Polynomial system solving with Gröbner bases and applications

26 reasons not to be scared

Mohab Safey El Din[1]

[1]Sorbonne University, CNRS

Solving polynomial equations exactly

Let $\mathbb{K}$ be a field (e.g. $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \frac{Z}{p\mathbb{Z}}$ with p prime or $\mathbb{K} = \mathbb{F}_q$, $q = p^k$).

$$\boxed{f_1 = \cdots = f_s = 0, \text{ with } f_i \in \mathbb{K}[x_1, \ldots, x_n], \text{ no restriction on } s}$$

Meaning of solving depends on $\mathbb{K}$ and geometric properties:

- $\mathbb{K} = \mathbb{Q}$, solutions in $\mathbb{Q}^n \rightsquigarrow$ undecidable
  solutions in $\mathbb{R}^n, \mathbb{C}^n \rightsquigarrow$ decidable
  how many? Enumerate them? Dimension?
- $\mathbb{K}$ is finite, solutions in $\mathbb{K}^n$? one can enumerate them

Exact methods. Compute an algebraic data-structure which

- determines the dimension of the solution set in $\overline{\mathbb{K}}^n$;
- can be exploited to extract global information on solutions (solutions in $\mathbb{K}^n$ when $\mathbb{K}$ is finite, otherwise solutions in $\mathbb{R}, \mathbb{C}$);
- comes with guarantees.

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$$f_1 = x_1 + x_2 - 1$$
$$f_2 = x_1 - x_2 + 1$$

This is **not** a
Gröbner basis

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$$f_1 = x_1 + x_2 - 1$$
$$f_2 = x_1 - x_2 + 1$$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1} + x_2 - 1$$
$$f_2 = \boxed{x_1} - x_2 + 1$$
$$\boxed{f_1 - f_2} = 2x_2 - 2$$

This is a Gröbner basis

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$f_1 = x_1 + x_2 - 1$
$f_2 = x_1 - x_2 + 1$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$
$f_2 = \boxed{x_1} - x_2 + 1$
$\boxed{f_1 - f_2} = 2x_2 - 2$

This is a Gröbner basis

- ☛ Ordering on the variables
- ☛ Vector space of linear equations
- ☛ triangular rewriting (eliminating monomials)

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$$f_1 = x_1 + x_2 - 1$$
$$f_2 = x_1 - x_2 + 1$$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1} + x_2 - 1$$
$$f_2 = \boxed{x_1} - x_2 + 1$$
$$\boxed{f_1 - f_2} = 2x_2 - 2$$

This is a Gröbner basis

- ☛ Ordering on the variables
- ☛ Vector space of linear equations
- ☛ triangular rewriting (eliminating monomials)

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1^2} + x_2^2 - 1$$
$$f_2 = \boxed{x_1^2} - x_2^2 + 1$$

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$f_1 = x_1 + x_2 - 1$

$f_2 = x_1 - x_2 + 1$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1} + x_2 - 1$

$f_2 = \boxed{x_1} - x_2 + 1$

$\boxed{f_1 - f_2} = 2x_2 - 2$

This is a Gröbner basis

☛ Ordering on the variables

☛ Vector space of linear equations

☛ triangular rewriting (eliminating monomials)

Picking $x_1 \succ x_2$

$f_1 = \boxed{x_1^2} + x_2^2 - 1$

$f_2 = \boxed{x_1^2} - x_2^2 + 1$

$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$

$\boxed{f_1 - \frac{1}{2}g} = x_1^2$

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$$f_1 = x_1 + x_2 - 1$$
$$f_2 = x_1 - x_2 + 1$$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1} + x_2 - 1$$
$$f_2 = \boxed{x_1} - x_2 + 1$$
$$\boxed{f_1 - f_2} = 2x_2 - 2$$

This is a Gröbner basis

- ☛ Ordering on the variables
- ☛ Vector space of linear equations
- ☛ triangular rewriting (eliminating monomials)

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1^2} + x_2^2 - 1$$
$$f_2 = \boxed{x_1^2} - x_2^2 + 1$$
$$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$$
$$\boxed{f_1 - \tfrac{1}{2}g} = x_1^2$$

What about?

$$f_1 = x_1^2 + x_2^2 + x_1x_2 - 1$$
$$f_2 = x_1^2 - x_2^2 - 2x_1x_2 + 1$$
$$f_1 - f_2 = 2x_2^2 + 2x_1x_2 - 2$$

What is a Gröbner basis?

Gröbner basis $\rightsquigarrow$ convenient rewriting of $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$

$$f_1 = x_1 + x_2 - 1$$
$$f_2 = x_1 - x_2 + 1$$

This is **not** a Gröbner basis

Picking $x_1 \succ x_2$

$$f_1 = \boxed{x_1} + x_2 - 1$$
$$f_2 = \boxed{x_1} - x_2 + 1$$
$$\boxed{f_1 - f_2} = 2x_2 - 2$$

This is a Gröbner basis

- ☛ Ordering on the variables
- ☛ Vector space of linear equations
- ☛ triangular rewriting (eliminating monomials)

Picking $x_1 \succ x_2$

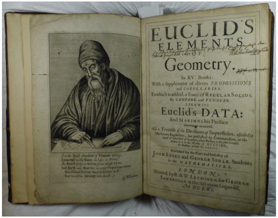
$$f_1 = \boxed{x_1^2} + x_2^2 - 1$$
$$f_2 = \boxed{x_1^2} - x_2^2 + 1$$
$$\boxed{g = f_1 - f_2} = 2x_2^2 - 2$$
$$\boxed{f_1 - \tfrac{1}{2}g} = x_1^2$$

What about?

$$f_1 = x_1^2 + x_2^2 + x_1x_2 - 1$$
$$f_2 = x_1^2 - x_2^2 - 2x_1x_2 + 1$$
$$f_1 - f_2 = 2x_2^2 + 2x_1x_2 - 2$$

- ☛ Monomial orderings
- ☛ Vector spaces are no more sufficient
- ☛ Ideals generated by polynomials

From Euclid's algorithm to Buchberger's algorithm



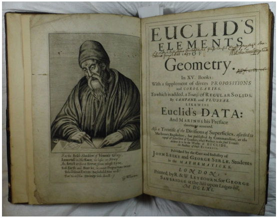
$\mathbb{K}[x] \rightsquigarrow$ Monomial ordering induced by $\mathbb{N}$

$g_1 = x^a + \cdots \qquad g_2 = x^b + \cdots \qquad$ with $a \geq b$

$S = 1 \times g_1 - x^{a-b} g_2 \in \langle g_1, g_2 \rangle$

$S = 0?$, $\mathrm{lm}(S) \notin \langle \mathrm{lm}(g_2) \rangle? \qquad \rightsquigarrow$ repeat

From Euclid's algorithm to Buchberger's algorithm



$\mathbb{K}[x] \rightsquigarrow$ Monomial ordering induced by $\mathbb{N}$

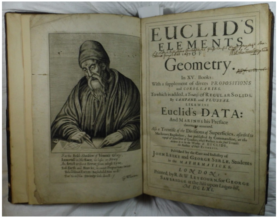
$g_1 = x^a + \cdots \qquad g_2 = x^b + \cdots \qquad$ with $a \geq b$

$S = 1 \times g_1 - x^{a-b} g_2 \in \langle g_1, g_2 \rangle$

$S = 0?$, $\mathrm{lm}(S) \notin \langle \mathrm{lm}(g_2) \rangle?$ $\qquad \rightsquigarrow$ repeat

$\mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ Admissible monomial orderings over $\mathbb{N}^n$

From Euclid's algorithm to Buchberger's algorithm



$\mathbb{K}[x] \rightsquigarrow$ Monomial ordering induced by $\mathbb{N}$

$g_1 = x^a + \cdots \qquad g_2 = x^b + \cdots \qquad$ with $a \geq b$

$S = 1 \times g_1 - x^{a-b} g_2 \in \langle g_1, g_2 \rangle$

$S = 0?$, $\operatorname{lm}(S) \notin \langle \operatorname{lm}(g_2) \rangle$? $\rightsquigarrow$ repeat

$\mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ Admissible monomial orderings over $\mathbb{N}^n$

$g_1 = \boldsymbol{x}^{\boldsymbol{\alpha}_{1,1}} + \cdots, \; g_2 = \boldsymbol{x}^{\boldsymbol{\alpha}_{2,1}} + \cdots, \; g_s = \boldsymbol{x}^{\boldsymbol{\alpha}_{s,1}} + \cdots$

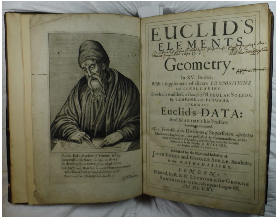
$\lambda_{i,j} = \operatorname{lcm}(\boldsymbol{x}^{\alpha_{i,1}}, \boldsymbol{x}^{\alpha_{j,1}})$

$S = \operatorname{spol}_{\prec}(g_i, g_j) = \frac{\lambda_{i,j}}{\operatorname{lm}_{\prec}(g_i)} g_i - \frac{\lambda_{i,j}}{\operatorname{lm}_{\prec}(g_j)} g_j \in \langle g_1, \ldots, g_s \rangle$

$S = 0?$, $\operatorname{lm}_{\prec}(S) \notin \langle \operatorname{lm}_{\prec}(g_1), \ldots, \operatorname{lm}_{\prec}(g_s) \rangle$?

$\rightsquigarrow$ **FullReduce** algorithm

From Euclid's algorithm to Buchberger's algorithm



$\mathbb{K}[x] \rightsquigarrow$ Monomial ordering induced by $\mathbb{N}$

$g_1 = x^a + \cdots \qquad g_2 = x^b + \cdots \qquad$ with $a \geq b$

$S = 1 \times g_1 - x^{a-b} g_2 \in \langle g_1, g_2 \rangle$

$S = 0?$, $\mathrm{lm}(S) \notin \langle \mathrm{lm}(g_2) \rangle$? $\qquad \rightsquigarrow$ repeat

$\mathbb{K}[x_1, \ldots, x_n] \rightsquigarrow$ Admissible monomial orderings over $\mathbb{N}^n$

$$g_1 = \boldsymbol{x}^{\boldsymbol{\alpha}_{1,1}} + \cdots, \; g_2 = \boldsymbol{x}^{\boldsymbol{\alpha}_{2,1}} + \cdots, \; g_s = \boldsymbol{x}^{\boldsymbol{\alpha}_{s,1}} + \cdots$$

$$\lambda_{i,j} = \mathrm{lcm}(\boldsymbol{x}^{\alpha_{i,1}}, \boldsymbol{x}^{\alpha_{j,1}})$$

$$S = \mathrm{spol}_{\prec}(g_i, g_j) = \frac{\lambda_{i,j}}{\mathrm{lm}_{\prec}(g_i)} g_i - \frac{\lambda_{i,j}}{\mathrm{lm}_{\prec}(g_j)} g_j \in \langle g_1, \ldots, g_s \rangle$$

$$S = 0?, \; \mathrm{lm}_{\prec}(S) \notin \langle \mathrm{lm}_{\prec}(g_1), \ldots, \mathrm{lm}_{\prec}(g_s) \rangle?$$

$\rightsquigarrow$ **FullReduce** algorithm

☛ S-polynomials

☛ Division/rewriting algorithm

Gröbner bases and Buchberger's algorithm

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ an admissible monomial ordering

Let $I \subset R$ be an ideal. A subset $G \subset R$ is a Gröbner basis for $(I, \prec)$ if *(i)* G is finite, *(ii)* $G \subset I$, *(iii)* $\langle \mathrm{lm}_\prec(G) \rangle = \langle \mathrm{lm}_\prec(I) \rangle$.

