ISSAC 2014

J.H. Davenport — J.H.Davenport@bath.ac.uk

21–25 July 2014

Contents

Chapter 1

Maple Tutorials 21 July 2014

1.1 Control Theory

(Presented in Japanese.)

Examples Inverted pendulum, child on Segway, rocket. The rocket has a reference attitude, an attitude sensor, the difference of which feed into the computer, hence a (hydraulic) actuator, and the the direction of the rocket nozzle. Same principle in air conditioning, and much else: the key is the *feedback*. conditioners. History from Ctesibius water clock (3rd C BC), Watt's Governor (1776), Maxwell's stability analysis (by coefficients of characteristic polynomial; 1868), Routh's Theorem (1877), up to 1960's Kalman.

Major application: autonomous ships for Kawasaki heavy Industry. This uses automatic code generation: code for the simulation is generate by Maple from the state equation and the performance index required. This C code is merged with control and libraries, and run to generate the data for Maple to lot.

Also discrete-time optimal control: $x_{k+1} = f(x_k, u_k)$. We can also handle implicit specification of the feedback which leads to recursive elimination of unknowns, via elimination ideals.

1.2 Model-free Adaptive Control using a Stochastic Approach

(Presented in Japanese.) Shinichi Ishizuka (Cybernet Systems Co.).

Watt's controller was designed by trial and error. Maxwell, Proc. Roy. Soc. 1867. Couldn't prove the general case — Routh solved it. Later Stodola

and Hurwitz.: his stability criterion was 1895. The inverted pendulum is a simplified example of the rocket control.

1.3 Advanced Mathematical Computations in Maple and Applications: JG

Limits of bivariate functions e.g. $\lim_{(x,y)\to(0,0)} \frac{xy}{x^2+y^2}$ (consider $= y$ and $x = -y$). See ArXiV 1011.1591. Similarly $\lim_{(x,y)\to(0,0)} \frac{x^2y}{x^4+y^2}$ were we can see that the limit does exist. Note that we always need an isolated singularity. Solved by considering a circle of radius r around the singularity and letting $r \to 0$.

Parametric polynomial systems Joint work with Paris VI and UWO. Then we ask "feasibility" (for which parameters are their solutions) or answers. Example $x^2 + ax + b$, which requires $a^2 - 4b \geq 0$. Many methods, e.g. RealRootIsolation. Common problem in Control Theory. Hurwitz: stable if no poles have positive real part.

Differential-algebraic equations

Chapter 2

22 July 2014

2.1 Symbolic–Numeric Algorithms for Computing Validated Results — Zhi

Lihong Zhi on joint work with many others, including Kaltofen and Safey El Din. JHD has paper copy of slides.

Quotes Wikipedia definition of Symbolic-Numeric.

- Certification using Sums of Squares
- Verification of Solutions of Polynomial Systems

2.1.1 Certification using Sums of Squares

Consider $f(x_1, x_2) = \cdots = \frac{1}{2}A^2 + 2B^2$ and so is positive. Can express with matrices. Note [Artin1927]: a polynomial is non-negative iff ratio of sum of squares, over $\mathbf{Q}$ if we started there. [Motzkin1967] — (3 arithmetic means − 3 geometric means)(x^4y^2, x^2y^4, z^6) is positive semi-definite but not a sum of squares.

Various software systems produce SoS formats, but numerically, so in fact only approximate. We certify a rational r such that $f(\mathbf{x})-t = m_d(\mathbf{x})^T \cdot W \cdot m_d(\mathbf{x})$ exactly. See [Rump2006] Model problem: solved $n \leq 8$ by Gröbner bases (Safey El Din) also COSY by .... Rump has $n \leq 12$.

[KLYZ08]: exact W has corank 1 when n even, 2 when n odd. We certify a slightly perturbed lower bound with a full rank W.

Also Voronoi2 [ELLP07]. Example has 253 monomials. We have various singular values of the Gram matrix, e.g. 43.06, which is the seventh largest. We do a truncated Cholesky decomposition with tolerance 43 and get a sum of seven squares.

SDP solvers based on interior point methods return matrices with maximal rank. [**?**] wants to find the matrix of **lowest** rank. Shows examples with ranks 14–17 versus traditional 200-300. This is very relevant when $m_d(\mathbf{x})$ is sparse.

Try to find non-zero $u_1, \ldots, u_s$ such that gives a certificate for the low dimensionality of $\ker W$.

For infeasibility certificates (there is not a quotient representation with degree of denominator bounded by $2e$), see [GKZ12]. Apply to even symmetric sextics [Choietal1987], and have first published lower bounds on degree. See also the ill-posed problem in [GKZ12].

Question 1 (Sturmfels) *Given a SoS over* $\mathbf{R}$*, can we find one over* $\mathbf{Q}$*? Also what is relationship between number of summands*

[Sch12] has a counterexample. Has one in $\mathbf{Q}(\alpha)$ where $\alpha < 0, -1 - 8\alpha + 8\alpha^3 = 0$ The Gram matrix is 6×6 symmetric. [Guoetal2013a] has an algorithm $O(D^{O(D^2)}$ to decide rationality. The certificates for SoS over $\mathbf{Q}$ are $O(M(d,n)^{M(d,n)^6})$ [SafeyElDinZhi2010a]. [GuoSafeyElDinZhi2013a] finds rational linear forms.

Key tool is the *polar variety* [Banketal,many].

[Sch06] can produce SoS certificates, assuming that the set of asymptotic values of f is finite.

2.1.2 Verified Error Bounds for Real Solutions

Question 2 ([Rump]) *Let* $F(c) = [f_1, \ldots, f_m]^T \in \mathbf{Q})\mathbf{x})$ *be an algebraic variety. We verify the existence of solutions in* $\mathbf{R}^m$*. For simplicity, assume* F *is radical.*

Assume $\mathbf{M} \in \mathbf{IR}_{n \times n}$ is an interval matrix .... If

$$-AF(\mathbf{x})_(I_n - A\mathbf{M})X \subseteq \text{int}(X)$$

then there is a unique $\hat{\mathbf{x}} \in \mathbf{x} + X$ satisfying $F(\hat{\mathbf{x}}) = 0$ and every $\overline{M} \in \mathbf{M}$ is nonsingular.

[GraillatRump2009] can certify double roots, but have

Example 1 ([GraillatRump]) $F = \{x_1^2 x_2 - x_1 x_2^2, x_1 - x_2^2\}$ *has (0,0) of multiplicity 4.*

[MantaflarisMourrain2011] can certify a multiple root *of given structure*. [LiZhi2013,2014] can do this without specifying the shape. Use deflation techniques, such that $(x, \hat{\lambda})$ is a unique solution of the deflated system. [Leykinetal2006] the number of deflations is strictly less than the multiplicity. The problem is that the deflated system is $(n+1) \times n$ over-determined.

[LiZhi2013] Assume the corank is 1, let μ be the multiplicity and $b_0, \ldots, b_{\mu-2}$ be *smoothing parameters*. Then construct a square regular system in $n\mu$ variables. Can solve Example 1. [DZ05] have a system with a 131-fold isolated zero.. INTLAB's verifynlss has a verified solution of width 10^{-32-1}.

Low-rank Moment Matrix Completion Method

(see previous subsection as well). Suppose there is a measure μ such that $y_\alpha = \int x^\alpha d\mu$, then y is called a truncated moment sequence. This seems to be replacing each monomial by a new variable. [YangZhiZhu2014a] applies their [MaZhi2012] MMCRSolver to finding an approximate solution $\mathbf{x}$ to ??. Has a table of results on dense random hypersurfaces. Done with her method, outpacing Safey El Din's RAGLib. Also positive dimensional radical ideals.

Existence of Real solutions of Semi-Algebraic systems

Again introduce a localised moment matrix.

Example 2 (Kissing Number Kissingnk) *Maximal number k of (or can we fit) unit spheres round a sphere in n dimensions. Kissing25 (possible) has 10 variables, and found. Kissing26 (limiting case) can only verify a nearby (perturbed) solution, and Safey El Din's RAGLib runs out of memory.*

All software is downloadable from her website. SIAM Applied Algebraic Geometry will be August 3–7 2015 in Daejeon South Korea, after third Hybrid SNC in Beijing.

Q–EK Ill-conditioning is a property of the problem, and no amount of restructuring can get rid of this.

2.2 How to develop a mobile computer algebra system

In parallel with the previous: JHD has the slides. These are David Wilson's notes.

2.2.1 How to develop a mobile computer algebra system — Mitsushi Fujimoto

Presenter created the InftyReader and InftyEditor OCR software. Main interest is Computer Algebra in Education (particularly for disabled students). Is currently looking at porting computer algebra systems to mobile devices. Comes with interesting issues.

Infty Project aims to help visually impaired people in scientific fields read mathematical documents (started in 1995). Mobile CAS system is the next step in the project.

InftyReader is an OCR reader designed for mathematical papers. Performs well but still tricked by things like continued fractions. InftyEditor is a typesetting tools that allows mouse/keyboard/handwriting input (internal data is XML but can output to LaTeX, MathML, HTML, Braille, Word etc). Handwriting recognition is pretty impressive! Can connect InftyEditor to a CAD engine to evaluate expressions (and put the input back into InftyEditor).

AsirPad is a pen-based CAS for PDAs. Input math formula by handwriting then can execute the result and manipulate the expressions (using a CAS engine running in the background). Used it for a lecture on RSA cryptography in a junior high school (particularly good as easy to input exponentitation).

Believes CAS is effective and feasible in school education and tablet devices are optimal for educations (portability,quick power, high resolution, simple manipulation etc). Current tablets are generally iOS, Android, or Windows 8.1. Can access a CAS from a tablet by four methods:

1. Native CAS application
2. Access CAS on another machine
3. Through web browser
4. Use worksheet including CAS kernel

Currently there are a few with Method 1 (including maxima, reduce, sympy), which will be the focus of the tutorial.

Make a native CAS application for Android/Windows (with same source code). CAS engine is Risa/Asir using File I/O as communication with a GUI by QtQuick.

A lot of CASs were designed for UNIX OS and can cross build for Android using Google tools. However, the C library of Android is not glibc but Bionic libc, which means they don't work. Also CASs need external libraries so many can't be built by cross-build. Therefore combine Arm rootfs, QEMU, and chroot (details in slides).

Can get Asir, Singular and GAP to run through a terminal app on Android tablet (Nexus 7). Binary and source code to do this conversion is available from the presenter's website.

Developing a GUI for CAS on tablets is very necessary. Use Qt (which has been used for GoogleEarth, TeXWorks etc) which is currently Qt5.3.1. Files needed are available from `http://www.inftyproject.org/issac2014/`.

Has MobileCAS working on tablets and is now looking at extending through incorporating the handwriting recognition and more math fonts.

2.3 Effective Quantifier Elimination for Industrial Applications

H. Anai (Fujitsu/ Kyushu/ NII). Explaining what we do in our company's R&D Labs.

2.3.1 Quantifier Elimination

Usual definition, notes that output is either *feasible regions*, or true/false if no free variables. Note $\exists x : x^2 + bx + c = 0$ is $b^2 - 4c > 0$, but $\exists x : ax^2 + bx + c = 0$ needs case distinction.

Three algorithms

1. Cylindrical Algebraic Decomposition (CAD) [Tar51, Col75, DH88, Hon90]. The output formula is generally simple (compared with others!)[1]. Illustrated with circle ∩ parabola. Project/isolate/lift: many projection operators proposed: "small is good". Lifting is expensive: verified numerics. A sample point has entries of the form (polynomial, interval).

2. Restricted classes — Virtual Substitution, when linear/quadratic w.r.t. quantified variables . Linear case[2] [Weispfenningetal1988], quadratic [Loosetal1993], cubic [Wei94]. Note that in non-linear cases we may have "degree violation", i.e. blowup to the point where not applicable[3].

$$\exists x \phi(x) \Leftrightarrow \wedge_{t \in S} \phi(x//t)$$

3. Sturm–Habicht sequences [GonzalezVegaetal1993][4]. Note that bounds on values are automatically used here. Basic tool is SDC = Sign Definite Condition. Note that, unlike Sturm, this is fraction-free. Hence consider 2^{2n-2} sign conditions of the parameters. Then look at which (combinatorial) cells are applicable. However, there may be unfeasible such cells. See [IYAY13]. Need a lot of Boolean simplification: done by ESPRESSO.

