Symbolic Computation: Current Trends

Bruno Buchberger

Talk at ACAT05 (Algorithmic Information Theory)
DESY, Zeuthen, Germany, May 26, 2005

RISC (Research Institute for Symbolic Computation)
Johannes Kepler University

RICAM (Radon Institute for Computational and Applied Mathematics)
Austrian Academy of Science

Linz, Austria

The Evolution of "Computing"

More Theory

Numerics

algorithms
in

approximate
finitary representations

of infinite
mathematical structures

Symbolics

algorithms
in

isomorphic
finitary representation

of infinite
mathematical structures

3 of 47

The Evolution of "Computing"

More Theory

„Intellectics“

algorithms
for

exploring theories

Numerics

algorithms
in

approximate
finitary representations

of infinite
mathematical structures

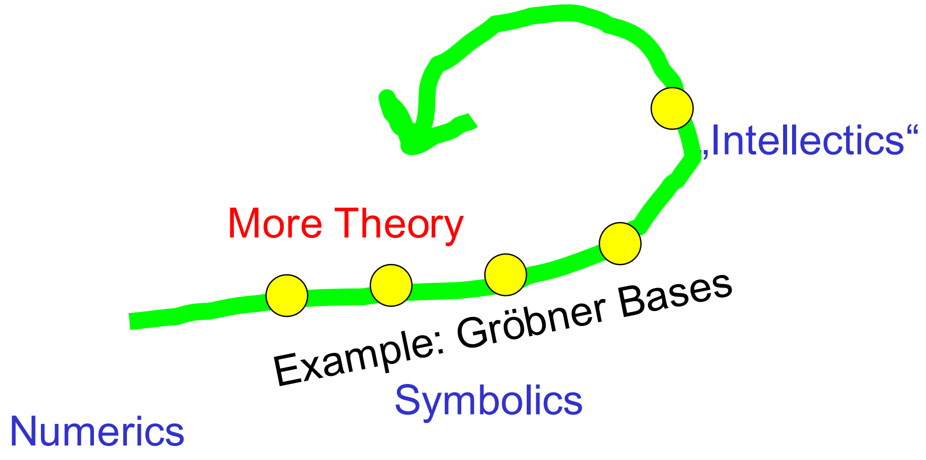
Symbolics

algorithms
in

isomorphic
finitary representation

of infinite
mathematical structures

In This Talk



5 of 47

Current Math Systems

More Interaction Numerics / Symbolics

More Symbolics

More Intellectics

Appendix

Current Math Systems

More Interaction Numerics / Symbolics

More Symbolics

More Intellectics

7 of 47

All Current Algorithmics (Numerics, Symbolics,...) is Available in Systems

- Systems like *Mathematica*, Maple, Derive, Mathlab, ... FORM, Singular, Cocoa, ...
- An enormous potential for science (physics, ...) and engineering.
- Help!

8 of 47

Example:

```
DSolve[{y''[x] == a y'[x] + y[x], y[0] == 1, y'[0] == 0}, y, x]
```

$$\left\{\left\{y \to \text{Function}\left[\{x\}, \frac{a\, e^{\frac{1}{2}\left(a-\sqrt{4+a^2}\right)x} + \sqrt{4+a^2}\, e^{\frac{1}{2}\left(a-\sqrt{4+a^2}\right)x} - a\, e^{\frac{1}{2}\left(a+\sqrt{4+a^2}\right)x} + \sqrt{4+a^2}\, e^{\frac{1}{2}\left(a+\sqrt{4+a^2}\right)x}}{2\sqrt{4+a^2}}\right]\right\}\right\}$$

Example:

$$\text{Solve}\left[\left\{\frac{1}{s}+\frac{1}{t}==\frac{1}{F}, \frac{1}{d+s}+\frac{1}{t-e}==\frac{1}{F}, c==\frac{e\,F}{f\,(t-e)}, M==\frac{t}{s}\right\}, \{d, e, s, t\}\right]$$

$$\left\{\left\{d \to -\frac{c\,f\,F\,(1+M)}{M\,(c\,f-F\,M)}, e \to \frac{c\,f\,F\,(1+M)}{c\,f+F}, s \to \frac{F\,(1+M)}{M}, t \to F\,(1+M)\right\}\right\}$$

Remark:

There is lots of new and deep mathematics behind the (numeric, discrete, graphic, algebraic, and symbolic) algorithms of the current math systems.

In this talk only one example: Gröbner bases theory:

- What are Gröbner bases?
- How can Gröbner bases be computed?
- Why are Gröbner bases important? (Dozens of fundamental problems can be reduced to Gröbner bases construction!)

The Linear Combination of Polynomials

```
f1 = -2 y + x y
f2 = -x^2 + y^2
```

Leading power products: w.r.t. an ordering of the power products (e.g. lexicographically, by total degreee or ...)

Consider now the following linear combination of f_1 and f_2:

```
g = (y) f1 + (-x + 2) f2
```

$y\,(-2\,y + x\,y) + (2 - x)\,(-x^2 + y^2)$

```
g = (y) f1 + (-x + 2) f2 // Expand
```

$-2\,x^2 + x^3$

Observation: The leading power product x^3 of g is

neither a multiple of the leading power product $x\,y$ of f_1

nor a multiple of the leading power product y^2 of f_2.

Definition of Groebner Bases

A set F of polynomials is called a Groebner basis (w.r.t. the chosen ordering of power products) iff the above phenomenon cannot happen, i.e.

for all $f_1,\ \ldots,\ f_m \in$ F and all (infinitely many) polynomials $h_1,\ \ldots,\ h_m$,

the leading power product of $h_1\,f_1\, +\, \ldots\, +\, h_m\,f_m$

is a multiple of the leading power product of

at least one of the polynomials in F.

Counterexample: The Set $F = \{f_1, f_2\}$ of the Above Example is not a Groebner basis.

The "Main Theorem" of Gröbner Bases Theory (BB 1965):

F is a Gröbner basis $\Longleftrightarrow \underset{f_1, f_2 \in F}{\forall}$ remainder[F, S–polynomial[f_1, f_2]] = 0.

```
S-polynomial[-2 y + x y, -x^2 + y^2] = y (-2 y + x y) - x (-x^2 + y^2)
```

$x^3 - 2\,y^2$

Proof: Nontrivial. Combinatorial.

The theorem reduces an infinite check to a finite check: Recall definition of "F is a Gröbner basis":

for all $f_1, \ldots, f_m \in$ F and all (infinitely many) polynomials $h_1, \ldots, h_m$,

the leading power product of $h_1 f_1 + \ldots + h_m f_m$

is a multiple of the leading power product of at least one of the polynomials in F.

The power of the Gröbner bases method is contained in this theorem and its proof.

The Problem of *Constructing* Gröbner Bases

Given F, find G such that G is a Gröbner basis

and F and G generate the same set of linear combinations.

An Algorithm for *Constructing* Gröbner Bases (BB 1965)

Recall the main theorem:

F is a Gröbner basis $\Longleftrightarrow \underset{f_1, f_2 \in F}{\forall}$ remainder[F, S–polynomial[f_1, f_2]] = 0.

