SIAM Applied Algebraic Geometry 2013

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

24 June 2013

Contents

Part I

Thursday 1 August 2013

Chapter 1

Invited — Ravi Vakil

How Applied Algebraic Geometry is Useful in Pure Mathematics.

"Hartshorne [Har77] brought Grothendieck's message down from the mountains". These days we should look at [CLO06]. Here are some examples.

1.1 Gröbner bases

Pure mathematicians said "so what" about [Buc65] initially, but I was converted by Sturmfelds. There are links to toric varieties, polytopes and probably to tropical geometry (which initially erupted in Computer Science).

1.2 Intersection Theory on the Moduli Space of Curves

Curves over $\mathbf{C}$ are Riemann surfaces. Consider genus 2. See Riemann, Mumford, Deligne–Mumford, Witten, Kontsevich etc.

Hau Xu's arguments, including his proof with Kefeng Liu of Faber's "Intersection Number" Conjecture, were much shorter than previous ones. See [J. Diff. Geom. 2009].

1.3 Galois/monodromy groups of enumerative problems

[1205.5972,1207.4280] [BMdCS12].

"How many roots does a polynomial of degree n have? — n" : except when ..., and its these exceptions that are interesting.

"The complex numbers are easy, the real numbers are hard, but when it comes to the rationals ...". The way the best results are being found in empirical.

1.4 Generalising the cross-ratio

Joint work with Howard (toric), Milson (classical), Snowden (number theorist, student of Wiles). Consider

$$x \mapsto \frac{ax+b}{cx+d}$$

Given four points on the projective line, there is one automorphism sending $p_1 \to 0$, $p_2 \to 1$, $p_3 \to \infty$, so where p_4 goes is determined: in fact by the cross-ratio.

Now consider the digraph $1 \to 2; 3 \to 4$ and we should think of this as corresponding to $(p_2 - p_1)(p_4 - p_3)$ etc. Other graphs give other products and addition of graphs is multiplication of products. Can generalise to > 4, e.g. 6, points. This is special, also 8 ....

Theorem 1 (condensed) *Except for $n = 6$, these (cross-ratio and 8-point) relations are all there are. Even "over the integers"and "with weights".*

This came out of "algorithmic thinking". The proof involved equations in 14-variables, and these were at the border of what was algorithmically possible.

Chapter 2

Developments in Cylindrical Algebraic Decomposition and Quantifier Elimination — Part I of II

2.1 JHD

See `http://staff.bath.ac.uk/masjhd/Slides/AG13Slides.pdf`.

2.2 Exact Nonlinear Optimization on Demand

Leonardo de Moura and Grant Passmore.

Idea 1 *A lazy CDCL-like approach to exact nonlinear optimization over the real numbers*

- CAD-based approach
- existential CAD on demand
- computable non-standard Real-closed fields.

Note that there are *many* real-closed fields. Since the theory is complete, we normally compute in $\mathbf{A_R}$ rather than $\mathbf{R}$. But we can add infinitesimals, when it is generally uncomputable. Work in $\overline{K}_{\mathbf{R}}$ where $K = \mathbf{Q}(t_1, \ldots, t_n, u_1, \ldots, u_m)$ (the t_i are transcendentals[1], and u_i infinitesimals.

[1] Such as π. In practice we have to assume Schanuel's conjecture.

2.2.1 Model Algorithm

- Let y be local minima, so $F(y, x_1, \ldots, x_n)$
- Eliminate x_i to produce $\phi(y)$
- Look at roots of this.

But this is too expensive, so Mathematica doesn't actually construct $\phi(y)$. But it's still too expensive.

2.2.2 nlset

Purely for the existential theory!

- Start building a model for the formula immediately, without going through a projection phase.
- When conflict arises, do "projection on demand"
- This is a real-algebraic equivalent of *conflict clauses*
- Non-chronological backtracking

See section **??** and [JovanonicdeMoura/CADE2013].

Roughly, if there's no equation in x only, pick a value for x and continue: if two (x, y) polynomials contradict, regard their resultant as a polynomial in x and backtrack.I But out decomposition of $\mathbf{R}$ corresponding to y is incomplete: where do we begin and how do we avoid missing key points?

Answer — infinitesimals. Start as $\frac{-1}{u_1} = -\infty$, and move right of this to the first key point etc.

Unfortunately, encoding α and polynomial+interval does not work if we allow infinitesimals: the field may not be Archimedean. However, Thom's Lemma *does* apply. Consider

$$RootOf(\epsilon^2 x^5 - \epsilon x^3 - \epsilon x^2 + 1),$$

see online demo. Would like to extent to $\exists\forall$ (meaning precisely this set of quantifiers).

Q–ME What projection?

A Answer: Collins–Hong, because we have assigned values. See section 6.3.

2.3 CAD for Simplification in Computer Algebra — England

Bath work [BD02] plus MapleSoft, Particularly Cheb-Terrab. Note that square root and logarithm aren't actually *functions* as such, but rather multivalued.

Hence Riemann surfaces in theory, but in practice branch cuts. Standard example:

$$\sqrt{1-z}\sqrt{1+z} \stackrel{?}{=} \sqrt{-1z^2} \tag{2.1}$$

$$\sqrt{z-1}\sqrt{z+1} \stackrel{?}{=} \sqrt{z^2-1} \tag{2.2}$$

Also [Kah87]. Is $f \stackrel{?}{=} g$ — Kahan's question, and does $f \stackrel{?}{=} h$? $f \neq g$ on the small region, but $f = h$ everywhere, despite the fact that both have branch cuts.

Note that we can work with functions with infinitely branch cuts using Maple's `solve` rather than CAD.

Q Adjacency?

A If only — DJW is thinking about this.

Chapter 3

A Tale of Two Theorems — Blekherman

A Journey into Convex Algebraic Geometry.

Claims that there is an intrinsic connection between sums of squares in real algebraic geometry and classical geometry.

Definition 1 $p \in \mathbf{R}[x_1, \ldots, x_n]$ *is* non-negative *iff* $\forall x_1, \ldots, x_n p(x_1, \ldots, x_n) \geq 0$.

Theorem 2 (Hilbert) *A nonnegative homogeneous polynomial p is always a sum of squares n three cases only*

- *Binary forms (i.e. univariate polynomials)*
- *Quadratics*
- *Ternary quartics.*

In all other cases there are counter-examples.

Definition 2 *If* $\deg X = \operatorname{codim} + 1$ *for a nonnegative irreducible variety, then* SX *is a* variety of minimal degree.

Theorem 3 (del Pezzo) *The only varieties of minimal degree are*

- *quadratic hypersurface*
- *Veronese embedding of* $\mathbf{P}^2$ *into* $\mathbf{P}^2$
- ...
- ...

Note that the Veronese Embedding takes forms of degree $2d$ n X to quadratic forms on $v_d(X)$.

Theorem 4 (B. Smith, Velasco) *Let $X \subset \mathbf{P}^n_{\mathbf{R}}$ be an irreducible real projective variety. Then sums of squares and precisely non-negatives iff $X_{\mathbf{C}}$ is a variety of minimal degree.*

Problem 1 (Hilbert 17th) *For every P nonnegative in $\mathbf{P}^n_{\mathbf{R}}$ there is a sum of squares h such that $p \cdot h$ is a sum of squares.*

Solved Artin (and Schreier). Methods were semi-algebraic.

Note that sums of squares can be solved by semi-definite programming, but non-negativity is hard. Many problems n combinatorial optimisation can be stated as minimising a quadratic function on $X = \{1, -1\}^n$. Testing for sums of squares is at least 87% as good [GoemansWilliamson].

