

Remembrance of Things Past

Erich L. Kaltofen

NCSU

google, bing->erich kaltofen

À la recherche du temps perdu [Marcel Proust]

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

Like my subquadratic polynomial factoring algorithm [with Shoup]

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

*Hat's mich jetzt mit meinem Apfelstrudel auf der Strudlhofstiege
hingestrudelt?*

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

Someone to the contrary: *“One can tell from the title of an ISSAC
submission if it will get accepted.”*

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

Someone to the contrary: *“One can tell from the title of an ISSAC
submission if it will get accepted.”*

My worst proposal title:

Efficient Computer Algorithms for Symbolic Mathematics

Outline (?)

*“Ein Werk der Erzählkunst ist es umso mehr,
je weniger man durch eine Inhaltsangabe
davon eine Vorstellung geben kann.”*

[Heimito von Doderer]

Translated: *“It is the more a work of artful storytelling,
the less a summary can give an idea about it.”*

Someone to the contrary: *“One can tell from the title of an ISSAC
submission if it will get accepted.”*

My best proposal titles:

1984: *Complexity Studies in Computer Algebra*

2014: *Symbolic Computation with Sparsity, Error Checking
and Error Correction*

Polynomial-time Polynomial Factoring

April 20, 1981 Letter by Hans Zassenhaus


Mr. Erich Kaltofen
Mathematical Sciences
Rensselaer Polytechnic Institute
Troy, New York 12181

Dear Mr. Kaltofen:

Please find attached a manuscript of my Ann Arbor presentation which should answer implicitly your question. Note that there is a problem of integral linear programming which finds its practical solution much more rapidly than available theoretic estimates would show.

Best regards

Yours sincerely,


Hans Zassenhaus

P.S. Please let me know how
the method works.

Polynomial-time Polynomial Factoring

October 7, 1981 Letter by Arjen K. Lenstra

Dear Mr. Kaltofen,

Unfortunately, my report on lattices & factorization of polynomials is not yet typed. I will send you a copy as soon as it is available.

The lattice algorithm (LA) will certainly not run in polynomial time of the degree of the polynomial to be factored. The last step of the LA is essentially the same as the last step of the Berlekamp-Hensel factorization algorithm in $\mathbb{Z}[X]$: combine a number of factors and try whether it is a true factor (after reduction of the coefficients modulo the reduced basis of the lattice), and therefore the LA is not polynomial in the degree.

E. 11

Polynomial-time Polynomial Factoring

June 28, 1982 Letter by Dima Grigor'ev

Dear Dr. Kaltofen:

It was very interesting for me to read your paper "A polynomial reduction" from the ACM Proc. After the recent article of Lenstra, A.K./Lenstra H.W. Jr./Lovasz, L. "Factoring polynomials with rational coefficients" I have, together with one of my colleagues, generalized their result and proved that factoring of one-variable polynomials over any global field (in particular, algebraic number field), can be done in polynomial time. If you are interested in this subject, I can send you the paper. At the very end of your already mentioned paper it is claimed (and also it was told to me according to your report by Martin Fürer who participated in the Conference) that you can reduce the many-variable case to one-variable one. So after compiling all these results a nice thing would be obtained and I ask you if it is possible to send me some of your work about this reduction. Thank you in advance.

Now I am working for a month in Zürich with Prof. V. Strassen. My permanent

address is: Dr. D. Grigor'ev
Fontanka 27, LOMI
Leningrad 191011 USSR

Sincerely,



(D. Grigor'ev)

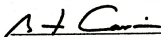
ON THE COMPLEXITY OF FACTORING POLYNOMIALS
WITH INTEGER COEFFICIENTS

by

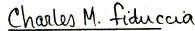
Erich Kaltofen

A Thesis Submitted to the Graduate
Faculty of Rensselaer Polytechnic Institute
in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
Major Subject: Computer Science

