since each h_i satisfies $h_i^{M_\sigma} = h_i$

Home Work

- write the equations
- change the variables
- compute the G-degree of each equations
- Are the polynomials G-homogeneous ?

Test 2:Random Systems

We consider a system of $f_1, \ldots, f_n$ equations in $\mathbb{F}_p[x_1, \ldots, , x_n]$ which are invariant by the action of cyclic group C_n

Home Work

- Generate the equations using the operator:

$$R(f) = \frac{1}{|G|} \sum_{\sigma \in G}^{\sigma} f$$

- change the variables
- compute the G-degree of each equations

Test 3: NTRU (basic problem of several PQC cryptosystem)

p is a prime number
$f_1 = \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in \{0, 1\}$
$f_2 = \sum_{i=0}^{n-1} b_i x^i$ with $b_i \in \{0, 1\}$

Then $Pub = f_1 \times (f_2)^{-1} \mod (x^n - 1) \mod p$

Goal: find a polynomial $f = \sum_{i=0}^{n-1} x_i x^i$ with $x_i \in \{0, 1\}$ such that:

all the coefficients of $Pub \times f \mod (x^n - 1) \mod p$ are in $\{0, 1\}$

Home Work

- write the original algebraic equations
- change the variables
- compute the G-degree of each equations
- Are the polynomials G-homogeneous ?

Fundamental Theorem

G is a diagonal group, and I is a G-stable ideal generated by $f_1, \ldots, f_m$. A Grbner basis computation preserves the G-degree, but the polynomials f_i are not necessarily G-homogeneous. Our aim here is to prove that the G-homogeneous components of the f_i are in I, and so to compute a Grbner basis of I, we take the G-homogeneous components of generators of I as inputs.

Fundamental Theorem

G is a diagonal group, and I is a G-stable ideal generated by $f_1, \ldots, f_m$. A Grbner basis computation preserves the G-degree, but the polynomials f_i are not necessarily G-homogeneous. Our aim here is to prove that the G-homogeneous components of the f_i are in I, and so to compute a Grbner basis of I, we take the G-homogeneous components of generators of I as inputs.

Definition

Let I be an ideal. I is said to be *stable* under the action of G (G-*stable*) if: $\forall f \in I, \forall A \in G \quad f^A \in I$

Fundamental Theorem

G is a diagonal group, and I is a G-stable ideal generated by $f_1, \ldots, f_m$. A Grbner basis computation preserves the G-degree, but the polynomials f_i are not necessarily G-homogeneous. Our aim here is to prove that the G-homogeneous components of the f_i are in I, and so to compute a Grbner basis of I, we take the G-homogeneous components of generators of I as inputs.

Definition

Let I be an ideal. I is said to be *stable* under the action of G (G*-stable*) if: $\forall f \in I, \forall A \in G \quad f^A \in I$

Definition

An ideal J is said to be G-homogeneous if for any polynomial $f \in J$, its G-homogeneous components are also in J.

Fundamental Theorem

G is a diagonal group, and I is a G-stable ideal generated by $f_1, \ldots, f_m$. A Grbner basis computation preserves the G-degree, but the polynomials f_i are not necessarily G-homogeneous. Our aim here is to prove that the G-homogeneous components of the f_i are in I, and so to compute a Grbner basis of I, we take the G-homogeneous components of generators of I as inputs.

Theorem

An ideal is G-homogeneous if and only if it is G-stable.

Remark

True also when $G = \{1\}$

Test 1,2,3

If $G = C_n$ then

$$f = \sum_{i=0}^{n-1} f^{(i)} \qquad \text{where} \quad G - \text{degree}(f^{(i)}) = i$$

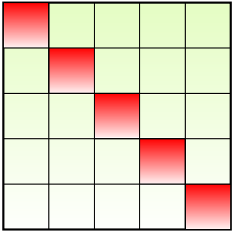
Home Work

- split the equations into G-homogeneous components:

Speedup the computation

Abelian Group $\approx$ Multi-homogeneous :

Use the new Grading to split the matrices



Instead of **one** matrix in degree d

$$\mathcal{M}_d$$

we can split $\mathcal{M}_d$ wrt G-degree $0, 1, 2, 3, 4$.