Based on the main theorem, the problem can be solved by the following algorithm:

Start with G:= F.

For any pair of polynomials f_1, $f_2 \in G$:

h := remainder[G, S–polynomial[f_1, f_2]]

If $h = 0$, consider the next pair.

If $h \neq 0$, add h to G and iterate.

Termination of the Algorithm

Termination: by Dickson's Lemma (Dickson 1913, BB 1970).

Example of Application: Solve Systems

```
f1 = x y - 2 y z - z;
f2 = y^2 - x^2 z + x z;
f3 = z^2 - y^2 x + x;

F = {f1, f2, f3};
```

```
{time, G} = GroebnerBasis[F] // Timing
```

$$\{0.01\,\text{Second}, \{z + 4 z^3 - 17 z^4 + 3 z^5 - 45 z^6 + 60 z^7 - 29 z^8 + 124 z^9 - 48 z^{10} + 64 z^{11} - 64 z^{12},$$
$$-22001 z + 14361 y z + 16681 z^2 + 26380 z^3 + 226657 z^4 + 11085 z^5 - 90346 z^6 - 472018 z^7 - 520424 z^8 - 139296 z^9 - 150784 z^{10} + 490368 z^{11},$$
$$43083 y^2 - 11821 z + 267025 z^2 - 583085 z^3 + 663460 z^4 - 2288350 z^5 + 2466820 z^6 - 3008257 z^7 + 4611948 z^8 - 2592304 z^9 + 2672704 z^{10} - 1686848 z^{11},$$
$$43083 x - 118717 z + 69484 z^2 + 402334 z^3 + 409939 z^4 + 1202033 z^5 - 2475608 z^6 + 354746 z^7 - 6049080 z^8 + 2269472 z^9 - 3106688 z^{10} + 3442816 z^{11}\}\}$$

```
zsol = NSolve[G[[1]] == 0, z]
```

$\{\{z \to -0.331304 - 0.586934\, i\}, \{z \to -0.331304 + 0.586934\, i\}, \{z \to -0.296413 - 0.705329\, i\}, \{z \to -0.296413 + 0.705329\, i\}, \{z \to -0.163124 - 0.37694\, i\}, \{z \to -0.163124 + 0.37694\, i\}, \{z \to 0.\}, \{z \to 0.0248919 - 0.89178\, i\}, \{z \to 0.0248919 + 0.89178\, i\}, \{z \to 0.468852\}, \{z \to 0.670231\}, \{z \to 1.39282\}\}$

```
Gsubnum = G /. zsol[[1]]
```

$\{1.33227 \times 10^{-15} + 9.71445 \times 10^{-17}\, i, (-523.519 - 4967.65\, i) - (4757.86 + 8428.97\, i)\, y, (-7846.9 - 8372.06\, i) + 43083\, y^2, (-16311.7 + 16611.\, i) + 43083\, x\}$

```
ysol = NSolve[ Gsubnum[[2]] == 0, y]
```

$\{\{y \to -0.473535 - 0.205184\, i\}\}$

Theorem (Roider, Kalkbrener et al. 1990): It suffices to consider the poly in y with lowest degree.

```
xsol = NSolve[ Gsubnum[[4]] == 0, x]
```

$\{\{x \to 0.378611 - 0.385558\, i\}\}$

```
F /. zsol[[1]] /. ysol[[1]] /. xsol[[1]]
```

$\{3.88578 \times 10^{-16} + 1.3739 \times 10^{-15}\, i, -9.15934 \times 10^{-16} - 2.91434 \times 10^{-16}\, i, -1.05471 \times 10^{-15} - 6.66134 \times 10^{-16}\, i\}$

18 of 47

Example of Application: Invariant Theory

A Question: Can

```
h = x1^7 x2 - x1 x2^7
```

$x_1^7\, x_2 - x_1\, x_2^7$

be expressed as a polynomial in

```
F = {x1^2 + x2^2, x1^2 x2^2, x1^3 x2 - x1 x2^3}
```

$\{x_1^2 + x_2^2, x_1^2\, x_2^2, x_1^3\, x_2 - x_1\, x_2^3\}$

?

Note: These polynomials are fundamental invariants for the group $\mathbb{Z}_4$.

19 of 47

Reduction to Groebner Bases Computation

```
{time, GB} = GroebnerBasis[
  {-i1 + x1^2 + x2^2, -i2 + x1^2 x2^2, -i3 + x1^3 x2 - x1 x2^3}, {x2, x1, i3, i2, i1}] // Timing
```

$$\{0.011\,\text{Second}, \{i_1^2 i_2 - 4 i_2^2 - i_3^2,\ -i_2 + i_1 x_1^2 - x_1^4,\ i_1^2 i_3 x_1 - 2 i_2 i_3 x_1 - i_1 i_3 x_1^3 + i_1^2 i_2 x_2 - 4 i_2^2 x_2,\ i_1^2 x_1 - 2 i_2 x_1 - i_1 x_1^3 + i_3 x_2,\ -i_1 i_3 + 2 i_3 x_1^2 - i_1^2 x_1 x_2 + 4 i_2 x_1 x_2,\ -i_3 x_1 - 2 i_2 x_2 + i_1 x_1^2 x_2,\ -i_3 - i_1 x_1 x_2 + 2 x_1^3 x_2,\ -i_1 + x_1^2 + x_2^2\}\}$$

```
PolynomialReduce[x1^7 x2 - x1 x2^7, GB,
 {x2, x1, i3, i2, i1}, MonomialOrder -> Lexicographic]
```

$$\left\{\left\{0,\ -i_3 - \frac{1}{2} i_1 x_1 x_2 - x_1^3 x_2,\ 0,\ \frac{3 i_1 x_2}{4} - \frac{1}{2} x_1^2 x_2 + \frac{x_2^3}{2},\ i_1 - \frac{x_1^2}{2} + \frac{3 x_2^2}{4},\ \frac{3 i_1 x_1}{2} + x_1 x_2^2,\ \frac{x_2^4}{2},\ -\frac{1}{4} i_1^2 x_1 x_2 - \frac{1}{2} i_1 x_1 x_2^3 - x_1 x_2^5\right\},\ i_1^2 i_3 - i_2 i_3\right\}$$

Theorem (Sweedler, Sturmfels et al. 1988): *h* can be represented in terms of *I* iff remainder of *h* w.r.t. "Groebner basis of *I* with slack variables" is a polynomial in the slack variables (which gives the representation).

```
i1^2 i3 - i2 i3 /. {i1 -> x1^2 + x2^2, i2 -> x1^2 x2^2, i3 -> x1^3 x2 - x1 x2^3} // Expand
```

$$x_1^7 x_2 - x_1 x_2^7$$

```
R = PolynomialReduce[x1^6 x2 - x1 x2^6, GB,
  {x2, x1, i3, i2, i1}, MonomialOrder -> Lexicographic]
```

$$\left\{\left\{0,\ \frac{i_1 x_1}{2} - i_1 x_2 - x_1^2 x_2,\ 0,\ \frac{3 i_1}{4} - \frac{x_1^2}{2} + \frac{x_2^2}{2},\ -\frac{x_1}{4} + \frac{3 x_2}{4},\ \frac{3 i_1}{4} + x_1 x_2,\ \frac{x_2^3}{2},\ -\frac{1}{4} i_1^2 x_1 - \frac{1}{2} i_1 x_1 x_2^2 - x_1 x_2^4\right\},\ -i_1^3 x_1 + 2 i_1 i_2 x_1 + \frac{1}{2} i_1 i_3 x_1 + i_1^2 x_1^3 - i_2 x_1^3 + \frac{1}{2} i_3 x_1^3 + \frac{1}{2} i_1 i_2 x_2\right\}$$

$x_1^6 x_2 - x_1 x_2^6$ can not be expressed by the fundamental invariants in I.

