Gröbner bases of ideals invariant under an abelian group

Jean-Charles Faugère, Jules Svartz

INRIA/LIP6/UPMC – Polsys Team

Lundi 13 mai 2013

Polynomials systems with symmetry

Action of Finite Groups on Polynomials

$GL_n(k)$ acts on $k[x_1, \ldots, x_n]$: $f^A(x) = f(A.x)$

Example

$$\sigma = (123) \hookrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\sigma \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}$$

$$(x_1^2 x_2 + x_3)^\sigma = x_2^2 x_3 + x_1$$

Problem

I ideal of $k[x_1, \ldots, x_n]$ stable under $G \subset GL_n(k)$. How can we compute $\mathbb{V}(I)$ while taking advantage of the action of G ?

Previous results on problems with symmetry

Group	**Invariant equations** $f_i^A = f_i$ for all $A \in G$.	**Invariant ideal** $f \in I, A \in G \Rightarrow f^A \in I$
$\mathfrak{S}_n$	$e_1, \ldots, e_n$	Divided differences[1] $\rightsquigarrow$ invariant equations
Reflexive Group	Invariant Theory : $\theta_1, \ldots, \theta_n$	
$G \subset \mathfrak{S}_n$	(Invariant Theory) / SAGBI-Gröbner[2]	
Abelian Group	(Invariant Theory)	Diagonalization and usual algorithms[3]
General Group	(Invariant Theory[4])	

All of these approaches : *non-modular case*.

[1] [Faugère, Hering & Phan03, Faugère&S.12]
[2] [Faugère & Rahmany09]
[3] [Stanley79, Gatermann90, Steidel13]
[4] [Colin97]

Contributions

G abelian, $char(k)$ does not divide $|G|$.

- Reduce to an ideal stable under a diagonal matrix group $G_{\mathcal{D}}$.
- Grading given by $G_{\mathcal{D}}$.
- Use the grading to split Macaulay/F_4/F_5 matrices and multiplication matrices in FGLM.
- Gain of $|G|^{\omega}$ in F_4/F_5 and $|G|^2$ in FGLM.
- Some problems solvable in polynomial time.
- Implementation that shows the success of the approach :
  - Speed-up $>$ 400 on Cyclic-10.
  - Cyclic-11 $\leq$ 8 hours.
  - Achieve previously intractable problems.

Example : Problem invariant under $C_2 \times C_4$

$$M_1 = \left(\begin{array}{cc|cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \text{ and } M_2 = \left(\begin{array}{cc|cccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right)$$

Example : Problem invariant under $C_2 \times C_4$

$$M_1 = \left(\begin{array}{cc|cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \text{ and } M_2 = \left(\begin{array}{cc|cccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right)$$

$G = \langle M_1, M_2 \rangle$ acts on $R = \mathbb{F}_{17}[x_1, x_2, x_3, x_4, x_5, x_6]$. M_1 exchanges x_1 and x_2 and M_2 performs a cycle on (x_3, x_4, x_5, x_6).

f_1 =Random polynomial of degree 2 invariant under M_2
f_2 =Random polynomial of degree 3 invariant under M_1.

If you insist...

$$f_1 = x_1^2 + 11x_1x_2 + 5x_2^2 + 4x_1x_3 + 11x_2x_3 + 4x_3^2 + 4x_1x_4 + 11x_2x_4 + x_3x_4 + 4x_4^2 + 4x_1x_5 + 11x_2x_5 + 6x_3x_5 + x_4x_5 + 4x_5^2 + 4x_1x_6 + 11x_2x_6 + x_3x_6 + 6x_4x_6 + x_5x_6 + 4x_6^2 + 14x_1 + 10x_2 + 15x_3 + 15x_4 + 15x_5 + 15x_6 + 14$$

$$f_2 = x_1^3 + 11x_1^2x_2 + 11x_1x_2^2 + x_2^3 + 7x_1^2x_3 + 14x_1x_2x_3 + 7x_2^2x_3 + 5x_1x_3^2 + 5x_2x_3^2 + 16x_3^3 + 16x_1x_2x_4 + 13x_1x_3x_4 + 13x_2x_3x_4 + 6x_3^2x_4 + 7x_1x_4^2 + 7x_2x_4^2 + 12x_3x_4^2 + 13x_4^3 + 13x_1^2x_5 + 6x_1x_2x_5 + 13x_2^2x_5 + 15x_1x_3x_5 + 15x_2x_3x_5 + x_3^2x_5 + 9x_1x_4x_5 + 9x_2x_4x_5 + 2x_4^2x_5 + 2x_1x_5^2 + 2x_2x_5^2 + 13x_3x_5^2 + 9x_4x_5^2 + 3x_1^2x_6 + x_1x_2x_6 + 3x_2^2x_6 + 9x_1x_3x_6 + 9x_2x_3x_6 + 4x_3^2x_6 + 5x_1x_4x_6 + 5x_2x_4x_6 + 7x_3x_4x_6 + 7x_4^2x_6 + 5x_1x_5x_6 + 5x_2x_5x_6 + x_3x_5x_6 + 16x_4x_5x_6 + 15x_5^2x_6 + 15x_1x_6^2 + 15x_2x_6^2 + 14x_3x_6^2 + 11x_4x_6^2 + 9x_5x_6^2 + 2x_6^3 + 13x_1x_2 + 6x_1x_3 + 6x_2x_3 + 4x_3^2 + 4x_1x_4 + 4x_2x_4 + 9x_3x_4 + 8x_4^2 + 13x_1x_5 + 13x_2x_5 + 12x_3x_5 + 6x_5^2 + 9x_1x_6 + 9x_2x_6 + 15x_4x_6 + 5x_5x_6 + 8x_6^2 + 8x_1 + 8x_2 + x_3 + 3x_4 + 10x_5 + 16x_6 + 3$$