Gröbner bases and Buchberger's algorithm

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ an admissible monomial ordering

Let $I \subset R$ be an ideal. A subset $G \subset R$ is a Gröbner basis for $(I, \prec)$ if *(i)* G is finite, *(ii)* $G \subset I$, *(iii)* $\langle \mathrm{lm}_\prec(G) \rangle = \langle \mathrm{lm}_\prec(I) \rangle$.

1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \mathrm{Pairs}(G)$
3. while $\mathscr{P} \neq \emptyset$
   - **Choose** $(f, g) \in \mathscr{P}$;
     $\mathscr{P} \leftarrow \mathscr{P} - \{(f, g)\}$
   - $r \leftarrow \mathbf{FullReduce}_\prec(\mathrm{spol}_\prec(f, g), G)$
   - if $r \neq 0$,
     $\star$ $G \leftarrow G \cup \{r\}$
     $\star$ $\mathscr{P} \leftarrow \mathscr{P} \cup \mathrm{Pairs}(G)$
4. return G

Gröbner bases and Buchberger's algorithm

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ an admissible monomial ordering

Let $I \subset R$ be an ideal. A subset $G \subset R$ is a Gröbner basis for $(I, \prec)$ if *(i)* G is finite, *(ii)* $G \subset I$, *(iii)* $\langle \mathrm{lm}_\prec(G) \rangle = \langle \mathrm{lm}_\prec(I) \rangle$.

1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \mathrm{Pairs}(G)$
3. while $\mathscr{P} \neq \emptyset$
   - **Choose** $(f, g) \in \mathscr{P}$; $\mathscr{P} \leftarrow \mathscr{P} - \{(f, g)\}$
   - $r \leftarrow$ $\textbf{FullReduce}_\prec(\mathrm{spol}_\prec(f, g), G)$
   - if $r \neq 0$,
     - $\star$ $G \leftarrow G \cup \{r\}$
     - $\star$ $\mathscr{P} \leftarrow \mathscr{P} \cup \mathrm{Pairs}(G)$
4. return G

- Correctness, by design
- Terminates because $\langle \mathrm{lm}_\prec(G) \rangle$ keeps increasing

Gröbner bases and Buchberger's algorithm

Let $\mathbb{K}$ be a field, $R = \mathbb{K}[x_1, \ldots, x_n]$, $\prec$ an admissible monomial ordering

Let $I \subset R$ be an ideal. A subset $G \subset R$ is a Gröbner basis for $(I, \prec)$ if *(i)* G is finite, *(ii)* $G \subset I$, *(iii)* $\langle \mathrm{lm}_\prec(G) \rangle = \langle \mathrm{lm}_\prec(I) \rangle$.

1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \mathrm{Pairs}(G)$
3. while $\mathscr{P} \neq \emptyset$
   - **Choose** $(f, g) \in \mathscr{P}$; $\mathscr{P} \leftarrow \mathscr{P} - \{(f, g)\}$
   - $r \leftarrow$ **FullReduce**$_\prec(\mathrm{spol}_\prec(f, g), G)$
   - if $r \neq 0$,
     - $\star\ G \leftarrow G \cup \{r\}$
     - $\star\ \mathscr{P} \leftarrow \mathscr{P} \cup \mathrm{Pairs}(G)$
4. return G

- 👍 Correctness, by design
- 👍 Terminates because $\langle \mathrm{lm}_\prec(G) \rangle$ keeps increasing
- 👎 Most of the time is spent on computing 0
- 👎 Not so clear how to organise the computations (choice of pairs, choice of reducers, etc.)

Some properties of Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$.

Normal form. FullReduce$_\prec(f, G)$ is unique (and 0 when $f \in \langle G \rangle$)

allows us to compute in $\frac{R}{I}$ ($f \sim g \Leftrightarrow f - g \in I$)

Some properties of Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$.

Normal form. $\mathbf{FullReduce}_{\prec}(f, G)$ is unique (and 0 when $f \in \langle G \rangle$)

allows us to compute in $\frac{R}{I}$ ($f \sim g \Leftrightarrow f - g \in I$)

Equality of ideals. Reduced Gröbner basis for $(I, \prec)$ is unique.

Some properties of Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$.

Normal form. $\mathbf{FullReduce}_{\prec}(f, G)$ is unique (and 0 when $f \in \langle G \rangle$)

allows us to compute in $\frac{R}{I}$ $(f \sim g \Leftrightarrow f - g \in I)$

Equality of ideals. Reduced Gröbner basis for $(I, \prec)$ is unique.

Elimination theorem. When $\prec$ is an ordering which eliminates $x_1, \ldots, x_i$, $G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I \cap \mathbb{K}[x_{i+1}, \ldots, x_n], \prec)$ and defines the Zariski closure of $\pi(V(I))$.

Some properties of Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$.

Normal form. FullReduce$_\prec(f, G)$ is unique (and 0 when $f \in \langle G \rangle$)

allows us to compute in $\frac{R}{I}$ $(f \sim g \Leftrightarrow f - g \in I)$

Equality of ideals. Reduced Gröbner basis for $(I, \prec)$ is unique.

Elimination theorem. When $\prec$ is an ordering which eliminates $x_1, \ldots, x_i$, $G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I \cap \mathbb{K}[x_{i+1}, \ldots, x_n], \prec)$ and defines the Zariski closure of $\pi(V(I))$.

Shape of lex Gröbner bases. $G = G_n \cup G_{n-1} \cup \cdots \cup G_1$ with $G_i \subset \mathbb{K}[x_i, \ldots, x_n]$

Triangular structure, relations discovery

Some properties of Gröbner bases

Let G be a Gröbner basis for $(I, \prec)$.

Normal form. **FullReduce**$_\prec(f, G)$ is unique (and 0 when $f \in \langle G \rangle$)

allows us to compute in $\frac{R}{I}$ $(f \sim g \Leftrightarrow f - g \in I)$

Equality of ideals. Reduced Gröbner basis for $(I, \prec)$ is unique.

Elimination theorem. When $\prec$ is an ordering which eliminates $x_1, \ldots, x_i$, $G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $(I \cap \mathbb{K}[x_{i+1}, \ldots, x_n], \prec)$ and defines the Zariski closure of $\pi(V(I))$.

Shape of lex Gröbner bases. $G = G_n \cup G_{n-1} \cup \cdots \cup G_1$ with $G_i \subset \mathbb{K}[x_i, \ldots, x_n]$ Triangular structure, relations discovery

Shape of graded Gröbner bases. $d = \min(\deg(f) \mid f \in I - \{0\})$.

$$\mathrm{Span}(g \in G \mid \deg(g) = d) = \mathrm{Span}(f \in I \mid \deg(f) = d)$$

G contains polynomials of the least possible degree achieved in $I - \{0\}$

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Grete Hermann. A foundational PhD for computational algebra. *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. 1926.
Constructive method with **doubly exponential bounds**.

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Grete Hermann. A foundational PhD for computational algebra.
Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. 1926.
Constructive method with **doubly exponential bounds**.
Mayr-Meyer'82 These bounds are "unavoidable".

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Grete Hermann. A foundational PhD for computational algebra. *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. 1926.
Constructive method with **doubly exponential bounds**.
Mayr-Meyer'82 These bounds are "unavoidable".

Bayer/Stillman'87'88'92. Hilbert series, function, polynomial and monomial orderings, regularity.

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Grete Hermann. A foundational PhD for computational algebra. *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. 1926.
Constructive method with **doubly exponential bounds**.
Mayr-Meyer'82 These bounds are “unavoidable”.

Bayer/Stillman'87'88'92. Hilbert series, function, polynomial and monomial orderings, regularity.

Gritzmann/Sturmfels'93, Caboara/Perry'14.
Monomial orderings $\rightsquigarrow$ Dynamic versions of Buchberger's algorithm?

Complexity issues, next generation of algorithms

Bayer, Mumford'93 *One of the difficulties in surveying this area is that mathematicians from so many specialties [...] tend to publish in their own specialized journals. [...] One group , the working algebraic geometers, are much more interested in actually computing examples. [...] Another group comes from theoretical computer science and is much more interested in theoretical bounds*

Grete Hermann. A foundational PhD for computational algebra. *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. 1926.

Constructive method with **doubly exponential bounds**.

Mayr-Meyer'82 These bounds are "unavoidable".

Bayer/Stillman'87'88'92. Hilbert series, function, polynomial and monomial orderings, regularity.

Gritzmann/Sturmfels'93, Caboara/Perry'14.
Monomial orderings $\rightsquigarrow$ Dynamic versions of Buchberger's algorithm?

Lazard, Lazard/Giusti. Macaulay matrices, regular sequences

Degree of regularity is bounded by Macaulay's bound: $1 + \sum_i (\deg(f_i) - 1)$

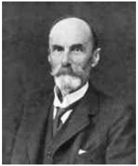
The F4 algorithm (Faugère, 1998)

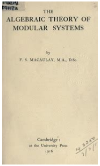
Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay





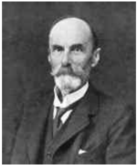
The F4 algorithm (Faugère, 1998)

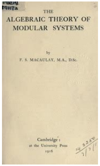
Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay





1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \{(af, bg) \mid f, g \in G\}$
3. while $\mathscr{P} \neq \emptyset$
   - $\mathscr{P}' \leftarrow \textbf{Select}(\mathscr{P})$, $\mathscr{P} \leftarrow \mathscr{P} - \mathscr{P}'$
   - $L \leftarrow \{af, bg \mid (af, bg) \in \mathscr{P}'\}$
   - $L \leftarrow \textbf{SymbolicPreProcessing}(L, G)$
   - $H \leftarrow \textbf{GaussianReduction}(\textbf{Macaulay}(L))$
   - for $h \in H$

     if $\mathrm{lm}_{\prec}(h) \notin \langle \mathrm{lm}(G) \rangle$

     $G \leftarrow G \cup \{h\}$ + update $\mathscr{P}$
4. return G

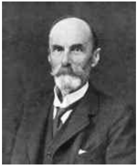
The F4 algorithm (Faugère, 1998)

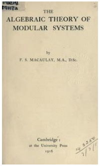
Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay





1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \{(af, bg) \mid f, g \in G\}$
3. while $\mathscr{P} \neq \emptyset$
   - $\mathscr{P}' \leftarrow \textbf{Select}(\mathscr{P})$, $\mathscr{P} \leftarrow \mathscr{P} - \mathscr{P}'$
   - $L \leftarrow \{af, bg \mid (af, bg) \in \mathscr{P}'\}$
   - $L \leftarrow \textbf{SymbolicPreProcessing}(L, G)$
   - $H \leftarrow \textbf{GaussianReduction}(\textbf{Macaulay}(L))$
   - for $h \in H$

     if $\mathrm{lm}_\prec(h) \notin \langle \mathrm{lm}(G) \rangle$

     $G \leftarrow G \cup \{h\}$ + update $\mathscr{P}$
4. return G

Differences with Buchberger.

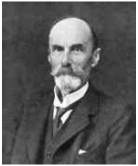
☛ selects a bunch of pairs at the same time

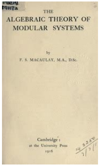
☛ does a symbolic-preprocessing

$\rightsquigarrow$ choice of reducers?

