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

Jean-Charles Faugère

F_5
Overdetermined systems
Boolean Solve
Algebraic Cryptanalysis of HFE (2nd part)

2022 - 2023 – MPRI

Algorithms

Algorithms: for *computing* Gröbner bases.

- Buchberger (1965,1979,1985)
  ☞ First and Second Criteria
- F_4 using linear algebra (1999) (strategies)
- F_5 no reduction to zero (2002)
  - Today $\longrightarrow$ simple matrix F_5 algorithm
- Signature-based Gröbner computations (2008-…)

F_5 *algorithm*

- Goal: avoid useless reduction to 0
  generate full rank matrices
- Incremental algorithm

$$(f_1) + G_{\text{prev}}$$

- We have to explain: new F_5 criterion

F_5 an example I

We consider the following example: (b is a parameter):

$$\mathcal{S}_b \left\{ \begin{array}{l} f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2 \\ f_2 = 3\,x^2 + (7 + \ b)\,x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2 \\ f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2 \end{array} \right.$$

For now we assume that $b = 0$
With Buchberger $x > y > z$:

- 5 useless reductions
- 5 useful pairs

F_5 *an example II*

We proceed degree by degree.

$$A_2 = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & 3 & 7 & 8 & 22 & 11 & 22 \\ f_1 & 6 & 12 & 4 & 14 & 9 & 7 \end{array}$$

$$\widetilde{A_2} = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & & 1 & 3 & 2 & 4 & -1 \\ f_1 & & & 1 & -11 & -3 & -5 \end{array}$$

“new” polynomials $f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$ and $f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$

F_5 an example III

$$f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2$$
$$f_2 = 3\,x^2 + 7x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2$$
$$f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2$$
$$f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$$
$$f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$$

$$f_2 \longrightarrow f_4$$
$$f_1 \longrightarrow f_5$$

Degree 3 (first try)

$$f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2$$
$$f_2 = 3\,x^2 + 7x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2$$
$$f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2$$
$$f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$$
$$f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$$

and

$$f_2 \longrightarrow f_4$$
$$f_1 \longrightarrow f_5$$

Degree 3 (first try)

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & 1 & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & 3 & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{array} \right) \end{array}$$

Degree 3 (first try)

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \textcircled{1} & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & 3 & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 (first try)

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \textcircled{1} & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{3} & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 (first try)

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \textcircled{1} & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{3} & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & 6 & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 (first try)

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \textcircled{1} & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{3} & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{6} & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3 (first try)

$$
A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array}
\begin{array}{c}
\begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\
\left(\begin{array}{cccccc}
0 & 0 & 0 & 0 & \textcircled{1} & \dots \\
0 & 1 & 18 & 19 & 0 & \dots \\
1 & 18 & 19 & 0 & 8 & \dots \\
0 & 0 & 0 & 0 & \textcircled{3} & \dots \\
0 & 3 & 7 & 8 & 0 & \dots \\
3 & 7 & 8 & 0 & 22 & \dots \\
0 & 0 & 0 & 0 & \textcircled{6} & \dots \\
0 & 6 & 12 & 4 & 0 & \dots \\
6 & 12 & 4 & 0 & 14 & \dots
\end{array}\right)
\end{array}
$$

Degree 3 (first try)

Already
Done !

$f_2 \longrightarrow f_4$

$f_1 \longrightarrow f_5$

$$A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} x^3 \quad x^2y \quad xy^2 \quad y^3 \quad x^2z \quad \dots \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \textcircled{1} & \dots \\ 0 & 1 & 18 & 19 & 0 & \dots \\ 1 & 18 & 19 & 0 & 8 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{3} & \dots \\ 0 & 3 & 7 & 8 & 0 & \dots \\ 3 & 7 & 8 & 0 & 22 & \dots \\ 0 & 0 & 0 & 0 & \textcircled{6} & \dots \\ 0 & 6 & 12 & 4 & 0 & \dots \\ 6 & 12 & 4 & 0 & 14 & \dots \end{pmatrix} \end{array}$$

Degree 3

$$
A_3 := \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_4 \\ yf_4 \\ xf_4 \\ zf_5 \\ yf_5 \\ xf_5 \end{array}
\begin{array}{c}
\begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\
\left(\begin{array}{cccccccccc}
 & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & 1 & 3 & 2 & 4 & 22 \\
 & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 & 0 \\
 & & & & & & 1 & 12 & 20 & 18 \\
 & & & 1 & 0 & 12 & 20 & 0 & 18 & 0 \\
 & & 1 & 0 & 12 & 20 & 0 & 18 & 0 & 0
\end{array} \right)
\end{array}
$$

Degree 3

$\tilde{A}_3 :=$

	x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3
xf_3	1	18	19	0	8	5	0	7	0	0
yf_3		1	18	19	0	8	5	0	7	0
yf_2			1	3	0	2	4	0	22	0
xf_2				1	0	0	8	1	18	15
zf_3					1	18	19	8	5	7
zf_2						1	3	2	4	22
zf_1							1	12	20	18
yf_1								1	11	13
xf_1									1	18

Degree 3

Summary: we have constructed 3 new polynomials

$$
\begin{aligned}
f_6 &= y^3 + 8\,y^2 z + xz^2 + 18\,yz^2 + 15\,z^3 \\
f_7 &= xz^2 + 11\,yz^2 + 13\,z^3 \\
f_8 &= yz^2 + 18\,z^3
\end{aligned}
$$

And we have the linear equivalences:

$$
x\,f_2 \leftrightarrow x\,f_4 \leftrightarrow f_6
$$
$$
f_4 \longrightarrow f_2
$$

Degree 4

The matrix whose rows are

$$x^2 f_i, x\,y f_i, y^2 f_i, x\,z f_i, y\,z f_i, z^2 f_i, \; i = 1, 2, 3$$

is not full rank !

Why ? (1)

$6 \times 3 = 18$ rows
$x^4, x^3 y, \ldots, y z^3, z^4$ 15 columns

Why ? (1)

$6 \times 3 = \boxed{\text{18 rows}}$

$x^4, x^3\,y, \ldots, y\,z^3, z^4$ $\boxed{\text{15 columns}}$

Simple linear algebra theorem: 3 useless row (but which ones ?)

Trivial relations

$$f_2\, f_3 - f_3\, f_2 = 0$$

can be rewritten

$$\begin{aligned} &3\,x^2\,f_3 + (7 + \ b)\,xy\,f_3 + 8\,y^2\,f_3 + 22\,xz\,f_3 \\ &+11\,yz\,f_3 + 22\,z^2\,f_3 - \boxed{x^2\,f_2} - 18\,xy\,f_2 - 19\,y^2\,f_2 \\ &-8\,xz\,f_2 - 5\,yz\,f_2 - 7\,z^2\,f_2 = 0 \end{aligned}$$

We can remove the row $x^2 f_2$

same way $f_1 f_3 - f_3 f_1 = 0 \longrightarrow$ remove $x^2 f_1$

but $f_1 f_2 - f_2 f_1 = 0 \longrightarrow$ remove $x^2 f_1$! ???

Combining trivial relations

$$
\begin{aligned}
0 &= (f_2 f_1 - f_1 f_2) - 3(f_3 f_1 - f_1 f_3) \\
0 &= (f_2 - 3f_3) f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= \boxed{f_4}\, f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= \boxed{\Big((1 - b)xy + 4\,yz + 2\,xz + 3\,y^2 - z^2\Big)}\, f_1 \\
&\quad -(6x^2 + \cdots) f_2 + 3(6x^2 + \cdots) f_3
\end{aligned}
$$

- if $b \neq 1$ remove $x\,y\;f_1$
- if $b = 1$ remove $y\,z\;f_1$

Need “some” computation

Degree 4 I

$$y^2 f_1, x\,zf_1, y\,zf_1, z^2 f_1, x\,yf_2, y^2 f_2, x\,zf_2,$$
$$y\,zf_2, z^2 f_2, x^2 f_3, x\,yf_3, y^2 f_3, x\,zf_3, y\,zf_3, z^2 f_3$$

In order to use previous computations (degree 2 and 3):

$$xf_2 \to f_6 \quad f_2 \to f_4$$
$$xf_1 \to f_8 \quad yf_1 \to f_7$$
$$f_1 \to f_5$$

$$yf_7, zf_8, zf_7, z^2 f_5, yf_6, y^2 f_4, zf_6, y\,zf_4,$$
$$z^2 f_4, x^2 f_3, x\,yf_3, y^2 f_3, x\,zf_3, y\,zf_3, z^2 f_3,$$

Degree 4 II

$$A_4 := \begin{bmatrix}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{bmatrix}$$

Degree 4 III

$$A_4 := \left[\begin{array}{cccccccccc|ccccc}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
\cline{11-15}
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{array}\right]$$

Degree 4 IV

We need to consider only a small sub-matrix:

$$A_4' := \begin{array}{c} \\ yf_7 \\ z^2 f_5 \\ zf_7 \\ zf_8 \\ z^2 f_4 \end{array} \begin{array}{c} \begin{array}{ccccc} xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \end{array} \\ \begin{pmatrix} 1 & 11 & 0 & 13 & 0 \\ & 1 & 12 & 20 & 18 \\ & & 1 & 11 & 13 \\ & & & 1 & 18 \\ 1 & 3 & 2 & 4 & 22 \end{pmatrix} \end{array}$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$
Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$
Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

(trivial) relation $h\, f_1 + \cdots = 0 \leftrightarrow \; h \in \mathrm{Id}(f_2, f_3)$

F5 Criterion : analysis

Example: compute a Gröbner basis of $[f_1, f_2, f_3]$

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_3 - f_3 f_2) + v(f_1 f_3 - f_3 f_1) + w(f_2 f_1 - f_1 f_2) = 0$$

where u, v, w are arbitrary polynomials.

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 + u\, f_2 f_3 - u\, f_3 f_2 + v\, f_1 f_3 - w f_1 f_2 = 0$$

$$\boxed{(w\, f_2 - v\, f_3)}\, f_1 \longrightarrow 0$$

(trivial) relation $h\, f_1 + \cdots = 0 \leftrightarrow \; h \in \mathrm{Id}(f_2, f_3)$

F_5 Criterion: compute a Gröbner basis G' of $Id(f_2, f_3)$.

Remove row $t\, f_1$ iff t reducible by $\mathrm{LT}(G')$

Keep row $t\, f_1$ iff t not reducible by $\mathrm{LT}(G')$

matrix-F_5 *algorithm*

- Incremental algorithm

$$(f_1) + G_{\text{prev}}$$

- Incremental degree by degree

Special/Simpler version of F_5 for dense/generic quadratic polynomials.
the maximal degree D is a *parameter* of the algorithm.

$$\begin{array}{l} \\ u_1 f_1 \\ \vdots \\ u_{r_1} f_1 \\ \vdots \\ v_{r_{k-1}} f_{k-1} \\ w_1 f_k \\ w_2 f_k \end{array} \begin{array}{c} \begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\ \left(\begin{array}{cccccc} 1 & x & x & x & x & \ldots \\ 0 & \ddots & x & x & x & \ldots \\ 0 & 0 & 1 & x & x & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\ 0 & 0 & 1 & x & x & \ldots \\ 0 & 0 & 0 & 1 & x & \ldots \\ 0 & 0 & 0 & 0 & 1 & \ldots \end{array}\right) \end{array}$$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$

Already computed
Groebner $(\langle f_1, \ldots, f_k \rangle), d)$

Matrix in degree d

$$
\begin{array}{l}
\\
u_1 f_1 \\
\vdots \\
u_{r_1} f_1 \\
\vdots \\
v_{r_{k-1}} f_{k-1} \\
w_1 f_k \\
w_2 f_k
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\
\begin{pmatrix}
1 & x & x & x & x & \ldots \\
 & \ddots & & & & \\
0 & & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{pmatrix}
\end{array}
$$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$

Matrix in degree d

$$
\begin{array}{l}
 \\
u_1 f_1 \\
\vdots \\
u_{r_1} f_1 \\
\vdots \\
v_{r_{k-1}} f_{k-1} \\
w_1 f_k \\
w_2 f_k
\end{array}
\quad
\begin{array}{c}
\begin{array}{cccccc}
m_1 & m_2 & m_3 & m_4 & m_5 & \ldots
\end{array} \\
\left(\begin{array}{cccccc}
1 & x & x & x & x & \ldots \\
 & \ddots & & & & \\
0 & & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{array}\right)
\end{array}
$$

