Résolution de systèmes zéro-dimensionnels avec symétries.

Jules Svartz

CNRS/INRIA/LIP6/UPMC – Polsys Team

Séminaire Specfun

Mardi 15 Avril

Polynomial Systems Solving

$$\boxed{\begin{array}{c} I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x_1, \ldots, x_n] \\ \text{Solve } f_1 = \cdots = f_t = 0 \end{array}}$$

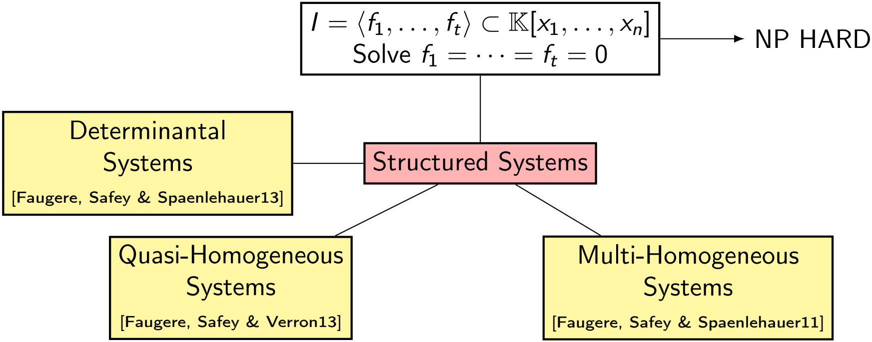
Polynomial Systems Solving

$$\boxed{\begin{array}{c} I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x_1, \ldots, x_n] \\ \text{Solve } f_1 = \cdots = f_t = 0 \end{array}} \longrightarrow \text{NP HARD}$$

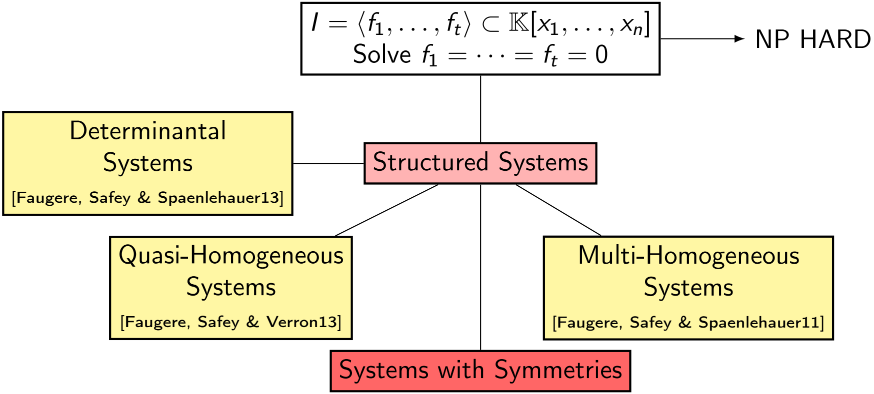
Polynomial Systems Solving

$I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$
Solve $f_1 = \cdots = f_t = 0$ $\longrightarrow$ NP HARD

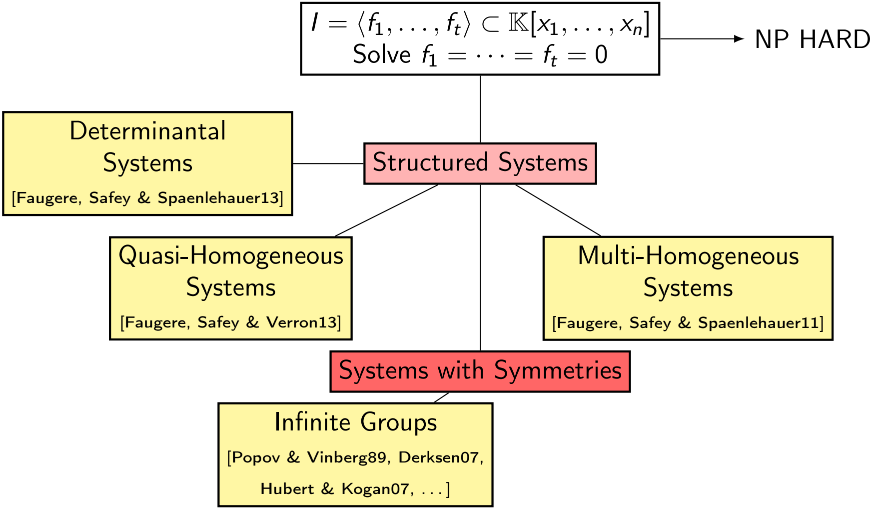
Structured Systems


$I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$
Solve $f_1 = \cdots = f_t = 0$
NP HARD
Structured Systems
Determinantal Systems
[Faugere, Safey & Spaenlehauer13]
Quasi-Homogeneous Systems
[Faugere, Safey & Verron13]
Multi-Homogeneous Systems
[Faugere, Safey & Spaenlehauer11]

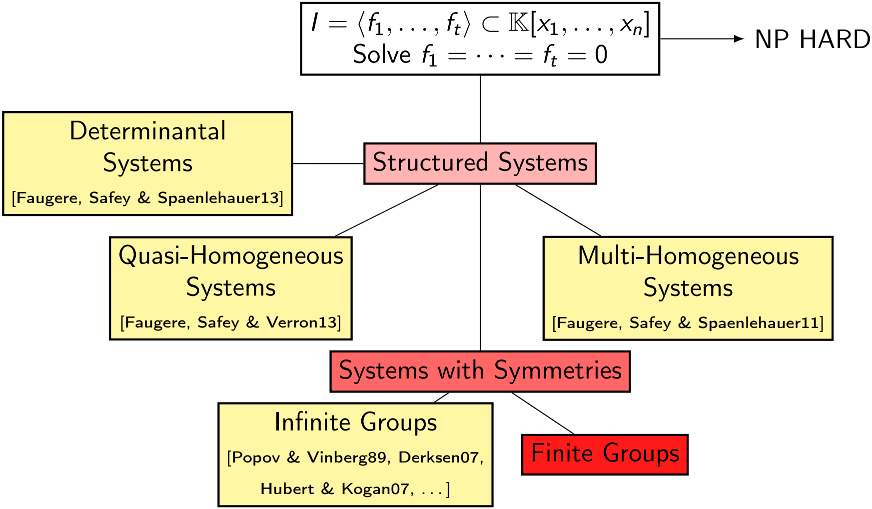
Polynomial Systems Solving



Polynomial Systems Solving



Polynomial Systems Solving



Action of Matrix Groups on Polynomials

Action of G

$G \subset GL_n(\mathbb{K})$ acts on $\mathbb{K}[x_1, \ldots, x_n]$: for $A \in G$, $f^A(x) = f(A.x)$ with $x = {}^t(x_1, x_2, \ldots, x_n)$.

Example

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

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

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

Stable Equations

$\forall A \in G \quad f_i^A = f_i$

Stable Ideal

$f \in I, A \in G \Rightarrow f^A \in I$

Local	Global
Stable Equations	Stable Ideal
$\forall A \in G \quad f_i^A = f_i$	$f \in I, A \in G \Rightarrow f^A \in I$

Systems Invariant Under Action of a Finite Group G

Local	Global
Stable Equations	Stable Ideal
$\forall A \in G \quad f_i^A = f_i$ $\Longrightarrow$	$f \in I, A \in G \Rightarrow f^A \in I$

Systems Invariant Under Action of a Finite Group G

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

Groups with small number of Invariants: Invariant Theory[1] $\rightarrow$ $\mathfrak{S}_n$

[1] [Sturmfels08]

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

Groups with small number of Invariants: Invariant Theory[1] $\rightarrow$ $\mathfrak{S}_n$

Subgroup of $\mathfrak{S}_n$: SAGBI Bases[2]

[1] [Sturmfels08]
[2] [Colin97, Faugère & Rahmany09]

Systems Invariant Under Action of a Finite Group G

Local

Stable Equations

$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Global

Stable Ideal

$f \in I, A \in G \Rightarrow f^A \in I$

$\mathfrak{S}_n$

Groups with small number of Invariants: Invariant Theory[1]

$\mathfrak{S}_n$: Divided Differences[3]

Subgroup of $\mathfrak{S}_n$: SAGBI Bases[2]

[1] [Sturmfels08]
[2] [Colin97, Faugère & Rahmany09]
[3] [Faugère, Hering & Phan03]

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

Groups with small number of Invariants: Invariant Theory[1]

$\mathfrak{S}_n$

$\mathfrak{S}_n$: Divided Differences[3]

Groups with Reflections: Split the System[4]

Subgroup of $\mathfrak{S}_n$: SAGBI Bases[2]

[1] [Sturmfels08]
[2] [Colin97, Faugère & Rahmany09]
[3] [Faugère, Hering & Phan03]
[4] [Gatermann90]

Systems Invariant Under Action of a Finite Group G

Local	Global
Stable Equations $\forall A \in G \quad f_i^A = f_i$	Stable Ideal $f \in I, A \in G \Rightarrow f^A \in I$

$\Longrightarrow$

Groups with small number of Invariants: Invariant Theory[1]

$\mathfrak{S}_n$

$\mathfrak{S}_n$: Divided Differences[3]

Groups with Reflections: Split the System[4]

Subgroup of $\mathfrak{S}_n$: SAGBI Bases[2]

Abelian Groups: Diagonalization[5]

[1] [Sturmfels08]
[2] [Colin97, Faugère & Rahmany09]
[3] [Faugère, Hering & Phan03]
[4] [Gatermann90]
[5] [Stanley79, Gatermann90, Steidel13]