☛ full reduction at once

The F4 algorithm (Faugère, 1998)





Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay

1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \{(af, bg) \mid f, g \in G\}$
3. while $\mathscr{P} \neq \emptyset$
   - $\mathscr{P}' \leftarrow \textbf{Select}(\mathscr{P})$, $\mathscr{P} \leftarrow \mathscr{P} - \mathscr{P}'$
   - $L \leftarrow \{af, bg \mid (af, bg) \in \mathscr{P}'\}$
   - $L \leftarrow \textbf{SymbolicPreProcessing}(L, G)$
   - $H \leftarrow \textbf{GaussianReduction}(\textbf{Macaulay}(L))$
   - for $h \in H$

     if $\mathrm{lm}_\prec(h) \notin \langle \mathrm{lm}(G) \rangle$

     $G \leftarrow G \cup \{h\}$ + update $\mathscr{P}$
4. return G

Differences with Buchberger.

☛ selects a bunch of pairs at the same time

☛ does a symbolic-preprocessing

$\rightsquigarrow$ choice of reducers?

☛ full reduction at once

👍fast sparse linear algebra

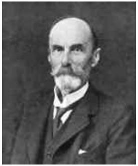
The F4 algorithm (Faugère, 1998)

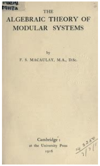
Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay





1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \{(af, bg) \mid f, g \in G\}$
3. while $\mathscr{P} \neq \emptyset$
   - $\mathscr{P}' \leftarrow \textbf{Select}(\mathscr{P})$, $\mathscr{P} \leftarrow \mathscr{P} - \mathscr{P}'$
   - $L \leftarrow \{af, bg \mid (af, bg) \in \mathscr{P}'\}$
   - $L \leftarrow \textbf{SymbolicPreProcessing}(L, G)$
   - $H \leftarrow \textbf{GaussianReduction}(\textbf{Macaulay}(L))$
   - for $h \in H$

     if $\mathrm{lm}_{\prec}(h) \notin \langle \mathrm{lm}(G) \rangle$

     $G \leftarrow G \cup \{h\}$ + update $\mathscr{P}$
4. return G

Differences with Buchberger.

☛ selects a bunch of pairs at the same time

☛ does a symbolic-preprocessing $\rightsquigarrow$ choice of reducers?

☛ full reduction at once

fast sparse linear algebra

still lots of reductions to zero $\rightsquigarrow$ F5 algorithm.

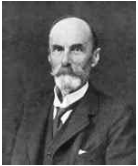
The F4 algorithm (Faugère, 1998)

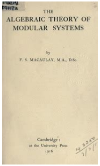
Macaulay matrices:

columns = monomials sorted by $\prec$

rows = coeffs of polynomials

Take the best of Buchberger and Macaulay





1. $G \leftarrow \boldsymbol{F}$
2. $\mathscr{P} \leftarrow \{(af, bg) \mid f, g \in G\}$
3. while $\mathscr{P} \neq \emptyset$
   - $\mathscr{P}' \leftarrow \textbf{Select}(\mathscr{P})$, $\mathscr{P} \leftarrow \mathscr{P} - \mathscr{P}'$
   - $L \leftarrow \{af, bg \mid (af, bg) \in \mathscr{P}'\}$
   - $L \leftarrow \textbf{SymbolicPreProcessing}(L, G)$
   - $H \leftarrow \textbf{GaussianReduction}(\textbf{Macaulay}(L))$
   - for $h \in H$

     if $\mathrm{lm}_{\prec}(h) \notin \langle \mathrm{lm}(G) \rangle$

     $G \leftarrow G \cup \{h\}$ + update $\mathscr{P}$
4. return G

Differences with Buchberger.

☛ selects a bunch of pairs at the same time

☛ does a symbolic-preprocessing $\rightsquigarrow$ choice of reducers?

☛ full reduction at once

fast sparse linear algebra

still lots of reductions to zero $\rightsquigarrow$ F5 algorithm.

probabilistic linear algebra

trace of the algorithm

Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

The "usual" good way to do

$$\boxed{\boldsymbol{F}} \xrightarrow[\text{Degree reverse lexicographic}]{\text{Compute Gröbner basis}} \boxed{GB_{grevlex}} \xrightarrow[\text{Lexicographic}]{\text{Change of ordering}} \boxed{GB_{LEX}}$$

Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

The "usual" good way to do

$$\boxed{\boldsymbol{F}} \xrightarrow[\text{Degree reverse lexicographic}]{\text{Compute Gröbner basis}} \boxed{GB_{grevlex}} \xrightarrow[\text{Lexicographic}]{\text{Change of ordering}} \boxed{GB_{LEX}}$$

Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

The "usual" good way to do

$$\boxed{\boldsymbol{F}} \xrightarrow[\text{Degree reverse lexicographic}]{\text{Compute Gröbner basis}} \boxed{GB_{grevlex}} \xrightarrow[\text{Lexicographic}]{\text{Change of ordering}} \boxed{GB_{LEX}}$$

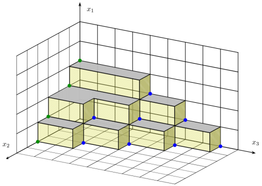
Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

The "usual" good way to do

$$\boxed{\boldsymbol{F}} \xrightarrow[\text{Degree reverse lexicographic}]{\text{Compute Gröbner basis}} \boxed{GB_{grevlex}} \xrightarrow[\text{Lexicographic}]{\text{Change of ordering}} \boxed{GB_{LEX}}$$



Gröbner basis $\rightsquigarrow$ (finite) monomial basis for $\frac{R}{I}$

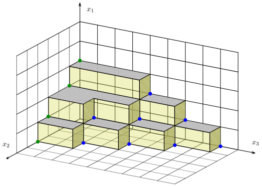
Change of orderings

Basic common case. $V(\boldsymbol{F})$ is finite in $\overline{\mathbb{K}}^n$

$\rightsquigarrow \frac{R}{\langle \boldsymbol{F} \rangle}$ is a finite dimensional $\mathbb{K}$-vector space

The "usual" good way to do

$$\begin{tikzcd}[column sep=huge] \boxed{\boldsymbol{F}} \arrow[r, "\substack{\text{Compute}\\ \text{Gröbner basis}}", "\substack{\text{Degree reverse}\\ \text{lexicographic}}"'] & \boxed{GB_{grevlex}} \arrow[r, "\substack{\text{Change}\\ \text{of ordering}}", "\text{Lexicographic}"'] & \boxed{GB_{LEX}} \end{tikzcd}$$



Gröbner basis $\rightsquigarrow$ (finite) monomial basis for $\frac{R}{I}$

Basic idea: recover linear relations between $\{1, x_n, \ldots, x_n^D\}$ in $\frac{R}{I}$ + other relations

Faugère/Gianni/Lazard/Mora

☛ **Linear system solving.**

The `msolve` library

plain C library implemented by Berthomieu, Eder, S.

$\simeq$ 55 000 lines, license GPLv2+

uses GMP and FLINT

`https://msolve.lip6.fr`

The `msolve` library

plain C library implemented by Berthomieu, Eder, S.

$\simeq$ 55 000 lines, license GPLv2+

uses GMP and FLINT

`https://msolve.lip6.fr`

`https://github.com/algebraic-solving/msolve`

`https://gitlab.lip6.fr/safey/msolve`

The `msolve` library

plain C library implemented by Berthomieu, Eder, S.

$\simeq$ 55 000 lines, license GPLv2+

uses GMP and FLINT

`https://msolve.lip6.fr`

`https://github.com/algebraic-solving/msolve`

`https://gitlab.lip6.fr/safey/msolve`

`https://algebraic-solving.github.io/`

The `msolve` library

plain C library implemented by Berthomieu, Eder, S.

$\simeq$ 55 000 lines, license GPLv2+

uses GMP and FLINT

`https://msolve.lip6.fr`

SORBONNE UNIVERSITÉ

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

GitHub GitLab

`https://github.com/algebraic-solving/msolve`

`https://gitlab.lip6.fr/safey/msolve`

`https://algebraic-solving.github.io/`

julia OSCAR SYMBOLIC TOOLS

The `msolve` library

plain C library implemented by Berthomieu, Eder, S.

$\simeq$ 55 000 lines, license GPLv2+

uses GMP and FLINT

`https://msolve.lip6.fr`

`https://github.com/algebraic-solving/msolve`

`https://gitlab.lip6.fr/safey/msolve`

`https://algebraic-solving.github.io/`

What does `msolve` compute?

- Computes *grevlex* Gröbner bases when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime)

  ```
  ./msolve -g 2 -f in.ms -o out.ms
  ```

  (coming soon $\rightsquigarrow \mathbb{K} = \mathbb{Q}$).

What does msolve compute?

- Computes *grevlex* Gröbner bases when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime)
  `./msolve -g 2 -f in.ms -o out.ms`

  (coming soon $\rightsquigarrow \mathbb{K} = \mathbb{Q}$).
- Computes *lex* Gröbner bases of the radical of the input ideal when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime) and when it is in shape position

  $$w(x_n), x_{n-1} - v_{n-1}(x_n), \ldots, x_1 - v_1(x_n)$$

  No shape position assumption? $\rightsquigarrow$ `msolve` performs a change of coordinate `./msolve -g 2 -f in.ms -o out.ms`

What does `msolve` compute?

- Computes *grevlex* Gröbner bases when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime)

  `./msolve -g 2 -f in.ms -o out.ms`

  (coming soon $\rightsquigarrow \mathbb{K} = \mathbb{Q}$).
- Computes *lex* Gröbner bases of the radical of the input ideal when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime) and when it is in shape position

  $$w(x_n), x_{n-1} - v_{n-1}(x_n), \ldots, x_1 - v_1(x_n)$$

  No shape position assumption? $\rightsquigarrow$ `msolve` performs a change of coordinate `./msolve -g 2 -f in.ms -o out.ms`
- When $\mathbb{K} = \mathbb{Q}$ and number of complex solutions is finite:
  - `msolve` isolates the real solutions

    `./msolve -f in.ms -o out.ms`

What does `msolve` compute?

- Computes *grevlex* Gröbner bases when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime)

  `./msolve -g 2 -f in.ms -o out.ms`

  (coming soon $\rightsquigarrow \mathbb{K} = \mathbb{Q}$).

- Computes *lex* Gröbner bases of the radical of the input ideal when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime) and when it is in shape position

  $$w(x_n), x_{n-1} - v_{n-1}(x_n), \ldots, x_1 - v_1(x_n)$$

  No shape position assumption? $\rightsquigarrow$ `msolve` performs a change of coordinate `./msolve -g 2 -f in.ms -o out.ms`

- When $\mathbb{K} = \mathbb{Q}$ and number of complex solutions is finite:
  - `msolve` isolates the real solutions

    `./msolve -f in.ms -o out.ms`

  - `msolve` computes a rational parametrization of the complex solutions

    $$w(x_n), \frac{\partial w}{\partial x_n} x_{n-1} - r_{n-1}(x_n), \ldots, \frac{\partial w}{\partial x_n} x_1 - r_1(x_n)$$

    `./msolve -P 1 -f in.ms -o out.ms`

What does msolve compute?

- Computes *grevlex* Gröbner bases when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime)

  `./msolve -g 2 -f in.ms -o out.ms`

  (coming soon $\rightsquigarrow \mathbb{K} = \mathbb{Q}$).
- Computes *lex* Gröbner bases of the radical of the input ideal when $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (with $p < 2^{31}$ prime) and when it is in shape position

  $$w(x_n), x_{n-1} - v_{n-1}(x_n), \ldots, x_1 - v_1(x_n)$$

  No shape position assumption? $\rightsquigarrow$ `msolve` performs a change of coordinate `./msolve -g 2 -f in.ms -o out.ms`
- When $\mathbb{K} = \mathbb{Q}$ and number of complex solutions is finite:
  - `msolve` isolates the real solutions

    `./msolve -f in.ms -o out.ms`
  - `msolve` computes a rational parametrization of the complex solutions

    $$w(x_n), \frac{\partial w}{\partial x_n} x_{n-1} - r_{n-1}(x_n), \ldots, \frac{\partial w}{\partial x_n} x_1 - r_1(x_n)$$

    `./msolve -P 1 -f in.ms -o out.ms`
- Some other more experimental functionalities

  (e.g. elimination ideals, saturations of ideals, normal forms)

How does it compute?