List of QE tools: QEPCAD, Redlog, Wolfram Mathematica 10, SyNRAC based on Maple.

2.3.2 Usage

Parameter Optimisation

using QE we can get guaranteed global optima even in the non-convex case. Also gets feasible regions (but note the remark about simplification). For multi-objective optimisation we can get the Pareto optimal front. One example is feasibility regions satisfying Routh–Hurwitz [Jir97].

Symbolic–Numeric Optimisation

Used [Rat02] [Ratschan2008]

2.3.3 Applications

Control1 Find b such that $\exists N \in [1, 10] : f(b, N) > 0$

Control2 Find b such that $\forall N \in [1, 10] : f(b, N) > 0$

[1] Apparently [Hon90] shows how to produce them via combinatorial optimisation.

[2] JHD added [LW93, Wei97].

[3] In conversation, he says that degree violation occurred very often for quadratics. Nevertheless he regarded VTS for quadratics as "a very useful idea to be applied once" [Sturm]. JHD added [Stu96, ST11].

[4] Seemed to be the basic Sturm–Habicht property.

Minimise $f(x_1, x_2)$ over R. $\exists(x_1, x_2) \in Ry = f(x)$ gives us the range of f. If f is a rational function, we an clear denominators, and then get the same range. This avoids several problems.

Parametric Minimisation similar.

Sign-definiteness used in parametric rigorous control design. Can do PI/PID for a plant with$n < 10$ in one hour.

Showed a window/mouse interface to the feasible regions problem, as used by system designers. "Not so easy" in 3D. See [MIA13]: "engineers do not care about quantifier elimination, they want to solve problems".

SyNRAC can be downloaded from our website. See examples at `hyyps://github.com/hiwane/qe_problems`.

2.4 Algebraic Complexity Theory and Matrix Multiplication

François Le Gall. In parallel with the previous: JHD has the slides.

2.5 Gröbner Bases of toric ideals and their application

Hidefumi Ohsugi.

Gröbner bases by [Buc65], see also standard bases in [Hironaka1964]. Key idea "division of polynomials" (by several others).

Definition 1 *A* toric ideal *is a prime idea generated by binomials.*

These have many applications.

Introduction to Gröbner bases. Need for term orderings, e.g. $<_{revlex}$, which is only admissible if we remember to test total degree first. Also weighted orders.

Theorem 1 (Division Algorithm) *Of f by $\{g_1, \ldots, g_n\}$. Note non-uniqueness.*

Examples of Buchberger's algorithm. Note that GB are not always unique.

Definition 2 *A Gröbner basis is* minimal *if each g_i is monic, and no initial divides any other.*

Note, even this is not unique.

Definition 3 *A Gröbner basis is* reduced *if each g_i is monic, and no initial divides any term in any other polynomial.*

Now unique. Also define S-polynomial. Buchberger algorithm and many improvements, e.g. [GMN$^+$91].

Theorem 2 (Elimination) *If $<$ satisfies the condition that $in_<(g) \in K[x_1, \ldots x_m]$ implies $g \in K[x_1, \ldots x_m]$, then $G \cap K[x_1, \ldots x_m]$ is a Gröbner basis of $I \cap K[x_1, \ldots x_m]$.*

Definition 4 *$A = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \in \mathbf{Z}^{d \times n}$ is called a* configuration *if $\exists \mathbf{w} \in \mathbf{R}^d$ such that $\mathbf{w}.\mathbf{a}_1 = \cdots = \mathbf{w}.\mathbf{a}_n = 1$. Each vector $a \in A$ corresponds to a binomial: $x^{a+} - x^{a-} = 0$. Let I_A be the ideal corresponding to A.*

A is a configuration iff I_A is homogeneous with respect to a usual grading. A is non-negative iff I_A is homogeneous with respect to some positive grading.

Theorem 3 *Let J be a homogeneous ideal, and $<$ be revlex. Let G be the reduced basis of J w.r.t. $<$. $(J : x_n^\infty) := \{f \in K[X] | \exists r \in \mathbf{N} : x_n^r f \in J\}$. Then a Gröbner basis of $(J : x_n^\infty)$ w.r.t. $<$ is obtained by dividing each element $g \in G$ by the highest possible power of x^n.*

2.5.1 Three breakthroughs

See [Stu95].

1. Integer Programming [CT91]. Nice worked example in the notes. "This is interesting, but there are lots of ways of solving Integer Programming".

2. Triangulations of Convex Polytopes [Stu91]. Assume A is a configuration, and identify it with the polytope whose vertices are given by each vector in A.

   Definition 5 *A polytope is a* simplex *if it has* $\dim + 1$ *vertices.*

   Definition 6 *A* covering Δ *of A is a set of simplices whose vertices belong to A such that* $\mathrm{Conv}(A) = \bigcup_{F \in \Delta} F$.

   Definition 7 *A covering Δ of A is* unimodular *if for the vertex set B of any maximal simplex in Δ, $\mathbf{Z}A = \mathbf{Z}B$,*

   Theorem 4 *$\Delta(\mathrm{in}_<(I_a))$ is unimodular iff $\sqrt{\mathrm{in}_<(I_A)} = \mathrm{in}_<(I_A)$.*

3. Conditional Test of contingency tables. Given two such, are they correlated?

Also Sagre-Veronese configurations.

Also The following properties are studied

   (a) There exists a monomial order such that a Gröbner base of I_a consists of quadratic binomials
   (b) $K[A]$ is a "Koszul algebra".
   (c) I_A is generated by quadratic ideals.

   The forward implications hold (a)→(b)→(c), but not the converses.

2.6 An introduction to Max-plus algebra

H. Goto. In parallel with the previous: JHD has the slides. These are David Wilson's notes.

2.6.1 An Introduction to Max-plus Algebra — Hirojuki Goto

Background is operational research and high performance computing.

Consider an industrial project running under PERT: performance, evaluation and review. Can set up a graph of various tasks encoding the relations of the activities (if activity A needs to run before activity B then connect with a directed edge $A \to B$). Can also set up a graph according the time steps, where an edge represents the activity used to move along a time step. The time steps may need to be expressed by max functions (for example, if A and B are both needed to move a time step then the next time will be $\max(t_A, t_B)$). The time steps can be expressed entirely by max functions and $+$: a lapse of time is represented by $+$ and synchronization is represented by max. The graph can be analysed to find earliest and latest node times but is limited. An alternative is max-plus algebras.

A max-plus algebra is defined over $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$ (use ϵ denotes $-\infty$) and has two operations and two special elements:

- **Addition:** $x \oplus y = \max(x, y)$
- **Multiplication:** $x \otimes y = x + y$
- **Zero element** $\epsilon = -\infty$**):** $x \oplus \epsilon = \epsilon \oplus x = x$ (corresponds to $\epsilon = \log(0)$)
- **Unit element**$(e = 0)$**:** $x \otimes e = e \otimes x = x$ (corresponds to $e = \log(1)$)

Can extend to matrics elementwise:

- **Addition:** $[X \oplus Y]_{ij} = [X]_{ij} \oplus [Y]_{i,j}$
- **Multiplication:** $[X \otimes Z]_{ij} = \bigoplus_{l=1}^{n} [X]_{il} \otimes [Z]_{lj} = \max_l([X]_{il} + [Z]_{lj})$
- **Zero element:** All elements are ϵ
- **Unit element:** Diagonal elements are e, off-diagonal elements are ϵ

Why are these useful? Can express a scheduling problem in matrix form (weight adjacency matrix from the graph) as two equations $x = M \otimes x \oplus e_1 \otimes u$ where e_1 is the basis vector $(e, \epsilon, \epsilon, \ldots, \epsilon)$ and u is the initial state vector. Can convert to Max-Plus Linear form (MPL): $x = A \otimes x \oplus b$. How to solve MPL? Substitute iteratively (as subtraction and division are not defined directly in max-plus algebra).

To consider latest times we need to define a subtraction, minimum, and pseudo division:

- **Subtraction:** defined standard way
- **Minimum:** $[X]_{ij} \wedge [Y]_{ij} = \min([X]_{ij}, [Y]_{ij})$
- **Pseudo Division:** $[X \odot Y]_{ij} = \min_l(-[X]_{il} + [Y]_{lj})$

A max-plus algebra is a class of Dioids: $(\mathbb{D}, \oplus, \otimes)$ is a Dioid if it is a semiring with idempotency ($\forall x, x \oplus x = x$). Other Dioids include max-times algebra, min-max algebra, min-plus algebra, boolean algebra.

Chapter 3

July 23

3.1 Mathematics by Machine –Todai Robot Project–

Given by Noriko Arai (NII): teamwork with Matsuzaki, Iwane and Anai.

There are > 100 researchers on the Todai[1] Robot project. Apparently she had the idea three months before IBM's Watson featured on jeopardy. The first test is a written multiple-choice examination (National Standard Test), requiring over 80% to pass. The second test is a written examination. Our first goal is passing NST at Tokyo level in 2016. This involves comprehension and thinking. The second goal, for 2021, is to pass the free-style written test, which also includes document summarisation and answer generation.

2011 Project start, analysis (big XML database of past questions).

2012–13 Technology mapping (Watson,Mathematica, SyNRAC, Maple etc.)

2014– Own platform.

One can imagine a sequential process like the following.

1. Problem
2. Machine Translation
3. Logical Form
4. CA and TP
5. Answer

[1] Entrance Examinations for Tokyo University.

3.1.1 Watson

Specially tuned for questions on Jeopardy. Won against two former contests. Jeopardy is always What/Who/..., never Why/How/.... Example

> Mozart's last symphony shares its name with which planet.

She showed how to Google for this: "Mozart's last symphony". Hence the trick of Machine Learning is to choose what to Google for, and how to recognise the answer. Hence ML is great for what it does, and ML (i.e. Google Translate) has no hope with the "Machine Translation" task flagged above. Also notes that there is deeper knowledge — showed an example:

> which is the wrong statement
>
> - The Janissaries were the standing army of the Ottoman Empire
> - The Frankish kingdom established the 'thema' system.

The Wikipedia articles for "Janissary" and "Thema" are not as much help, and you need to know that Frankish≠Byzantine. Claims this is a hard entailment problem in NLP, well beyond current ML. Showed examples of entailment challenges from recent conferences. In 2010, 17 teams participated, with NII teams coming 1/2/3 with 57–55%, against IBM teams of 38%, and a baseline of 20%. Humans do about 90%.

Therefore we have reverted to grammar-driven translation, against the consensus data-driven approach. What do we translate into? Showed an example (Hokkaido, same as the example in [IMAA14]) and its translation into a subset of ZF. There are many possible readings, giving "exponential blowup".

> If a closed, non-self-intersecting loop lies in a plane, then the loop divides the plane into two regions.

This is the Jordan Curve Theorem, which took a century to formalise.

Also gave two similar sentences, one of which is RCF, the other involves (implicitly — "the circumference of the circle") π, so is not.

3.1.2 Quantifier Elimination

But RCF/QE is doubly-exponential in the number of variables[2], with a practical limit of 5 or 6. Shows a small example whose naïve translation has eleven bound and one free variable.

1. Problem
2. Language Understanding
3. Logical form in F
4. Formula rewriting

[2] See [**?**, BD07].

5. ...

47& of problems are RCF, 10% are Peano, 23% are transcendental functions, 15% are RCF+PA, and the rest are misc.

Looked at our performance on the National Centre prep test. We are close to the mode of human participants On Mathematics preparation test, we get 59.4 for humanities maths (against human average 57.4), for sciences 61.2 versus 59.4. This has been reported in WSJ and IEEE Spectrum."Can a Robot Get into Japan's Most Prestigious University". `http://21robot.org`.

Q–DJW Which step is the most expensive.

A That depends: if we have a lot of variables, then it's certainly E, but if the language is ambiguous, we may have > 1000 readings and then that is the bottleneck.