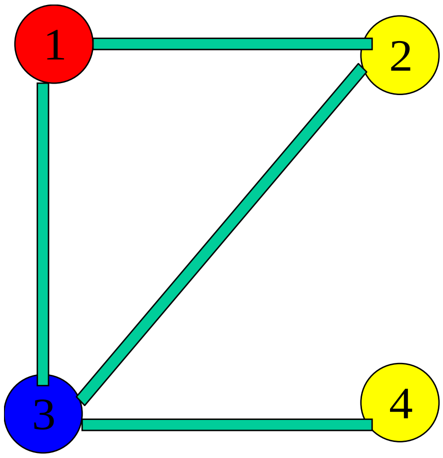
20 of 47

Application: Graph Coloring

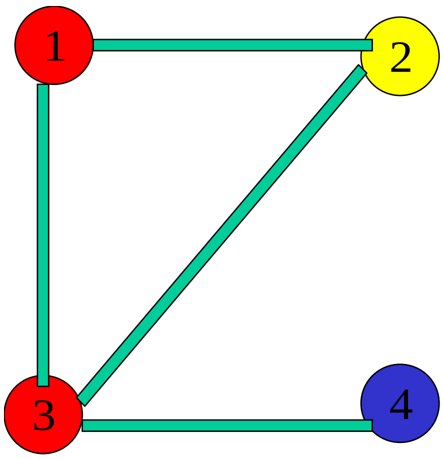
The Problem:

Find all admissible colorings in k colors of a graph with n vertices and edges E:

An admissible coloring in 3 colors of a graph with 4 vertices and edges {1,2}, {1,3}, {2,3}, {3,4}:



Not an admissible coloring in 3 colors of the same graph:



The Translation into a Groebner Bases Problem

Theorem: The possible colorings of the above graph correspond 1-1 to the common solutions of the following set of polynomials:

```
{ -1 + x1^3,     ... at vertex 1 color is a 3 - ary root of 1
  -1 + x2^3,     ... at vertex 2 color is a 3 - ary root of 1
  -1 + x3^3,
 -1 + x4^3,
 x1^2 + x1 x2 + x2^2,   ... the colors at 1 and 2 must be different,
 x1^2 + x1 x3 + x3^2,
 x2^2 + x2 x3 + x3^2,
 x3^2 + x3 x4 + x4^2}
```

22 of 47

Solution by Groebner Bases

Compute a Groebner basis of this polynomial set and compute all solutions.

```
GB = GroebnerBasis[{-1 + x1^3, -1 + x2^3, -1 + x3^3, -1 + x4^3,
   x1^2 + x1 x2 + x2^2, x1^2 + x1 x3 + x3^2, x2^2 + x2 x3 + x3^2, x3^2 + x3 x4 + x4^2},
  {x4, x3, x2, x1}]
```

$\{-1 + x_1^3,\ x_1^2 + x_1 x_2 + x_2^2,\ -x_1 - x_2 - x_3,\ -x_1 x_2 + x_1 x_4 + x_2 x_4 - x_4^2\}$

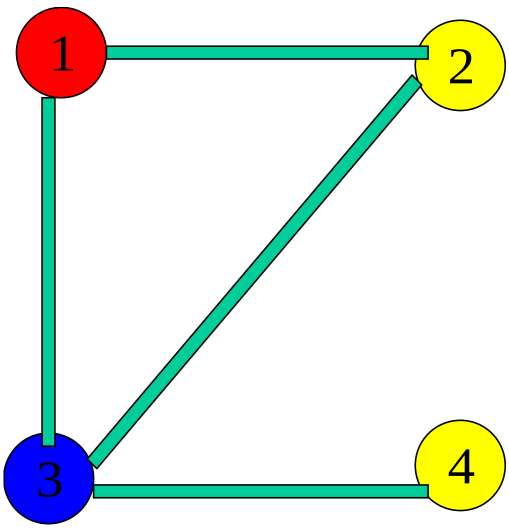
```
Solve[{-1 + x1^3 == 0, -1 + x2^3 == 0, -1 + x3^3 == 0, -1 + x4^3 == 0,
  x1^2 + x1 x2 + x2^2 == 0, x1^2 + x1 x3 + x3^2 == 0, x2^2 + x2 x3 + x3^2 == 0, x3^2 + x3 x4 + x4^2 == 0},
 {x4, x3, x2, x1}]
```

$$
\begin{aligned}
&\{\{x_4 \to 1,\ x_2 \to 1,\ x_1 \to -1 + (-1)^{1/3},\ x_3 \to -(-1)^{1/3}\},\\
&\{x_4 \to 1,\ x_2 \to -1 + (-1)^{1/3},\ x_1 \to 1,\ x_3 \to -(-1)^{1/3}\},\\
&\{x_4 \to 1,\ x_2 \to -1 - (-1)^{2/3},\ x_1 \to 1,\ x_3 \to (-1)^{2/3}\},\\
&\{x_4 \to 1,\ x_2 \to (-1)^{1/3} - (-1)^{2/3},\ x_1 \to -(-1)^{1/3},\ x_3 \to (-1)^{2/3}\},\\
&\{x_4 \to -(-1)^{1/3},\ x_2 \to -1 + (-1)^{1/3},\ x_1 \to -(-1)^{1/3},\ x_3 \to 1\},\\
&\{x_4 \to -(-1)^{1/3},\ x_2 \to -1 - (-1)^{2/3},\ x_1 \to 1,\ x_3 \to (-1)^{2/3}\},\\
&\{x_4 \to -(-1)^{1/3},\ x_2 \to -1 - (-1)^{2/3},\ x_1 \to (-1)^{2/3},\ x_3 \to 1\},\\
&\{x_4 \to -(-1)^{1/3},\ x_2 \to (-1)^{1/3} - (-1)^{2/3},\ x_1 \to -(-1)^{1/3},\ x_3 \to (-1)^{2/3}\},\\
&\{x_4 \to (-1)^{2/3},\ x_2 \to -1 + (-1)^{1/3},\ x_1 \to -(-1)^{1/3},\ x_3 \to 1\},\\
&\{x_4 \to (-1)^{2/3},\ x_2 \to -1 - (-1)^{2/3},\ x_1 \to (-1)^{2/3},\ x_3 \to 1\},\\
&\{x_4 \to -1 + (-1)^{1/3},\ x_2 \to 1,\ x_1 \to -1 + (-1)^{1/3},\ x_3 \to -(-1)^{1/3}\},\\
&\{x_4 \to -1 + (-1)^{1/3},\ x_2 \to -1 + (-1)^{1/3},\ x_1 \to 1,\ x_3 \to -(-1)^{1/3}\}\}
\end{aligned}
$$