- Gröbner basis engine: F4 algorithm (variation of Eder's gb library)
  Memory usage | Fast divisibility check | Linear algebra | AVX2

How does it compute?

- Gröbner basis engine: F4 algorithm (variation of Eder's gb library)
  Memory usage | Fast divisibility check | Linear algebra | AVX2
- Change of orderings: "Sparse-FGLM" **Faugère/Mou**
  ☛ Matrix multiplications can be "read" from the GB.
  ☛ Wiedemann's algorithm + Berlekamp-Massey
  Dedicated storage | Cache aware matrix-vector product | AVX2
- F4 trace algorithm **Traverso'88**

How does it compute?

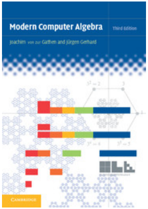
- Gröbner basis engine: F4 algorithm (variation of Eder's gb library)
  Memory usage | Fast divisibility check | Linear algebra | AVX2
- Change of orderings: "Sparse-FGLM" **Faugère/Mou**
  ☛ Matrix multiplications can be "read" from the GB.
  ☛ Wiedemann's algorithm + Berlekamp-Massey
  Dedicated storage | Cache aware matrix-vector product | AVX2
- F4 trace algorithm **Traverso'88**

Multi-threading through Openmp

How does it compute?

- Gröbner basis engine: F4 algorithm (variation of Eder's gb library)
  Memory usage | Fast divisibility check | Linear algebra | AVX2
- Change of orderings: "Sparse-FGLM" **Faugère/Mou**
  ☛ Matrix multiplications can be "read" from the GB.
  ☛ Wiedemann's algorithm + Berlekamp-Massey
  Dedicated storage | Cache aware matrix-vector product | AVX2
- F4 trace algorithm **Traverso'88**

Multi-threading through Openmp



- Multi-modular arithmetics $\frac{a}{b}$ uniquely determined by its image in $\frac{\mathbb{Z}}{p_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k\mathbb{Z}}$ provided that $2p_1 \cdots p_k \geq \|a\|\|b\|$
- Computations over $\mathbb{Q}$ use this multi-modular arithmetics
- Low memory usage
  $\rightsquigarrow$ parallel multi-modular computations
- + extra computer algebra algorithms

Some timings

Examples	DEG	msolve(trace)	msolve(prob)	speed-up	maple	speed-up	magma	speed-up
Katsura-9	256	4.89	7.49	1.53	104	21.27	2522	515
Katsura-10	512	43.7	70.5	1.61	1 278	29.24	82 540	1 888
Katsura-11	1024	424	814	1.92	7 812	18.4	-	
Katsura-12	2048	6 262	11 215	1.79	120 804	19.29	-	
Katsura-13	4096	89 390	148 372	1.66	-		-	
Katsura-14	8192	1 308 602	2 000 170	1.53	-		-	
Eco-10	256	12.5	21.2	1.69	26.3	2.1	6520	521.6
Eco-11	512	90.3	161	1.78	312	3.45	214 770	2378
Eco-12	1024	877	1 619	1.84	4 287	4.88	-	
Eco-13	2048	12 137	19 553	1.61	66 115	5.44	-	
Eco-14	4096	167 798	254 389	1.51	-		-	
Henrion-5	100	0.71	0.83	1.17	2.7	3.8	93	130.98
Henrion-6	720	138	157	1.13	1 470	10.65	-	
Henrion-7	5040	117 803	127 456	1.08	-		-	
CP(3,5,2)	288	18.1	19.2	1.06	249	13.75	-	
CP(3,6,2)	720	390	450	1.15	23 440	60	-	
CP(3,7,2)	1728	9 643	11 511	1.19	-		-	
CP(3,8,2)	4032	269 766	323 838	1.2	-		-	

☛ Katsura-16 259 240 secs (learn grevlex), 7 518 (tracer), 15 688 secs (fglm)

Some timings

Examples	DEG	msolve(trace)	msolve(prob)	speed-up	maple	speed-up	magma	speed-up
Katsura-9	256	4.89	7.49	1.53	104	21.27	2522	515
Katsura-10	512	43.7	70.5	1.61	1 278	29.24	82 540	1 888
Katsura-11	1024	424	814	1.92	7 812	18.4	-	
Katsura-12	2048	6 262	11 215	1.79	120 804	19.29	-	
Katsura-13	4096	89 390	148 372	1.66	-		-	
Katsura-14	8192	1 308 602	2 000 170	1.53	-		-	
Eco-10	256	12.5	21.2	1.69	26.3	2.1	6520	521.6
Eco-11	512	90.3	161	1.78	312	3.45	214 770	2378
Eco-12	1024	877	1 619	1.84	4 287	4.88	-	
Eco-13	2048	12 137	19 553	1.61	66 115	5.44	-	
Eco-14	4096	167 798	254 389	1.51	-		-	
Henrion-5	100	0.71	0.83	1.17	2.7	3.8	93	130.98
Henrion-6	720	138	157	1.13	1 470	10.65	-	
Henrion-7	5040	117 803	127 456	1.08	-		-	
CP(3,5,2)	288	18.1	19.2	1.06	249	13.75	-	
CP(3,6,2)	720	390	450	1.15	23 440	60	-	
CP(3,7,2)	1728	9 643	11 511	1.19	-		-	
CP(3,8,2)	4032	269 766	323 838	1.2	-		-	
Noon-7	2173	4039	5 045	1.25	432	0.1	-	
Noon-8	6545	598 647	640 177	1.07	5997	0.01	-	

Some timings

Examples	DEG	msolve(trace)	msolve(prob)	speed-up	maple	speed-up	magma	speed-up
Katsura-9	256	4.89	7.49	1.53	104	21.27	2522	515
Katsura-10	512	43.7	70.5	1.61	1 278	29.24	82 540	1 888
Katsura-11	1024	424	814	1.92	7 812	18.4	-	
Katsura-12	2048	6 262	11 215	1.79	120 804	19.29	-	
Katsura-13	4096	89 390	148 372	1.66	-		-	
Katsura-14	8192	1 308 602	2 000 170	1.53	-		-	
Eco-10	256	12.5	21.2	1.69	26.3	2.1	6520	521.6
Eco-11	512	90.3	161	1.78	312	3.45	214 770	2378
Eco-12	1024	877	1 619	1.84	4 287	4.88	-	
Eco-13	2048	12 137	19 553	1.61	66 115	5.44	-	
Eco-14	4096	167 798	254 389	1.51	-		-	
Henrion-5	100	0.71	0.83	1.17	2.7	3.8	93	130.98
Henrion-6	720	138	157	1.13	1 470	10.65	-	
Henrion-7	5040	117 803	127 456	1.08	-		-	
CP(3,5,2)	288	18.1	19.2	1.06	249	13.75	-	
CP(3,6,2)	720	390	450	1.15	23 440	60	-	
CP(3,7,2)	1728	9 643	11 511	1.19	-		-	
CP(3,8,2)	4032	269 766	323 838	1.2	-		-	
Noon-7	2173	4039	5 045	1.25	432	0.1	-	
Noon-8	6545	598 647	640 177	1.07	5997	0.01	-	

☛ Katsura-16 259 240 secs (learn grevlex), 7 518 (tracer), 15 688 secs (fglm)

Applications of Gröbner bases

$\boxed{\textbf{Applications in cryptology}}$

$\mathbb{K}$ **finite**.

Security assessment through complexity

Applications of Gröbner bases

Applications in cryptology

$\mathbb{K}$ **finite**.

Security assessment through complexity

Geometric applications

Applications of Gröbner bases

Applications in cryptology

$\mathbb{K}$ **finite**.

Security assessment through complexity

Geometric applications

Applications in combinatorics

Compute algebraic relations

Applications of Gröbner bases

Applications in cryptology

$\mathbb{K}$ **finite.**

Security assessment through complexity

Geometric applications

Applications in combinatorics

Compute algebraic relations

Using Gröbner bases to improve numerical computing

Discover properties, algebraic relations

Applications of Gröbner bases

Applications in cryptology

$\mathbb{K}$ **finite.**

Security assessment through complexity

Geometric applications

Applications in combinatorics

Compute algebraic relations

Using Gröbner bases to improve numerical computing

Discover properties, algebraic relations

Image-based visual servoing

Gröbner bases at the rescue...

Gröbner bases in cryptography (I)

National Institute of Standards and Technology
U.S. Department of Commerce

Polynomial system solving is hard even when $\mathbb{K} = \frac{\mathbb{Z}}{2\mathbb{Z}}$

Encryption/decryption scheme

Take $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$ chosen such that
the map $\boldsymbol{x} \mapsto \boldsymbol{F}(\boldsymbol{x})$ is "easy" to invert.

Choose $\boldsymbol{S}$ and $\boldsymbol{T}$ in $\mathrm{GL}_n(\mathbb{K})$.

$\boldsymbol{P} = \boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{S}$ is the public key.

Encrypt $m \in \mathbb{K}^n$. $c = \boldsymbol{P}(m)$ **Decrypt**. $m = \boldsymbol{S}^{-1} \circ \boldsymbol{F}^{-1} \circ \boldsymbol{T}^{-1}(c)$

Gröbner bases in cryptography (I)

National Institute of Standards and Technology
U.S. Department of Commerce

Polynomial system solving is hard even when $\mathbb{K} = \frac{\mathbb{Z}}{2\mathbb{Z}}$

Encryption/decryption scheme

Take $\boldsymbol{F} = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$ chosen such that

the map $\boldsymbol{x} \mapsto \boldsymbol{F}(\boldsymbol{x})$ is "easy" to invert.

Choose $\boldsymbol{S}$ and $\boldsymbol{T}$ in $\mathrm{GL}_n(\mathbb{K})$.

$\boldsymbol{P} = \boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{S}$ is the public key.

Encrypt $m \in \mathbb{K}^n$. $c = \boldsymbol{P}(m)$ **Decrypt**. $m = \boldsymbol{S}^{-1} \circ \boldsymbol{F}^{-1} \circ \boldsymbol{T}^{-1}(c)$

Signature scheme

Check signature σ from a digest $\delta \rightsquigarrow \boldsymbol{P}(\sigma) \stackrel{?}{=} \delta$

Generate σ from $\delta \rightsquigarrow \boldsymbol{F}(\sigma') = \delta \boldsymbol{T}^{-1} \rightsquigarrow \sigma \stackrel{\text{def}}{=} \sigma' \boldsymbol{S}^{-1}$

Gröbner bases in cryptography (II)

Trapdoor examples.

- **Triangular structure.** F is triangular (and $n = s$)

Gröbner bases in cryptography (II)

Trapdoor examples.

- **Triangular structure.** F is triangular (and $n = s$)
- **Oil and vinegar.** $O = \{x_1, \ldots, x_{n-s}\}$, $V = \{x_{n-s+1}, \ldots, x_n\}$ and f_i is quadratic but linear when V is instantiated.

Gröbner bases in cryptography (II)

Trapdoor examples.