3.1 Bounds for the multipliers

Problem 2 *Can we bound the degree of h? In particular $X = \mathbf{P}^3_{\mathbf{R}}$ and $2d = 4$, i.e. quartics in four variables (just non-Hilbert). Do quadratic h suffice?*

We have bounds for curves, but these come from Hilbert's methods rather than the more general machinery.

Q Numbers of monomials?

A We have done some work on Newton polytopes.

Chapter 4

Exact Certificates in Nonlinear Global Optimization — Part II of II

4.1 Proving Inequalities and Solving Global Optimization Problems via Simplified CAD Projection — Bican Xia

Three problems.

1. For $f \in \mathbf{R}[\mathbf{x}]$ prove or disprove $f(\mathbf{x}) \geq 0 \forall \mathbf{x}$
2. Find the minimum
3. ...

Problems 1 and 2 are classical, problem 3 is a special case of QE, there algorithms of single-exponential complexity [Ren92a, Ren92b, Ren92c].

We propose a simplified version of Brown's projection operator.

Example 1 (Problem 1) *Prove or disprove* $\forall x, y, z f(x, y, z) \geq 0$ *where*

$$f(x, y, z) = 4z^4 - 4z^2y^2 - 4z^2 + \cdots$$

$f_1 := \mathrm{Res}_z(f) = 1048576 g_1^3 g_2 h_1^2 h_2^2$ *and* $f_2 = \mathrm{Res}_y(f_1) = (\cdots)^{15} \cdots$

Our method improves on Brown at the f_2 stage, because we analyse separately the even and odd multiplicity factors of f_1. We only need the resultants of the odd factors, and the resultants and cross-discriminants of the even factors.

Lemma 1 (Weiss,1963)

Lemma 2 (Derined by us from Weiss,1963) *To show that f is positive semi-definite we need to show that the odd multiplicity factors are positive semi-definite and the even are ....*

Theorem 5 *f is positive semi-definite on $\mathbf{R}^n$ iff both*

- *The polynomials in $\mathtt{Nproj}_1(f, x_n)$ are positive semi-definite on $\mathbf{R}^{n-1}$*
- *For every connected component U of $\mathtt{Nproj}_2(f, x_n)$ there is an $\alpha \in U$ such that $f(\alpha, x_n) \geq 0$ on R and α is not a zero of any $\mathtt{Nproj}_1(f, x_n)$*

Example 2 (problem 2) *Compute minimum of a rational function.*

This maps back into problem 1, and the new projection works.

Example 3 *Find all $k \in \mathbf{R}$ such that*

$$\forall x, y \in \mathbf{R} f(x, y, k) = x^2 + y^2 - k \geq 0$$

There are "bad" values of k. The good ones work with our projection, and we treat the bad ones differently.

For a problem in n variables, our method solves one more n than any of QEPCAD, Maple and Mathematica.

Q Brown's projection needs extra checks. Do you need these extra checks?

A It wasn't clear the question was understood. The audience generally thought that, since Brown-McCallum is always valid for full-dimensional cells, this should be OK.

Q Can you parallelise the recursive step?

A Presumably.

4.2 Exact Safety Verification of Interval Hybrid Systems Based on Symbolic-Numeric Computation — Zhengfeng Yang

Much previous research [YWL13] etc..

A hybrid system is discrete transitions coupled with continuous evolutions. Many cyber-physical systems can be modelled this way, but we may need an *uncertain hybrid system*, where there is an uncertainty parameter $\mathbf{u}$. Instead we will use interval methods.

Definition 3 *Given an* initial region $\Theta \subset \mathbf{R}^n$ *and an* unsafe region $\Psi \subset \mathbf{R}^n$, *the* safety problem *is to show that no path starting in Θ ends in Ψ.*

We would like to produce a separating hyperplane between Θ and Ψ such that the trajectory can never cross this. This is basically an invariant generation problem. We use Sum-Of-Squares relaxation, and Rational Vector Recovery [KLYZ12, YWL13]. Existing technology solves most problems, but we also need to verify that an *interval* polynomial is non-negative.

Quadrant Decomposition when computation of the lower bound over the whole interval doesn't work.

Interval Computation Let $g(\mathbf{x}) = m(\mathbf{x})^T \cdot W \cdot m(\mathbf{x})$ and $W \geq 0$ then $g(\mathbf{x}) \geq 0$. Compute this representation fro the midpoint of the interval polynomial to get $\widehat{W}$. If this is ≥ 0 and of full rank, we can proceed as in [Rum10]. But $\widehat{W}$ singular is more difficult — he gave details I didn't follow.

Non-polynomial systems can be handled by functional approximation (Taylor, continued fractions) and the error term regarded as making this an interval hybrid problem.

4.3 Computing Rational Solutions of Linear Matrix Inequalities

Presented by Safey El Din.

Definition 4 *Indeterminates $X_1, \ldots, X_k$, symmetric $D \times D$ matrices $A_0, \ldots, A_k$, and a linear matrix inequality $A = A_0 + X_1 A_1 + \cdots \geq 0$, meaning that all eigenvalues ≥ 0. Let $\mathfrak{S} = \{x : this\}$. We want the* rational *part of $\mathfrak{S}$.*

Motivation — algebraic certificates of positivity. [Sch12] shows that there is an example which only has SOS over the reals, not over the rationals. See [SEDZ09], but $O(\tau^{O(1)} M(d,n)^{O(M(d,n)^6)}$ with $M(d,n) = \min(n^d, \ldots)$.

$D = 1$, $k = 1$ are trivial. If $\dim \mathfrak{S}(A) = k$, we use the critical point method. Otherwise we write $A' = P^* A P = \begin{pmatrix} L_1 & \ldots & L_D \\ \vdots & \tilde{A} & \\ L_D & & \end{pmatrix}$ and if $L = 0$ has solutions, we use Gaussian elimination to reduce the size and recurse, and otherwise the answer is that $\mathfrak{S} \cap \mathbf{Q}^k = \emptyset$.

[Sch12] gives 6 inequalities with 6 indeterminates of maximal degree 6, solved in 82.8 seconds with RAGLib. This showed that the full-dimensional case showed that $\mathfrak{S} \cap \mathbf{Q}^k = \emptyset$, but we also have to rule out the lower-dimensional case (apparently not in [Sch12]).

4.4 Polar Varieties and Global Optimization — Safey El Din

Note the change of title, was originally "Polar Varieties and Algebraic Certificates"

Definition 5 *$F = (f_1, \ldots, f_p) \subset \mathbf{Q}[X_1, \ldots, X_n]$ and $G \in \mathbf{Q}[X_1, \ldots, X_n]$. D is the maximum degree of all of these. Let V be the common zeros of F. Want to compute $g^* = \inf_{\mathbf{x} \in V \cap \mathbf{R}^n} G(\mathbf{x})$*

From the Real Algebraic Geometry point of view we have CAD, where n is limited to 4 by doubly exponential behaviour [DH88, BD07], but works, and singly-exponential methods [Ren92a, Ren92b, Ren92c] which are not implemented. Then there are the sum-of-squares methods.

There are methods based on Schmüdgen's theorem, and methods around Schweighofer which also look at limit points. For this we need the *polar variety* $W_{I,G}$ associated to $V(F)$ and G. This variety also encodes the question of the rank of a modified Jacobian of F and G being deficient. However, we make a regularity assumption that the rank of the ordinary Jacobian of F is not deficient.

Claims that this method is cubic in $(pD)^n$. See `http://www-polsys.lip6.fr/~greuet`. Uses FGb. For example a random problem with $n = 11, D = 2$ and 2 constraints can be solved in 5.3 hours.