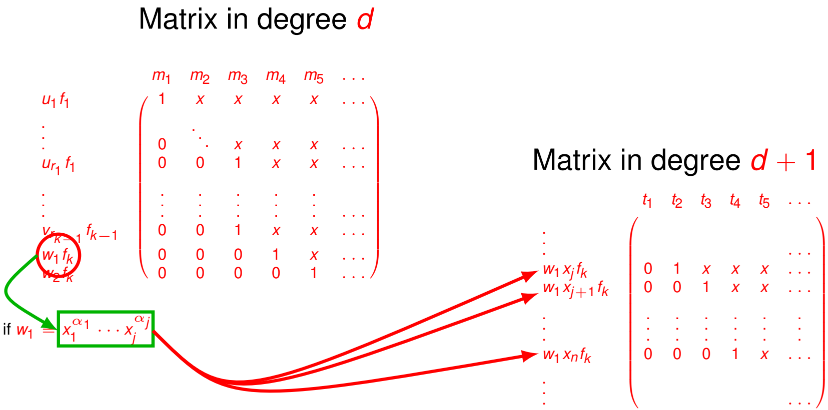
F5: compute Groebner$(\langle f_1, \ldots, f_k\rangle), d+1)$

Matrix in degree d

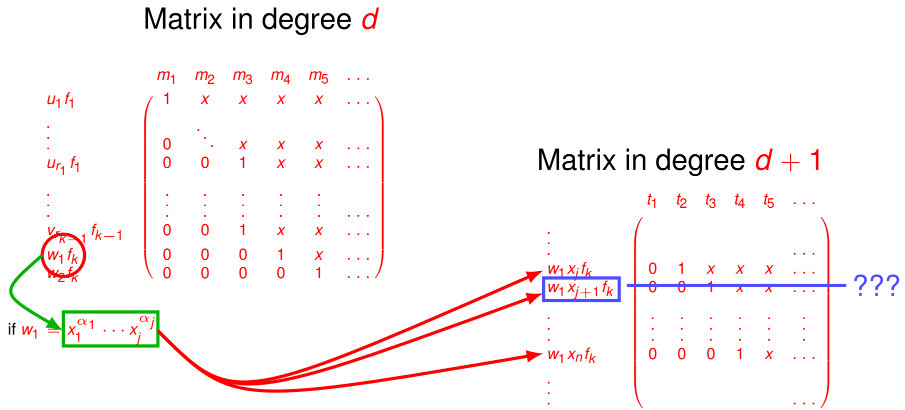
$$
\begin{array}{l}
\\
u_1 f_1 \\
\vdots \\
u_{r_1} f_1 \\
\vdots \\
v_{r_{k-1}} f_{k-1} \\
w_1 f_k \\
w_2 f_k
\end{array}
\quad
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\
\begin{pmatrix}
1 & x & x & x & x & \ldots \\
0 & \ddots & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{pmatrix}
\end{array}
$$

if $w_1 = x_1^{\alpha_1} \ldots x_j^{\alpha_j}$

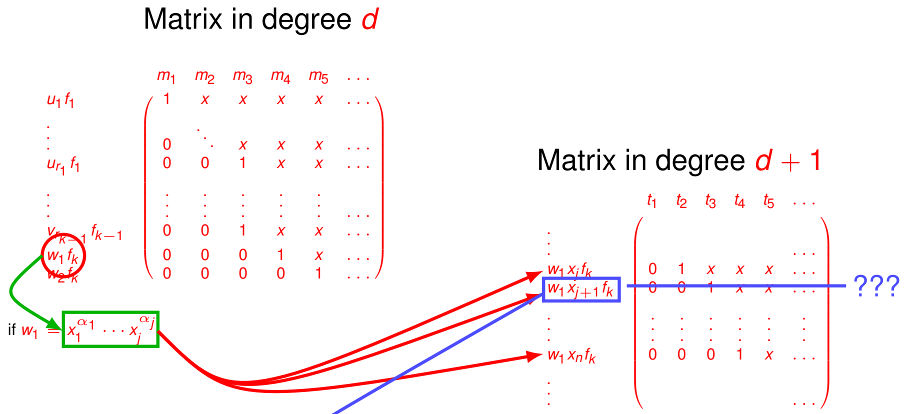
F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



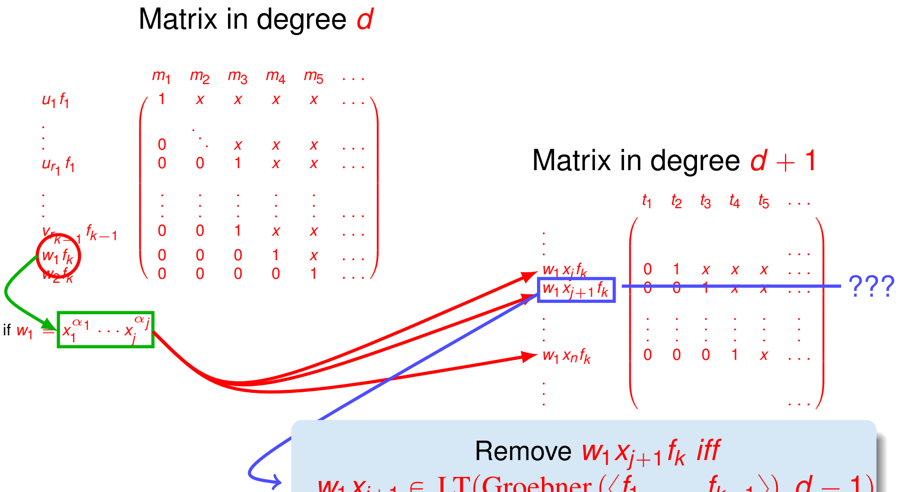
F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



Remove $w_1 x_{j+1} f_k$ *iff*

$w_1 x_{j+1} \in \mathrm{LT}(\langle f_1, \ldots, f_{k-1} \rangle)$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



Remove $w_1 x_{j+1} f_k$ *iff*

$w_1 x_{j+1} \in \mathrm{LT}(\text{Groebner}(\langle f_1, \ldots, f_{k-1} \rangle), d-1)$

(Final) F5: compute Groebner $(\langle f_1, \dots, f_k \rangle), d+1)$

Matrix in degree $d-1$

$$\begin{array}{c|cccccc}
 & m_1 & m_2 & m_3 & m_4 & m_5 & \dots \\
u'_1 f_1 & \boxed{1} & x & x & x & x & \dots \\
\vdots & 0 & \ddots & x & x & x & \dots \\
u'_{r_1} f_1 & 0 & 0 & \boxed{1} & x & x & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots \\
v'_{r_{k-1}} f_{k-1} & 0 & 0 & 0 & \boxed{1} & x & \dots \\
w'_1 f_k & 0 & 0 & 0 & 0 & \boxed{1} & \dots \\
w'_2 f_k & 0 & 0 & 0 & 0 & \dots & \dots
\end{array}$$

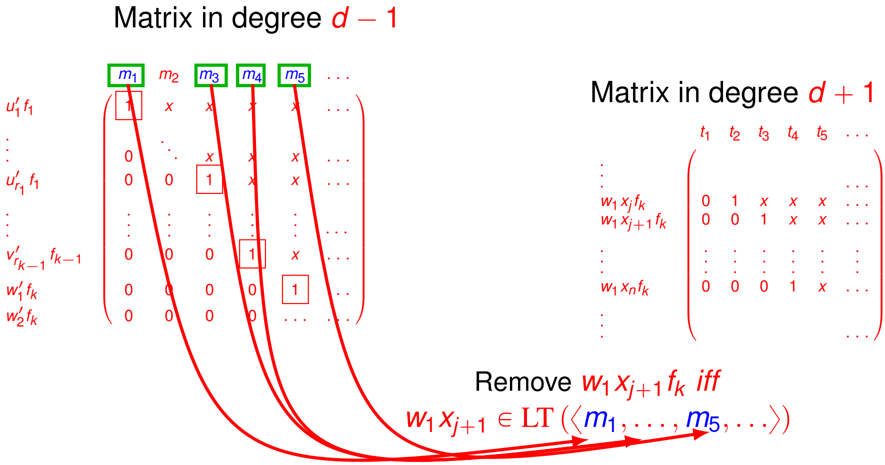
Matrix in degree $d+1$

$$\begin{array}{c|cccccc}
 & t_1 & t_2 & t_3 & t_4 & t_5 & \dots \\
\vdots & & & & & & \dots \\
w_1 x_j f_k & 0 & 1 & x & x & x & \dots \\
w_1 x_{j+1} f_k & 0 & 0 & 1 & x & x & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
w_1 x_n f_k & 0 & 0 & 0 & 1 & x & \dots \\
\vdots & & & & & & \dots
\end{array}$$

Remove $w_1 x_{j+1} f_k$ *iff*

$w_1 x_{j+1} \in \mathrm{LT}(\langle m_1, \dots, m_5, \dots \rangle)$

(Final) F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



Properties of F_5

Theorem

If $F = [f_1, \ldots, f_m]$ is a (semi) regular sequence, then all the matrices generated by the algorithm have full rank.

- Easy to adapt for special cases $\mathbb{F}_2$

  ☞ *new trivial relation: $f_i^2 = f_i$*

- Swap the two loops: degree first and the equation by equation
- Full version of the algorithm F_5 : D is no more a parameter
- However, matrix F_5 is very easy to implement and efficient for dense system: for instance HFE Challenge 1 broken

  80 dense equations in 80 variables

Properties of F_5

Theorem

If $F = [f_1, \ldots, f_m]$ is a (semi) regular sequence, then all the matrices generated by the algorithm have full rank.

- Easy to adapt for special cases $\mathbb{F}_2$
  ☞ *new trivial relation:* $f_i^2 = f_i$
- Swap the two loops: degree first and the equation by equation
- Full version of the algorithm F_5 : D is no more a parameter
- However, matrix F_5 is very easy to implement and efficient for dense system: for instance HFE Challenge 1 broken
  80 dense equations in 80 variables

	Buchberger					
	Maple	slimGb	Macaulay 2	Singular	F_4	F_5
after 10m	12	17	19	19	22	35

Properties of F_5

Theorem

If $F = [f_1, \ldots, f_m]$ *is a (semi) regular sequence, then all the matrices generated by the algorithm have full rank.*

- Easy to adapt for special cases $\mathbb{F}_2$

  ☞ *new trivial relation:* $f_i^2 = f_i$
- Swap the two loops: degree first and the equation by equation
- Full version of the algorithm F_5 : D is no more a parameter
- However, matrix F_5 is very easy to implement and efficient for dense system: for instance HFE Challenge 1 broken

  80 dense equations in 80 variables

	Buchberger					
	Maple	slimGb	Macaulay 2	Singular	F_4	F_5
after 10m	12	17	19	19	22	35
after 2h	14	19	21	21	28	45

Signature-based Grbner basis computations

To obtain the algorithm F_5 we need critical pairs and polynomials.

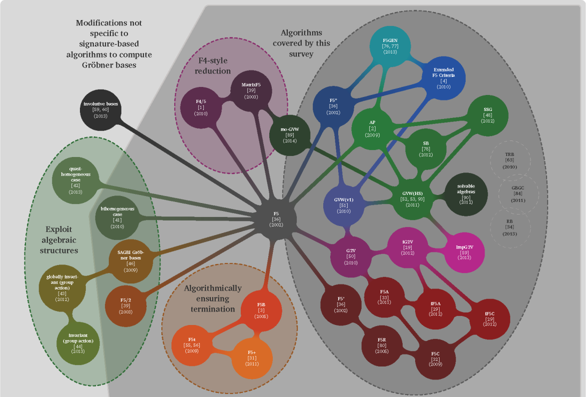
Linear Algebra	Polynomials
Index of a row $s \in T$	Signature s of polynomial p
	$p = \sum_{i=1}^{r} h_i f_i$ and $s = LT(h_r)$
Gauss without pivoting	$\cdots$

Signature-based Grbner basis computations

To obtain the algorithm F_5 we need critical pairs and polynomials.

Linear Algebra	Polynomials
Index of a row $s \in T$	Signature s of polynomial p
	$p = \sum_{i=1}^{r} h_i f_i$ and $s = LT(h_r)$
Gauss without pivoting	$\dots$

with C. Eder "*A survey on signature-based Grbner basis computations*": the area of signature-based Grbner basis algorithms is confusing and vast.



Hilbert function I

Hilbert function of an ideal I : combinatorial and geometric properties of I.
Intrinsic: does not depend on the chosen generator set [4].

For $d \in \mathbb{N}$ we define the set
$\mathbb{K}[x_1, \ldots, x_n]_d = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \deg(f) = d\}$ it is a $\mathbb{K}$ vectorial space of dimension $\binom{n+d-1}{d}$. If I is an ideal, then $I_d = I \cap \mathbb{K}[x_1, \ldots, x_n]_d$ is also a $\mathbb{K}$ vectorial space.

Definition

The Hilbert function of an homogeneous ideal $I = \mathrm{Id}(f_1, \ldots, f_m)$ in degree d is defined by

$$\mathrm{HF}_I(d) = \mathrm{HF}(d) = \dim(\mathbb{K}[x_1, \ldots, x_n]/I)_d = \dim(\mathbb{K}[x_1, \ldots, x_n]_d) - \dim(I_d)$$

Hilbert function II

Theorem (Hilbert)

For some degree d_0 there exists a polynomial P such that

$$\mathrm{HF}_I(d) = P(d) \text{ when } d \geqslant d_0$$

d_0 is the index of regularity; it is denoted by $H(I)$.
The degree of P is also the dimension of the ideal; it is denoted by $\dim(I)$.

