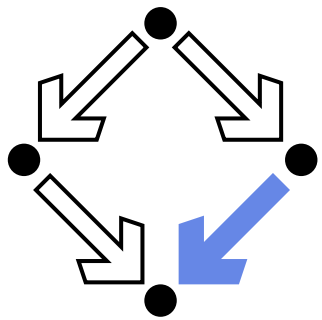
The Role of Symbolic Computation in Mathematics

Franz Winkler

Research Institute for Symbolic Computation
Johannes Kepler University Linz, Linz, Austria



invited lecture at EACA 2012, Alcalá, June 13–15, 2012
DK lecture, October 19, 2012

Abstract

Symbolic Computation (Mathematics Subject Classification 2000, 68W30) is often treated as just another subject in the wide field of special topics within mathematics; on the same level as mesh generation (65L50) or quasi-Frobenius rings (16L60). Here we want to argue that actually Symbolic Computation is not so much a topic in mathematics, but a relatively novel approach to mathematical epistemology; a different and, as we believe, fruitful way of looking at mathematics and the acquisition of knowledge in mathematics.

Outline

1. What is Symbolic Computation ?
2. Examples of Symbolic Computation
3. SC as a holistic approach to math
4. SC as a new epistemological approach to math
5. SC is changing math & science

Conclusion

1. What is Symbolic Computation ?

Wikipedia:

Symbolic computation

Symbolic computation or **algebraic computation**, relates to the use of machines, such as computers, to manipulate mathematical equations and expressions in symbolic form, as opposed to manipulating the approximations of specific numerical quantities represented by those symbols. Such a system might be used for symbolic integration or differentiation, substitution of one expression into another, simplification of an expression, etc.

Symbolic computation is also sometimes referred to as **symbolic manipulation**, **symbolic processing**, **symbolic mathematics**, or **symbolic algebra**, but these terms also refer to non-computational manipulation.

Software applications that perform symbolic calculations are called computer algebra systems.

See also

- Automated theorem prover
- Computer-assisted proof
- Proof checker
- Model checker
- Symbolic-numeric computation
- Symbolic simulation
- Symbolic execution

References

- Symbolic Computation (An Editorial), Bruno Buchberger, Journal of Symbolic Computation (1985) 1, pp. 1–6.
- Making Computer Algebra More Symbolic (Invited), Stephen M. Watt, pp. 43–49, Proc. Transgressive Computing 2006: A conference in honor of Jean Della Dora, (TC 2006), April 24-26 2006, Granada Spain.

In our view, Symbolic Computation is the field in which we

develop, analyze, and apply

mathematical algorithms, with the following characteristics:
math. expressions are first class objects both in input and in output, solutions are given exactly, objects are taken from any area of mathematics.

Typical (but in no way exclusive) content areas are:

computer algebra
computational logic
symbolic geometric methods

2. Examples of Symbolic Computation

2.1. Solution of algebraic equations

Before the advent of SC we had methods for determining solutions to algebraic equations. But they were either inefficient or incomplete.

Since the advent of SC we have witnessed great progress in

- greatest common divisors of polynomials
- resultant methods
- Gröbner bases for systems of multivariate polynomials

Resultant methods

resultants have a long history in elimination theory, the theory of polynomial ideals and their solutions

$$\begin{aligned} f_1(x,y,z) &= 2xy + yz - 3z^2 \\ f_2(x,y,z) &= x^2 - xy + y^2 - 1 \\ f_3(x,y,z) &= yz + x^2 - 2z^2 \end{aligned}$$

solutions, e.g. $(1,1,1)$, are solutions of resultants,
but not vice versa: no common solution $(\ldots,\ldots,1/\sqrt{3})$

$$\begin{aligned} \mathrm{res}_y(\mathrm{res}_x(f_1,f_3),\mathrm{res}_x(f_2,f_3)) = (3z^2-1)\cdot z^4\cdot(z-1)\cdot \\ (z+1)\cdot(127z^4-91z^2+16)\cdot(457z^4-175z^2+16) \end{aligned}$$

resultants are in elimination ideals, but do not generate them

Gröbner bases

Buchberger (1965) introduced GB into SC and mathematics

Gröbner basis for f_1, f_2, f_3 w.r.t. lex$(x > y > z)$:

