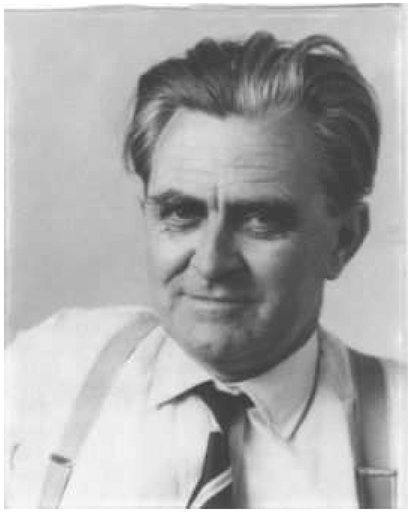
# *From* Gauss

# *to* Gröbner Bases



John Perry

The University of Southern Mississippi

# Overview

- *Questions:* Common zeroes?
- *Tool:* Gaussian elimination $\rightsquigarrow$ Gröbner bases
- *Solutions* to questions
- Recent *advances*

# Part 1: some interesting questions

*Given* $(f_1, f_2, \ldots, f_m)$ *in* $\mathbb{Q}[x_1, x_2, \ldots, x_n]$:

- *are there common zeroes over* $\mathbb{C}^n$*?*
- *if so, dimension of solution space? (variety)*
- *if zero-dimensional, how many solutions?*

# *Example 1*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

- Common zeroes in $\mathbb{C}^2$?
- If so, dimension of solution space?
- If zero-dimensional, how many solutions?

# *Example 1*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

- Common zeroes in $\mathbb{C}^2$?
- If so, dimension of solution space?
- If zero-dimensional, how many solutions?

$$\begin{aligned} x^2 + 1 = 0 &\quad \Longrightarrow \quad x = \pm i \\ y^2 + 1 = 0 &\quad \Longrightarrow \quad y = \pm i \end{aligned}$$

$$\therefore (i, \pm i), (-i, \pm i)$$

# *Example 1*

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$

- Common zeroes in $\mathbb{C}^2$?
- If so, dimension of solution space?
- If zero-dimensional, how many solutions?

# *Motivation*

Mathematical applications

- **Algebraic geometry**
  (Cox, Little, O'Shea textbooks)
- **Algebraic statistics**
  (Sturmfels)
- **Automated theorem proving**
  (various textbooks)
- **Commutative algebra**
  (Kreuzer, Robbiano textbooks)
- **Differential equations and differential algebra**
  (Lidl, Pilz textbook)
- **Partial differential equations**
  (Golubitsky, Hebert, Ovchinnikov)

# *Motivation*

Non-mathematical applications

- **Astronomy** (singularities)
- **Coding Theory** (de Boer, Pellikaan)
- **Cryptography** (cell phones, NSA, Ackerman and Kreuzer)
- **Mathematical biology** (Stigler: reverse-engineering gene networks)
- **Military** (Arnold: automatic radar targeting)
- **Petri nets** (von zur Gathen, Gerhard: parallel processes)

# *Example 1: linear*

$$f_1 = 4w - 8x - 12z \qquad f_2 = 3w + 3y - 12z$$

$$f_3 = 2x + 4y \qquad f_4 = 3y + z$$

- Common zeroes in $\mathbb{C}$?
- If so, dimension of solution set?
- If zero-dimensional, how many solutions?

*Tool: Gaussian elimination*

# *Example 1: linear*

**start with inputs:**

$$\begin{array}{rrrrr} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ 3w & & +3y & -12z & = 0 \end{array}$$

# Example 1: linear

**identify critical pair:**

$$\begin{array}{rrrrl} {\color{red}4w} & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ {\color{red}3w} & & +3y & -12z & = 0 \end{array}$$