If you insist...

$$f_1 = x_1^2 + 11x_1x_2 + 5x_2^2 + 4x_1x_3 + 11x_2x_3 + 4x_3^2 + 4x_1x_4 + 11x_2x_4 + x_3x_4 + 4x_4^2 + 4x_1x_5 + 11x_2x_5 + 6x_3x_5 + x_4x_5 + 4x_5^2 + 4x_1x_6 + 11x_2x_6 + x_3x_6 + 6x_4x_6 + x_5x_6 + 4x_6^2 + 14x_1 + 10x_2 + 15x_3 + 15x_4 + 15x_5 + 15x_6 + 14$$

$$f_2 = x_1^3 + 11x_1^2x_2 + 11x_1x_2^2 + x_2^3 + 7x_1^2x_3 + 14x_1x_2x_3 + 7x_2^2x_3 + 5x_1x_3^2 + 5x_2x_3^2 + 16x_3^3 + 16x_1x_2x_4 + 13x_1x_3x_4 + 13x_2x_3x_4 + 6x_3^2x_4 + 7x_1x_4^2 + 7x_2x_4^2 + 12x_3x_4^2 + 13x_4^3 + 13x_1^2x_5 + 6x_1x_2x_5 + 13x_2^2x_5 + 15x_1x_3x_5 + 15x_2x_3x_5 + x_3^2x_5 + 9x_1x_4x_5 + 9x_2x_4x_5 + 2x_4^2x_5 + 2x_1x_5^2 + 2x_2x_5^2 + 13x_3x_5^2 + 9x_4x_5^2 + 3x_1^2x_6 + x_1x_2x_6 + 3x_2^2x_6 + 9x_1x_3x_6 + 9x_2x_3x_6 + 4x_3^2x_6 + 5x_1x_4x_6 + 5x_2x_4x_6 + 7x_3x_4x_6 + 7x_4^2x_6 + 5x_1x_5x_6 + 5x_2x_5x_6 + x_3x_5x_6 + 16x_4x_5x_6 + 15x_5^2x_6 + 15x_1x_6^2 + 15x_2x_6^2 + 14x_3x_6^2 + 11x_4x_6^2 + 9x_5x_6^2 + 2x_6^3 + 13x_1x_2 + 6x_1x_3 + 6x_2x_3 + 4x_3^2 + 4x_1x_4 + 4x_2x_4 + 9x_3x_4 + 8x_4^2 + 13x_1x_5 + 13x_2x_5 + 12x_3x_5 + 6x_5^2 + 9x_1x_6 + 9x_2x_6 + 15x_4x_6 + 5x_5x_6 + 8x_6^2 + 8x_1 + 8x_2 + x_3 + 3x_4 + 10x_5 + 16x_6 + 3$$

$I = \langle f_1, f_1^{M_1}, f_2, f_2^{M_2}, f_2^{M_2^2}, f_2^{M_2^3} \rangle$ is a (globally) G-invariant ideal.

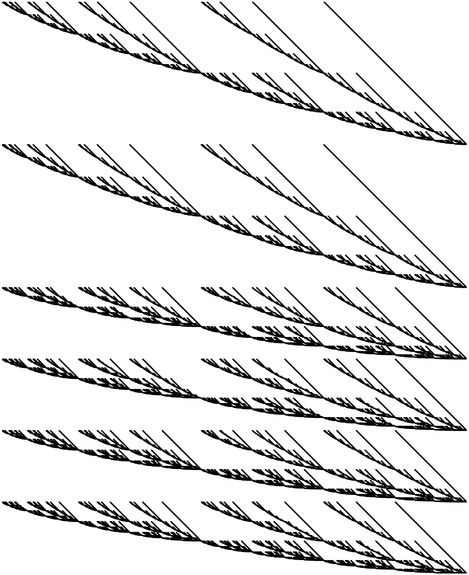
Affine Macaulay matrix in degree d of $f_1, \ldots, f_j$ in $k[x_1, \ldots, x_n]$

Ordering $\preceq$ on the monomials is fixed.

$$M_d = \begin{array}{c} \\ m_1.f_1 \\ \vdots \\ m_\mu f_i \\ \vdots \\ m_\gamma f_j \end{array} \begin{array}{c} \widetilde{m}_1 \succeq \quad \widetilde{m}_2 \quad \succeq \cdots \succeq \quad \widetilde{m}_\nu \\ \begin{pmatrix} \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix} \end{array}$$

with $\widetilde{m}_\beta$ describing all monomials of degree $\leq d$ and $m_\mu f_i$ all couples such that $deg(m_\mu) + deg(f_i) \leq d$.

Macaulay matrix in degree 8 of $f_1, f_1^{M_1}, f_2, f_2^{M_2}, f_2^{M_2^2}, f_2^{M_2^3}$



Size 3696× 3003. Non-zero entries : 1.73%

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(k)$, I a G-stable ideal.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(k)$, I a G-stable ideal.

- $A^{|G|} = I_n \quad \forall A \in G \rightsquigarrow$ Every matrix of G is diagonalizable in a finite extension of k.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(k)$, I a G-stable ideal.