Slightly re-organized output:

$$\{\{x_1 \to 1,\ x_2 \to -(-1)^{1/3},\ x_3 \to -1+(-1)^{1/3},\ x_4 \to 1\},$$
$$\{x_1 \to 1,\ x_2 \to -(-1)^{1/3},\ x_3 \to -1+(-1)^{1/3},\ x_4 \to -(-1)^{1/3}\},$$
$$\{x_1 \to 1,\ x_2 \to (-1)^{2/3},\ x_3 \to -1-(-1)^{2/3},\ x_4 \to 1\},$$
$$\{x_1 \to 1,\ x_2 \to (-1)^{2/3},\ x_3 \to -1-(-1)^{2/3},\ x_4 \to (-1)^{2/3}\},$$
$$\{x_1 \to -(-1)^{1/3},\ x_2 \to 1,\ x_3 \to -1+(-1)^{1/3},\ x_4 \to 1\},$$
$$\{x_1 \to -(-1)^{1/3},\ x_2 \to 1,\ x_3 \to -1+(-1)^{1/3},\ x_4 \to -(-1)^{1/3}\},$$
$$\{x_1 \to -(-1)^{1/3},\ x_2 \to -1+(-1)^{1/3},\ x_3 \to 1,\ x_4 \to -(-1)^{1/3}\},$$
$$\{x_1 \to -(-1)^{1/3},\ x_2 \to -1+(-1)^{1/3},\ x_3 \to 1,\ x_4 \to -1+(-1)^{1/3}\},$$
$$\{x_1 \to (-1)^{2/3},\ x_2 \to 1,\ x_3 \to -1-(-1)^{2/3},\ x_4 \to 1\},$$
$$\{x_1 \to (-1)^{2/3},\ x_2 \to 1,\ x_3 \to -1-(-1)^{2/3},\ x_4 \to (-1)^{2/3}\},$$
$$\{x_1 \to (-1)^{2/3},\ x_2 \to -1-(-1)^{2/3},\ x_3 \to 1,\ x_4 \to (-1)^{2/3}\},$$
$$\{x_1 \to (-1)^{2/3},\ x_2 \to -1-(-1)^{2/3},\ x_3 \to 1,\ x_4 \to -1-(-1)^{2/3}\}\}$$

For example, $\{x_1 \to 1,\ x_2 \to -(-1)^{1/3},\ x_3 \to -1+(-1)^{1/3},\ x_4 \to -(-1)^{1/3}\}$ corresponds to



23 of 47

Application: Integer Optimization

Example (B. Sturmfels):

What is the minimum number of coins (e.g. p Pennies, n Nickels, d Dimes, q Quarters) for composing a given value, e.g. 117?

Reduction to Gröbner Bases Problem (C. Traverso et al. 1986):

Code the integer values p, n, d, q as exponents of power products!

Code the goal function as the (generalized) degree of the power products!

Code the exchange rules of the coins (the relations between the quantities) as polynomials consisting of power products:

```
F = {P^5 - N, P^10 - D, P^25 - Q}
```

$\{-N + P^5,\ -D + P^{10},\ P^{25} - Q\}$

Now compute the Gröbner basis of F (w.r.t. degree ordering):

```
G = GroebnerBasis[F, MonomialOrder → DegreeLexicographic]
```

$\{-D + N^2,\ -D^3 + N\,Q,\ D^2\,N - Q,\ -N + P^5\}$

Now you can be sure that, starting with any admissible solution (e.g. (p=17, n=10, d=5, q=0), by reduction modulo G, you will end up with a minimal solution:

```
PolynomialReduce[P^17 N^10 D^5, G, , MonomialOrder → DegreeLexicographic]
```

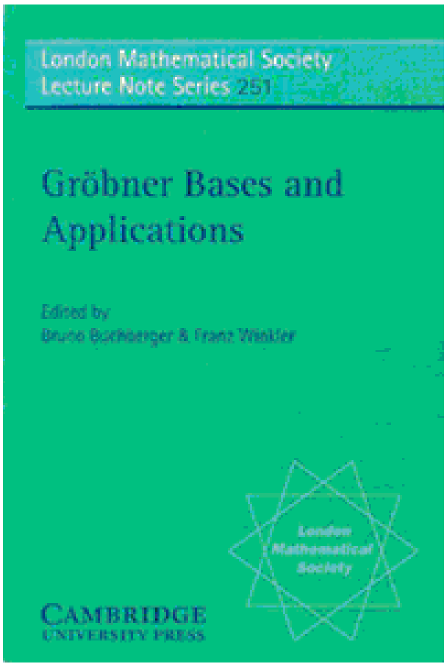
$\{\{D^9\,P^{17} + D^8\,N^2\,P^{17} + D^7\,N^4\,P^{17} + D^6\,N^6\,P^{17} + D^5\,N^8\,P^{17} + D^4\,P^{17}\,Q^2 + P^7\,Q^4,$
$-D^7\,P^{17} - D^4\,N\,P^{17}\,Q - D^2\,P^{17}\,Q^2,\ P^{17}\,Q^3,\ D\,P^2\,Q^4 + N\,P^7\,Q^4 + P^{12}\,Q^4\},\ D\,N\,P^2\,Q^4\}$

Answer: take 4 quarters, 1 dime, 1 nickel, 2 pennies.

More Applications

Gröbner Bases 98 Conference:

B. B., F. Winkler. Gröbner *Bases: Theory and Applications.* Cambridge University Press, 1998. 560 pages.



This book contains tutorials and original papers.

This book contains also:

B. B. *Introduction to Gröbner Bases*, pp. 3-31.

B. B. *An Algorithmic Criterion for the Solvability of Systems of Algebraic Equations, pp. 540-560.* (English translation of the original paper from 1970, in which Gröbner bases were introduced.)

A continuation of this book is the special issue of the JSC on Gröbner bases edited by Q.N. Tran and F. Winkler, 2000.

25 of 47

Current Math Systems

More Interaction Numerics / Symbolics

More Symbolics

More Intellectics

26 of 47

Example: The Numerics of Gröbner Bases

In both directions (H. Stetter 1987 - 2005):

- Start from Gröbner bases and compute solutions (reduction to an eigenvalue problem).
- Numerically, compute (a numerical variant) of Gröbner bases.

27 of 47

Current Math Systems

More Interaction Numerics / Symbolics

More Symbolics

More Intellectics

Example: Computation on Operators

computation on (finitary representations of) numbers: e.g. computation on algebraic numbers

↓

computation on (finitary representations of) functions (on numbers): e.g. symbolic integration

↓

computation on (finitary representations of) operators (on functions): e.g. symbolic generation of Green's funtions for boundary-value problems

Project SFB 1322 (B.B. and H. Engl, RICAM), PhD thesis and postdoc work of M. Rosenkranz:

M.Rosenkranz, B.B, H.W.Engl. Solving Linear BVPs via Non–commutative Gröbner Bases. Applicable Analysis, 82(7), July 2003, pp. 655–675.

