# Notes at ISSAC 2010

JHD

25–26 July 2010
Technische Universität München

**Abstract**

Note (page 15) the earlier dates for ISSAC 2011: `http://www.issac-conference/2011`.

The most surprising fact, to JHD, was that for the past eight years Daimler have been using parameterised quantified SAT-solving to configure cars according to customer orders (page 13).

# Contents

# Chapter 1

# 25 July 2010

## 1.1 Tutorial: Algebraic Invariants and Their Differential Algebra

JHD arrived part-way through this. The talk was advertised as being given by Tsarev, but in fact was given by Ke.

### 1.1.1 Finite Groups

There are as many invariants $f_1, \ldots, f_n$ as the dimension of $V$. These are the *primary invariants*. Then the homogeneous generators of $K[V]^G$ as a module over $K[f_1, \ldots, f_n]$ are the secondary invariants.

### 1.1.2 non-modular case

$|G|$ is *not* a multiple of $\mathrm{char}(K)$ (in paricular

Then we have the **Cohen-Macauley** property: $K[V]^G$ is free as a $K[f_1, \ldots, f_n]$-module. Then **Molien's formula** says that the **Hilbert series** is

$$H(K[V]^G, t) = \sum_{d=0}^{\infty} \dim(K[V]^G_d) t^d = \frac{1}{|G} \sum_{\sigma \in G} \frac{1}{\det(1 - t\sigma)}.$$

If the $f_i$ are the primary invariants, then

$$H(K[V]^G, t) == \frac{t^{d_1} + \cdots + t^{d_m}}{\prod (1 - t^{\deg f_i})}$$

where the $d_i$ are the degrees of the secondary invariants.

### 1.1.3 Application: coding theory

Let $c \subseteq \mathbf{F}_3^n$ be a self-dual linear code with $\mathbf{1} \in C$. Let the **complete weight enumerator** be

$$f(x, y, z) = \sum_{c \in C} x^{n_0(c)} y^{n_1(c)} z^{n_2(c)}$$

where $n_i(c)$ is the number of occurrences of $i$ in $c$. There are various invariants, e.g. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 0 & 0 & \end{pmatrix}$, and the MacWilliams identity.

This can be done in Magma, and the result is

$$\frac{1 + t^{24}}{\left(1 - t^{12}\right)^2 \left(1 - t^{36}\right)},$$

which is, to say the least, very suggestive.

### 1.1.4 modular case

Neither CM nor Molien's formula are available. Let $A = K[f_1, \ldots, f_n]$. The group generators $\sigma_1, \ldots, \sigma_l$ define $A$-linear maps $K[V] \to K[V]$. The kernel of the combined map $K[V] \to K[V]^l$ is $K[V]^G$.

### 1.1.5 Noether's degree bound

Let $G$ be finite and $V$ a $g$-module. Let $\beta(K[V]^G)$ be

$$\min \left\{ K \mid K[V]^g \text{ can be generated in degree} \leq k \right\}.$$

**Theorem 1 (Noether's degree bound)** *If* $|G|$ *is not a multiple of* $\mathrm{char}(K)$*, then*

$$\beta(K[V]^G) \leq |G|.$$

In the case $\mathrm{char}(K) < |G|$ this was only proved by Fleischmann and Fogarty in 2000. This can fail badly in the modular case.

### 1.1.6 Infinite Group Case

### 1.1.7 The Derksen ideal

Let $G$ act on a $K$-algebra $R$. Let $x_1, \ldots, x_n \in R$ (which *might* be generators, but certainly no necessarily independent). Let $y_1, \ldots, y_n$ be indeterminates. Thern there are three forms of Derksen ideal

**Algebraic** $D := \bigcap_{\sigma \in G} (y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n))$

**Geometric** If $R = K[V] = K[x_1, ldots, x_n]$ the $D$ is the vanishing ideal of the set

$$\{(x, y) \in V \times V \mid G(x) = G(y)\}.$$

**Computational** If $G \subset K^m$ is given by its vanishing ideal $I_G \subset K[t_1, \ldots, t_m]$ and $\sigma(x_i) = f_i(\sigma)$ with $f_i \in R[t_1, \ldots, t_m]$, then

$$D = I_G \cup \{y_1 - f_1, \ldots, y_n - f_n\} = \cdots.$$

Derksen's algorithm (essentially the third form) is in Magma (or at least he showed a piece of code which implemented it).

### 1.1.8 Invariant Fields

Assume $G$ acts on $N = K(x_1, \ldots, x_n)$. Then compute a reduced Gröbner baseis $B$ or

$$D := \bigcap_{\sigma \in G} \langle y - \sigma(x_1), \ldots, y_n - \sigma(x_n) \rangle_{N[y_1, \ldots, q_n]}.$$

Let $L$ be $K$ extended by all the coefficients in $B$.

**Theorem 2 (Müller-Quade, Beth, Ke)** $N^G = L$.

1. $D$ is $G$-stable. Reduced Gröbner bases are unique, so $\sigma(B) = B \forall \sigma$. Hence $\sigma(g) = g$ for $g \in B$. Hence $L \subseteq N^G$.

2. Let $\alpha \in N^G$. Write

   $$a = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}.$$

   Then $f - \alpha g \in D$, so

   $$0 = \mathrm{NF}_B(f - \alpha g) = \mathrm{NF}_B(f) - \alpha \, \mathrm{NF}_B(b).$$

Daigle & Freudenburg gave a "small" example of a $G_\alpha$-action with a non-finitely-generated invariant ring.

**Theorem 3 (Rosenlicht's Theorem)**

We can do better if we look at *separating* invariants, when Noether's degree bound holds for separating invariants even in the modular case (providing $G$ is finite). We can compute $K[V]^G$ (Ke 2003). There is an extension that computes $K[X]^G$ (Derksen & Ke, 2008).

# Chapter 2

# 26 July 2010

## 2.1 Opening — Mayr

This is the third ISSAC in Germany (1991 Bonn; 1998 Rostock), and fifth in German-speaking lands (2008 Hagenberg; 1994 Zürich). Grateful to maplesoft and TI for support. The registered attendance is 205, which is good.

`http://www.issac-conferences.org/proceedings2010`.

## 2.2 Theory of Reals for Verification and Synthesis of Hybrid Dynamical Systems — Ashish Tiwari

There is increasing interaction between embedded software/cyber and the physical world. Notable areas include Aerospace and Automobile.

$$\begin{aligned} \dot{v} &= a \\ \dot{a} &= -4v - 3v_f \cdots \\ \cdots &= \cdots \end{aligned}$$

Some states are initial, and some are bad. How can we prove that we never end up in a 'bad' region. Hence we need an invariant

$$c_1 v + c_2 + 3c_3 v_f + c_4 gap \leq c_5 \tag{2.1}$$

which acts as a 'barrier' between starting states and bad states.More formally:

- All initial states do satisfy (2.1);
- All evolution of a state satisfing (2.1) continues to satisfy (2.1);
- All bad states do not satisfy (2.1).

### 2.2.1 Aircraft Model

$$\frac{\mathrm{d}\vec{x}}{\mathrm{d}t} = f(\vec{x}) \tag{2.2}$$

where $\vec{x}$ is a state vector consisting of airspeed, angle of attack, pitch rate ....

We need "satisfiability modulo theories" and such solvers exist that can solve probems with thousands of variables and constraints. They include decision procedures for many areas. He visualises this as a loop between searching for a model of $F$ and searching for a proof of $\neg F$. Modern systems now 'learn from failures', which makes the searching feasible. Hence this technology realises the dream of having embedded deduction.

But very limited support for computer algebra topics such as nonlinear constraints, which is essential for complex cyber/physical probelms, and models from systems biology. Hence can we integrate the two isn a way that does *not* compromise the speed and efficacy of the SMT systems.

Model analysis is the canonical application area for SMT solvers. Most verification problems are, in principle, undecidable.. Given an instance $\phi$ of an undecidable probem $L$, we can either:

- Focus on showing $\phi \in L$;
- Focus on showing $\phi \notin L$ (bug finding).

If the problem is undecidable, we cannot have a sound complete terminating program! So what do we give up.