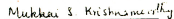
Approved by the
Examining Committee



Bobby F. Caviness, Thesis Adviser



Charles M. Fiduccia, Member



Mukkai S. Krishnamoorthy, Member



Robert McNaughton, Member



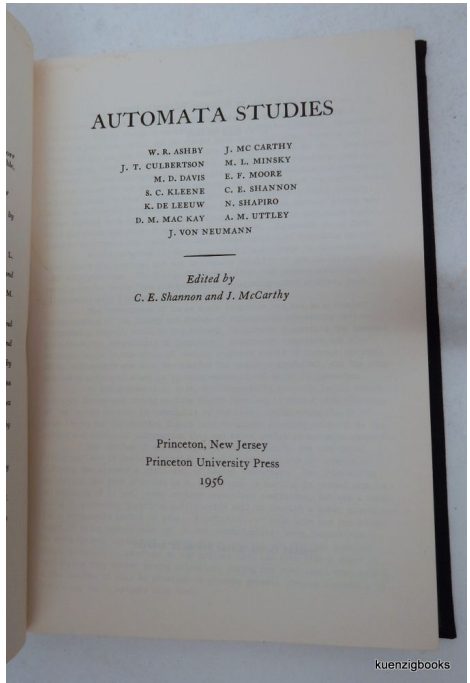
B. David Saunders, Member

Rensselaer Polytechnic Institute
Troy, New York

December 1982

Complexity Studies...

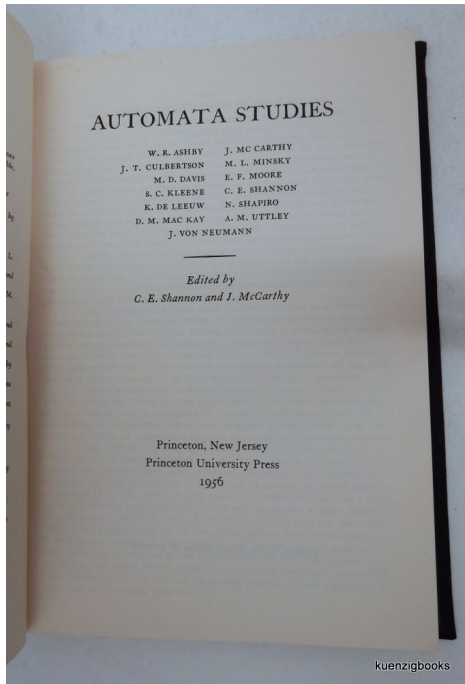
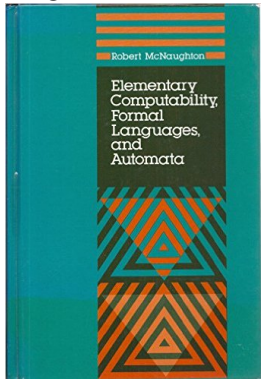
Bob McNaughton used to cite
“Intelligence of the Artificial”



Complexity Studies...

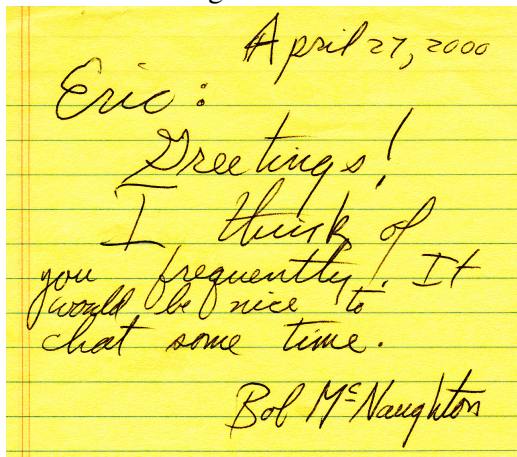
Bob McNaughton used to cite
“Intelligence of the Artificial”

Section 1.1 in Bob’s textbook:
“Algorithm” Defined



Complexity Studies...

and Bob McNaughton remembered me after I left RPI



April 27, 2000
Eric:
Greetings!
I think of
you frequently. It
would be nice to
chat some time.
Bob McNaughton

M.S.Krishnamoorthy, Robert McNaughton, Me [June 2008]



Polynomial Multiplication with David G. Cantor [1986]

*“In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an **arbitrary, not necessarily commutative, not necessarily associative**, algebra \mathcal{A} . Our main result is an algorithm to multiply polynomials of degree $< n$ in $O(n \log n)$ algebra multiplications and $O(n \log n \log \log n)$ algebra additions/subtractions (we count a subtraction as an addition). The constant implied by the “ O ” does not depend upon the algebra \mathcal{A} . The parallel complexity of our algorithm, i.e., the depth of the corresponding arithmetic circuit, is $O(\log n)$.”*