M.Rosenkranz. A New Symbolic Method for Solving Linear Two–Point BVPs on the Operator Level. Journal of Symbolic Computation, 39, February 2005, pp.171–199.

29 of 47

Basic Idea and Procedure

FGiven a two–point BVP (e.g. beam equation):

$$T\,u = f$$
$$B_1\,u = \ldots = B_n\,u = 0$$

Example: Beam Deflection

■

We want to find its Green's operator in the sense of

$$T\,G = 1 \quad (i.e.\ T\,(G\,f\,) = f)$$
$$B_1\,G = \ldots = B_n\,G = 0 \quad (i.e.\ B_1(G\,f\,) = 0)$$

We do the following:

- Compute the solution space N of the homogeneous equation $Tu = 0$.
- Determine a projector P onto N such that $M = (1-P)\,C^\infty[a, b]$ fulfills the boundary conditions.
- Find the right inverse $T^\blacklozenge$ of T (a variant of Moore-Penrose inverse).
- Build up $G = (1-P)\,T^\blacklozenge$ as the crude Green's operator.
- Reduce G with respect to the Green's system (a non-commutative Gröbner basis by the main theorem; 233 S-polys needed!) for obtaining a standard representation.
- (Optionally, extract Green's function g from standard representation of G).

30 of 47

The Green's System

```
System["1. Equalities for Isolating Differential Operators", any[f],
                 D A = 1                        "DA"
                 D B = -1                       "DB"
          ----------------------------------------------
          D ⌈f⌉ = ⌈f⌉ D + ⌈f'⌉                  "DM"
          ----------------------------------------------
                 D L = 0                        "DL"
                 D R = 0                        "DR"
]
```

```
System["2. Equalities for Isolating Boundary Operators", any[f],
                 L A = 0                        "LA"
               R A = A + B                      "RA"
               L B = A + B                      "LB"
                 R B = 0                        "RB"
          ----------------------------------------------
              L ⌈f⌉ = f← L                      "LM"
              R ⌈f⌉ = f→ R                      "RM"
          ----------------------------------------------
                 L L = L                        "LL"
                 L R = R                        "LR"
                 R L = L                        "RL"
                 R R = R                        "RR"
]
```

```
System["Equalities for Algebraic Simplication", any[f, g],
             ⌈f⌉ ⌈g⌉ = ⌈f g⌉                    "MM"
]
```

System[*"3. Equalities for Contracting Integration Operators"*, any[f],

$A \lceil f \rceil A = \lceil \int^* f \rceil A - A \lceil \int^* f \rceil$	"AMA"
$A \lceil f \rceil B = \lceil \int^* f \rceil B + A \lceil \int^* f \rceil$	"AMB"
$B \lceil f \rceil A = \lceil \int_* f \rceil A + B \lceil \int_* f \rceil$	"BMA"
$B \lceil f \rceil B = \lceil \int_* f \rceil B - B \lceil \int_* f \rceil$	"BMB"
$A\,A = \lceil \int^* 1 \rceil A - A \lceil \int^* 1 \rceil$	"AA"
$A\,B = \lceil \int^* 1 \rceil B + A \lceil \int^* 1 \rceil$	"AB"
$B\,A = \lceil \int_* 1 \rceil A + B \lceil \int_* 1 \rceil$	"BA"
$B\,B = \lceil \int_* 1 \rceil B - B \lceil \int_* 1 \rceil$	"BB"

]

System[*"4. Equalities for Absorbing Integration Operators"*, any[f],

$A \lceil f \rceil D = -f^{\leftarrow} L + \lceil f \rceil - A \lceil f' \rceil$	"AMD"
$B \lceil f \rceil D = f^{\rightarrow} R - \lceil f \rceil - B \lceil f' \rceil$	"BMD"
$A\,D = -L + 1$	"AD"
$B\,D = R - 1$	"BD"
$A \lceil f \rceil L = \lceil \int^* f \rceil L$	"AML"
$B \lceil f \rceil L = \lceil \int_* f \rceil L$	"BML"
$A \lceil f \rceil R = \lceil \int^* f \rceil R$	"AMR"
$B \lceil f \rceil R = \lceil \int_* f \rceil R$	"BMR"
$A\,L = \lceil \int^* 1 \rceil L$	"AL"
$B\,L = \lceil \int_* 1 \rceil L$	"BL"
$A\,R = \lceil \int^* 1 \rceil R$	"AR"
$B\,R = \lceil \int_* 1 \rceil R$	"BR"

]

Current Math Systems

More Interaction Numerics / Symbolics

More Symbolics

More Intellectics

32 of 47

Automated (Dis-) Proving in Geometry

Reduction of the Problem to Gröbner bases computation:

Geo Theorem $\longrightarrow$ (by coordinatization)

$\underset{x,y,\ldots}{\forall}$ (poly1(x,y,...)=0 $\wedge$ ... $\Rightarrow$ poly(x,y,...)=0) $\longrightarrow$

$\neg \underset{x,y,\ldots}{\exists}$ (poly1(x,y,...)=0 $\wedge$ ... $\wedge$ poly(x,y,...)$\neq$0) $\longrightarrow$

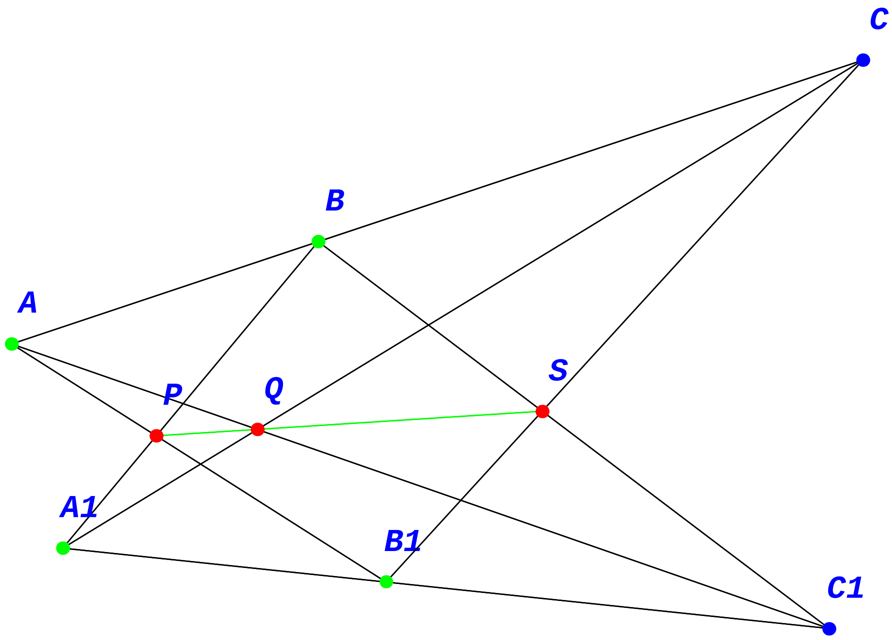
$\neg \underset{x,y,\ldots,a}{\exists}$ (poly1(x,y,...)=0 $\wedge$ ... $\wedge$ a . poly(x,y,...) - 1 = 0)

The latter question can be decided by the Gröbner basis method!