Q These proofs don't produce insight?

A That's a good point for the second test. Note that our ultimate aims are wider than just Todai.

Q–EK US has several similar challenges.

A History and Chemistry, also English, have international (automated?) computations[3]. Next week's AAAI should see progress.

Q Running time.

A We set one hour as the limit, and assume parallelism.

Q Humans can't use dictionaries etc. in examinations. Hence this isn't fair.

A This isn't really the point (we don't use the dynamic nature of the Internet; could have a static Wikipedia), but also humans have experience to learn from.

3.2 Constructing Fewer Open Cells by GCD ...

Current CAD techniques suffer from scalability. Many applications need to check whether a given polynomial is non-negative or not.

Example 3 *Eliminate z, then y. The univariate has eight distinct real roots. End up with 113 sample points of $f \neq 0$ in $\mathbf{R}^3$. Eliminating y then z also gives a univariate with eight real roots,* $\gcd(f_{yz}, f_{zy}$ *has only six real roots.*

Lemma 1 *No matter what the variable order used when lifting, under our conditions, there will be a non-empty intersection of sample points*

[3]This is what JHD wrote. Nevertheless, it probably should read "competitions".

This means (JHD not sure how) we can just use the decomposition of $\mathbf{R}^1$ by $\gcd(f_{yz}, f_{zy}$ to start lifting from. Showed statistics on 100 random degree-8 trivariates. So this method produces fewer sample points.

Comparisons of various software, including SOStools on MatLab2011b. Times much better, and cell counts down. Also an example for showing non-negative, where only their PSD and SOStools could go beyond $n = 8$ They claims $n = 23$ for PSD–Hptwo, where SOStools finally gave up.

3.3 Quantifier Elimination by Cylindrical Algebraic Decomposition Based on Regular Chains

Paper by Chen and MorenoMaza, talk given by JHD. No questions.

3.4 Cylindrical Algebraic Decomposition using Local Projections: Strzeboński

Using projection sets computed for each cell separately. Define semi-algebraic etc.

Problem 1 *Given a (possibly quantified) system of equations/inequalities, find a cell decomposition of the solution set (not the whole of* $\mathbf{R}^k$*, and certainly not of* $\mathbf{R}^n$*).*

A Cylindrical Algebraic Formulation lets us tests for emptiness, find minimal/maximal values, volume, compute integrals, and do set-theoretic operations. Idea: the Boolean structure of S can be used to find a smaller set of polynomials whose signs are sufficient to determine the Boolean value of S on the current cell. Only these polynomials need to be projected. Example in paper: 357 cells with global projection, 13 with local.

So we define a "local projection", taking a set of polynomials $\subset \mathbf{R}[x_1, \ldots, x_n]$ and $a = (a - 1, \ldots, a_{n-1})$.. The lifting algorithm takes in addition the actual system S of equations/inequalities.

We gain nothing on Brown's projection, except that ours always works. Compared with Hong's projection (a) we can use McCallum/Brown if *locally* well-oriented (b) we don't need to dd (case-dependent) nearly as many special ideas.

Examples from [Wil12], and random polynomials.

3.5 A near-optimal algorithm for isolating the roots of sparse

Problem 2 *given a (not necessarily square-free)k-nomial of magnitude* (n, L)*, can we compute isolating intervals in* $Poly(k, \log n, L)$*.*

Yes $O(k^3 \cdots \log(nL) \ldots$, which is asymptotically fast for very sparse polynomials.

For dense polynomials, the best known in Pan's fast factorisation method $O(n^2 L)$, but this isolates all complex roots, so can't benefit greatly from sparsity. Hard to implement. There's a hybrid Descartes/newton method, which needs $\tilde{O}(n^2)$ operations on items of amortised size $\tilde{O}(n + L)$. The Taylor shift operations destroy sparsity, though. Implementation of this are coming.

There are polynomial time operations for integer/rational solutions [CKS99, Len99]. Also methods for 3,4-nomials.

Overall strategy is to work from isolating intervals from the first fractional derivative: $f_1(x) = x\hat{f}'(x) + e_1\hat{f}'(x)$ where $\hat{f}'(x)$ is derivative of f with powers of x suppressed.

We need bounds for evaluating f at a root of g. Root refinement works well if the roots are isolated. But we also do Newton iteration for clusters. Here the number of iterations is linear in the size of the cluster. Newton iteration for r-fold roots is well-understood, and also works for clusters (as long as this cluster is well-separated from other roots). But how do we know? A trial/error Initially set $I : -I_0$; $N_0 := 4$. In each iteration, take three sample points t_i and solve $t_i - r\frac{f(t_i)}{f'(t_i)} = t_j - r\frac{f(t_j)}{f'(t_j)}$ for each pair (i, j). If this produces a consistent integer r, assume an r-fold cluster. Otherwise use bisection. Each iteration is $O(k \log n)$. Any sequence of intervals whose one-circle regions contains the same number of roots has length bounded by $O(\log(nL))$. This therefore looks like $O(r_0 \log(nL))$, but can replace r_0 by number of sign variations in ....

Our bound is near-optimal for $k = O(\log(nL)^c)$.

3.6 Computing low-degree factors of lacunary polynomials; a Newton-Puiseux Approach

Many algorithms for factorisation: generally (at best) polynomial in degree.

Example 4 *$x^{102}y^{101} + x^{101}y^{102} - x^{101}y^{101} - x - y + 1$ has a factor $x + y - 1$, but the cofactor is dense.*

Linear factors [CKS99]. Low-degree factors over $\mathbf{Q}(\alpha)[X]$ [Len99]. See also [KaltofenKoiran??].

3.6.1 Bivariate

$Y - uX - v$ divides $f(X, Y)$ iff $f(X, uX + v) = 0$. Then can produce a Gap Theorem. Also has a technical proposition about what happens if two valuations produce the same bound.

Theorem 5 (Ostrowski) *If $f - gh$ then* $\mathrm{Newt}(f) = \mathrm{Newt}(g) + \mathrm{Newt}(h)$.

Then use Newton–Puiseux Theorem. We only need those slopes p/q where $p, q \leq d$, d being the desired bound on degrees of the factors. For each (p, q) use lacunary univariate factorisation.

In fact, we get multiplicities of factors for free.

3.6.2 Multivariate

We can't use the Newton polygon directly. Compute rather $\text{Newt}_{i,j}$ of $f \in K[\mathbf{X} \setminus \{X_i, X_j\}][X_i, X_j]$. Weighted homogeneous factors given one-dimensional factors, non-homogeneous reduce to ??.

Software: `LacunaryX` in Mathemagix.

Open Can we get lacunary factors in polynomial time? Can we do anything in finite characteristic — partial results in large case?

3.7 Wilson's Notes

The last two were talks in parallel with the session JHD attended.

3.7.1 Mathematics by MachineL Todai Robot Project — *N. Arai*

Aim to pass the Tokyo University entrance exam: multiple choice by 2016, written exam by 2021.

Real Closed Fields questions form 47% of the mathematics problems.

`http://21robot.org`

3.7.2 Constructing Fewer Open Cells by GCD Computation in CAD Projection — J. Han, *L. Dai*, B. Xia

Goal is to obtain one sample point from every connected component of highest dimension (alternative is critical points methods).

Example: compute projection polynomials for $x \prec y \prec z$ splits $\mathbb{R}^1$ into 17 cells. Doing the same for $x \prec z \prec y$ also gives 17 cells. But only 6 roots are shared between both cells.

Lemma proves that lifting order is unomportant for open cells. Using this gcd projection operator gives 87 sample points in $\mathbb{R}^3$ (compared to 113).

Not only does the gcd projection operator produce fewer sample points, but if $n > 3$ it also reduces the scale of the projection.

Compare to many software packages (including Mathematica, RAGlib [critical points] and SOSTOOLS [Matlab numerical package]). First consider:

$$F(x_n) = \left(\sum_{i=1}^{n} x_i^2\right)^2 - 4\sum_{i=1}^{n} x_i^2 x_{i+1}^2 > 0.$$

Everyone can deal with $n = 5$. With $n = 8$ only gcd, RAGlib, SOSTOOLS. With $n = 11$ only gcd and SOSTOOLS. With $n = 23$ just them (140 seconds).

Can permute slightly:

$$G(x_n) = F(x_n) - \frac{1}{10^{10}} x_1^4.$$

Everyone struggles but gcd. Can cope easily with $n = 20$ or $n = 30$ (13.85 seconds).

3.7.3 Quantifier Elimination by Cylindrical Algebraic Decomposition Based on Regular Chains — C. Chen, M. Moreno Maza (*JHD*)

3.7.4 Cylindrical Algebraic Decomposition Using Local Projections — *A. Strzeboński*

CAD where projection set is computed for each cell separately. Generate cylindrically algebraic formula which can be used to decide nonemptiness, min/max of first variable, generate elements, graphical representations, volume, integrals etc.

New algorithm computes customized projection set: uses boolean structure of the input (only project relevant polynomials for that cell) and signs of polynomials on the cell (if know one of the coefficients is non-zero don't include later coefficients).

Example is $f_1 < 0 \vee (f_2 \leq 0 \wedge f_3 \leq 0)$. Global projection produces 357 cells but local only produces 13 cells. For example, when $f_1 < 0$ it ignores f_2 and f_3. It can completely ignore f_3 which is a degree 6 complicated curve.

Used the Bath repository and considered all examples without equational constraints. Very impressive results.

3.7.5 Synthesis of Optimal Numerical Algorithms using Real Quantifier Elimination — *M. Erascu*, H. Hong

Case Study: Square Root Computation.

In general want to synthesize $f(y) = x$ with input x (real number) and ϵ (error bound) and want to output an interval I of width less than ϵ with $y \in I \wedge y = f(x)$. Numerical algorithm initialises I and refines until satisfies width bound. Want to find a refining operator that shrinks I fastest. Will look at $y^2 = x$.

Have improved the convergence of an existing numerical algorithm for square root. They also demonstrate the power of symbolic methods and advance QE.

Square root - use Secant-Newton Refining Map. Is there a better refinement map? Have quadratic template (of which SN is a special case). Need to guarantee correctenss and temination: translate to a quantified formula.

Want to optimize the ratio of the new interval and old interval. Standard numerical optimization methods cannot be applied because of parameters and quantified formulae. There are infinitely many solutions.

Translate optimality criterion to a QE problem. End up with huge formula.

Need to solve three QE problems: correctness, termination, optimality. Even the simplest (correctness) can't be solved after days. Used a collection of strategies:

- Divide QE into simpler subproblems
- Apply QE on some of them
- Manually simplify the complicated ones
- Impose a condition (including two equational constraints!) on the parameters to simplify elimination (to artificially reduce the number of variables).

Use a combination of REDLOG, Mathematica and Qepcad to divide, simplify, and solve. Get a condition on the parameters to improve the SN map: reduce the Lipshitz constant from $\frac{1}{2}$ to $\frac{1}{4}$ and reduces number of loop iterations from $\log_2(\frac{I_0}{\epsilon})$ to $\log_2(\frac{I_0}{\epsilon})/2$. Practical improvement shows it works too!

Gain a lot of insight into what can use to synthesize other algorithms. Also want to try and remove the condition (with equational constraints) which limits the search space (although the result still holds in this case). Want to try and derive the result completely automatically (without human intervention). Want to generalise the work to n^{th} root comptation.

Advertisement for SYNASC.

3.7.6 An a posteriori certification algorithm for Newton homotopies — *J. D. Hauenstein*, I. Haywood, A. Liddell

Use numerical computations to prove theorems. Application: prove a nice smooth movement of a robot.

Want to solve a square system $f(x)$ of nonlinear equations. Homotopy continuation finds a new (easy) system g, solves $g(x) = 0$, constructs homotopy $H(x,t) = (1-t)f(x) + tg(x)$, and tracks solution curves for H.

How to find g? Reverse the idea and pick a point you want to be a solution and then construct g around that point: commonly used techniques are fixed point homotopies $[g(x) = x - x_0]$ and Newton homotopies $[g(x) = f(x) - f(x_0)]$. Newton homotopies give $H(x,t) = f(x) - tf(x_0)$ so only constant terms depend on t.