Hilbert function III

Definition (Hilbert series)

The Hilbert series is the generated series of HF_I:

$$\mathrm{HS}_I(t) = \sum_{d \geqslant 0} \mathrm{HF}_I(d)\, t^d$$

from the Hilbert theorem we deduce that it is a rational function:

$$\mathrm{HS}_I(t) = \frac{N(t)}{(1-t)^d} \text{ with } N(1) \neq 0$$

where d is the *dimension* of I
and $\deg(I) := N(1)$ is the *degree of the ideal* I.

Hilbert Series

Generating series: $HS(t) = \sum_{d=0}^{\infty} r_d t^d$, where

$$r_d = \#\,\text{Cols} - \text{Rank}(Macaulay(\mathbf{F}, d))$$

Finite number of solution: $HS(t) = \sum_{d=0}^{d_{\text{reg}}-1} r_d t^d$

Degree of regularity

Definition

The degree of regularity of an homogeneous ideal $I = \langle f_1, \ldots, f_m \rangle$ in the ring $\mathbb{K}[x_1, \ldots, x_n]$ is

$$d_{\text{reg}} = \min \{ d \geqslant 0 \mid \dim_{\mathbb{K}}(\{ f \in I, \ \deg(f) = d \}) = M_d(n) \}$$

where $M_d(n) := \binom{n+d-1}{d}$ is the number of monomials in degree d.

Degree of regularity

Definition

The degree of regularity of an homogeneous ideal $I = \langle f_1, \ldots, f_m \rangle$ in the ring $\mathbb{K}[x_1, \ldots, x_n]$ is

$$d_{\text{reg}} = \min \{ d \geqslant 0 \mid \dim_{\mathbb{K}}(\{ f \in I, \ \deg(f) = d \}) = M_d(n) \}$$

where $M_d(n) := \binom{n+d-1}{d}$ is the number of monomials in degree d.

Remark

For a non zero-dimensional ideal $d_{\text{reg}} = \infty$

Degree of regularity

Definition

The degree of regularity of an homogeneous ideal $I = \langle f_1, \ldots, f_m \rangle$ in the ring $\mathbb{K}[x_1, \ldots, x_n]$ is

$$d_{\text{reg}} = \min \{ d \geqslant 0 \mid \dim_{\mathbb{K}}(\{ f \in I, \ \deg(f) = d \}) = M_d(n) \}$$

where $M_d(n) := \binom{n+d-1}{d}$ is the number of monomials in degree d.

Remark

Consequence: the maximal degree occurring in the computation of a DRL Gröbner basis is bounded by d_{reg}.

Degree of regularity

Definition

The degree of regularity of an homogeneous ideal $I = \langle f_1, \ldots, f_m \rangle$ in the ring $\mathbb{K}[x_1, \ldots, x_n]$ is

$$d_{\mathrm{reg}} = \min \{ d \geqslant 0 \mid \dim_{\mathbb{K}}(\{ f \in I, \ \deg(f) = d \}) = M_d(n) \}$$

where $M_d(n) := \binom{n+d-1}{d}$ is the number of monomials in degree d.

Remark

Consequence: the maximal degree occurring in the computation of a DRL Gröbner basis is bounded by d_{reg}.

Theorem

The complexity of computing a DRL Gröbner basis is bounded by:

$$O\left(\binom{n + d_{reg}}{d_{reg}}^{\omega} \right)$$

Examples Hilbert

$$I = \left\langle x^3, x\,y, y^2 \right\rangle \text{ in } \mathbb{Q}[x,y]$$

then

$$\mathrm{HS}_I(t) = t^2 + 2\,t + 1 \Rightarrow \begin{cases} \dim(I) = 0 \\ \deg(I) = 4 \end{cases}$$

Examples Hilbert

$$I = \left\langle x^3, x\,y, y^2 \right\rangle \text{ in } \mathbb{Q}[x,y]$$

then

$$\mathrm{HS}_I(t) = t^2 + 2\,t + 1 \Rightarrow \begin{cases} \dim(I) = 0 \\ \deg(I) = 4 \end{cases}$$

$$I = \langle x\,y, y\,z, x\,z \rangle \text{ in } \mathbb{Q}[x,y,z]$$

then

$$\mathrm{HS}_I(t) = \frac{2\,t + 1}{1 - t} \Rightarrow \begin{cases} \dim(I) = \\ \deg(I) = \end{cases}$$

Examples Hilbert

$$I = \left\langle x^3, x\,y, y^2 \right\rangle \text{ in } \mathbb{Q}[x, y]$$

then

$$\mathrm{HS}_I(t) = t^2 + 2\,t + 1 \Rightarrow \begin{cases} \dim(I) = 0 \\ \deg(I) = 4 \end{cases}$$

$$I = \langle x\,y, y\,z, x\,z \rangle \text{ in } \mathbb{Q}[x, y, z]$$

then

$$\mathrm{HS}_I(t) = \frac{2\,t + 1}{1 - t} \Rightarrow \begin{cases} \dim(I) = 1 \\ \deg(I) = 3 \end{cases}$$

Regular sequences (revisited) I

original definition:

Definition

Geometric definition: the homogeneous polynomial system $(f_1, \ldots, f_m)$ is **regular** if for all $i \in \{1, \ldots, m\}$, the dimension of $\langle f_1, \ldots, f_i \rangle$ est $n - i$. In that case, the sequence $(f_1, \ldots, f_m)$ said regular.

new definition of semi-regularity: Algebraic definition: the homogeneous polynomial system $(f_1, \ldots, f_m)$ is **regular** if for all $i = 1, \ldots, m$ and g such that

$$g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

then g is also in $\langle f_1, \ldots, f_{i-1} \rangle$.

The non homogeneous system of polynomial equations $(f_1, \ldots, f_m)$ is regular if $(f_1^h, \ldots, f_m^h)$ is regular (f_i^h is the homogenous part of highest degree of f_i).

Regular sequences (revisited) II

Remark

In other words, one cannot find algebraic relations

$$\sum_i g_i \cdot f_i = 0 \text{ with } g_i \in \mathbb{K}[x_1, \ldots, x_n]$$

except the trivial relations (or combined from the) $f_i f_j = f_j f_i$.

Remark

From the geometric definition: regular sequences do not exist when $m > n$.

Regular sequences are well understood mathematical objects:

- We can predict their Hilbert function

Example of generating series

Theorem

n quadratic equations f_i over $\mathbb{Q}$ then under regularity assumption:

$$HS(t) = (1 + t)^n$$

Example of generating series

Theorem

n quadratic equations f_i over $\mathbb{Q}$ then under regularity assumption:

$$HS(t) = (1+t)^n$$

Consequently, $d_{reg} = n + 1$.

Example

Over $\mathbb{Q}$, $n = m = 50$ quadratic equations

$$(1+z)^{50} = 1 + 50\,z + \cdots + z^{50} + 0\ \boxed{z^{51}}$$

Hence the maximal degree occurring in the computation is $\boxed{51}$.

Unifying the Boolean case with the standard case

Describe simultaneously the general case $\mathbb{K}$ and the particular case $\mathbb{F}_2$ $\longrightarrow$ notation: $\delta_{\mathbb{K},\mathbb{F}_2}$ Kronecker 's symbol is equal to 1 if $\mathbb{K} = \mathbb{F}_2$ et 0 else.

If $\mathbb{K} = \mathbb{F}_2$ if want to search the solutions in $\mathbb{K}$ of the algebraic system $(f_1, \ldots, f_m)$, then we need to add to $I = \mathrm{Id}(f_1, \ldots, f_m)$ the field equations $x_i^2 - x_i$.
In the quotient ring:

$$\mathbb{F}_2[\overline{x_1}, \ldots, \overline{x_n}] = \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle,$$

any polynomial f of the ideal $\mathrm{Id}(f_1, \ldots, f_m)$ is solution of the trivial equation

$$f^2 = f$$

Boolean case

$R_{\mathbb{K}}$ denotes the polynomial ring

$$R_{\mathbb{K}} = \mathbb{K}[x_1, \ldots, x_n] \text{ if } \mathbb{K} \neq \mathbb{F}_2$$

and

$$R_{\mathbb{F}_2} = \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle \text{ if } \mathbb{K} = \mathbb{F}_2$$

(Square free polynomials)
Hence if $M_d(n)$ denotes the number of terms in n variables of degree d in $R_{\mathbb{K}}$ it is easy to see that $M_d(n) = \binom{n+d-1}{d}$ and $M_d(n) = \binom{n}{d}$ if $\mathbb{K} = \mathbb{F}_2$.
Consequently:

$$\sum_{d=0}^{\infty} M_d(n) z^d = \left(\frac{1 - \delta_{\mathbb{K},\mathbb{F}_2} z^2}{1 - z} \right)^n \qquad (1)$$

Degree of regularity (Boolean/Standard case)

There is no regular sequence when $m > n \longrightarrow$ we need to change the usual definition of regular sequence by imposing a limit on the degree of non zero divisors:

Definition (Degree of Regularity)

The degree of regularity of an homogeneous ideal $I = \langle f_1, \ldots, f_m \rangle$ in the ring $R_{\mathbb{K}}$ is

$$d_{\text{reg}} = \min \{ d \geqslant 0 \mid \dim_{\mathbb{K}}(\{ f \in I, \ \deg(f) = d \}) = M_d(n) \}$$

Semi-regularity

Definition

Algebraic definition: the homogeneous polynomial system $(f_1, \ldots, f_m)$ is **regular** if for all $i = 1, \ldots, m$ and g such that

$$g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

then g is also in $\langle f_1, \ldots, f_{i-1} \rangle$.

Definition

The homogeneous polynomial system $(f_1, \ldots, f_m)$ is **semi-regular** if for all $i = 1, \ldots, m$ and g such that

$$g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

then g is also in $\langle f_1, \ldots, f_{i-1} \rangle$ if $\deg(g \cdot f_i) \leqslant d_{reg}$.

Overdetermined systems- Complexity

with M. Bardet, B Salvy

$$m \gg n$$

Goal

Estimate $d_{\max}$ the maximal degree of the polynomials occurring in the Gröbner basis computation.

Method

We build A_d following step by step the F_5 algorithm $\longrightarrow$ A_d non singular matrices $\longrightarrow$ number of rows.

$$A_d = \begin{array}{c} \\ \textit{monom } (\mathbf{d}-\mathbf{2}) \times f_{i_1} \\ \textit{monom } (\mathbf{d}-\mathbf{2}) \times f_{i_2} \\ \textit{monom } (\mathbf{d}-\mathbf{2}) \times f_{i_3} \end{array} \begin{array}{c} \textit{momoms degree } \mathbf{d} \textit{ in } x_1, \ldots, x_n \\ \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \end{array} \right) \end{array}$$

F_5 *criterion*

F_5 *criterion*

Keep $t\,f_j$ is in the matrix if $t \notin \mathrm{Id}(\mathrm{LT}_<(G_{j-1}))$, where G_{j-1} is a Gröbner basis of $\{f_1, \ldots, f_{j-1}\}$.

$U_{d,i}(n) :=$ number of rows in the matrix generated by F_5 when computing a Gröbner basis of $[f_1, \ldots, f_i]$ in degree d.