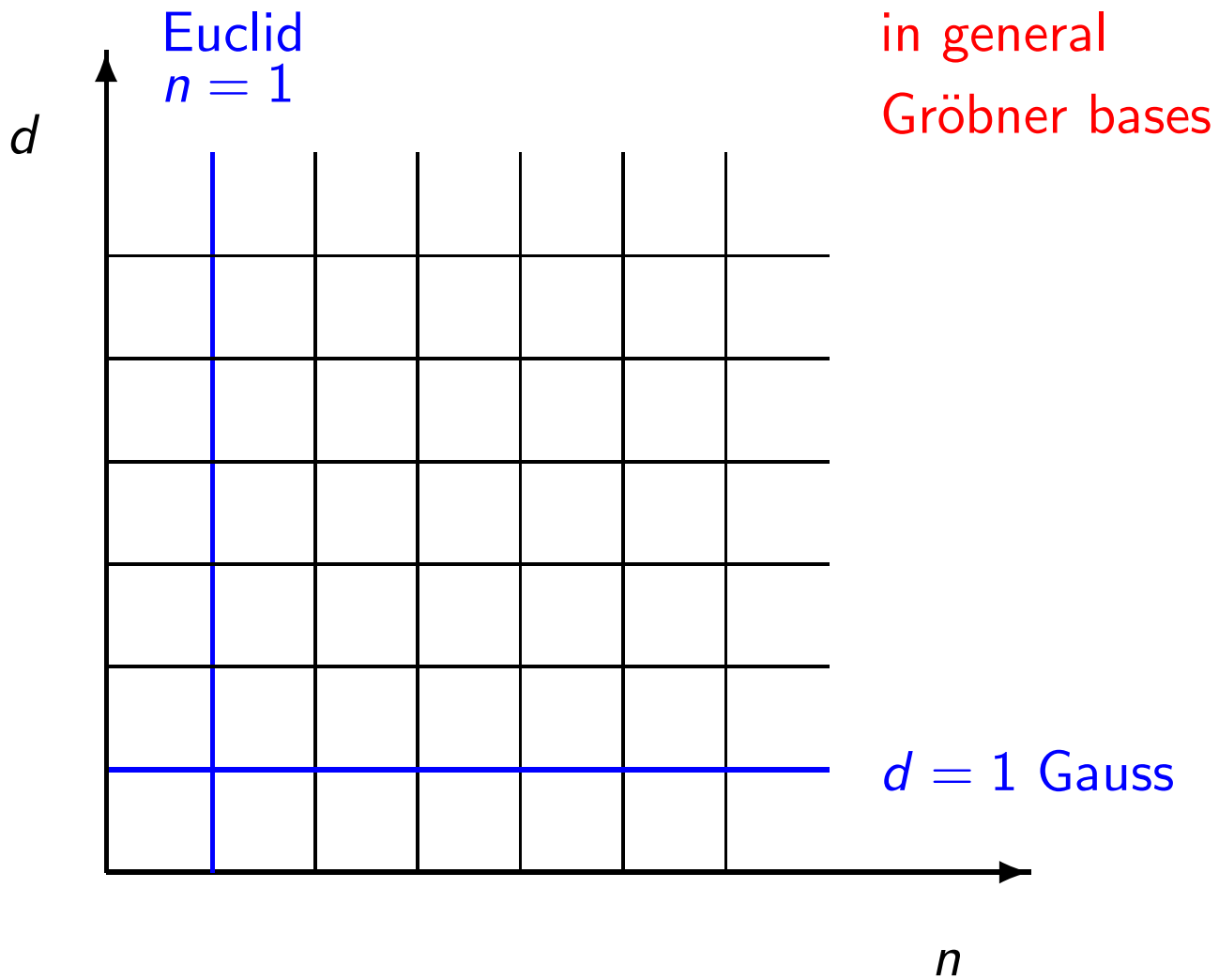
$$\begin{aligned} g_1 &= 78x - 2921z^5 + 3744z^3 - 901z \\ g_2 &= 104y^2 - 2667z^6 + 3562z^4 - 895z^2 - 104 \\ g_3 &= 52yz - 2667z^6 + 3562z^4 - 947z^2 \\ g_4 &= z(z+1)(z-1)(127z^4 - 91z^2 + 16) \end{aligned}$$

properties of the Gröbner basis:

- **generates** the elimination ideals
- partial solutions are extendable: $-1 \longrightarrow (-1, -1, -1)$
- $8 = \#$ solutions $= \#$ irreducible terms $=$ dimension of the coordinate ring

solving systems of polynomial/algebraic equations

n = number of variables, d = maximal degree



2.2. Equational theorem proving and rewriting

- consider first-order axioms which contain only "=" as predicate symbol, and are universally quantified
- the corresponding **equational theory** consists of all universally quantified statements derivable from these axioms

Examples:

- groups, rings, modules, ...
- abstract data types

Problem: can we automatically decide provability/validity of statements in equational theories?

Example Group Theory:

$$\begin{array}{ll} (\text{G1}) & 1 \cdot x = x \\ (\text{G2}) & x^{-1} \cdot x = 1 \\ (\text{G3}) & (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array}$$

Question:
is $((x \cdot y)^{-1} \cdot x) \cdot x = (x^{-1} \cdot y)^{-1}$ a theorem in group theory?

Example Data Type Queue:

$$
\begin{array}{ll}
\text{(Q1)} & \mathtt{app}(x, \mathtt{newq}) = x \\
\text{(Q2)} & \mathtt{app}(x, \mathtt{add}(y, z)) = \mathtt{add}(\mathtt{app}(x, y), z) \\
\text{(Q3)} & \mathtt{app}(\mathtt{app}(x, y), z) = \mathtt{app}(x, \mathtt{app}(y, z))
\end{array}
$$

Question: is

$$
\begin{aligned}
\mathtt{app}(x, \mathtt{app}(\mathtt{add}(y, z), w)) \; = \\
\mathtt{app}(\mathtt{add}(\mathtt{app}(\mathtt{app}(x, \mathtt{newq}), y), z), w)
\end{aligned}
$$

a theorem in the equational theory of queues?