- **Triangular structure.** F is triangular (and $n = s$)
- **Oil and vinegar.** $O = \{x_1, \ldots, x_{n-s}\}$, $V = \{x_{n-s+1}, \ldots, x_n\}$ and f_i is quadratic but linear when V is instantiated.
- **Field extensions.** $\mathbb{K} = \mathbb{F}_{q^n} \simeq \mathbb{F}_q^n$

  Take $F = \sum_{\substack{1 \le i \le j \le n \\ q^i + q^j \le D}} a_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i < n \\ q^i \le D}} b_i X^{q^i} + c$

  and a basis $(1, \alpha, \ldots, \alpha^{n-1})$ of $\mathbb{F}_{q^n}$.

  $F(\sum_{i=1}^{n-1} \alpha^{i-1} x_i) = \sum_{i=0}^{n-1} f_i(x_1, \ldots, x_n) \alpha^i$

Gröbner bases in cryptography (II)

Trapdoor examples.

- **Triangular structure.** F is triangular (and $n = s$)
- **Oil and vinegar.** $O = \{x_1, \ldots, x_{n-s}\}$, $V = \{x_{n-s+1}, \ldots, x_n\}$ and f_i is quadratic but linear when V is instantiated.
- **Field extensions.** $\mathbb{K} = \mathbb{F}_{q^n} \simeq \mathbb{F}_q^n$
  Take $F = \sum_{\substack{1 \leq i \leq j \leq n \\ q^i + q^j \leq D}} a_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leq i < n \\ q^i \leq D}} b_i X^{q^i} + c$
  and a basis $(1, \alpha, \ldots, \alpha^{n-1})$ of $\mathbb{F}_{q^n}$.
  $F(\sum_{i=1}^{n-1} \alpha^{i-1} x_i) = \sum_{i=0}^{n-1} f_i(x_1, \ldots, x_n) \alpha^i$

Gröbner bases are used to “attack” crypto-systems
(i.e. recover encrypted secrets, forge signatures)
“sharp” complexity analysis of the attacks helps to
identify secure parameters

Gröbner bases in cryptography (II)

Trapdoor examples.

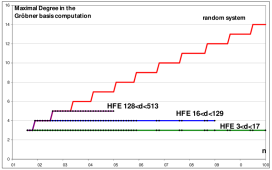
- **Triangular structure.** F is triangular (and $n = s$)
- **Oil and vinegar.** $O = \{x_1, \ldots, x_{n-s}\}$, $V = \{x_{n-s+1}, \ldots, x_n\}$ and f_i is quadratic but linear when V is instantiated.
- **Field extensions.** $\mathbb{K} = \mathbb{F}_{q^n} \simeq \mathbb{F}_q^n$

  Take $F = \sum\limits_{\substack{1\leq i\leq j\leq n \\ q^i+q^j\leq D}} a_{i,j}X^{q^i+q^j} + \sum_{\substack{0\leq i<n \\ q^i\leq D}} b_iX^{q^i} + c$

  and a basis $(1, \alpha, \ldots, \alpha^{n-1})$ of $\mathbb{F}_{q^n}$.

  $F(\sum_{i=1}^{n-1} \alpha^{i-1}x_i) = \sum_{i=0}^{n-1} f_i(x_1, \ldots, x_n)\alpha^i$

Gröbner bases are used to “attack” crypto-systems (i.e. recover encrypted secrets, forge signatures) “sharp” complexity analysis of the attacks helps to identify secure parameters



Using Gröbner bases in geometry (I)

Take C_1, C_2, C_3, C_4, C_5 in $\mathbb{Q}[x_1, x_2]$ of degree 2.
Compute $U \in \mathbb{Q}[x_1, x_2]$ such that
$V(U)$ is tangent to $V(C_i)$ for $1 \leq i \leq 5$.

Using Gröbner bases in geometry (I)

Take C_1, C_2, C_3, C_4, C_5 in $\mathbb{Q}[x_1, x_2]$ of degree 2.
Compute $U \in \mathbb{Q}[x_1, x_2]$ such that
$V(U)$ is tangent to $V(C_i)$ for $1 \leq i \leq 5$.

Breiding, Sturmfels, Timme'20 Solving means computing a Gröbner basis G. Indeed, crucial invariants, such as the dimension and degree of the solution variety, [...] The number of real solutions is found by applying techniques [...]. Yet Gröbner bases can take a very long time to compute. We found them impractical for Steiner's problem.

☛ Various modelings proposed, difficulty is to "force" U to be generic.

One suits better with numerical homotopy continuation

Using Gröbner bases in geometry (I)

Take C_1, C_2, C_3, C_4, C_5 in $\mathbb{Q}[x_1, x_2]$ of degree 2.
Compute $U \in \mathbb{Q}[x_1, x_2]$ such that
$V(U)$ is tangent to $V(C_i)$ for $1 \leq i \leq 5$.

Breiding, Sturmfels, Timme'20 Solving means computing a Gröbner basis G. Indeed, crucial invariants, such as the dimension and degree of the solution variety, [...] The number of real solutions is found by applying techniques [...]. Yet Gröbner bases can take a very long time to compute. We found them impractical for Steiner's problem.

☛ Various modelings proposed, difficulty is to "force" U to be generic.
One suits better with numerical homotopy continuation

"New" alternative modeling which suits "well" to Gröbner bases

👍 `msolve` can solve one instance within $\simeq 2.5$ hours (!)

👎 using 36 threads (memory consumption is ok but not tiny)...

Using Gröbner bases in geometry (II)

Theorem. Surfaces of degree 3 always contain lines and conics.

Noether–Lefschetz theorem $\Longrightarrow$ surfaces of degree ≥ 4 almost never do.

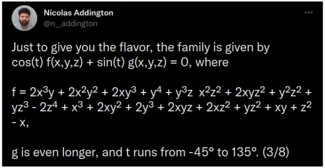
Using Gröbner bases in geometry (II)

Theorem. Surfaces of degree 3 always contain lines and conics.

Noether–Lefschetz theorem $\Longrightarrow$ surfaces of degree ≥ 4 almost never do.

$\boxed{\text{What about some special surfaces of degree 4?}}$ $\cos(t)f + \sin(t)g = 0$

UNIVERSITY OF
OREGON



Using `msolve` 7 secs to compute the lines

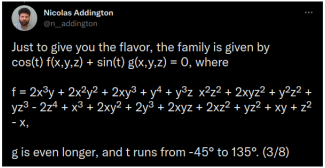
Using Gröbner bases in geometry (II)

Theorem. Surfaces of degree 3 always contain lines and conics.

Noether–Lefschetz theorem $\Longrightarrow$ surfaces of degree ≥ 4 almost never do.

What about some special surfaces of degree 4? $\cos(t)f + \sin(t)g = 0$

UNIVERSITY OF OREGON



Using `msolve` 7 secs to compute the lines

... several days/weeks to obtain the conics

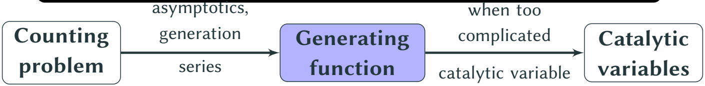
Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting

Counting problem $\xrightarrow[\text{series}]{\text{asymptotics, generation}}$ **Generating function** $\xrightarrow[\text{catalytic variable}]{\text{when too complicated}}$ **Catalytic variables**

Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting



Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting

Counting problem —asymptotics, generation / series→ **Generating function** —when too complicated / catalytic variable→ **Catalytic variables**

Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting

$$\text{Counting problem} \xrightarrow[\text{series}]{\text{asymptotics, generation}} \text{Generating function} \xrightarrow[\text{catalytic variable}]{\text{when too complicated}} \text{Catalytic variables}$$

Algebraicity result Bousquet-Mélou/Jéhanne'06, Popescu'86

Let $f \in \mathbb{Q}[u]$ and $Q \in \mathbb{Q}[x, y, t, u]$.

Let $\mathscr{F} \in \mathbb{Q}[u][[t]]$ be the solution to $\boxed{\mathscr{F} = f(u) + tQ(\mathscr{F}, \Delta(\mathscr{F}), t, u)}$

where $\Delta = \frac{\mathscr{F}(t,u)-\mathscr{F}(t,1)}{u-1}$. Then, $\mathscr{F}$ is algebraic over $\mathbb{Q}(t, u)$

$\exists R \in \mathbb{Q}[t, z] - \{0\}, R(t, \mathscr{F}(t, 1)) \equiv 0$.

Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting

Counting problem $\xrightarrow[\text{series}]{\text{asymptotics, generation}}$ **Generating function** $\xrightarrow[\text{catalytic variable}]{\text{when too complicated}}$ **Catalytic variables**

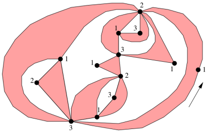
Algebraicity result **Bousquet-Mélou/Jéhanne'06, Popescu'86**

Let $f \in \mathbb{Q}[u]$ and $Q \in \mathbb{Q}[x, y, t, u]$.

Let $\mathscr{F} \in \mathbb{Q}[u][[t]]$ be the solution to $\boxed{\mathscr{F} = f(u) + tQ(\mathscr{F}, \Delta(\mathscr{F}), t, u)}$

where $\Delta = \frac{\mathscr{F}(t,u) - \mathscr{F}(t,1)}{u-1}$. Then, $\mathscr{F}$ is algebraic over $\mathbb{Q}(t, u)$

$\exists R \in \mathbb{Q}[t, z] - \{0\}, R(t, \mathscr{F}(t, 1)) \equiv 0.$



FPE $\longrightarrow$ Polynomial systems

Elimination

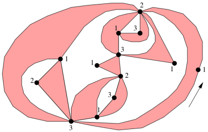
Using Gröbner bases in combinatorics

The Flajolet-Sedgewick machinery for counting

Counting problem $\xrightarrow[\text{series}]{\text{asymptotics, generation}}$ **Generating function** $\xrightarrow[\text{catalytic variable}]{\text{when too complicated}}$ **Catalytic variables**

Algebraicity result **Bousquet-Mélou/Jéhanne'06, Popescu'86**

Let $f \in \mathbb{Q}[u]$ and $Q \in \mathbb{Q}[x, y, t, u]$.
Let $\mathscr{F} \in \mathbb{Q}[u][[t]]$ be the solution to $\boxed{\mathscr{F} = f(u) + tQ(\mathscr{F}, \Delta(\mathscr{F}), t, u)}$
where $\Delta = \frac{\mathscr{F}(t,u) - \mathscr{F}(t,1)}{u-1}$. Then, $\mathscr{F}$ is algebraic over $\mathbb{Q}(t, u)$
$\exists R \in \mathbb{Q}[t, z] - \{0\}, R(t, \mathscr{F}(t, 1)) \equiv 0.$



FPE $\longrightarrow$ Polynomial systems

Elimination

Bostan/Chyzak/Notarantonio/S.

Optimal solution to inverse kinematics

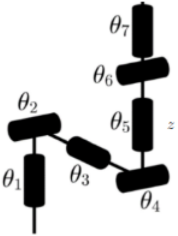
Problem. find robot control parameters to bring it into the desired position under the kinematics and collision constraint

$\rightsquigarrow$ 7DOF serial manipulators are harder.

Optimal solution to inverse kinematics

Problem. find robot control parameters to bring it into the desired position under the kinematics and collision constraint

→ 7DOF serial manipulators are harder.

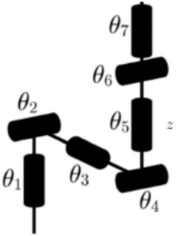


+ **Pavel Trutman**

Optimal solution to inverse kinematics

Problem. find robot control parameters to bring it into the desired position under the kinematics and collision constraint

⇝ 7DOF serial manipulators are harder.