# *Example 1: linear*

**compute "subtraction" polynomial s:**

$$\begin{array}{rrrrr} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ & 24x & +12y & -12z & = 0 \end{array}$$

$$-3f_1 + 4f_4 = 24x + 12y - 12z$$

# *Example 1: linear*

**reduce s modulo current F:**

$$\begin{array}{rrrrl} 4w & -8x & & -12z & =0 \\ & 2x & +4y & & =0 \\ & & 3y & +z & =0 \\ & 24x & +12y & -12z & =0 \end{array}$$

$$-3f_1 + 4f_4 = 24x + 12y - 12z$$

# *Example 1: linear*

**reduce s modulo current F:**

$$
\begin{array}{rrrrr}
4w & -8x & & -12z & = 0 \\
 & 2x & +4y & & = 0 \\
 & & 3y & +z & = 0 \\
 & & -36y & -12z & = 0
\end{array}
$$

$$-3f_1 + 4f_4 = 12f_2 - 36y - 12z$$

# *Example 1: linear*

**echelon form!**

$$\begin{array}{rrrrl} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ & & & 0 & = 0 \end{array}$$

$$-3f_1 + 4f_4 = 12f_2 - 12f_3$$

# *Example 1: linear*

**echelon form!**

$$\begin{array}{rrrrl} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ & & & 0 & = 0 \end{array}$$

$$-3f_1 + 4f_4 = 12f_2 - 12f_3$$

***Echelon form:***

- Infinitely many zeroes
- One-dimensional set of zeroes
- $(-13s, -2s, s, -3s)$, $\forall s \in \mathbb{C}$

## *Summary so far*

Given a linear system...

- Gaussian elimination $\rightsquigarrow$ "nice form"
- "nice form" $\rightsquigarrow$ info: zeroes

*What about* ***non****-linear systems???*

# *Aim*

- Linear: Gaussian elimination $\rightsquigarrow$ echelon form
- Non-linear: Buchberger's algorithm $\rightsquigarrow$ Gröbner basis

# Example 2: nonlinear

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$

- Common zeroes in $\mathbb{C}^2$? Yes
- If so, dimension? 0
- If zero-dimensional, how many? 5

*Nice form and its application are not obvious!*

# Part 2: Gröbner bases

*How can we find (and use) this "nice form"?*

## *Goal*

**Algorithm** *"Generalized Gaussian elimination"*

**Input:** $F = (f_1, f_2, \ldots, f_m)$

**Output:** $G = (g_1, g_2, \ldots, g_r)$, a "nice form" of $F$

# *Goal*

**Algorithm** *"Generalized Gaussian elimination"*

**Input:** $F = (f_1, f_2, \ldots, f_m)$

**Output:** $G = (g_1, g_2, \ldots, g_r)$, a "nice form" of $F$

1. $G = F$
2. Identify "critical pairs" $p, q$ from pivots
3. Loop through critical pairs:
   (a) $s = \sigma_p p - \sigma_q q$
   (b) reduce $s$ modulo $G$, append reduced to $G$
4. ***"Nice form"?***

YES: Done!

NO: go to 2

# *Generalize to non-linear:*

- Pivots?
- Elimination?
- Reduction?
- “Nice form”?

# Pivots?

$$f_1 = x^2 + xy + y^2 \qquad f_2 = xz + z^3$$

- For $f_1$:

$$x^2 + xy + y^2 \quad x^2 + xy + y^2 \quad x^2 + xy + y^2$$

- For $f_2$:

$$xz + z^3 \quad xz + z^3$$

# *Pivots? Leading terms!*

**Notation:** leading term $\leftrightsquigarrow \mathbf{lt}_{\succ}(f)$

**Term ordering** ($\succ$) **admissible iff** $\forall t, u, v \in \mathcal{T}$

1. $u \succ v$ or $v \succ u$ or $u = v$
2. $u \mid v$ implies $v \succ u$ or $v = u$
3. $u \succ v$ implies $tu \succ tv$

# Leading terms, examples

$$f_1 = x^2 + xy + y^2 \qquad f_2 = xz + z^3$$

- **lex** $(x \succ y \succ z)$:

$$x^2 + xy + y^2 \qquad xz + z^3$$

- **tdeg** $(x \succ y \succ z)$:

$$x^2 + xy + y^2 \qquad xz + z^3$$

# *Term orderings: notes*

- $\{\succ\} \quad \rightsquigarrow \quad \mathbb{R}^{m\times n}$

$$\textbf{lex} \leftrightsquigarrow \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix} \qquad \textbf{tdeg} \leftrightsquigarrow \begin{pmatrix} & 1 & 1 & 1 \\ \cdots & 1 & 1 & \\ & 1 & & \end{pmatrix}$$

- Use: multiply matrix by exponent vector to obtain "weight vector", compare top to bottom

# *Term orderings: examples*

Compare $x, yz$ using lex:

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

So $x \succ_{\mathrm{lex}} yz$.