2.3. Other developments

- factorization theory
- integration theory
- matrix normal forms and linear algebra
- recurrence relations
- unification theory
- automated theorem proving in predicate logic
- .....

3. SC as a holistic approach to math

The biological theory of evolution knows many instances of similar solutions having been developed for similar problems; examples are the wings of insects, birds, and bats, or the different realizations of light sensitive organs such as eyes.

The same phenomenon can be observed in the development of the sciences, and also in mathematics.
Often symbolic methods allow us to realize that the same algorihmic idea applies to problems from different parts of mathematics, or
we need to combine several seemingly distant mathematical areas in order to create symbolic algorithms.

3.1. Completion algorithms

Many algorithmic methods in different fields of mathematics, e.g. linear algebra, commutative algebra, or logic, can be seen as constructing canonical systems for deciding membership problems. Important examples are

- Gauss' elimination method for linear systems,
- Euclid's algorithm for computing GCDs,
- Buchberger's algorithm for constructing Gröbner bases,
- the Knuth-Bendix procedure for equational theories.

Here we explain the basic concept of a canonical system and investigate the close connections between these algorithms.

Canonical reduction systems are supposed to solve the following kind of problem:

- we are given a mathematical structure $\mathcal{S}$
  and a congruence relation $\cong$ on $\mathcal{S}$, (i.e. $\cong \subseteq \mathcal{S}^2$)
  given by a finite set of generators G (i.e. $\cong = \cong_G$)
- for any given $s, t \in \mathcal{S}$, we want to decide whether $s \cong_G t$
- this should be achieved by a general algorithm depending only on $\mathcal{S}$, and **not** on the particular congruence $\cong_G$ or its set of generators G

We introduce a reduction relation

$$\longrightarrow_G \quad \subseteq \quad \mathcal{S} \times \mathcal{S}$$

with the properties

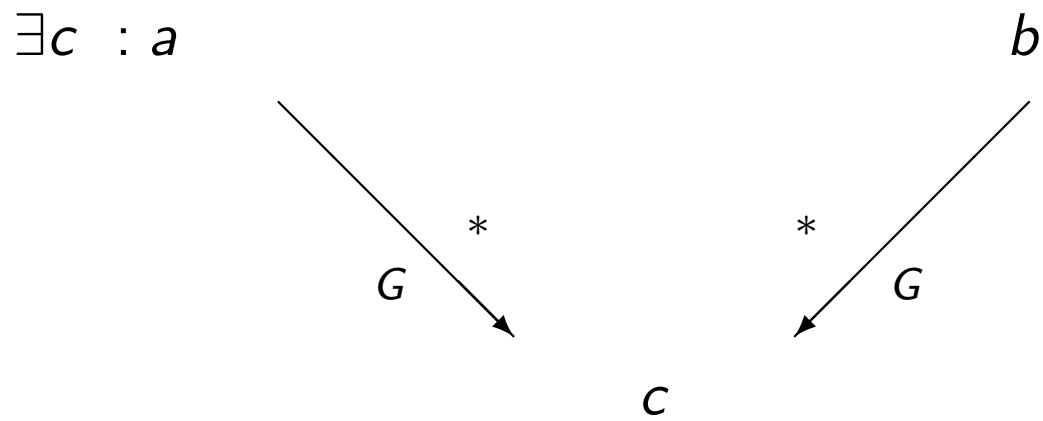
- $\cong_G = \longleftrightarrow_G^*$, i.e. the symmetric reflexive transitive closure of $\longrightarrow_G$ is equal to the congruence generated by G
- $\longrightarrow_G$ is terminating or Noetherian, i.e. every reduction chain is finite

if in addition to being Noetherian the reduction relation is also Church-Rosser, then we can solve our problem

the reduction relation $\longrightarrow_G$ is Church-Rosser iff connectednes w.r.t. "$\longleftrightarrow_G$", i.e.

$$a \longleftrightarrow_G^* b \ ,$$

implies the existence of a common successor, i.e.



in particular this means that two irreducible elements a, b are congruent if and only if they are syntactically equal.

If $\longrightarrow_G$ is Noetherian and Church-Rosser, we can now decide whether $a \cong_G b$:

- reduce a and b to (any) irreducible a' and b' s.t.

$$a \longrightarrow_G^* a' \qquad b' \longleftarrow_G^* b$$

  (because of Noetherianity reduction chains are finite)

- check whether $a' = b'$;
  if so $a \cong_G b$, otherwise not

But of course in general our set of generators G will not have this nice Church-Rosser property.
The goal now is to transform G into an equivalent set of generators $\hat{G}$, having the Church-Rosser property.