+ **Pavel Trutman**

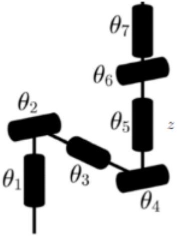
Solutions that minimize the weighted sum of distances of the joint angles from their preferred values ⇝ optimization problem

- 14 variables
- quadratic objective function
- equality constraints of degree 4

Optimal solution to inverse kinematics

Problem. find robot control parameters to bring it into the desired position under the kinematics and collision constraint

⇝ 7DOF serial manipulators are harder.



+ **Pavel Trutman**

Solutions that minimize the weighted sum of distances of the joint angles from their preferred values ⇝ optimization problem

- 14 variables
- quadratic objective function
- equality constraints of degree 4

- 1st Lasserre relaxation
  ⇝ SDP with 3060 variables
- 2nd Lasserre relaxtion
  ⇝ SDP with 38760 variables

Optimal solution to inverse kinematics

$$[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - 2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + 49953414\, s_2\, s_6 - 49996703\, s_3\, s_5, 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - 47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + 2063733\, s_1\, s_6, 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - 47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - 49953414\, c_2\, s_6 - 49996703\, c_5\, s_4, 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + 14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + 2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2, 14721294\, c_1\, c_7\, s_6 - 47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - 49996703\, s_3\, s_4, 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - 47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + 49953414\, c_2\, c_6 - 49996703\, c_4, -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + 14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + 2048843\, s_2\, s_7, -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + 14719214\, c_7\, s_1 - 47736318\, s_1\, s_7, -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + 14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5, 171288941990000\, c_1\, c_2 + 27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2, 49996703000000\, s_3\, s_4 + 13502153845963\, c_1 - 85644470995000\, s_1, 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + 91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000, {c_1}^2 + {s_1}^2 - 1, {c_2}^2 + {s_2}^2 - 1, {c_3}^2 + {s_3}^2 - 1, {c_4}^2 + {s_4}^2 - 1, {c_5}^2 + {s_5}^2 - 1, {c_6}^2 + {s_6}^2 - 1, {c_7}^2 + {s_7}^2 - 1]$$

Optimal solution to inverse kinematics

$[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - 2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + 49953414\, s_2\, s_6 - 49996703\, s_3\, s_5, 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - 47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + 2063733\, s_1\, s_6, 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - 47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - 49953414\, c_2\, s_6 - 49996703\, c_5\, s_4, 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + 14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + 2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2, 14721294\, c_1\, c_7\, s_6 - 47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - 49996703\, s_3\, s_4, 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - 47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + 49953414\, c_2\, c_6 - 49996703\, c_4, -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + 14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + 2048843\, s_2\, s_7, -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + 14719214\, c_7\, s_1 - 47736318\, s_1\, s_7, -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + 14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5, 171288941990000\, c_1\, c_2 + 27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2, 49996703000000\, s_3\, s_4 + 13502153845963\, c_1 - 85644470995000\, s_1, 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + 91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000, {c_1}^2 + {s_1}^2 - 1, {c_2}^2 + {s_2}^2 - 1, {c_3}^2 + {s_3}^2 - 1, {c_4}^2 + {s_4}^2 - 1, {c_5}^2 + {s_5}^2 - 1, {c_6}^2 + {s_6}^2 - 1, {c_7}^2 + {s_7}^2 - 1]$

Optimal solution to inverse kinematics

$$[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - 2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + 49953414\, s_2\, s_6 - 49996703\, s_3\, s_5,\, 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - 47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + 2063733\, s_1\, s_6,\, 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - 47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - 49953414\, c_2\, s_6 - 49996703\, c_5\, s_4,\, 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + 14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + 2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2,\, 14721294\, c_1\, c_7\, s_6 - 47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - 49996703\, s_3\, s_4,\, 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - 47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + 49953414\, c_2\, c_6 - 49996703\, c_4,\, -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + 14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + 2048843\, s_2\, s_7,\, -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + 14719214\, c_7\, s_1 - 47736318\, s_1\, s_7,\, -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + 14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5,\, 171288941990000\, c_1\, c_2 + 27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2,\, 49996703000000\, s_3\, s_4 + 13502153845963\, c_1 - 85644470995000\, s_1,\, 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + 91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000,\, {c_1}^2 + {s_1}^2 - 1,\, {c_2}^2 + {s_2}^2 - 1,\, {c_3}^2 + {s_3}^2 - 1,\, {c_4}^2 + {s_4}^2 - 1,\, {c_5}^2 + {s_5}^2 - 1,\, {c_6}^2 + {s_6}^2 - 1,\, {c_7}^2 + {s_7}^2 - 1]$$

Optimal solution to inverse kinematics

$[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - 2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + 49953414\, s_2\, s_6 - 49996703\, s_3\, s_5, 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - 47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + 2063733\, s_1\, s_6, 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - 47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - 49953414\, c_2\, s_6 - 49996703\, c_5\, s_4, 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + 14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + 2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2, 14721294\, c_1\, c_7\, s_6 - 47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - 49996703\, s_3\, s_4, 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - 47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + 49953414\, c_2\, c_6 - 49996703\, c_4, -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + 14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + 2048843\, s_2\, s_7, -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + 14719214\, c_7\, s_1 - 47736318\, s_1\, s_7, -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + 14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5, 171288941990000\, c_1\, c_2 + 27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2, 49996703000000\, s_3\, s_4 + 13502153845963\, c_1 - 85644470995000\, s_1, 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + 91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000, {c_1}^2 + {s_1}^2 - 1, {c_2}^2 + {s_2}^2 - 1, {c_3}^2 + {s_3}^2 - 1, {c_4}^2 + {s_4}^2 - 1, {c_5}^2 + {s_5}^2 - 1, {c_6}^2 + {s_6}^2 - 1, {c_7}^2 + {s_7}^2 - 1]$

Optimal solution to inverse kinematics

$$
\begin{aligned}
&[47736318\, c_1 c_2 c_6 c_7 + 14719214\, c_1 c_2 c_6 s_7 + 14721294\, c_2 c_6 c_7 s_1 - 47779557\, c_2 c_6 s_1 s_7 - \\
&2063733\, c_1 c_2 s_6 - 260282\, c_2 s_1 s_6 + 49996703\, c_3 c_4 c_5 + 2048843\, c_6 c_7 s_2 + 359142\, c_6 s_2 s_7 + \\
&49953414\, s_2 s_6 - 49996703\, s_3 s_5,\ 14721294\, c_1 c_6 c_7 - 47779557\, c_1 c_6 s_7 + 49996703\, c_4 c_5 s_3 - \\
&47736318\, c_6 c_7 s_1 - 14719214\, c_6 s_1 s_7 - 260282\, c_1 s_6 + 49996703\, c_3 s_5 + \\
&2063733\, s_1 s_6,\ 47736318\, c_1 c_6 c_7 s_2 + 14719214\, c_1 c_6 s_2 s_7 + 14721294\, c_6 c_7 s_1 s_2 - \\
&47779557\, c_6 s_1 s_2 s_7 - 2063733\, c_1 s_2 s_6 - 2048843\, c_2 c_6 c_7 - 359142\, c_2 c_6 s_7 - 260282\, s_1 s_2 s_6 - \\
&49953414\, c_2 s_6 - 49996703\, c_5 s_4,\ 47736318\, c_1 c_2 c_7 s_6 + 14719214\, c_1 c_2 s_6 s_7 + \\
&14721294\, c_2 c_7 s_1 s_6 - 47779557\, c_2 s_1 s_6 s_7 + 2063733\, c_1 c_2 c_6 + 260282\, c_2 c_6 s_1 + \\
&2048843\, c_7 s_2 s_6 + 359142\, s_2 s_6 s_7 - 49996703\, c_3 s_4 - 49953414\, c_6 s_2,\ 14721294\, c_1 c_7 s_6 - \\
&47779557\, c_1 s_6 s_7 - 47736318\, c_7 s_1 s_6 - 14719214\, s_1 s_6 s_7 + 260282\, c_1 c_6 - 2063733\, c_6 s_1 - \\
&49996703\, s_3 s_4,\ 47736318\, c_1 c_7 s_2 s_6 + 14719214\, c_1 s_2 s_6 s_7 + 14721294\, c_7 s_1 s_2 s_6 - \\
&47779557\, s_1 s_2 s_6 s_7 + 2063733\, c_1 c_6 s_2 - 2048843\, c_2 c_7 s_6 - 359142\, c_2 s_6 s_7 + 260282\, c_6 s_1 s_2 + \\
&49953414\, c_2 c_6 - 49996703\, c_4,\ -14719214\, c_1 c_2 c_7 + 47736318\, c_1 c_2 s_7 + 47779557\, c_2 c_7 s_1 + \\
&14721294\, c_2 s_1 s_7 - 49996703\, c_3 c_4 s_5 - 49996703\, c_5 s_3 - 359142\, c_7 s_2 + \\
&2048843\, s_2 s_7,\ -49996703\, c_4 s_3 s_5 + 47779557\, c_1 c_7 + 14721294\, c_1 s_7 + 49996703\, c_3 c_5 + \\
&14719214\, c_7 s_1 - 47736318\, s_1 s_7,\ -14719214\, c_1 c_7 s_2 + 47736318\, c_1 s_2 s_7 + 47779557\, c_7 s_1 s_2 + \\
&14721294\, s_1 s_2 s_7 + 359142\, c_2 c_7 - 2048843\, c_2 s_7 + 49996703\, s_4 s_5,\ 171288941990000\, c_1 c_2 + \\
&27004307691926\, c_2 s_1 + 99993406000000\, c_3 s_4 - 91729827067889\, s_2,\ 49996703000000\, s_3 s_4 + \\
&13502153845963\, c_1 - 85644470995000\, s_1,\ 171288941990000\, c_1 s_2 + 27004307691926\, s_1 s_2 + \\
&91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000,\ {c_1}^2 + {s_1}^2 - 1,\ {c_2}^2 + {s_2}^2 - 1,\ {c_3}^2 + \\
&{s_3}^2 - 1,\ {c_4}^2 + {s_4}^2 - 1,\ {c_5}^2 + {s_5}^2 - 1,\ {c_6}^2 + {s_6}^2 - 1,\ {c_7}^2 + {s_7}^2 - 1]
\end{aligned}
$$

Optimal solution to inverse kinematics

$$
\begin{aligned}
&[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - \\
&2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + \\
&49953414\, s_2\, s_6 - 49996703\, s_3\, s_5,\ 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - \\
&47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + \\
&2063733\, s_1\, s_6,\ 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - \\
&47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - \\
&49953414\, c_2\, s_6 - 49996703\, c_5\, s_4,\ 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + \\
&14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + \\
&2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2,\ 14721294\, c_1\, c_7\, s_6 - \\
&47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - \\
&49996703\, s_3\, s_4,\ 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - \\
&47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + \\
&49953414\, c_2\, c_6 - 49996703\, c_4,\ -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + \\
&14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + \\
&2048843\, s_2\, s_7,\ -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + \\
&14719214\, c_7\, s_1 - 47736318\, s_1\, s_7,\ -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + \\
&14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5,\ 171288941990000\, c_1\, c_2 + \\
&27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2,\ 49996703000000\, s_3\, s_4 + \\
&13502153845963\, c_1 - 85644470995000\, s_1,\ 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + \\
&91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000,\ {c_1}^2 + {s_1}^2 - 1,\ {c_2}^2 + {s_2}^2 - 1,\ {c_3}^2 + \\
&{s_3}^2 - 1,\ {c_4}^2 + {s_4}^2 - 1,\ {c_5}^2 + {s_5}^2 - 1,\ {c_6}^2 + {s_6}^2 - 1,\ {c_7}^2 + {s_7}^2 - 1]
\end{aligned}
$$

