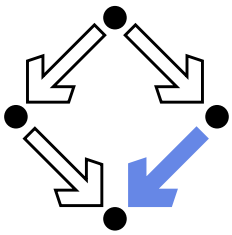
invited plenary lecture at ICAI 2010, Eger, Jan. 2010

Symbolic Computation

A philosophy of mathematics

Franz Winkler
RISC
Research Institute for Symbolic Computation
Johannes Kepler University Linz, Austria



0. Introduction

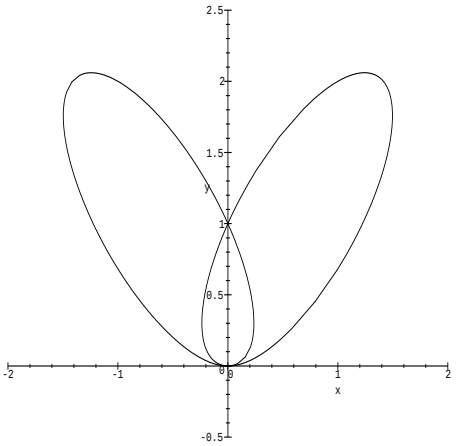
approaches to mathematics:

- existential theorems
- constructive proofs
- symbolic algorithms

the approach we take determines

- what we consider to be a satisfactory mathematical result and
- which problems we work on

1. Parametrization of curves



tacnode curve implicit:
$f(x, y) =$
$2x^4 - 3x^2y + y^4 - 2y^3 + y^2 = 0$

tacnode curve parametric:
$x(t) = \frac{t^3-6t^2+9t-2}{2t^4-16t^3+40t^2-32t+9},$
$y(t) = \frac{t^2-4t+4}{2t^4-16t^3+40t^2-32t+9}$

existential theorem:

Theorem: [1] *An irreducible algebraic curve $\mathcal{C}$ is rational if and only if the genus of $\mathcal{C}$ is 0.*

[1] cf. Sendra/W./Perez-Diaz, "Rational Algebraic Curves", Springer (2008), Theorems 4.11 and 4.63

constructive proof:

derive degree bound for parametrization:

Theorem: (SWP Thm.4.21)
Let $\mathcal{C}$ *be defined by* $f(x, y) = 0$, *and* $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$ *a proper parametrization of* $\mathcal{C}$. *Then*

$$\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}$$

$$\text{and} \quad \deg(\chi_1(t)) = \deg_y(f), \deg(\chi_2(t)) = \deg_x(f).$$

Ansatz:

$$x(t) = \frac{a_{mn}x^m y^n + \cdots a_{00}}{c_{mn}x^m y^n + \cdots c_{00}} \quad , \quad y(t) = \frac{b_{mn}x^m y^n + \cdots b_{00}}{c_{mn}x^m y^n + \cdots c_{00}}$$

plug ansatz into implicit equation $f(x, y) = 0$ and solve the corresponding system of algebraic equations

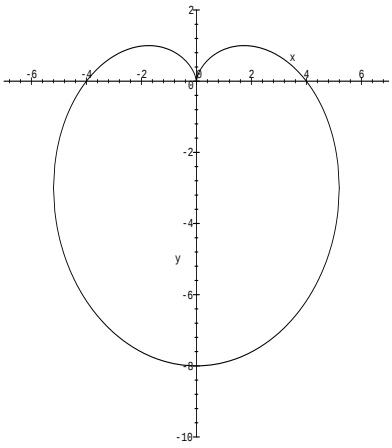
this is possible in principle, but not in practice

symbolic algorithm: [2]

- determine singularities and genus of the curve $\mathcal{C}$, and decide parametrizability
- determine a system of adjoint curves $h(x, y, t)$ of dimension 1; this involves finding a regular point on $\mathcal{C}$ with coefficients in an optimal field
- determine the common factor of $f(x, y)$ and $h(x, y, t)$ depending on t by resultant computation; this yields rational expressions for the coordinates of the "moving" intersection point, which correpond to a parametrization

[2] cf. Sendra/W./Perez-Diaz, "Rational Algebraic Curves", Springer (2008), Theorems 4.11 and 4.63

Example: cardioid curve $\mathcal{C}$



defining polynomial
$f(x, y) =$
$(x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$

- the cardioid has a double point at the origin

$$O = (0, 0)$$

and two more complex double points at infinity

$$P_{1,2} = (1 : \pm i : 0).$$

So the genus of $\mathcal{C}$ is

$$\frac{1}{2} \cdot [3 \cdot 2 \ - \ 3 \cdot 2 \cdot 1] \ = \ 0$$

and therefore $\mathcal{C}$ has a rational parametrization

- $\mathcal{C}$ hat the regular point

$$Q = (0, -8)$$

Now we consider adjoint curves of degree 2;
i.e. conics passing through all the singular points and also through the regular point Q;
the defining polynomial for this 1-dimensional system of adjoints is

$$h(x, y, t) = tx^2 + ty^2 + x + 8ty$$

- Now we determine the intersection points of the cardioid and the system of adjoints:
  the factors of $\mathrm{res}_y(f_2(x,y), h(x,y,t))$ are

$$x^3, \quad (256t^4 + 32t^2 + 1)x + 1024t^3$$

  the factors of $\mathrm{res}_x(f_2(x,y), h(x,y,t))$ are

$$y^2, \quad y + 8, \quad (256t^4 + 32t^2 + 1)y + (2048t^4 - 128t^2)$$

  So we have found a rational parametrization of $\mathcal{C}$, namely

$$x(t) = \frac{-1024t^3}{256t^4 + 32t^2 + 1}, \quad y(t) = \frac{-2048t^4 + 128t^2}{256t^4 + 32t^2 + 1}$$