33 of 47

Example: Pappus Theorem

- What does the theorem say geometrically?



- Textbook formulation:

Let A,B, C and A1,B1, C1 be on two lines and P = AB1 ⋂ A1B, Q = AC1 ⋂ A1C, S = BC1 ⋂ B1C. Then P, Q, and S are collinear.

- Input to the system:

```
Proposition["Pappus", any[A, B, A1, B1, C, C1, P, Q, S],
 point[A, B, A1, B1] ∧ pon[C, line[A, B]] ∧ pon[C1, line[A1, B1]] ∧
   inter[P, line[A, B1], line[A1, B]] ∧ inter[Q, line[A, C1], line[A1, C]] ∧
   inter[S, line[B, C1], line[B1, C]] ⇒ collinear[P, Q, S]]
```

- Input to the system:

```
Prove[Proposition["Pappus"], by → GeometryProver,
 ProverOptions → {Method -> "GroebnerProver", Refutation → True}]
```

- Notebook generated automatically by the proving algorithm based on Groebner basis algorithm:

Prove:

(Proposition (Pappus))

$$\forall_{A,B,A1,B1,C,C1,P,Q,S} (\text{point}[A, B, A1, B1] \wedge \text{pon}[C, \text{line}[A, B]] \wedge \text{pon}[C1, \text{line}[A1, B1]] \wedge \text{inter}[P, \text{line}[A, B1], \text{line}[A1, B]] \wedge \text{inter}[Q, \text{line}[A, C1], \text{line}[A1, C]] \wedge \text{inter}[S, \text{line}[B, C1], \text{line}[B1, C]] \Rightarrow \text{collinear}[P, Q, S])$$

with no assumptions.

To prove the above statement we shall use the Gröbner basis method. First we have to transform the problem into algebraic form.

Algebraic Form:

To transform the geometric problem into algebraic form we have to chose first an orthogonal coordinate system.

Let's have the origin in point A, and points $\{B, C\}$ on the two axes.

Using this coordinate system we have the following points:

$$\{\{A, 0, 0\}, \{B, 0, u_1\}, \{A1, u_2, u_3\}, \{B1, u_4, u_5\}, \{C, 0, u_6\}, \{C1, u_7, x_1\}, \{P, x_2, x_3\}, \{Q, x_4, x_5\}, \{S, x_6, x_7\}\}$$

The algebraic form of the assertion is:

(1)

$$\forall_{x_1,x_2,x_3,x_4,x_5,x_6,x_7} (u_3 u_4 + -u_2 u_5 + -u_3 u_7 + u_5 u_7 + u_2 x_1 + -u_4 x_1 == 0 \wedge u_5 x_2 + -u_4 x_3 == 0 \wedge -u_1 u_2 + u_1 x_2 + -u_3 x_2 + u_2 x_3 == 0 \wedge x_1 x_4 + -u_7 x_5 == 0 \wedge -u_2 u_6 + -u_3 x_4 + u_6 x_4 + u_2 x_5 == 0 \wedge u_1 u_7 + -u_1 x_6 + x_1 x_6 + -u_7 x_7 == 0 \wedge -u_4 u_6 + -u_5 x_6 + u_6 x_6 + u_4 x_7 == 0 \Rightarrow x_3 x_4 + -x_2 x_5 + -x_3 x_6 + x_5 x_6 + x_2 x_7 + -x_4 x_7 == 0)$$

This problem is equivalent to:

(2)

$$\neg \left(\exists_{x_1,x_2,x_3,x_4,x_5,x_6,x_7} (u_3 u_4 + -u_2 u_5 + -u_3 u_7 + u_5 u_7 + u_2 x_1 + -u_4 x_1 == 0 \wedge u_5 x_2 + -u_4 x_3 == 0 \wedge -u_1 u_2 + u_1 x_2 + -u_3 x_2 + u_2 x_3 == 0 \wedge x_1 x_4 + -u_7 x_5 == 0 \wedge -u_2 u_6 + -u_3 x_4 + u_6 x_4 + u_2 x_5 == 0 \wedge u_1 u_7 + -u_1 x_6 + x_1 x_6 + -u_7 x_7 == 0 \wedge -u_4 u_6 + -u_5 x_6 + u_6 x_6 + u_4 x_7 == 0 \wedge x_3 x_4 + -x_2 x_5 + -x_3 x_6 + x_5 x_6 + x_2 x_7 + -x_4 x_7 \neq 0)\right)$$

To remove the last inequality, we use the Rabinowitsch trick: Let v_0 be a new variable. Then the problem becomes:

(3)

$$\neg \left(\exists_{x_1,x_2,x_3,x_4,x_5,x_6,x_7,v_0} (u_3 u_4 + -u_2 u_5 + -u_3 u_7 + u_5 u_7 + u_2 x_1 + -u_4 x_1 == 0 \wedge u_5 x_2 + -u_4 x_3 == 0 \wedge -u_1 u_2 + u_1 x_2 + -u_3 x_2 + u_2 x_3 == 0 \wedge x_1 x_4 + -u_7 x_5 == 0 \wedge -u_2 u_6 + -u_3 x_4 + u_6 x_4 + u_2 x_5 == 0 \wedge u_1 u_7 + -u_1 x_6 + x_1 x_6 + -u_7 x_7 == 0 \wedge -u_4 u_6 + -u_5 x_6 + u_6 x_6 + u_4 x_7 == 0 \wedge 1 + -v_0 (x_3 x_4 + -x_2 x_5 + -x_3 x_6 + x_5 x_6 + x_2 x_7 + -x_4 x_7) == 0)\right)$$

This statement is true iff the corresponding Gröbner basis is {1}.

The Gröbner bases is $\{1\}$.

Hence, the statement and the original assertion is true.

Statistics:

Time needed to compute the Gröbner bases: `0.42 Seconds`.

Automated Proofs of Theorems in Analysis (The "PCS" Prover: BB 2001)

Initialize Theorema

Example

```
Definition["limit:", any[f, a],
    limit[f, a] ⟺ ∀_{ϵ, ϵ>0} ∃_N ∀_{n, n≥N} |f[n] - a| < ϵ]
```

```
Proposition["limit of sum", any[f, a, g, b],
    (limit[f, a] ∧ limit[g, b])  ⇒  limit[f + g, a + b]]
```

```
Definition["+:", any[f, g, x],
    (f + g)[x] = f[x] + g[x]]
```

```
Lemma["|+|", any[x, y, a, b, δ, ϵ],
    (|(x + y) - (a + b)| < (δ + ϵ))  ⟸  (|x - a| < δ ∧ |y - b| < ϵ)]
```

```
Lemma["max", any[m, M1, M2],
    m ≥ max[M1, M2]  ⇒  (m ≥ M1 ∧ m ≥ M2)]
```

```
Theory["limit",
    Definition["limit:"]
    Definition["+:"]
    Lemma["|+|"]
    Lemma["max"]          ]
```

```
Prove[Proposition["limit of sum"], using → Theory["limit"], by → PCS]
```

- ProofObject -

Proof contains interesting algorithmic and didactic information!