Contributions

Local | **Global**

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

Groups with small number of Invariants: Invariant Theory

$\mathfrak{S}_n$

Vortex Problem

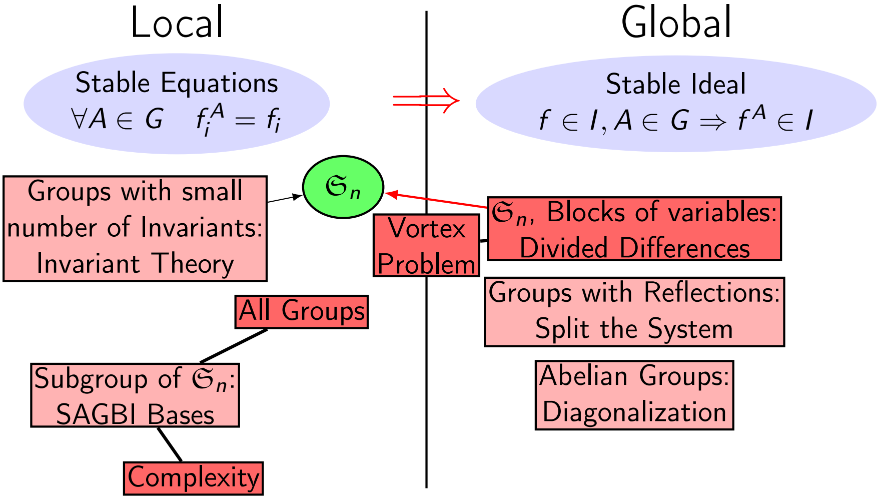
$\mathfrak{S}_n$, Blocks of variables: Divided Differences

Groups with Reflections: Split the System

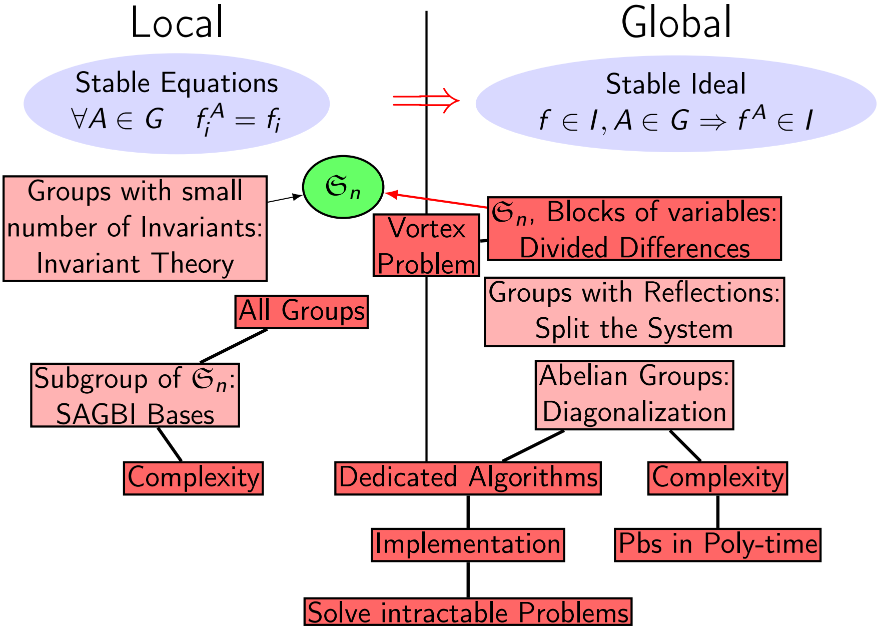
Subgroup of $\mathfrak{S}_n$: SAGBI Bases

Abelian Groups: Diagonalization

Contributions



Contributions

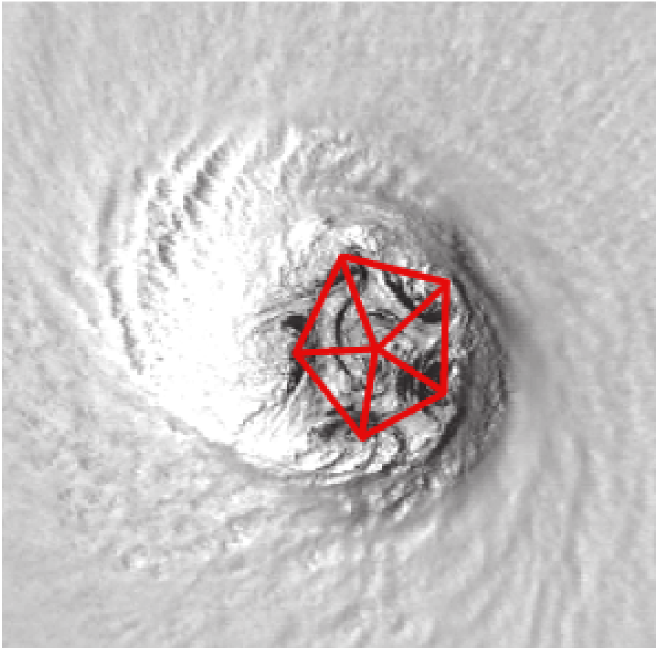


Vortex Problem: A Symbolic Approach.

Jean-Charles Faugère, J.S.

ISSAC 2012

Hurricane



Symmetry

Equations

$$\forall i \in \{1, \dots, N\} \qquad f_i = \overline{z_i} - \sum_{j \neq i} \frac{1}{z_i - z_j} = 0$$

Equations

$$\forall i \in \{1, \ldots, N\} \qquad f_i = \overline{z_i} - \sum_{j \neq i} \frac{1}{z_i - z_j} = 0$$

Invariance under $\mathfrak{S}_N$

Action of $\mathfrak{S}_N$: $\sigma(z_i) = z_{\sigma(i)}$ for all i. For any σ, $f_i^\sigma = f_{\sigma(i)}$.

Equations

$$\forall i \in \{1, \ldots, N\} \qquad f_i = \overline{z_i} - \sum_{j \neq i} \frac{1}{z_i - z_j} = 0$$

Invariance under $\mathfrak{S}_N$

Action of $\mathfrak{S}_N$: $\sigma(z_i) = z_{\sigma(i)}$ for all i. For any σ, $f_i^\sigma = f_{\sigma(i)}$.

Invariance under complex conjugation

$(z_1, \ldots, z_N)$ solution $\Rightarrow (\overline{z_1}, \ldots, \overline{z_N})$ solution.

Divided Differences

$N = 3$: Equations

$U_1 = Z_1(z_1 - z_2)(z_1 - z_3) - 2z_1 + z_2 + z_3$ of degree 3 (6 equations)

Divided Differences

$N = 3$: Equations

$U_1 = Z_1(z_1 - z_2)(z_1 - z_3) - 2z_1 + z_2 + z_3$ of degree 3 (6 equations)

$N = 3$: Divided Differences

$4\sum_i Z_i z_i^2 = 3, \quad \sum_i Z_i z_i - 9 = \sum_i Z_i = 0$ (Degree 1, 2, 3).

Divided Differences

$N = 3$: Equations

$U_1 = Z_1(z_1 - z_2)(z_1 - z_3) - 2z_1 + z_2 + z_3$ of degree 3 (6 equations)

$N = 3$: Divided Differences

$4\sum_i Z_i z_i^2 = 3, \quad \sum_i Z_i z_i - 9 = \sum_i Z_i = 0$ (Degree 1, 2, 3).

New Invariants

$$\underbrace{s_k = \sum_{i=1}^{N} z_i^k \qquad S_k = \sum_{i=1}^{N} Z_i^k}_{\text{Newton sums}} \qquad r_k = \sum_{i=1}^{N} z_i^k Z_i \qquad R_k = \sum_{i=1}^{N} z_i Z_i^k$$

Divided Differences

$N = 3$: Equations

$U_1 = Z_1(z_1 - z_2)(z_1 - z_3) - 2z_1 + z_2 + z_3$ of degree 3 (6 equations)

$N = 3$: Divided Differences

$4\sum_i Z_i z_i^2 = 3, \quad \sum_i Z_i z_i - 9 = \sum_i Z_i = 0$ (Degree 1, 2, 3).

New Invariants

$$\underbrace{s_k = \sum_{i=1}^{N} z_i^k \qquad S_k = \sum_{i=1}^{N} Z_i^k}_{\text{Newton sums}} \qquad r_k = \sum_{i=1}^{N} z_i^k Z_i \qquad R_k = \sum_{i=1}^{N} z_i Z_i^k$$

Theorem: Vortex Problem Equations

For each k, $2r_k = \sum_{i=0}^{k-1} s_i s_{k-1-i} - k s_{k-1}$ and same equation with $z \leftrightarrow Z$.

Removing Capital Letters

Equivalent problem : use of the $\mathfrak{S}_N$-symmetry

Find all solutions $(z_1, \dots, z_N)$
$\Leftrightarrow$ Find all possible symmetric functions $(e_1, \dots, e_N)$ of the z_i
$\Leftrightarrow$ Find all polynomials $Q = x^N + e_2 x^{N-2} + \cdots + (-1)^N e_N$
with $\mathrm{Disc}(Q) \neq 0$

Removing Capital Letters

Equivalent problem : use of the $\mathfrak{S}_N$-symmetry

Find all solutions $(z_1, \ldots, z_N)$
$\Leftrightarrow$ Find all possible symmetric functions $(e_1, \ldots, e_N)$ of the z_i
$\Leftrightarrow$ Find all polynomials $Q = x^N + e_2 x^{N-2} + \cdots + (-1)^N e_N$
with $\mathrm{Disc}(Q) \neq 0$

Theorem

$Q = \prod(x - z_i)$ solution of Vortex Problem $\Longleftrightarrow \forall i \quad \overline{z_i} = \frac{Q''(z_i)}{2Q'(z_i)}$.