# Term orderings: examples

Compare $x, yz$ using tdeg:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$$

So $x \prec_{\mathbf{tdeg}} yz$.

# *Term orderings: notes*

- Often useful to change $\succ$
- To answer our questions, any $\succ$ ok
- To find explicit zeroes, need **lex**

# *Elimination?* S-*polynomials!*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

Multiply to lcm, subtract:

$$\begin{array}{rr} & y^2 \cdot \left(x^2 + 1\right) \\ - & x^2 \cdot \left(y^2 + 1\right) \\ \hline & y^2 - x^2 \end{array}$$

Thus the **S-polynomial**

$$\mathrm{S}_{\succ}(f_1, f_2) = y^2 - x^2$$

# *Reduction? linear case*

Recall

$$\begin{array}{rrrrl} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ & 24x & +12y & -12z & = 0 \end{array} \longrightarrow \cdots$$

$$\cdots \longrightarrow \begin{array}{rrrrl} 4w & -8x & & -12z & = 0 \\ & 2x & +4y & & = 0 \\ & & 3y & +z & = 0 \\ & & & 0 & = 0 \end{array}$$

$$3f_1 - 4f_4 = -12f_2 + 12f_3$$

# *Reduction? non-linear case*

$$f_1 = x^2 + 1$$
$$f_2 = y^2 + 1$$

$$\mathbf{S}_{\succ}(f_1, f_2) \;=\; y^2 - x^2$$

# *Reduction? non-linear case*

$$f_1 = x^2 + 1$$
$$f_2 = y^2 + 1$$

$$\mathrm{S}_{\succ}(f_1, f_2) \;=\; -1 f_1 + 1 f_2$$

# *Representation*

$\mathbf{S}_{\succ}(f_1, f_2)$ has a **representation modulo** $(\mathbf{f_1}, \mathbf{f_2}, \ldots, \mathbf{f_m})$ if $\exists h_1, h_2, \ldots, h_m$ s.t.

- $\mathbf{S}_{\succ}(f_1, f_2) = h_1 f_1 + h_2 f_2 + \cdots + h_m f_m$
- $h_k$'s obtainable by reduction:
  $\forall k = 1, \ldots, m \; h_k \neq 0$ implies

$$\mathbf{lt}_{\succ}(h_k) \cdot \mathbf{lt}_{\succ}(f_k) \prec \mathbf{lcm}(\mathbf{lt}_{\succ}(f_1), \mathbf{lt}_{\succ}(f_2))$$

# ***Representation, example***

Consider

$$f_1 = x^4 + x^3 - 11x^2 - 9x + 18$$
$$f_2 = x^2y - 3x^2 - xy + 3x - 6y + 18$$

$$\mathbf{S}_{\succ}(f_1, f_2) \;=\; 2x^3y - 5x^2y - 9xy + 18y + 3x^4 - 3x^3 - 18x^2$$

# *Representation, example*

Consider

$$f_1 = x^4 + x^3 - 11x^2 - 9x + 18$$
$$f_2 = x^2y - 3x^2 - xy + 3x - 6y + 18$$

$$\begin{aligned} \mathbf{S}_{\succ}(f_1, f_2) &= -3x^2y + 3xy + 18y + 3x^4 - 3x^3 - 24x^2 - 36x \\ &\quad +2x f_2 \end{aligned}$$

# *Representation, example*

Consider

$$f_1 = x^4 + x^3 - 11x^2 - 9x + 18$$
$$f_2 = x^2y - 3x^2 - xy + 3x - 6y + 18$$

$$\begin{aligned} \mathbf{S}_{\succ}(f_1, f_2) &= 3x^4 + 3x^3 - 33x^2 - 27x + 54 \\ &\quad + (2x-3)\,f_2 \end{aligned}$$