Algorithm-Supported Mathematical Theory Exploration

A new world-wide movement (approx. 20 research groups, e.g. Mizar, Isabelle, Omega, NuPrL, Coq, etc.)

Our Theorema Group is a (founding) member of this network.

Goals:

- invent (axioms, definitions for) new concepts (operations: predicates, functions) (e.g. limit)
- invent and prove properties of notions
- invent problems about notions
- invent methods (algorithms) for problems and prove their correctness
- compute (apply algorithms to data)
- organize, store, and retrieve knowledge

Example: Automated Synthesis of the Gröbner Bases Algorithm (BB 2005)

Starting from a formal (predicate logic) specification of the problem,

by this new algorithm synthesis method,

the key idea of the main theorem (the notion of S-polynomial) is automatically generated and verified.

Conclusions

Intellectics:

= algorithm-supporte mathematical theory exploration

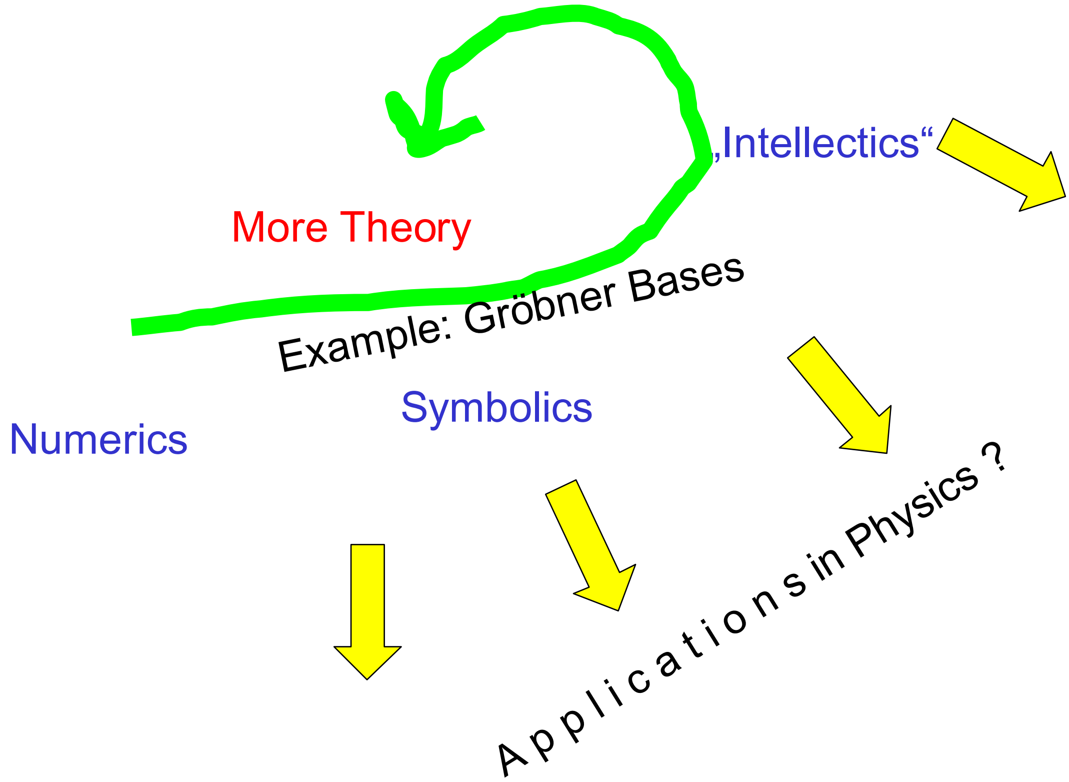
= mathematical knowledge management

= "(Anti)bourbakism of the 21st century"

Will drastically change the way

- how we do research in math,
- how we teach math,
- how we apply math,
- how we store and retrieve math knowledge.

For Physics ?



Special Semester on Gröbner Bases, Feb - July 2006

At RICAM and RISC, see

www.ricam.ac.at

goto "expression of interest" form: visiting researcher, postdoc, and doc fellowships available.

40 of 47

Appendix: More Details on Gröbner Bases and References

How Difficult is the Construction of Gröbner Bases?

Very Easy

The structure of the algorithm is easy. The operations needed in the algorithm are elementary. "Every high-school student can execute the algorithm." (See palm-top TI-98.)

Very Difficult

The inherent complexity of the problems that can be solved by the GB method (e.g. graph colorings) is "exponential". Hence, the worst-case complexity of the GB algorithm *must* be high.

Sometimes Easy

Mathematically interesting examples often have a lot of "structure" and, in concrete examples, GB computations can be reasonably, even surprisingly, fast.

Enormous Potential for Improvement

More *mathematical* theorems can lead to drastic speed-up:

- The use of "criteria" for eliminating the consideration of certain S-polynomials.
- *p*-adic approaches and floating point approaches.
- The "Gröbner Walk" approach.
- The "linear algebra" approach. (Generalized Sylvester matrices.)
- The "numerics" approach.

Tuning of the algorithm:

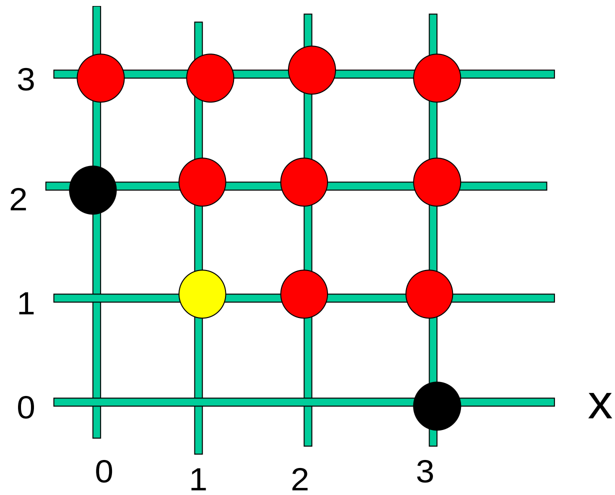
- Heuristics, strategies for choosing orderings, selecting S-polynomials etc.
- Good implementation techniques.

A huge literature.

Why "Gröbner" Bases?

Professor Wolfgang Gröbner (1899-1980) was my PhD thesis supervisor.

He gave me the problem of finding "the uncovered points if the black points are given".



In my thesis (1965) and journal publication (1970) I introduced:

* the concept of Gröbner bases and reduced Gröbner bases

* the S-polynomials

* the main theorem with proof

* the algorithm with termination and correctness proof

* the uniqueness of Gröbner bases

* first applications (computing in residue rings, Hilbert function, algebraic systems)

* the technique of base-change w.r.t. to different orderings

* a complete computer implementation

* first complexity considerations.

However, in the thesis, I did not use the name "Gröbner bases". I introduced this name only in 1976, for honoring Gröbner, when people started to become interested in my work.

My later contributions:

* the technique of criteria for eliminating unnecessary reductions

* an abstract characterization of "Gröbner bases rings".