Part II

Friday 2 August 2013

Chapter 5

Baryshnikov

Exotic Configuration Spaces

For a topological space X, its (coloured) configuration space is the collection of $n$tuples of distinct points in X, i.e. $X^n \backslash$all diagonals. The uncoloured one is obtained by quotienting out by S_n. The configuration space of $\mathbf{R}^2$ has Poincaré polynomial $(1_t(\cdot \cdots \cdot (1 + (n-1)t)$. Of importance in theoretical robotics and beyond.

Björner and Lovász introduced the "No-k-equal space" $\mathrm{conf}_k(X, n)$ which is $X^n \backslash$ all k-diagonals. More generally assume with have a finite set $\mathfrak{F}$ of types of particles. For example, two types, which may not coincide: $\mathrm{conf}_{1,1}(X, n, m)$ which is $X^{n+m} \backslash$ all diagonals of mixed type.

Suppose we have an algebraic decision tree, which is a computational model based on a "universal covering" of a flow-chart. Yao–Björner–Lovász model. The total Betti number (of the decision set) leads to lower bounds on the volume (depth) of the algebraic decision trees $\Omega(\log \beta(C))$, where the constants depend on the degree of the polynomials and the dimension d. Estimates through the Euler characteristic of C are weaker.

Another application is in control theory. $\dot{x} = f(x, u)$ and we are int rested in feedback stabilisation. This gives us some necessary conditions.

The manifolds for no-k-equal Over $\mathbf{R}$) have great similarities with braid arrangements (over $\mathbf{C}$). Both are of codimension 2. He has a relationship between the Euler characteristic and the total Betti number.

More generally, to understand the cohomology even for usual configuration spaces is difficult (but see Totaro's work for smooth complex projective varieties). We will therefore aim at the easier task of Euler characteristics. The triangulation theorem allows us to assume that X has a stratification satisfying local conicity. The allowed interactions between points of different types are governed by $I \subset \mathbf{N}^{|\mathfrak{F}|}$. Then he has a formula for the Euler characteristic as a product over all strata.

Q There are motivic versions for other characteristics. These become nice when the number of points goes to infinity. So what happens for you when the

number of points goes to infinity?

A I have no idea. But motivic ζs are an interesting topic.

Q Are the Betti numbers unimodal?

A Good question!

Chapter 6

Developments in Cylindrical Algebraic Decomposition and Quantifier Elimination — Part II of II

6.1 An Incremental Algorithm for Computing Cylindrical Algebraic Decomposition and Its Application to Quantifier Elimination — Changbo Chen

Definition 6 (Cylindricity) *Two subsets A and B of $\mathbf{R}^n$ are* cylindrically arranged *if, for any $k < n$, the projections of A and B onto $\mathbf{R}^k$ (the first k coordinates) are either equal or disjoint.*

- Original scheme from [Col75] or variants, known as PCAD. We either use a strong operator (Collins) which does too much, or a weak operator (McCallum) which may fail
- Therefore develop a system based on triangular decompositions, which makes case discussions during the projection

Definition 7 *Let $S \subset \mathbf{C}^{n-1}$ and $P \subset \mathbf{C}[x_1, \ldots, x_n]$. We say that P separates above S if for every $\alpha \in S$*

- *For each $p \in P$, $lc_{x_n}(p) \neq 0$*

- *The polynomials $\Phi_\alpha(p)$ are square-free and relatively prime.*

Example 4 *The quadratic ax^2+bx+c: if $a=0$ the question $b\stackrel{?}{=}0$ is vital, but doesn't matter if $a\neq 0$. Hence a smaller tree.*

6.1.1 Incremental

See [Laz91, MM99, etc].

Example 5 *Start with a y^2+x sign-invariant complex tree: $x\stackrel{?}{=}0$ with $y\stackrel{?}{=}0$ (if $x=0$) or $y^2+x\stackrel{?}{=}0$ (otherwise). Then refine with y^2+y. $x=0, y\neq 0$ needs a split for $y=1$ etc.*

If we have equations, then we can have a *partial cylindrical tree*, only handling the = branches.

Given a complex cylindrical tree, it is easy to deduce a real tree.

Given a real cylindrical tree, propagate the truth value of the formula. Then reflect any quantification back up the tree as far as appropriate. If signs of initial polynomials are not sufficient, use Thom's lemma.

6.1.2 Maple

The universal tree is always up-to-date. This basic algorithms is never slower than [CMMXY09], and sometimes much faster. If we take into account that some of the polynomials are equations, much faster again, and in this context is comparable with Mathematica.

6.2 An Application of Quantifier Elimination to Automatic Parallelization of Computer Programs — Moreno Maza

We are largely looking as nested for loops. Standard techniques, (polyhedron model) introduce linear equations/inequalities.However, CUDA can introduce nonlinear constraints in the parameters introduced.

Traditional Just replace `for` by `parfor`.

Polyhedral e.g. for Pascal's triangle computations, need a change of coordinates of the loop space. [Feautrier] and students, among others.

- Dependency Analysis, produces a polyhedron in the space defined by the loop variables.
- Parallelization: produce a new coordinate space, and map it to time×processor number.
- Code generation. The hard part!

Now A response to [GGL05, also JSC 2006]. Regard the previous method as asking which points are *not* n the cone of another one. See `ProgramAnalysis` in Maple. The linear case is normally solver by Fourier–Motzkin elimination. Believed i the field to be $O(n^{2^d})$ for n half-spaces of $\mathbf{R}^d$

Theorem 6 (with Rong Xiao) $O(2^s(\delta+\delta^2)^1\log(d\delta T))$ *bit operations, where* δ *is the* face span*, and hence bounds number of irredundant inequalities, (which might be exponential, but need not be)*

Example 6 (Dense univariate polynomial multiplication) *Each processor computes one coefficient of the output. Uses* `QuantifierElimination` *in Maple to get the necessary case discussion, and a new routine to simplify the case output produced.*

Q–JHD Nonlinear?

A Yes if the block size is a parameter, so $n = iB + j$. Later: also non-linear boundary conditions.

6.3 Turning CAD Upside Down — Jovanović

Generalising SAT to $\exists\mathbf{R}$

Problem 3 *Is this set of equations and inequalities satisfiable — and produce a witness! Example was aeroplane collision.*

This problem is somewhere between NP and PSPACE: it encodes SAT, so is at least NP, but we come from the SAT community, so aren't too scared by this. We think of projection as being saturation of the set of polynomials, which will allow lifting to produce a model. We lift one point, and backtrack if this fails.

This is analogous to Davis–Putnam satisfiability: saturation (resolution) followed by model building. The breakthrough here is Conflict-Directed Clause Learning (CDCL). Use the search to direct the resolution: note that this starts with building, and only does resolution if it finds a contradiction. Note that the backtrack to the man variable of the clause produced by resolution.

- assign values to variables
- detect conflicts for top variables
- provides a clausal explanation for conflicts.

Example 7 $C_1 := x^2 + y^2 < 1$, $C_2 := xy > 1$. *Assign* $C_1 = C + 2 = true$. *Try* $x = \sqrt{2}/2$. *This is invalid, but that's not helpful enough. So actually use the CAD projection to produce constraints in* x *only.*

The Collins projection[1] is coefficients/(sub-)resultants/(sub-)discriminants. This is about #complex roots, # distinct roots, c̃ommon roots respectively. We are instantiated down to one variable, so only need a small subset of these (determined by the instantiation).

This is implemented as `nlsat` in the `z3` solver. On Metitarski benchmark solved 1002 versus Mathematica's 1006, but in half the time. See [JdM12].

Q What's the worst-case?