Newton homotopies are a local method to search for solution. Can use for path tracking to certify that a smooth connected path exists between a start and end point. Lots of work using a priori information (necessarily pessimistic: small certifiable regions even though it works elsewhere).

Instead can use heuristic method to approximate the path. For each sequential pair of points approximate a smooth curve (independent and parallelisable). Can be optimistic (because using heuristics) and then can refine the intervals into smaller segments if needed for certification.

Performs very well compared to a priori methods: can get larger regions and less steps. Robot system in 12 variables looking for smooth path. Heuristic takes 16 steps and 0.01 seconds. A posteriori certification only takes 51 intervals and 2.2 seconds.

3.8 Sparse Polynomial Interpolation in Practice

By van der Hoeven and Lecerf. Software from `mathematgix.org`, but warning: there are three versions, in various stages of developments. Let `M(12)` denote the generic 12×12 matrix. Then his code can do in your face `simplify(M(12)*inverse(M(12)))`, whereas most systems will expand and this will kill you.

In mathemagix, series are truly lazy objects, and he showed this.

Our goal is that, if the answer is small, it should be computed swiftly, irrespective of intermediate expression swell.

First implementation is [BOT88]. Improvements by modular arithmetic, and Kronecker [AR14]. However, this may require a multi-word prime. Idea of coefficient ratios [JavadiMonagan2010].

Aim to provide a C++ API.

Q Zippel's interpolation? This led to a heated debate: incremental or not.

3.9 Formal Series Solutions of Iterative Functional Equations: Izumi

Equations of the form

$$\sum_{i=0}^{n} c_k f^k(x) = g(x).$$

3.10 Parallel Telescoping and Parametrised Picard–Vessiot Theory

Example 5 (Telescoping)

$$I(t) = \int_a^b f(t,x)dx$$

OK if there's an indefinite integral. Let D_t and D_x be the usual differentiations. Want $L(t, D_t)(f) = D_x(g)$, so $L(I(t)) = g(t,b) - g(t,a)$.

Parallel telescoping

$$L(t, D(t) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} D_{x_1} \\ \vdots \\ D_{x_n} \end{pmatrix} (g)$$

Definition 8 *A function $f(t,x)$ is D-finite over $k(t,)$ if f and its derivatives span a a finite dimensional vector space over $k(t,x)$.*

Definition 9 *A function $h(t,x)$ is hyperexponential if ...*

Definition 10 *Functions $f_1,\ldots,f_n$ are*compatible *w.r.t.* $\mathbf{x}$ *if $D_{x_i}(f_j) = D_{x_j}(f_i) \forall i,j$.*

Theorem 6 *Compatible functions always have a parallel telescoper.*

3.10.1 Computation

1. Compute a telescoper (classical) for f_1
2. ... (iteratively to n)

3.10.2 Parametrised Picard-Vessiot theory

Direct problem: compute the Galois group of a linear differential equation. Also inverse problem. The defining operator for the Galois Group is the minimal parallel telescoper. Also, can show that the group $(F,+)$ is not the Galois group of any equation.

3.11 A Generalised Apagodu–Zeilberger Algorithm; Koutschan

Elimination approach — Zeilberger's slow algorithm, Takayama's algorithm. Works for general ∂-finite holonomic functions. Loop approach: Zeilberger's fast algorithm, Almkvist–Zeilberger algorithm. Generalisation to ∂-finite functions [Chyzak]. Prediction Approach: Apagodu–Zeilberger Algorithm.

Recall Ore algebras ,with automorphisms σ_x and σ_y. $A = K(x,y)[\partial_x, \partial_y]$.

3.12 Bounds for D-Finite Closure Properties: Kauers

"I did a lengthy calculation, which was tedious".

Definition 11 *A sequence $(a_n)_{n=0}^{\infty}$ is D-finite ... A power series id D-finite if it is a solutions of a differential equation with polynomial coefficients. Write in terms of shift/differential operators, belonging to Ore algebras. In general, $f \in F$ is D-Finite if there is an $L \in A \setminus \{0\}$ with $L \cdot f = 0$.*

There are closure properties: if f and g are D-finite, so are $f+g$, fg. Hence, if we can make this constructive, we know how many finite checks are sufficient to prove a desired identity.

Proposition 1 *If f has order r and g has order s, then $f+g$ has order $\leq r+s$*

Proposition 2 *If f has order r and g has order s, then fg has order $\leq r+s$*

Example 6 $2^n + n!$. *Here* $a_{n+1} = 2a_n$ *and* $b_{n+1} = (n+1)b_n$.

$$\begin{pmatrix} 4 & 271 & \\ (n+2)(n+1) & (n+1) & 1 \end{pmatrix}$$

is the relevant matrix, and it clearly has solutions.

Want to bound order, degree and height.

Theorem 7 *If* $f_1, \ldots, f_n$ *have degrees* d *and heights* h*, then the operator* L *for* $f_1 + \cdots + f_n$ *has*

$$\begin{aligned} \operatorname{ord}(L) &\leq r := \sum \operatorname{ord}(L_i) \\ \deg(L) &\leq (n(r+1) - r)d \\ h(L) &\leq h(r) + h((n(r+1) - r - 1)!) + (n(r+1) - r)(h(d)_c^{(r)}(d, h)) \end{aligned}$$

Similar (more complicated) result for multiplication.

Q Sharp?

A Generically, yes, for order. See paper. Degree/height they are not quite sharp.

Q Powers?

A See paper: better than repeated multiplication.

3.13 DJW Notes on Parallel Sessions

3.13.1 Improved Algorithm for Computing Separating Linear Forms for Bivariate Systems

Triangular decomposition. Key is resultant computations. Want to compute the difference:

$$\sum \mu(\alpha, \beta) - \sum (\mu(\alpha, \beta) - 1)$$

where μ is the multiplicity of β in $gcd(P(\alpha, y), Q(\alpha, y)$. Can do by triangular decomposition in d^4.

Rather than considering a general system, they consider a system of critical points with respect to one direction.

Use a Las Vegas gcd method to select a good prime for computing number of solutions.

3.13.2 On the computation of the topology of plane curves

Can distinguish existing approaches into such which permit to shear the curve as a first step and those that don't. Combine sub-algorithms for computing CAD with new reslts on computation of the local topology.

Main step is to compute critical boxes and special fibers of curve (with CAD) then compute the horizontal boundary points and their slope sign. Then compute relative position of boundary points and critical points and then reconstruct the local topology inside the critical boxes.

3.13.3 Covering of surfaces parametrized without projective base points

Can represent a surface implicitly ($f(X) = 0$) or parametrically ($X = g(T)$). If parametric then ideally it should be injective and surjective. The latter is called normality and want to answer how far an affine surface parametrization can be from surjectivity.

If surjectivity fails then finding critical points becomes difficult. Important to think outside of $\mathbb{R}^3$ (complex projective space). Need to be careful about degenerate points (where you essentially have 0/0). Can cope with local 'patches' of 2-dimensional parametrization.

3.14 SIGSAM Business

Presented by Agnes Szanto on Ilias's behalf. Publishes CCA, sponsors conferences including ISSAC, also SNC, ECCAD, PASCO and PLMMS. "in cooperation" means SIGSAM/ACM takes no risk, just publications. "Sponsorship" means ACM/SIGSAM takes the risk and ACM, on SIGSAM's behalf, takes the profit/loss.

History SIGSAM was founded in 1967. There's a lot around, both SIGSAM and ISSAC, that should be collected to help new officers. ISSAC 2013 generated USD7541 in overhead (stays in SIGSAM) and a profit of USD4135. It was noted that the awards at ISSAC came out of the ISSAC budget, rather than SIGSAM general.

SIGSAM has around 150 professional members and 70 affiliates. This is down from a big spike in 2010, believed to be due to tying membership to ISSAC membership. Dan Roche said that had been impossible in 2013. The aim is that the difference in registration fee is equal to (students, USD1 more than) SIGSAM membership fee. This doesn't always work, since grants don't allow it, even though they don't notice!

3.15 ISSAC Business Meeting

3.15.1 Bids 2016

Notre Dame (College of Science) Jonathan Hauenstein. 375-seater in new conference centre. Dorms and hotels (one on campus). Week commencing 18 July meets the criteria. There is an airport in South Bend. Connections via Chicago and Newark, also limousines to O'Hare. Some funding; USD7500 for students/postdocs at tutorials, plus various other sums. Discussion of registration fee — inconclusive. Weather — high 80F.

Georgia Tech Leykin, via student. Georgia Tech is in Atlanta. "Any dates before August 15". Lots of hotels (15 walking distance) and dorms should

be a possibility (previous summer school). Expects fees to be USD200–300. Significant local interest — Emory and Georgia State. Many tourist attractions, including Coca Cola Museum. Weather like Kobe — high 32C.

Wilfred Laurier Zima. WLU is building a new Maths/Computing building. Transport is generally Toronto (90km), though there are flights into Waterloo. We have run several smaller workshops etc. Seeking support from Perimeter Institute, Fields, NSERC etc. Aiming at CAD100 for normal SIGSAM members. Proposed dates 20–22 July 2016.

Votes for this, and ISSAC SC member.

ISSAC2014 6 tutorials, 3 invited, 51 talks, approximately 150 people. 37 students, 85 academics and 5 industrial. Europe 48, North America 37, Asia 46 (Japan 39, China 7).

Fees 2.1MYen from fees, 900KYen grants, 600KYen companies. Banquet 1095KYen, speakers 706KYen.

Wolfram Announced this is the last ISSAC they can support (by the Japanese office).

papers 51 accepted papers, 284 reviews, 184 external reviewers. Submitted authors: 43 France, 27 China, 21 US, 19 Canada, 16 Japan, 10 Germany, 10 Spain, 5 Austria, 4 UK, 3 Netherlands, 3 India, 2 Australia, 2 Greece, 1 Russia, 1 Senegal etc. (Recent) tradition is not to disclose the acceptance rate. Note that abstracts helped the reviewing process —basically gained a week. Note that the reviewing process is published on the ISSAC page.

Results Waterloo/Agnes Szanto.

Chapter 4

24 July 2014

4.1 Stoutemyer — Invited

Some high-level Mathematica functions are float-robust, but many are not, and I've had to do *ad hoc* adjustments. Hence I now have a more general solution, `fuzzySimplify`. Deals with

1. rational/symbolic constants
2. machine floats
3. Mathematica bigfloats (which carry significance with them — these are first-class Mathematica objects: `1.2``3` is "1.2 to three decimal places")
4. intervals

Has a menu-based interface for various options, such as "after `fuzzySimplify`, convert intervals to arbitrary floats". Also four levels — "conservative", "intermediate", "aggressive", "reckless". Note that he handles complex intervals as well. Much of Mathematica is not complex-interval, or even interval, aware, so `fuzzySimplify` goes via significance floats. Not totally rigorous, but works!

Has a tab for the definition of "approximately equal". One definition is "subset of", another is "intersection non-empty". User-stated, e.g. "to 3 decimal places" is also possible. Expressions are equal if the trees are isomorphic up to the previous definition on the leaves. However, implicit 1/0 are also matched as above.

There's a definition of unification. Various options, such as "unify to arithmetic mean", inversely weighted to variances (as estimated from significance). There's also a "more concise" option, which he demonstrated. This has to deal with "ghost terms", i.e. intervals that contain 0. Unification is recursive, so arguments of unspecified functions unify, which means the whole terms can unify, and hence this chain can continue. This extends to "approximatively proportional" to combine expressions.

Floats are all rationals, so we can convert and then do gcds, but this tends to produce very large denominators. Hence only consider results when the denominator as $< 1/3$ as may digits as you'd expect. "The floats that participate get a reward for participating". One option is to "look for floats that round to 0, ± 1", as these produce significant collapse of the expression tree.

Maple has a really neat `Identify` function, to find floats that are "really" nice numbers such as π, so I wrote my own.

"Beautification" is an idea when to discard a term in a sum. We now have one, which compares the norm of the summand to the others, and discards "small" ones w.r.t. the tolerances. We increase the interval widths of the others to compensate.