Gauss Elimination

the setting:

- vector space $V = K^n$ over field K
- generating elements B for a subvectorspace $W = \mathrm{span}(B)$
- equivalence relation $v \cong_W w \iff v - w \in W$

the problem:

- for $v \in V$
- decide: "$v \cong_W 0$", i.e. "$v \in \mathrm{span}(B) = W$" ?

define a reduction relation $\longrightarrow_B$:
for vector $b = (0, \ldots, 0, b_i, \ldots, b_n)$ with $b_i \neq 0$:

$$c = (c_1, \ldots, c_i \neq 0, \ldots, c_n) \longrightarrow_b c - \frac{c_i}{b_i} \cdot b$$

and

$$c \longrightarrow_B d \iff \exists b \in B : c \longrightarrow_b d$$

clearly $\longrightarrow_B$ has the following properties:

- $\longrightarrow_B$ is terminating
- if $c \longrightarrow_B d$ then $c - d \in \mathrm{span}(B) = W$

but in general $\longrightarrow_B$ is **not** Church-Rosser

completion process: Gauss elimination can be seen as completing the reduction relation $\longrightarrow_B$;
if a unit vector can be reduced by 2 different generators b_i and b_j, we add the difference of the 2 reduction results to the basis B

this process terminates and yields a set of generators $\hat{B}$ s.t.

- $\longleftrightarrow_B^* \quad = \quad \cong_W \quad = \quad \longleftrightarrow_{\hat{B}}^*$
- $\longrightarrow_{\hat{B}}$ is both Noetherian and CR

So we can decide the membership problem for W by reduction w.r.t. $\hat{B}$

if in the end we interreduce the elements in $\hat{B}$, we basically get the Hermite matrix associated to B

Example:

$$\begin{array}{lll} B \to & b_1 = & (1,0,0) \\ & b_2 = & (1,1,1) \\ & - - - & - - - - - \\ & b_3 = & (0,1,1) \qquad \to \hat{B} \end{array}$$

now $\hat{B}$ spans the same vector space W, and we can use the reduction w.r.t.$\hat{B}$ to decide membership in W:

$$\begin{array}{lllll} B: & (1,2,2) & \longrightarrow_{b_1} & (0,2,2) & \text{irreducible} \\ & & \longrightarrow_{b_2} & (0,1,1) & \text{irreducible} \end{array}$$

$$\begin{array}{lllllll} \hat{B}: & (1,2,2) & \longrightarrow_{b_1} & (0,2,2) & \longrightarrow_{b_3} & (0,0,0) \\ & & \longrightarrow_{b_2} & (0,1,1) & \longrightarrow_{b_3} & (0,0,0) \end{array}$$

So $(1,2,2) \in W$.

Euclid's algorithm for GCDs

the setting:

- $K[x]$, the ring of polynomials over a field K
- $F = \{f_1(x), f_2(x)\} \subset K[x]$
  generating an ideal $I = \langle F \rangle$ in $K[x]$
- equivalence relation $g \equiv_I h \iff g - h \in I$

the problem:

- for $g \in K[x]$
- decide: "$g \equiv_i 0$", i.e. "$g \in \langle F \rangle = I$" ?

define a reduction relation $\longrightarrow_F$:
for polynomial $f(x) = f_n x^n + \cdots f_1 x + f_0$ with $f_n \neq 0$:

$$c(x) = c_m x^m + \cdots + \underbrace{c_i}_{\neq 0} x^i + \cdots + c_0$$

$$\longrightarrow_f$$

$$c(x) \; - \; \tfrac{c_i}{f_n} x^{i-n} f(x), \qquad \text{if } i \geq n$$

and

$$c \longrightarrow_F d \quad \Longleftrightarrow \quad \exists f \in F : c \longrightarrow_f d$$

clearly $\longrightarrow_F$ has the following properties:

- $\longrightarrow_F$ is terminating
- if $c \longrightarrow_F d$ then $c - d \in \langle F \rangle = I$

but in general $\longrightarrow_F$ is **not** Church-Rosser

completion process: computation of remainder sequence can be seen as completing the reduction relation $\longrightarrow_F$;
if a term can be reduced by 2 different generators f_i and f_j, we add the difference of the 2 reduction results to the basis F

this process terminates and yields a set of generators $\hat{F}$ s.t.

- $\longleftrightarrow_F^* \quad = \quad \equiv_I \quad = \quad \longleftrightarrow_{\hat{F}}^*$
- $\longrightarrow_{\hat{F}}$ is both Noetherian and CR

So we can decide the membership problem for I by reduction w.r.t. $\hat{F}$

if in the end we interreduce the elements in $\hat{F}$, we simply get only the gcd in the generating set $\hat{F}$