### 2.2.2 Nonlinear Real Arithmetic

Focus on $\forall$ problems first. Given a set of nonlieanr equations and inequalities

$$\begin{aligned} p &= 0 \quad p \in P \\ q &> 0 \quad q \in Q \\ r &\geq 0 \quad r \in R \end{aligned}$$

Decidable ([Tar51]), and indeed elementary ([Col75]), but not practicable. So we need an SMT$-$ procedure. We introduce *slack variables* $\mathbf{v}$ and $\mathbf{w}$. A *witness* for unsatisfiability would be a $p \in Ideal(P, Q - \mathbf{v}, R - \mathbf{w})$ which is (demonstrably) a positive variable. Given $x^3 = x$, $x > 2$ introduce a slakc $v$ and get $v^3 + 6v^2 + 11v + 6$, which is clearly positive, and so has no prsitive root $v$, hence unsatisfiable. This example works, but in general the witness polynomial may not appear in the Gröbner basis. In linear situations, we can solve this by pivoting: what is the nonlinear analogue? Hence we need a Positivstellensatz.

Semi-definite programming solves many of these problems, notably by Sum-Of-Squares techniques.

### 2.2.3 Concluson

There is a market for fast, but incomplete, tools. Reasoning about nonlinear constraints is presently a critical bottleneck. We will need to augment sound symbolic techniques with fast numerical approaches.

**Q.—CWB** A lot of QEPCAD work has gone into simplification: is that important? Do the SMT tools alrready do simplification?

**A.** yes — certainly. The current tools do not do a good job of simplification.

**Q.—FW** For an incomplete tool, do you want to measure "how far away"?

**A.** Certainly. There's a trivial incomplete tool that always says "maybe".

## 2.3 A New Algorithm for Computing Groebner Bases — Volny

The version in in the paper, G2V, is incremental. This version needs not be. Let $R = F[x_1, \ldots, x_n]$. Let $G = \{g_1, \ldots, g_m\} \in R$.

**Definition 1** *$H$, the syzygy module of $G$ is ...*

We compute simulteneously, the basis of $G$ it and $H$: every "usless" relcomputation for $GB(G)$ is in fact a datum for $GB(H)$.

**Definition 2** *A $(\mathbf{u}, v) \in R^m \times R$ pair is such that $\sum u_i g_i = v$.*

**Definition 3** *We say that $(u_1, v_1)$ is top-reducible by $(u_2, v_2)$ if*

1. $\mathrm{lm}(v_2)$ *divides* $\mathrm{lm}(v_1)$
2. $\mathrm{lm}(tu_2) \leq \mathrm{lm}(tu_1)$

*We compute all the regular top-reductions first, then super-top-reductions.*

**Definition 4** *We consider the module*

$$M = \{(u, v) \ldots\}$$

We have a concept of Gröbner base for $J$-reduction. If we have one, then $\{u_i\}$ is a Gröbner basis for $H$ and $\{v_i\}$ is a Gröbner basis for $G$.

1. initialise$H$ with the principle syzygies.
2. Initialise $S$ with $(E_i, g_i)$.
3. Form $J$-pairs not reducible by $H$
4. Process $J$-pairs in order

Note that we are free to choose the ordering on $R^m$ for the syzygy module if we are eventually only interested in the Gröbner basis for $G$. For any odering on $R$, there are severla extensions to $R^m$.

Shows an implementation in Singular showing a 2–10 fold increase. Orderings TOP and $g_1$ work well until cyclic–7, when they run for days.

Note that correctness is proved, but termination is still open.

**Q.** Is this not possible by taking an implementation of Buchberger, and adding extra information.

**A.** We only keep the leading monomial of the $u_i$, so this may be what we mean.

**Q.** Why just a jump?

**A.** We'd like to find out? But TOP is generally poor.

**Q.—SMW** Have you considered changing orders in flight?

**A.** No — we'd have to patch up the observation that suprt-top reducible things remain super-top reducible, but.

### 2.3.1 Postscript

JHD discussed this paper with CT. CT observed that the comment "a zero reduction in computing $G$ is useful information for $H$" had been made before (e.g. [MMT92]), but not as effectively as here. [GM86] had confused people here. The ordering on $H$ is critical. He observed that this ordering has actually to depend on the $f_i$ (or at least the $\mathrm{lm}(f_i)$), and can't just depend on the ordering chosen in $G$.

JHD also discussed this with HS. He thought that the algorithm was actually $\mathrm{F}_5$,

## 2.4 Degree bounds for Gröbner bases of Low-dimensional Polynomial Ideals — Ritscher

$K[x_1, \ldots, x_n]$ polyoial rind, $I = \langle f_1, \ldots, f_s \rangle$ with total degrees pounded by $d$. let $G$ be a reduced Gröbner basis for $I$. Can we bound the total degree of elements of $G$?

**Theorem 4 (Dubé1990)**

$$\deg(G) \leq 2\left(\frac{1}{2}d^2 + d\right)^{2^{n-1}}$$

*Looks frightening, but consider [MM82].*

Define the affine ideal dimension to be the degree of the Hilbert polynomial.

**Theorem 5** *Our contribution:*

$$\deg(G) \leq 2\left(\frac{1}{2}d^{n-r} + d\right)^{2^r}$$

This proof is based on Dubé, $C(h,U) = h \cdot K[U]$. Let $T = C(h_1,U_1)\oplus = cdots \oplus C(h_l,U_l)$. Call the set of cone a "cone decomposition" of $T$. Let deg $P=$ max degree cones. Dubé's strategy was to prove that the degree of a Gröbner basis was at worst the degree of the cone decompoisition. We proceed simuilarly, embedding a reular sequence $(g_1,\ldots,g_{n-r})$ in $I$; computing a cone decompoisition $Q$ of $N_{angleg_1,\ldots,g_{n-r}\rangle}$ extending one of $N_I$. We can then (worst case!) canonicalise $Q$. We then compute $\deg(Q)$ from the Hilbert polynoial, with a better special-case contruction.

So our upper and lower bounds are both doubly exponential, but only in the ideal dimension not the number of variables. The lower bounds are almost matching.

## 2.5 A New Algorithm for Computing Comprehensive Gröbner Bases — Sun

Main application a of Comprehensive Gröbner bases are solving systems of parametric equations, but also in geometric theorem proving. Our contributions are

1. A new algorithm for computing
2. some new methods for checking consistency of parametric constraints.

### 2.5.1 New Algorithm

A specialisation is a homomorphism $\sigma : K[U] \to L$ where $L$ is the algebraic closure of $k$.

**Definition 5** $\mathcal{G} = \{(A_1,G_1),\ldots,(A_k,G_k)\}$ *is defined to be a comprehensive Gröbner basis for* $F$ *if* $\forall a \in A_i$, $\sigma(G_i)$ *is a Gröbner basis for* $\sigma(F)$.

There are various step-by-step methods ([Wei92] etc.), and direct methods ([SS02]).

**Definition 6** *We say* $F$ *is the set Noncomparable*$(G)$ *if*

- $F \subset G$
- $\langle \mathrm{lpp}_X(F)\rangle = \langle \mathrm{lpp}_X(G)\rangle = \langle x,y\rangle$
- *No redundant polynomials in* $F$

**Theorem 6** *If .... Let* $G_r = G \cap k[U]$, *and* $G_m$*=Noncomparable*$(G \backslash G_r)$. *Then* $\sigma(G_m)$ *is a minimal Gröbner basis of* $\langle\sigma(F)\rangle$.

### 2.5.2 Consistency

If $V(E) \setminus V(N) \neq \emptyset$ we say that the parametric constraint $(E, N)$ is consistent. This is equivalent to $N \subset \sqrt{I}$. In general this is inefficient, but if $\dim(E) = 0$ we are OK. If not,

**Theorem 7** *Let $v$ be the maximal independent set of $E$ and $v' = U \setminus v$, $\alpha \in L^n$ be a random $n$-tuple, then if $F(\alpha, v') \notin \sqrt{\langle E(\alpha, v') \rangle}$, $F \notin \sqrt{E}$.*

Shows timings in Magma, much more efficient than [SS02]. Only 4% of the time do we need the general check for radical membership, thanks to a fast trivial check and Theorem 7.

## 2.6 Maple 14 — Gerhardt

New option `discont=removable` to the plotting packages. Better ability to select regions or points from plots. Pointers to the more effienct code for polynomials *ex parte* Monagan. New commands for ODEs and PDEs. Polynomial system solvers now allow domain restriction. e.g. `RealSolutions` etc. There is also new functionality for parametric case discussion.[1] Consider Also case discussion in `ComprehensiveTriangularize`.

Improved computation of numerical limits, e.g. limits of Bessel functions *with respect to* $\nu$. New ODE solvers, based on Cash/Karp (largeyly riven by MapleSim, but more generally available). Also for algerbric Riccati equations.

Polynomial root finding has bounding boxes, and winess points (guaranteed at least one on each connected component).