Polynomial Multiplication with David G. Cantor [1986]

*“In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an **arbitrary, not necessarily commutative, not necessarily associative**, algebra \mathcal{A} . Our main result is an algorithm to multiply polynomials of degree $< n$ in $O(n \log n)$ algebra multiplications and $O(n \log n \log \log n)$ algebra additions/subtractions (we count a subtraction as an addition). The constant implied by the “ O ” does not depend upon the algebra \mathcal{A} . The parallel complexity of our algorithm, i.e., the depth of the corresponding arithmetic circuit, is $O(\log n)$.”*

Best complexity today (after 30 years) [don't let others fool you!]

Google scholar: my most cited paper

On fast multiplication of polynomials over arbitrary algebras

DG Cantor, E Kaltofen - Acta Informatica, 1991 - Springer

In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an arbitrary, not necessarily commutative, not necessarily associative, algebra d . Our main result is an ...

Cited by 333 Related articles All 16 versions Cite Save

Google scholar: my most cited paper

On fast multiplication of polynomials over arbitrary algebras

DG Cantor, E Kaltofen - Acta Informatica, 1991 - Springer

In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an arbitrary, not necessarily commutative, not necessarily associative, algebra d . Our main result is an ...

Cited by 333 Related articles All 16 versions Cite Save

Not David's most cited paper:

Computing in the Jacobian of a hyperelliptic curve

DG Cantor - Mathematics of computation, 1987 - ams.org

Abstract: In this paper we present algorithms, suitable for computer use, for computation in the Jacobian of a hyperelliptic curve. We present a reduction algorithm which is asymptotically faster than that of Gauss when the genus g is very large.

Cited by 524 Related articles All 3 versions Cite Save

Date: Sat, 27 Apr 91 18:53:09 +0100
From: "David G. Cantor" <dgc@math.ucla.edu>
Subject: Our joint paper
To: Professor Erich Kaltofen <kaltofen@cs.rpi.edu>

... [stuff about our paper]

I am finally completing what turned out to be a lengthy project, partly because of health problems and partly because of intrinsic difficulty. I don't know whether or not you are familiar with the "division polynomials" for elliptic curves, but they play a fundamental role in, for example, Schoof's algorithm, etc.

I have succeeded in finding their analogues for hyperelliptic curves. At the moment, I am writing up the formulas that enable you to multiply by n an element of the Jacobian of such a curve which is represented by a single point (in general, elements of the Jacobian need up to g points to represent them, where g is the genus). What I get is a polynomial of degree $\leq g$ whose zeros are the x -coordinates of this multiple. The leading coefficient is a square of a polynomial. This polynomial is the analogue of the ordinary division polynomial for elliptic curves and satisfies quite similar recurrence relations.

I will send you a draft shortly.
Best wishes,
dgc

David Cantor and me at La Jolla Shores, August 1993



An email from smwatt@watson.ibm.com

From smwatt@watson.ibm.com Fri Apr 19 12:19:42 1991

To: ..., kaltofen@cs.rpi.edu, ...

Subject: What are you doing Friday April 26?

!!!!!!!!!! Taste that Malt !!!!!!!!!!!

When? Friday April 26, 8:00pm

Where? 731 Locksley Road, Yorktown

Don't be caught out by bourgeois pseudo-intellectuals --
educate your taste buds.

Compare and contrast the single malt whiskies of Scotland.

From the Highlands:

The Singleton of Auchroisk

Glenfiddich

From the Isle of Islay:

The Bowmore

Talisker

You will not be expected to eat a haggis, nor toss a caber.

Malts selected by Michael Dewar

Gilles Villard: first contact

Date: Thu, 11 Mar 1993 12:05:47 +0100
From: Gilles Villard <gvillard@aquilon.imag.fr>
Subject: Smith
To: kaltofen@cs.rpi.edu
Cc: gvillard@aquilon.imag.fr

Dear Prof. Kaltofen

Few months ago, I sent you a technical report on matrix normal forms (I. Gil & G. Villard, TR91-IMAG France), and especially, a new result on the computation of the Smith form of polynomial matrices.

... [technical stuff about Gilles's ISSAC 1993 submission]

You now understand the aim of this message : did you read the paper ? If yes, what do you think of the different results I am claiming ?