- $A^{|G|} = I_n \quad \forall A \in G \rightsquigarrow$ Every matrix of G is diagonalizable in a finite extension of k.
- G abelian $\rightsquigarrow$ Same base-change matrix P.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(k)$, I a G-stable ideal.

- $A^{|G|} = I_n \quad \forall A \in G \rightsquigarrow$ Every matrix of G is diagonalizable in a finite extension of k.
- G abelian $\rightsquigarrow$ Same base-change matrix P.
- $G_D = \{P^{-1}AP \mid A \in G\}$: group of diagonal matrices.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(k)$, I a G-stable ideal.

- $A^{|G|} = I_n \quad \forall A \in G \rightsquigarrow$ Every matrix of G is diagonalizable in a finite extension of k.
- G abelian $\rightsquigarrow$ Same base-change matrix P.
- $G_D = \{P^{-1}AP \mid A \in G\}$: group of diagonal matrices.
- $I_D = \{f^P \mid f \in I\}$ is G_D-stable.

Example : Change of variables

$$M_1 = \left(\begin{array}{cc|cccc} 0 & 1 & & & & \\ 1 & 0 & & & & \\ \hline & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{array}\right) = {\color{red}P} \underbrace{\left(\begin{array}{cc|cccc} -1 & & & & & \\ & 1 & & & & \\ \hline & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{array}\right)}_{\color{red}D_1} {\color{red}P^{-1}}$$

Example : Change of variables

$$M_1 = \left(\begin{array}{cc|cccc} 0 & 1 & & & & \\ 1 & 0 & & & & \\ \hline & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{array}\right) = P \underbrace{\left(\begin{array}{cc|cccc} -1 & & & & & \\ & 1 & & & & \\ \hline & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{array}\right)}_{D_1} P^{-1}$$

$$M_2 = \left(\begin{array}{cc|cccc} 1 & & & & & \\ & 1 & & & & \\ \hline & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \\ & & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \end{array}\right) = P \underbrace{\left(\begin{array}{cc|cccc} 1 & & & & & \\ & 1 & & & & \\ \hline & & 4 & & & \\ & & & -1 & & \\ & & & & -4 & \\ & & & & & 1 \end{array}\right)}_{D_2} P^{-1}$$

$$f_1 = x_1^2 + 11x_1x_2 + 5x_2^2 + 4x_1x_3 + 11x_2x_3 + 4x_3^2 + 4x_1x_4 + 11x_2x_4 + x_3x_4 + 4x_4^2 + 4x_1x_5 + 11x_2x_5 + 6x_3x_5 + x_4x_5 + 4x_5^2 + 4x_1x_6 + 11x_2x_6 + x_3x_6 + 6x_4x_6 + x_5x_6 + 4x_6^2 + 14x_1 + 10x_2 + 15x_3 + 15x_4 + 15x_5 + 15x_6 + 14$$

$$f_2 = x_1^3 + 11x_1^2x_2 + 11x_1x_2^2 + x_2^3 + 7x_1^2x_3 + 14x_1x_2x_3 + 7x_2^2x_3 + 5x_1x_3^2 + 5x_2x_3^2 + 16x_3^3 + 16x_1x_2x_4 + 13x_1x_3x_4 + 13x_2x_3x_4 + 6x_3^2x_4 + 7x_1x_4^2 + 7x_2x_4^2 + 12x_3x_4^2 + 13x_4^3 + 13x_1^2x_5 + 6x_1x_2x_5 + 13x_2^2x_5 + 15x_1x_3x_5 + 15x_2x_3x_5 + x_3^2x_5 + 9x_1x_4x_5 + 9x_2x_4x_5 + 2x_4^2x_5 + 2x_1x_5^2 + 2x_2x_5^2 + 13x_3x_5^2 + 9x_4x_5^2 + 3x_1^2x_6 + x_1x_2x_6 + 3x_2^2x_6 + 9x_1x_3x_6 + 9x_2x_3x_6 + 4x_3^2x_6 + 5x_1x_4x_6 + 5x_2x_4x_6 + 7x_3x_4x_6 + 7x_4^2x_6 + 5x_1x_5x_6 + 5x_2x_5x_6 + x_3x_5x_6 + 16x_4x_5x_6 + 15x_5^2x_6 + 15x_1x_6^2 + 15x_2x_6^2 + 14x_3x_6^2 + 11x_4x_6^2 + 9x_5x_6^2 + 2x_6^3 + 13x_1x_2 + 6x_1x_3 + 6x_2x_3 + 4x_3^2 + 4x_1x_4 + 4x_2x_4 + 9x_3x_4 + 8x_4^2 + 13x_1x_5 + 13x_2x_5 + 12x_3x_5 + 6x_5^2 + 9x_1x_6 + 9x_2x_6 + 15x_4x_6 + 5x_5x_6 + 8x_6^2 + 8x_1 + 8x_2 + x_3 + 3x_4 + 10x_5 + 16x_6 + 3$$

$I = \langle f_1, f_1^{M_1}, f_2, f_2^{M_2}, f_2^{M_2^2}, f_2^{M_2^3} \rangle$ is a G-invariant ideal.