## 2.7 — Strzebonski

Semi-algebraic set is a disjunction of conjunctions of polynomial equations and inequalities. Quantified systems

$$Q_1 t_1 \ldots Q - m t_m S(t_1, \ldots, t_m, x_1, \ldots, x_n)$$

which is semi-algebraic by Tarski's Theorem [Tar51]. Collins's algorithm [Col75] also gives us delineability.

The CAF formalosm lets us decide

- If a set is non-empty
- find min/max values if the first coordinate
- Find sample points.
- Find a graphical representation
- Find volume.

[1] JHD suspects this builds on the work at MathUI 2009.

So can we manipulate such sets? Shows how to do `unoin` and `intersection`. Why — his construction.

## 2.8 Black-box/White-box simplification and applications to cylindrical decomposition — C.W. Brown

Tarski formulae. Issues sucj as

- Satisfiability ($\equiv$ non-emptyness of the corresponding sets) of the formulae.
- Difficult
- very sensitive to precise formulation
- memory intensive

Hence, can we simplify the prsentations? Our method, *fast simplification* has been integrated with existing implementation of cylindrical algebraic decomposition and quantifier elimination by virtual term substitution. [Hon92, DS97, Bro01, YA05].

Vague specification is that $F \Leftrightarrow F'$ and is "fast" and "simple". Fast is defined by "the proof of the pudding is in the eating". Black box simplification is based on the factor structure, while white box will look inside. Suggests that one should iterate until there is no progress. Blakc box is based on [Bro09] and is guaranteed fast, and will guarantee to detect .

Examples of white box (which is less well-defined:

1. $1 + y^2$ is always positive
2. $x^2 + y^2$ is always nonnegative, and positive if $x \neq 0$
3. $1 - x + y^2[\wedge 2x < -1]$ is always positive

For CAD, our construction never slowed this down, and occasionally gave 100-fold improvements in time and/or size of the utput CAD. For application-derived term substitution ones, might slow small examples down, but sped bigger problems up, often by a factor of 70 or 50. Size of formulae was up to 1000.

## 2.9 Parametric Quantified SAT Solving — Zengler

Example $\exists x \forall y \ldots$. [SS03] embedded propositional logic in first-order logic. Despite theoretical equivalence, current SAT-solvers perform much better than SS-QRE. SAT-solving started with [DavisPutnam1960], which is complete search

over $2^n$ with early cuts, which a restriction to CNF permits. In [MarquesSilvaSakallah1996] the field introduced clause learning.

We introduce PQSAT, whose input is a propositional formula $\phi$ with arbitrary qauntification, and te output is a DNF on the free variables. The idea is DPLL-style top algorithm using QSAT as the black-box decision procedure for the quantified formulae. We transport learned facts from one QSAT instance to another[2]. The algorithm is complete and terminates. Its worst case is $2^{|\phi|}$.

Pratical example from Daimler, where $> 30K$ options. There are customer options and hidden parts. There is a 'product overview formula' (POF).. There are constructibility conditions, and product conditions. Examples:

1. Exactly one engine
2. Exactly on gear box
3. Engine 1 implies gearbox 1
4. Engine 3 and air conditioning 2 implies gear box 2

PQSAT can be used to suggest replacememt to render an unconstructible car constructible. Implemented in Redlog, and is 10–300 times faster than [SS03]. Being fair, this doesn't compete with very specialised systems. *But* we can build this on any QSAT solver, not just Redlog's, so we feel this is still worthwhile.

## 2.10 SCCP implementaion — Kovalov

GAP, KANT, Maple, MuPAD, Macauley2, TRIP, Coq, Magma (wrapper). We have Java and Openmath tools to help with this. Shows an exmaple involving GAP, which asks for a group identification. Thisis done via a "transient CD". Also demonstrates coputing with $M_{24}$, where we have `output=cookie` to avoid transmitting the group itself over the network.

## 2.11 SymGridPar — Chris Brown (St. Andrews

Orchestrate symbolic computation via a coordination server (currently written in Haskell) which sits in the middle, talking SCSCP/OpenMath to servers and clients. We want to write the parallelism skeletons only once, so this is done in Haskell (written as a Haskell function the introduced to the master routine in the coordinator). Note the fact that Haskell doesn't "understand" the mathematical objects being passed around doesn't matter.

**Q.** Any experience of scalability?

**A.** We have run as far as 16 nodes, and one application on 8 nodes was seeing 8.2 speedup?

[2] Valid since these facts are learned by resolution.

## 2.12 Polynomial Homotopy Continuation with PHCPack — Verschelde

PHCPack is open-source code i Ada, with interefaces to C and Python. Lists a lot of related work. Mixed volumes are a necessary tool for much of these. The aim is to solve $f(x) = 0$ by first solving $g(x) = 0$, then moving $t$ form 1 to 0 on $h(x, t) = tg + (1 - t)f$.

## 2.13 ISSAC Business Meeting

**Present:** André Galligo (Chair) and over 110 members.

1. **Election of a new SC member**
   Three people were nominated by the Steering Committee, and spoke briefly.

   - Marc Moreno Maza had been the organiser for ISSAC 2002 in Lille, and other meetings such as PASCO. He said that we should encourage student participation. He would like to see a "best application" award.
   - Lihong Zhi is part of the big group of the Chinese Academy of Science. There is an annual conference in China. She would like to see more symbolic–numeric computation.
   - Moulay Barkatou is part of the French community and is willing to give his time to the organisation of the international community.

2. **Location of ISSAC 2012**

   **University of Kent** Elizabeth Mansfield presented the bid, noting that Kent had recently been joined by Markus Rosenkranz. Canterbury, where the University is situated, in a small medieval town, within walking distance[3] of the town centre. There is student accommodation, but also a great deal of hotels etc. in what is a "tourist mecca". She noted, to a great deal of applause, that the food was getting better and better in England.

   She noted that 2012 was the year of the London Olympics, so proposed moving two weeks earlier, to 14–19 July. She estimated the conference fee as 250UK pounds. She noted the travel connections, notably the Channel Tunnel. Thanks to the fast link, trains to London are down to one hour.

   **Grenoble** Jean-Guillaume Dumas presented the case. Lyon is the nearest serious airport, but Geneva is also close. The proposers are hoping for support from INRIA–Colloques, which should mean they can keep

[3] 15 minutes, but also frequent buses.

the fee at the same level as 2010. The conference would be held on the campus. There is student housing on campus, and hotels, including an IBIS 2* on campus. Grenoble had just been the venue for PASCO 2010, and they were proposing broadly similar arrangements.

There are no real constraints on date — July is free.

3. **Description and Organisation of ISSAC 2010**
   Wolfram Koepf (General Chair) reported on ISSAC 2010. It was noted that in Germany the treasurer had to be local because of sponsorship requirements etc. By ISSAC 2009 we had a complete slate of officers and had a web page. Immediately afterwards we were making provisional hotel reservations etc (necessary for Munich), had plenary and tutorial speakers, *and were able to publicise abstracts online*. The poster was out nine months before. This was probably important in terms of the attendance (188 — a very good number for ISSAC).

   Registration on-line is important, and needs to work. The poster deadline and acceptance was probably too late, but we had to set it there because of late take-up.

   In terms of registration, we had: members 59, nonmembers 48, with student registrations 16+40, and 14 complimentary. Including late registrants, the total is 188. He noted that making the tutorials inclusive was a success, with over 100 in one tutorial. **Future ISSAC**
   There were two parallel strands, which in his view was inevitable in a three-day schedule.

   He noted that "in cooperation with ACM" had been somewhat hollow, though it *had* led to the proceedings being in the ACM Digital Library, which was the most important result. Jeremy Johnson noted, though, that when it came to ACM cooperation "you got what you paid for".

4. **Result of the votes**
   Marc Moreno Maza was elected to the Committee, with 37 (Zhi 36 and Barkatou 30). AG thanked all three for standing. SMW remarked that AG's term was drawing to an end, and the meeting acclaimed his service to ISSAC.

   Grenoble was chosen for ISSAC 2012 (77 versus 35).

5. **ISSAC 2011**
   Eric Schost showed the ISSAC 2011 website, which is again using `www.issac-conference.org/2011`. He asked whether could we all please link to it, since ISAAC 2011 was now beating it in Google. **All**
   ISSAC 2011 will be part of the quadriennial Federated Computing Research Conference: the first time this has happened. He noted that this meant that one could attend other conferences *on the days for which one was registered*. For example STOC's last day is ISSAC's tutorial day.

   Ioannis Emiris reminded people that **we start on the 8th of June 2011**, so the whole schedule was significantly earlier. The abstract deadline was

January 8th, with full papers January 13th. Answers by March 11, and camera-ready copies by march 31st. He noted the tightness of the dates, but said that there was **no room for adjustment**. The appearance at FCRC would be positive for our field.