Hoping that I do not waste too much your time.

Best regards.

Gilles.

A Quotation

Gilles used to say to me:

“Erich, can one not ...?”

Erich, why is ...?”

Erich, what if we ...?””

A Quotation

Gilles used to say to me:

“Erich, can one not ...?”

Erich, why is ...?”

Erich, what if we ...?””

I finally said:

*“Please stop asking me questions,
and start giving me answers.”*

A Quotation

Gilles used to say to me:

“Erich, can one not ...?”

Erich, why is ...?

Erich, what if we ...?”

I finally said:

*“Please stop asking me questions,
and start giving me answers.”*

And the answer is: **2.694691**

A Quotation

Gilles used to say to me:

“Erich, can one not ...?”

Erich, why is ...?”

Erich, what if we ...?””

I finally said:

*“Please stop asking me questions,
and start giving me answers.”*

And the answer is: **2.694691**

= our complexity exponent for division-free det computation

Lihong Zhi: first contact

Date: Mon, 30 Aug 1999 09:58:22 +0900 (JST)
From: Zhi Lihong <lzhi@ichigo.cs.ehime-u.ac.jp>
Subject: Re: Your JSC 26 paper
To: kaltofen@eos.ncsu.edu

Dear Prof.Kaltofen:

Thank you very much for the comments. Actually, we have derived the explicit expression of the least square solution in our new paper attached below. But we could not find the explicit expression of the nearest singular polynomial with a root of multiplicity $k > 4$. The algorithm has also been implemented in Maple. ... [comments on the efficiency of the implementation.]

Thank you for sending us your papers. Hope we can keep in touch!

Best wishes,

Lihong Zhi

URL: <http://hpc.cs.ehime-u.ac.jp/~lzhi/English>

Photo from

<http://hpc.cs.ehime-u.ac.jp/~lzhi/English>



Photo 2002, Forbidden City



Paradoxes

West Lake in Hangzhou, China is nicer in rain than in sunshine,
but best in snowfall [Ming dynasty saying]

I was there twice, it was hot:

Dreaming of melting snow on the Broken Bridge of the White Snake

Paradoxes

West Lake in Hangzhou, China is nicer in rain than in sunshine,
but best in snowfall [Ming dynasty saying]

I was there twice, it was hot:

Dreaming of melting snow on the Broken Bridge of the White Snake

Sidebar: what does the Lesser Yingzhou Island in West Lake
and Manitoulin Island in Lake Huron have in common?

Paradoxes

West Lake in Hangzhou, China is nicer in rain than in sunshine,
but best in snowfall [Ming dynasty saying]

I was there twice, it was hot:

Dreaming of melting snow on the Broken Bridge of the White Snake

Sidebar: what does the Lesser Yingzhou Island in West Lake
and Manitoulin Island in Lake Huron have in common?

Both islands have lakes on them, in fact Lake Manitou is the
largest lake on an island in a lake in the world: $104\text{km}^2=16$ West Lakes

Both those lakes on islands in lakes have themselves islands.

Paradoxes

Ugly coins become the more expensive

Few people buy them, so they become rare

Paradoxes

Climbing mountain faces is easier in winter than in summer

One can ice-climb, no falling rocks

Paradoxes

The poorest farms in Tyrol (when I was a child) are now the richest
They are high up with steep mountain meadows,
then skiing tourism happened.

(If Bruno Buchberger were here, I would ask him now
to jodel)

Paradoxes

Symbolic computation prospers even though many famous algorithms are exponential-time (except polynomial factorization)

Paradoxes

Symbolic computation prospers even though many famous algorithms are exponential-time (except polynomial factorization)

I have tried to explain this paradox in my 2012 talks
“*Symbolic Computation and Complexity Theory*”
in Lyon, Paris, and Beijing,
but today I find it even more difficult to explain.

Date: Thu, 5 Sep 2002 17:14:26 -0400
From: Erich Kaltofen <kaltofen@unity.ncsu.edu>
Subject: Re: 2 comments on your book
To: Stephen Wolfram <sw@wolfram.com>

On Aug 22, 11:46pm, Stephen Wolfram wrote:

> Subject: Re: 2 comments on your book

... [exchange on blackbox polynomials.]