Example:

$$
\begin{array}{lll}
F \to & f_1 = & x^5 + x^4 + x^3 - x^2 - x - 1 \\
& f_2 = & x^4 + x^2 + 1 \\
& - - - & - - - - - \\
& f_3 = & x^4 - x^2 - 2x - 1 = \qquad f_1 - x \cdot f_2 \\
& f_4 = & x^2 + x + 1 = \qquad \frac{1}{2}(f_2 - f_3) \\
& f_5 = & 0 = \qquad f_3 - (x^2 - x - 1) f_4 \\
& & \to \hat{F}
\end{array}
$$

now $\hat{F}$ generates the same ideal I, and we can use the reduction w.r.t.$\hat{F}$ to decide membership in I:

$$
\begin{array}{llllll}
x^5 - x^2 & \longrightarrow_{f_1} & -x^4 - x^3 + x + 1 & \longrightarrow_{f_2} & -x^3 + x^2 + x + 2 \\
 & \longrightarrow_{f_4} & 2x^2 + 2x + 2 & \longrightarrow_{f_4} & 0 \\
x^5 - x^2 & \longrightarrow_{f_2} & -x^3 - x^2 - x & \longrightarrow_{f_4} & 0
\end{array}
$$

So $x^5 - x^2 \in I$.

Gröbner Bases algorithm for polynomial ideals

the setting:

- $K[x_1, \ldots, x_n]$, the ring of multivariate polynomials over a field K
- $F = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ generating an ideal $I = \langle F \rangle$ in $K[x_1, \ldots, x_n]$
- equivalence relation $g \equiv_I h \iff g - h \in I$

the problem:

- for $g \in K[x_1, \ldots, x_n]$
- decide: "$g \equiv_I 0$", i.e. "$g \in \langle F \rangle = I$" ?

define a reduction relation $\longrightarrow_F$:
consider an **admissible ordering** $<$ on the terms;
$\mathrm{le}(f) :=$ exponent (vector) of the leading term of f;
for $g = \cdots + g_e x^{e=(e_1,\ldots,e_n)} + \cdots$ with $g_e \neq 0$ and
$e - \mathrm{le}(f) \in \mathbb{N}^n$ let

$$g \quad \longrightarrow_f \quad g \; - \; \frac{g_e}{\mathrm{lc}(f)} x^{e-\mathrm{le}(f)} f(x)$$

and

$$g \longrightarrow_F h \quad \Longleftrightarrow \quad \exists f \in F : g \longrightarrow_f h$$

clearly $\longrightarrow_F$ has the following properties:

- $\longrightarrow_F$ is terminating
- if $g \longrightarrow_F h$ then $g - h \in \langle F \rangle = I$

but in general $\longrightarrow_F$ is **not** Church-Rosser

completion process: we complete the reduction relation $\longrightarrow_F$; we investigate the "smallest" situations in which a term can be reduced in essentially 2 different ways, and we add the difference of the 2 reduction results to the basis F

this process terminates and yields a set of generators $\hat{F}$ s.t.

- $\longleftrightarrow_F^* \quad = \quad \equiv_I \quad = \quad \longleftrightarrow_{\hat{F}}^*$
- $\longrightarrow_{\hat{F}}$ is both Noetherian and CR

So we can decide the membership problem for I by reduction w.r.t. $\hat{F}$

If in the end we interreduce the elements in $\hat{F}$, we get a minimal Gröbner basis for the ideal I.

Example:

$$
\begin{array}{lllll}
F \rightarrow & f_1 = & x^2y^2 + y - 1 & & \\
& f_2 = & x^2y + x & & \\
& --- & ----- & & \\
& f_3 = & -xy + y - 1 = & f_1 - y \cdot f_2 & \\
& f_4 = & y - 1 = & f_2 + (x+1)f_3 & \\
& f_5 = & -x = & f_3 + (x-1)f_4 & \\
& & & \rightarrow \hat{F} &
\end{array}
$$

now $\hat{F}$ generates the same ideal I, and we can use the reduction w.r.t.$\hat{F}$ to decide membership in I:

$$
\begin{array}{llllll}
x^2y^2 & \longrightarrow_{f_1} & -y + 1 & \longrightarrow_{f_4} & 0 \\
x^2y^2 & \longrightarrow_{f_2} & -xy & \longrightarrow_{f_5} & 0
\end{array}
$$

So $x^2y^2 \in I$.

Knuth-Bendix algorithm for equational theories

the setting:

- a term algebra $\mathcal{T}(\Sigma, V)$ over a signature Σ and variables V
- $E = \{s_i = t_i \mid i \in I\}$ a set of equations over $\mathcal{T}$ generating an equational theory $=_E$
- equivalence relation $s \equiv_E t \iff s = t \in =_E$

the problem:

- for $s, t \in \mathcal{T}(\Sigma, V)$
- decide: "$s =_E t$" ?

turn equations E into rewrite rules R and
define a reduction relation $\longrightarrow_R$:
if there is a substitution σ such that $\sigma(s_i) = u$, then any term containing u as a subterm can be reduced to the corresponding term, where u is replaced by $\sigma(t_i)$:

$$u \longrightarrow_R v \quad \Longleftrightarrow \quad \exists p, i, \sigma : \; u_{|p} = \sigma(s_i), \text{ and } v = u[p \leftarrow \sigma(t_i)] \; .$$

then $\longrightarrow_R$ has the following properties:

- $\longrightarrow_R$ is terminating (if, e.g., the rules are ordered w.r.t. a reduction ordering $<$)
- $\longleftrightarrow_R^* = =_E$

but in general $\longrightarrow_R$ is **not** Church-Rosser

completion process:

we investigate "smallest" situations in which a term can be reduced in essentially 2 different ways, and if the results can be compared w.r.t. $<$, we add a new rule to R

if this process terminates and yields a set of rules $\hat{R}$ then

- $\longleftrightarrow_R^* \quad = \quad =_E \quad = \quad \longleftrightarrow_{\hat{R}}^*$
- $\longrightarrow_{\hat{R}}$ is both Noetherian and CR

So we can decide equality modulo E by reduction w.r.t. $\hat{R}$

in the end we can interreduce the elements in $\hat{R}$ and so get a minimal set of rewrite rules for $=_E$

Example:
for the case of group theory the Knuth-Bendix procedure terminates and yields the following minimal rewrite rule system:

$$
\begin{array}{rcl}
1 \cdot x = x & (1) & 1 \cdot x \longrightarrow x, \\
x^{-1} \cdot x = 1 & (2) & x^{-1} \cdot x \longrightarrow 1, \\
(x \cdot y) \cdot z = x \cdot (y \cdot z) & (3) & (x \cdot y) \cdot z \longrightarrow x \cdot (y \cdot z), \\
 & (4) & x^{-1} \cdot (x \cdot y) \longrightarrow y, \\
 & (5) & x \cdot 1 \longrightarrow x, \\
 & (6) & 1^{-1} \longrightarrow 1, \\
 & (7) & (x^{-1})^{-1} \longrightarrow x, \\
 & (8) & x \cdot x^{-1} \longrightarrow 1, \\
 & (9) & x \cdot (x^{-1} \cdot y) \longrightarrow y, \\
 & (10) & (x \cdot y)^{-1} \longrightarrow y^{-1} \cdot x^{-1}.
\end{array}
$$

So the question in 2.2, whether

$$((x \cdot y)^{-1} \cdot x) = (x^{-1} \cdot y)^{-1} \ ,$$

can be answered positively.

Example:

Similarly we get the canonical rewrite rule system for the data type Queue:

$$
\begin{array}{ll}
\text{(Q1)} & \mathtt{app}(x, \mathtt{newq}) \longrightarrow x \\
\text{(Q2)} & \mathtt{app}(x, \mathtt{add}(y, z)) \longrightarrow \mathtt{add}(\mathtt{app}(x, y), z) \\
\text{(Q3)} & \mathtt{app}(\mathtt{app}(x, y), z) \longrightarrow \mathtt{app}(x, \mathtt{app}(y, z)) \\
\text{(Q4)} & \mathtt{app}(x, \mathtt{app}(\mathtt{newq}, y)) \longrightarrow \mathtt{app}(x, y) \\
\text{(Q5)} & \mathtt{app}(x, \mathtt{app}(\mathtt{add}(y, z), w)) \longrightarrow \\
 & \qquad \mathtt{app}(\mathtt{add}(\mathtt{app}(x, y), z), w)
\end{array}
$$

So the question in 2.2, whether

$$
\begin{aligned}
\mathtt{app}(x, \mathtt{app}(\mathtt{add}(y, z), w)) \; = \\
\mathtt{app}(\mathtt{add}(\mathtt{app}(\mathtt{app}(x, \mathtt{newq}), y), z), w) \; ,
\end{aligned}
$$

can be answered positively.

3.2. Rational solutions of algebraic ODEs

an algebraic ODE is defined polynomially, e.g.

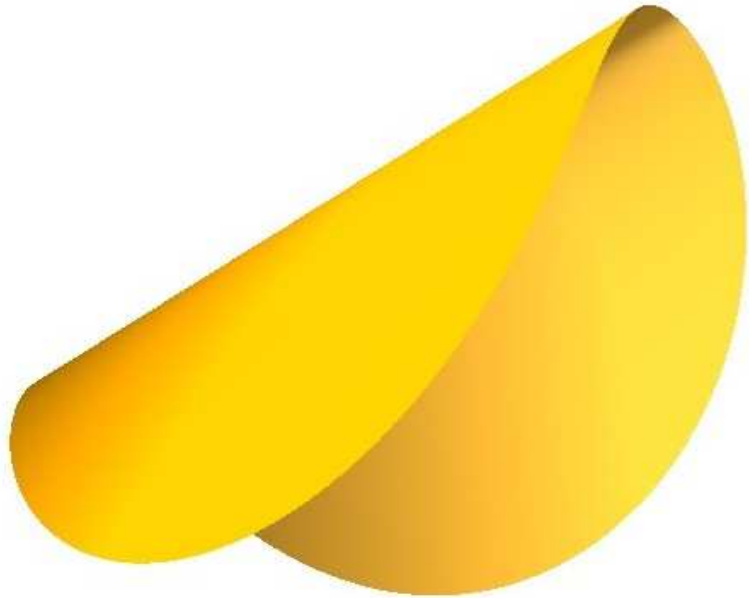
$$F(x, y, y') = y'(x)^2 + 3y'(x) - 2y(x) - 3x = 0$$