# Representation, example

Consider

$$f_1 = x^4 + x^3 - 11x^2 - 9x + 18$$
$$f_2 = x^2y - 3x^2 - xy + 3x - 6y + 18$$

$$\mathbf{S}_{\succ}(f_1, f_2) \;=\; 3f_1 + (2x-3)f_2$$

- $\mathbf{lt}_{\succ}(3) \cdot \mathbf{lt}_{\succ}(f_1) = 3x^4 \quad \prec \quad x^4y$
- $\mathbf{lt}_{\succ}(2x-4) \cdot \mathbf{lt}_{\succ}(f_2) = 2x^3y \quad \prec \quad x^4y$
- $h_3 = 0$

# *Nice form?*

**Difficulty:**

$$f_1 = xy + z \qquad f_2 = y^2 - z \qquad \succ = \mathbf{tdeg}(x \succ y \succ z)$$

$$\mathbf{S}_\succ(f_1, f_2) = yz - xz$$

$$\mathbf{S}_\succ(f_1, f_2) \quad \rightsquigarrow \quad \textbf{new}\ \text{leading terms}$$

Linear analogue:

$$\begin{array}{rrrrl} w & +2x & -5y & +z & =0 \\ & x & +3y & +z & =0 \\ & & & z & =0 \\ 2w & +4x & & & =0 \end{array} \quad \rightsquigarrow \quad \begin{array}{rrrrl} w & +2x & -5y & +z & =0 \\ & x & +3y & +z & =0 \\ & & & z & =0 \\ & & 10y & -2z & =0 \end{array}$$

# *Nice form: definition*

$F$ is a **Gröbner basis** iff

$$\forall p \in \mathscr{I}(f_1, f_2, \ldots, f_m)$$

$$\mathbf{lt}_{\succ}(f_k) \mid \mathbf{lt}_{\succ}(p) \text{ for some } k = 1, \ldots, m$$

where $\mathscr{I}(f_1, f_2, \ldots, f_m)$ is
the ideal of $F$ in $\mathbb{Q}[x_1, x_2, \ldots, x_n]$; that is,

$$\{h_1 f_1 + h_2 f_2 + \cdots + h_m f_m : h_1, h_2, \ldots, h_m \in \mathbb{Q}[x_1, x_2, \ldots, x_n]\}$$

# *Nice form? result*

**Theorem (Buchberger, 1965)**

$$F \text{ is a Gröbner basis}$$

$$\Updownarrow$$

$$\text{every } \mathbf{S}_{\succ}\left(f_i, f_j\right) \text{ has a representation modulo } F$$

# *Nice form? algorithm*

**Algorithm** *"Gröbner basis"* (Buchberger, 1965)

**Input:** $F = (f_1, f_2, \ldots, f_m), \succ$

**Output:** $G = (g_1, g_2, \ldots, g_n)$, a Gröbner basis of $F$ wrt $\succ$

1. $G = F$
2. Identify critical pairs $g_i, g_j$ from $t_i, t_j$ $\forall i \neq j$
3. Loop through critical pairs:
   (a) $\mathbf{S}_{\succ}(f_i, f_j) = \sigma_{ij} g_i - \sigma_{ji} g_j$
   (b) Reduce $\mathbf{S}_{\succ}(g_i, g_j)$ modulo $G$, append to $G$
4. Gröbner basis?

   YES: Done!