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d + 1)$

Already computed
Groebner $(\langle f_1, \ldots, f_k \rangle), d)$

Matrix in degree d

$$
\begin{array}{l}
 \\
u_1 f_1 \\
\vdots \\
u_{r_1} f_1 \\
\vdots \\
v_{r_{k-1}} f_{k-1} \\
w_1 f_k \\
w_2 f_k
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\
\left(\begin{array}{cccccc}
1 & x & x & x & x & \ldots \\
 & \ddots & & & & \\
0 & & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{array}\right)
\end{array}
$$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$

Matrix in degree d

$$
\begin{array}{l}
\\
u_1 f_1 \\
\vdots \\
u_{r_1} f_1 \\
\vdots \\
v_{r_{k-1}} f_{k-1} \\
w_1 f_k \\
w_2 f_k
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\
\left(\begin{array}{cccccc}
1 & x & x & x & x & \ldots \\
0 & \ddots & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{array}\right)
\end{array}
$$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$

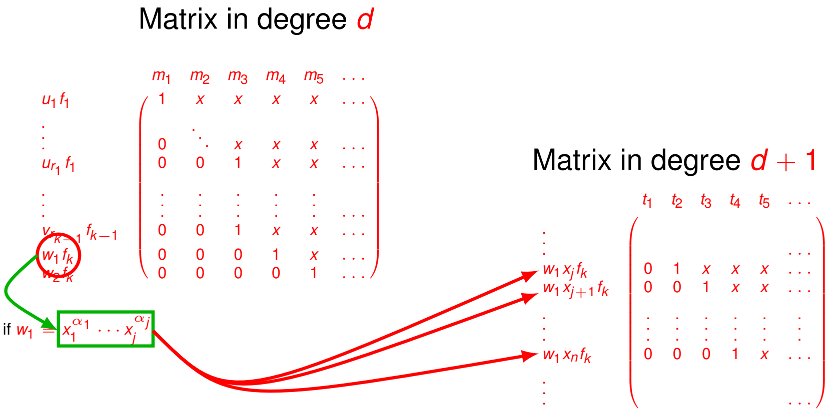
Matrix in degree d

$$
\begin{array}{l}
u_1 f_1 \\ \vdots \\ u_{r_1} f_1 \\ \vdots \\ v_{r_{k-1}} f_{k-1} \\ w_1 f_k \\ w_2 f_k
\end{array}
\quad
\begin{array}{cccccc}
m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \\
\end{array}
$$

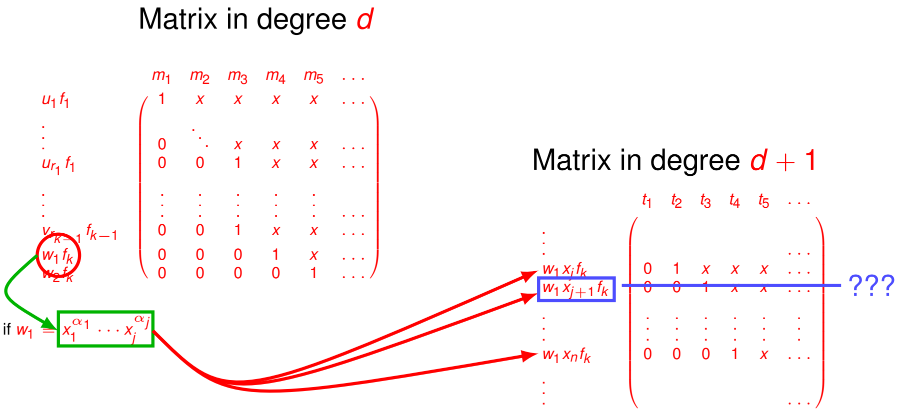
$$
\begin{pmatrix}
1 & x & x & x & x & \ldots \\
0 & \ddots & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots
\end{pmatrix}
$$

if $w_1 = x_1^{\alpha_1} \cdots x_j^{\alpha_j}$

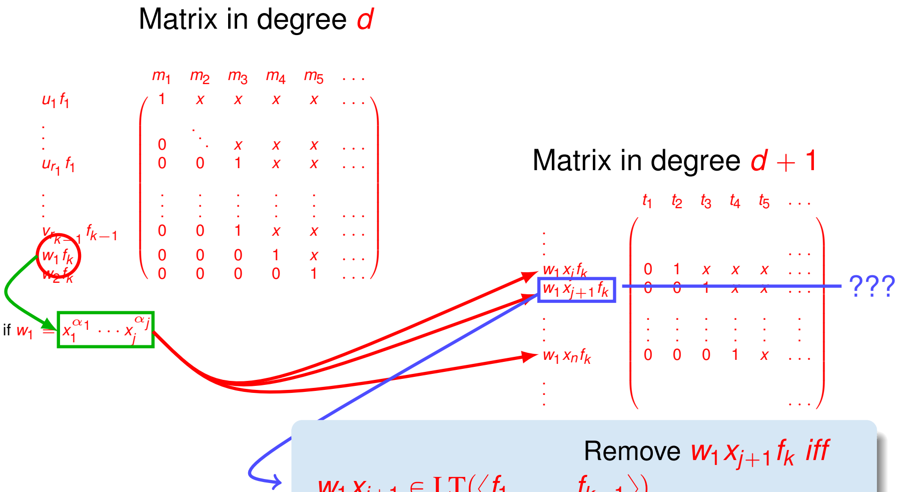
F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



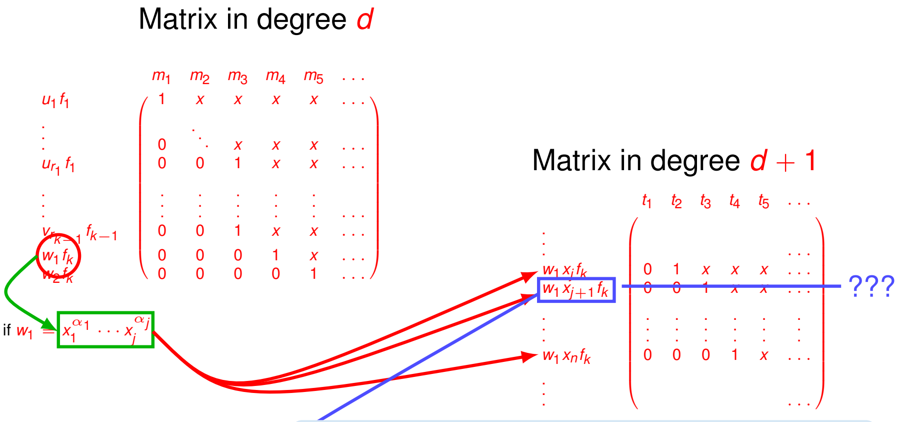
F5: compute Groebner$(\langle f_1, \ldots, f_k \rangle), d + 1)$



Remove $w_1 x_{j+1} f_k$ *iff*

$w_1 x_{j+1} \in \mathrm{LT}(\langle f_1, \ldots, f_{k-1} \rangle)$

F5: compute Groebner $(\langle f_1, \ldots, f_k \rangle), d+1)$



Remove $w_1 x_{j+1} f_k$ *iff*

$w_1 x_{j+1} \in \mathrm{LT}(\text{Groebner}(\langle f_1, \ldots, f_{k-1} \rangle), d-1)$

Induction

When $d \geqslant 1$:

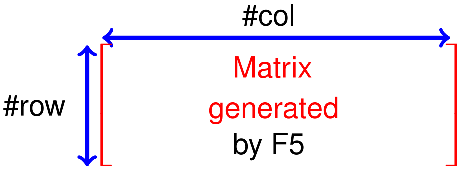
$$U_{d+1,i}(n) = i \cdot \underbrace{M_{d-1}(n)}_{\substack{\text{number of monomials} \\ \text{degree} \leqslant d-1}} - \underbrace{\sum_{j=1}^{i-1} U_{d-1,j}(n)}_{F_5 \text{ criterion}}$$

Induction

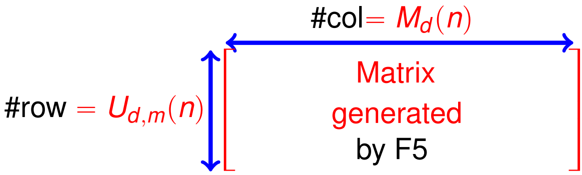
When $d \geqslant 1$:

$$U_{d+1,i}(n) = i \cdot \underbrace{M_{d-1}(n)}_{\substack{\text{number of monomials} \\ \text{degree} \leqslant d-1}} - \underbrace{\sum_{j=1}^{i-1+\delta_{\mathbb{K},\mathbb{F}_2}} U_{d-1,j}(n)}_{F_5 \text{ criterion}}$$

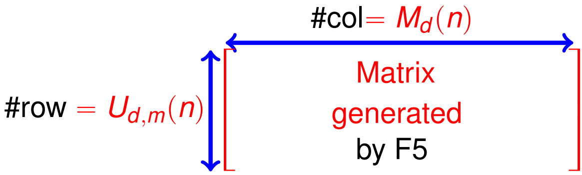
End of the computation



End of the computation



End of the computation



☞ When $h_{d,m}(n) = \#col - \#row \leqslant 0$ this end of the computation !

We can compute explicitly: $h_{d,m}(n) = M_d(n) - h_{d,m}(n)$

and so **compute** the biggest real root $n > 0$ of $h_{d,m}(n) = 0$.

Example

For quadratic equations, $m = n$ over $\mathbb{F}_2$: using the previous recurrence relation we can compute explicitly:

$$U_{0,i}(n) = U_{1,i}(n) = 0$$
$$U_{2,i}(n) = i\binom{n}{0} - 0 = i$$
$$U_{3,i}(n) = i\binom{n}{1} - \sum_{j=1}^{i} U_{1,j}(n) = i\,n$$
$$U_{4,i}(n) = i\binom{n}{2} - \sum_{j=1}^{i} U_{2,j}(n) = i\,\frac{n\,(n-1)}{2} - \sum_{j=1}^{i} j = \frac{i\left(n^2-n-i-1\right)}{2}$$

Example

For quadratic equations, $m = n$ over $\mathbb{F}_2$: using the previous recurrence relation we can compute explicitly:

$$U_{0,i}(n) = U_{1,i}(n) = 0$$

$$U_{2,i}(n) = i\binom{n}{0} - 0 = i$$

$$U_{3,i}(n) = i\binom{n}{1} - \sum_{j=1}^{i} U_{1,j}(n) = i\,n$$

$$U_{4,i}(n) = i\binom{n}{2} - \sum_{j=1}^{i} U_{2,j}(n) = i\,\frac{n\,(n-1)}{2} - \sum_{j=1}^{i} j = \frac{i\left(n^2-n-i-1\right)}{2}$$

Then:

$$\begin{aligned} h_{3,n}(n) &= M_3(n) - U_{3,n}(n) \\ &= \binom{n}{3} - n^2 \\ &= \frac{n\left(n^2-9\,n+2\right)}{6} \end{aligned}$$

Example

For quadratic equations, $m = n$ over $\mathbb{F}_2$: using the previous recurrence relation we can compute explicitly:

$$U_{0,i}(n) = U_{1,i}(n) = 0$$

$$U_{2,i}(n) = i\binom{n}{0} - 0 = i$$

$$U_{3,i}(n) = i\binom{n}{1} - \sum_{j=1}^{i} U_{1,j}(n) = i\,n$$

$$U_{4,i}(n) = i\binom{n}{2} - \sum_{j=1}^{i} U_{2,j}(n) = i\,\frac{n\,(n-1)}{2} - \sum_{j=1}^{i} j = \frac{i\left(n^2-n-i-1\right)}{2}$$

Then:

$$\begin{aligned} h_{3,n}(n) &= M_3(n) - U_{3,n}(n) \\ &= \binom{n}{3} - n^2 \\ &= \frac{n\left(n^2-9\,n+2\right)}{6} \end{aligned}$$

Compute the biggest real root of this polynomial:

$$h_{3,n}(n) = n\,\left(n - 9/2 - 1/2\sqrt{73}\right)\left(n - 9/2 + 1/2\sqrt{73}\right)$$

Example

$$h_{3,n}(n) = n\left(n - 9/2 - 1/2\sqrt{73}\right)\left(n - 9/2 + 1/2\sqrt{73}\right)$$

the biggest real root is: $9/2 + 1/2\sqrt{73} \approx 8.772$ so that $N_3 = \mathbf{9}$.

Example

$$h_{3,n}(n) = n\left(n - 9/2 - 1/2\sqrt{73}\right)\left(n - 9/2 + 1/2\sqrt{73}\right)$$

the biggest real root is: $9/2 + 1/2\sqrt{73} \approx 8.772$ so that $N_3 = \mathbf{9}$.
So that $d \leqslant 3$ when then number of variables is $n \leqslant 9$ and:

d	2	3	4	5	6	7	8	9
N_d	3	9	16	24	32	41	49	58

Example

$$h_{3,n}(n) = n\left(n - 9/2 - 1/2\sqrt{73}\right)\left(n - 9/2 + 1/2\sqrt{73}\right)$$

the biggest real root is: $9/2 + 1/2\sqrt{73} \approx 8.772$ so that $N_3 = \mathbf{9}$.
So that $d \leqslant 3$ when then number of variables is $n \leqslant 9$ and:

d	2	3	4	5	6	7	8	9
N_d	3	9	16	24	32	41	49	58

To read the previous tabular we start from the bottom line:

1. When $3 \leqslant n < 9 = N_3$ then the maximal degree in F_5 is 3; consequently the maximal matrix is of size $n^3 \times n^3$; the total complexity cost is thus $O(n^9)$.
2. When $N_3 = 9 \leqslant n < N_4 = 16$ the maximal degree is 4 and the total complexity is bounded by $O(n^{12})$.
3. When $N_4 = 16 \leqslant n < N_5 = 24$ the maximal degree is $5$and the total complexity is bounded by $O(n^{15})$.