Theorem ([F., Svartz 2013])

$\mathbf{I} = (f_1, \ldots, f_m)$ a 0-dimensional ideal, invariant under an Abelian Group G. Divides the GB complexity by: $|G|^3$

☞ *Provide dedicated F_5 and FGLM algorithms.*

Abelian F5

Abelian-F_5 (homogeneous-case)

Input: The set $\hat{G}$ of $G_{\mathscr{D}}$-degrees, homogeneous and $G_{\mathscr{D}}$-homogeneous polynomials $(f_1,\ldots,f_m)$ with degrees $d_1 \leq \ldots \leq d_m$ and a maximal degree D.
Output: the elements of degree at most D of a Gröbner basis of $(f_1,\ldots,f_i)$ for $i = 1,\ldots,m$.

---

for i **from** 1 **to** m **do** $\mathscr{G}_i := \emptyset$ **end for**
for d **from** d_1 **to** D **do**
  for g **in** $\hat{G}$ **do**
    $M_{d,0,g} := \emptyset$, $\tilde{M}_{d,0,g} := \emptyset$
      for i **from** 1 **to** m **do**
        case
          $d < d_i)$ $M_{d,i,g} := \tilde{M}_{d,i-1,g}$
          $d = d_i)$ **if** $g = \deg_{G_{\mathscr{D}}}(f_i)$ **then**
              $M_{d,i,g} :=$ add new row f_i to $\tilde{M}_{d,i-1,g}$ with index $(i,1)$
                else
              $M_{d,i,g} := \tilde{M}_{d,i-1,g}$
            end if
          $d > d_i)$ $M_{d,i,g} :=$add new row $m.f_i$ for all monomials m of degree $d - d_i$ with $\deg_{G_{\mathscr{D}}}(m) = g - \deg_{G_{\mathscr{D}}}(f_i)$ that do not appear as leading monomials in the matrix $\tilde{M}_{d-d_i,i-1,u-\deg_{G_{\mathscr{D}}}(f_i)}$ to $\tilde{M}_{d,i-1,g}$ with index (i,m).
        end case
        Compute $\tilde{M}_{d,i,g}$ by Gaussian elimination from $M_{d,i,g}$.
        Add to $\mathscr{G}_i$ all rows of $\tilde{M}_{d,i,g}$ not reducible by $\mathrm{LM}(\mathscr{G}_i)$.
      end for
  end for
end for
return $\mathscr{G}_1,\ldots,\mathscr{G}_m$

Faster?

Consider the following system: 5 degree 3 equations in 5 variables: invariant by the action of $G = C_5$ (ground field is $\mathbb{F}_{65521}$):

$f_1 =$
$y_1^3+y_2^3+y_3^3+y_4^3+y_5^3+52524\,y_1\,y_5{}^2+52524\,y_1{}^2y_2+52524\,y_2{}^2y_3+52524\,y_3{}^2y_4+52524\,y_4{}^2y_5+$
$19910\,y_2{}^2y_4+19910\,y_1{}^2y_3+37058\,y_1{}^2y_4+30323\,y_1{}^2y_5+30323\,y_1\,y_2{}^2+12774\,y_1\,y_2\,y_3+$
$2708\,y_1\,y_2\,y_4+12774\,y_1\,y_2\,y_5+37058\,y_1\,y_3{}^2+2708\,y_1\,y_3\,y_4+2708\,y_1\,y_3\,y_5+19910\,y_1\,y_4{}^2+$
$12774\,y_1\,y_4\,y_5+y_2{}^3+37058\,y_2{}^2y_5+30323\,y_2\,y_3{}^2+12774\,y_2\,y_3\,y_4+2708\,y_2\,y_3\,y_5+37058\,y_2\,y_4{}^2+$
$2708\,y_2\,y_4\,y_5+19910\,y_2\,y_5{}^2+y_3{}^3+19910\,y_3{}^2y_5+30323\,y_3\,y_4{}^2+12774\,y_3\,y_4\,y_5+37058\,y_3\,y_5{}^2+$
$y_4{}^3+30323\,y_4\,y_5{}^2+y_5{}^3+19604\,y_1{}^2+42627\,y_1\,y_2+4321\,y_1\,y_3+4321\,y_1\,y_4+42627\,y_1\,y_5+$
$19604\,y_2{}^2+42627\,y_2\,y_3+4321\,y_2\,y_4+4321\,y_2\,y_5+19604\,y_3{}^2+42627\,y_3\,y_4+4321\,y_3\,y_5+$
$19604\,y_4{}^2+42627\,y_4\,y_5+19604\,y_5{}^2+1032\,y_1+1032\,y_2+1032\,y_3+1032\,y_4+1032\,y_5+9254$

$f_2, f_3, f_4, f_5 =$ same shape $\cdots$

The system has 125 solutions.