   NO: go to 2

# *Part 3: Solutions to questions*

*How do Gröbner bases answer our questions?*

# *Common zeroes?*

$$F \text{ has common zeroes}$$

$$\Updownarrow$$

$$\text{GBasis}(F) \text{ has common zeroes}$$

$$\Updownarrow$$

$$\text{constant} \notin \text{GBasis}(F)$$

Linear parallel:

$$x + y = 0$$

$$-1 = 0$$

# Common zeroes? example 1

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

# *Common zeroes? example 1*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

$$\text{GBasis}(F) = F$$

$$\left( \begin{array}{rcl} \mathbf{S}_{\succ}(f_1, f_2) & = & y^2 - x^2 \\ & = & f_2 - f_1 \end{array} \right)$$

$$c \notin F \text{ for any } c \in \mathbb{C}$$

$\therefore$ **COMMON ZEROES**

# Common zeroes? example 2

$$f_2 = f_1 + 1$$

# *Common zeroes? example 2*

$$f_2 = f_1 + 1$$

$$\mathrm{S}_{\succ}(f_1, f_2) \quad = \quad -1$$

$$\mathrm{GBasis}(F) = \{f_1, f_2, -1\}$$

$\therefore$ **NO COMMON ZEROES**

# *Finitely many solutions?*

Finitely many zeroes
*(Zero-dimensional)*

$$\Updownarrow$$

a power of *each* variable
appears in LeadingTerms(GBasis($F$))

Linear parallel: all variables in diagonal

$$\begin{array}{cccrr}
x & -y & +z & & 3 \\
 & 3y & +z & & -5 \\
 & & z & = & 1
\end{array}$$

# *Dimension of zeroes? example 1*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$

$x^i$ in $f_1$, $y^j$ in $f_2$

$\therefore$ **ZERO-DIMENSIONAL!**

# *Dimension of zeroes?*

Dimension of Zeroes($F$)

$$
\begin{aligned}
&= \text{Dimension of Zeroes(GBasis(}F\text{))} \\
&= \text{Dimension of Zeroes(LeadingTerms(GBasis(}F\text{))}
\end{aligned}
$$

# *Dimension of zeroes? example 2*

$$f_1 = wx + \cdots \qquad f_2 = wy + \cdots \qquad f_3 = wz + \cdots$$

- $x^i$ not a leading term $\Longrightarrow$ not zero-dimensional
- Dimension of Zeroes$(F)$

  $= \text{Dimension of Zeroes}(wx,\ wy,\ wz)$

  $= 3$ $\qquad (0, s, t, u)\ \forall s, t, u \in \mathbb{C}$

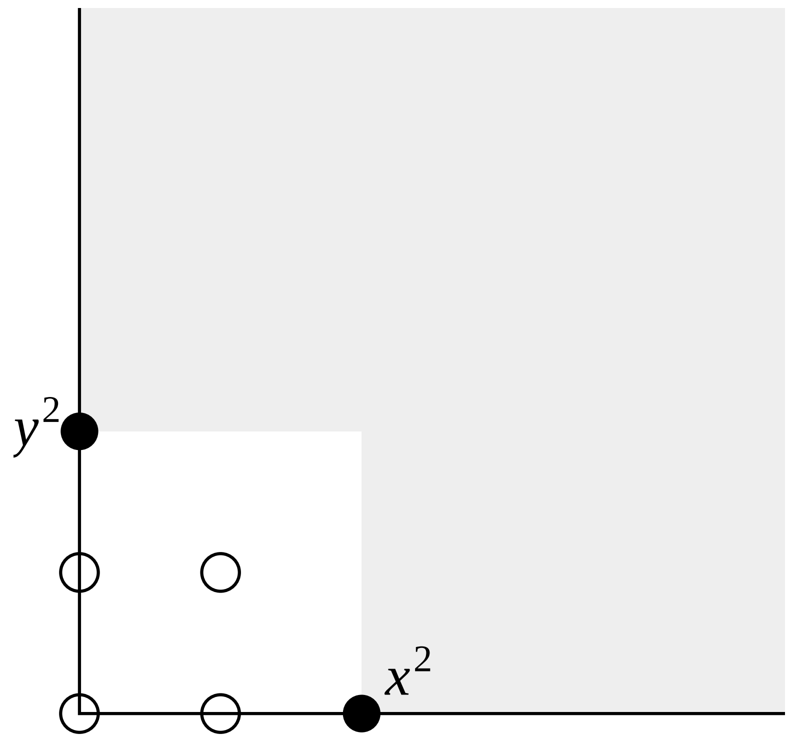
# *Number of zeroes?*

- Plot lt's on axis
- count terms *not* divisible by lt's

(Why? Span $\left(\mathbf{x}^{\mathbf{i}} : \mathbf{x}^{\mathbf{i}} \notin \mathscr{I}\left(t_1, \ldots, t_m\right)\right) \cong \dfrac{\mathbb{C}\left[x_1, \ldots, x_n\right]}{\mathscr{I}\left(f_1, f_2, \ldots, f_m\right)}$)