Combining theories of

- differential equations
- differential algebra
- algebraic geometry

we can determine (all) rational solutions to algebraic ODEs

Ref.: L.X.C. Ngô and FW, JSC 45 (2010) and 46 (2011)
L.X.C. Ngô, J.R. Sendra, FW, Cont.Math. 572 (2012)



For computing the rational general solution we parametrize the solution surface

$$\mathcal{S} : z^2 + 3z - 2y - 3x = 0 \ ,$$

$$\left(\underbrace{\frac{t}{s} + \frac{2s + t^2}{s^2}}_{\chi_1}, \underbrace{\frac{1}{s} - \frac{2s + t^2}{s^2}}_{\chi_2}, \underbrace{\frac{t}{s}}_{\chi_3} \right)$$

From this parametrization of the solution surface we derive the associated system

$$s' = st,$$
$$t' = s + t^2$$

having the irreducible invariant algebraic curves

$$G_1(s,t) = s,\ \ G_2(s,t) = t^2 + 2s,\ \ G_3(s,t) = s^2 + ct^2 + 2cs$$

G_3 can be parametrized as

$$(s(x), t(x) = (-\frac{2c}{1+cx^2},\ -\frac{2cx}{1+cx^2})$$

now we normalize

$$c = \chi_1(s(x), t(x)) - x$$

$$y = \chi_2(s(x - c), t(x - c))$$

getting the general rational solution

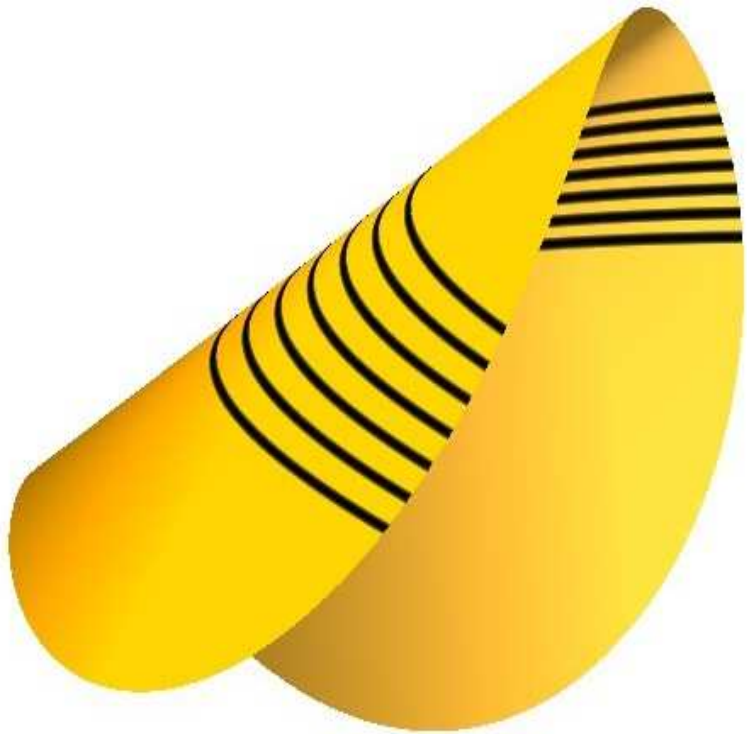
$$y(x) = \frac{1}{2c^2}(c^2x^2 + 2cx + 3c + 1)$$

and after a change of parameter

$$y(x) = \frac{1}{2}(x^2 + 2cx + c^2 + 3c)$$

solution curves $(x, \frac{1}{2}(x+c)^2 + \frac{3}{2}c, x+c)$, $c = -3, \ldots, 3$

on the solution surface $\mathcal{S} : y'^2 + 3y' - 2y - 3x = 0$



If the separant $2y' + 3$ (derivative w.r.t. y') vanishes we get the singular solution $y(x) = -\frac{3}{2}x - \frac{9}{8}$

4. SC as a new epistemological

What does it mean to "know" a mathematical object?

- if we have an existential proof guaranteeing its existence?
- if we have a constructive proof?
- if we have an efficient symbolic algorithm for determining it?

Example syzygy problem:

given: $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, where K is a field

determine: all solutions $z_1, \ldots, z_s \in K[x_1, \ldots, x_n]$ of

$$f_1 z_1 + \cdots + f_s z_s = 0$$

Solutions are called **syzygies** of $f_1, \ldots, f_s$.
They generalize the concept of "linear dependence" from linear algebra.