ES noted that there would be a student poster presentation competition (single-author, and having to be ACM Members) across the majority of FCRC.

It was asked whether there would be, as in previous years, an extension of the submission deadline. IE said that it was his wish that there was no extension. JHD noted that there wasn't time in the schedule for both an extension and a rebuttal period.

IE thought that a rebuttal period was, on balance, positive, but that it would have to be lighter and shorter than 2010.

6. **Budget of ISSAC 2010**
   It was noted that this conference is under the financial management of GI, but 'in cooperation with' ACM. He noted, as had already been praised, the low student fee. Tutorials had cost 1800Euro, so making them free had been worthwhile. Conference[4] fees were 20K, but there was also a DFG grants of 18.5K, which went a long way to make the student fees low. There was a slight positive (contingency) balance.

7. **Reviewing Process and description of the work of the Programme Committee for ISSAC 2010**
   Stephen Watt spoke to this. We had a 2-stage submission process, with an abstract submitted first and the full paper having a later deadline. He felt this worked well, and allowed some flexibility without extending the paper due date. There were 122 abstracts submitted[5], and 112 full papers. 2 papers were combined into one, and one was withdrawn. Each of the 110 was handled by 3 PC members. There were 349 referee reports. Austria was the clear winner in terms of submissions/head of population.

   He had coordinated referee requests in the Programme Committee to avoid duplication, but this turns out not to have been worth the hassle. He would *not* suggest this. Rather it would be simpler to include a paragraph in the letter in the referee request letter with instructions of how to handle multiple requests from different PC members.

   SMW reported that this was the first year with an author response period, and that process seemed to have worked well and helped decide the fate of a number of papers. He noted that the response period afforded authors the ability to point out factual errors in referee reports, and was not intended for extensive discourse on all aspects of papers. The system of

[4] Excluding banquets.

[5] These were used for conflict declarations. He noted that there were 100 conflicts declared, out of approximately 2000 possibilities, so the process is very valuable.

a designated PC member to 'vet' the referee reports and write summaries *had* been valuable. There were three issues he wished formally to raise.

(a) The question of "extended abstracts" has come up. The call for papers had explicitly mentioned 'papers', and the submissions were evaluated as such. SMW noted that the label 'Extended Abstract' had been often used in the theory community, but that was no longer so much the case.

(b) Voting had been a problem, since the number of conflicts varied per paper, and hence the electorate varied. He had weighted the votes on a per-paper basis according to the number of eligible voters (non-conflicted PC members), and recommended that this process (which had, without fanfare, been used in 2009) be standardised. **Future PC**

(c) The 2010 acceptance rate was 41%, which was the historical average for those conferences with more than 80 submissions.

Von zur Gathen wished to raise the 'Extended Abstract' issue. There are papers whose full proofs do not fit into the allotment of 8 pages. What do we do with them? We could reject, or offer more pages, neither of which he thought was feasible. He would like to allow submission of the full paper as well as eight-page version, and the eight-page version in the proceedings **should** be labelled an extended abstract. AG pointed out that we often have additional experiments on websites, or other supporting evidence elsewhere. SAL stated that the eight-page limit was an artefact of paper proceedings, and asked whether we needed these any more. People who had had to defend the quality of ISSAC meetings in promotion committees etc. stated that the inclusion of items labelled as abstracts would make such defence more difficult. It was also pointed out that it was difficult to referee such a paper in the time line allowed for a conference. It was also pointed out that 'best paper' awards had historically been given to extended abstracts[6]. IE stated that we allowed technical reports to be published in parallel, and cited in the paper, so the space issue was already taken care of in practice.

JvzG restated his motion, that it be possible to submit additional material (such as proofs which did not fit into the 8-page limit), and that such papers, if accepted, be labelled as 'Extended Abstract' in the proceedings. The motion was not carried, by over 40 to 12.

8. **Close**
AG announced that the meeting had to close, and those who wished to raise the 'acceptance rate' issue should do so with the Steering Committee (as in the proceedings −AG +MMM). The meeting closed at 19:20, to be followed by the SIGSAM Business Meeting.

[6] JHD's note: 2002 and 2003.

# Chapter 3

# 27 July 2010

## 3.1 Global Optimization of Polynomails Using Generalized Critical Values and Sums of Squares — Zhi

Trying to find

$$f^* = \inf\{f(x) \mid x \in \mathbf{R}^n\}.$$

This problem is NO-hard, but can be approximatex by sum-of-squares relaxation.

$$f^{sos} = \sup\{a \in \mathbf{R} \mid f - a \text{ can be writtten as s sum ofsquares}\}.$$

We also look at $f^*_{grad}$, the infimum of $f$ on the gradient variety. If $f$ attains its minimum on $\mathbf{R}^n$.

- New algebraic certificate
- Use of MatLab's SDP
- Numerical methods.

Schweighofer (SIAM J Opt. 2006).

**Theorem 8** *Let* $f, g_1, \ldots g_m \in \mathbf{R}\mathbf{X}]$. ...

This is used in Schweighofer's *gradient tentacles*. The *critical values* $K_0(f)$ are the values of $f$ on the gradient variety. If $A \in GL_n(\mathbf{Q})$, then $f^A(x) = f(AX)$. Let $W_i^A$ be the set where $X_1 = \ldots = x_i = \frac{\partial f^A}{\partial X_{i+2}} = \ldots = 0$.

Looking at unbounded problems, we should also look at the dual structure. This depends on the choice of monomial basis. We try to take advantage of the sparsity structure. We wish to improve this further. Further work will also explore optimization with constraints.

**Q.—SMW** How heavily does this rely on the fact that you're using a monomial basis, and could you use, say, Chebyshev?

**A.** Good question.

## 3.2 A Slice Algorithms for Corners and Hilbert–Poincaré Series —

Variables $x_1, \ldots, x_n$ with $\mathbf{x} = x_1 cdots x_n$. Note sthe pictorial representation of monomial ideals. Informally, a *corner* is a a place where the staircase bends in every direction. To make this more formal, we need the *Koszul uppersimplicial complex*

$$\Delta_m^I = \left\{ v \subset \{x_1, \ldots, x_n\} \mid \frac{m}{\prod v} = 1 \right\}.$$

Can therefore define a reuced Euler characteristic. The algoeirithm takes a monomial ideal as iput and returns the corners **of full support** and their upper Koszul simplicial complexes.

**Definition 7** *A slice is a 3-tuple $(I, S, q)$ where $I$ and $S$ are monomial ideals and $q$ is a monmial. The context is*

$$con(I, S, q) = \{(mq, \Delta \ldots\}.$$

If $A = (I, S, q)$, $B = (I : p, S : p, qp)$ and $C = (I, S + \langle p \rangle, q)$, then $con(A) = con(B) \cup con(C)$ and this is the key of our divide-and-conquer approach. Note that the union is disjoint. If we call $p$ the 'pivot', then can prove termination is we always choose a valid pivot. The proof is an application (non-trivial) of noetherianity.

Has examples with up to 20 variables and 4000 cgenerators. For generic Hilbert–Poincaré Series problems his is much faster, but for square-free problems[1] [BCRT93] is much better. Of course, this is not the real point. He can do multigraded Hilbert–Poincaré Series, where he is significantly better, but noone else can compute corners as such.

**Q.** Does choice of pivot mattter in terms of performance?

**A.** Indeed. Shoudl choose the pivot with most variables, and most "balanced", but still a heuristic.

## 3.3 Composition collisions and projective polynomials — Ziegler

In $F[x]$ ther eis the composition operator $f = g \circ h$. Look at the inverse problem. $g$ and $h$ are the left and right components of $f$. We can assume all are monic

[1] For which the base case in [BCRT93] is apparently much more powerful.

and have constant coefficient zero. Knowing $f$ and $h$ determines $g$.[BZ85] solves all cases, but exponential. [KL89] solves the tame case ($\mathrm{char}(F) \not| \deg(g)$. We can also wish to count the number of compositions. [vzG90, and elsewhere]

example: $\mathbf{F}_{27}$ when $x^9 + x^6 - x^5 + \cdots$ has four fundamentally different decompositions. We call a $k$-collision if we have $k$ distinct ones with the same $\deg h_i$. Let $r$ be a power of $p$ and $q$ a power of $r$.

$$\mathbf{F}_q[x, r] = \left\{ f = a_m x^{r^m} + a_{m-1} x^{r^{m-1}} + \cdots \right\}$$

is the additive polynomials. If$f$ is such and squarefree. Then there is a bijectio between the right components of $f$ with degree $r$ and the $\sigma_q$ components of .... Let $f^{(a,b)} = x^{r^m} + ax^r + bx$. Abhyankar(1997) produced $\Psi^{(a,b)} = (x^{(r^m-1)/(r-1)} + ax + b$.