# *Number of zeroes? example 1*

$$f_1 = x^2 + 1 \qquad f_2 = y^2 + 1$$



# *Summary of method*

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$
$$\prec = \mathrm{lex}(y \prec x)$$

$$S_{\prec}(f_1, f_2) = -f_1 + f_2 + \left(-x^2 - 2y^2 + 3\right)$$

$\therefore$ Add $f_3 = x^2 + 2y^2 - 3$

# *Summary of method*

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$
$$f_3 = x^2 + 2y^2 - 3$$

$$\mathbf{S}_{\prec}(f_1, f_3) = -f_1 - 2f_3 + \left(2y^4 - 6y^2 + 4\right)$$

$\therefore$ Add $f_4 = y^4 - 3y^2 + 2$

# Summary of method

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$
$$f_3 = x^2 + 2y^2 - 3$$
$$f_4 = y^4 - 3y^2 + 2$$

$$\mathrm{S}_{\prec}(f_2, f_3) = -f_3 + \left(2y^3 - 2y^2 - 4y + 4\right)$$

$\therefore$ Add $f_5 = y^3 - y^2 - 2y + 2$

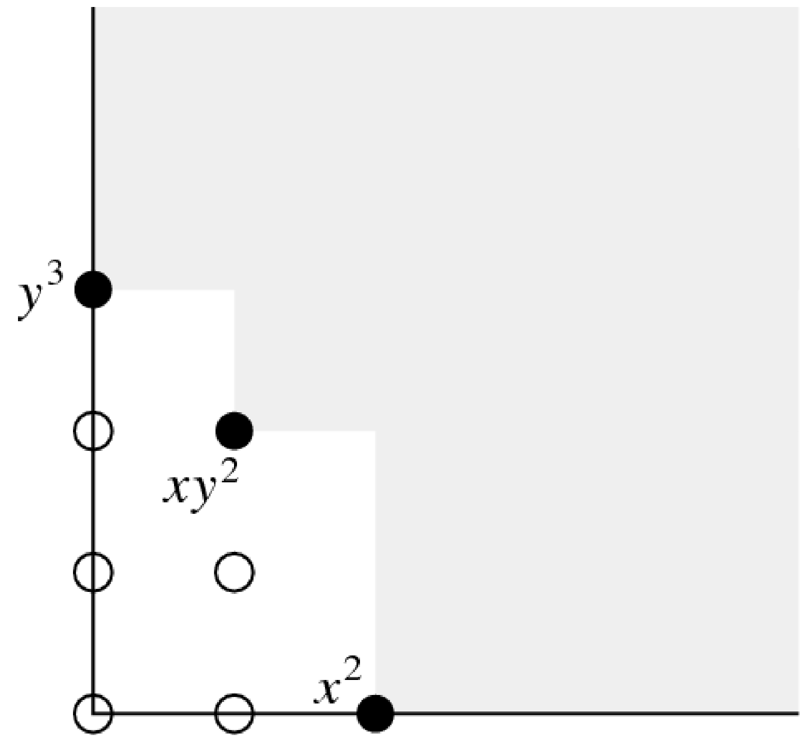
# Summary of method

$$f_1 = xy^2 - 2x - y^2 + 2$$
$$f_2 = x^2y - x^2 + y - 1$$
$$f_3 = x^2 + 2y^2 - 3$$
$$f_4 = y^4 - 3y^2 + 2$$
$$f_5 = y^3 - y^2 - 2y + 2$$

$$\mathrm{GB}(\{f_1, f_2\}) = \{f_1, f_2, f_3, f_4, f_5\}$$

# *Summary of method*

leading terms: $xy^2, x^2y, x^2, y^4, y^3$




*five* solutions

(in fact $f_1 = (x-1)\left(y^2-1\right)$ and $f_2 = \left(x^2+1\right)(y-1)$)

# *Part 3: Recent advances*

*Optimizations of Buchberger's algorithm?*

# ***Difficulty with Gröbner bases***

Worst-case:

***Doubly-exponential in variables, total degree***

Can we skip some $S$-polys?