Equivalent problem : use of the $\mathfrak{S}_N$-symmetry

Find all solutions $(z_1, \dots, z_N)$
$\Leftrightarrow$ Find all possible symmetric functions $(e_1, \dots, e_N)$ of the z_i
$\Leftrightarrow$ Find all polynomials $Q = x^N + e_2 x^{N-2} + \cdots + (-1)^N e_N$
with $\mathrm{Disc}(Q) \neq 0$

Theorem

$Q = \prod (x - z_i)$ solution of Vortex Problem $\Longleftrightarrow \forall i \quad \overline{z_i} = \frac{Q''(z_i)}{2Q'(z_i)}$.

Plug $Z_i = \frac{Q''(z_i)}{2Q'(z_i)}$ in the invariant equations !

Removing Capital Letters: Example $N = 3$

$N = 3$: Inverse of Q' with $Q = x^3 + e_2 x - e_3$

$Q'(x) \times (-6e_2x^2 - 9e_3x - 4e_2^2) \equiv 1[Q]$

Removing Capital Letters: Example $N = 3$

$N = 3$: Inverse of Q' with $Q = x^3 + e_2 x - e_3$

$$Q'(x) \times (-6e_2x^2 - 9e_3x - 4e_2^2) \equiv 1[Q]$$

$N = 3$: Mix both equations

$$4\sum Z_i^2 z_i = 3 \text{ and } Z_i = \frac{Q''(z_i)}{2Q'(z_i)} \rightsquigarrow \mathrm{Disc(Q)}e_2e_3 = 0$$

Removing Capital Letters: Example $N = 3$

$N = 3$: Inverse of Q' with $Q = x^3 + e_2 x - e_3$

$Q'(x) \times (-6e_2x^2 - 9e_3x - 4e_2^2) \equiv 1[Q]$

$N = 3$: Mix both equations

$4\sum Z_i^2 z_i = 3$ and $Z_i = \frac{Q''(z_i)}{2Q'(z_i)} \rightsquigarrow \mathrm{Disc(Q)}e_2e_3 = 0$

$N = 3$: Solve the equations

$e_2 \neq 0$ and $e_3 = 0$ or $e_2 = 0$ and $e_3 \neq 0$

Removing Capital Letters: Example $N = 3$

$N = 3$: Inverse of Q' with $Q = x^3 + e_2 x - e_3$

$Q'(x) \times (-6e_2x^2 - 9e_3x - 4e_2^2) \equiv 1[Q]$

$N = 3$: Mix both equations

$4\sum Z_i^2 z_i = 3$ and $Z_i = \frac{Q''(z_i)}{2Q'(z_i)} \rightsquigarrow \mathrm{Disc(Q)}e_2e_3 = 0$

$N = 3$: Solve the equations

$e_2 \neq 0$ and $e_3 = 0$ or $e_2 = 0$ and $e_3 \neq 0$

$N = 3$: Recover Solutions in z_i, up to symmetries

Two Solutions: regular triangle or three aligned points.

Example $N = 4$

$N = 4$: Reformulation in term of e_i

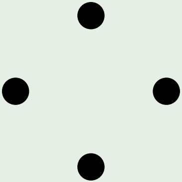
$$\begin{cases} e_3(e_2^2 + 12e_4)^2 = 0 \\ e_2(e_2^4 - 16e_2^2 e_4 + 9e_2 e_3^2 + 48e_4^2) = 0 \\ 16e_2^4 e_4 - 4e_2^3 e_3^2 - 128e_2^2 e_4^2 + 144e_2 e_3^2 e_4 - 27e_3^4 + 256e_4^3 \neq 0 \end{cases}$$

Example $N = 4$

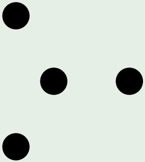
$N = 4$: Reformulation in term of e_i

$$\begin{cases} e_3(e_2^2 + 12e_4)^2 = 0 \\ e_2(e_2^4 - 16e_2^2e_4 + 9e_2e_3^2 + 48e_4^2) = 0 \\ 16e_2^4e_4 - 4e_2^3e_3^2 - 128e_2^2e_4^2 + 144e_2e_3^2e_4 - 27e_3^4 + 256e_4^3 \neq 0 \end{cases}$$

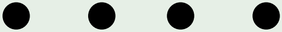
$N = 4$: Solutions



Roots of $z^4 - 1$



Roots of $z^4 - z$



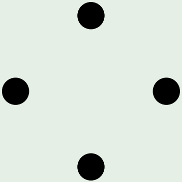
Roots of $z^4 - 3z^2 + 3/4$

Example $N = 4$

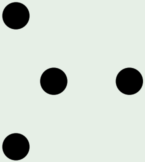
$N = 4$: Reformulation in term of e_i

$$\begin{cases} e_3(e_2^2 + 12e_4)^2 = 0 \\ e_2(e_2^4 - 16e_2^2e_4 + 9e_2e_3^2 + 48e_4^2) = 0 \\ 16e_2^4e_4 - 4e_2^3e_3^2 - 128e_2^2e_4^2 + 144e_2e_3^2e_4 - 27e_3^4 + 256e_4^3 \neq 0 \end{cases}$$

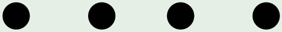
$N = 4$: Solutions



Roots of $z^4 - 1$



Roots of $z^4 - z$



Roots of $z^4 - 3z^2 + 3/4$

$N = 4$: Naive Approach

205 Polynomials in the DRL Gb of Max Length 111, Degree 6.

Experimental Results

Direct Approach : Obtain a Gröbner Basis, with $z_1 = Z_1 = 1$.

	3	4	5
$\mathbb{Q}$	$0.02s$	$176.8s$	∞
$\mathbb{F}_{65521}$	$0.01s$	$0.2s$	∞

Time to generate the symmetric system

	4	5	6	7	8
Magma	$0.0s$	$0.0s$	$0.06s$	$70.6s$	$7649.6s$
Maple	$0.0s$	$0.2s$	$0.9s$	$41.9s$	$2407.3s$

Time to solve the symmetric system (Magma)

	4	5	6	7
$\mathbb{Q}$	$0.02s$	$0.10s$	$297s$	$\infty \rightarrow 20mn\ (FGb)$
$\mathbb{F}_{65521}$	$0.00s$	$0.02s$	$3.9s$	$1681s \rightarrow 144s\ (FGb)$

SAGBI Bases and Polynomial Systems with Stable Equations.

Jean-Charles Faugère, Guënael Renault, J.S

Contributions

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

Groups with small number of Invariants: Invariant Theory

$\mathfrak{S}_n$

Subgroup of $\mathfrak{S}_n$: SAGBI Bases

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

$\mathfrak{S}_n$: Divided Differences

Groups with Reflections: Split the System

Abelian Groups

Contributions

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

Groups with small number of Invariants: Invariant Theory

$\mathfrak{S}_n$

All Groups

Subgroup of $\mathfrak{S}_n$: SAGBI Bases

Complexity

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

$\mathfrak{S}_n$: Divided Differences

Groups with Reflections: Split the System

Abelian Groups

Aim

- In this talk: $G \subset \mathfrak{S}_n$, $\quad \mathrm{char}(\mathbb{K}) \nmid |G|$.
- $f_1, \ldots, f_t \in \mathbb{K}[x_1, \ldots, x_n]^G$ generating I.
- Aim: Computing $V = \mathbb{V}(I)$ faster than with usual algorithms.

Aim

- In this talk: $G \subset \mathfrak{S}_n$, $\quad \mathrm{char}\,(\mathbb{K}) \nmid |G|$.
- $f_1, \ldots, f_t \in \mathbb{K}[x_1, \ldots, x_n]^G$ generating I.
- Aim: Computing $V = \mathbb{V}(I)$ faster than with usual algorithms.

Idea

Work in $R^G = \mathbb{K}[x_1, \ldots, x_n]^G$ instead of $R = \mathbb{K}[x_1, \ldots, x_n]$.
$I^G := \langle f_1, \ldots, f_t \rangle_{R^G}$

Use Structure to reduce the size of the matrices

$$\boxed{\text{System}} \xrightarrow{F_4 \text{ or } F_5} \boxed{\text{GB DRL}} \xrightarrow{\text{FGLM}} \boxed{\text{GB LEX}}$$

- Compute Macaulay Matrices
- Use Grading $R = \oplus_d R_d$

- Compute Multiplication matrices
- Use maps
$$\begin{array}{ccc} R/I & \to & R/I \\ f & \mapsto & NF(fx_i, \mathcal{G}_{\text{DRL}}) \end{array}$$

Use Structure to reduce the size of the matrices

$$\boxed{\text{System}} \xrightarrow{F_4 \text{ or } F_5} \boxed{\text{GB DRL}} \xrightarrow{\text{FGLM}} \boxed{\text{GB LEX}}$$

- Compute Macaulay Matrices
- Use Grading $R = \oplus_d R_d$

- Compute Multiplication matrices
- Use maps
$$\begin{array}{ccc} R/I & \to & R/I \\ f & \mapsto & NF(fx_i, \mathcal{G}_{\text{DRL}}) \end{array}$$

Ideal in R^G:

- $R^G = \oplus_d R_d^G$
- SAGBI-Normal Form.
- Smaller matrices !

Definition

Since char $(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|} \sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Reynolds Operator: $G \subset \mathfrak{S}_n$

Definition

Since $\operatorname{char}(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|}\sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Properties [Sturmfels08, Kemper & Steel98]

- $\{\Re(m) \mid m \text{ monomial of degree } d\}$ is a basis of R_d^G.