Solving Systems with Symmetries

Recall that we want to solve the following system: 5 degree 3 equations in 5 variables which are invariant by the action C_5

$f_1 =$
$y_1^3+y_2^3+y_3^3+y_4^3+y_5^3+52524\,y_1\,y_5^2+52524\,y_1^2y_2+52524\,y_2^2y_3+52524\,y_3^2y_4+52524\,y_4^2y_5+19910\,y_2^2y_4+19910\,y_1^2y_3+37058\,y_1^2y_4+30323\,y_1^2y_5+30323\,y_1\,y_2^2+12774\,y_1\,y_2\,y_3+2708\,y_1\,y_2\,y_4+12774\,y_1\,y_2\,y_5+37058\,y_1\,y_3^2+2708\,y_1\,y_3\,y_4+2708\,y_1\,y_3\,y_5+19910\,y_1\,y_4^2+12774\,y_1\,y_4\,y_5+y_2^3+37058\,y_2^2y_5+30323\,y_2\,y_3^2+12774\,y_2\,y_3\,y_4+2708\,y_2\,y_3\,y_5+37058\,y_2\,y_4^2+2708\,y_2\,y_4\,y_5+19910\,y_2\,y_5^2+y_3^3+19910\,y_3^2y_5+30323\,y_3\,y_4^2+12774\,y_3\,y_4\,y_5+37058\,y_3\,y_5^2+y_4^3+30323\,y_4\,y_5^2+y_5^3+19604\,y_1^2+42627\,y_1\,y_2+4321\,y_1\,y_3+4321\,y_1\,y_4+42627\,y_1\,y_5+19604\,y_2^2+42627\,y_2\,y_3+4321\,y_2\,y_4+4321\,y_2\,y_5+19604\,y_3^2+42627\,y_3\,y_4+4321\,y_3\,y_5+19604\,y_4^2+42627\,y_4\,y_5+19604\,y_5^2+1032\,y_1+1032\,y_2+1032\,y_3+1032\,y_4+1032\,y_5+9254$

$f_2, f_3, f_4, f_5 =$ same shape $\cdots$

Diagonalize the group !
Change of variables

$g_1 = 41\,x_0^3+9\,x_0\,x_1\,x_4+7\,x_0\,x_2\,x_3-17\,x_1^2x_3+28\,x_1\,x_2^2+15\,x_2\,x_4^2+44\,x_3^2x_4-21\,x_0^2-42\,x_1\,x_4-27\,x_2\,x_3+22\,x_0-4120$

$g_2, g_3, g_4, g_5 =$ same shape $\cdots$

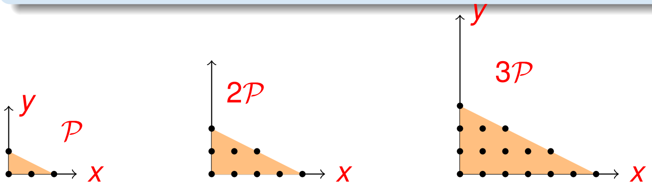
☞ Use the sparsity !

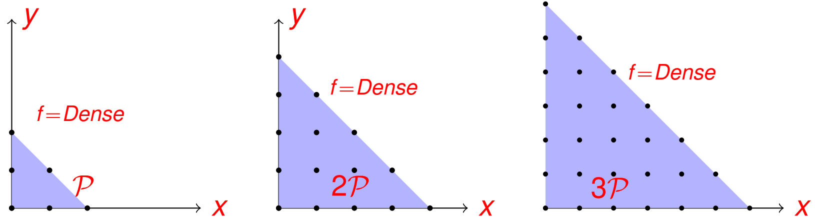
New Unified Approach : Sparse Gröbner basis

with PJ Spaenlehauer and J Svartz - 2014

Unified approach based on monomial sparsity

- Consider only monomials in the initial Support: polytope $\mathcal{P}$
- Multiply these monomials $\rightsquigarrow 2\mathcal{P} = \{u \times v \mid (u, v) \in \mathcal{P}^2\}$