# Skip? previous work

1965 Buchberger, B.

1979 Buchberger, B.

1988 Gebauer, R. and Möller, H.

2002 Caboara, M.; Kreuzer, M.; Robbiano, L.

2003 Faugère, J.C. (criterion on other terms, coefficients)

# *Skip? example 1*

$$f_1 = x^2 + R_1 \qquad f_2 = y^2 + R_2$$

$$\mathbf{S}_{\succ}(f_1, f_2) \;=\; R_1 f_2 - R_2 f_2$$

$\therefore$ We can skip $\mathbf{S}_{\succ}(f_1, f_2)$!

# *Skip? first result!*

**Theorem BCRP** *(Buchberger, 1965)*

***If*** $t_1, t_2$ are relatively prime

***Then*** can skip $\mathbf{S}_{\succ}(f_1, f_2)$
$\forall f_1, f_2$ with leading terms $t_1, t_2$

Linear parallel: two equations already in "nice form"

$$\begin{array}{ccc} x & +2y & +\cdots \\ 0 & 3y & +\cdots \end{array}$$

# *Skip? summary example*

leading terms: $xy^2, x^2y, x^2, y^4, y^3$

$$\begin{aligned}
\mathbf{S}_{\succ}(f_3, f_4) &= y^3\mathbf{S}_{\succ}(f_2, f_3) + \mathbf{S}_{\succ}(f_2, f_4) \\
\mathbf{S}_{\succ}(f_3, f_5) &= y^2\mathbf{S}_{\succ}(f_2, f_3) + \mathbf{S}_{\succ}(f_2, f_5)
\end{aligned}$$

$\therefore$ We can skip $\mathbf{S}_{\succ}(f_3, f_4)$ and $\mathbf{S}_{\succ}(f_3, f_5)$!

# *Skip? second result!*

**Theorem BCLD** *(Buchberger, 1979)*

***If*** $t_2$ divides $\mathbf{lcm}(t_1, t_3)$

***Then*** can skip $\mathbf{S}_{\succ}(f_1, f_3)$
$\forall f_1, f_2, f_3$ with leading terms $t_1, t_2, t_3$

# *How common are BC skips?*

| BCRP, BCLD skips | not skipped | Polys in GB |
|---|---|---|
| 16 | 11 | 8 |
| 22 | 14 | 9 |
| 113 | 77 | 20 |
| 13 | 23 | 9 |
| 244 | 133 | 28 |
| 22 | 29 | 11 |

- compute GBasis of polynomials $f_1, f_2, f_3$
- two to five variables
- two to five monomials, total degree 5, exponents from 0 to 10
- random coefficients in $\mathbb{Z}_2$
- total-degree term ordering

# *Skip? example 3*

$$f_1 = wx + \cdots \qquad f_2 = wy + \cdots \qquad f_3 = wz + \cdots$$

$$\begin{array}{rcrcrcr} \mathbf{S}_\succ(f_1,f_2) & = & 1\cdot f_1 & + & 3\cdot f_2 & & \\ \mathbf{S}_\succ(f_2,f_3) & = & & & -2\cdot f_2 & + & 1\cdot f_3 \\ \mathbf{S}_\succ(f_1,f_3) & = & -2\cdot f_1 & & & - & 3\cdot f_3 \end{array}$$

Curious pattern...