**Theorem 9 (Main)** *There are bijections between*

1. *right components of $f^{(a,b)}$ with degree $r$*
2. *roots of $\Psi^{(a,b)} = (x^{(r^m-1)/(r-1)} + ax + b$*
3. *$\sigma_q$-invariant $\mathbf{F}_r$-subspaces of $V_{f^{(a,b)}}$*

Shows various matrix shapes that correspond.

**Theorem 10** *Choose amb $\in \mathbf{F}_q; b \neq 0$, .... Then get a maximal #T-collision*

We conjecture that any square-free maximal $k$-collision $f$ at degree $p^2$ with $k \geq 2$ is a linear transformation of this construction. This has been experimentally verified for $q \leq 9$.

## 3.4 Decomposition of generaic multivariate polynomials — Faugère

**Definition 8** *FDP$(l, m)$ is the problem of taking a system $f$ of homogeneous miltvariate polynomials and output compative $g$ and $h$ with $f = g \circ h$ and $\deg g = l$, $\deg h = m$.*

believing this problem to be hard, [GoubinPatarin1997] proposed a $2R^-$ cryptosystem. But this has been broken. [FP09] considers a particular case, and produces `MultiComPoly`. In this paper we will prove that that computes a 'unique' decomposition, for generic decomposable instances. We need to define a 'normal form' and study th rank of the linear system corresponding to recovey of the left-component when the right-component is known. We also wants to prove that the set of elements for which this holds in a non-empty Zariski-open set.

If $f = g \circ h$ then also $f = (g \circ A^{-1}) \circ (A \circ h$ for any invertibale matrix $h$. So wesay that 'nofmrlaform' is such that $A \circ h$ is in row echelon form. Put another

Table 3.1: cases for Faugère

| | polys | dgree | #variables |
|---|---|---|---|
| $f = g \circ h$ | $t+1$ | $n - lm$ | $r+1$ |
| $g$ | $t+1$ | $l$ | $s+1$ |
| $h$ | $s+1$ | $m$ | $r+1$ |

way, ... `MultiComPoly`(3,2). If we take second derivatives, each $\frac{\partial^2 f_i}{\partial x_j \partial x - k}$ is a linear combination of the $h$s. Last year we said that if the Gröbner basis contains $s+1$ polynomials then we reconstruct the span of the matrix. We now prove that $s+1$ is generic for the cases of $(2,2)$ and $(3,2)$ decompositions.

After various manipulations of partial derivatives, get an explicit matrix ($\operatorname{char} K \neq 2, 3$)

**Theorem 11** *If this example, if* $\operatorname{char}(K) \geq s+5$*, then our decomposition is in fact generic.*

## 3.5 Verfiicaton methods: Rigorous results using floating-point arithmetic — Rump

`www.ti3.tu-hamburg.de` — survey paper. We want to prove results such as

- $\det(A) \neq 0$
- 

There have been various formal proofs via *integer* arithmetic, notably in group theory. Tucker was awarded the 2004 EMS prize for his (floating-point) proof of the xistenc eof the Lorenz attractor. Claims that rigorous proofs can be achieved by *appropriate* us eof interval arithmetic. Example of a spurious solution of the discretized Emden equation. Note that floating-point is now (since IEEE 754) at least properly defined. Note his INTLAB MatLab toolbox (free for academic use from `www.ti3.tu-hamburg.de`).

Verification methods for him are mathematical theorems which can be formulated in a way that aloows computer verfifcation.

**Theorem 12** *Let* $A, R \in \mathbf{R}^{n \times n}$ *with* $||I - RA||_\infty < 1$*. Then* $A$ *is non-singular. This can be verified by computing* $C_1 = (R * A - I)_\nabla$ *and* $C_2(R * A - I)_\Delta$*, then computing (elementwise)* $C = \max(|C_1|, |C_2|)$ *and* $||C||_\infty$*.*

This is seven lines of INTLAB code. [Rump2001] for elementary functions on intervals.

This is always correct, but can be wildly overestimated. Looking for bounds on $\sinh(2x^2/(\sqrt{\cosh(x)}) - x) - \operatorname{atanh}(x)$ over $x \in [0,4]$ gives an overestimate: what should be $[-2, 6 \cdot \ldots]$ becomes $[-2, 10^{13}$. (sin instead of sinh is OK).

Newton iteration does not work well with intervals, but there is a theorem due to Moore (1969). This requires interval matrix operations (see INTLAB). Naïve interval Gaussian elimination, even with pivoting,

**Theorem 13 (Krawchuk)** *Assume* $\exists \hat{x} \in X^{(0)}$ *with* $A\hat{x} = b$*, and we have*

$$X^{(k+1)} := x + R(-Ax) + \{I - RA\}(X^{(k)} - x)$$

*Then* $\hat{x} \in X^{(k)}$ *for all* $k$*.*

[Rump1980] makes this effective, but needs to incorporate a certain amount of $\epsilon$-inflation.

We can verify positive definiteness as well, and this works (based on IEEE–754), up to condition numbers $\approx 10^{15}$, i.e. pretty close to the limit. **Challenge:** do the same for general symmetric matrices.

### 3.5.1 Automatic Differentiation

Note that we regard differentiation as an algebaric operator, as in [Ris69] (Rump's citation).. Note that the computig time for $f$ and $\nabla f$ is at most 5 times that of $f$ **indpendent of** $n$. This extends to intervals, and is in INTLAB.

Consider $\int_0^8 \sin(x + e6x)\mathrm{d}x$. In MatLab we get 0.2511 in 1.77 seconds.For his system, relying on bounds for the fourth derivative of the integrand, at $n = 2^{14}$ gets $[0.14, 0.55]$, with $n = 2^{16}$ get $[0.346, 0.349]$ (in less than 1 second) and so the MatLab result has no significant figures.

A major problem is that "multiple root" is ill-posed. However, [Rump2009] formalises a computable Cauchy bound, which can say "there are exactly $k$ roots, counting possible multiplicities, in a disc $D$".

Can also produce results of the form that there are *true* solutions of a two-point boundary problem (and not merely of the discretised version). Similarly semi-linear elliptic boundary value problems. $\Delta u + u^2 = s\sin(\pi x_1)\sin(\pi x_2)$ has been conjectured to have four essentially different solutions for large $s$. This has now been verified.

## 3.6 Algorithmic and Experimental methods in Algebra, Geometry and Number Theory — DFG Priority Programme (Decker)

Decker is the Chair of the Programme (SPP 1489). The distinguishing feature of such a prgoramme is the national collaboration. As a rule one gets six years of funding (two three-year tranches). He will talk about the first tranche. 10Meuro for the next six years. Plenty of money for schools and workshops, also travel.

**No.v 2008** Proposal submitted.

**Spring 2009** Programme establlished.

**Nov 2009** Proposal submitted.

**Feb 2010** Panel Meeting

**July 2010** Funding started.

**Aug 2010** Summer school (Berlin)

**Feb. 2011** First Annual Conference (Aachen)

"To combine the diffent methods where needed, and to apply them to central questions in theory and praxis". Several key problem areas.

**Automorphic Forms** Langlands conjecture etc.

**Rational Points on Curves**

**...**

**Classificiations and electronic Tabies in Group Theory** Libraries, generic character tables etc.

**Computer algebra methods in Lie Theory** Complex reflection groups, cyclotomic Hecke algebras, quantum groups, representations of groups of Lie type

**Cohomolgy of Groups** High degree cohomology, cohomology rings, classification os $p$-groups by coclass.

**Families of Varieties** Deformation theory, stiudy of modular spaces, monodromy.

**Desingularization** Further improvements in characteristic 0,

**Toric and Tropical Geometry** Mirrow Symmetry, Cox rings, tropical intersection tehory,tropical mirror construction.

**System and Control Theory**

**Codes**

**Certified Solving via Hybrid Methods**

**Algebraic Methods in Cryptology**

**Pairings** Weil, Tate etc.

"Also of interest are interactions with applicatons areas outside, such as cryptography, CAD etc.". "Moreover the programme is meant to support the further development of free computer algebra systems with development centers in Germany, and which, in the framework of different projects, may require cross-lining".

here are many possible linkings.

1. Exploiting torus actions in algebraic geometry.

15 Triangulations and other decompositions ...

### 3.6.1 Schools

$SS^2AM$ August 16–20 Berlin. Invited speakers: Jan Christophersen, Gerhard Frey, Graham Ellis. Organised by *young* researchers who choose the the invited speakers, and next year's committee.