$f_1^P = 12x_1^2 + 8x_1x_2 + 7x_4^2 + 8x_3x_5 + 11x_1x_6 + 9x_2x_6 + 15x_6^2 + 13x_1 + 7x_2 + 9x_6 + 14$

$f_2^P = x_1^2x_2 + 7x_2^3 + 9x_1^2x_3 + 9x_2^2x_3 + 16x_2x_3^2 + 3x_1^2x_4 + 14x_2^2x_4 + 13x_2x_3x_4 + 4x_3^2x_4 + 9x_2x_4^2 + 12x_4^3 + 16x_1^2x_5 + 7x_2^2x_5 + 2x_2x_3x_5 + 16x_3^2x_5 + 15x_2x_4x_5 + 7x_3x_4x_5 + x_4^2x_5 + 16x_2x_5^2 + 2x_3x_5^2 + 7x_4x_5^2 + 15x_5^3 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_2x_3x_6 + 6x_3^2x_6 + 3x_2x_4x_6 + 15x_3x_4x_6 + 9x_4^2x_6 + 6x_2x_5x_6 + 12x_3x_5x_6 + 2x_4x_5x_6 + 10x_5^2x_6 + 16x_3x_6^2 + 6x_5x_6^2 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_2x_3 + 15x_3^2 + 5x_2x_4 + 2x_3x_4 + 5x_4^2 + 15x_2x_5 + 15x_3x_5 + 6x_4x_5 + 8x_5^2 + 13x_2x_6 + 13x_3x_6 + x_4x_6 + 13x_5x_6 + 16x_6^2 + 16x_2 + 11x_3 + 8x_4 + 15x_5 + 13x_6 + 3$

$I = \langle f_1^P, f_1^{PD_1}, f_2^P, f_2^{PD_2}, f_2^{PD_2^2}, f_2^{PD_2^3} \rangle$ is a G_D-invariant ideal with $G_D = \langle D_1, D_2 \rangle$.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1 | q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1|q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \text{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1|q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \mathrm{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.
- $m = \prod_{i=1}^{n} x_i^{\alpha_i}$.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1 | q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \mathrm{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.
- $m = \prod_{i=1}^n x_i^{\alpha_i}$.
- $m^{D_1} = \prod_{i=1}^n (x_i \xi_1^{\lambda_i})^{\alpha_i} = \xi_1^{\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n} m$.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1 | q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \mathrm{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.
- $m = \prod_{i=1}^n x_i^{\alpha_i}$.
- $m^{D_1} = \prod_{i=1}^n (x_i \xi_1^{\lambda_i})^{\alpha_i} = \xi_1^{\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n} m$.
- $g_1 = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n \in \mathbb{Z}/q_1\mathbb{Z}$ is called the $\langle D_1 \rangle$-degree of m.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1|q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \mathrm{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.
- $m = \prod_{i=1}^{n} x_i^{\alpha_i}$.
- $m^{D_1} = \prod_{i=1}^{n} (x_i \xi_1^{\lambda_i})^{\alpha_i} = \xi_1^{\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n} m$.
- $g_1 = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n \in \mathbb{Z}/q_1\mathbb{Z}$ is called the $\langle D_1 \rangle$-degree of m.
- Same action for D_2 $\rightsquigarrow$ $\langle D_2 \rangle$-degree.

Action of G on Monomials.

Notations

- G diagonal group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, with $q_1 | q_2$.
- D_1, D_2 two diagonal matrices generating $\mathbb{Z}/q_1\mathbb{Z}$ and $\mathbb{Z}/q_2\mathbb{Z}$.

- $D_1^{q_1} = I_n \Rightarrow D_1 = \mathrm{Diag}(\xi_1^{\lambda_1}, \ldots, \xi_1^{\lambda_n})$ with ξ_1 a q_1-primitive root of 1 and $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.
- $m = \prod_{i=1}^n x_i^{\alpha_i}$.
- $m^{D_1} = \prod_{i=1}^n (x_i \xi_1^{\lambda_i})^{\alpha_i} = \xi_1^{\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n} m$.
- $g_1 = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n \in \mathbb{Z}/q_1\mathbb{Z}$ is called the $\langle D_1 \rangle$-degree of m.
- Same action for D_2 $\rightsquigarrow$ $\langle D_2 \rangle$-degree.
- $(g_1, g_2) \in \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$ is called the G-degree of m.

Remember

$f_1^P = 12x_1^2 + 8x_1x_2 + 7x_4^2 + 8x_3x_5 + 11x_1x_6 + 9x_2x_6 + 15x_6^2 + 13x_1 + 7x_2 + 9x_6 + 14$

$f_2^P = x_1^2x_2 + 7x_2^3 + 9x_1^2x_3 + 9x_2^2x_3 + 16x_2x_3^2 + 3x_1^2x_4 + 14x_2^2x_4 + 13x_2x_3x_4 + 4x_3^2x_4 + 9x_2x_4^2 + 12x_4^3 + 16x_1^2x_5 + 7x_2^2x_5 + 2x_2x_3x_5 + 16x_3^2x_5 + 15x_2x_4x_5 + 7x_3x_4x_5 + x_4^2x_5 + 16x_2x_5^2 + 2x_3x_5^2 + 7x_4x_5^2 + 15x_5^3 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_2x_3x_6 + 6x_3^2x_6 + 3x_2x_4x_6 + 15x_3x_4x_6 + 9x_4^2x_6 + 6x_2x_5x_6 + 12x_3x_5x_6 + 2x_4x_5x_6 + 10x_5^2x_6 + 16x_3x_6^2 + 6x_5x_6^2 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_2x_3 + 15x_3^2 + 5x_2x_4 + 2x_3x_4 + 5x_4^2 + 15x_2x_5 + 15x_3x_5 + 6x_4x_5 + 8x_5^2 + 13x_2x_6 + 13x_3x_6 + x_4x_6 + 13x_5x_6 + 16x_6^2 + 16x_2 + 11x_3 + 8x_4 + 15x_5 + 13x_6 + 3$