# *Skip? Third result!*

**Theorem EBC3** *(To appear 2007)*

***If*** (EC-div) and (EC-var)

***Then*** can skip $\mathbf{S}_{\succ}(f_1, f_3)$ **modulo** $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3)$
$\forall f_1, f_2, f_3$ with leading terms $t_1, t_2, t_3$

# *Skip? Third result!*

**Theorem EBC3** *(To appear 2007)*

***If*** (EC-div) and (EC-var)

***Then*** can skip $\mathbf{S}_{\succ}(f_1, f_3)$ **modulo** $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3)$
$\forall f_1, f_2, f_3$ with leading terms $t_1, t_2, t_3$

(EC-div): $\gcd(t_1, t_3) \mid t_2$, *or*
$t_2 \mid \mathbf{lcm}(t_1, t_3)$

(EC-var): $\forall x$ $\deg_x t_1 = 0$, *or*
$\deg_x t_3 = 0$, *or*
$\deg_x t_2 \leq \max(\deg_x t_1, \deg_x t_3)$

# *How often can we skip?*

*Chained* Polynomial Skips

| vars | BCRP, BCLD skips | EC skips |
|---|---|---|
| 3 | ~53,000 | ~7,000 |
| 4 | ~43,000 | ~6,000 |
| 5 | ~35,000 | ~5,000 |
| 6 | ~28,000 | ~4,000 |

- 100,000 triplets $t_1, t_2, t_3$
- maximum degree of each indeterminate: 10
- ordered from least to greatest
- consistent in lexicographic, total-degree term orderings

# *Skip? new result!*

**Theorem NC*m*** *(Discovered Dec. 2006)*

***If*** (BCLM) or (EC)

***Then*** can skip $\mathbf{S}_{\succ}\left(f_1, f_m\right)$ **modulo** $\left(\mathbf{f_1}, \mathbf{f_2}, \ldots, \mathbf{f_m}\right)$
$\forall f_1, f_2, \ldots, f_m$ with leading terms $t_1, t_2, \ldots, t_m$

# *Skip? new result!*

**Theorem NC*m*** *(Discovered Dec. 2006)*

***If*** (BCLM) or (EC)

***Then*** can skip $\mathbf{S}_{\succ}\left(f_1, f_m\right)$ **modulo** $\left(\mathbf{f_1}, \mathbf{f_2}, \ldots, \mathbf{f_m}\right)$
$\forall f_1, f_2, \ldots, f_m$ with leading terms $t_1, t_2, \ldots, t_m$

$$
\text{(EC):} \quad \begin{array}{rl}
\forall k : 1 \leq k \leq m & \gcd\left(t_1, t_m\right) \mid t_k, \text{ and} \\
\forall x & \deg_x t_1 = 0, \textit{ or} \\
& \deg_x t_3 = 0, \textit{ or} \\
& \deg_x t_1 \leq \deg_x t_2 \leq \cdots \leq \deg_x t_m, \textit{ or} \\
& \deg_x t_1 \geq \deg_x t_2 \geq \cdots \geq \deg_x t_m
\end{array}
$$

# *Skip? fifth result!*

**Corollary**

***If*** $t_k = x_0 x_k$ for $k = 1, \ldots, m$

***and*** for $i = 1, \ldots, m-1$
$\mathrm{S}_\succ(f_i, f_{i+1})$ has a representation modulo $(f_1, \ldots, f_m)$,

***Then*** $(f_1, \ldots, f_m)$ is GB
$\forall f_1, \ldots, f_m$ with leading terms $t_1, \ldots, t_m$

# Summary

| | *Gauss* |
|---|---|
| “nice form”? | elimination does not introduce lt |
| elimination | lcm of coefficients, subtract |
| common zeroes? | consistent systems |
| dimension of zeroes? | variables that are not pivots |
| number of zeroes? | zero, one, infinite |

## *Summary*

| | *Gröbner* |
|---|---|
| "nice form"? | $S$-poly does not introduce lt |
| elimination | lcm of lts, subtract |
| common zeroes? | no constant in basis |
| dimension of zeroes? | dimension of lts |
| number of zeroes? | terms not divided by lts |

# Questions

1. GB detection?
   (Exists $\succ$ such that already GB?)
2. GBs under composition?
   (“Chain Rule” for GB computation?)
3. Criterion in noncommutative rings?
   ($xy \neq yx$, with possible application to cryptography)

# *Finis*

***Thank you!***