The syzygies $(z_1, \ldots, z_s)$ form a submodule $\mathrm{Syz}(f_i)$ of $K[x_1, \ldots, x_n]^s$ over $K[x_1, \ldots, x_n]$

can be generalized to a system of equations

existential theorem:

Theorem: (D. Hilbert [1]) *The module* $\mathrm{Syz}(f_i)$ *has a finite basis; so there are syzygies*

$$\begin{aligned} z^{(1)} &= (z_1^{(1)}, \ldots, z_s^{(1)}) \,, \\ &\vdots \\ z^{(k)} &= (z_1^{(k)}, \ldots, z_s^{(k)}) \,, \end{aligned}$$

s.t. every syzygy z *can be written as*

$$z = a_1 z^{(1)} + \cdots + a_k z^{(k)}$$

for some polynomials $a_1, \ldots, a_k$.
(also for system of equations)

[1] cf. D.Hilbert, *Über die Theorie der algebraischen Formen*, Math. Annalen 36, 473–534 (1890); Kap. I, p.208

constructive proof:

from the school of Emmy Noether:

Theorem: (Grete Hermann [2])
Let q be the maximal degree of any f_i.
Then the module $\mathrm{Syz}(f_i)$ has a finite basis, the elements of which all satisfy the double exponential degree bound

$$\sum_{r=1}^{n-1} q^{2^r} \ .$$

(also for system of equations)

[2] cf. G.Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Annalen 95, 736–788 (1926); Satz 2

symbolic algorithm: [3]

- let $F = (f_1, \ldots, f_s)^T$;
  determine a Gröbner basis $G = (g_1, \ldots, g_t)^T$ for the ideal $\langle F \rangle$, and transformation matrices A, B s.t. $G = A \cdot F$ and $F = B \cdot G$
- then from reductions of the S-polynomials of G to 0 we get a basis for $\mathrm{Syz}(G)$, which we can write as the rows of a matrix R
- then the rows of Q form a basis for $\mathrm{Syz}(F)$:

$$Q = \begin{pmatrix} I_s - B \cdot A \\ \cdots\cdots \\ R \cdot A \end{pmatrix}$$

[3] cf. F.Winkler, Polynomial Algorithms in Computer Algebra, Springer-Verlag Wien New York (1996), Chap. 8

Example: Consider the linear equation

$$(z_1, z_2, z_3) \cdot \underbrace{\begin{pmatrix} xz - xy^2 - 4x^2 - \frac{1}{4} \\ y^2z + 2x + \frac{1}{2} \\ x^2z + y^2 + \frac{1}{2}x \end{pmatrix}}_{F} = 0 \ ,$$

where the coefficients are in $\mathbb{Q}[x, y, z]$.
Basis for $\mathrm{Syz}(F)$:

$$(y^2z + 2x + \frac{1}{2},\ -xz + xy^2 + 4x^2 + \frac{1}{4},\ 0)$$

$$(x^2z + y^2 + \frac{1}{2}x,\ 0,\ -xz + xy^2 + 4x^2 + \frac{1}{4})$$

$$(y^4 + \frac{1}{2}xy^2 - 2x^3 - \frac{1}{2}x^2,\ -x^3y^2 - xy^2 - 4x^4 - \frac{3}{4}x^2,$$

$$xy^4 + 4x^2y^2 + \frac{1}{4}y^2 + 2x^2 + \frac{1}{2}x)$$

$$(0,\ x^2z + y^2 + \frac{1}{2}x,\ -y^2z - 2x - \frac{1}{2})$$

5. SC is changing math & science

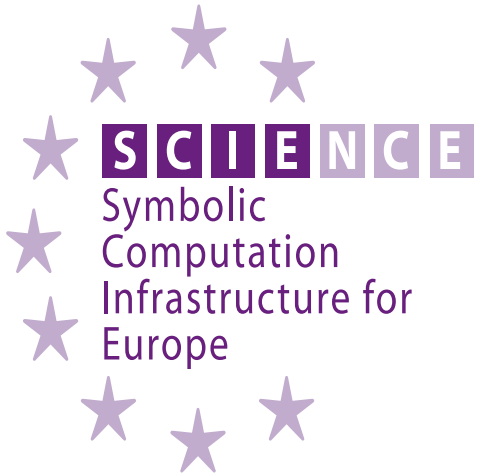
SC is now routinely used in

- mathematical research
- science and engineering
- education

European **SCIEnce** project
(**S**ymbolic **C**omputation **I**nfrastructure for **E**urope)

- The Centre for Interdisciplinary Research in Computational Algebra, **St.Andrews**, Scotland, **coordinator**
- **RISC**, Linz, Austria
- **CNRS**, Paris, France
- **Univ. Kassel**, Kassel, Germany
- **KANT**, Berlin, Germany
- **TU Eindhoven**, Eindhoven, Netherlands
- **e-Austria**, Timisoara, Romania
- **Maplesoft**, Waterloo, Canada
- **Heriot-Watt Univ.**, Edinburgh, Scotland

European **SCIEnce** project
(**S**ymbolic **C**omputation **I**nfrastructure for **E**urope)



visitors at RISC (2006–2011):

scientific area	number of visitors
mathematics	65
informatics	28
physics	6
engineering	5
	104

Conclusion

Symbolic Computation ...

- has created a lot of interesting mathematics
- helps to reunify mathematics
- changes our understanding of mathematics
- makes mathematics more useful to other scientific fields

Thank you for your attention!