Reynolds Operator: $G \subset \mathfrak{S}_n$

Definition

Since $\operatorname{char}(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|} \sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Properties [Sturmfels08, Kemper & Steel98]

- $\{\Re(m) \mid m \text{ monomial of degree } d\}$ is a basis of R_d^G.
- $\dim R_d^G \simeq \dim R_d / |G|$

Reynolds Operator: $G \subset \mathfrak{S}_n$

Definition

Since $\operatorname{char}(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|} \sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Properties [Sturmfels08, Kemper & Steel98]

- $\{\Re(m) \mid m \text{ monomial of degree } d\}$ is a basis of R_d^G.
- $\dim R_d^G \simeq \dim R_d / |G|$

Reynolds Operator: $G \subset \mathfrak{S}_n$

Definition

Since $\mathrm{char}\,(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|} \sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Properties [Sturmfels08, Kemper & Steel98]

- $\{\Re(m) \mid m \text{ monomial of degree } d\}$ is a basis of R_d^G.
- $\dim R_d^G \simeq \dim R_d / |G|$

Cyclic-5, $\preceq$ = DRL-ordering

$$\begin{cases} f_1 = x_1 + x_2 + x_3 + x_4 + x_5 \\ f_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 \\ f_3 = x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 \\ f_4 = x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 \\ f_5 = x_1x_2x_3x_4x_5 - 1 \end{cases}$$

Reynolds Operator: $G \subset \mathfrak{S}_n$

Definition

Since $\mathrm{char}\,(\mathbb{K}) \nmid |G|$, $\Re(f) = \frac{1}{|G|}\sum_{A \in G} f^A$ defined a projection from $R_d = \mathbb{K}_d[x_1, \ldots, x_n]$ to $R_d^G = \mathbb{K}_d[x_1, \ldots, x_n]^G$ for each d.

Properties [Sturmfels08, Kemper & Steel98]

- $\{\Re(m) \mid m \text{ monomial of degree } d\}$ is a basis of R_d^G.
- $\dim R_d^G \simeq \dim R_d / |G|$

Cyclic-5, $\preceq$ = DRL-ordering

$$
\begin{cases}
f_1 = 5\Re(x_1) \\
f_2 = 5\Re(x_1 x_2) \\
f_3 = 5\Re(x_1 x_2 x_3) \\
f_4 = 5\Re(x_1 x_2 x_3 x_4) \\
f_5 = \Re(x_1 x_2 x_3 x_4 x_5) - \Re(1)
\end{cases}
$$

Very Compact Representation !

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

- $\mathcal{S}$ SAGBI-Gröbner Basis of I^G, ideal of $R^G = \mathbb{K}[x_1, \ldots, x_n]^G$ for $\preceq$, iff
$\forall f \in I^G \quad \exists\, g \in \mathcal{S}, h \in R^G \qquad \mathrm{LM}_{\preceq}(f) = \mathrm{LM}_{\preceq}(g)\mathrm{LM}_{\preceq}(h)$

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \dots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

- $\mathcal{S}$ SAGBI-Gröbner Basis of I^G, ideal of $R^G = \mathbb{K}[x_1, \dots, x_n]^G$ for $\preceq$, iff
  $\forall f \in I^G \quad \exists\, g \in \mathcal{S}, h \in R^G \qquad \mathrm{LM}_{\preceq}(f) = \mathrm{LM}_{\preceq}(g)\mathrm{LM}_{\preceq}(h)$

Reynolds Operator and SAGBI-Bases in R^G

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

- $\mathcal{S}$ SAGBI-Gröbner Basis of I^G, ideal of $R^G = \mathbb{K}[x_1, \ldots, x_n]^G$ for $\preceq$, iff
  $\forall f \in I^G \quad \exists\, g \in \mathcal{S}, h \in R^G \qquad \mathrm{LM}_{\preceq}(f) = \mathrm{LM}_{\preceq}(g)\mathrm{LM}_{\preceq}(h)$

Properties

- Notion of SAGBI-Top reduction.

Reynolds Operator and SAGBI-Bases in R^G

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

- $\mathcal{S}$ SAGBI-Gröbner Basis of I^G, ideal of $R^G = \mathbb{K}[x_1, \ldots, x_n]^G$ for $\preceq$, iff
  $\forall f \in I^G \quad \exists\, g \in \mathcal{S}, h \in R^G \qquad \mathrm{LM}_{\preceq}(f) = \mathrm{LM}_{\preceq}(g)\mathrm{LM}_{\preceq}(h)$

Properties

- Notion of SAGBI-Top reduction.
- $\rightsquigarrow$ SAGBI-Full reduction

Reynolds Operator and SAGBI-Bases in R^G

Definition

- $\mathcal{G}$ Gröbner Basis of I, ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$ for $\preceq$, iff

$$\forall f \in I \quad \exists\, g \in \mathcal{G} \qquad \mathrm{LM}_{\preceq}(g) | \mathrm{LM}_{\preceq}(f)$$

- $\mathcal{S}$ SAGBI-Gröbner Basis of I^G, ideal of $R^G = \mathbb{K}[x_1, \ldots, x_n]^G$ for $\preceq$, iff
  $\forall f \in I^G \quad \exists\, g \in \mathcal{S}, h \in R^G \qquad \mathrm{LM}_{\preceq}(f) = \mathrm{LM}_{\preceq}(g)\mathrm{LM}_{\preceq}(h)$

Properties

- Notion of SAGBI-Top reduction.
- $\rightsquigarrow$ SAGBI-Full reduction
- $\rightsquigarrow$ SAGBI-Normal Form.

Matrix F_5-algorithm

Equations : $f_1, \ldots, f_t$. f_i of degree d_i.

for $d = d_1$ to D do

  for $i = 1$ to t do

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

  end for

end for

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

$m_j^{d-d_i}$: 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 : $f_1, \ldots, f_t$. f_i of degree d_i in R^G.

for $d = d_1$ to D do
  for $i = 1$ to t do

$$\widetilde{M_{d,i}} = \text{Row-Echelon}\; \begin{array}{c} \\ \\ \Re(m_1^{d-d_i})f_i \\ \vdots \\ \Re(m_\ell^{d-d_i})f_i \end{array} \begin{array}{ccc} \Re(m_1^d) \succeq & \ldots & \succeq \Re(m_\mu^d) \end{array} \hspace{-12em} \left(\begin{array}{ccc} & \widetilde{M_{d,i-1}} & \\ \hline \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{array}\right)$$

  end for
end for

m_j^d: monomials of degree $\leq d$ such that $\{\Re(m_j^d)\}$ basis of R_d^G.
$m_j^{d-d_i}$: monomials of degree $\leq d - d_i$, such that $\{\Re(m_j^{d-d_i})\}$ basis of $R_{d-d_i}^G$, $\underbrace{\text{except those in } LM(\widetilde{M_{d-d_i,i-1}})}_{SAGBI-F_5\text{-criterion}}$.

Theorem : Dimension of ring of Invariants

$$\frac{\sum_{d=0}^{D} \dim R_d^G}{\sum_{d=0}^{D} \dim R_d} \underset{D \to +\infty}{\longrightarrow} \frac{1}{|G|}$$

Theoretical Complexity of SAGBI-F_5

$O\left(\frac{t}{|G|^{\omega}}\binom{D+n}{D}^{\omega}\right)$, to obtain a SAGBI basis up to degree D of $\langle f_1, \ldots, f_t \rangle_{R^G}$.

- SAGBI-F_5 allows us to compute a SAGBI-Gröbner basis of I^G up to some degree D.

Gröbner Basis in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$

- SAGBI-F_5 allows us to compute a SAGBI-Gröbner basis of I^G up to some degree D.
- ⚠ SAGBI Bases are not finite in general.

Gröbner Basis in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$

- SAGBI-F_5 allows us to compute a SAGBI-Gröbner basis of I^G up to some degree D.
- ⚠ SAGBI Bases are not finite in general.
- 💡 The symmetric functions $\sigma_i(x_1, \ldots, x_n)$ belong to R^G.

- SAGBI-F_5 allows us to compute a SAGBI-Gröbner basis of I^G up to some degree D.
- SAGBI Bases are not finite in general.
- The symmetric functions $\sigma_i(x_1, \ldots, x_n)$ belong to R^G.
- Use the SAGBI Basis up to degree D to compute SAGBI-Normal Forms of symmetric polynomials in $K[x_1, \ldots, x_n]^{\mathfrak{S}_n} = \mathbb{K}[\sigma_1, \ldots, \sigma_n]$ of degree less than D with respect to I^G, and look for a Gröbner basis.

General Strategy

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathrm{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

General Strategy

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathrm{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

$$\boxed{\begin{array}{c} I = \langle f_1, \ldots, f_t \rangle \\ D = \min \{\deg(f_i)\} \end{array}}$$

General Strategy

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$

$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$

$\preceq_{\mathsf{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

$$\boxed{\begin{array}{c} I = \langle f_1, \ldots, f_t \rangle \\ D = \min\{\deg(f_i)\} \end{array}} \xrightarrow{\text{SAGBI-}F_5} \boxed{\begin{array}{c} \text{SAGBI Gröbner basis up to} \\ \text{degree } D \text{ of } I^G \text{ in } R^G \text{ for } \preceq \end{array}}$$

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathsf{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

$I = \langle f_1, \ldots, f_t \rangle$
$D = \min\{\deg(f_i)\}$

$\xrightarrow{\text{SAGBI-}F_5}$

SAGBI Gröbner basis up to degree D of I^G in R^G for $\preceq$

$\downarrow$ SAGBI-FGLM

The elements of degree at most D of a Gröbner Basis for $\preceq_w$ of $(\langle f_1, \ldots, f_t \rangle + (e_i - \sigma_i)) \cap \mathbb{K}[e_1, \ldots, e_n]$

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathrm{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