A

6.4 Relative Equilibria in the Four-Vortex Problem with Two Pairs of Equal Vorticities

Accepted to *J. Nonlinear Sciences*. Typical example might be a water-spout. Point-vortices introduced in [Helmholtz1858]. No internal structure, so just need to track them (i.e. PDE has become ODE). This is generally easier than the gravitational n-body problem (e.g.planar 3-vortex is integrable) but many techniques still apply. Note that vorticities, unlike masses, can be negative!

$$\Gamma_i = \text{Hamiltonian expressions.}$$

We are interested in relative equilibria, all rotating about a central point, which can only happen if initial locations satisfy the *central configuration equations*. There is a vortex equivalent of Lagrange's gravitational solution. Also regular n-gon (all vorticities equal if $n \geq 4$).

Problem 4 (Planar) $\Gamma_1 = \Gamma_2 = 1$*;* $\Gamma_3 = \Gamma_4 = m$ *with* $-1 < m < 1$. *There are many open problems in the gravitational equivalent*

Use the relative distances $r_{i,j}$ as coordinates, and insist on planarity (volume of tetrahedron=0). Has $r_{i,j}^2$ where the gravitational equivalent has $r_{i,j}^3$. Write $s_{i,j} = r_{i,j}^2$for simplicity. Take a Gröbner-base of all the equations.

Theorem 7 *For each* m *there are exactly four asymmetric such configurations.*

Proof is by saturation of this Gröbner-base with respect to various $s_{i,j} - s_{i',j'}$ to eliminate symmetry. Use Maple's regular chains: there are trivial solutions (vorticity zero etc.), and a non-trivial system whose quartic equation has four real roots.

In fact the author has a complete classification of all solutions, symmetric or not.

Q Was 'asymmetric' the hardest case?

A Collinear is also hard, but this one needed triangularisation.

[1] Subsequently: we normally only have one or two polynomials to look at.

Chapter 7

Numerics and Algebraic Geometry — Di Rocco

Note special issues of JSC (ex-MEGA) and of MiCS.

The interplay between Numerics and Algebraic Geometry is in both directions — generally →examples and ←tools. [DiRoccoetal2010]

7.1 Algebraic Geometry

Fundamental objects are systems of polynomial equations.

- Dimension 0 — find/describe the solutions
- Dimension > 0 — describe the variety via invariants, e.g. genus.

Of course, numerical methods only provide sample points, so one way of thinking of this is as a "big data" problem. See Bertini: `http://www3.nd.edu/~sommese/bertini`, but also Macauley2 (and in fact the two interface). Bertini uses homotopy continuation to find isolated solutions (not my own area!).

7.2 Robot Motion

Example 8 (The six-revolute serial-link manipulator) *Known that for the general 6-chain there are 16 solutions [TsaiMorgan1985,LiLiang1988].*

We want the Special Euclidean transforms $SE_3(\mathbf{R})$ is a (dense Zariski subset of) a non-singular quadratic in $\mathbf{P}^7$.

7.3 Invariants

For a generic curve we can do well. Topological Euler of C_1: $\chi_{top} = 2 - 2g = deg(c_n(C))$ where $c_n(C)$ is the top Chern class.

Theorem 8 (Bezout) *Exactly r hypersurfaces X_i whose intersection W is finite, and let $n_i = \deg X_i$. Then*

$$\prod n_i = \sum_{p \in W} m_p.$$

Example 9 (Generalised Bezout) *$X_i \subset \mathbf{P}^3$ which intersect in a smooth connected curve C such that $X_1 \cap X_2 \cap X_3 = C \cup R$, $C \cap R = \emptyset$ where R is a finite set. Then n_i, $\#R$ and g are related — there is a precise formula.*

Theorem 9 (Fulton) *Let $X_1, \ldots, X_r \subset \mathbf{P}^r$ be hypersurfaces that intersect in a connected n-dimensional smooth component Z and a finite scheme R:*

$$\bigcap X_i = Z \cup R; Z \cap R = \emptyset$$

Then $\prod n_i = e + \deg R$ where $e = \sum_i \left(\sum_j (-1)^j \binom{r+j}{j} \sigma_{n-i-j} \right) \deg c_i$.

7.4 Algebraic Statistics

The Maximum Likelihood Estimate is identified with certain algebraic varieties X, embedded in high-dimensional complex projective space.

$$\text{MLdegree}(X) = (-1)^{\dim(X)} \chi(X \setminus H)$$

in the smooth case. See [HRS12], also [HS10].

In Swedish pure/applied = clean/dirty!

Chapter 8

On Coppersmith's Heuristic Algorithm for Finding Roots of Multivariate Polynomials

Mini-symposium chaired by Damien Stehlé who subsequently agreed with JHD that [HG98] was a useful resource to explain these issues.

8.1 An Introduction to Coppersmith's Theorem and its Applications — Tibouchi

Given monic polynomial f with integer coefficients, can we find its roots.

Over $\mathbf{Z}$ Factoring a_0 is obvious, but not best: choose roots in $\mathbf{R}$ and look for approximations, or better do it p-adically?

Over $\mathbf{Z}/p\mathbf{Z}$ Berlekamp, or Cantor–Zassenhaus or ....

Over $\mathbf{Z}/p^n\mathbf{Z}$ Lift the above by Hensel's lemma.

Over $\mathbf{Z}/N\mathbf{Z}$ As above and Chinese Remainder from the factorisation?

Over $\mathbf{Z}/N\mathbf{Z}$: factorisation of N unknown As hard as factoring — see square roots mod N, which gives us a probabilistic factorisation method.

General unbreakability of RSA. Note that if $m < N^{1/3}$,$m^3 \pmod N$ is just m^3, so we can compute the cube root. Coppersmith says this generalises.

Theorem 10 ([Cop97]) *If we have a polynomials of degree d with roots $< N^{1/d}$, we can find them in time polynomial in $d, \log N$.*

Uses lattices, i.e. subgroups L of $\mathbf{Z}^m$. The LLL algorithm [LLJL82] returns a $v \in L$ with $||v|| < 2^{d/4} \operatorname{vol}(L)^{1/d}$ where $d = \operatorname{rank}(L)$.

If f has very small coefficients, its small modular roots are in fact roots over $\mathbf{Z}$: easy to find. So what we want, for general f, is a polynomial g with small coefficients which has the same root $x_0 \bmod N$. The ideal of all polynomials with root $x_0 \pmod N$ is generated by f and N. Truncate this to polynomials of degree $\leq d$, which is a lattice generated by $N, Nx, \ldots, Nx^{d-1}, f, xf, \ldots, x^{m-d-1}f$. Slight problem is the tension between $||\cdot||_1$ and $||\cdot||_2$. Per se, this is Hastad's attack, and not very good.

To get Coppersmith's full attack, we work modulo N^h where $h \approx d$. Wanted to present [HG97], but ran out of time.

8.2 The Heuristic Coppersmith Technique from a Computer Algebra Point of View — Renault

$S = \{s_1(x_1, \ldots, x_n), \ldots, s_k(x_1, \ldots, x_n)\}$ underdetermined: find small roots.

Theorem 11 ([Cop96]) *This problem for bivariates.*

8.2.1 Computer Algebra point of view

$\langle S \rangle$ is of positive dimension, so we want to add generators to make t zero-dimensional.

1. Some algebraic preparation of S to yield $T = \{f_i\}$, which also vanishes on $\mathcal{Z}$.

   - Choose just one f
   - Resultants to eliminate variables
   - Gröbner bases

   We suppose T is a Gröbner base and $\langle T \rangle$ is prime.

2. Produce some shifted g_i which also vanish on $\mathcal{Z}$ modulo some R. R is $W \cdot \prod X_j^{l_j}$ where X_j is bound on x_j at a root, $W = \max_i(||f(\ldots)||$. The g_j are monomials times R and monomials times weighted powers of f.

3. Reduce the lattice L generated by the coefficients of g_i. We hope that this will produce h_j such that $\langle f_i, h_j \rangle$ is zero-dimensional.