## 3.7 Computing the Singularities of Rational Space Curves

A singularity is a point where the tangent is not well-defined. The interesection multiplicity of a generic line and the curve at $Q$ is the order of $Q$. For an ordinary singular point, the tangents are all distinct. For a non-ordinary singular point, we have singularities arsing from perturbations — infinitely near singular points.

A moving line is $L(s,u)$, which is said to follow a rational curve $P(s,u)$ if $L \cdot P = 0$. $p$ and $q$ are said to form a $\mu$-basis for the curve $P$ if $p$ and $q$ form a bais for the Gröbner basis of such moving lines. Similar with moving planes in 3D. If we know a $\mu$-basis for a rational plane curve then the inversion formula of $Q$ on the curve is given in terms of the basis. $\mu$-bases are computed in terms of the Smith form of the resultants of three (if space) polynomials.

**Q.** Did you comapre with other methods.

**A.** We do better than the resultant method, sinc ethe degree is smaller.

**Q.** Is thre a way of checking the results (in case you were unlucky)?

**A.** ...

## 3.8 Solving Schubert problems with Littlewood–Richardson Homotopies — Verschelde

A Schubert variety is defined by an $n$-dimensioanl falg $F$ and a $k$-dimensional bracket $\omega$.

**Q.** Where do you use the Schubert calculus?

**A.** With the poster calculations.

## 3.9 Triangular Decomposition of semi-algebraic systems — Chen

Consider solutions of $ax^2 + bx + c$, which required $a \neq 0$ and $b^2 - 4ac > 0$ for tehe general solution, but has other components. [BM05]: when does $z^3 + az + b$ have a non-real root $x + iy$ with $xy < 1$. `LazyRealTriangularize` gives the mail component ($h_1 \neq 0, h_2 \neq 0$), and two deferred calls, one of hwich is in fatc empty, andthe other one splits again.

**Proposition 1** *Let $T = \{t_1, \ldots, t_s\}$ be a regular chain of $k[x]$. Then the saturated ideal* $\mathrm{sat}(T) := \langle T \rangle : \prod$ *initials is regaular.*

Some square-free reaular chains may specialise badly: it specialises well iff the *border polynomial* is non-zero.

**Definition 9** *$R := [Q, T, P_>]$ is a* regular semi-algebraic system *is*

1. *$Q$ defined a non-empty open semi-algebraic set $S$;*
2. *The regular system $[T, P]$ specialises well at every point of $S$*
3. 

**Theorem 14 (Full decomposition)** *Every semi-algebraic system $S$ can be decomposed as a finite union of regular semi-algebraic systems such that the union of their zero sets is the zero set of $S$.*

**Theorem 15 (Lazy decomposition)** *A* lazy decomposition *gives a family $R_i$ of regular semi-algebraic systems whose zero sets have dimension $c$ such that*

1. *For each $i$, $Z_{\mathbf{R}}(R_i) \subset Z_{\mathbf{R}}(S)$ holds and*
2. *The difference $Z_{\mathbf{R}}(S) \setminus \bigcup Z_{\mathbf{R}}(R_i)$ has dimension less than $c$.*

This has a singly-exponential complexity. There is a QE procedure required to produce $Q$, but this is a very special problem.

**Definition 10** *We call $D$ a fingerprint polynomial set if*

1. *$\forall \alpha \in \mathbf{R}^d$, $b \in B$, id $dp((\alpha) \neq 0$, then $b(\alpha) \neq 0$*
2. *$\forall \alpha, \beta$*

**Q.** How doe sthis comparew ith discriminant variety?

**A.** The Border polynomial is a related topic, but in fact contains more information.

**Q.** About the nechmarks, were the coefficients polynomials?

**A.** The coefficients were integers, but the conversion from graded to lexicographic accounted for a large part of the cost.

# Chapter 4

# 28 July 2010

## 4.1 Real and complex root finding — Pan

[Pan1995] divide-and-conquer algorithm is optimal up to a polylog factor, but has not been implemented. The algorithms in many packages do well in practice, despite the absence of theoretical support. The constants are also low. We look at the Frobenius companion matrix $F_c$, and the generalised companion, which is "diagonal plus rank 1" (DPRI). MatLab applies the QR matrix to $F_c$, but ignores the special structure. Note that DPRI has fast operations such as matvec.

[Binietal2004], which only works with all real roots, did take advantage of this structure. An alternative is to apply the "Rayliegh quotient" (inverse QR). This has $O(n)$ memeory and $O(n)$ time bper step, and, empirically $O(1)$ steps per eigenvalue.

Input: a matrix $A$, a tolerance $t > 0$ and $\lambda$ a simple isolated eigenvalue. Fix $y$, compute $v := (A - \lambda I)^{-1}y$, then $y := v/||v||$..

We generate vectors $u_i$ and $v_i^T$ $(1 \leq i \leq m)$, and hence matrices $U$ and $V$ with these columns. Consider now $C - A - \mu I + UV^T$, where $\mu$, or the custer near $mu$, has multiplicity $m$. Claims $2n + 2$ operations per iteration, rather than previous $4n$ or $5n$.

The case of looking for real roots is even more efficient. Assume there are $r$ real roots. Transform $A$ to $A^{(0)} = 1 + 2i(A - iI)^{-1}$, where the real eigenvalues have gone to the unit circle.

## 4.2 Computing the radius of positive semi-definiteness of a multivariate real polynomial — Hutton

Example: $0.33x^2 - 0.66x + 0.33 \geq 0$.

**Theorem 16 (Stetter)** *Goven a root $\alpha$ the distance is $\frac{f(\alpha)^2}{||\tau||_2^2}$.*

Example: $x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2 + 1 \geq 1$, where the polynomial is always positive but it not a sum of squares.

We have a new proof via Lagrange multipliers, and "sums of squares" certificates. Need a weighted two-norm, where $w_i \to \infty$ fixed the $u$th corfficients, and $w_i = 0$ is "don't care". With such weighted norms, can have an equivalent of Holder's inequality, and mimic Stetter's proof.

Baisc methodology is to take the $W$ matrix from the sum-of-squares solver, 'adjust' it (in particular convert to rationals by continued fractions), then do Newton iteration.

Had $f_1 = x^4 + y^4 + 1$, $f_2 = x^2 + x^2y^2 - 2xy + 1$. Take the Gröbner basis of the numeators of the partical derivatives, ..., but to 20 digits get the wrong answer (which doesn't certfy!). Needed 25 digits to get a correct value.

## 4.3 Random Polynomials and Expected Complexity of Bisection Methods for Real Solving — Tsigaridas

Computethe real roots of a polynomial of degree $d$ $H(f) = \max \log |coeff|$. We need a seprataion bound, $\Delta = \text{sep}(f) = \min_{i \neq j} |\gamma_i - \gamma_j| = 2^{-s}$. So for the Wilkinson polynomial, we compute $\Delta \approx 10^{-344}$, but the true answer is 1. Note that 'hard' examples, be they Wilkinson or Chebyshev, have $n$ real roots for a polynomial of dgeree $n$, whereas a "random" polynomial has only 4 real roots. His definition of 'random' is that the coefficients are independent $N(0, C_i^d)$. [EdelemanKostlan1985]. Physicists transform the roots to be on a unit circle, and then look at the "two-point correlation". Have two cases

- $\Delta \leq 1/(d^c\tau)$
- $\Delta \leq 1/(d^c\tau)$

Another example is characteristic polynomials of matrices with random entries, were the $i$th coefficient is $N(0, 1/i!)$. For these the expected complexity of Sturm is $O(rd^2\tau)$. Note that for random polynomials the expected number of real roots (in the monomial basis) is $\frac{2}{\pi}\log(d) + o(1)$ (apparently Erdős).

**Theorem 17** *The expected number of real roots of a polynomial in the Bernstein basis is $O(\sqrt{d})$ (their formula is more precise.*

This work has all been about Sturm: what about Descartes? Equally, what about symmetric or sparse polynomials?

**Q.** For polybomial systems, do you have an idea of the mean value?

**A.** If we make the coefficients $N(0, \sqrt{\binom{d}{i_1, \ldots, i_m}})$, then the expected number of real roots is $\sqrt{d_1 \ldots d_m}$ [JHD doesn't understand the notation]

## 4.4 The DMM Bound — Tsigaridas

We are interested in a polynomial system and its (complex) roots, How close are the roots to zero and/or each other. These are important questions for exact geometric computations, and interesting in their own right. Unfortunately, while the bounds are exponential, they are optimal [Mig81].