$I = \langle f_1, \ldots, f_t \rangle$
$D = \min \{\deg(f_i)\}$

SAGBI-F_5 $\longrightarrow$

SAGBI Gröbner basis up to degree D of I^G in R^G for $\preceq$

$\downarrow$ SAGBI-FGLM

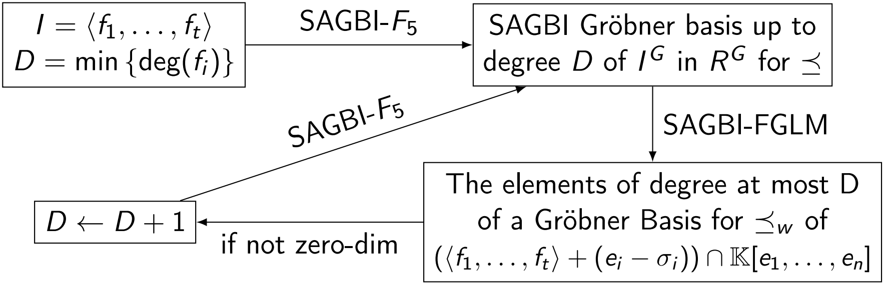
The elements of degree at most D of a Gröbner Basis for $\preceq_w$ of $(\langle f_1, \ldots, f_t \rangle + (e_i - \sigma_i)) \cap \mathbb{K}[e_1, \ldots, e_n]$

$\longleftarrow$ if not zero-dim

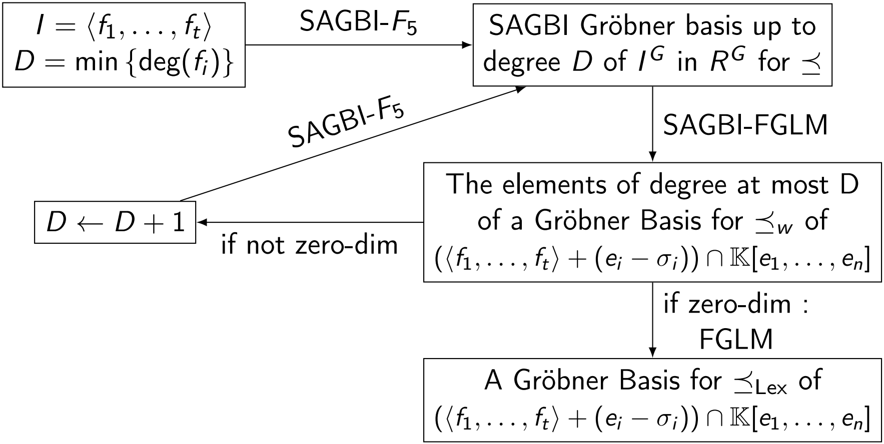
$D \leftarrow D + 1$

General Strategy

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathsf{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.

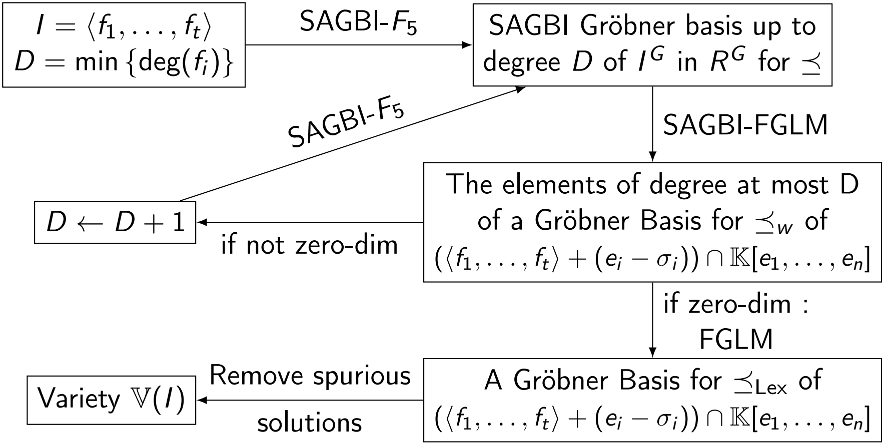


$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathrm{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.



General Strategy

$\preceq$=DRL ordering in $R = \mathbb{K}[x_1, \ldots, x_n]$
$\preceq_w$= weighted DRL ordering in $\mathbb{K}[e_1, \ldots, e_n]$
$\preceq_{\mathrm{Lex}}$= Lexicographic ordering in $\mathbb{K}[e_1, \ldots, e_n]$.



Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1 x_2) \\ f_3 = 5\Re(x_1 x_2 x_3) \\ f_4 = 5\Re(x_1 x_2 x_3 x_4) \\ f_5 = \Re(x_1 x_2 x_3 x_4 x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i = i-$th symmetric function in $(x_1, \ldots, x_5)$.

Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1x_2) \\ f_3 = 5\Re(x_1x_2x_3) \\ f_4 = 5\Re(x_1x_2x_3x_4) \\ f_5 = \Re(x_1x_2x_3x_4x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i = i-$th symmetric function in $(x_1, \ldots, x_5)$.
- SAGBI Basis in Degree 8 for DRL ordering : 99 polynomials.

Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1x_2) \\ f_3 = 5\Re(x_1x_2x_3) \\ f_4 = 5\Re(x_1x_2x_3x_4) \\ f_5 = \Re(x_1x_2x_3x_4x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i \ = \ i-$th symmetric function in $(x_1, \ldots, x_5)$.
- SAGBI Basis in Degree 8 for DRL ordering : 99 polynomials.
- w-DRL $\mathfrak{S}_n$-Gröbner Basis:
  ${e_2}^3 + 5\, {e_3}^2$, ${e_2}^2 e_3 - 25\, e_2$, $e_2\, {e_3}^2 - 25\, e_3$, ${e_3}^3 + 5\, {e_2}^2$, e_1, e_4, $e_5 - 1$

Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1x_2) \\ f_3 = 5\Re(x_1x_2x_3) \\ f_4 = 5\Re(x_1x_2x_3x_4) \\ f_5 = \Re(x_1x_2x_3x_4x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i = i-$th symmetric function in $(x_1, \ldots, x_5)$.
- SAGBI Basis in Degree 8 for DRL ordering : 99 polynomials.
- w-DRL $\mathfrak{S}_n$-Gröbner Basis:
  $e_2{}^3 + 5\,e_3{}^2,\ e_2{}^2 e_3 - 25\,e_2,\ e_2\,e_3{}^2 - 25\,e_3,\ e_3{}^3 + 5\,e_2{}^2,\ e_1,\ e_4,\ e_5 - 1$
- Lex $\mathfrak{S}_n$-Gröbner Basis:
  $e_5 - 1, e_4, e_3(e_3^5 + 5^5)\,e_3, 125e_2 + e_3^4, e_1$

Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1x_2) \\ f_3 = 5\Re(x_1x_2x_3) \\ f_4 = 5\Re(x_1x_2x_3x_4) \\ f_5 = \Re(x_1x_2x_3x_4x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i = i-$th symmetric function in $(x_1, \ldots, x_5)$.
- SAGBI Basis in Degree 8 for DRL ordering : 99 polynomials.
- w-DRL $\mathfrak{S}_n$-Gröbner Basis:
  $e_2{}^3 + 5\, e_3{}^2,\, e_2{}^2 e_3 - 25\, e_2,\, e_2\, e_3{}^2 - 25\, e_3,\, e_3{}^3 + 5\, e_2{}^2,\, e_1,\, e_4,\, e_5 - 1$
- Lex $\mathfrak{S}_n$-Gröbner Basis:
  $e_5 - 1, e_4, e_3(e_3^5 + 5^5)\, e_3, 125 e_2 + e_3^4, e_1$
- 6 solutions in $(e_i)_i \rightsquigarrow$ at most $6 \times 5! = 720$ solutions in $\mathbb{V}(I)$

Example: Cyclic-5 Problem

$$\begin{cases} f_1 = 5\Re(x_1) \\ f_2 = 5\Re(x_1 x_2) \\ f_3 = 5\Re(x_1 x_2 x_3) \\ f_4 = 5\Re(x_1 x_2 x_3 x_4) \\ f_5 = \Re(x_1 x_2 x_3 x_4 x_5) - \Re(1) \end{cases}$$

- $G = C_5 \subset \mathfrak{S}_5$, $e_i = i-$th symmetric function in $(x_1, \ldots, x_5)$.
- SAGBI Basis in Degree 8 for DRL ordering : 99 polynomials.
- w-DRL $\mathfrak{S}_n$-Gröbner Basis:
  ${e_2}^3 + 5\,{e_3}^2,\ {e_2}^2 e_3 - 25\,e_2,\ e_2\,{e_3}^2 - 25\,e_3,\ {e_3}^3 + 5\,{e_2}^2,\ e_1,\ e_4,\ e_5 - 1$
- Lex $\mathfrak{S}_n$-Gröbner Basis:
  $e_5 - 1, e_4, e_3(e_3^5 + 5^5)\, e_3, 125 e_2 + e_3^4, e_1$
- 6 solutions in $(e_i)_i \rightsquigarrow$ at most $6 \times 5! = 720$ solutions in $\mathbb{V}(I)$
- Removing spurious solutions: Only 70 solutions !

Extensions

- This approach can be used with any Group.

Extensions

- This approach can be used with any Group.
- Both Modular and Non-modular Cases.

Extensions

- This approach can be used with any Group.
- Both Modular and Non-modular Cases.
- Can be generalized to other algebras.

Gröbner Bases of ideals invariant under a commutative group : the non-modular case.

Jean-Charles Faugère, J.S.