The lattice is no longer generated by a triangular matrix, so we don't have an easy bound on the volume on the lattice.


The $\{f_i, h_j\}$ have to be algebraically independent.

4. Extract roots. Assume that $\langle f_i, h_j \rangle$ is zero-dimensional and vanishes on $\mathcal{Z}$. $m = 1, n = 3$ — see next talk. Note [Cop01] that the problem is NP-hard (in the worst case).

Experimental conclusion — no single winner. However, Gröbner bases are always better than successive resultants.

Problem 5 (MSB) *Given many RSA moduli where the primes share (but unknown) most-significant bits, factor them.*

Done by [MaitraSarkar] for two moduli. For three, we don't get zero-dimensional. In fact the h were in $\langle f_i \rangle$, so the g_j were useless. But these are pretty small-coefficient polynomials whose coefficients are $qiq_j(p_i - p_j)$ or similar. This discovery in fact gave a *rigorous* solution for the two-moduli problem when it failed!

8.3 Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables — Bauer

Consider $p_1(x, y, z)$ where $p_1(x_0, y_0, z_0) = 0$ over $\mathbf{Z}$ at a small solution. So next compute p_2 with $p_2(x_0, y_0, z_0) = 0$ over $\mathbf{Z}$, then p_3 with $p_3(x_0, y_0, z_0) = 0$ over $\mathbf{Z}$.

Example 10 $p_1 = ax + by + cz + d$. *The monomials define a pyramid M of edge 1. Enlarge M to a pyramid of edge 2, and construct independent p_2 inside this new shape, where independence means not in $\langle p_1, xp_1, yp_1, zp_1 \rangle$. There is a lattice which will find this (JHD didn't really follow).*

This works in general with p_1 irreducible. **If** $\langle p_1, p_2 \rangle$ is prime, then any $p_3 \notin \langle p_1, p_2 \rangle$ will be independent. If necessary, we will do a prime decomposition. If $p_3 \in \langle p_1, p_2 \rangle$, then $p_3 = q_1 p_1 + q_2 p_2$, so we would like to consider a pseudodivision of p_1 by p_2. But this may not work, so we actually take a Gröbner basis of $\langle p_1, p_2 \rangle$. The monomial order must be compatible (this is a significant technical issue, and may not even be possible) with the enlarged monomial support, then we compute a similar lattice of polynomials to the above. There are also conditions on the bounds.

Q–JHD What happens if the GB has more than two entries?

A Then we get a larger lattice. Still polynomial time, of course. In practice, often $\{p_1, p_2\}$ is already Gröbner.

8.4 Polynomial Analogues of Coppersmith's Method, with Applications to List-decoding of Error-correcting Codes — Heninger

See [CH10]. Polynomial lattice basis reduction (von zur Gathen, Mulders, Stor-

Table 8.1: Dictionary

integers	polynomials with coefficients in a field
primes	irreducible
absolute value	degree
lattice over $\mathbf{Z}$	$F[z]$-module
subexponential factoring	fast factoring
SVP is NP-hard	SVP is easy
Riemann hypothesis	Riemann hypothesis proven
Cryptography	Coding Theory
finding roots of f modulo N	$\gcd(f(r(z)), N(z)) >$??
multivariate ugly	much nicer

johann).

Definition 8 *A basis is reduced if the pivots are in different columns*

Theorem 12 ([GJV03]) $n^{\omega+o(1)}D^{1+o(1)}$ *for reduction.*

Why do we care about this — factoring polynomials is easy, so why should be do this in the polynomial setting?

8.4.1 Reed–Solomon

Low-degree polynomial interpolation.

Theorem 13 (Unique decoding radius)

Theorem 14 (Efficient Algorithm) *Guruswami–Sudan via linear algebra.*

The degree of the gcd is the number of matching points.

8.4.2 Multivariate extension

Look for $Q \in \langle f_1(x_1), \ldots, f_m(x_m), N\rangle$. We actually need the m shortest vectors, not just the shortest. But in polynomial land, we can really find shortest, not just short vectors. We still have the algebraic independence problem.

In multivariate Reed–Solomon we can n fact prove algebraic independence. Claims that this tolerates more errors and is 100–1000$\times$ faster.

8.4.3 Parvaresh–Vardy codes

Define the algebraic independence away. More specifically, the code is ..., and we only need to reconstruct one polynomial from the lattice.

Also had an (integer?) application to Taiwan's smart cards, which have a RNG problem. Coppersmith bivariate worked *much* better than expected, but we got lots of algebraic **dependence**, however the shared part was related to the root we were looking for, so bad news became good news.

Part III

Saturday 3 August 2013

Chapter 9

Invited — Wiuf

Algebraic Geometry in System Biology

> Mathematics is biology's next microscope, only better, and biology is mathematics' next physics, only better —- Cohen in PLOS Biology 2004.

Two topics, but closely related. Concerned with *positive* solutions to a set of polynomial equations. Some in $\mathbf{R}[k_1, \ldots, x_1, \ldots]$, where the k_i are parameters. Also have equations in the α_i — JHD didn't quite follow the difference.

Example 11 (Signal Transduction) *Chemical reaction with four chemical species and four reaction constants* $\mathbf{k} = (k_i)$*. Write as* $\dot{\mathbf{x}} = \Gamma\nu_{\mathbf{k}}(\mathbf{x})$*, where* Γ *is the stoichiometric matrix whose columns describe the consumption/production of molecules in each equation, and* $\nu_{\mathbf{k}}$ *describes the speeds, each entry is a monomial in the* x_i*, with a constant multiplier.*

Let $\mathcal{P}$ be some (qualitative) property, e.g. "there are two steady states". We are interested in questions such as "there exists $\mathbf{k}$, α such that $\mathcal{P}$ is fulfilled.

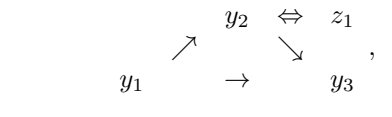
9.1 Reasoning about Models

In general rate constants $\mathbf{k}$ are unknown, or only known to within an order of magnitude. We may also be missing intermediate steps: is example 11 correct, or are there some missing species/rate constants? If we add to the model in example 11, does the new model have the same (or some of the same) $\mathcal{P}$.

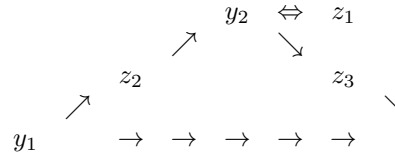
Given a base model (or core network)

$$\begin{array}{ccccc} & & y_2 & & \\ & \nearrow & & \searrow & \\ y_1 & & \rightarrow & & y_3 \end{array} \tag{9.1}$$

we can build extension models such as



(9.2)



(9.3)

and these can be ordered by set inclusion: (9.1)⊂(9.2)⊂(9.3)

Theorem 15 *If the core network has N core states for given $\mathbf{k}, \alpha$, then any extension has at least that many steady states.*

Proof; essentially elimination of variables via a Laplacian.

Also has a concept of a "maximal canonical model", and this gives him a decision tree to help model building

9.2 Relationship between Deterministic and Stochastic Models

The model above is deterministic: we can build a stochastic version by using Markov chains. There is not a clear relationship between the two — indeed we can't even use a common vocabulary. For example, the deterministic system may have a steady state, but the stochastic system wobbles. We need the concept of a *stochastic equilibrium*.

Theorem 16 *If the deterministic system has "complex balance" (an algebraic condition) then the stochastic equilibrium takes a Poisson-type (simple) form.*

Again, we have questions of inclusion of models.