2. Algebraic equations and syzygies

syzygy problem:

$f_1, \ldots, f_s$ polynomials in $x_1, \ldots, x_n$ over the field K

determine all solutions (in $K[x_1, \ldots, x_n]$) $z_1, \ldots, z_s$ of the equation

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

solutions are called **syzygies** of $f_1, \ldots, f_s$

these solutions $(z_1, \ldots, z_s)$ 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 [3]) *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)

[3] 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 [4])
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)

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

symbolic algorithm: [5]

- 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 $\mathrm{Syz}(F)$:

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

[5] 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 $\mathrm{Syz}(F)$:

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

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

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

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

syzygies play an essential role in resolution of ideals and modules

for a commutative ring R,
e.g. polynomial ring $R = K[x_1, \ldots, x_n]$,
and a module M over R,
a **free resolution** of M is:

$$\cdots \longrightarrow R^{s_2} \longrightarrow^{\varphi_2} R^{s_1} \longrightarrow^{\varphi_1} R^{s_0} \longrightarrow^{\varphi_0} M \longrightarrow 0 \ ,$$

where all these maps are linear and $\mathrm{im}(\varphi_{i+1}) = \ker(\varphi_i)$ everywhere.

Free resolutions for submodules of $K[x_1, \ldots, x_n]^m$ can be computed by Gröbner bases.
Hilbert (1890) has shown that such resolutions are always finite and not longer than m.

3. Equational logic

the problem:
given:

- 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 $s \equiv_E t \iff s = t \in =_E$

decide:

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

existential theorem:

this is a problem in predicate logic and as such semidecidable

symbolic algorithm:

(also applicable for the computation of Gröbner bases)

define a reduction relation on $\mathcal{T}(\Sigma, V)$ by orienting the equations

$$e_i : \quad s_i = t_i$$

in one of the ways (according to a reduction ordering)

$$r_i : \quad s_i \longrightarrow t_i \quad \text{or} \quad t_i \longrightarrow s_i$$

(w.l.o.g. assume $r_i : s_i \longrightarrow t_i$.
This leads to a so-called "rewrite rule system (RRS)"

$$R = \{r_i \mid i \in I\}$$

The reduction $\longrightarrow_R$ works in the following way: 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 $\sigma(t_i)$:

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

In general the termination property is undecidabel for rewrite rule systems. But there are several sufficient conditions; e.g. $s_i > t_i$ w.r.t. a reduction ordering. For the following let us assume that the rules can be ordered w.r.t. such a reduction ordering.

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

let G consist of the axioms of group theory

$$G = \{ \begin{array}{ll} (1) & 1 \cdot x = x, \\ (2) & x^{-1} \cdot x = 1, \\ (3) & (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \}$$

which are oriented (lexicographic path ordering with $^{-1} > \cdot > 1$) to give the rewrite rule system

$$R = \{ \begin{array}{ll} (1) & 1 \cdot x \longrightarrow x, \\ (2) & x^{-1} \cdot x \longrightarrow 1, \\ (3) & (x \cdot y) \cdot z \longrightarrow x \cdot (y \cdot z) \end{array} \}$$

then

$$x^{-1} \cdot (x \cdot y) \longleftarrow_{(3)} (x^{-1} \cdot x) \cdot y \longrightarrow_{(2)} 1 \cdot y \longrightarrow_{(1)} y$$

both results are irreducible,
they are congruent modulo $=_E$,
but they have no common successor

The goal is to transform the RRS R into an equivalent $\hat{R}$

$$\longleftrightarrow_R^* \quad = \quad \longleftrightarrow_{\hat{R}}^*$$

which has the Church-Rosser property

As in the previous cases (Gauss elimination, Euclidean algorithm, Gröbner bases) we investigate "smallest" situations in which a term can be reduced in essentially 2 different ways

- we look at terms which can be reduced w.r.t. two different rules $r_i : s_i \longrightarrow t_i,\ r_j : s_j \longrightarrow t_j$
- this means that there is a most general unifier (substitution) σ s.t.

  $$\sigma(s_j) \ = \ \sigma(s_i)_{|p}$$

  for some position p

if

$$\sigma(s_i)_{|p} \;=\; \sigma(s_j)$$

then

$$\begin{array}{cc} \sigma(s_i) = u & \\ \downarrow \quad \downarrow & \\ \sigma(t_i) \qquad \sigma(s_i)[p \leftarrow \sigma(t_j)] & \end{array}$$

these reduction results are obviously equal modulo $=_E$; so are normal forms v_1, v_2 to which they can be reduced. If $v_1 \neq v_2$, then we try to orient them into a new rule which will not violate the termination property

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 the 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 $=_E$

for the example of group theory this means that because of

$$x^{-1} \cdot (x \cdot y) \longleftarrow_{(3)} (x^{-1} \cdot x) \cdot y \longrightarrow_{(2)} 1 \cdot y \longrightarrow_{(1)} y$$

we add the new rule

$$(4)\ x^{-1} \cdot (x \cdot y) \longrightarrow y$$

for group theory this Knuth-Bendix process [6] actually terminates and yields the following minimal rewrite rule system:

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

[6] D.E. Knuth, P.B. Bendix, *Simple word problems in universal algebra*, in J. Leech (ed.), Computational Problems in Abstract Algebra, Pergamon Press (1970)

Conclusion

symbolic computation

is not so much a subfield of mathematics/computer science,
but a particular way of looking at mathematical problems. a

philosophy of mathematics

Thank you !