ISSAC 2013

Contributions

Local

Stable Equations
$\forall A \in G \quad f_i^A = f_i$

$\Longrightarrow$

Global

Stable Ideal
$f \in I, A \in G \Rightarrow f^A \in I$

Groups with small number of Invariants: Invariant Theory $\rightarrow$ $\mathfrak{S}_n$

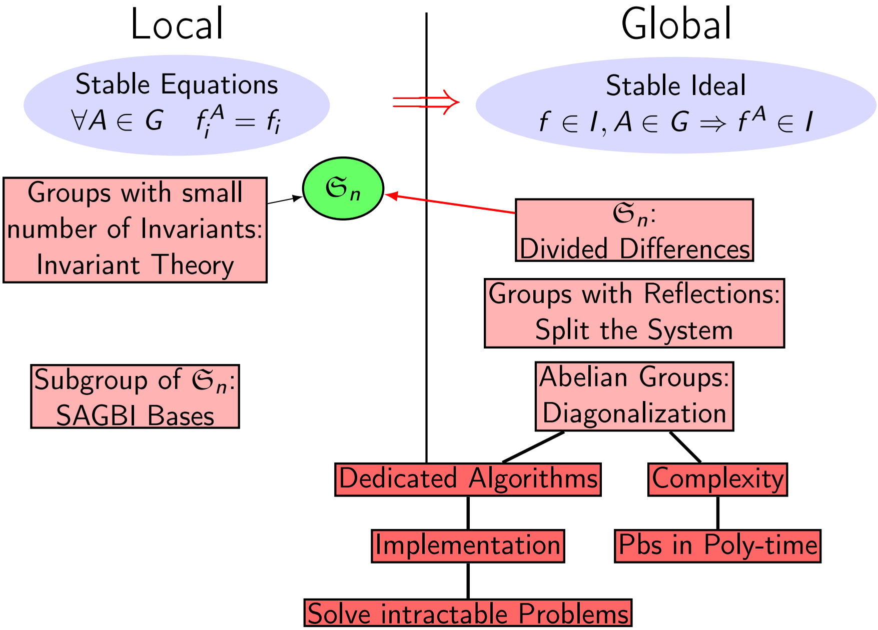
$\mathfrak{S}_n$: Divided Differences $\rightarrow$ $\mathfrak{S}_n$

Groups with Reflections: Split the System

Subgroup of $\mathfrak{S}_n$: SAGBI Bases

Abelian Groups: Diagonalization

Contributions



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

$G = \langle M_1, M_2\rangle$ 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, $f_1^{M_2} = f_1$.
f_2 =Random polynomial of degree 3, $f_2^{M_1} = f_2$.

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-stable ideal.

G finite abelian subgroup of $GL_n(\mathbb{K})$, $\mathrm{char}(\mathbb{K}) \nmid |G|$, I a G-stable ideal.

G finite abelian subgroup of $GL_n(\mathbb{K})$, $\mathrm{char}(\mathbb{K}) \nmid |G|$, 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 $\mathbb{K}$.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(\mathbb{K})$, char$(\mathbb{K}) \nmid |G|$, 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 $\mathbb{K}$.
- G abelian $\rightsquigarrow$ Same base-change matrix P.

G finite abelian subgroup of $GL_n(\mathbb{K})$, $\mathrm{char}(\mathbb{K}) \nmid |G|$, 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 $\mathbb{K}$.
- G abelian $\rightsquigarrow$ Same base-change matrix P.
- $G_{\mathcal{D}} = \{P^{-1}AP \mid A \in G\}$: group of diagonal matrices.

Reducing the problem to the case of diagonal groups

G finite abelian subgroup of $GL_n(\mathbb{K})$, $\mathrm{char}(\mathbb{K}) \nmid |G|$, 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 $\mathbb{K}$.
- G abelian $\rightsquigarrow$ Same base-change matrix P.
- $G_{\mathcal{D}} = \{P^{-1}AP \mid A \in G\}$: group of diagonal matrices.
- $I_{\mathcal{D}} = \{f^P \mid f \in I\}$ is $G_{\mathcal{D}}$-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

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

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

Remember

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

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

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

And Now

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

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

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

Action of $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Action of $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\dots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $\mathbb{Z}/q_2\mathbb{Z}$.

Action of $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $\lambda_i \in \mathbb{Z}/q_1\mathbb{Z}$.

Action of $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $G_{\mathcal{D}}$ on Monomials.

Theorem: Structure of Finite Abelian Groups

Evey Abelian Group $\simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|q_2|\ldots|q_\ell$.

Notations

- $G_{\mathcal{D}}$ 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 $D_2 \quad \rightsquigarrow \langle D_2\rangle$-degree.
- $(g_1, g_2) \in \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$ is called the $G_{\mathcal{D}}$-degree of m.

Remember

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

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

$G_{\mathcal{D}}$-homogeneous components

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

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

$G_{\mathcal{D}}$-homogeneous components

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

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

Sums of Terms of same $G_{\mathcal{D}}$-degree are called $G_{\mathcal{D}}$-homogeneous components.

$G_{\mathcal{D}}$-homogeneous components

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

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

Sums of Terms of same $G_{\mathcal{D}}$-degree are called $G_{\mathcal{D}}$-homogeneous components.

Theorem

If $I_{\mathcal{D}}$ is $G_{\mathcal{D}}$-stable and $f \in I_{\mathcal{D}}$, the $G_{\mathcal{D}}$-homogeneous components of f belong to $I_{\mathcal{D}}$.

Extract $G_{\mathcal{D}}$-homogeneous components

$$I_{\mathcal{D}} = \langle h_1, \dots, h_6 \rangle, \text{ with:}$$

$h_1 = x_1x_2 + 12x_1x_6 + 8x_1$ of $G_{\mathcal{D}}$-degree $(1,0)$.

$h_2 = x_1^2 + 2x_4^2 + 12x_3x_5 + 5x_2x_6 + 14x_6^2 + 2x_2 + 5x_6 + 4$ of $G_{\mathcal{D}}$-degree $(0,0)$.

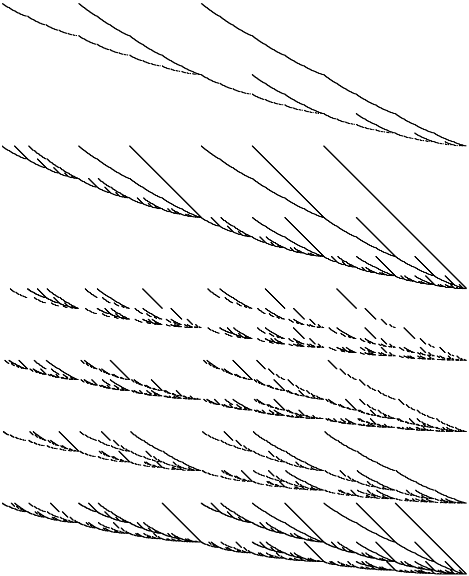
$h_3 = x_2x_3x_4 + 13x_1^2x_5 + 11x_2^2x_5 + 4x_4^2x_5 + 8x_3x_5^2 + 9x_3x_4x_6 + 7x_2x_5x_6 + 7x_5x_6^2 + 8x_3x_4 + 9x_2x_5 + x_5x_6 + 9x_5$ of $G_{\mathcal{D}}$-degree $(0,3)$.

$h_4 = x_2x_3^2 + 14x_1^2x_4 + 3x_2^2x_4 + 5x_4^3 + 10x_3x_4x_5 + x_2x_5^2 + 11x_3^2x_6 + 14x_2x_4x_6 + 7x_5^2x_6 + 2x_3^2 + 12x_2x_4 + 9x_5^2 + 16x_4x_6 + 9x_4$ of $G_{\mathcal{D}}$-degree $(0,2)$.

$h_5 = x_1^2x_3 + x_2^2x_3 + 15x_3^2x_5 + 13x_2x_4x_5 + 13x_5^3 + x_2x_3x_6 + 4x_4x_5x_6 + 15x_3x_6^2 + 10x_2x_3 + 12x_4x_5 + 9x_3x_6 + 5x_3$ of $G_{\mathcal{D}}$-degree $(0,1)$.

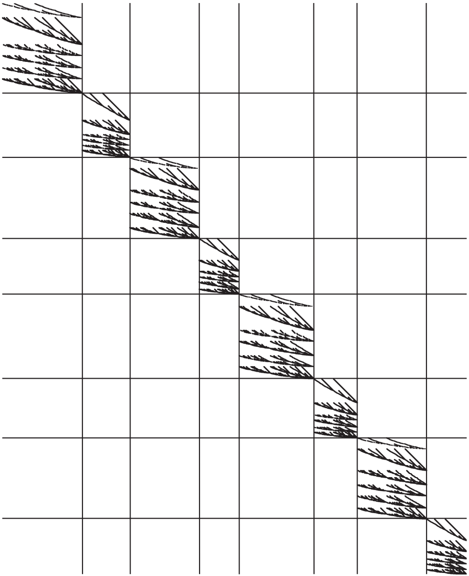
$h_6 = x_1^2x_2 + 7x_2^3 + 4x_3^2x_4 + 9x_2x_4^2 + 2x_2x_3x_5 + 7x_4x_5^2 + 9x_1^2x_6 + 15x_2^2x_6 + 9x_4^2x_6 + 12x_3x_5x_6 + 5x_6^3 + 4x_1^2 + 13x_2^2 + 5x_4^2 + 15x_3x_5 + 13x_2x_6 + 16x_6^2 + 16x_2 + 13x_6 + 3$ of $G_{\mathcal{D}}$-degree $(0,0)$.

Macaulay's matrix in degree 8 of $h_1, h_2, h_3, h_4, h_5, h_6$



Size 3696×3003

Same matrix, row and columns sorted by $G_{\mathcal{D}}$-degrees first



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

Product of two monomials

For all monomials m and m',
$\deg_{G_{\mathcal{D}}}(mm') = \deg_{G_{\mathcal{D}}}(m) + \deg_{G_{\mathcal{D}}}(m')$.

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

Product of two monomials

For all monomials m and m',
$\deg_{G_{\mathcal{D}}}(mm') = \deg_{G_{\mathcal{D}}}(m) + \deg_{G_{\mathcal{D}}}(m')$.