Optimal solution to inverse kinematics

$$
\begin{gathered}
[47736318\, c_1\, c_2\, c_6\, c_7 + 14719214\, c_1\, c_2\, c_6\, s_7 + 14721294\, c_2\, c_6\, c_7\, s_1 - 47779557\, c_2\, c_6\, s_1\, s_7 - \\
2063733\, c_1\, c_2\, s_6 - 260282\, c_2\, s_1\, s_6 + 49996703\, c_3\, c_4\, c_5 + 2048843\, c_6\, c_7\, s_2 + 359142\, c_6\, s_2\, s_7 + \\
49953414\, s_2\, s_6 - 49996703\, s_3\, s_5,\, 14721294\, c_1\, c_6\, c_7 - 47779557\, c_1\, c_6\, s_7 + 49996703\, c_4\, c_5\, s_3 - \\
47736318\, c_6\, c_7\, s_1 - 14719214\, c_6\, s_1\, s_7 - 260282\, c_1\, s_6 + 49996703\, c_3\, s_5 + \\
2063733\, s_1\, s_6,\, 47736318\, c_1\, c_6\, c_7\, s_2 + 14719214\, c_1\, c_6\, s_2\, s_7 + 14721294\, c_6\, c_7\, s_1\, s_2 - \\
47779557\, c_6\, s_1\, s_2\, s_7 - 2063733\, c_1\, s_2\, s_6 - 2048843\, c_2\, c_6\, c_7 - 359142\, c_2\, c_6\, s_7 - 260282\, s_1\, s_2\, s_6 - \\
49953414\, c_2\, s_6 - 49996703\, c_5\, s_4,\, 47736318\, c_1\, c_2\, c_7\, s_6 + 14719214\, c_1\, c_2\, s_6\, s_7 + \\
14721294\, c_2\, c_7\, s_1\, s_6 - 47779557\, c_2\, s_1\, s_6\, s_7 + 2063733\, c_1\, c_2\, c_6 + 260282\, c_2\, c_6\, s_1 + \\
2048843\, c_7\, s_2\, s_6 + 359142\, s_2\, s_6\, s_7 - 49996703\, c_3\, s_4 - 49953414\, c_6\, s_2,\, 14721294\, c_1\, c_7\, s_6 - \\
47779557\, c_1\, s_6\, s_7 - 47736318\, c_7\, s_1\, s_6 - 14719214\, s_1\, s_6\, s_7 + 260282\, c_1\, c_6 - 2063733\, c_6\, s_1 - \\
49996703\, s_3\, s_4,\, 47736318\, c_1\, c_7\, s_2\, s_6 + 14719214\, c_1\, s_2\, s_6\, s_7 + 14721294\, c_7\, s_1\, s_2\, s_6 - \\
47779557\, s_1\, s_2\, s_6\, s_7 + 2063733\, c_1\, c_6\, s_2 - 2048843\, c_2\, c_7\, s_6 - 359142\, c_2\, s_6\, s_7 + 260282\, c_6\, s_1\, s_2 + \\
49953414\, c_2\, c_6 - 49996703\, c_4,\, -14719214\, c_1\, c_2\, c_7 + 47736318\, c_1\, c_2\, s_7 + 47779557\, c_2\, c_7\, s_1 + \\
14721294\, c_2\, s_1\, s_7 - 49996703\, c_3\, c_4\, s_5 - 49996703\, c_5\, s_3 - 359142\, c_7\, s_2 + \\
2048843\, s_2\, s_7,\, -49996703\, c_4\, s_3\, s_5 + 47779557\, c_1\, c_7 + 14721294\, c_1\, s_7 + 49996703\, c_3\, c_5 + \\
14719214\, c_7\, s_1 - 47736318\, s_1\, s_7,\, -14719214\, c_1\, c_7\, s_2 + 47736318\, c_1\, s_2\, s_7 + 47779557\, c_7\, s_1\, s_2 + \\
14721294\, s_1\, s_2\, s_7 + 359142\, c_2\, c_7 - 2048843\, c_2\, s_7 + 49996703\, s_4\, s_5,\, 171288941990000\, c_1\, c_2 + \\
27004307691926\, c_2\, s_1 + 99993406000000\, c_3\, s_4 - 91729827067889\, s_2,\, 49996703000000\, s_3\, s_4 + \\
13502153845963\, c_1 - 85644470995000\, s_1,\, 171288941990000\, c_1\, s_2 + 27004307691926\, s_1\, s_2 + \\
91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000,\, {c_1}^2 + {s_1}^2 - 1,\, {c_2}^2 + {s_2}^2 - 1,\, {c_3}^2 + \\
{s_3}^2 - 1,\, {c_4}^2 + {s_4}^2 - 1,\, {c_5}^2 + {s_5}^2 - 1,\, {c_6}^2 + {s_6}^2 - 1,\, {c_7}^2 + {s_7}^2 - 1]
\end{gathered}
$$

Optimal solution to inverse kinematics

$$
\begin{aligned}
&[47736318\, c_1 c_2 c_6 c_7 + 14719214\, c_1 c_2 c_6 s_7 + 14721294\, c_2 c_6 c_7 s_1 - 47779557\, c_2 c_6 s_1 s_7 - \\
&2063733\, c_1 c_2 s_6 - 260282\, c_2 s_1 s_6 + 49996703\, c_3 c_4 c_5 + 2048843\, c_6 c_7 s_2 + 359142\, c_6 s_2 s_7 + \\
&49953414\, s_2 s_6 - 49996703\, s_3 s_5,\ 14721294\, c_1 c_6 c_7 - 47779557\, c_1 c_6 s_7 + 49996703\, c_4 c_5 s_3 - \\
&47736318\, c_6 c_7 s_1 - 14719214\, c_6 s_1 s_7 - 260282\, c_1 s_6 + 49996703\, c_3 s_5 + \\
&2063733\, s_1 s_6,\ 47736318\, c_1 c_6 c_7 s_2 + 14719214\, c_1 c_6 s_2 s_7 + 14721294\, c_6 c_7 s_1 s_2 - \\
&47779557\, c_6 s_1 s_2 s_7 - 2063733\, c_1 s_2 s_6 - 2048843\, c_2 c_6 c_7 - 359142\, c_2 c_6 s_7 - 260282\, s_1 s_2 s_6 - \\
&49953414\, c_2 s_6 - 49996703\, c_5 s_4,\ 47736318\, c_1 c_2 c_7 s_6 + 14719214\, c_1 c_2 s_6 s_7 + \\
&14721294\, c_2 c_7 s_1 s_6 - 47779557\, c_2 s_1 s_6 s_7 + 2063733\, c_1 c_2 c_6 + 260282\, c_2 c_6 s_1 + \\
&2048843\, c_7 s_2 s_6 + 359142\, s_2 s_6 s_7 - 49996703\, c_3 s_4 - 49953414\, c_6 s_2,\ 14721294\, c_1 c_7 s_6 - \\
&47779557\, c_1 s_6 s_7 - 47736318\, c_7 s_1 s_6 - 14719214\, s_1 s_6 s_7 + 260282\, c_1 c_6 - 2063733\, c_6 s_1 - \\
&49996703\, s_3 s_4,\ 47736318\, c_1 c_7 s_2 s_6 + 14719214\, c_1 s_2 s_6 s_7 + 14721294\, c_7 s_1 s_2 s_6 - \\
&47779557\, s_1 s_2 s_6 s_7 + 2063733\, c_1 c_6 s_2 - 2048843\, c_2 c_7 s_6 - 359142\, c_2 s_6 s_7 + 260282\, c_6 s_1 s_2 + \\
&49953414\, c_2 c_6 - 49996703\, c_4,\ -14719214\, c_1 c_2 c_7 + 47736318\, c_1 c_2 s_7 + 47779557\, c_2 c_7 s_1 + \\
&14721294\, c_2 s_1 s_7 - 49996703\, c_3 c_4 s_5 - 49996703\, c_5 s_3 - 359142\, c_7 s_2 + \\
&2048843\, s_2 s_7,\ -49996703\, c_4 s_3 s_5 + 47779557\, c_1 c_7 + 14721294\, c_1 s_7 + 49996703\, c_3 c_5 + \\
&14719214\, c_7 s_1 - 47736318\, s_1 s_7,\ -14719214\, c_1 c_7 s_2 + 47736318\, c_1 s_2 s_7 + 47779557\, c_7 s_1 s_2 + \\
&14721294\, s_1 s_2 s_7 + 359142\, c_2 c_7 - 2048843\, c_2 s_7 + 49996703\, s_4 s_5,\ 171288941990000\, c_1 c_2 + \\
&27004307691926\, c_2 s_1 + 99993406000000\, c_3 s_4 - 91729827067889\, s_2,\ 49996703000000\, s_3 s_4 + \\
&13502153845963\, c_1 - 85644470995000\, s_1,\ 171288941990000\, c_1 s_2 + 27004307691926\, s_1 s_2 + \\
&91729827067889\, c_2 + 99993406000000\, c_4 + 99993406000000,\ {c_1}^2 + {s_1}^2 - 1,\ {c_2}^2 + {s_2}^2 - 1,\ {c_3}^2 + \\
&{s_3}^2 - 1,\ {c_4}^2 + {s_4}^2 - 1,\ {c_5}^2 + {s_5}^2 - 1,\ {c_6}^2 + {s_6}^2 - 1,\ {c_7}^2 + {s_7}^2 - 1]
\end{aligned}
$$

Optimal solution to inverse kinematics

- We had thousands of optimization problems to solve

Optimal solution to inverse kinematics

- We had thousands of optimization problems to solve
- 70% of such problems could be solved

efficiently with **GloptiPoly**

Optimal solution to inverse kinematics

- We had thousands of optimization problems to solve
- 70% of such problems could be solved

  efficiently with **GloptiPoly**
- Numerical issues + dramatic slow down on the other 30%

Optimal solution to inverse kinematics

- We had thousands of optimization problems to solve
- 70% of such problems could be solved

  efficiently with **GloptiPoly**

- Numerical issues + dramatic slow down on the other 30%
- Critical points $\rightsquigarrow$ Gröbner basis solver $\rightsquigarrow$ $\simeq$ 30 secs(!) **msolve**

  Still too long for the actual application

Optimal solution to inverse kinematics

- We had thousands of optimization problems to solve
- 70% of such problems could be solved

  efficiently with **GloptiPoly**
- Numerical issues + dramatic slow down on the other 30%
- Critical points $\rightsquigarrow$ Gröbner basis solver $\rightsquigarrow$ $\simeq$ 30 secs(!) **msolve**

  Still too long for the actual application
- System of constraints is always the same.
  - The ideal is generated by quadrics **Property of Gröbner bases**!!
  - $\Longrightarrow$ one can reformulate the problem with quadrics

    (and hence avoid quartics)

Optimal solution to inverse kinematics

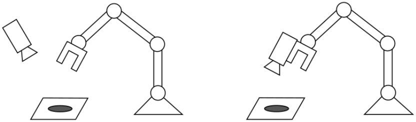
- We had thousands of optimization problems to solve
- 70% of such problems could be solved

  efficiently with **GloptiPoly**
- Numerical issues + dramatic slow down on the other 30%
- Critical points $\rightsquigarrow$ Gröbner basis solver $\rightsquigarrow$ $\simeq$ 30 secs(!) **msolve**

  Still too long for the actual application
- System of constraints is always the same.
  - The ideal is generated by quadrics **Property of Gröbner bases**!!
  - $\Longrightarrow$ one can reformulate the problem with quadrics

    (and hence avoid quartics)
- Using this reformulation, **GloptiPoly** can solve 99% of the systems
  - Gröbner basis solver was used for the remaining 1%.