Generating series

Theorem

f_i *of degree* d_i, $i = 1, \ldots, m$ *finite field* $\mathbb{F}_q$ *then*

$$\boxed{H_m = \sum_{d=0}^{\infty} h_{d,m}\, z^d = \prod_{i=1}^{m} \left(\frac{1-(1-\delta)\, z^{d_i}}{1+\delta}\right) \left(\frac{1-\delta\, z^2}{1-z}\right)^n} \text{ with } \delta = \delta_{\mathbb{K},\mathbb{F}_2}$$

Generating series

Theorem

f_i *of degree* d_i, $i = 1, \dots, m$ *finite field* $\mathbb{F}_q$ *then*

$$\boxed{H_m = \sum_{d=0}^{\infty} h_{d,m}\, z^d = \prod_{i=1}^{m} \left(\frac{1-(1-\delta)\, z^{d_i}}{1+\delta}\right) \left(\frac{1-\delta\, z^2}{1-z}\right)^n} \quad \textit{with } \delta = \delta_{\mathbb{K},\mathbb{F}_2}$$

particular case: $d_i = 2$, $\mathbb{F}_2$, $n = m$ equations

$$\sum_{d=0}^{\infty} h_{d,n}\, z^d = \left(\frac{1+z}{1+z^2}\right)^n$$

Generating series

particular case: $d_i = 2$, $\mathbb{F}_2$, $n = m$ equations

$$\sum_{d=0}^{\infty} h_{d,n}\, z^d = \left(\frac{1+z}{1+z^2}\right)^n$$

Example

$\mathbb{F}_2$, $n = m = 50$ quadratic equations

$$\left(\frac{1+z}{1+z^2}\right)^{50} = 1 + 50\,z + 1175\,z^2 + 17100\,z^3 + 170325\,z^4 + 1202510\,z^5 + 5915475\,z^6 + 17831400\,z^7 + 9196475\,z^8 - 205886050\,\boxed{z^9} + O\left(z^{10}\right)$$

Hence the maximal degree occurring in the computation is $\boxed{9}$.

Asymptotic estimate (sketch of the proof)

Biggest real root of

$$h_{d,n} = \frac{1}{2i\pi} \int_C \left(\frac{1+z}{1+z^2} \right)^n \frac{dz}{z^{d+1}}$$

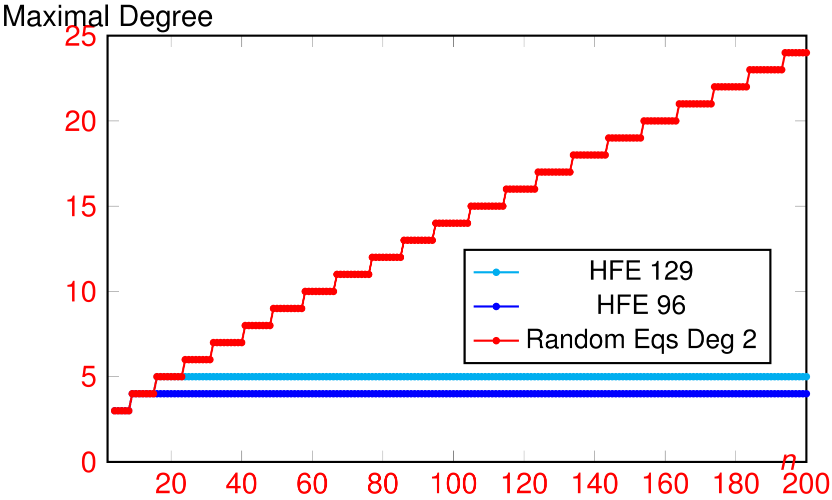
$$d_n = \frac{1}{\lambda_0} n - \frac{\lambda_1}{\lambda_0^{\frac{4}{3}}} n^{\frac{1}{3}} + O\left(\frac{1}{n^{\frac{1}{3}}}\right)$$

$$d_n \approx \frac{\mathbf{n}}{\mathbf{11.114}} + \mathbf{1.003}\, \mathbf{n}^{\frac{1}{3}} + \mathbf{O}\left(\frac{\mathbf{1}}{\mathbf{n}^{\frac{1}{3}}}\right)$$

where $\lambda_0 = 3/2\sqrt{3} + 5/2 + 1/2\sqrt{72 + 42\sqrt{3}} \approx 11.11360$
the expression of λ_1 contains the biggest real root of the Airy function (solution of $\frac{\partial^2 y}{\partial z^2} - zy = 0$)

The formula is almost exact when $n \geqslant 3$!

Maximal degree



Complexity: classification I

k is a constant (does not depend on n).
d_i total degree of f_i.

m	Degree	$d_{\max}$
$m \leqslant n$	$\mathbb{K}, d_i = 2$	$m + 1$ (Macaulay bound)
$m \leqslant n$	$\mathbb{K}$	$1 + \sum_{i=1}^{n+1} (d_i - 1)$ (Macaulay bound)
$n + k$	$\mathbb{K}, d_i = 2$	$\frac{m}{2} - h_{k,1}\sqrt{\frac{m}{2}} + o(1)$
$n + k$	$\mathbb{K}$	$\sum_{i=1}^{n+k} \frac{d_i - 1}{2} - h_{k,1}\sqrt{\sum_{i=1}^{n+k} \frac{d_i^2 - 1}{6}} + o(1)$
$2\,n$	$\mathbb{K}, d_i = 2$	$\frac{n}{11.6569} + 1.04\,n^{\frac{1}{3}} - 1.47 + 1.71\,n^{-\frac{1}{3}} + O\left(n^{-\frac{2}{3}}\right)$
$k\ \ n$	$\mathbb{K}, d_i = 2$	$(k - \frac{1}{2} - \sqrt{k(k-1)})n + \frac{-a_1}{2(k(k-1))^{\frac{1}{6}}} n^{\frac{1}{3}} + O(1)$
n	$\mathbb{F}_2, d_i = 2$	$\frac{n}{11.1360} + 1.0034\,n^{\frac{1}{3}} - 1.58 + O(n^{-\frac{1}{3}})$
$k\ \ n$	$\mathbb{F}_2, d_i = 2$	$\left(-k + \frac{1}{2} + \frac{1}{2}\sqrt{2k(k-5) - 1 + 2(k+2)\sqrt{k(k+2)}}\right)$

Classification

Classification: m number of polynomials, n number of variables

Number of Eqs	Complexity
$m = \mathrm{cste}\ \ n$	exponential
$m = \mathrm{cste}\ \ n^{1+\beta}$	sub exponential
$m = \mathrm{cste}\ \ n^2$	polynomial

For instance: if we have $m = \alpha\, n^{1+\beta}$ quadratic equations with $\beta > 0$

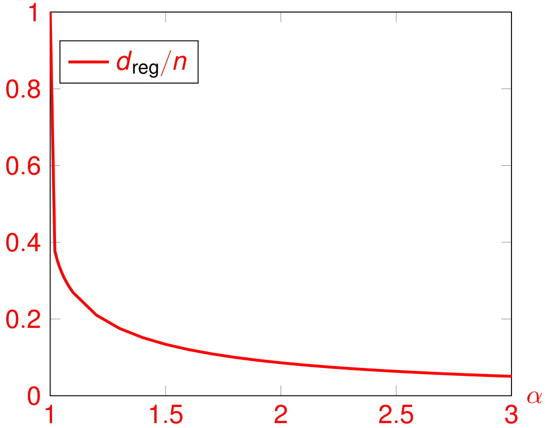
$$d_{\max} \approx \frac{n^{1-\beta}}{8\,\alpha}$$

Overdetermined systems

Theorem (Bardet, Faugère, Salvy)

For $m = \alpha\, n$ semi-regular quadratic equations ($\alpha > 1$) in $\mathbb{Q}[x_1, \ldots, x_n]$:

$$HS(t) = \frac{(1-t^2)^m}{(1-t)^n} \quad \text{and} \quad d_{reg} \approx (\alpha - \frac{1}{2} - \sqrt{\alpha(\alpha-1)})n$$

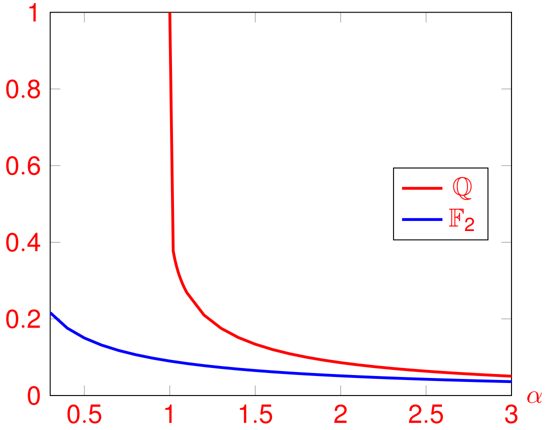


Overdetermined systems

Theorem (Bardet, Faugère, Salvy)

For $m = \alpha\, n$ *semi-regular quadratic equations* ($\alpha \geqslant 1$) *in* $\mathbb{F}_2[x_1, \ldots, x_n]$*:*

$$HS(t) = \frac{(1+t)^n}{(1+t^2)^m} \quad \text{and} \quad d_{reg} \approx \left(-\alpha + \frac{1+\sqrt{2\,\alpha^2 - 10\,\alpha - 1 + 2\,(\alpha+2)\sqrt{\alpha\,(\alpha+2)}}}{2} \right) n$$



The Boolean case

The Boolean case: problem Statement

Boolean Multivariate Quadratic Polynomial Problem (Boolean MQ)

Input: $(f_1, \ldots, f_m) \in \mathbb{F}_2[x_1, \ldots, x_n]^m$ with $\deg(f_i) = 2$

Question: Find – if any – *one* $z \in \mathbb{F}_2^n$ such that

$$f_1(z) = \cdots = f_m(z) = 0.$$

- It is an NP-complete problem whose random instances seem difficult to solve.
- Decrease significantly this complexity of 2^n is a long-standing open problem

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption best complexity bound to solve Boolean MQ is operations.

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: we have n equations / n unknowns over $\mathbb{F}_2$

What is the complexity ?

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\,\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: we have n equations / n unknowns over $\mathbb{F}_2$

What is the complexity ?

$$\binom{n}{d_{\text{reg}}}^{\omega} \text{ and } d_{\text{reg}} \approx \frac{n}{11.11}$$

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: we have n equations / n unknowns over $\mathbb{F}_2$

What is the complexity ?

$$\binom{n}{d_{\text{reg}}}^{\omega} \text{ and } d_{\text{reg}} \approx \frac{n}{11.11}$$

$$\ln_2 \binom{n}{n/\beta} \approx (-(\beta-1)\ln(\beta-1)/\beta + \ln(\beta))\,n/\ln(2)$$

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\,\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: we have n equations / n unknowns over $\mathbb{F}_2$

What is the complexity ?

$$\binom{n}{d_{\text{reg}}}^{\omega} \text{ and } d_{\text{reg}} \approx \frac{n}{11.11}$$

$$\ln_2 \binom{n}{n/\beta} \approx \left(-(\beta-1)\,\ln(\beta-1)/\beta + \ln(\beta)\right) n/\ln(2)$$

$$\ln_2 \binom{n}{n/\beta} \approx 0.436\,n$$

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\,\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: we have n equations / n unknowns over $\mathbb{F}_2$

What is the complexity ?

$$\binom{n}{d_{\text{reg}}}^{\omega} \text{ and } d_{\text{reg}} \approx \frac{n}{11.11}$$

$$\ln_2 \binom{n}{n/\beta} \approx \left(-(\beta-1)\,\ln(\beta-1)/\beta + \ln(\beta)\right) n/\ln(2)$$

$$\ln_2 \binom{n}{n/\beta} \approx 0.436\,n$$

The total Complexity is $2^{1.04\,n}$ with $\omega = 2.376$

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption best complexity bound to solve Boolean MQ is operations.
- using Gröbner bases: n equations/unknowns over $\mathbb{F}_2$ $O(2^{1.04\,n})$

Related Works

Boolean MQ problem is NP-complete $\longrightarrow$ cannot expect to solve it in sub-exponential time.

- Worst case complexity $4\ \log_2(n)2^n$ [Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10].
- $O(2^{0.8765\,n})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- using Gröbner bases: n equations/unknowns over $\mathbb{F}_2$ $\quad O(2^{1.04\,n})$
- for very Sparse Equations (sparse $=$ each equation depends on ℓ variables), the expected complexity of the Agreeing-Gluing Algorithm is:

$$\begin{array}{ll} O(2^{0.4157n}) & \text{when } \ell = 6 \\ O(2^{0.1544n}) & \text{when } \ell = 3\ . \end{array}$$

I. Semaev.
Sparse algebraic equations over finite fields.
SIAM J. Comput., 39(2):388–409, 2009.

Finite Fields
The Boolean case

The Boolean case: problem Statement

Boolean Multivariate Quadratic Polynomial Problem (Boolean MQ)

Input: $(f_1, \ldots, f_m) \in \mathbb{F}_2[x_1, \ldots, x_n]^m$ with
$\deg(f_i) = 2$

Question: Find – if any – *one* $z \in \mathbb{F}_2^n$ such that

$$f_1(z) = \cdots = f_m(z) = 0.$$

- It is an NP-complete problem whose random instances seem difficult to solve.
- Decrease significantly this complexity of 2^n was a long-standing open problem

Main result

☞ Algorithm BooleanSolve to solve determined or overdetermined systems ($m = \alpha n$ with $\alpha \geqslant 1$).

Deterministic and Las Vegas variants, depending on the choice of some linear algebra subroutines

Theorem (Bardet,Faugère,Salvy,Spaenlehauer J.Complexity'12)

$m = n$ and under some algebraic assumptions, the Boolean MQ Problem can be solved in:

- $O(2^{0.841n})$ *using the deterministic variant;*
- $O(2^{0.792n})$ *using the Las Vegas probabilistic variant.*

Las Vegas: the result is always correct, but the complexity is a random variable.