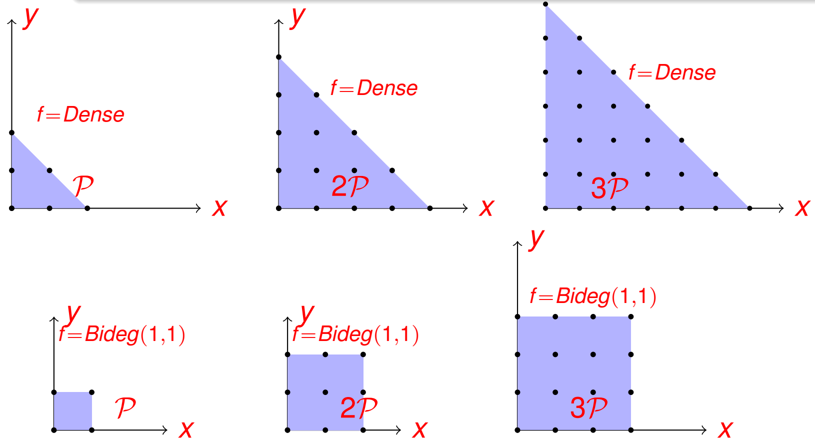


New Unified Approach : Sparse Gröbner basis

with PJ Spaenlehauer and J Svartz - 2014

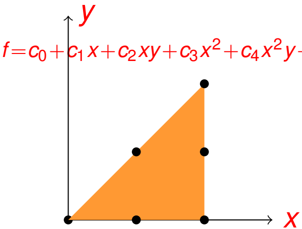
Unified approach based on monomial sparsity

- Consider only monomials in the initial Support: polytope $\mathcal{P}$
- Multiply these monomials $\rightsquigarrow 2\mathcal{P} = \{u \times v \mid (u, v) \in \mathcal{P}^2\}$

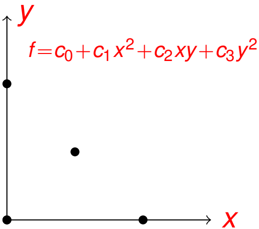


New Approach ! Sparse Polynomials

with PJ Spaenlehauer and J Svartz

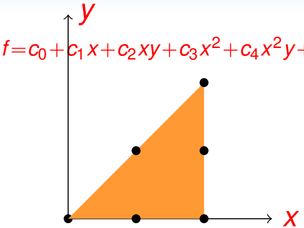


or

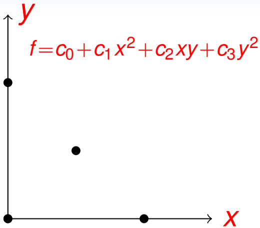


We want to keep the initial structure!

New Approach ! Sparse Polynomials



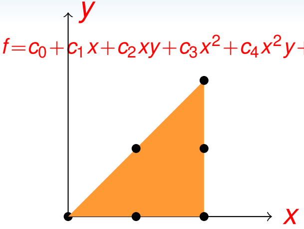
or



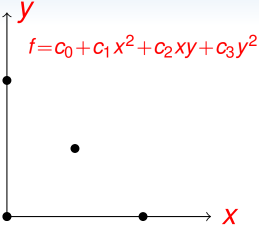
We want to keep the initial structure!

- Monomials of degree 1:
  $\mathcal{M}_1 = \text{Support}(f)$
- Monomials of degree 2:
  $\mathcal{M}_2 = \{u \times v \mid (u, v) \in \mathcal{M}_1 \times \mathcal{M}_1\}$
- ...
- Monomials of degree d:
  $\mathcal{M}_d = \{u \times v \mid (u, v) \in \mathcal{M}_{d-1} \times \mathcal{M}_1\}$

New Approach ! Sparse Polynomials



or



We want to keep the initial structure!

- Monomials of degree 1:
  $\mathcal{M}_1 = \text{Support}(f)$
- Monomials of degree 2:
  $\mathcal{M}_2 = \{u \times v \mid (u, v) \in \mathcal{M}_1 \times \mathcal{M}_1\}$
- ...
- Monomials of degree d:
  $\mathcal{M}_d = \{u \times v \mid (u, v) \in \mathcal{M}_{d-1} \times \mathcal{M}_1\}$

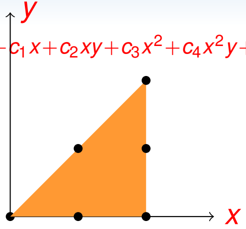
Macaulay Matrix in degree d

$$\begin{array}{cc} & m_1 > m_2 > \cdots > m_k \\ M_d = \begin{array}{c} t_{1,1} f_1 \\ t_{1,2} f_1 \\ \vdots \\ t_{2,1} f_2 \\ \vdots \end{array} & \left(\begin{array}{c} \cdots \\ \cdots \\ \operatorname{coeff}(t\, f_i, m_j) \\ \cdots \\ \vdots \end{array} \right) \end{array}$$

all products $t\, f_i$, $t \in \mathcal{M}_{d-\deg(f_i)}$

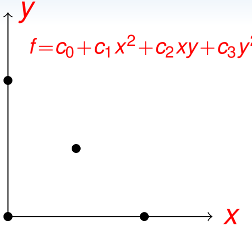
New Approach ! Sparse Polynomials

$f = c_0 + c_1 x + c_2 xy + c_3 x^2 + c_4 x^2 y + c_5 x^2 y^2$



or

$f = c_0 + c_1 x^2 + c_2 xy + c_3 y^2$



We want to keep the initial structure!