Theorem 17 (See Theorem 15) *There is* stochastic convergence *between the steady states of an extension model and the steady states of the core model.*

9.3

Chapter 10

Algorithms in Real Algebraic Geometry and its Applications — Part III of III

10.1 Real analogue of Bezout's inequality — Barone

Theorem 18 (Bezout) *Let $P_i \in \mathbf{C}[X_1, \ldots, X_n]$ with $\deg P_i = d_i$, then the number of (complex) common zeros, if finite, is bounded by $\prod d_i$.*

Example 12 (non-Bezout) *Three polynomials defining complex dimension 1, but real dimension 0. Degree sequence $1, 1, 2d$, but d^2 isolated points over $\mathbf{R}$.*

What about real varieties of dimension 0? Partial answer.

Theorem 19 (Basu) *Let $Q_i \in \mathbf{C}[X_1, \ldots, X_n]$ with $\deg P_i = d_i$. Suppose the real dimension of $\mathrm{Zer}(Q_1, \ldots, Q_k, \mathbf{R}^k) = k_i$, then $b_0(V)$ depends on $d_i^{k_i - k_{i-1}}$.*

Note that "sum of squares" destroys each degree except the largest.

Theorem 20 ([GabrielovVorobjob2009a]) $O(sd)^{2k}$

Theorem 21 ([Basuetal2005]) *Sign conditions on a variety:*

Theorem 22 ([Basu2011a]) $O(1)^k (sd)^{k'} d_0^{k-k'}$ *where k' is the dimension of the variety, and d_0 is "the degree defining the variety".*

Theorem 23 (speaker) *Sum of all sign conditions $\leq$ depends on $(sd)^{k_l} \prod d_i^{k_i - k_{i-1}}$*

So why is this refined dependence so useful? See Guth–Katz solving the hard Erdős distinct distance problem.

- Given n points, an r-partitioning polynomial f exists such that each connected component of $\mathbf{R}^k \setminus \mathrm{Zer}(f)$ has .... — "polynomial ham sandwich cut".
- ...

Hence the more refined dependence on the degrees matters.

- Currently no bound on higher Betti numbers.
- What about other measures than degree — additive complexity etc.?

Q–JHD Do I read that as saying that adding a polynomial which does not decrease real dimension doesn't affect the bound?

A That's right, and I can choose the order in which I add the Q_i.

10.2 Safety Verification of Cyber-Physical Systems Using the Theory of Reals — Tiwari

Showed examples of badly- and well-designed (their methodology) controllers for car control. Three exciting developments.

- Lazy CAD and `nlsat`
- symbolic–numeric using Bernstein polynomials, which has a PVS implementation [CADE2012]. See also CMU's `dReal`, which produces a proof of unsatsifiabilty. Used in Flyspeck.
- Symbolic-numeric CAD [CADE2013], only running in a small box.

Example 13 (Car controller) *Required: distance* > 0. $v = \dot{x}, a = \dot{v}$ *is under our control. Car 2 the same, but its a is not under our control.* $\exists$*? a region* V *of state space such that for all points in it, there is an a which keeps it in the safe region, and* $V \cap danger = \emptyset$.

Example 14 (Ford) *Had a car whose automatic gearbox, on some hills, kept chattering between gears.*

Note that SMT solvers decide existence only. Note that CDCL allows one to prune many branches based on one refutation: see section 6.3.

Conclusion: the fragments $\exists$ and $\exists\forall$ are important in their own right.

10.3 Some Applications of Cylindrical Algebraic Decomposition — Pillwein

We want to prove inequalities on expressions involving discrete parameters. The inputs are infinite sequences represent by a finite about of data with algebraic structure (generally a linear recurrence equation).

Definition 9 *A sequence $f : \mathbf{N} \mapsto \mathbf{R}$ is* holonomic *if it satisfies a linear recurrence equation with polynomial coefficients.*

Some techniques for equalities, but very little for inequalities. [GK06] by induction. The induction step formula can be verified by CAD. These are much shorter than the classical proofs.

Also proved [SKP11], which is $\forall$–quantified.

Q Only Mathematica?

A At the time Maple didn't have one.

10.4 Applications of Real Numerical Algebraic Geometry — Hauenstein

interested n problems such as $\dim_{\mathbf{R}} \neq \dim_{\mathbf{C}}$. Also, even if of full dimension, very small.

Example 15 (Conics) *How many conics meet 8 lines in $\mathbf{C}^3$ in general position: answer 92. What happens over $\mathbf{R}$? Tried 15,000,000 and never got 92. Want to force complex conjugate solutions to become real, and therefore pass through discriminant locus.*

Theorem 24 *There exist 8 lines in $\mathbf{R}^3$ which are met by 92 real plane conics.*

Proof: real certification based on Smale's α-theory and `alphaCertified`, using exact rational arithmetic.

Note that algebraic information is lost when decomposing via connectivity. Consider $\sqrt[\mathbf{R}]{\langle R \rangle}$. But might not be defined over the same field, *and* therefore cannot be found by a Gröbner-like algorithm. $g(x, y) = (x^3 - 2)^2 + (y - 1)^2 \in \mathbf{Q}[x, y]$ has real radical $\langle x - \sqrt[3]{2}, y - 1 \rangle$.

For an irreducible algebraic variety V, a witness set is $\{g, L, W\}$ where g is a polynomial system with V an irreducible component of its variety ....

Definition 10 *An* isosingular *set is either ... (similar definition to irreducible).*

Example 16 *Sextic curve (oval-like plus isolated point) and*

Example 17 (With Mathers at GM) *There's a toy which is a cubic-centred 12-bar mechanism. 18 variables and 17 quadratics F. V is a union of irreducible curves in $V_{\mathbf{C}}(F)$. 6 of degree 4 ad two of degree 6, which are complex conjugate. So resolves to points in $\mathbf{R}^{18}$.*

Working on extending Bertini to do this.

10.5 The Geometry of the TDOA–based Localization

Aim: locate the source using Time Differences Of Arrival (TDOA) of a signal to distinct receivers lying n a plane. Heavily studied in Engineering. The deterministic problem is existence and uniqueness of the solution. But if the errors are non-zero, there's a statistical problem.

Example 18 (GPS, a related problem) $t_i(x) = d_i(x) + \epsilon_i + b$ *where* b *is the bias of the clock.*

10.5.1 Deterministic

Assume $\mathbf{x} \in \mathbf{R}^2$ a source, $n+1$ synchronised and calibrated receivers $m_0, \ldots, m_n \in \mathbf{R}^2$, with arrival times τ_i. Then the TDOA map $\underline{\tau}_n : \mathbf{R}^2 \to \mathbf{R}^n : \mathbf{x} \mapsto (\tau_1 - \tau_0, \ldots, \tau_n - \tau_0)$. $n = 2$ is the least value allowing injectivity of $\underline{\tau}$, hence even the possibility of uniqueness. Consider this first.There are six half-lines (from m_i heading away from m_j) where the rank of the Jacobian drops.

We have a 3D Minkowski space. Use Descartes' rule of signs to characterise the real (negative) solutions. We get a six-sided polytope, defined by the six linear factors of the discriminant. $\underline{\tau}$ is normally 1:1 in an ellipse inscribed in the polytope, but $2:1$ in polytope\ellipse.

10.5.2 Noisy

Claims that we now must consider $\underline{\tau}_n^* : \mathbf{R}^2 \to \mathbf{R}^{n+1} : \mathbf{x} \mapsto (\tau_0, \tau_1 \ldots, \tau_n)$ (JHD didn't follow this). We again have problems of uniqueness.