Grading

$R = \oplus_{g \in G_{\mathcal{D}}} R_g = \oplus_{d \in \mathbb{N}, g \in G_{\mathcal{D}}} R_{d,g}$

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

Product of two monomials

For all monomials m and m',
$\deg_{G_{\mathcal{D}}}(mm') = \deg_{G_{\mathcal{D}}}(m) + \deg_{G_{\mathcal{D}}}(m')$.

Grading

$R = \oplus_{g \in G_{\mathcal{D}}} R_g = \oplus_{d \in \mathbb{N}, g \in G_{\mathcal{D}}} R_{d,g}$

S-polynomials of G-homogeneous polynomials

$S(f,h) = \frac{LM(f) \vee LM(h)}{LM(f)} f - \frac{LM(f) \vee LM(h)}{LM(h)} \frac{LC(f)}{LC(h)} h$ is $G_{\mathcal{D}}$-homogeneous if f and h are.

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

Product of two monomials

For all monomials m and m',
$\deg_{G_{\mathcal{D}}}(mm') = \deg_{G_{\mathcal{D}}}(m) + \deg_{G_{\mathcal{D}}}(m')$.

Grading

$R = \oplus_{g \in G_{\mathcal{D}}} R_g = \oplus_{d \in \mathbb{N}, g \in G_{\mathcal{D}}} R_{d,g}$

S-polynomials of G-homogeneous polynomials

$S(f,h) = \frac{LM(f) \vee LM(h)}{LM(f)} f - \frac{LM(f) \vee LM(h)}{LM(h)} \frac{LC(f)}{LC(h)} h$ is $G_{\mathcal{D}}$-homogeneous if f and h are.

Computation

Any Gröbner basis algorithm preserves the $G_{\mathcal{D}}$-homogeneity !
$\rightsquigarrow$ Application to F_5.

- $I_{\mathcal{D}}$ a $G_{\mathcal{D}}$-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of $I_{\mathcal{D}}$ for $\preceq_1$.

- $I_{\mathcal{D}}$ a $G_{\mathcal{D}}$-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of $I_{\mathcal{D}}$ for $\preceq_1$.

$\mathcal{E}$: Basis of R/I given by monomials not reducible by $\mathcal{G}_{\preceq_1}$.

- $I_{\mathcal{D}}$ a $G_{\mathcal{D}}$-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of $I_{\mathcal{D}}$ for $\preceq_1$.

$\mathcal{E}$: Basis of R/I given by monomials not reducible by $\mathcal{G}_{\preceq_1}$.

FGLM computes matrices of the maps:

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

- $I_{\mathcal{D}}$ a $G_{\mathcal{D}}$-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of $I_{\mathcal{D}}$ for $\preceq_1$.

$\mathcal{E}$: Basis of R/I given by monomials not reducible by $\mathcal{G}_{\preceq_1}$.
FGLM computes matrices of the maps:

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

Normal-Form preserves the $G_{\mathcal{D}}$-homogeneity

$$deg_{G_{\mathcal{D}}}(NF(mx_i, \mathcal{G}_{\preceq_1})) = deg_{G_{\mathcal{D}}}(mx_i) = deg_{G_{\mathcal{D}}}(m) + deg_{G_{\mathcal{D}}}(x_i)$$

- $I_{\mathcal{D}}$ a $G_{\mathcal{D}}$-stable zero-dimensional ideal.
- $\mathcal{G}_{\preceq_1}$: Gröbner basis of $I_{\mathcal{D}}$ for $\preceq_1$.

$\mathcal{E}$: Basis of R/I given by monomials not reducible by $\mathcal{G}_{\preceq_1}$.
Abelian-FGLM computes matrices of the maps:

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

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

Normal-Form preserves the $G_{\mathcal{D}}$-homogeneity

$deg_{G_{\mathcal{D}}}(NF(mx_i, \mathcal{G}_{\preceq_1})) = deg_{G_{\mathcal{D}}}(mx_i) = deg_{G_{\mathcal{D}}}(m) + deg_{G_{\mathcal{D}}}(x_i)$

Continuation of the example

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

- $I_{\mathcal{D}} = \langle h_1, h_2, h_3, h_4, h_5, h_6 \rangle$ is zero-dimensional of degree 308.

Continuation of the example

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

- $I_{\mathcal{D}} = \langle h_1, h_2, h_3, h_4, h_5, h_6 \rangle$ 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

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

- $I_{\mathcal{D}} = \langle h_1, h_2, h_3, h_4, h_5, h_6 \rangle$ 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 $|\mathcal{E}_g| \times |\mathcal{E}_{g+deg_{G_{\mathcal{D}}}(x_i)}|$.

Continuation of the example

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

- $I_{\mathcal{D}} = \langle h_1, h_2, h_3, h_4, h_5, h_6 \rangle$ 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 $|\mathcal{E}_g| \times |\mathcal{E}_{g+deg_{G_{\mathcal{D}}}(x_i)}|$.
- 83402 coefficients instead of 569184.

Reminder : Repartition of the monomials

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

Reminder : Repartition of the monomials

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

Theoretical speed-up

Matrices have number of rows and columns divided by $\simeq |G_{\mathcal{D}}| \rightsquigarrow$ Gain of $|G_{\mathcal{D}}|^{\omega}$ in F_5 and $|G_{\mathcal{D}}|^2$ in FGLM compared to classical algorithms.

Complexity Questions

Reminder : Repartition of the monomials

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

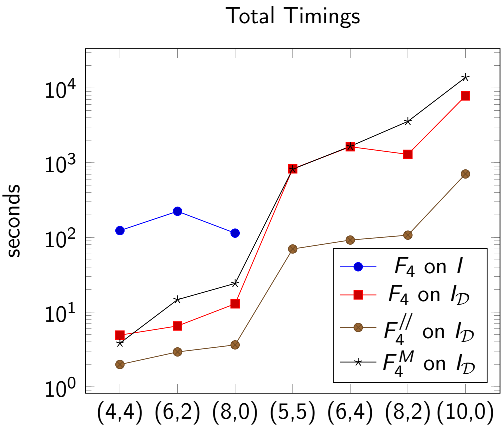
Theoretical speed-up

Matrices have number of rows and columns divided by $\simeq |G_{\mathcal{D}}| \rightsquigarrow$ Gain of $|G_{\mathcal{D}}|^{\omega}$ in F_5 and $|G_{\mathcal{D}}|^2$ in FGLM compared to classical algorithms.

In practice

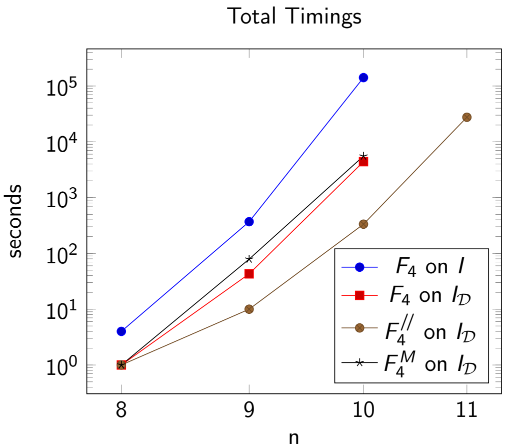
- Abelian-F_4 has been implemented in C and Abelian-FGLM in Magma.
- In Practice, Cyclic-9 Problem with Abelian-F_4: 9 Matrices of sizes $8073 \pm 3.4\% \times 10435 \pm 2.6\%$ instead of one matrix of size 72558×93917.

Some Timings with Abelian-F_4



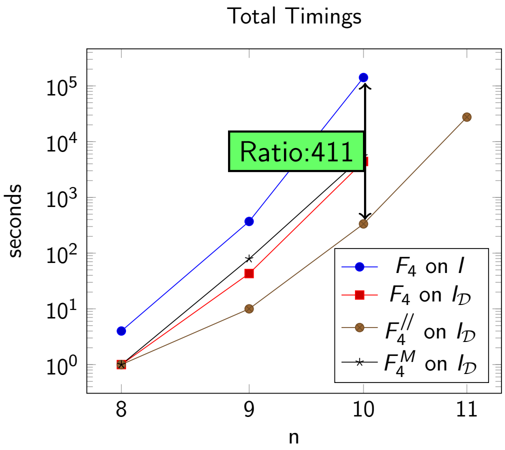
$n = k_1 + k_2$ cubic equations invariant under $C_{k_1} \times C_{k_2}$

Cyclic-n Timings



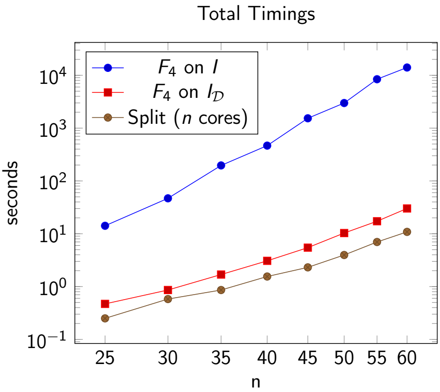
The Cyclic-n Problem

Cyclic-n Timings

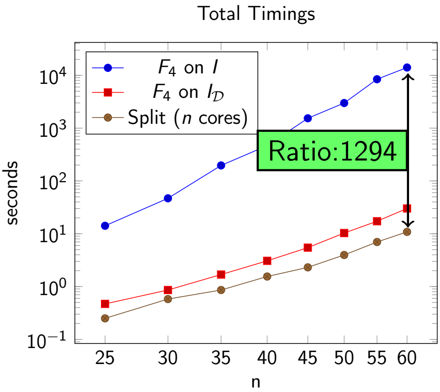


The Cyclic-n Problem

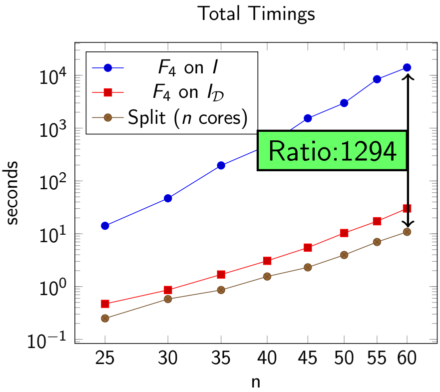
Quadratic Equations of $G_{\mathcal{D}}$-degrees 0 and 1.