- dedicated matrix-F_5 algorithm

Goal

Under algebraic assumptions: m eqs with the same support

- complexity ?
- Hibert Series?

Macaulay Matrix in degree d

$$M_d = \begin{array}{c} \\ t_{1,1} f_1 \\ t_{1,2} f_1 \\ \vdots \\ t_{2,1} f_2 \\ \vdots \end{array} \begin{array}{c} m_1 > m_2 > \cdots > m_k \\ \left(\begin{array}{c} \cdots \\ \cdots \\ \mathrm{coeff}\,(t\, f_i, m_j) \\ \cdots \\ \vdots \end{array} \right) \end{array}$$

all products $t\, f_i$, $t \in \mathcal{M}_{d-\deg(f_i)}$

Solving with symmetries using sparsity

Initial support $\mathcal{P} = \{h_1, \ldots, h_{12}\} =$ Support$(g_i) = \{x_i x_j x_k$ s.t. $i + j + k = 0 \mod 5\} \longrightarrow \#\mathcal{P} = 12$

We have to estimate $d_{\max}$?

- Monomials of degree 1: $\#\mathcal{P} = 12$
- Monomials of degree 2:
  $2\mathcal{P} = \{u \times v \mid (u, v) \in \mathcal{P} \times \mathcal{P}\} \longrightarrow \#2\mathcal{P} = 68$
- ...
- Monomials of degree d: $d\mathcal{P} = \{u \times v \mid (u, v) \in (d-1)\mathcal{P} \times \mathcal{P}\}$

Compute the Hilbert series of the monomial ring:

$$H_R(z) = 1 + \sum_{d>0} \#(d\mathcal{P})\, z^d = \frac{z^4 + 6\,z^3 + 11\,z^2 + 6\,z + 1}{(1-z)^6}$$

Compute the Hilbert series of the monomial ring:

$$H_R(z) = 1 + \sum_{d>0} \#\mathcal{M}_d\, z^d = \frac{z^4+6\,z^3+11\,z^2+6\,z+1}{(1-z)^6}$$
$$= 1 + 12\,z + 68\,z^2 + 254\,z^3 + 730\,z^4 + 1756\,z^5 + \cdots$$

Since we have 5 equations of "degree" 1, the Hilbert series is

$$H(z) = H_R(z)(1-z)^5$$
$$= 1 + 7\,z + 18\,z^2 + 24\,z^3 + 25\,z^4 + 25\,z^5 + 25\,z^6 + \cdots$$

Hence we have only $25 = \frac{125}{|G|}$ solutions
and the maximal degree $d_{\mathrm{max}} = 4$.

☞ We can run the sparse matrix F_5 and compute the minimal polynomial of M_t (where $t = x_0^2$) of degree 25:
$t^{25} + 62732\,t^{24} + 26240\,t^{23} + 63778\,t^{22} + 38558\,t^{21} + 9283\,{h_8}^{20} + 29068\,t^{19} + 49606\,t^{18} + 34528\,t^{17} + 22383\,t^{16} + 11568\,{h_8}^{15} + 8861\,t^{14} + 38583\,t^{13} + 60089\,t^{12} + 23443\,t^{11} + 62330\,{h_8}^{10} + 38047\,t^{9} + 41549\,t^{8} + 42497\,t^{7} + 32676\,t^{6} + 13919\,t^{5} + 22256\,t^{4} + 25537\,t^{3} + 61988\,t^{2} + 108\,t + 60264$ then recover the values of $m \in \mathcal{P}$, and the values of $x_0, x_1, \ldots, x_4$.

Références I

B. Buchberger.
An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal.
Journal of Symbolic Computation, 41(3-4):475–511, 3 2006.

Buchberger B.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Innsbruck, 1965.

Buchberger B.
An Algorithmical Criterion for the Solvability of Algebraic Systems.
Aequationes Mathematicae, 4(3):374–383, 1970.
(German).

Cox D., Little J., and O'Shea D.
Ideals, Varieties and Algorithms.
Springer Verlag, New York, 1992.