General approach for finite fields

- mix efficiently exhaustive search, field equations and Gröbner bases.
- Use complexity results to estimate the complexity.

Simple Idea:
we fix k variables (trade-off.) $\longrightarrow$ we increase the ratio $\frac{\#equations}{\#vars} = \frac{m}{n-k}$

The gain obtained by solving overdetermined systems may overcome the loss due to the exhaustive search on the fixed variables.

overdetermined systems

exhaustive search

The goal is to find k the **best trade-off**

Complexity of the General Hybrid Method

Theorem

$[f_1, \ldots, f_m]$ of quadratic equations in n variables. Under assumptions, when $n \to \infty$, $q \to \infty$ and $n > \log(q)$, asymptotically:

$$k \sim 0.30 \, \frac{n\,\omega^2}{\log_2(q)^2}$$

$$C_{hyb} \sim 2^{\left(1.38\,\omega - 0.44\,\omega^2 \, \log_2(q)^{-1}\right)\,n}$$

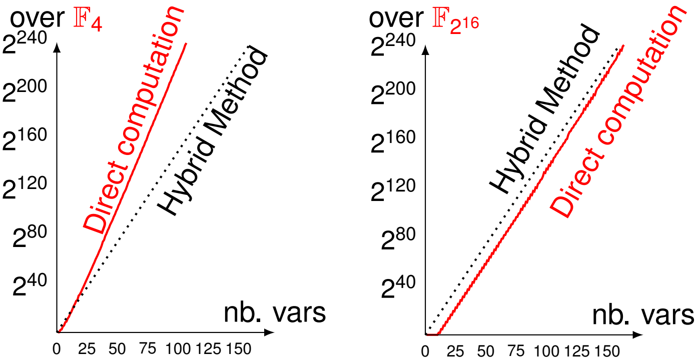
$$\frac{\text{direct Gröbner basis approach}}{\text{hybrid approach}} \sim 2^{0.62\,\omega\,n}$$

Complexity of the General Hybrid Method

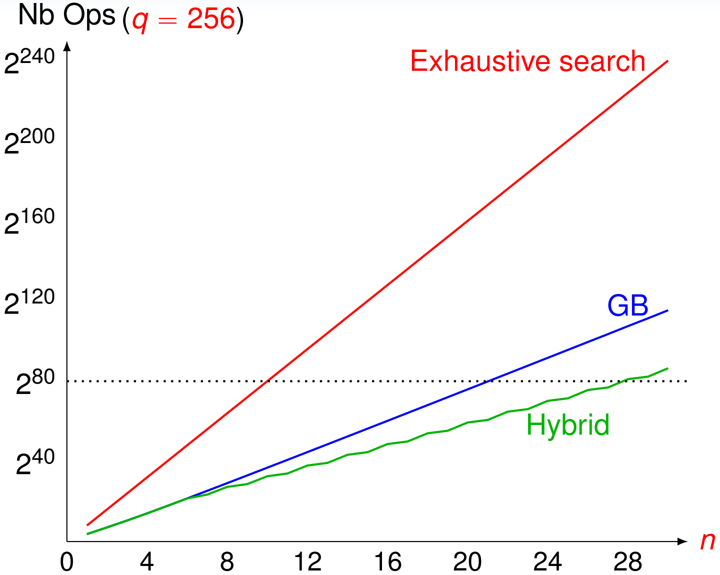
Theorem

$[f_1, \ldots, f_m]$ *of quadratic equations in* n *variables. Under assumptions, when* $n \to \infty$, $q \to \infty$ *and* $n > \log(q)$, *asymptotically:*

$$C_{hyb} \sim 2^{\left(1.38\,\omega - 0.44\,\omega^2\ \log_2(q)^{-1}\right)\,n}$$



Comparison Solving Methods (fixed $q = 256$)



Theoretical complexity (explicit formula).

Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

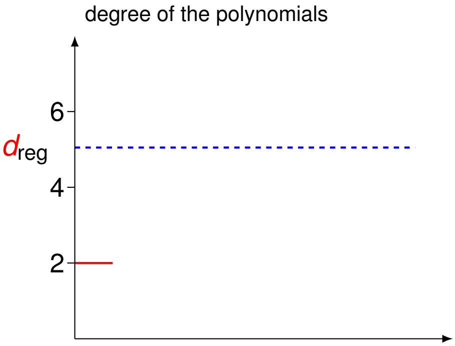
- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

The usual strategy is the following:

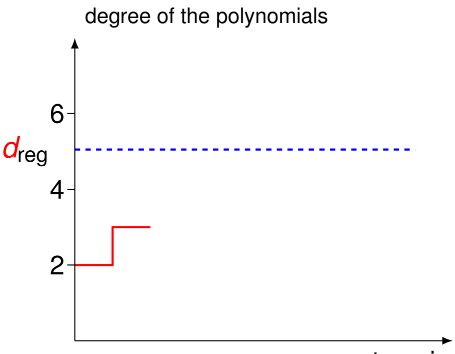


Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

The usual strategy is the following:

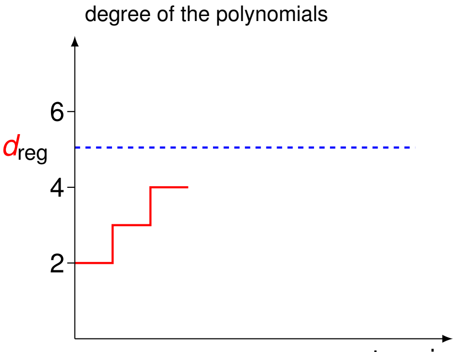


Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

The usual strategy is the following:

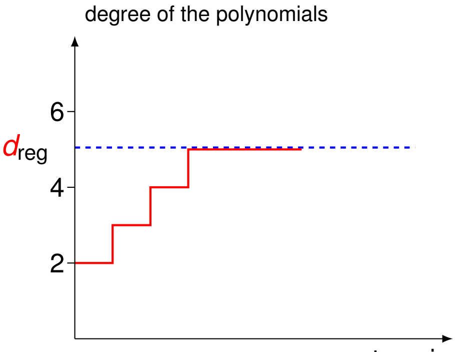


Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

The usual strategy is the following:

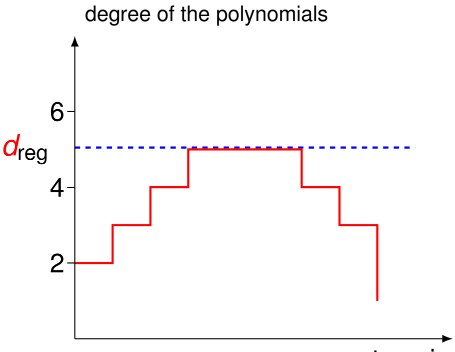


Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

The usual strategy is the following:

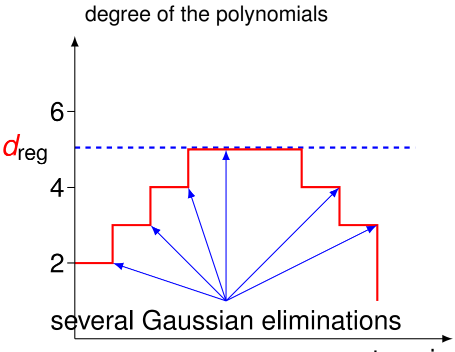


Roadmap of the new algorithm over $\mathbb{F}_2$

with M Bardet, B Salvy, PJ Spaenlehauer

- Instead of applying Gaussian Elimination on several matrices we want to solve only **one** linear system.
- To solve this linear system: use the Wiedemann algorithm so that $\omega = 2$.
- Find the new optimal trade-off

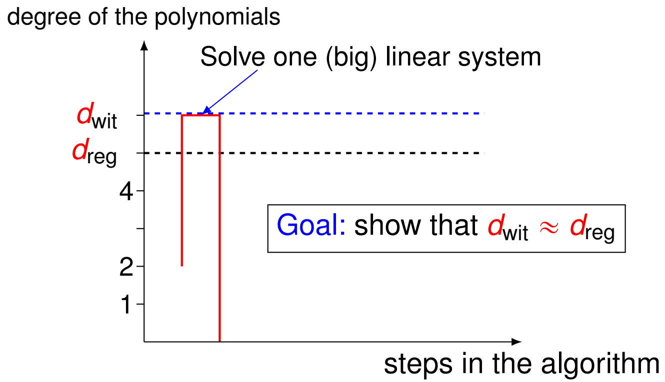
The usual strategy is the following:



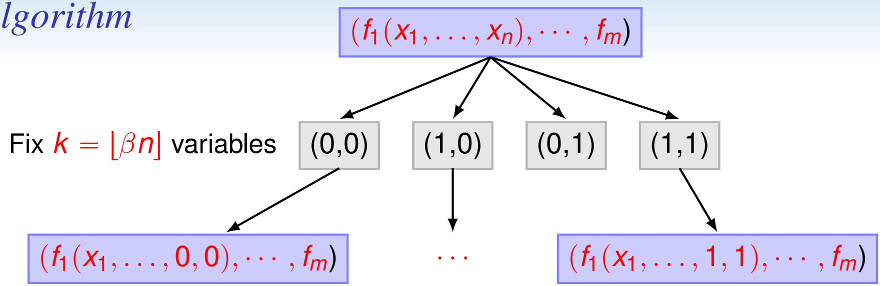
Idea/Goal of the new algorithm

- Use the Wiedemann algorithm so that $\omega = 2$.
- Hide as much as possible the Gröbner basis algorithm to solve only **one** linear system.
- Combine with exhaustive search

We define a new d_{wit} so that we obtain the final GB in one step:

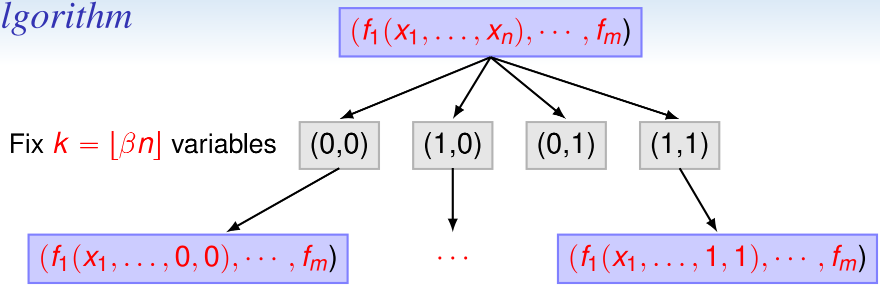


Algorithm



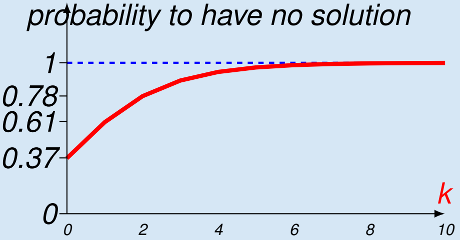
$(f_1(x_1, \ldots, x_n), \cdots, f_m)$
Fix $k = \lfloor \beta n \rfloor$ variables
(0,0)
(1,0)
(0,1)
(1,1)
$(f_1(x_1, \ldots, 0, 0), \cdots, f_m)$
$\cdots$
$(f_1(x_1, \ldots, 1, 1), \cdots, f_m)$

Algorithm

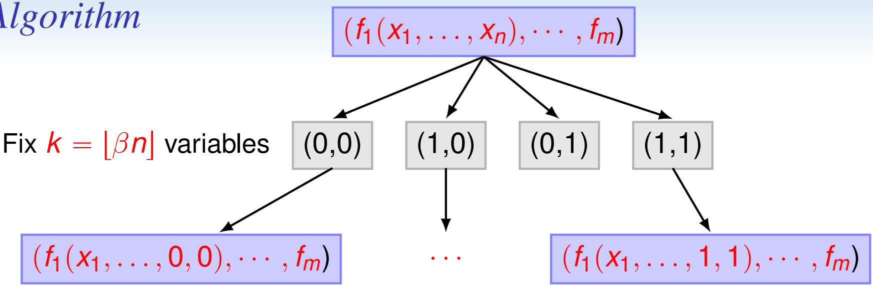


Theorem (Fusco and Bach, TAMC 2007)

The probability that a random polynomial system of $n + k$ random equations of degree d ($d \geqslant 2$) in n variables over $\mathbb{F}_2$, has no solution is $e^{-2^{-k}}$ (asymptotically)



Algorithm



Instead of solving $\longrightarrow$ test consistency of the specialized overdetermined systems

Consistency check: Hilbert's Nullstellensatz over $\mathbb{F}_2$

$f_1, \cdots, f_m = 0$ has no solution $\iff$ Find $h_1, \ldots, h_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}]$

$$h_1\, f_1 + \cdots + h_m\, f_m = 1 \mod \left\langle x_i^2 - x_i,\, i = 1, .., (n-k) \right\rangle.$$

Given a bound $\mathrm{d_{wit}}$ on $\deg(h_i)$, the h_i can be founded by linear algebra:

Consistency check: Hilbert's Nullstellensatz over $\mathbb{F}_2$

$f_1, \cdots, f_m = 0$ has no solution $\iff$ Find $h_1, \ldots, h_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}]$

$$h_1\, f_1 + \cdots + h_m\, f_m = 1 \mod \left\langle x_i^2 - x_i,\, i = 1, .., (n-k) \right\rangle.$$

Given a bound $\mathrm{d_{wit}}$ on $\deg(h_i)$, the h_i can be founded by linear algebra:

$$\text{Macaulay Matrix}_{\prec}(d) = \begin{array}{c} \\ \vdots \\ t\, f_i \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} m_1 & \cdots & m_\ell \end{array} \\ \left(\begin{array}{c} \\ c_{i,j} = \text{coeff}(t\, f_i, m_j) \\ \\ \end{array} \right) \end{array}$$

Columns: squarefree monomials of degree d.
Rows: all products $t\, f_i$ (remove squares) where $\deg(t) \leqslant d - 2$.