> I am also puzzled by your remark about my alleged remark about NP hardness!

> Where in NKS is the remark that you're referring to?

The remark is on pp. 1142-1143 on computational complexity theory.
You write: ``But increasingly it became clear that general asymptotic results [a proof of NP-completeness as you write just above it] are often quite irrelevant in typical problems of reasonable size.'' And you continue: ``And certainly pattern matching with `__` in Mathematica as well as polynomial manipulation functions like `GroebnerBasis` routinely deal with problems that are formally NP-complete.''

> ... [SW remarks on NKS and Computer Algebra]

I certainly will keep paying attention to what you say.

Sincerely yours,

Erich

Which Problems I Would Love to See Solved

“Modern Computer Algebra” is a sad book because

Which Problems I Would Love to See Solved

“*Modern Computer Algebra*” is a sad book because it has too many problems

Which Problems I Would Love to See Solved

The “Usual Suspects”

Matrix multiplication in $n^{2+o(1)}$

Polynomial multiplication in $O(n \log(n))$ additions, subtractions, multiplications (and no constants, then it is the lower bound)

Polynomial factorization in $\mathbb{Z}_2[x]$ in $n^{1+o(1)}$

Integer Sylvester Resultant in $(\deg(f) + \deg(g))^{1+o(1)}$ **bit** complexity
[added by Arne]

Integer factoring in polynomial time. Are you kidding?

Squareroot modulo p in **deterministic** polynomial time in $\log(p)$.
I don't care much.

Which Problems I Would Love to See Solved

Esoterica

Characteristic polynomial of a sparse matrix in quadratic time

Division-free determinant in $n^{\omega+o(1)}$

Polynomial-time interpolation of fractions of supersparse polynomials

Avoiding shifting by one in early termination of sparse interpolation.
SOLVED! [ISSAC 2016]

Removing crypto from linear algebra certificates. Why remove a tool?

Downloadable software for sum-of-squares certificates

Which Problems I Would Love to See Solved

Esoterica

Characteristic polynomial of a sparse matrix in quadratic time

Division-free determinant in $n^{\omega+o(1)}$

Polynomial-time interpolation of fractions of supersparse polynomials

Avoiding shifting by one in early termination of sparse interpolation.
SOLVED! [ISSAC 2016]

Removing crypto from linear algebra certificates. Why remove a tool?

Downloadable software for sum-of-squares certificates

Reversing the order of sample use and description in the help pages of Maple. Never going to happen

My favorite algorithm

For a long time: Karatsuba integer multiplication

Donald Knuth told me his: the Euclidean algorithm

My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}$, $\lim_{i \rightarrow \infty} f(x_i) = 0$

Example 1: $f = \frac{1}{x} - a$

$x_{i+1} = 2x_i - ax_i^2$ no division \Rightarrow division = $O(\text{multiplication})$

$$\underbrace{\frac{1}{a} - x_{i+1}}_{\varepsilon_{i+1}} = \frac{1}{a} - 2x_i + ax_i^2 = a \underbrace{\left(\frac{1}{a} - x_i\right)^2}_{\varepsilon_i^2}$$

My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}$, $\lim_{i \rightarrow \infty} f(x_i) = 0$

Example 2: $f = x^2 - 316914293398696569$,

$$x_{i+1} = \left[\frac{x_i}{2} + \frac{316914293398696569}{2x_i} \right]$$

$$\begin{aligned} x_0 &= 500000000, x_1 = 566914293, x_2 = 562965263, \\ x_3 &= 562951413, x_4 = 562951413, \\ 562951413^2 &= 316914293398696569. \end{aligned}$$

My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}, \quad \lim_{i \rightarrow \infty} f(x_i) = 0$

Example 3: SAT-solver: $\dots \wedge (\neg p_3 \vee p_5 \vee \neg p_8) \wedge \dots \iff$
 $\dots, p_3(1-p_5)p_8=0, \dots, p_3(p_3-1)=0, p_5(p_5-1)=0, p_8(p_8-1)=0.$

“Just” solve the polynomial system with multivariate

Newton/homotopy iteration: how difficult can it be to initialize the iteration?