Q–SMW What happens if you leak over a branch question.

A Good question: here are some nuts.

Q Where does inaccurate data come from?

A Good question. We can measure time, the most accurate of all, to 10^{-14}, which is less accurate than IEEE-floats.

4.2 p-adic precision and Gröbner bases: Vaccon

Why $\mathbf{Q}_p$ — allows more computation than $\mathbf{F}_p$, and controls coefficient growth better than $\mathbf{Q}$.

4.2.1 Row echelon computation

Proposition 3 (non-archimedean) *p-adic errors don't add.*

Theorem 8 *Let $M \in M_{n.n}(\mathbf{Z}_p)$ with*

- *All entries known up to $O(p^k)$*
- *Condition on minor*

then we can compute the determinant to precision $k - \sum$ valuations of minors.

Definition 12 *The* Macaulay matrix $\mathrm{Mac}_\alpha(f_i)$ *has rows $\mathbf{x}^\alpha f_i$ written n the basis of the x^{d_i}*

F5 basically builds $\mathrm{Mac}_d(f_i)$ and row-echelons them.

Definition 13 *We say that I is a weakly-ω ideal if*

- *for all x^α a leading monomial according to ω of the reduced Gröbner basis of I*
- *For all β such that $|\alpha| = |\beta|$, ...*

Weak Matrix F5 algorithm:

- $(f_1, \ldots, f_s)$ is ... (H1)
- ...

Proposition 4 *If F has H1 and H2, the LM ideal is constant around F, the reduced GB is rational around F, and we can give an explicit neighbourhood of F*

We have examples that show these conditions can't be relaxed.

With the regular sequence and weakly-ω assumptions, we can actually compute Gröbner bases with Matrix F5.

But, in real life the Macaulay matrices are sparse, so we may be too pessimistic.

Q Why matrix F5?

A Precision control is easy.

Q-Sturmfels What is genericity in the tropical setting?

A I won't need "weakly-ω", so regularity should be sufficient.

4.3 Sparse Gröbner Bases: the unmixed case: Svartz

Polynomial system solving, over $\mathbf{K}$ or $\overline{\mathbf{K}}$. Known to be NP-hard. Applications tend to have structured GBs. How do we use this.

- All polynomials have the same support in a polytope
- or weighted-homogeneous case.

Convex case Kushnirenko–Bernshtein bounds. Resultants: Canny/Emiris, etc. [Sturmfels1993,Sturmfels1999].

We want to work in the semigroup generated by the monomials of the support. New algorithms Sparse-F5, Sparse-FGLM. If $M = \mathcal{P} \cap \mathbf{Z}^n$ we have complexity bounds depending on $\mathcal{P}$.. Hence we need semi-group algebras: $\mathbf{K}[S]$.

A sparse GB (sGB) I is $\langle LM(G)\rangle_{\mathbf{K}[s]}$ .... Note that these are **not** GB in the traditional sense. The *sparse degree* of f is the smallest k such that $f \in \mathrm{Span}_{\mathbf{K}}(k \cdot M)$

Definition 14 *The* toric homogenization *of S is $\{(s, 1) : s \in S\}$. Denotes S^h.*

Ideas of sparse Macaulay matrices, and as above we get sparse-matrix F5.

If we forget the homogenisation variable, we get a sGB in $\mathbf{K}[S]$. We look for linear combinations of (X^{h_i}) in $\mathbf{K}[S]/I$. Associate new variables H_i to X^{h_i}, and the sGB then becomes a normal GB on $\mathbf{K}[H_i]$.

In the special case of a lattice polytope, the witness degree is $(n+1-l)+1+\sum(d_i-1)$ where $l=\min\{j : j.\mathcal{P} \text{ has an interior point}\}$. This extends to multilinear systems. We can solve in polynomial time, even if one component is not size-bounded.

Examples of overdetermined sparse systems with one forced solution (so do not need sparse FGLM). Speedup 10–1000 w.r.t general F5. Also examples with support $\{1\}\cup$ random set of k quadratic monomials. But in general (non-regular) have no bound on witness degree. Also if the semigroup algebra is not CM we don't know. It is not clear how to go from sparse Matrix F5 to sparse F5 (the "LMS" of two monomials is not unique). Idea in [Sturmfels1994].

Q-Sturmfels Anything special about the term order?

A We have to ....

Q Benchmarking — did you try structured examples? Cyclic, Katsura etc.

A Cyclic is the fewnomial case, and this doesn't help.

4.4

assume radical, zero-dimensional. **K** infinite. some special cases.

[Mourrain,Pan1998] approximate all real roots $\tilde{O}(12^n D^2)$

[Salvy] ...

As in FGLM, we will concentrate on lex as the output. By [Bardet,Faugere, Salvy2005] $O(d^{\omega n}$ for a TRDL GB, then nongeneric ideals given $O(nD^{3n})$,and this is the bottleneck. [FM13] does better. We want a sparse FGLM, but not in the same sense as previous talk. They assume the lexGB is in shape position. All we really want is the last polynomial. Then reconstruct this via deterministic Wiedemann.

We need to look at the FGLM Lemma. Computing μ_{x_n} is computing the $NF_{DRL}(\epsilon_i x_n)$ for $i \in \{1,\ldots,D\}$. Can be interior (nothing to do), go to top (not much to do), or we arrive on the vertical border. This is OK if we have the $(1,2)$-staircases position case. So[MorenoSocias2012]. [Galligo,BayerStillman,Pardue] says that there is a Zariski open subset such that the $(1,2)$-staircase position is true — see also Shape Lemma. Therefore both $(1,2)$ and Shape are generic, and we have $\tilde{O}(d^{\omega n}+nD^{\omega})$.

For an example on Edwards curves (D=65536) we go from impossible to 6 hours for the FGLM. Note that the TRDL GB computation was 3.5 hours.

4.5 Tame Decompositions and Collisions: Ziegler

Composition of univariate polynomials over a finite field of characteristic p.

wild char(**K**) divides deg(f)

tame otherwise

Let P_n be the set of polynomials of degree n, and D_n the decomposables. $D_{d,e}$ is those decomposable with degrees d, e. Get D_n from $D_{d,e}$ by inclusion/exclusion. Intersections of these sets are *collisions*. By counting $|D_{d,e}| = q^{d+e-2}$ with one-collisions, i.e. no multiple cases.

Let $f^{[a]} = f(+a) = f(a) \in P_n$. This operation respects compositions. 2-collisions are studied in Ritt's Second Theorem (when $\gcd(d, e) = 1$. Example: $f = g \circ x^e =^e \circ h^*$. These are *exponential components* E_n. Dixon polynomials give us *trigonometric components* T_n. [vonzurGathen2014] has a normal form.

For non-coprime cases, we can reduce to coprime cases by taking gcds (tame!). In general, has a matrix-based procedure working on the possible degrees.

So start with all factorisation of n, refine the factorisation by matrices, , build the relation graph, spit into strongly connected components, use the unidirectional subgraph to sort E.

The number is always a polynomial in q (integer coefficients), which is not the case for the wild case.

Q Any structure to the polynomials.

A I can't find one, using OEIS [Slo03].

4.6 The MMO Problem: Gómez-Pérez

Use $\langle f \rangle_p$ to mean "reducing all the coefficients modulo p".

HIMMO developed by Philips to communicate via a TTP, who sends shared secrets to nodes. This depends on the nodes identifiers. Once done, this allows secret keys between any pairs, with the TTP playing no further rôle.

1. The TTP generates α, p, q (JHD thinks α is the security parameter). Select randomly symmetric $f(x, y)$, $g(x, y)$.

2. Node publishes his identifier x_1. Requests his TTP, which is $(\langle f \rangle_p, \langle g \rangle_q)$.

Can nodes collude to recover f, g? MMO = "Mixing Modular Operation".

Problem 3 *Let $h : \mathbf{Z} \to \mathbf{Z}$ be the sum of two unknown reduced polynomial $\langle f \rangle_p + \langle g \rangle_q$. Suppose we know*

$$J = \{(x_1, h(x_1)), \ldots, (x_,h(_c))\}$$

can we find f, g.

Special case is when p, q are known.

On average the number of values needed is 2α.

Had some reasonable conjectures, but computer search disproved these.

Can solve the MMO problem with known moduli, and can reduce the unknown moduli problem to a lattice problem, for which we have a heuristic algorithm. Still need to study the uniqueness problem.

4.7 David Wilson's Notes

4.7.1 A New Deterministic Algorithm for Sparse Multivariate Polynomials

Given an underlying ring and a black box which tells you value of polynomial at points, want to decide what points to ask about to determine the polynomial.

New algorithm works over integers. Uses black box with a point and an integer and will give you polynomial value modulo the integer. Model makes sense as we don't gain extra information by may help to design algorithms running in sub-linear time in d.

Basic idea to interpolate with many primes and use Chinese remainder theorem. Issues are bad primes and how to use CRT.

Interpolating modulo p we ask value mod p at integers $0, 1, 2, \ldots, p-1$. Interpolation gives coefficients mod p. Want all coefficients but if p is bad then a coefficient may vanish or be equivalent to another coefficient modulo $p-1$.

Consider primes in arithmetic progression $1+k, 1+2k, 1+3k$. Use Linnik's Theorem.

At most there are $5m \log H$ bad primes for coefficients vanishing, and $\binom{m}{2} \log d$ bad primes for coefficients being equivalent. Can find many good primes through a set method.

4.7.2 Sparse Polynomial Interpolation Codes and Their Decoding Beyond Half the Minimal Distance

If dense want to know degree bound, and if sparse want to know either the support or sparsity. Concerned with sparsity of sparse polynomials with errors (outliers).

A code is a subset of a set of words: a sub vector space. Hamming distance is the number of different components, and minimum distance, δ, is the smallest hamming distance. Correction capacity is at most $(\delta - 1)/2$. Unique coding problem is given a point find the unique word less than the correction capactity away.

Goal is to generalise Reed-Soloman codes in sparse polynomials. Have a polynomial assmed to be t-sparse, evaluated at errors and try to decode.

Surprising link to Erdős-Turán theory on arithmetic progressions. Link to Szemeredi's theorem.

4.7.3 Sparse Multivariate Function Recovery With a High Error Rate in the Evaluations

Looking for a rational fraction of polynomials.

4.7.4 Sparse interpolation over finite fields via low-order roots of unity

Striaght line programs. Given a division-free SLP with L instructions computing f (of bounded degree and number of terms) then want to construct the sparse representation of f (assume that f is sparse). Don't want to just expand SLP as can become exponentially large.

Deterministic polynomial time algorithm given in 2009 (quartic). ince then have been Las Vegas and Monte Carlo methods to quadratic and linear. This talk is linear but with a lower log term.

Work modulo various primes and need to guarantee that we have enough good primes. Issue: we don't know f so we don't know if a prime is okay.

4.7.5 Multivariate sparse interpolation using randomized Kronecker substitutions

Main result - a new randomization that improves teh Kronecker substitution trick by reducing the degree when the polynomial is sparse (initial application is sparse interpolation).

Kronecker substitution is a map from multivariate polynomials to univariate. In bivariate: $f(x, y) \mapsto f(z, z^D)$ where $D > \deg_x(f)$. Can think of the terms forming a staircase: Kronecker substitution is invertible. Often used to multiplying polynomials. Original motivation was to discover factorisation of multivariate polynomials and has been improved.

What is the trick? Choose random values p, q: $f(x, y) \mapsto f(z^p, z^q)$. How to choose p and q such that f can be recovered? Want $p \deg_x + q \deg_y << D$. Problem can occur if terms overlap: the difficult bit. Can reduce a $\deg_x = \deg_y = 6350$: Kronecker gives degree 40328900, now down to 659100 (61 times smaller, with 6610 collisions).

A collision means that you have p and q dividing differences in coefficients. Will always be collisions, else you wouldn't do any better than Kronecker. The map is also no longer invertible so have to deal with it depending on the application. There are ways to deal with this for sparse interpolation.

4.8 Maple 18: JG

Startup Get a new start-up page, looking rather like an iPad! Note that this is modifiable.