The concept of "aggregation" is to consider *all* the distances, rather than just the least. For univariates, we get [Dav85] $2^{-O(d^2+dt)}$. In the multivariate ($n$ variables) [Can87, BY09] says that two roots are equal or at least a certain distance apart. Bu this is not optimal when $n = 1$. For the time being we assume that the sytsem is 0-dimensional. To reduce to one variable we add a $u$-polynomial and eliminate the $x_i$ to get $U(u)$. This can all be bounded, so we can talk about the bounds for $u$. Then $|u_i - u_j|^2$ is $|\sum r_k\gamma_{i,k} - \sum r_k\gamma_{j,k}|^2$. In general, $\Delta > 2^{-O(\dots)}$.

What is the coplexity of subdivision, given a "more than one root" oracle[1]? Look at 2D Consider the sub-division tree, the heigt of the tree for $\gamma$ is $-\lceil -log - 2\Delta_\gamma \rceil$. Summing this over all roots gives $O(d^5\tau)$, but arrgeration gives us $O(d^4 + d^3\tau)$. In general, they get within a logarithmic factor of [Dav85].

What we really want is a separating bound for the isolated roots of not-necessarily-0-dimensional systems. This can be used to give lower bounds on positive polynomials.

We know these bounds are optimal for 1 variable, provably so for 2, but probably not in general. What about average case bounds (see the previous talk for the 1-variable case).

## 4.5 Algebraic Invariants and Their Differential Algebra — Hubert

Differential invariants arise in equivalence problems (applications in computer graphics form the 1990s) and for symmetry reduction. This is used in differential elimination [Man01], classification[LR98] and in biological systems.

### 4.5.1 Local and Algebraic Invariants

One-dimensional Lie group actions on the plane: scaling, translation and rotation $SO(2)$. Given such an action, we can also look at the infinitesimal generators, so for scaling by $\lambda^2, \lambda$, we have $2x\mathrm{d}x + y\mathrm{d}y$, etc. The corresponding invariants would be $\frac{y^2}{x}$ etc. If $G$ is an $r$-dimensional Lie group, I will have a basis $V_1, \dots, V_r$ of infinitesimal generators. Restrict to $M \subset \mathbf{R}^n$ where all orbits have the same dimensions. Then the orbit of $z$ is $O_z = \{\lambda * z \mid \lambda \in G\}$. $f$ will be a local invariant on $U \subset M$ if $V_i f = 0 \forall i$..

Let $p$ be an embedded maniforld of dimension $n - d$, then $P$ interesects $O_z$ at a unique point for each $z$. $P$ is transverse of $O_z$ at $z \in P \Leftrightarrow V(P) = (V_i(p_j))$

[1] e.g. Milne's algorithm.

has rank $d$. We introduce normalized invariants $\bar{\imath}z_i, \ldots, \bar{\imath}z_n$ and then $f$ is a local invariant means that $f(z_1, \ldots, z_n) = f(\bar{\imath}z)_1, \ldots, \bar{\imath}z_n)$. Alternatively $f(x, y)$ is invariant imples that $f(x, y) = f(\bar{\imath}x, 0)$.

In the algebraic case, the normalized invariants form a $\overline{K(z)}^G$-zero of the graph-section ideal

$$(G + (Z - \lambda * z) + P) \cap K(z)[Z]$$

The coefficients of the reduced Gröbner basis of the graph-section ideal formal a generating set for the $K(z)^G$ endowed witha simple rewriting algorithm. [Kemper2007,MullerQuadeBeth1999]. We actauly don't need the explicit normalzed invariants, but work formally with them subject to $p_i(\bar{\imath}z) = 0$ $(1 \leq i \leq d)$.

### 4.5.2 Invariant Derivations

Classical invariant is the curvature $\sigma = \sqrt{\frac{y_{xx}^2}{(1+y_x^2)^3}}$. This is a local invariant in the sense defined before, for an extended action. The invariant derivation is $\frac{\mathrm{d}}{\mathrm{d}s} = \frac{1}{\sqrt{1+y_x^2}} \frac{\mathrm{d}}{\mathrm{d}x}$.

$f : J^k \to \mathbf{R}$ is a differential invariant of oder $k$ if $K^k(f) = 0$. An *inavriant derivation* is one which commutes with the invariant generators: $D \circ V = V \circ D$. Then if $f$ is a differnetial invariant of order $k$, $Df$ wil be one of order $k+1$. The dimension of orbits on $J^k$, $r_k$, stabilizes. Say $r_s = r_{s+1} = \cdots$. Then $V_1^s, \ldots, V_r^s$ has rank $r$.

$$D_i(\bar{\imath}f) = \bar{\imath}(D_i(f)) - K_{ia}\bar{\imath}(V - a)f)).$$

Any differential invariant can be constructively written in terms of

- the normalized invariants of order $s + 1$:

$$I^{s+1} = \{\bar{\imath}x_1, \ldots, \bar{\imath}x_m\} \cup \{\bar{\imath}u_a lpha\}$$

- the edge invariants, when the cross-section is of minimal order
- the Maurer-Cartan invariants $\mathcal{K} = \{K_{ia}\} \cup I^0$ and their derivatives w.r.t. $D_1, \ldots, D_m$. $\mathcal{K}$ is relatively small $(n + m(r + 1))$.

What are the syzygies for the normalized invariants? It turns out that the 'obvious' set of relationsips is in fact complete. On the Maurer-Cartan invariants, we have formulae $D_i(K_{jc}) - D_j(K_{ic}) =$ explicit right-hand side, but non-zero, i.e. non-commuting derivations.

### 4.5.3 Generalized Differential Algebra

The normla setting of differential algebra is commuting derivations. Write $\delta_i\delta_j - \delta_j\delta_i = \sum c_{ijl}\delta_l$. We need essentailly a Jacobi-identity on the $c_{ijl}$. We also need an admissible ranking. [Hubert2005]. We can work with this effectively, e.g. generalized orthogonal groups.

### 4.5.4 Moving Frames

Return to the geometric setting. We are tring to ascertain an orthogonal frame at each point of the curve we are moving along. This can be seen as Serret–Frenet equations. [MansfieldvanderKamp2006]. In terms of Maurer-Cartan forms, we can look at their duals $\omega = (\omega_1, \ldots, \omega_r)$. Then we have an equivariant $\rho : J^k \to G$ with $\rho(\lambda * z) = \rho(z) \cdot \lambda^{-1}$.

$$(D_1, \ldots, D_m)^T = (\rho^* A)^{-1} D$$

where $A = (D_i(g^* x_j))$. Then $\mu = \rho^* omega$ satisfy $\mathrm{d}\mu_k = -\sum_{1 \le i < j \le r} C_{ijk} \mu_i \wedge \mu_j$.

**Theorem 18** *$\rho^* \omega = -K^T \tau$ modulo contact.*

**Q.** How do differential invariants arise in the classification problem?

**A.** [Long debate]

## 4.6 Liouvillian Solution — van Hoeij

Currently we consider irreducible second-order ODEs. Let $\tau : n \mapsto n + 1$. We consider $T \in \mathbf{C}(n)[\tau]$.

**Definition 11** *Let $S = \mathbf{C}^{\mathbf{N}}/\ $ where $\ $ means "eventually coincide".*

$V(L) = \{u \in S \mid Lu = 0\}$. If $a + 0 \neq 0$, $a_k \neq 0$, then $\dim(V(L)) = k$ ($A = B$ Theorem 8.2.1).

**Definition 12** *$L - 1$ is* gauge equivalent *to $L_2$ if $D/DL_1$ and $D/DL_2$ are isomorphic as $D$-modules.*

**Definition 13** *$r_1$ and $r_2$ are shift-equivalent, $r_1 \overset{\mathrm{SE}}{=} r_2$ iff $\tau - r_1/r_2$ has a trational solution or the diffence modules ofr $\tau - r_1$ and $\tau - r_2$ are isomorphic.*

Liouvillian solutions are as in [HS99].

**Theorem 19 (***op. cit.* **Lemma 4.1)** *An irreducible $k$th order operator $L$ has a Liouvillian solution iff $L$ is gauge equivalent to $\tau^k + \alpha$ with $\alpha \in \mathbf{C}(n)$.*

**Definition 14** *$L_1, l_2 \in C(N)[\tau]$. The symmetric product is the smallest operator such that, if $L_i u_i = 0$, then $L(u_1 u_2) = 0$. Denoted $L_1 \otimes L_2$. Hence symmetric square: $L^{\otimes^2}$.*

Consider $L$ of order 2. Assume $\deg L^{\otimes^2} = 3$ (the case of 2 is trivial). Then the algorithm basically follows form the commutative diagram.