Extract G-homogeneous components

$f_1^P = 12x_1^2 + 8x_1x_2 + 7x_4^2 + 8x_3x_5 + 11x_1x_6 + 9x_2x_6 + 15x_6^2 + 13x_1 + 7x_2 + 9x_6 + 14$

$f_2^P = x_1^2x_2 + 7x_2^3 + 9x_1^2x_3 + 9x_2^2x_3 + 16x_2x_3^2 + 3x_1^2x_4 + 14x_2^2x_4 + 13x_2x_3x_4 + 4x_3^2x_4 + 9x_2x_4^2 + 12x_4^3 + 16x_1^2x_5 + 7x_2^2x_5 + 2x_2x_3x_5 + 16x_3^2x_5 + 15x_2x_4x_5 + 7x_3x_4x_5 + x_4^2x_5 + 16x_2x_5^2 + 2x_3x_5^2 + 7x_4x_5^2 + 15x_5^3 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_2x_3x_6 + 6x_3^2x_6 + 3x_2x_4x_6 + 15x_3x_4x_6 + 9x_4^2x_6 + 6x_2x_5x_6 + 12x_3x_5x_6 + 2x_4x_5x_6 + 10x_5^2x_6 + 16x_3x_6^2 + 6x_5x_6^2 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_2x_3 + 15x_3^2 + 5x_2x_4 + 2x_3x_4 + 5x_4^2 + 15x_2x_5 + 15x_3x_5 + 6x_4x_5 + 8x_5^2 + 13x_2x_6 + 13x_3x_6 + x_4x_6 + 13x_5x_6 + 16x_6^2 + 16x_2 + 11x_3 + 8x_4 + 15x_5 + 13x_6 + 3$

Extract G-homogeneous components

$f_1^P = 12x_1^2 + 8x_1x_2 + 7x_4^2 + 8x_3x_5 + 11x_1x_6 + 9x_2x_6 + 15x_6^2 + 13x_1 + 7x_2 + 9x_6 + 14$

$f_2^P = x_1^2x_2 + 7x_2^3 + 9x_1^2x_3 + 9x_2^2x_3 + 16x_2x_3^2 + 3x_1^2x_4 + 14x_2^2x_4 + 13x_2x_3x_4 + 4x_3^2x_4 + 9x_2x_4^2 + 12x_4^3 + 16x_1^2x_5 + 7x_2^2x_5 + 2x_2x_3x_5 + 16x_3^2x_5 + 15x_2x_4x_5 + 7x_3x_4x_5 + x_4^2x_5 + 16x_2x_5^2 + 2x_3x_5^2 + 7x_4x_5^2 + 15x_5^3 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_2x_3x_6 + 6x_3^2x_6 + 3x_2x_4x_6 + 15x_3x_4x_6 + 9x_4^2x_6 + 6x_2x_5x_6 + 12x_3x_5x_6 + 2x_4x_5x_6 + 10x_5^2x_6 + 16x_3x_6^2 + 6x_5x_6^2 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_2x_3 + 15x_3^2 + 5x_2x_4 + 2x_3x_4 + 5x_4^2 + 15x_2x_5 + 15x_3x_5 + 6x_4x_5 + 8x_5^2 + 13x_2x_6 + 13x_3x_6 + x_4x_6 + 13x_5x_6 + 16x_6^2 + 16x_2 + 11x_3 + 8x_4 + 15x_5 + 13x_6 + 3$

The terms of same color in f_1^P or f_2^P are of same G-degree, and are called the G-homogeneous components.

G-homogeneous polynomials

Theorem

If I is G-stable and $f \in I$, the G-homogeneous components of f belong to I.

Theorem

If I is G-stable and $f \in I$, the G-homogeneous components of f belong to I.

Consequence

$\rightsquigarrow$ Extract from polynomials $f_1, \ldots, f_m$ generating I the G-homogeneous components.

Extract G-homogeneous components

$g_1 = x_1x_2 + 12x_1x_6 + 8x_1$ of G-degree $(1, 0)$.

$g_2 = x_1^2 + 2x_4^2 + 12x_3x_5 + 5x_2x_6 + 14x_6^2 + 2x_2 + 5x_6 + 4$ of G-degree $(0, 0)$.

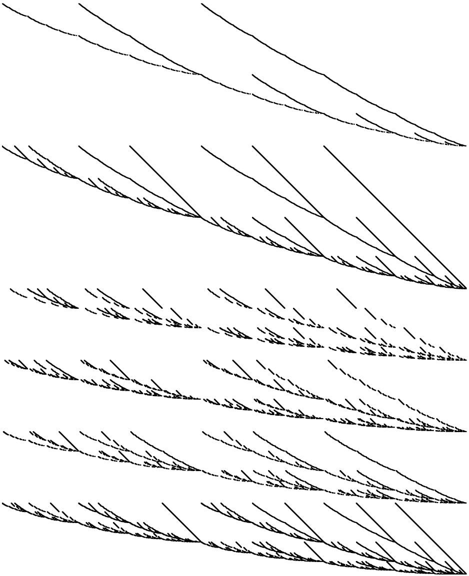
$g_3 = x_2x_3x_4 + 13x_1^2x_5 + 11x_2^2x_5 + 4x_4^2x_5 + 8x_3x_5^2 + 9x_3x_4x_6 + 7x_2x_5x_6 + 7x_5x_6^2 + 8x_3x_4 + 9x_2x_5 + x_5x_6 + 9x_5$ of G-degree $(0, 3)$.