Shortcut component — needed to support the above.

Help various changes,including full-text search.

Visualisation `embed` (images in worksheet), verb+size+ option to control size of plot.

Fractals New package.

Groups including `PerfectGroup` command/database.

Engineering Dynamic systems, Signal processing

Performance GMP 5.1.1 is faster, a factor of 4 faster than Maple 17 on some cases, 33 on $\gcd(F_n, F_{n-1})$. New data structure for (some) polynomials. Based on [MP12].

Compiler LLVM now included.

Education Calculus palette, Student:-Statistics etc.

Web access packages (example is OEIS)

Code generation: Python, Perl, better MatLab support. He used the CodeTools:-Usage command. It tells you things like the memory usage, alloc change, cpu time, real time, and gc time (garbage collection time) for any command (plus the result of the command if you end with a ';').

4.9 Automated Math Problem Solving by Grammar-Driven Natural Language Understanding and Real Quantifier Elimination

4.9.1 Natural Language

Part of Todai project. Shows (English translation of Japanese original of) Hokkaido2011. The project employs Language Understanding and Automated Reasoning, but the interaction is not simple. Showed a demo. Needed a manual hint to insert "paragraph heads" at the moment. Note the importance of this. Goes through to automatically-generated answer sheet.

Reformulation from ZF to RCF. Obviously not always possible, and quite hard in practice. Furthermore, this produces very unreadable code.

4.9.2 QE simplification

Example Human parsing uses 5 variables, but robot parsing 19.

Equational constraints often come up, especially in Geometry.

Special algorithm — VTS and SH sequences.

QE–conjunction Sort the formulae in increasing complexity (weighted sum of indicators)

Data Manually-constructed FoF solves 40, Manually-constructed Lisp is 28, and raw FoF 23.

Q English or Japanese?

A Not much different in terms of difficulty.

4.10 Mathematica: AS

Regions (geometric) can now be computed with: built-in or user-defined. Intersection etc. (apparently lazily), plotting, discretisation. Can we used as inputs to routines, and, for example "integrate over".

4.11 Root counts of semi-mixed systems, and an application to counting Nash equilibria

A Nash equilibrium is one where no player can improve his payoff unilaterally.

2 players Assume players play with probabilities $p_1, \ldots, p_n$ and $q_1, ldots, q_m$ respectively. Supports the actual supports are Ω_1 and Ω_2 respectively. Then a Nash equilibrium exists iff all $p_i \in \Omega_1$ are equal, and no other p_i are larger, and resp. If $|\Omega_1| \neq |\Omega_2|$, there is generically no Nash equilibrium.

$S > 2$ **players** Little is known. Suppose $m_1, \ldots, m_S$ options respectively. Consider Bernstein–Khovanskii–Koushnirenko bound. The number of solutions is generically the mixed volume of the Newton polytopes. When polytope Q_i is repeated k_i times, we have *semi-mixed volume* $\mathrm{MV}(Q_1, k_1; \ldots, Q_s, k_s)$. The most effective computations of MV is via Minkowski sums.

In our setting, the equations are multilinear. The Newton polytopes are sums of simplices.

permanent Theorem 9 ([Pedersen1994,McLennan1999]) *Consider an algebraic system on $\mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_s}$ of $N = n_1 + \cdots + n_s$ equations. Assume the ith equations has degree $a_{i,j}$ on the jth variable block. Let A be the matrix $(a_{i,j})$, with columns repeated n_j times. Then BKK bound is $\frac{1}{n_1! \cdots n_s!} \operatorname{perm} A$.*

Of course, computing permanents is NP-complete.

m-Bezout bound. This is generically tight.

McKelvey–McLennan bound. A card game with S players, each getting n_i cards. The all cards are shuffled together, and each gets the same number of cards as before. Let $E(n_1, \ldots, n_s)$ be the probability that no player gets a card he held earlier. $E(n, n, n) = \sum_{k=0}^{n}$??

Laguerre polynomials (linearised). Gives a polynomial time algorithm for these E numbers.

4.12 Toric Border Basis

4.12.1 Toric Methods

Equations give Quotient Algebra (Gröbner bases/Sparse Resultants/Toric Border Bases) and hence real roots. S is the multivariate Laurent polynomial ring.

$B^\times$ is the result of shifting B by all x_i and x_i^{-1}. $B^* = B^\times \setminus B$.

4.12.2 Gröbner bases

Need to double the number of variables to introduce invertibility constraints. Also Janet bases [Gerdt2000] Border bases [KR00].

2000 generic

2005 Zero-dimensional

2012 Any affine system

2014 This

Open: Does this actually reduce the size of the matrix?

4.13 Randomised detection of extraneous factors: Minimair

Is a polynomial contained in an elimination ideal? Polynomials $f_0, \ldots, f_n$ in variables $x_1, \ldots, x_{n+1}$, parameters $y_1, \ldots, y_k$.

Motivation is application of resultant methods. The resultant of $f_0, \ldots, f_n$, e.g. Dixon, is a member of elimination ideal times extraneous factors. We say g is *extraneous* if it is irreducible and $\notin J$.

We present a MC-type randomised algorithm for deciding elimination ideal membership, with a detailed analysis of probability of success (asymptotically 1). We replace all parameters by random positive integers $\leq t$. If the Macaulay matrix has full rank, say "extraneous", otherwise not. Technical condition is to be properly zero-dimensional (i.e. the parameter variety on which the system is not zero-dimensional in the variables) is not full-dimensional. Reduces to Schwartz–Zippel lemma. Need to use [Kal85].

EK Best estimate is that the first t that does Hilbert irreducibility may have exponentially-many bits.

Chapter 5

5.1 Sturmfels: Maximum Likelihood for Matrices with Rank Constraints

5.1.1 Maximum Likelihood for Matrices with Rank Constraints

Matrices represent joint probability distributions for two random variables: $p_{i,j}$ = probability first distribution in state i and second is state j. $\sum\sum p_{i,j} = 1$. Hence a rank $mn-1$ simplex. Let $\mathcal{M}_r$ be the manifold of rank-r matrices. Note that no correlation $\equiv$ rank$= 1$.

The likelihood function is the monomial $l_U(P) = \prod\prod p_{i,j}^{u_{i.j}}$.

Frequentists =Maximise = today's talk.

Bayesians =Integrate (against a prior distribution).

Want to maximise $l_U(P)$ subject to $P \in \mathcal{M}_r$.

rank 1 Easy: teach to freshman biologists.

$$\hat{P} = \frac{1}{(u_{++})^2} \cdot \begin{pmatrix} u_{1+} \\ \vdots \\ u_{m+} \end{pmatrix} \cdot \; u_{+1} \quad u_{+2} \quad \cdots$$

(an algebraic, **not analytic**, solution).

rank 2, 3×3 Write down Lagrange multipliers — a 3×9 matrix:

$$\begin{pmatrix} u_{11} & \cdots \\ p_{11} & \cdots \\ p_{11}a_{11} & \cdots \end{pmatrix}$$

where $a_{i,j} = \frac{\partial \det(P)}{\partial p_{i,j}}$.

The known values of the ML-degrees are given by a symmetric (very surprising) table. June Huh has identified this with topological invariants of an open variety.

For a symmetric 3×3 matrix, in an example, all the six critical points of the likelihood function are real positive. Three local maxima, 3 local minima (no saddle points in this case). In fact, the Galois group is S_4, and they are soluble in radicals, using ζ_3. This is a preliminary to the following result.

Given a data matrix U which is $m \times n$, write $\Omega_{i,j}$ for the $m \times n$ matrix $\frac{u_{i,j} \cdot y_{i+} \cdot u_{+j}}{(u_{++})^3}$.

Theorem 10 (Draisma and Rodriguez [DR13]) *The ML-degree is symmetric, via a bijection between the critical points P_i of the likelihood function on $\mathcal{V}_r$ and Q_j of $\mathcal{V}_{m-r-1}$ given by $P_i * Q_i = \Omega_U : \forall i$*

Hero is Bertini which led us to conjecture this equality.

5.1.2 Fixed points of the EM-Algorithm

Statisticians really care about the mixture model: the set of $m \times n$ matrices $P = A\Lambda B$ where A is a non-negative $m \times r$ matrix whose rows sum to 1, Λ is a non-negative $r \times r$ matrix whose diagonal sum to 1, and B is a non-negative $r \times n$ matrix whose columns sum to 1. This is the *non-negative rank*, i.e. insist that the (weighted by Λ) summands be non-negative.

rank 2 For nonnegative matrices, rank = nonnegative rank

rank > 2 No longer true, the low rank model $\mathcal{M}_r$ is the Zariski closure of the mixture model Mix_r inside our simplex Δ_{mn-1}.

Write $\partial \,\mathrm{Mix}_r$ for the topological boundary of the model Mix_r (which is connected: image of a polytope under a polynomial map). The MLE $\hat{P}$ is usually on the boundary. Shows a table of probabilities. Being on the boundary, it cannot be found by differentiation.

By the *algebraic boundary* of Mix_r we mean the Zariski closure $\overline{\partial \,\mathrm{Mix}_r}$ of the topological boundary.

Theorem 11 *The algebraic foundation $\overline{\partial \,\mathrm{Mix}_3}$ is a reducible variety of pure dimension $3m + 3n = 11$ in $\mathbf{P}_{\mathbf{C}}^{mn-1}$. The number of components is*

$$mn + \frac{m(m-1)(m-2)(m+n-6)n \cdots}{6}.$$

For 4×4 matrices we have 16 components with $p_{i,j} = 0$, 144 components corresponding to matrix factorisations, and 144 components from transposes. The variety has degree 633.

We have a quantifier-free semialgebraic formula for Mix_3. We can characterise the variety of fixed points of the expectation maximisation algorithm for Mix_r.

5.1.3 Conclusion

Symbolic Computing matters for statistics. An immediate generalisation is the rth mixture model of several random variables. The corresponds to tensors of nonnegative rank. Many areas of Pure Mathematics are very relevant for Big Data: Algebraic Statistics, Topological Statistics and the third is Differential Geometry applied in Information Geometry

Q–AS How does non-negative rank apply to semi-definite rank?

A Every semi-definite has a Cholesky decomposition: we can require that the Cholesky factors are non-negative.

5.2 Grasegger

Let F be irreducible in $\mathbf{K}[x, y]$ with a rational parametrisation $P(t) = (r(t), s(t))$. Want to look at these defines in a tower of radical extensions: $F(r(t), s(t)) \equiv 0$. Example: $f = x^3 + y^3 - 1$.

First-order, autonomous DE: $F(y, y') = 0$. Consider the curve $F(y, z)$. Then $\mathcal{L} = (y, y')$ is a parametrisation. There is a precise characterisation (two options) in the rational case [FG04]: we aim to extend to radical.

Given an AODE, then the following (if it works) is a method.

1. Compute a radical parametrisation
2. Compute $A_p = \frac{s(t)}{r'(t)}$.
3. Compute $g(t) = \int \frac{1}{A_P(t)} dt$
4. Compute h such that $g(h(t)) = 1$
5. $y(x) = r(h(x))$ is a solution.

Shows an example where step 4 fails. Need a theorem of Ritt on invertibility in radicals.

Suppose w s a radical function with a radical inverse, and $\overline{g}$ is polynomial. Then can use $g = \overline{g}(w(t))$.

Note that it is possible to reduce the degree of an AODE by 1, writing $y' = u(y)$. Example: $y_4'^6 9yy'2 - 7 = 0$ has a complicated parametrisation that was simpler our way. Also an example with a genuine genus 1 curve.

Note that in general we have a semi-decision procedure. There are first results on the generalisation to PDEs.[1]

[1] CASC 2014.

5.3 On the reduction of Singularly-Perturbed Linear Differential Systems

$$\epsilon \frac{dT}{dX} = A(x,\epsilon)Y = \epsilon^{-h} x^{-p} sum \dots$$

This reduced to solving non-homogeneous singular linear differential equations. Get different (annular) codomains around a singularity.

Note that the unperturbed system has had major advances in the last two decades. Goal: give an efficient algorithm for the computation of ...