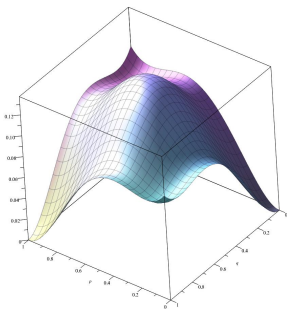
My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}$, $\lim_{i \rightarrow \infty} f(x_i) = 0$

Example 3: SAT-solver: $\dots \wedge (\neg p_3 \vee p_5 \vee \neg p_8) \wedge \dots \iff$
 $\dots, p_3(1-p_5)p_8=0, \dots, p_3(p_3-1)=0, p_5(p_5-1)=0, p_8(p_8-1)=0.$

“Just” solve the polynomial system with multivariate

Newton/homotopy iteration: how difficult can it be to initialize the iteration?



$$\begin{aligned} & (p^2 - p)^2 + (q^2 - q)^2 \\ & + \frac{1}{10}p^2(1 - q)^2 + \frac{1}{10}(1 - p)^2q^2 \\ & \iff (\neg p \vee q) \wedge (p \vee \neg q) \\ & \iff p \equiv q \end{aligned}$$

My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}$, $\lim_{i \rightarrow \infty} f(x_i) = 0$

Example 3: SAT-solver: $\dots \wedge (\neg p_3 \vee p_5 \vee \neg p_8) \wedge \dots \iff$
 $\dots, p_3(1-p_5)p_8=0, \dots, p_3(p_3-1)=0, p_5(p_5-1)=0, p_8(p_8-1)=0.$

“Just” solve the polynomial system with multivariate Newton/homotopy iteration: how difficult can it be to initialize the iteration?

If too difficult, use *Buchberger's Algorithm* modulo 2
 Jean-Charles Faugère tried, of course

My favorite algorithm

Now it is Newton-Raphson: $x_{i+1} = x_i - \frac{f(x_i)}{\frac{\partial f}{\partial x}(x_i)}, \quad \lim_{i \rightarrow \infty} f(x_i) = 0$

Example 3: SAT-solver: $\dots \wedge (\neg p_3 \vee p_5 \vee \neg p_8) \wedge \dots \iff$
 $\dots, p_3(1-p_5)p_8=0, \dots, p_3(p_3-1)=0, p_5(p_5-1)=0, p_8(p_8-1)=0.$

“Just” solve the polynomial system with multivariate
 Newton/homotopy iteration: how difficult can it be to initialize the
 iteration?

Question:

can Buchberger (and its derivatives such as FGb)
 ever beat Newton (and its derivatives such as SeDuMi)
 on hard problems over the real numbers?

At who I shall never get angry again...

Mark Giesbrecht: he nominated me **twice** for the ACM Fellowship

Mark, if I get angry at you just say "Fellow"

At who I shall never get angry again...

Mark Giesbrecht: he nominated me **twice** for the ACM Fellowship

Mark, if I get angry at you just say “Fellow”

Wen-shin Lee, Lihong Zhi and Arne Storjohann

Wen-shin, Lihong, Arne, if I get angry at you just say “MICA”

(It's impossible to get angry at Shaoshi Chen)

My Mistress...

is scientific research: I have spent all my live with it

My Mistress...

is scientific research: I have spent all my life with it

Hoang has patiently been by my side:

“Hoang, it works!!!” and 5 minutes later “Shoot, it doesn’t.”

$f(\alpha) = \alpha^p$ is a linear map in \mathbb{F}_q over \mathbb{F}_p computable in $(\log(p)\log(q))^{1+o(1)}$ on which the transposition principle fails.

Subquadratic factoring is ruined...

but wait, there is a linear matrix-times-vector product in the minpoly eval step

“Hoang, it does work!” “Erich, I hope so.”

My Mistress...

is scientific research: I have spent all my life with it

Hoang has patiently been by my side:

“Hoang, it works!!!” and 5 minutes later “Shoot, it doesn’t.”

$f(\alpha) = \alpha^p$ is a linear map in \mathbb{F}_q over \mathbb{F}_p computable in $(\log(p)\log(q))^{1+o(1)}$ on which the transposition principle fails.

Subquadratic factoring is ruined...

but wait, there is a linear matrix-times-vector product in the minpoly eval step

“Hoang, it does work!” “Erich, I hope so.”

Research is my mistress, but ...

Hoang, you are the love of my life.
Thank you!

Thank you everybody!