Chapter 11

Cluster algebra and complex volumes of knots — Inoue

11.1 Volume of a knot

Showed how a simple knot is a diagram on the edges of a tetrahedron S_3, or more accurately $S_3 \setminus$ four balls at the four vertices. More complex knots are $s_3 \setminus$ complex structures.

$$i(\mathrm{Vol}(M) + iCS(M)) = \sum_v sgn(\Delta_n) L(z_v; p_v, q_v)$$

where L is the extended Rogers dilogarithm and CS is the Chern–Simons invariant $\in \mathbf{R}$.

Had a dictionary: 2D/3D/Cluster Algebras

11.2 Cluster Algebras

Definition 11 *A cluster algebra is given by*

$(\mathbf{P}, \cdot)$ *a commutative group*

$(\mathbf{P}, \oplus, \cdot)$ *a semifield*

$\mathbf{Q}\emptyset$ *The quotient field of the group ring* $\mathbf{ZP}$.

A em seed is a triple $(Q, \mathbf{x}, \epsilon)$ *where*

Q *is a finite quiver of . . .*

Can define a mutation *of a seed at* k *to change* x_k *and* ϵ_k*, and* ϵ_j *if* j *is a neighbour of* k *in* Q.

I actually only use seeds and mutations, not really cluster algebras themselves.

Chapter 12

Exact Linear Algebra — Part I of II

12.1 Linear Algebra with Errors: On the Complexity of the Learning with Errors Problem — Albrecht

Definition 12 *Let $n \geq 1$, $m \gg n$, q odd, χ be a probability distribution on $\mathbf{Z}_q$ and $\mathbf{s}$ a secret vector on $\mathbf{Z}_q^n$. Let A be a random matrix, we send (several) $(A, c := A\dot{s}+e)$ and the recipient/attacked has to decide whether what is received really is this (? and therefore what $\mathbf{s}$ is?) or random. This is the* LWE problem.

Asymptotically hard, but what about practice?

- Bounded Distance Decoding
- Short Integer Solution — our approach.

If the error is zero, linear algebra.

[Blumetal, J, ACM 50(2003) pp. 509-519]. Gaussian elimination is really bad for noise propagation. They do good complexity.

Now let's assume [**?**] that the secret $\mathbf{s}$ is small, say all 0/1. This is useful in FHE .e.g running AES under FHE. Take a sample (A, c). Choose a $p < d$, rather like computing with lower precision. Then consider $(\lfloor a\frac{p}{q} \cdot a \rfloor, \lfloor a\frac{p}{q} \cdot c \rfloor)$. **If** $\mathbf{s}$ is small, the errors from this are small. Typically $p \approx q \cdot \sqrt{n/12}\sigma_s/\sigma_{errors}$.

Does "lazy" modulus reduction, which means we can reduce p by a factor of $a/2$, where $a \approx \log n$.

For $n = 1024$, reduces from 2^{705} operations [Blumetal, J, ACM 50(2003) pp. 509-519] to 2^{405}, and also reduces memory requirements.

Q–EK Lattice methods.

A That's the alternative approach. But it's less efficient, at least in time terms.

12.2 Fast Matrix Decomposition in $\mathbf{F}_2$ — Bertolazzi

We had to compute the rank of many random large matrices over $\mathbf{F}_2$ on a cluster. Had various attempts, and were happy until found M4RI, which is very efficient.

Theorem 25 *Can compute a permutation matrix P such that $PM = LU$ where L and U are* block-*triangular matrices.*

Typically 1.5× faster than M4RI etc., but $> 2\times$ for $1000 < n < 10,000$, probably due to a better transition to [Str69] — they have an analytic formula for when to switch from 4R to [Str69].

Pack bits b- = 32-, 64- or 128- wide. Do LU-factorization in-place. Write $PA = \begin{pmatrix} B & C \\ D & E \end{pmatrix}$ where B is of full rank and D depends on B. Doing thin matrix multiplications via "Four Russians". Partition A and do a block-recursive LU. Cost for the non-recursive version is $\frac{n^3}{3bc}$ where c is the size of the 4R tables.

Q Cache?

A Considered when we decide c, and also in practice we split very long rows by recursion.

Q Why did you use machine code for `popcount` rather than just the instruction?

A Because it is, bizarrely, faster. See `http://graphics.stanford.edu/~seander/bithacks.html`.

12.3 Online Relaxed Hensel Lifting for Dense, Sparse and Structured Linear System Solving — Lebreton

Given $A \in M_{r\times 1}$ and $B \in M_{r\times r}$ invertible over $[[x]]$, both entries polynomials of degree $< d$, want to solve $A = B \cdot C$ at precision $N \gg d$. See [Dix82], which only inverts B at precision 1. The cost is that we are doing naïve polynomial arithmetic. Also [MoenckCarter], which is essentially an x^d-adic version of [Dix82]. Ths will let us use fast multiplication.

Dixon computes $D = \left(\left(\frac{B-B_0}{x}\right)\cdots\right)\cdot C$ but only needs up to C_{i-1} when computing D_i. Use fast on-line multiplication [vdH97, and many others]. Also use Newton iteration to build B^{-1} to required precision.

For $n = d$ we are $\tilde{O}(r^\omega + r^2 d)$, which beats [Storjohann2003] $\tilde{O}(r^\omega d)$. But when $N = rd$ this beats us, since we are now $\tilde{O}(r^3 d)$. In practice, for large matrices we do much better than LinBox.

Definition 13 *Say that a matrix is* structured *of displacement rank α if we can write it as a sum of semi-Toeplitz lower/upper triangular products.*

We do well on such matrices.

12.4 Rational Linear Solvers and Local Smith Forms and How They Apply to Homology Computation — Saunders

Build boundary matrices for the adjacencies of a triangularisation. The structure of these matrices are revealed by their Smith forms. These matrices are very sparse. Had a useful graph showing where dense/blackbox/sparse methods fitted depending on size/density. When size is 10^3 need density $< 10^{-2}$ for sparse to beat blackbox[1]. Dense always wins if density $> 10^{-1}$. "Good elimination" will be a $PLUQ$ decomposition of a 2/row matrix (This may be limited to $\pi 1$ matrices). U is bi-diagonal, and this is linear time.

Hence various quadratic operations using PLUQ (with constant-size matrices).

[1] Looks to JHD roughly like size $\cdot$ density$^{3/2} = 1$ is the critical curve.

Part IV

Sunday 4 August 2013

Chapter 13

Speeding up Lattice Reduction with Numerical Linear Algebra Techniques — Stehlé

Definition 14 *A* lattice *is a discrete subgroup of* $(\mathbf{R}, +)$. *Represented (not uniquely!) by a basis.*

Bases are transformed by integral unimodular matrices. Invariants:

minimum $\lambda(L) := \min_{b \in L \setminus \{0\}} ||b||$.

determinant Volume of parallelepiped given by *any* basis.

Theorem 26 (Minkowski) $\lambda(L) \leq \sqrt{n} \cdot (\det L)^{1/n}$.

Problem 6 (Shortest Vector Problem) *Find a vector* $b \neq 0$ *with* $||b|| \leq \gamma\lambda(L)$.

13.1 Hardness of SVP

$\gamma = O(1)$ NP-hard

$\gamma > \sqrt{n}$ In NP∩co-NP.

γ **growing exponentially with** n polynomial.

Note that a short vector in $\begin{pmatrix} C\gamma_1 & C\gamma_2 & \dots & C\gamma_n \\ 1 & 0 & \dots & \\ 0 & 1 & \dots & \\ \vdots & \vdots & & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}$ implies a good $\mathbf{Z}$-relation between γ_i.

[LLJL82] — not described in detail. Lattice-based cryptography.

post-quantum at least if applying for research grants.

more secure since relies on worst-case hardness rather than average-case as RSA etc.

No exponentiation Possibly more efficient.