Vision-based control schemes in robotics



☛ eye-in-hand with configuration camera

☛ dynamic control observation

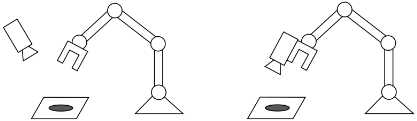
observation $\rightsquigarrow$ desired position

Lyapunov theory $\rightsquigarrow$ **critical points of a polynomial map**

local extrema $\rightsquigarrow$ stability analysis

Briot/Colotti/Garcia-Fontan/Goldsztein/S.

Vision-based control schemes in robotics



- ☛ eye-in-hand with configuration camera
- ☛ dynamic control observation

observation $\rightsquigarrow$ desired position

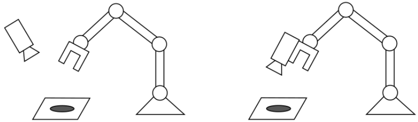
Lyapunov theory $\rightsquigarrow$ **critical points of a polynomial map**

local extrema $\rightsquigarrow$ stability analysis

System	msolve(×12)	HC.jl (×1)	Out. (algebraic)	Out. (numeric)
sys1	15 days	1630 secs	402/50	403/50
sys2	24 days	1495 secs	1016/44	1016/44
sys3	27 days	1950 secs	1064/48	871/32
sys4	41 days	2280 secs	3656/84	3537/95

Briot/Colotti/Garcia-Fontan/Goldsztein/S.

Vision-based control schemes in robotics



- eye-in-hand with configuration camera
- dynamic control observation

observation $\rightsquigarrow$ desired position

Lyapunov theory $\rightsquigarrow$ **critical points of a polynomial map**

local extrema $\rightsquigarrow$ stability analysis

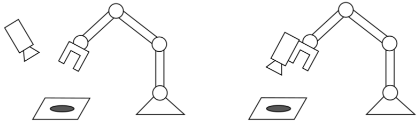
System	msolve(×12)	HC.jl (×1)	Out. (algebraic)	Out. (numeric)
sys1	15 days	1630 secs	402/50	403/50
sys2	24 days	1495 secs	1016/44	1016/44
sys3	27 days	1950 secs	1064/48	871/32
sys4	41 days	2280 secs	3656/84	3537/95

Using co-planarity conditions

System	msolve(×12)	HC.jl (×1)	Out. (algebraic)	Out. (numeric)
sys1	478 secs	14499 secs	402/50	402/50
sys2	21.2 h	15480 secs	1016/44	1016/44
sys3	18.4h	20099 secs	1064/48	871/32
~~sys4~~	~~41 days~~	~~2280 secs~~	~~3656/84~~	~~3537/95~~

Briot/Colotti/Garcia-Fontan/Goldsztein/S.

Vision-based control schemes in robotics



- ☛ eye-in-hand with configuration camera
- ☛ dynamic control observation

observation $\rightsquigarrow$ desired position

Lyapunov theory $\rightsquigarrow$ **critical points of a polynomial map**

local extrema $\rightsquigarrow$ stability analysis

System	msolve(×12)	HC.jl (×1)	Out. (algebraic)	Out. (numeric)
sys1	15 days	1630 secs	402/50	403/50
sys2	24 days	1495 secs	1016/44	1016/44
sys3	27 days	1950 secs	1064/48	871/32
sys4	41 days	2280 secs	3656/84	3537/95

Using co-planarity conditions

System	msolve(×12)	HC.jl (×1)	Out. (algebraic)	Out. (numeric)
sys1	478 secs	14499 secs	402/50	402/50
sys2	21.2 h	15480 secs	1016/44	1016/44
sys3	18.4h	20099 secs	1064/48	871/32
~~sys4~~	~~41 days~~	~~2280 secs~~	~~3656/84~~	~~3537/95~~

System	msolve(×12)	msolve(×12)	msolve(×12)
sys1	15 days	1630 secs	172 secs
sys2	24 days	1495 secs	10243 secs
sys3	27 days	1950 secs	8035 secs
sys4	41 days	-	$26h$

- Symetries arise naturally in the formulation.
- Using GBs one can rewrite the polynomial system w.r.t. invariants.
- Last column reports on timings.

Briot/Colotti/Garcia-Fontan/Goldsztein/S.

Recent works and on-going developments

A module approach $fg = gf \rightsquigarrow \mathrm{lt}(f)g = gf - \mathrm{tail}(f)g$

Compact representations of module of syzygies (F5) **Eder/Faugère**

Recent works and on-going developments

A module approach $fg = gf \rightsquigarrow \mathrm{lt}(f)g = gf - \mathrm{tail}(f)g$

Compact representations of module of syzygies (F5) **Eder/Faugère**

- Complexity issues in F5 algorithms
- Specializations of F5 in some structured setting
- Determinantal setting $\rightsquigarrow$ Crypto applications

Gopalakrishnan/Neiger/S.

Recent works and on-going developments

A module approach $fg = gf \rightsquigarrow \mathrm{lt}(f)g = gf - \mathrm{tail}(f)g$

Compact representations of module of syzygies (F5) **Eder/Faugère**

- Complexity issues in F5 algorithms
- Specializations of F5 in some structured setting
- Determinantal setting $\rightsquigarrow$ Crypto applications

Gopalakrishnan/Neiger/S.

Ideal theoretic operations Nothing new since Bayer's PhD (!)

☛ F4 variant to compute saturation of ideals **Berthomieu/Eder/S.**

Recent works and on-going developments

A module approach $fg = gf \rightsquigarrow \mathrm{lt}(f)g = gf - \mathrm{tail}(f)g$

Compact representations of module of syzygies (F5) **Eder/Faugère**

- Complexity issues in F5 algorithms
- Specializations of F5 in some structured setting
- Determinantal setting $\rightsquigarrow$ Crypto applications

Gopalakrishnan/Neiger/S.

Ideal theoretic operations Nothing new since Bayer's PhD (!)

☛ F4 variant to compute saturation of ideals **Berthomieu/Eder/S.**

☛ F5 variant for saturations + equidimensional decomposition

- Some reductions to 0 are unavoidable
- Exploit them $\rightsquigarrow$ decomposition of ideals

Eder/Lairez/Mohr/S.

Recent works and on-going developments

$\boxed{\text{Paradigm shift}}$ ~~sparse~~ $\rightarrow$ structured **Berthomieu/Neiger/S.**

$$\left[\begin{array}{cccc|cc|cc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -22 & -3 & -3 & -26 & -23 & 0 & -15 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
-17 & 0 & -3 & 0 & -15 & -28 & -19 & -5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
-3 & -9 & -19 & -18 & 0 & -27 & -2 & -24
\end{array}\right]$$

Recent works and on-going developments

$\boxed{\text{Paradigm shift}}$ ~~sparse~~ → structured **Berthomieu/Neiger/S.**

$$\left[\begin{array}{cccc|cc|cc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -22 & -3 & -3 & -26 & -23 & 0 & -15 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -17 & 0 & -3 & 0 & -15 & -28 & -19 & -5 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -3 & -9 & -19 & -18 & 0 & -27 & -2 & -24 \end{array}\right] \rightsquigarrow \underset{\text{basis of } \mathbb{K}[x_3]\text{-module of } I \cap (\mathbb{K}[x_3] + x_2\mathbb{K}[x_3] + x_1\mathbb{K}[x_3])}{\begin{bmatrix} x_3^4 + 3x_3^3 + 3x_3^2 + 22x_3 & 23x_3 + 26 & 15x_3 \\ 3x_3^2 + 17 & x_3^2 + 28x_3 + 15 & 5x_3 + 19 \\ 18x_3^3 + 19x_3^2 + 9x_3 + 3 & 27x_3 & x_3^2 + 24x_3 + 2 \end{bmatrix}} \in \mathbb{K}[x_3]^{t \times t}$$

Hermite normal form ⇝ lex Gröbner basis

Complexity: $O\left(t^{\omega-1}D\right)$

Recent works and on-going developments

Paradigm shift ~~sparse~~ $\to$ structured **Berthomieu/Neiger/S.**

$$\left[\begin{array}{cccc|cc|cc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -22 & -3 & -3 & -26 & -23 & 0 & -15 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
-17 & 0 & -3 & 0 & -15 & -28 & -19 & -5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
-3 & -9 & -19 & -18 & 0 & -27 & -2 & -24
\end{array}\right] \rightsquigarrow \begin{bmatrix} x_3^4 + 3x_3^3 + 3x_3^2 + 22x_3 & 23x_3 + 26 & 15x_3 \\ 3x_3^2 + 17 & x_3^2 + 28x_3 + 15 & 5x_3 + 19 \\ 18x_3^3 + 19x_3^2 + 9x_3 + 3 & 27x_3 & x_3^2 + 24x_3 + 2 \end{bmatrix} \in \mathbb{K}[x_3]^{t \times t}$$

basis of $\mathbb{K}[x_3]$-module of $I \cap (\mathbb{K}[x_3] + x_2\mathbb{K}[x_3] + x_1\mathbb{K}[x_3])$

Hermite normal form $\rightsquigarrow$ lex Gröbner basis

Complexity: $O\left(t^{\omega-1}D\right)$

Gröbner bases in semi-algebraic geometry

- Real solutions to positive dimensional systems (with inequalities)
- grab sample points in each connected component
- answer connectivity queries
- compute the projection on some coordinate subspace

`msolve` todo list

1. Lift Gröbner bases over the rationals (started, on-going)
2. Test more and stabilize new algorithms for ideal saturation (started, on-going)
3. Mix F5 and F4 $\rightsquigarrow$ F6 algorithm (started, on-going)
4. Implement new change of orderings algorithms (started, on-going)
5. Implement Hilbert series computations
6. Implement weighted orderings
7. Implement ideal decompositions (zero-dimensional case)
8. Develop the `AlgebraicSolving.jl` package (basic solving)
9. Develop the `AlgebraicSolving.jl` package for semi-algebraic geometry
10. Improve parallelism in hashing
11. Use AVX512 + Apple M2 chip instructions
12. Use MPI to have `msolve` running on clusters
13. Write an interface to the tracer (in `AlgebraicSolving.jl`)
14. Write a C interface with a documented API
15. Integrate Hensel lifting techniques $\rightsquigarrow$ quadratic convergence when lifting rationals
16. Modular arithmetics with floating point arithmetics
17. Linear algebra improvements: matrices are not only sparse
    but structured $\rightsquigarrow$ matrix multiplication $\leftrightarrow$ Gaussian elimination
18. Use code generation techniques
19. Have a dedicated implementation for the boolean field
20. Continue to disseminate `msolve` in computer algebra systems
    (Oscar ✓, SageMath ✓, Macaulay2 ✗, Symbolics.jl ✗)
21. **Hunt bugs, write documentations**, etc, etc, etc, etc...

Recent trends in computer algebra

https://rtca2023.github.io/

- Effective Aspects in Diophantine Approximation (March 27-31)
- Certified and Symbolic-Numeric Computation (May 22-26)
- Mathematical Software and High Performance Algebraic Computing (June 26-30)
- Fundamental Algorithms and Algorithmic Complexity (Sep. 25-29)
- Geometry of Polynomial System Solving, Optimization and Topology (Oct. 16-20)
- Computer Algebra for Functional Equations in Combinatorics and Physics (Dec. 4-8)