Gröbner Bases on Your Desk and in Your Palm

GB implementations are contained in all the current math software systems like *Mathematica* (see demo), Maple, Magma, Macsyma, Axiom, Derive, Reduce, Mupad, ...

Software systems specialized on Gröbner bases: RISA-ASIR (M. Noro, K. Yokoyama), CoCoA, Macaulay, Singular, ...

Gröbner bases are now availabe on the TI-98 (implemented in Derive).

Textbooks on Gröbner Bases

T. Kreuzer, L. Robbiano: *Algorithmic Commutative Algebra I.* Springer, Heidelber, 2000: Contains a list of all other, approx. 10, textbooks on GB.

W.W.Adams, P. Loustenau. *Introduction to* Gröbner *Bases*. Graduate Studies in Mathematics: Amer. Math. Soc., Providence, R.I., 1994.

T.Becker, V.Weispfenning. Gröbner *Bases: A Computational Approach to Commutative Algebra.* Springer, New York, 1993.

D.Cox, J.Little, D.O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, New York, 1992.

....

M. Maruyama. Gröbner Bases and Applications. 2002.

M. Noro, K. Yokoyama. Computational Fundamentals of Gröbner Bases. University of Tokyo Press, 2003.

Gröbner Bases on the Web

Search. E.g. in the Research Index you obtain ~ 3000 citations.

45 of 47

Original Publications on Gröbner Bases

Approximately 600 papers appeared meanwhile on Gröbner bases.

J of Symbolic Computation, in particular, special issues.

ISSAC Conferences.

Mega Conferences.

ACA Conferences.

...

The essential additional original ideas in the literature:

- Gröbner bases can be constructed w.r.t. arbitrary "admissible" orderings (W. Trinks 1978)
- Gröbner bases w.r.t. to "lexical" orderings have the elimination property (W. Trinks 1978)
- Gröbner bases can be used for computing syzygies and the S-polys generate the module of syzygies (G. Zacharias 1978)
- A given F, w.r.t. the *infinitely* many admissible orderings, has only *finitely* many Gröbner bases and, hence, we can construct a "universal" Gröbner bases for F (L. Robbiano, V. Weispfenning, T. Schwarz 1988)
- Starting from a Gröbner bases for F for ordering O_1 one can "walk", by changing the basis only slightly, to a basis for a "nearby" ordering O_2 and so on ... until one arrives at a Gröbner bases for a desired ordering O_k (Kalkbrener, Mall 1995, Nam 2000).
- Use arbitrary linear algebra algorithms for the reduction (remaindering) process: (Faugère 1997).
- ... numerours applications,

46 of 47

Research Topics

- the inner structure of Groebner bases: generalized Sylvester matrices
- the numerics of GB computations
- axiomatic characterization of Groebner rings
- generalizations (e.g. non-commutative poly-rings)
- speeding up the computation
- Groebner bases for particular classes of ideals (avoid computation)
- the study of admissible orderings
- applications (problem reductions, e.g. functional analysis, BV problems, **Rosenkranz 2003**)

47 of 47

References

On Gröbner Bases

[Buchberger 1970]

B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems (An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations). Aequationes mathematicae 4/3, 1970, pp. 374-383. (English translation in: [Buchberger, Winkler 1998], pp. 535 -545.) Published version of the PhD Thesis of B. Buchberger, University of Innsbruck, Austria, 1965.

[Buchberger 1998]

B. Buchberger. Introduction to Gröbner Bases. In: [Buchberger, Winkler 1998], pp.3-31.

[Buchberger, Winkler, 1998]

B. Buchberger, F. Winkler (eds.). Gröbner Bases and Applications, Proceedings of the International Conference "33 Years of Gröbner Bases", 1998, RISC, Austria, London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 1998.

[Becker, Weispfenning 1993]

T. Becker, V. Weispfenning. Gröbner Bases: A Computational Approach to Commutative Algebra, Springer, New York, 1993.

■ On Mathematical Knowledge Management

B. Buchberger, G. Gonnet, M. Hazewinkel (eds.)

Mathematical Knowledge Management.

Special Issue of Annals of Mathematics and Artificial Intelligence, Vol. 38, No. 1-3, May 2003, Kluwer Academic Publisher, 232 pages.

A.Asperti, B. Buchberger, J.H.Davenport (eds.)

Mathematical Knowledge Management.

Proceedings of the Second International Conference on Mathematical Knowledge Management (MKM 2003), Bertinoro, Italy, Feb.16-18, 2003, Lecture Notes in Computer Science, Vol. 2594, Springer, Berlin-Heidelberg-NewYork, 2003, 223 pages.

A.Asperti, G.Bancerek, A.Trybulec (eds.).

Proceedings of the Third International Conference on Mathematical Knowledge Management, MKM 2004,

Bialowieza, Poland, September 19-21, 2004, Lecture Notes in Computer Science, Vol. 3119, Springer, Berlin-Heidelberg-NewYork, 2004

■ On Theorema

[Buchberger et al. 2000]

B. Buchberger, C. Dupre, T. Jebelean, F. Kriftner, K. Nakagawa, D. Vasaru, W. Windsteiger. The Theorema Project: A Progress Report. In: M. Kerber and M. Kohlhase (eds.), Symbolic Computation and Automated Reasoning (Proceedings of CALCULEMUS 2000, Symposium on the Integration of Symbolic Computation and Mechanized Reasoning, August 6-7, 2000, St. Andrews, Scotland), A.K. Peters, Natick, Massachusetts, ISBN 1-56881-145-4, pp. 98-113.

■ On Theory Exploration and Algorithm Synthesis

[Buchberger 2000]

B. Buchberger. Theory Exploration with *Theorema*.

Analele Universitatii Din Timisoara, Ser. Matematica-Informatica, Vol. XXXVIII, Fasc.2, 2000, (Proceedings of SYNASC 2000, 2nd International Workshop on Symbolic and Numeric Algorithms in Scientific Computing, Oct. 4-6, 2000, Timisoara, Rumania, T. Jebelean, V. Negru, A. Popovici eds.), ISSN 1124-970X, pp. 9-32.

[Buchberger 2003]

B. Buchberger. Algorithm Invention and Verification by Lazy Thinking.

In: D. Petcu, V. Negru, D. Zaharie, T. Jebelean (eds), Proceedings of SYNASC 2003 (Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, October 1–4, 2003), Mirton Publishing, ISBN 973–661–104–3, pp. 2–26.

[Buchberger, Craciun 2003]

B. Buchberger, A. Craciun. Algorithm Synthesis by Lazy Thinking: Examples and Implementation in Theorema. in: Fairouz Kamareddine (ed.), Proc. of the Mathematical Knowledge Management Workshop, Edinburgh, Nov. 25, 2003, Electronic Notes on Theoretical Computer Science, volume dedicated to the MKM 03 Symposium, Elsevier, ISBN 044451290X, to appear.

[Buchberger 2004]

B. Buchberger.

Towards the Automated Synthesis of a Gröbner Bases Algorithm.

RACSAM (Review of the Royal Spanish Academy of Science), Vol. 98/1, to appear, 10 pages.