Consistency check: Hilbert's Nullstellensatz over $\mathbb{F}_2$

$f_1, \cdots, f_m = 0$ has no solution $\Longleftrightarrow$ Find $h_1, \ldots, h_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}]$

$$h_1\, f_1 + \cdots + h_m\, f_m = 1 \mod \left\langle x_i^2 - x_i,\, i = 1, .., (n-k) \right\rangle .$$

Given a bound $\mathrm{d_{wit}}$ on $\deg(h_i)$, the h_i can be founded by linear algebra:

$$\text{Macaulay Matrix}_{\prec}(d) = \begin{array}{c} \\ \vdots \\ t\, f_i \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} m_1 & \cdots & m_\ell \end{array} \\ \left(\begin{array}{c} \\ c_{i,j} = \mathrm{coeff}(t\, f_i, m_j) \\ \\ \end{array} \right) \end{array}$$

Columns: squarefree monomials of degree d.
Rows: all products $t\, f_i$ (remove squares) where $\deg(t) \leqslant d-2$.

Lemma

$\mathbf{1} = {}^T[1, 0, \ldots]$ *vector which represent the monomial* 1. *If the linear system* $\mathbf{u} \cdot \mathrm{M} = \mathbf{1}$ *has a solution, then* $f_1 = \cdots = f_m = 0$ *has no solution.*

Consistency check: Hilbert's Nullstellensatz over $\mathbb{F}_2$

$$\text{Macaulay Matrix}_{\prec}(d) = \begin{array}{c} \vdots \\ t\, f_i \\ \vdots \end{array} \overset{\begin{array}{ccc} m_1 & \cdots & m_\ell \end{array}}{\left(\quad c_{i,j} = \mathrm{coeff}(t\, f_i, m_j) \quad \right)}$$

Columns: squarefree monomials of degree d.
Rows: all products $t\, f_i$ (remove squares) where $\deg(t) \leqslant d - 2$.

Lemma

$\mathbf{1} = {}^T[1, 0, \dots]$ *vector which represent the monomial* 1. *If the linear system* $\mathbf{u} \cdot \mathrm{M} = \mathbf{1}$ *has a solution, then* $f_1 = \cdots = f_m = 0$ *has no solution.*

Proposition

If $D = \frac{d}{n} < \frac{1}{2}$

number of columns of $M < \frac{1-D}{1-2D} \binom{n}{d}$

number of rows of $M < m \frac{D^2}{(1-2D)(1-D)} \binom{n}{d}$

density of $M < n^2 \frac{1-2D}{1-D} \binom{n}{d}^{-1} \longrightarrow 0.$

Solving sparse linear systems

D. Wiedemann.
Solving sparse linear equations over finite fields.
IEEE Transactions on Information Theory, 32(1):54–62, 1986.

E. Kaltofen and B. David Saunders.
On Wiedemann's method of solving sparse linear systems.
AAECC, p. 29–38, 1991.

G. Villard.
Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems.
ISSAC'97, p. 32–39. ACM, 1997.

M. Giesbrecht, A. Lobo, and B. D. Saunders.
Certifying inconsistency of sparse linear systems.
ISSAC'98, p. 113–119, 1998.

Wiedemann : main idea

We want to solve $M\,x = b$ where b is a given vector and M is a sparse $n \times n$ matrix. (we assume that $\det(M) \neq 0$).
The goal is to find a polynomial $P(X) = \sum_{i=0}^{d} p_i X^i$ with $p_0 \neq 0$ and $d \leqslant n$ such that

$$P(M).b = 0$$

Note that the characteristic (minimal) polynomial of M is a solution.

$$p_0 b + \sum_{i=1}^{d} p_i M^i b = 0$$

so that a solution of $M\,x = b$ is $x = -\sum_{i=1}^{d} \frac{p_i}{p_0} M^{i-1} b$
To compute P, we choose a random vector and the sequences

$$\begin{cases} v_0 = n \text{ and } v_i = M\,v_{i-1} \text{ for } i = 1, \ldots, (2 * n - 1) \\ z_i = \langle v_i\,,\, r \rangle \text{ (scalar product) for } i = 0, 1, \ldots, (2 * n - 1) \end{cases}$$

We then apply the Berlekamp-Massey algorithm to retrieve a candidate polynomial P.

Complexity ?

Consistency of singular linear system (Wiedemann)

TestConsistency (Gisbrecht,Lobo,Saunders 98)

Input: Black boxes for $\mathbf{x} \mapsto A \cdot \mathbf{x}$ and $\mathbf{x} \mapsto {}^{T}\!A \cdot \mathbf{x}$ where $A \in \mathbb{K}^{N \times N}$ and $\mathbf{b} \in \mathbb{K}^{N \times 1}$

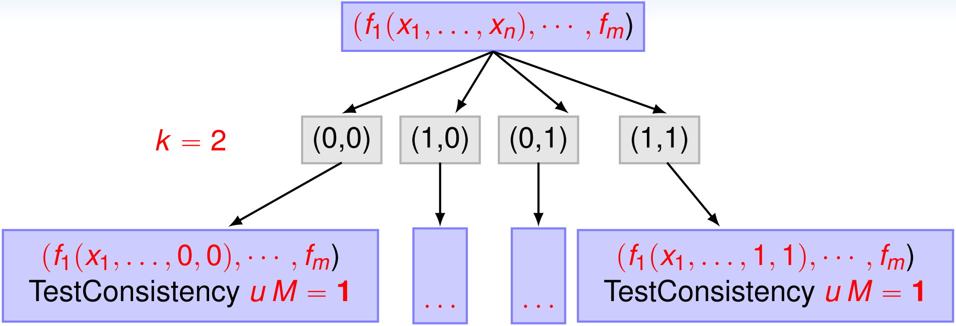
Output:

- ("consistent",$\mathbf{x}$) with $A \cdot \mathbf{x} = \mathbf{b}$ if the system has a solution
- ($\emptyset$ ="inconsistent",$\mathbf{u}$) if the system does not have a solution, with $\mathbf{u} \cdot A = 0$ and $\mathbf{u} \cdot \mathbf{b} \neq 0$, certifying the inconsistency.

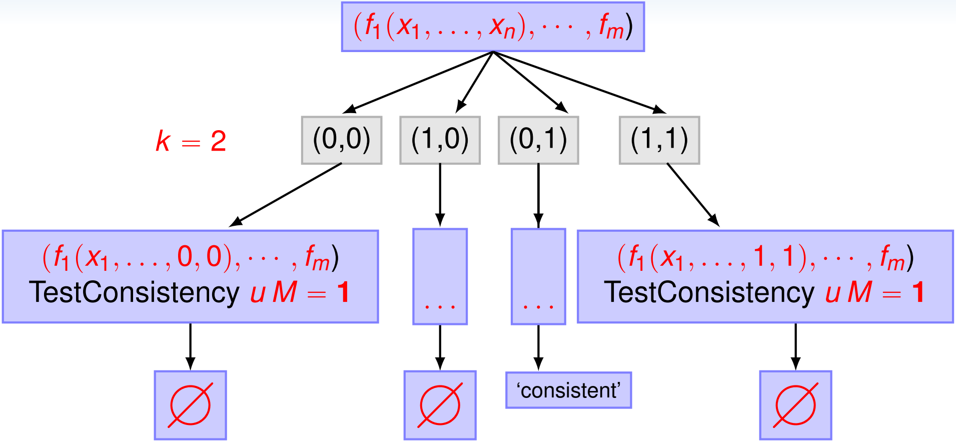
Theorem (Gisbrecht,Lobo,Saunders 98)

Algorithm determines the consistency of an $N \times N$ matrix with expected complexity $O(N \log N)$ evaluations of the black boxes and $O(N^2 \log^2 N \log \log N)$ additional operations in $\mathbb{F}_2$.

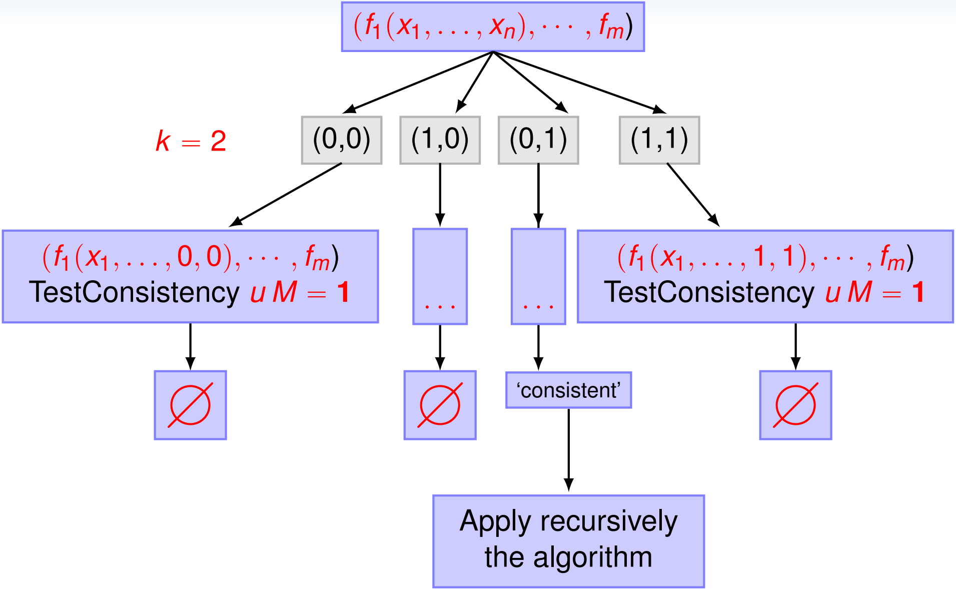
Algorithm : a filtering process



Algorithm : a filtering process



Algorithm : a filtering process



Bounding the Witness Degree

$f_1, \cdots, f_m = 0$ has no solution $\Longleftrightarrow$ Find $g_1, \ldots, g_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}]$

$$g_1 \, f_1 + \cdots + g_m \, f_m = 1 \mod \left\langle x_i^2 - x_i, \, i = 1, .., (n-k) \right\rangle.$$

$\Longleftrightarrow$ Find homogeneous $h_1, \ldots, h_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}, h]$

$$h_1 \, f_1 + \cdots + h_m \, f_m = h^{\mathsf{d_{wit}}} \mod \left\langle x_i^2 - x_i h, \, i = 1, .., (n-k) \right\rangle.$$

Bounding the Witness Degree

$f_1, \cdots, f_m = 0$ has no solution $\Longleftrightarrow$ Find $g_1, \ldots, g_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}]$

$$g_1\, f_1 + \cdots + g_m\, f_m = 1 \quad \text{mod} \ \left\langle x_i^2 - x_i,\, i = 1, .., (n-k) \right\rangle.$$

$\Longleftrightarrow$ Find homogeneous $h_1, \ldots, h_m$ in $\mathbb{F}_2[x_1, \ldots, x_{n-k}, h]$

$$h_1\, f_1 + \cdots + h_m\, f_m = h^{\mathrm{d_{wit}}} \quad \text{mod} \ \left\langle x_i^2 - x_i h,\, i = 1, .., (n-k) \right\rangle.$$

Proposition

Let $\mathbf{F} = \left(f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\right)$ *s.t. the system* $\mathbf{F} = 0$ *has no solution. Then,* $\mathrm{d_{wit}} \leqslant d_{reg}(I^{(h)})$ *the homogenized ideal*

$$I^{(h)} = \left\langle f_1^{(h)}, \ldots, f_m^{(h)}, x_1^2 - x_1 h, \ldots, x_n^2 - x_n h \right\rangle.$$

Bounding the Witness Degree

Proposition

Let $\mathbf{F} = \left(f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\right)$ *s.t. the system* $\mathbf{F} = 0$ *has no solution. Then,* $\mathrm{d_{wit}} \leqslant d_{reg}(I^{(h)})$ *the homogenized ideal*

$$I^{(h)} = \left\langle f_1^{(h)}, \ldots, f_m^{(h)}, x_1^2 - x_1 h, \ldots, x_n^2 - x_n h \right\rangle.$$