$g_4 = x_2x_3^2 + 14x_1^2x_4 + 3x_2^2x_4 + 5x_4^3 + 10x_3x_4x_5 + x_2x_5^2 + 11x_3^2x_6 + 14x_2x_4x_6 + 7x_5^2x_6 + 2x_3^2 + 12x_2x_4 + 9x_5^2 + 16x_4x_6 + 9x_4$ of G-degree $(0, 2)$.

$g_5 = x_1^2x_3 + x_2^2x_3 + 15x_3^2x_5 + 13x_2x_4x_5 + 13x_5^3 + x_2x_3x_6 + 4x_4x_5x_6 + 15x_3x_6^2 + 10x_2x_3 + 12x_4x_5 + 9x_3x_6 + 5x_3$ of G-degree $(0, 1)$.

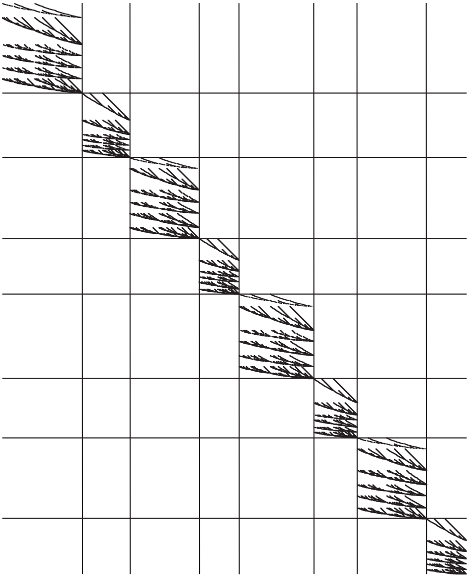
$g_6 = x_1^2x_2 + 7x_2^3 + 4x_3^2x_4 + 9x_2x_4^2 + 2x_2x_3x_5 + 7x_4x_5^2 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_4^2x_6 + 12x_3x_5x_6 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_4^2 + 15x_3x_5 + 13x_2x_6 + 16x_6^2 + 16x_2 + 13x_6 + 3$ of G-degree $(0, 0)$.

Macaulay's matrix in degree 8 of $g_1, g_2, g_3, g_4, g_5, g_6$



Size 3696× 3003. Non-zero entries : 0.33%

Same matrix, with a permutation of rows and columns



Block diagonal matrix with 8 blocks of size $\simeq 462 \times 375$.

Grading on $R = k[x_1, \ldots, x_n]$

Product of two monomials

For all monomials m and m', $\deg_G(mm') = \deg_G(m) + \deg_G(m')$.

Grading

$R = \oplus_{g \in \hat{G}} R_g$

Grading on $R = k[x_1, \ldots, x_n]$

Product of two monomials

For all monomials m and m', $\deg_G(mm') = \deg_G(m) + \deg_G(m')$.

Grading

$R = \oplus_{g \in \hat{G}} R_g$

S-polynomials of G-homogeneous polynomials

$S(f, g) = \frac{LM(f) \vee LM(g)}{LM(f)} f - \frac{LM(f) \vee LM(g)}{LM(g)} \frac{LC(f)}{LC(g)} g$ is G-homogeneous if f and g are.

Computation

Any Gröbner basis algorithm preserves the G-homogeneity !

Equations : $f_1, \ldots, f_m$ G-homogeneous.

F_5 constructs matrices degree by degree and equation by equation.

$$\widetilde{M_{d,i}} = \text{Row-Echelon} \quad \begin{array}{c} \\ \\ m_1 f_i \\ \vdots \\ m_\ell f_i \end{array} \overset{\begin{array}{ccc} m_1^* \succeq & \ldots & \succeq m_\mu^* \end{array}}{\left(\begin{array}{ccc} & \widetilde{M_{d,i-1}} & \\ \hline \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{array} \right)}$$

m_j^*: monomials of degree $\leq d$

m_j: monomials of degree $\leq d - d_i$

$\underbrace{\text{except those in } LM(\widetilde{M_{d-d_i,i-1}})}_{F_5\text{-criterion}}$.

Equations : $f_1, \ldots, f_m$ G-homogeneous.
Abelian-F_5 constructs matrices degree by degree and equation by equation and G-degree by G-degree.

$$\widetilde{M_{d,i,g}} = \text{Row-Echelon} \quad \begin{array}{c} \\ \\ \hline m_1 f_i \\ \vdots \\ m_\ell f_i \end{array} \overset{\begin{array}{ccc} m_1^* \succeq & \ldots & \succeq m_\mu^* \end{array}}{\left(\begin{array}{ccc} & \widetilde{M_{d,i-1,g}} & \\ \hline \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{array}\right)}$$

m_j^*: monomials of degree $\leq d$ and G-degree g
m_j: monomials of degree $\leq d - d_i$ and G-degree $g - g_i$
$\underbrace{\text{except those in } LM(\widetilde{M_{d-d_i,i-1,g-g_i}})}_{F_5\text{-criterion}}$.

Multiplication matrices in FGLM algorithm

- I a G-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of I for $\preceq_1$.
- $\mathcal{E}$: Monomials not reducible by $\mathcal{G}_{\preceq_1}$.