## 4.7

We say that $L_2$ is a term product of $L_1$ when $V(L_2)$ is ...

Many special functions satisfy known recurrences relatiosn with respect to their parameters. Let $L_{\nu,z}$ be the Bessel operator. Can we find $L \sim_{gt} L_{\nu,z}$? If so, $L$ is soluble in terms on Bessel functions. So we compare the local data of $L$ with $L_{\nu,z}$, using only data that are equivalent under $\sim_{gt}$. Finite singularities and order of growth are two candidates. Claims that $Max_p - Min_p$ is $\sim_{gt}$-invariant for all $p \in \mathbf{C} \setminus \mathbf{Z}$. There is no valuation growth data for Bessel J/Y, but two for Whittaker-M (except for a special case when the two coincide), and also for ${}_2F_1$.

When it comes to singularities at infinity, there is a concept of generalized exponent, and a generalized quotient of such exponents. This Gquo data *does* exist for Bessel's J: $\frac{1}{4}t^2z^2(1-(1+2\nu)t)$. This will limit the choice of $\nu$ and $z$. Using OEIS, there were 10659 sequences with a second-order recurrence, but 9455 are reducible. 161 are irreducible Liouvillian, 86 Bessel, 330 Legendre, 374 Hermite, 21 Jacobi, etc. `A143414` has Gquo data $-\frac{1}{16}t^2(1-2t)$, which is Bessel-compatible, with four candidates, and indeed our sequence is spanned by

$$(-1)^x\left((2x-1)I(\frac{1}{2}+x,\frac{1}{2})-I(-\frac{1}{2}+x,\frac{1}{2})\right)$$

and

$$(-1)^x\left((2x-1)K(\frac{1}{2}+x,\frac{1}{2})-K(-\frac{1}{2}+x,\frac{1}{2})\right).$$

## 4.8 On some decidable and undecidable problems related to $q$-difference equations with parameters — Abramov

**Theorem 20 ([Bou99] quotes J.-A. Weil)** *Let $L$ have the form*

$$r_p(x,t_1,\ldots,t_m)D^p+\cdots+r_o(x,t_1,\ldots,t_m).$$

*Are there values of the $t_i$ such that there are (liouvilian? rational?) solutions? Insoluble.*

Generalised to difference equations by Abramov. Based on David–Matiyasevich–Putman–Robinson theorem, which states that it is undecidable whether a polynonial with integer coefficients has an integer solutions. What about the $q$-difference analogue? We will show that this case is more interesting.

1. There is an algorithm which recognizes the existence of numerical (real, complex) values of the parameters for which a given linear $q$-difference equation has a solution in terms of rational functions.

2.

In the differential and difference case there is no bound (independent of the parameters) on the degrees of polynomial solutions: e.g. $xy' - ty = 0$ has solution $y = x^t$. This is not the case in the $q$-dfference case.

**Proposition 2** *Let $L$ be such a $q$-dfference equation and $w_q = \max i = 0^p \deg_q(r_i)$. Then $\deg_x(f) \leq \max(\ldots, w)$ for any solution $f$. Therefore the problem is soluble over* $\mathbf{C}$ *(Gröbner etc.), or* $\mathbf{R}$ *(Tarski–Collins).*

What of $\mathbf{Q}$? This is reducible by Abromov to the $\mathbf{Q}$-analogue of the David–Matiyasevich–Putman–Robinson theorem, and therefore is *probably* undecidable. The key results are clearly [Den78]

# Bibliography


[BCRT93] A. Bigatti, P. Conti, L. Robbiano, and C. Traverso. A Divide and Conquer Algorithm for Hilbert-PoincaréSeries, Multiplicity and Dimension of Monomial Ideals. In G. Cohen, T. Mora, and O. Moreno, editors, *Proceedings AAECC-10*, pages 76–88, 1993.

[BM05] C.W. Brown and S. McCallum. On using bi-equational constraints in CAD construction. In *Proceedings ISSAC 2005*, pages 76–83, 2005.

[Bou99] D. Boucher. About the Polynomial Solutions of Homogeneous Linear Differential Equations Depending on Parameters. In S. Dooley, editor, *Proceedings ISSAC '99*, pages 261–268, 1999.

[Bro01] C.W. Brown. Simple CAD construction and its applications. *J. Symbolic Comp.*, 31:521–547, 2001.

[Bro09] D. Brown. Primitive Integral Solutions to $x^2 + y^3 = z^10$. `http://arxiv.org/abs/0911.2932`, 2009.

[BY09] W.D. Brownawell and C.K. Yap. Lower bounds for zero-dimensional projections. In *Proceedings ISSAC 2009*, pages 79–86, 2009.

[BZ85] D.R. Barton and R. Zippel. Polynomial Decomposition Algorithms. *J. Symbolic Comp.*, 1:159–168, 1985.

[Can87] J.F. Canny. The Complexity of Robot Motion Planning. *ACM Doctoral Dissertation award*, 1987.

[Col75] G.E. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. In *Proceedings 2nd. GI Conference Automata Theory & Formal Languages*, pages 134–183, 1975.

[Dav85] J.H. Davenport. Computer Algebra for Cylindrical Algebraic Decomposition. *TRITA-NA-8511*, 1985.

[Den78] J. Denef. The diophantine problem for polynomial rings and fields of rational functions. *Trans. A.M.S.*, 242:391–399, 1978.

[DS97] A. Dolzmann and Th. Sturm. Simplification of Quantifier-free formulae over Ordered Fields. *J Symbolic Comp.*, 24:209–231, 1997.

[FP09] J.-C. Faugère and L. Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *J. Symbolic Comp.*, 44:1676–1689, 2009.

[GM86] R. Gebauer and H.M. Möller. Buchberger's Algorithm & Staggered Linear Bases. In *Proceedings SYMSAC 86*, pages 218–221, 1986.

[Hon92] H. Hong. Simple Solution Formula Construction in Cylindrical Algebraic Decomposition Based Quantifier Elimination. In P.S. Wang, editor, *Proceedings ISSAC 1992*, pages 177–188, 1992.

[HS99] P.A. Hendriks and M.F. Singer. Solving difference equations in finite terms. *J. Symbolic Comp.*, 27:239–259, 1999.

[KL89] D. Kozen and S. Landau. Polynomial Decomposition Algorithms. *J. Symbolic Comp.*, 7:445–456, 1989.

[LR98] I.G. Lisle and G.J. Reid. Geometry and Structure of Lie Pseudogroups from Infinitesimal Defining Systems. *J. Symbolic Comp.*, 26:355–379, 1998.

[Man01] E.L. Mansfield. Algorithms for symmetric differential systems. *Found. Comput. Math.*, 1:335–383, 2001.

[Mig81] M. Mignotte. Some Inequalities About Univariate Polynomials. In *Proceedings SYMSAC 81*, pages 195–199, 1981.

[MM82] E. Mayr and A. Mayer. The Complexity of the Word Problem for Commutative Semi-groups and Polynomial Ideals. *Adv. in Math.*, 46:305–329, 1982.

[MMT92] H. Möller, T. Mora, and C. Traverso. Gröbner bases computation using syzygies. In *Proceedings ISSAC '92*, pages 320–328, 1992.

[Ris69] R.H. Risch. The Problem of Integration in Finite Terms. *Trans. A.M.S.*, 139:167–189, 1969.

[SS02] A. Suzuki and Y. Sato. An Alternative Approach to Comprehensive Gröbner Bases. In T. Mora, editor, *Proceedings ISSAC 2002*, pages 255–261, 2002.

[SS03] A. Seidl and T. Sturm. Boolean quantification in a first-order context. *Computer Algebra in Scientific Computing (CASC '03)*, pages 329–345, 2003.

[Tar51] A. Tarski. A Decision Method for Elementary Algebra and Geometry, 2nd ed. *Univ. Cal. Press*, 1951.

[vzG90] J. von zur Gathen. Functional Decomposition of Polynomials: the Tame Case. *J. Symbolic Comp.*, 9:281–299, 1990.

[Wei92] V. Weispfenning. Comprehensive Gröbner Bases. *J. Symbolic Comp.*, 14:1–29, 1992.

[YA05] H. Yanami and H. Anai. SyNRAC: A Maple Toolbox for Solving Real Algebraic Constraints. In *Proceedings A3L*, pages 275–280, 2005.

## .1 Dramatis Personae

**HS** Hans Schönemann — Universität Kaiserslautern (SINGULAR)

**CT** Carlo Traverso — Università di Pisa

**SMW** Stephen Watt — University of Western Ontario