1. Formal Reduction. A fundamental matrix of formal solutions $\Phi(x^{1/\alpha}) \cdots$ [Barkatou, Pfluegel]. Look for a change of basis, either reducing the dimension or the Poincaré rank. This gives recursive reduction [**?**]. The key is the leading coefficient matrix. Two distinct eigenvalues means we can split the system.

   If there is only one eigenvalue, we do eigenvalue shifting. $m(A)$ is the Moser rank $\max(0, p + \frac{rank(A+0)}{n})$. There is a criterion for Moser-irreducibility [Moser1960]: if not met, we can reduce. [BP09].

2. Resolution of Turning points. If A_0 depends on x then the eigenvalues are power series, and we uncouple over power series. If $A_0(0)$ is nilpotent but A_0 is not, we get *turning points*. $A_0(x)$ has a turning point if its Jordan form is unstable. Then there is a ramification $s\ x - t^s$, and we can then apply the splitting lemma.

3. Moser-based reduction. then has to be done over a bivariate field? Needs, apparently, to ramify in ϵ as well.

Hence the next talk!

5.4 Formal Solutions of a Class of Pfaffian Systems in Two Variables

Assume a linear system of PDEs

$$x_1^{p_1+1} \frac{\partial Y}{\partial x_1} = A^{(1)}(x)Y, \dots . \tag{5.1}$$

$(p_1, \dots)$ is the Poincaré rank. $A^{(i)} \in \mathcal{M}_n(\mathcal{O})$. Integrability conditions. We do not have the turning point problem, but other ones.

1. Generalise ODEs. Let $\Delta_i = x_i^{p_i+1} \frac{\partial}{\partial x_i - A^{(i)}(x)}$. These operators commute. It is possible to triangularise the matrix, hence a univariate problem. This is our formal reduction. [many]. Aim: to compute a Fundamental Matrix of Formal Solutions for the bivariate problem. However, the generalisation of the previous talk is not simple, as a change of basis in one component can affect the other, sometimes badly.

2. Computing exponential parts. Note also that x_1 and x_2 can both ramify, with $\exp(Q_i(x_i^{1/s_i})$. Matrices Q_1, Q_2 are invariant under gauge transformations. If not zero ,the origin is an irregular singular point.

3. Rank reduction. Again, this is harder than the first talk. [Deligne1970] regularity of the system is equivalent to the regularity of the individual systems. Can reduce the Moser ran via either unimodular transforms *good) or polynomial transformations based on $\mathrm{diag}(x^{\alpha_i})$, which don't interfere with the other system.

Aim to generalise this to $m > 2$. The exponential part seems to go through.

Q (5.1) is a very special form of singularity.

A Yes: the mixed singularity is more difficult.

5.5 Unimodular Completion of Polynomial Matrices: Labahn

Given a non-square matrix, how to complete it to be unimodular (determinant constant). This came out of our Fast Polynomial Arithmetic Programme. Note that completing F by G is only possible if there is an unimodular U such that $F \cdot U = [I_m, 0]$. We should produce an

Note that in the case of multivariate polynomials this solves Serre's conjecture [Quillan–Suslin Theorem]. Multivariate differential polynomial matrices have also been considered.

Example 7 (1×2 **case)**

$$\begin{pmatrix} u & w \\ v & z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Need column degrees, shifted column degrees, leading coefficient matrix, shifted leading coefficient matrix. "Shifted" $\mathrm{lcoeff}_{d_1,\cdots,d_m}$ etc. means multiply columns by x^{d_i} and then take lcoeff. Need to reverse a polynomial p to get $p^* = x^d p(1/x)$. For matrix polynomials look at $x^{-\mathbf{d}_1} M(1/x) x^{-bfd_2}$.

All costs $\tilde{O}(n^\omega s)$.

5.6 LLL Reducing with the most significant bits: Villard

Paper has two aspects: only talk about one (the other is scaling).

Example: NTRU system [HPS98].. Recently [NKM2010] tried to extend to NTRU with real numbers. [Buc94] related the number of digits to the log of the orthogonality defect, and this is what we will improve.

Coppersmith bases [BietalPC2014]. Noticed that there is special structure. $O(d) + \log \frac{\max a_{ii}}{\min a_{jj}}$ digits. Our contribution is that, in general, one can use fewer digits.

"QR is the same as the Gram–Schmidt you learned at school".

Error in Gram–Schmidt. If we replace A by $A + \Delta A$, when A reduces to AU, does $A + \Delta A$ also reduce by U. The amplification of the error is the "condition number cond(R)" (not the real one) of the transformation matrix R: $|| \, |R| \cdot |R^{-1}| \, ||$. Even if we end up in the right place, the reduction might not be quite as good. If B is (δ, θ, η)-reduced, $B + \Delta B$ is only $(\delta', \theta', \eta')$-reduced.

But LLL is multiple Gram–Schmidt. In fact only need cond$(R)^2$. Have tight bound, and good practical savings.

5.7 Wilson's notes

5.7.1 Asymptotic analysis of interpolated recurrence relations

Consider recurrence relations viewed as either a class of recurrence relations, an iterated functinal compostition, or a discrete dynamical system.

Consider interpolating the system: looking for a continuous $Y : \mathbb{C} \to \mathbb{C}$ such that $Y(n) = y_n$. Can be used for asymptotic analysis or fractional functional iteration.

Given a sequence $\{y_n\}$ determined by $y_{n+1} = y_n \phi(y_n)$ there exists a function with an explicit formula (arises from Lagrance inversion).

Related to the Lambert W function and the Wright ω function (`Wrightomega` in Maple). Have to appeal to branch cuts of Lambert W and use the unwinding number (`unwindK` in Maple). Wright ω solves $y + \log y = z$ for $y = \omega(z)$ (except for some special cases).

5.7.2 Evaluating parametric holonomic sequences using rectangular splitting

Compute the nth entry in a sequence satisfying a linear recurrence relation: expressed as a vector multiplied by a square matrix with entries that are polynomials in n. Computing elements can be done recursively but better to work out the product $M(n)M(n-1)\cdots M(1)$ and mulitplying by the initial vector. Can also do binary splitting (divide and conquer). Can do fast multipoint evaluation (useful if arithmetic operations have a fixed cost).

Considering case where M involves an extra parameter x. Want to evaluate at an expensive value of x (such as x being π to high accuracy). Adding coefficients or the parameter is relatively cheap, but multiplying x with itself is very expensive. Can appeal to rectangular splitting.

In practice, the coefficients grow very large to the point where scalar multiplications become slower than the the non-scalar multiplications. Can get better

rectangular by expanding $O(\sqrt{n})$ polynomials of $O(\sqrt{n})$. Through this you can get a speed up factor of $\sqrt{500}$.

5.8 On isomorphisms of modules over non-commutative PID

Note that we don't have unique factorisation, e.g. over $\mathbf{F}_4$

$$(x^2+1) = (x+1)(x+1) = (x+a)(x+a+1).$$

Two elements a, $b \in R$ are similar ($\sim$) iff ....

Theorem 12 (structure theorem) *Any finitely generated left R-Module M can be written*

$$M \equiv \underbrace{R^s}_{\textit{free part}} \oplus \underbrace{\frac{R}{Ra_1} \oplus \cdots \oplus \frac{R}{Ra_n}}_{\textit{torsion part}}.$$

We need a similarity test. Impose some restrictions. Under these conditions, R has finite rank over its centre.

Proposition 5 *R/RF is centrally bounded iff f x-torsion-free iff $(f,x)_r = 1$*

There is a solutions for non-x-torsion-free polynomials. There is an algorithm for similarity in the generic setting.

The reduction to cyclic [Jacobsen1934] is a generalisation of Smith normal form.

5.9 Factoring Differential Operators in n Variables: Heinle

K is always of characteristic 0. Write $\underline{n}$ for $\{1,\ldots,n\}$, also $\underline{v} = \{v_1,\ldots,v_n\}$.

Rational Weyl algebra:

$$\partial_i x_j = \begin{cases} x_j\partial_i & (i \neq j) \\ x_j\partial_i + 1 & (i = j) \end{cases}. \tag{5.2}$$

Shows a one-line polynomial with 3407 distinct factorisation. Polynomial Weyl algebras have only finitely many factorisations (just proved by us), but for rational ones infinitely many is possible This talk is about nth Weyl algebra: skipping over shift Weyl and q-Weyl today.

We introduce a $\mathbf{Z}^n$-grading on A_n with weight vector $[-,v]$, with for simplicity $v = [1,\ldots,1]$. With this the commutation rule (5.2) is homogeneous.

Compared our `ncfactor.lib` (Singular)[2] with Reduce, and ($n = 1$) to Maple's `DETools`, and it's much faster.

[2] To be bundled in the next Singular release

5.10 Solving Higher Order Linear Differential Equations having Elliptic Function Coefficients: Burger

nth order homogeneous linear ODE, where the coefficients are elliptic functions. Want hyperexponential solutions.

Elliptic Doubly-periodic and meromorphic.

Weierstrass functions $\mathfrak{p}, \mathfrak{p}'$: $(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3 =: \omega(\mathfrak{p})$. Any elliptic function can be expressed as a rational combination of $\mathfrak{p}, \mathfrak{p}'$.

Picard's Theorem If the general solution of DE is path-independent, then there is a solution hyperexponential over $\mathbf{C}(\mathfrak{p}, \mathfrak{p}')$, i.e. over $\mathbf{C}(z, \sqrt{\omega(z)})$.

Want solutions $y = \exp(\int r(x)dx)$: consider the partial fraction expression of r. There can be poles that are *not* poles of the coefficients of the ODE.

Can't use Maple's `gen_exp` directly, but get round this by using $\overline{L}$ as well as L. In general, for an nth order ODE, there are $n^2 - 1$ (e, f) pairs to resolve.

5.11 Online order basis algorithm and its impact on block Wiedemann algorithm

Integer factorisation, discrete logarithm etc. all need fast implementations. Also algebraic K-theory.

1. choose random $u, v \in \mathbf{K}^{n+1}$
2. Compute the sequence $S = (S_i(_{i \in \mathbf{N}}$ of projections $S_i = u^T A^i v$
3. return the minimal polynomial Π.

But in fact we do it in blocks of size m. Then step 3 is challenging, e.g. [Cop94]. Note that block is more likely to success if $\mathbf{K}$ is small.

How many terms do we need. Worst case is $2n$. Generically $2N/m + O(1)$. If you know the rank, you can precondition A.

The K-theory matrices have 29–46% rank deficiency. Hence also want early detection/termination.

heuristic [Lobo1995,KaltofenLee2003] look for stability of Π.

deterministic using determinental degree.

Alternatively, keep doubling the precision of S, and Π This means we can only stop at power s of 2.

Our contribution is to link the two and do a fast online algorithm for Π.

Definition 15 *Let (F, σ) be the $\mathbf{K}[x]$-module $\{v \in \mathbf{K}[[x]]^{1 \times m}$ such that $vF = 0 \pmod{x^\sigma}$*

Our algorithm is online in the sense that it only reads $F \pmod{x^\sigma}$ when computing $\pmod{x^\sigma}$.

"Shifted online middle product algorithm". $\tilde{O}(m^\omega \sigma)$. Shows relative performance of on-line against best off-line — his is no more than $\times 2$, whereas previous was worse as order increased, up to $\times 64$.

Implemented in LinBox, soon to be released.

5.12 Essentially Optimal Interactive Certificates in Linear Algebra

Same example as previous. GL7d19 1911130×1955309 matrix. 1050 CPU days gave rank 1033058. How do you believe this? Also important for cloud computing.

Frievalds for LU Prover exhibits P,L,U,Q.

Verifier Checks that these are permutation, triangular matrices. Then check $Av - P(L(U(v)))$ for random v.

This doesn't work in cases where the prover chooses p, because could be a bad prime. [KNS11] return n^2 primes (too many for all to be bad) and prover checks a few at random. Problem is the size of the certificate.

It would be better if the verifier could choose the prime.But the problem is that the certificate is not verifiable by a third party who didn't choose p. So use Fiat–Shamir derandomisation. Prover chooses p =NextPrime(CryptHash(A)).