- I a G-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of I for $\preceq_1$.
- $\mathcal{E}$: Monomials not reducible by $\mathcal{G}_{\preceq_1}$.

Goal: Compute matrices of the maps:

$$\begin{array}{cccc} M_i & : & \mathrm{Vect}(\mathcal{E}\ ) & \longrightarrow & \mathrm{Vect}(\mathcal{E}) \\ & & f & \mapsto & NF(x_i f, \mathcal{G}_{\preceq_1}) \end{array}$$

- I a G-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of I for $\preceq_1$.
- $\mathcal{E}$: Monomials not reducible by $\mathcal{G}_{\preceq_1}$.

Goal: Compute matrices of the maps:

$$\begin{array}{rccc} M_i & : & \mathrm{Vect}(\mathcal{E}\ ) & \longrightarrow & \mathrm{Vect}(\mathcal{E}) \\ & & f & \mapsto & NF(x_i f, \mathcal{G}_{\preceq_1}) \end{array}$$

Normal-Form preserves the G-degree

$$deg_G(NF(m_j x_i, \mathcal{G}_{\preceq_1})) = deg_G(m_j x_i) = deg_G(m_j) + deg_G(x_i)$$

Multiplication matrices in Abelian-FGLM algorithm

- I a G-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of I for $\preceq_1$.
- $\mathcal{E}$: Monomials not reducible by $\mathcal{G}_{\preceq_1}$.

Goal: Compute matrices of the maps:

$$\begin{array}{rccc} M_{i,g}: & \mathrm{Vect}(\mathcal{E}_g) & \longrightarrow & \mathrm{Vect}(\mathcal{E}_{g+deg_G(x_i)}) \\ & f & \mapsto & NF(x_i f, \mathcal{G}_{\preceq_1}) \end{array}$$

with $\mathcal{E}_g$ the subset of monomials in $\mathcal{E}$ of G-degree g.

Normal-Form preserves the G-degree

$$deg_G(NF(m_j x_i, \mathcal{G}_{\preceq_1})) = deg_G(m_j x_i) = deg_G(m_j) + deg_G(x_i)$$

Continuation of the example

- $I = \langle g_1, g_2, g_3, g_4, g_5, g_6 \rangle$ is zero-dimensional of degree 308.

Continuation of the example

- $I = \langle g_1, g_2, g_3, g_4, g_5, g_6 \rangle$ is zero-dimensional of degree 308.
- The sizes of the staircases $\mathcal{E}_g$ for $g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are : 69, 23, 51, 17, 60, 20, 51, 17.

Continuation of the example

- $I = \langle g_1, g_2, g_3, g_4, g_5, g_6 \rangle$ is zero-dimensional of degree 308.
- The sizes of the staircases $\mathcal{E}_g$ for $g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are : 69, 23, 51, 17, 60, 20, 51, 17.
- Instead of building 6 matrices of sizes 308×308, we build 48 matrices of various sizes $|\mathcal{E}_g| \times |\mathcal{E}_{g+deg_G(x_i)}|$.

Continuation of the example

- $I = \langle g_1, g_2, g_3, g_4, g_5, g_6 \rangle$ is zero-dimensional of degree 308.
- The sizes of the staircases $\mathcal{E}_g$ for $g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are : 69, 23, 51, 17, 60, 20, 51, 17.
- Instead of building 6 matrices of sizes 308×308, we build 48 matrices of various sizes $|\mathcal{E}_g| \times |\mathcal{E}_{g+deg_G(x_i)}|$.
- 83402 coefficients instead of 569184.

Complexity Questions

Theorem : Repartition of the monomials

$$\frac{\#\{\text{Monomials of degree} \leq d \text{ and } G\text{-degree } g\}}{\#\{\text{Monomials of degree} \leq d\}} \underset{d \to +\infty}{\longrightarrow} \frac{1}{|G|}$$

Complexity Questions

Theorem : Repartition of the monomials

$$\frac{\#\{\text{Monomials of degree} \leq d \text{ and } G\text{-degree } g\}}{\#\{\text{Monomials of degree} \leq d\}} \underset{d \to +\infty}{\longrightarrow} \frac{1}{|G|}$$

Theoretical speed-up

$|G|^\omega$ in F_5 and $|G|^2$ in FGLM.

Complexity Questions

Theorem : Repartition of the monomials

$$\frac{\#\{\text{Monomials of degree} \leq d \text{ and } G\text{-degree } g\}}{\#\{\text{Monomials of degree} \leq d\}} \underset{d \to +\infty}{\longrightarrow} \frac{1}{|G|}$$

Theoretical speed-up

$|G|^\omega$ in F_5 and $|G|^2$ in FGLM.

In practice

- Abelian$-F_4$ has been implemented in C and Abelian-FGLM in Magma.
- Matrices have *effectively* number of rows and columns divided by $\simeq |G|$.

Some Timings with Abelian-F_4.