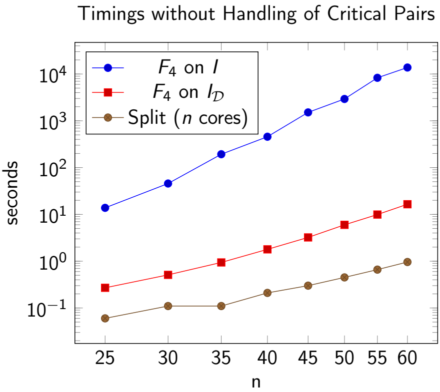


Quadratic Equations of $G_{\mathcal{D}}$-degrees 0 and 1.

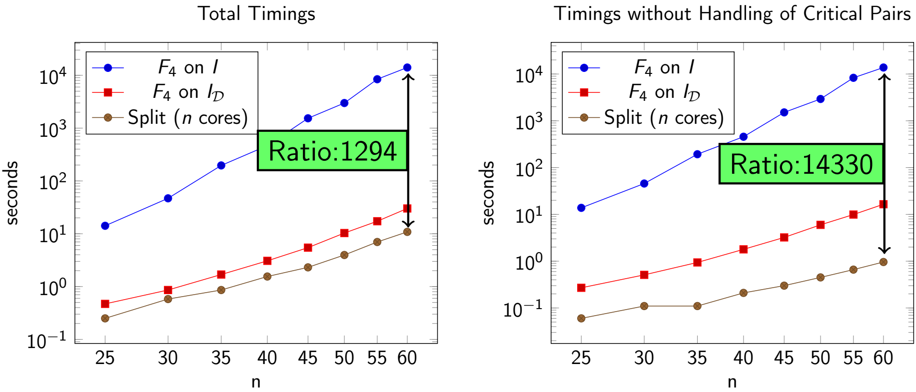


Quadratic Equations of $G_{\mathcal{D}}$-degrees 0 and 1.

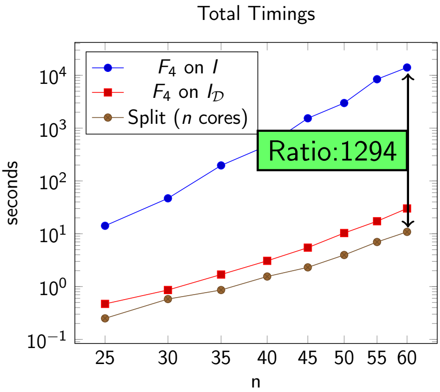


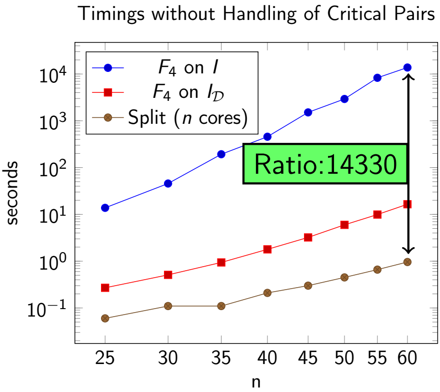


Quadratic Equations of $G_{\mathcal{D}}$-degrees 0 and 1.



Quadratic Equations of $G_{\mathcal{D}}$-degrees 0 and 1.





Theorem

$G_{\mathcal{D}}$-invariant ideals generated by quadratic equations with a fixed number of distincts $G_{\mathcal{D}}$-degrees invariant under the Cyclic group of order n can be solved in polynomial-time.

NTRU 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 $\{0, 1\}$.

Cryptography: NTRU Timings

NTRU 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 $\{0, 1\}$.

Equations

- The coefficients of $(f\,h \bmod x^n - 1)$ are linear forms in the variables f_j, given by $\ell_i = \sum_{j=0}^{n-1} f_j h_{[(i-j) \bmod n]}$.

NTRU 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 $\{0, 1\}$.

Equations

- The coefficients of $(f\, h \bmod x^n - 1)$ are linear forms in the variables f_j, given by $\ell_i = \sum_{j=0}^{n-1} f_j h_{[(i-j) \bmod n]}$.
- With $\sigma = (0\ 1\ 2\ \ldots n-1)$ acting on $(f_0, \ldots, f_{n-1})$, we have $\ell_i^\sigma = \ell_{\sigma(i)}$

Cryptography: NTRU Timings

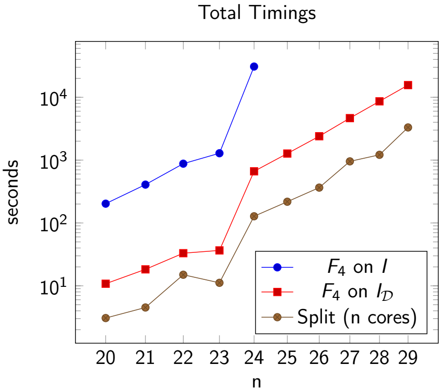
NTRU Basic Underlying Problem [Silvermann&al.96]

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 $\{0, 1\}$.

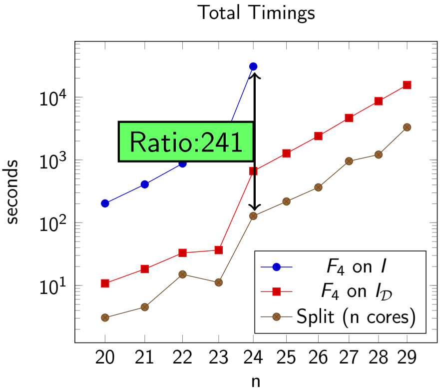
Equations

- The coefficients of $(f\ h \bmod x^n - 1)$ are linear forms in the variables f_j, given by $\ell_i = \sum_{j=0}^{n-1} f_j h_{[(i-j) \bmod n]}$.
- With $\sigma = (0\ 1\ 2\ \ldots n-1)$ acting on $(f_0, \ldots, f_{n-1})$, we have $\ell_i^\sigma = \ell_{\sigma(i)}$
- $\{f_i^2 - f_i\} \cup \{\ell_i^2 - \ell_i\}$ form a system of $2n$ equations globally stable under σ.

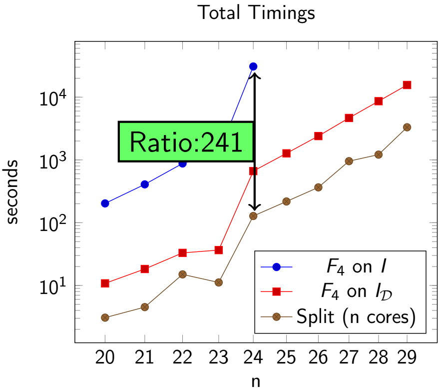
Cryptography: NTRU Timings

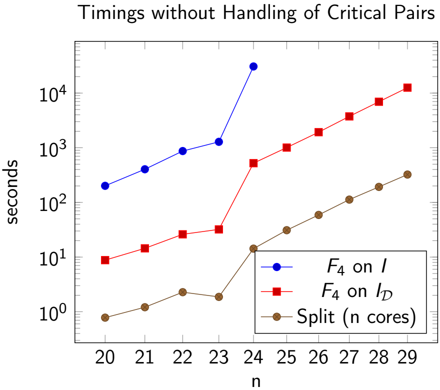


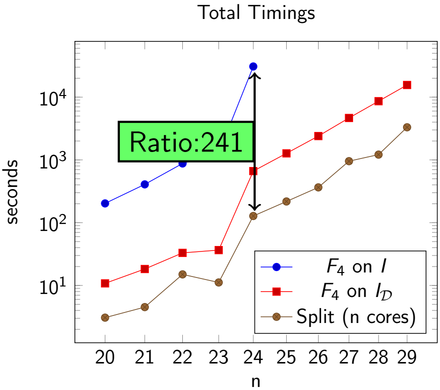
Cryptography: NTRU Timings

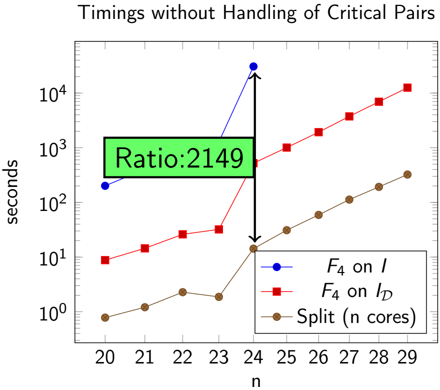


Cryptography: NTRU Timings






Total Timings
Ratio:241
seconds
10^1
10^2
10^3
10^4
20 21 22 23 24 25 26 27 28 29
n
F_4 on I
F_4 on $I_{\mathcal{D}}$
Split (n cores)


Timings without Handling of Critical Pairs
Ratio:2149
seconds
10^0
10^1
10^2
10^3
10^4
20 21 22 23 24 25 26 27 28 29
n
F_4 on I
F_4 on $I_{\mathcal{D}}$
Split (n cores)

Perspectives

- Better speed-up in FGLM ?

Perspectives

- Better speed-up in FGLM ?
- Take the sparsity of the system after change of variables into account. $\rightsquigarrow$ Work in progress !

Perspectives

- Better speed-up in FGLM ?
- Take the sparsity of the system after change of variables into account. $\rightsquigarrow$ Work in progress !
- Extension to other groups (Representation Theory ?) ?

Thank you for your attention !