[KV04] uses integer characteristic polynomial. Note that this is worse than n^ω: $n^{2.5}$ even if $\omega = 2$.

5.13 Linear independence oracles and applications to rectangular and low rank linear systems

Given $A \in \mathbf{K}^{n \times m}$ compute the rank r and lexicographically minimal list of row indices such that they are independent. Also given $b \in \mathbf{K}^{n \times 1}$, compute a solution to $Ax = b$ or a certificate of inconsistency. Our cost model is that K is finite and we count scalar operations in K. Let $|A|$ be the number of nonzero in A. Let $\mu(A)$ be the time required to compute Av in a black-box model.

[Dumasetal2013] Rank Profile on $O(nmr^{\omega-2})$ deterministic.

[KS91] probabilistic.

Note [MS00] gives us oracle linear solving in $O((n+m)r^2)$. Goals:

1. decouple the cubic part

2. exploit sparsity of A: $2r^3 + (r^2 + |A|)^{1+o(1)}$

3. incorporate fast matrix multiplication, say $(r^\omega + |A|)^{1+o(1)}$

Computing with linear independence oracles (seems to be a tree-based solution: not fully understood by JHD).

Q What data structure?

Q–EK Las Vegas?

A Monte Carlo

Chapter 6

Rikkyo University 31 July

6.1 JHD

Spoke on "Cylindrical Algebraic Decomposition: from Polynomials to Formulae".

6.2 Formula simplification by Boolean function manipulation: Iwane

This is in the context of the Todai project. Example from Hokkaido 2011: Sphere centred at (a, b, c): where does in mean the line $(t + 2, t + 2, t)$. We can eliminate r and t by QE. But the NLP builds a much more complicated FOF. FOf constructed by robot often contains equational constraints. We use VTS for Equational constraints. The output of these specialised QE is very redundant. Hence we need simplification of intermediate formulae.

Sign-Definite Conditions [AnaiHarak2000]. $\forall x(x \geq 0) \Rightarrow f(x) > 0)$. These SDC crop up in Fujitsu's Parametric Robust Control Toolbox.

Sturm–Habicht

Example Quadratic problem.

VTS used for output simplification. Apparently have had success in the cubic case as well.

Logic minimisation should also be applied.

	Human	NLP
Variables	5	19
Quantifiers	2	16

Q Source of Espresso?

A No — black box.

6.3 Quantifier Elimination based on Comprehensive Gröbner Systems: Fuaksaku

Definition 16 *$\overline{x} = (x_1, \ldots, x_m)$ variables and $\overline{A} = (a_1, \ldots, a_m)$ parameters. $\{S_1, \ldots, S_t\}$ is a partition of K^m. Then $\{(S_1, G_1), \ldots, (S_t, G_t)\}$ is a* comprehensive GB *...*

Theorem 13 ([PRS93]) $\text{sign}(Q) = \#\{\overline{X} \in \mathbf{R}^n : f(\overline{X}) = 0 for f \in I\}$.

Apply Descartes.

6.3.1 Basic Algorithm

Input Simple conjunction

Output

1. Introduce new variables for every polynomial $\neq$, $>$ or $\geq$.

2. Compute CGB.

3 for each G_i,if zero-dimensional add the result of GBQE, otherwise use another QE system

6.3.2 GBQE

1. Let V be a basis for the residue class ring.

2.

Example 8 (Worked in Mathematica) $\exists x : x^2 + ax + b$??. *Note that* $^2 + ax + b$ *is always a GB— no problem. $V = \{1, x\}$. Various matrices $M_{i,j}$, and the matrix of traces is ....*

Gets a very complicated formula equivalent to "discriminant > 0". This involves also $-2 - a^2 + 2b$, which came out as a coefficient in his manipulation.

On a more complicated one, computes in 5 seconds on top of Mathematica, with a DNF of length 20. Other systems don't terminate. Currently using Mathematica's `BooleanMinimise`, but would like to use Expresso in future.

Bibliography

[AR14] A. Arnold and D.S. Roche. Multivariate sparse interpolation using randomized Kronecker substitutions. `http://arxiv.org/abs/1401.6694`, 2014.

[BD07] C.W. Brown and J.H. Davenport. The Complexity of Quantifier Elimination and Cylindrical Algebraic Decomposition. In C.W. Brown, editor, *Proceedings ISSAC 2007*, pages 54–60, 2007.

[BOT88] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proceedings 20th. Symp. Theory of Computing*, pages 301–309, 1988.

[BP09] M.A. Barkatou and E. Pflügel. On the Moser- and super-reduction algorithms of systems of linear differential equations and their complexity. *J. Symbolic Comp.*, 44:1017–1036, 2009.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden des basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Math. Inst. University of Innsbruck, 1965.

[Buc94] J. Buchmann. Reducing lattice bases by means of approximations. In *Proceedings 1st Algorithmic Number Theory Symposium*, pages 160–168, 1994.

[CKS99] F. Cucker, O. Koiran, and S. Smale. A Polynomial Time Algorithm for Diophantine Equations in One Variable. *J. Symbolic Comp.*, 27:21–29, 1999.

[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.

[Cop94] D. Coppersmith. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. *Math. Comp.*, 62:333–350, 1994.

[CT91] P. Conti and C. Traverso. Buchberger algorithm and integer programming. In *Proceedings AAECC 9*, pages 130–139, 1991.

[DH88] J.H. Davenport and J. Heintz. Real Quantifier Elimination is Doubly Exponential. *J. Symbolic Comp.*, 5:29–35, 1988.

[DR13] J. Draisma and J. Rodriguez. Maximum likelihood duality for determinental varieties. *Intern. Math. Research Notices*, 2013.

[DZ05] B.H. Dayton and Z. Zeng. Computing the multiplicity structure in solving polynomial systems. In *Proceedings ISSAC 2005*, pages 116–123, 2005.

[ELLP07] H. Everett, D. Lazard, S. Lazard, and M. Pouget. The Voronoi diagram of three lines in $\mathbf{R}^3$. *SoCG '07: Proceedings of the 23-rd annual symposium on computational geometry*, pages 255–264, 2007.

[FG04] R. Feng and X.-S. Gao. Rational General Solutions of Algebraic Ordinary Diferential Equations. In J. Gutierrez, editor, *Proceedings ISSAC 2004*, pages 155–162, 2004.

[FM13] J.-C. Faugère and C. Mou. Sparse FGLM algorithms. `http://arxiv.org/abs/1304.1238`, 2013.

[GKZ12] F. Guo, E.L. Kaltofen, and L. Zhi. Certificates of Impossibility of Hilbert-Artin Representations of a Given Degree for Definite Polynomials and Functions. In *Proceedings ISSAC 2012*, pages 195–202, 2012.

[GMN+91] A. Giovini, T. Mora, G. Niesi, L. Robbiano, and C. Traverso. One sugar cube, please, or selection strategies in the Buchberger algorithm. In S.M. Watt, editor, *Proceedings ISSAC 1991*, pages 49–54, 1991.

[Hon90] H. Hong. *Improvements in CAD-Based Quantifier Elimination.* PhD thesis, OSU-CISRC-10/90-TR29 Ohio State University, 1990.

[HPS98] J Hoffstein, J. Pipher, and J.H. Silverman. NTRU: a Ring-based Public Key Cryptosystem. In J. Buhler, editor, *Proceedings 3rd Algorithmic Number Theory Symposium*, pages 267–288, 1998.

[IMAA14] H. Iwane, T. Matsuzaki, N.H. Arai, and H. Anai. Automated Natural Language Geometry Math Problem Solving by Real Quantifier Elimination. In *Proceedings ADG 2014*, 2014.

[IYAY13] H. Iwane, H. Yanami, H. Anai, and K. Yokoyama. An effective implementation of symbolic-numeric cylindrical algebraic decomposition for quantifier elimination. *Theoretical Computer Science*, 479:43–69, 2013.

[Jir97] M. Jirstrand. Nonlinear control system design by quantifier elimination. *J. Symbolic Comp.*, 24:161–187, 1997.

[Kal85] E. Kaltofen. Effective Hilbert irreducibility. *Information and Control*, 66:123–137, 1985.

[KLYZ08] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact Certification of Global Optimality of Approximate Factorizations Via Rationalizing Sums-Of-Squares with Floating Point Scalars. In D.J.Jeffrey, editor, *Proceedings ISSAC 2008*, pages 155–164, 2008.

[KNS11] E. Kaltofen, M. Nehring, and B.D. Saunders. Quadratic-Time Certificates in Linear Algebra. In *Proceedings ISSAC 2011*, pages 177–185, 2011.

[KR00] M Kreuzer and L. Robbiano. Computational commutative algebra 1. *Springer-Verlag*, 2000.

[KS91] E. Kaltofen and B.D. Saunders. On Wiedemann's Method of Solving Sparse Linear Systems. In L. Huguet and A. Poli, editors, *Proceedings AAECC-5*, pages 29–38, 1991.

[KV04] E. Kaltofen and G. Villard. Computing the sign or the value of the determinant of an integer matrix, a complexity survey. *J. Comp. Appl. Math.*, 162:133–146, 2004.

[Len99] H.W. Lenstra Jr. On the factorization of lacunary polynomials. *Number theory in progress*, pages 277–291, 1999.

[LW93] R. Loos and V Weispfenning. Applying Linear Quantifier Elimination. *Computer J.*, 36:450–462, 1993.

[MIA13] Y. Matsui, H. Iwane, and H. Anai. Two controller design prcedures using SDP and QE for a Power Supply Unit. *Development of Computer Algebra Research and Collaboration with Industry*, pages 43–52, 2013.

[MP12] M. Monagan and R. Pearce. POLY : A new polynomial data structure for Maple 17. *Comm. Computer Algebra*, 46:164–167, 2012.

[MS00] T. Mulders and A. Storjohann. Rational Solutions of Singular Linear Systems. In C. Traverso, editor, *Proceedings ISSAC 2000*, pages 242–249, 2000.

[PRS93] P. Pedersen, M.-F. Roy, and A. Szpirglas. Counting Real Zeroes in the Multivariate Case. In *Proceedings MEGA '92*, pages 203–224, 1993.

[Rat02] S. Ratschan. Approximate quantified constraint solving by cylindrical box decomposition. *Reliable Computing*, 8:21–42, 2002.

[Sch06] M. Schweighofer. Global optimization of polynomials using gradient tentacles and sums of squares. *SIAM J. Optimization*, 17:920–942, 2006.

[Sch12] C. Scheiderer. Descending the ground field in sums of squares representations. `http://arxiv.org/abs/1209.2976`, 2012.

[Slo03] N.J.A. Sloane. The Online Encyclopedia of Integer Sequences. *Notices A.M.S.*, 50:912–915, 2003.

[ST11] Thomas Sturm and Ashish Tiwari. Verification and synthesis using real quantifier elimination. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, pages 329–336. ACM, 2011.

[Stu91] B. Sturmfels. Gröbner bases of toric varieties. *Tôhoku Math. J.*, 43:249–261, 1991.

[Stu95] B. Sturmfels. Gröbner Bases and Convex Polytopes. *Amer. Math. Sci.*, 1995.

[Stu96] T. Sturm. Real quadratic quantifier elimination in RISA/ASIR. Technical Report Memorandum ISIS-RM-5E ISIS Fujitsu Laboratories Limited, 1996.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* 2nd ed., Univ. Cal. Press. Reprinted in *Quantifier Elimination and Cylindrical Algebraic Decomposition* (ed. B.F. Caviness & J.R. Johnson), Springer-Verlag, Wein-New York, 1998, pp. 24–84., 1951.

[Wei94] V. Weispfenning. Quantifier elimination for real algebra — the cubic case. In *Proceedings ISSAC 1994*, pages 258–263, 1994.

[Wei97] V. Weispfenning. Quantifier elimination for real algebra — the quadratic case and beyond. *AAECC*, 8:85–101, 1997.

[Wil12] D.J. Wilson. Polynomial System Example Bank. `http://opus.bath.ac.uk/29503`, 2012.