			——————— Ratios ———————		
n	k_1, k_2	$F_4^{\mathcal{A},k_1 k_2}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},k_1 k_2}$	$F_4/F_4^{\mathcal{A},k_1 k_2}$	$F_4^{\mathrm{M}}/F_4^{\mathcal{A},k_1 k_2}$
8	8,0	3.6s	3.6	31	22
8	4,4	2.0s	2.4	62	37
8	6,2	2.9s	2.2	76	44
10	5,5	70s	12	∞	∞
10	6,4	92s	18	∞	∞
10	8,2	107s	12	∞	∞
10	10,0	706s	11	∞	∞

Table: $n = k_1 + k_2$ cubic equations invariant under $C_{k_1} \times C_{k_2}$

The cyclic-n problem

Ideal generated by the polynomials

$$\begin{cases} f_1 = x_1 + \cdots + x_n \\ f_2 = x_1 x_2 + x_2 x_3 + \cdots + x_n x_1 \\ \vdots \\ f_{n-1} = x_1 x_2 \ldots x_{n-1} + x_2 \ldots x_n x_1 + \cdots + x_n x_1 \ldots x_{n-2} \\ f_n = x_1 x_2 \ldots x_{n-1} x_n - 1 \end{cases}$$

Invariant under the n-cycle $(12\ldots n)$. After diagonalization, problem invariant under $diag(1, \xi, \xi^2, \ldots, \xi^{n-1})$ with ξ a n-primitive root of 1.

Timings on Cyclic-n

		Ratios		
n	$F_4^{\mathcal{A},n}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},n}$	$F_4/F_4^{\mathcal{A},n}$	$F_4^{\mathrm{M}}/F_4^{\mathcal{A},n}$
8	0.5s	2.5	7.8	6.0
9	10s	4.3	37.0	30.5
10	334s	13.2	411	207
11	27539s	∞	∞	∞

Table: The Cyclic-n problem

Polynomial Timings

		Ratios	
n	$F_4^{\mathcal{A},n}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},n}$	$F_4/F_4^{\mathcal{A},n}$
25	0.25s	1.9	56.60
30	0.58s	1.5	80.79
35	0.86s	1.9	228.5
40	1.55s	2.0	300.6
45	2.31s	2.4	664.5
50	3.96s	2.6	753.8
55	6.98s	2.5	1207
60	10.85s	2.8	1294

Table: n quadratic equations of G-degree 0 or 1

n	$F_4^{\mathcal{A},n}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},n}$ (Ratios)	$F_4/F_4^{\mathcal{A},n}$ (Ratios)
25	0.25s : 0.06s	1.9 : 4.5	56.60 : 230.0
30	0.58s : 0.11s	1.5 : 4.6	80.79 : 415.1
35	0.86s : 0.11s	1.9 : 8.5	228.5 : 1755
40	1.55s : 0.21s	2.0 : 8.5	300.6 : 2174
45	2.31s : 0.30s	2.4 : 10.7	664.5 : 5043
50	3.96s : 0.45s	2.6 : 13.3	753.8 : 6504
55	6.98s : 0.66s	2.5 : 15.0	1207 : 12570
60	10.85s : 0.96s	2.8 : 17.2	1294 : 14330

Table: n quadratic equations of G-degree 0 or 1

In red, only timings/ratios for the parallelized part.

Polynomial Timings

		——— Ratios ———	
n	$F_4^{\mathcal{A},n}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},n}$	$F_4/F_4^{\mathcal{A},n}$
25	0.25s : 0.06s	1.9 : 4.5	56.60 : 230.0
30	0.58s : 0.11s	1.5 : 4.6	80.79 : 415.1
35	0.86s : 0.11s	1.9 : 8.5	228.5 : 1755
40	1.55s : 0.21s	2.0 : 8.5	300.6 : 2174
45	2.31s : 0.30s	2.4 : 10.7	664.5 : 5043
50	3.96s : 0.45s	2.6 : 13.3	753.8 : 6504
55	6.98s : 0.66s	2.5 : 15.0	1207 : 12570
60	10.85s : 0.96s	2.8 : 17.2	1294 : 14330

Table: n quadratic equations of G-degree 0 or 1

In red, only timings/ratios for the parallelized part.

G-invariant ideals generated by quadratic equations with a fixed number of distincts G-degrees can be solved in polynomial-time.

Basic Underlying Problem [Silvermann&al.96]

Given $h = \sum_{i=0}^{n-1} h_i x^i \in \mathbb{F}_p[x]$, find $f = \sum_{i=0}^{n-1} f_i x^i \in \mathbb{F}_p[x]$ such that f and $f\,h \bmod x^n - 1$ have their coefficients in $\{0, 1\}$.

Resulting equations

This problem leads to $2n$ equations under the group generated by $(12..n)$.

NTRU Timings

n	$F_4^{\mathcal{A},n}$	$F_4^{\mathcal{A}}/F_4^{\mathcal{A},n}$	$F_4/F_4^{\mathcal{A},n}$
		Speed-up	
20	3.0s:0.8s	3.5:11.3	66.0:257.8
21	4.5s:1.2s	4.0:11.9	90.15:334.0
22	15.0s:2.3s	2.2:11.4	58.4:381.6
23	11.1s:1.9s	3.3:17.2	115.2:686.1
24	128s:14.3s	5.2:36.5	241.1:2149.0
25	218s:31.0s	5.8:32.5	∞
26	365s:59.0s	6.6:32.6	∞
27	955s:113s	4.9:33.3	∞
28	1214s:192s	7.1:36.1	∞
29	3310s:323s	4.7:38.8	∞

Table: NTRU equations

In red, only timings/ratios for the parallelized part.

Perspectives

- Better speed-up for FGLM ?

Perspectives

- Better speed-up for FGLM ?
- Study the Hilbert series of such invariant problems.

Perspectives

- Better speed-up for FGLM ?
- Study the Hilbert series of such invariant problems.
- Extension to the modular case ?

Perspectives

- Better speed-up for FGLM ?
- Study the Hilbert series of such invariant problems.
- Extension to the modular case ?
- Extension to other groups ?

Thank you for your attention !