Theorem

Assuming $m = \alpha\, n$. *Under some semi-regularity assumption:*

$$\mathrm{HS}_{n,m}(t) := \frac{1}{1-t}\frac{(1+t)^n}{(1+t^2)^m} \qquad \textit{(Hilbert Series)}$$

Bounding the Witness Degree

Proposition

Let $\mathbf{F} = \left(f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\right)$ *s.t. the system* $\mathbf{F} = 0$ *has no solution. Then,* $\mathrm{d}_{\mathrm{wit}} \leqslant d_{reg}(I^{(h)})$ *the homogenized ideal*

$$I^{(h)} = \left\langle f_1^{(h)}, \ldots, f_m^{(h)}, x_1^2 - x_1 h, \ldots, x_n^2 - x_n h \right\rangle.$$

Theorem

Assuming $m = \alpha\, n$. *Under some semi-regularity assumption:*

$$\mathrm{HS}_{n,m}(t) := \frac{1}{1-t} \frac{(1+t)^n}{(1+t^2)^m} \qquad \textit{(Hilbert Series)}$$

$$\mathrm{d}_{\mathrm{wit}} \sim d_{reg} \sim \left(-\alpha + \frac{1+\sqrt{2\alpha^2 - 10\alpha - 1 + 2(\alpha+2)\sqrt{\alpha(\alpha+2)}}}{2} \right) n.$$

Complexity: putting all together

Complexity $= 2^{\beta n}$ Consistency$(n - \beta n$ vars$, \alpha n$ equations$)$

Complexity: putting all together

$$\begin{aligned} \text{Complexity} &= 2^{\beta n}\ \text{Consistency}(n - \beta n \text{ vars}, \alpha n \text{ equations}) \\ \log_2 \text{Complexity} &= (\beta + 2(\beta - 1)\log_2(D^D(1-D)^{1-D}))\, n \end{aligned}$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2 - 10\gamma - 1 + 2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Complexity: putting all together

$$\text{Complexity} = 2^{\beta n}\ \text{Consistency}(n - \beta n \text{ vars}, \alpha n \text{ equations})$$
$$\log_2 \text{Complexity} = (\beta + 2(\beta - 1)\log_2(D^D(1-D)^{1-D}))\, n$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2-10\gamma-1+2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Remaining task : find $1 > \beta \geqslant 0$ to minimize the complexity

Complexity: putting all together

$$\begin{aligned}\text{Complexity} &= 2^{\beta n}\ \text{Consistency}(n-\beta n \text{ vars}, \alpha n \text{ equations})\\ \log_2 \text{Complexity} &= (\beta + 2(\beta-1)\log_2(D^D(1-D)^{1-D}))\, n\end{aligned}$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2-10\gamma-1+2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Remaining task : find $1 > \beta \geqslant 0$ to minimize the complexity

Theorem (J.Complexity 12)

Under algebraic assumption, a Boolean quadratic polynomial $(f_1, \ldots, f_{\alpha n})$ can be solved in probabilistic time:

$$O(2^{(1-0.208\alpha)n}) \textit{ for } \alpha \leqslant 1.82 \textit{ using } \beta = 1 - 0.55\alpha$$

If $\alpha > 1.82$, the best complexity is achieved for $\beta = 0$.

Complexity: putting all together

Complexity $= 2^{\beta n}$ Consistency$(n - \beta n$ vars$, \alpha n$ equations$)$

Complexity: putting all together

$$\begin{aligned} \text{Complexity} &= 2^{\beta n}\ \text{Consistency}(n - \beta n \text{ vars}, \alpha n \text{ equations}) \\ \log_2 \text{Complexity} &= (\beta + 2(\beta - 1) \log_2(D^D(1-D)^{1-D}))\, n \end{aligned}$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2-10\gamma-1+2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Complexity: putting all together

$$\text{Complexity} = 2^{\beta n}\ \text{Consistency}(n - \beta n \text{ vars}, \alpha n \text{ equations})$$
$$\log_2 \text{Complexity} = (\beta + 2(\beta - 1)\log_2(D^D(1-D)^{1-D}))\, n$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2-10\gamma-1+2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Remaining task : find $1 > \beta \geqslant 0$ to minimize the complexity

Complexity: putting all together

$$\begin{array}{ll} \text{Complexity} & = 2^{\beta n}\ \text{Consistency}(n - \beta n \text{ vars}, \alpha n \text{ equations}) \\ \log_2 \text{Complexity} & = \left(\beta + 2(\beta - 1)\log_2\left(D^D (1-D)^{1-D}\right)\right) n \end{array}$$

where

$$D = -\gamma + \frac{1+\sqrt{2\gamma^2 - 10\gamma - 1 + 2(\gamma+2)\sqrt{\gamma(\gamma+2)}}}{2} \text{ and } \gamma = \frac{\alpha}{1-\beta}$$

Remaining task : find $1 > \beta \geqslant 0$ to minimize the complexity

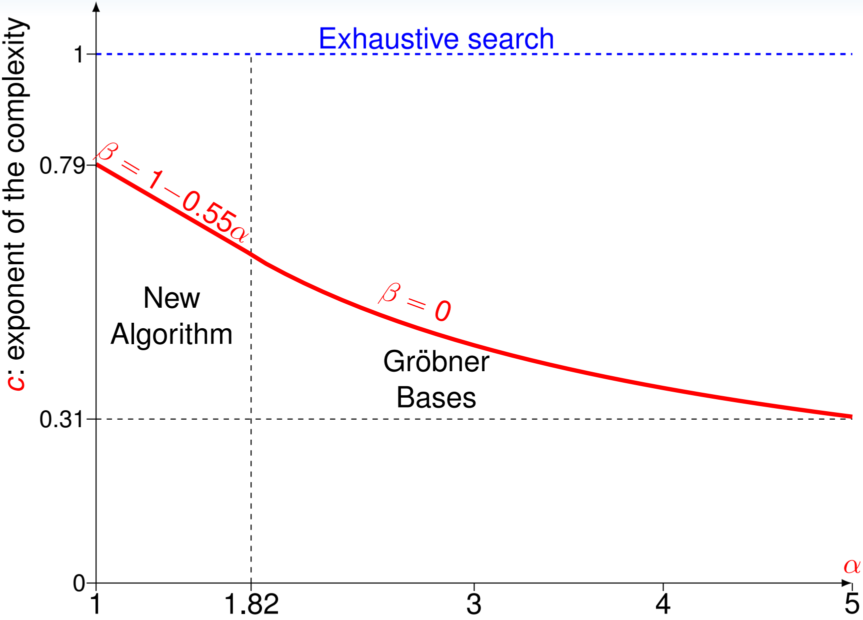
Theorem

A Boolean quadratic polynomials $(f_1, \ldots, f_{\alpha n})$ *which is* $(1 - .55\alpha)$*-strong semi-regular, can be solved in probabilistic time:*

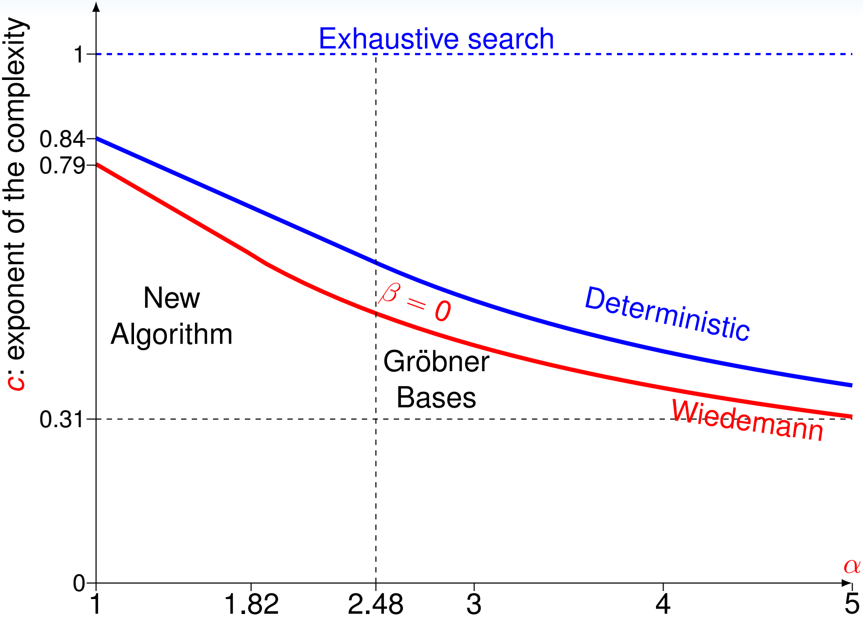
$$O(2^{(1-0.208\alpha)n}) \text{ for } \alpha \leqslant 1.82 \text{ using } \beta = 1 - 0.55\alpha$$

If $\alpha > 1.82$*, the best complexity is achieved for* $\beta = 0$*.*

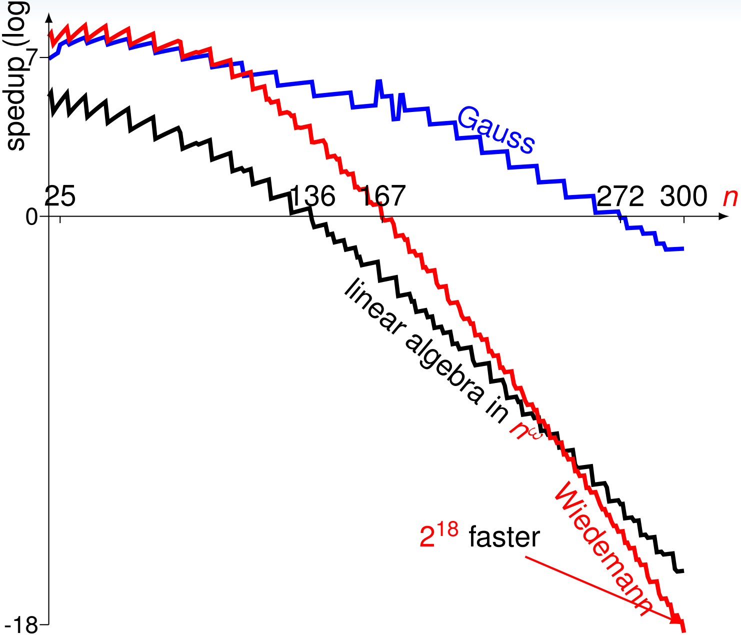
Solving αn equations in n variables: 2^{cn}



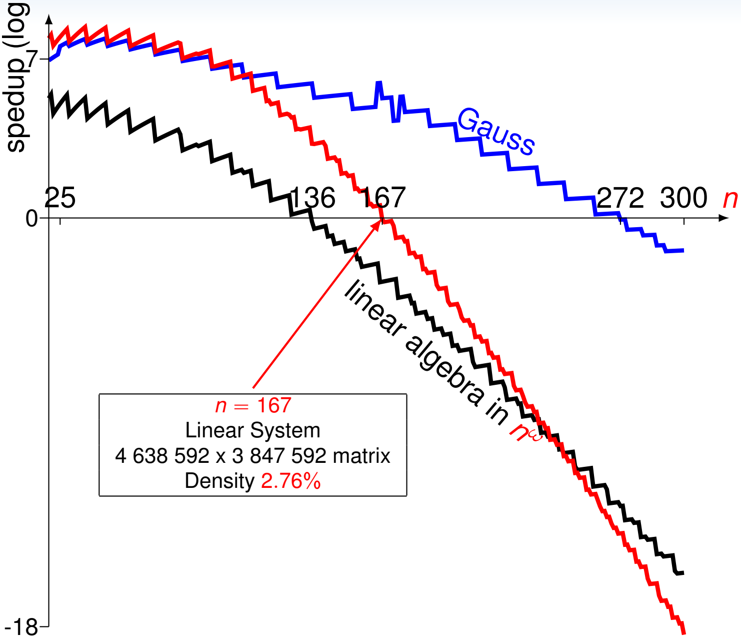
Solving αn equations in n variables: $2^{c\,n}$



Is it practical ? Comparison w Exhaustive Search



Is it practical ? Comparison w Exhaustive Search



Références I

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

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

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

Références II

D. Cox, J. Little, and D. O'Shea.
Ideals, Varieties and Algorithms.
Undergraduate Texts in Mathematics. Springer Verlag, New York, 3rd ed. 2007. corr. 2nd printing, 2008, xvi edition, 2007.
560 p. 93 illus., Hardcover.

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

R. Fröberg.
An introduction to Gröbner bases.
Pure and Applied Mathematics. John Wiley and Sons Ltd., Chichester, 1997.

Références III

S. Lang.
Algebra (3nd Ed.).
Graduate Texts in Mathematics – vol. 211. Springer-Verlag, New York, 2002.

Lazard D.
Gaussian Elimination and Resolution of Systems of Algebraic Equations.
In *Proc. EUROCAL 83*, volume 162 of *Lect. Notes in Comp. Sci*, pages 146–157, 1983.