FHE [Gen09]

13.2 Lattice Reduction

Define the $b_i^* := \arg\min_{||\cdot||} b_i - \sum_{j<i} c_j b_j$ — Gram-Schmidt Optimisation. The LLL conditions are the following, for $\delta \in (\frac{1}{4}, 1)$:

- $\forall i, j \ \mu_{i,j} \leq 1/2$;
- $\forall i \quad \delta \cdot ||b_i^*||^2 \leq ||b_{i+1}^*||^2 + \mu_{i,i+1}^2 ||b_i^*||^2$ (Lovász condition) for suitable δ.

Then $\lambda(L) \leq ||b_1|| \leq (\delta - \frac{1}{4})^{\frac{n-1}{2}}$. Hence the LLL algorithm to ensure this — clearly correct, but termination isn't obvious. let alone that it's polynomial-time. See [LLJL82, Kal83].

Example 19 (Magma) *With a random 25-dim matrix, LLL took 11.5 seconds, versus today's Magma (default) of 0.24 seconds.*

Algebraic (Exact) the time is dominated by the GSO

Numeric Floating-point — much faster but wrong!

Why? LLL is *looking for* cancellations! For example, numerical GCD is always wrong, for exactly the same reason.

[Odlyzko1982] Hybrid approach: handle the basis with integer operations, but the GSO in floating-point, refreshed from the exact basis.

Numerically GSO is algebraically equivalent to QR factorisation, with many backward-stable algorithms known, but we really need forward stability. We also need *precise* error bounds in order to fix the precision of computation.

Theorem 27 (Last year) *An LLL-reduced basis is well-conditioned w.r.t. GSO/QR, i.e. $O(n)$-bit precision is sufficient.*

Hence a greedy LLL-variant: take the *first* i such that the Lovász condition is violated, so that the previous basis *is* LLL-reduced, and therefore well-conditioned. Asymptotically, this isn't a great improvement, but really helps in practice, especially if, as often happens, machine-precision suffices. Faster?

blocking of the matrix updates

Precision Depends on $\mathrm{cond}(B)$. If $B \cdot U$ is LLL-reduced $\mathrm{cond}(B \cdot U) \leq 2^{O(n)}$.
[Sey93] $\forall B \exists U$ $\mathrm{cond}(B \cdot U) \leq 2^{O(\log n)}$

See `fplll` on my web-page (C++), or implementations in SAGE, MAGMA, PariGP. Still need to implement all of [Sey93].

Can we find shorter vectors than LLL? There exist (more expensive) algorithms. Can we apply these ideas to PSLQ?

Chapter 14

Exact Linear Algebra — Part II of II

14.1 Software Design in the LinBox Library for Fast Exact Linear Algebra —Boyer

Goals for LinBox

- efficient algorithms
- modern environment (multicore, GPU etc.)

Also attract others to contribute to Linbox.

14.1.1 Introduction

Aims — exact linear algebra over a variety of fields/rings. Generic code (LGPL 2.1). A generic C++ template. 185 Kloc (LinBox+FFLAS+FPACK+$\cdots$). Used by Maple and Sage. Uses BLAS. Matrices can be dense/structured/BlackBox ($x \mapsto Ax$ or block $X \mapsto AX$)/Sparse.

Allocation/destruction is only done in the constructor/destructor. Arguments are passed by reference. There is a "mother model": `BlasMatrix<Field>` owns its memory, but `BlasSubMatrix<Field>` points to these. Only the owner deals with memory, which views share it.. Thus works because sizes are known (or at least bounded) in advance. It's lighter than garbage collection and reference counting, and we can rely on C++'s memory management.

Rather than have a top-level 'strategy' module, invoking recursive algorithms, we have a controller which is called also for recursive calls, which deals with
citeStrassen1969/classical, but as well as size this has to deal with memory limitations etc.

Data parallelism or task parallelism? Data: `lba::foreach` etc.

14.2 Simultaneous Computation of Row and Column Rank Profiles — Pernet

Gaussian elimination is the "Swiss Army knife" of computer algebra.

Definition 15 *The* rank profile *is the first r linearly independent rows, or more precisely the lexico-minimal subsequence of $(1, \cdots, m)$ of r indices of linearly independent rows.*

Definition 16 *Note that "generic rank profile" is often used to mean that all principal sub-minors are nonzero, which is not quite the same think: he had an example.*

LU only exists with generic rank profile: generic row rank profile implies LUQ decomposition, etc., but not unique. PLUQ is known as full-pivoting. Claims that some pivoting strategies can reveal the row rank profile. Either are already known: we claim to be able to produce both. Quad-recursive $O(mnr^{\omega-2}$ and an $O(mnr)$ base case. The base case works by fanning out equally along rows and columns.

Unless previous LU, we do quad-splitting. LEU decomposition [Malaschonok2010], where E is a permutation matrix with $n - r$ rows zeroed out. E is unique, and has the same profiles as A.

We can do delayed modular reductions if $k(p-1)^2 < 2^{53}$, where k is the tile size. This buys us an overall speedup of around 15% in the best case.

14.3 A Polynomial Time Algorithm for Computing the Hermite Normal Form of a Module over the Integers of a Number Field — Biasse

HNF over $\mathbf{Z}$ has applications to ideal arithmetic in number fields, notably representations of bounded size.

If an O_K-module can be expressed as

$$M = \mathfrak{a}_1 A_1 + \cdots,$$

where the $\mathfrak{a}_i$ are fractional ideals, we say that $(\mathfrak{a}_i, A_i)$ are a pseudo-generating set for M. The HNF in this context is known as pseudo-HNF. Applications in cryptography [FiekerStehle2010]. Claim polynomial-time computation of this (in $\log|\Delta|$, d, n and sizes).

First case is $\mathbf{Z}$. Recall Gaussian elimination with fractions $(-b/a)$, and if we can't divide, cross-multiply *after* taking out gcd. Bad coefficient growth, even though output is bounded. Therefore work modulo (a multiple of) the determinant. This gives away some information on the lattice, but can be recovered.

[BosmaPohst,Cohen]. Cohen has a modular approach, which he conjectured was polynomial-time. The generalisation is fairly straightforward. Note that a lot of the operations here on ideals in number fields themselves invoke HNF over $\mathbf{Z}$. Note that reducing by an ideal doesn't necessarily reduce "size". Has a better idea including 'denominator reduction'. Our complexity dependence on d is worse than we would get if we embedded $O_K^{n\times n}$ in $\mathbf{Z}^{nd\times nd}$, but of course the latter would lose information on the lattice.

Q–EK Relation to ISSAC 2012 [BF12]?

A Basically the same.

14.4 Lattice Reduction of Polynomial Matrices — Storjohann

> Chapter 13 had an hour for integer lattices, but I only have half an hour — appropriate since it's half as difficult.

Input a matrix in $K[X]^{n\times m}$ and we want a reduced $R \in K[X]^{n\times m}$ whose rows span the same space, and the degrees of R are minimal. Note that we also get the rank out of this. Note that these are not unique, so we also need a concept of normalisation [Popov]. Define the row pivot to be the right-most element of maximal degree. Want then all to be in different columns (weak Popov), and pivots to dominate their columns, plus some tie-breaking rules.

2×1 matrix is just gcd! Note that we're doing repeated subtraction rather than full division. $O(nmrd^2)$ field operations. [MS03].

For a square full-rank matrix, this is $O(n^3d^2)$ — can we do better? Target is $O(n^\omega d^{1+\epsilon})$ — claims $O(n^\omega M(d)\log d)$ since gcds are involved. Note that half-gcd doesn't work since the cofactors blow up. See [BL00, GJV03].[1]

Actually needs a dual-space expansion. Take Taylor expansions of the fractions (need to ensure that there are no factors of x in the denominators, which was DB's point. Apparently solved by [GuptaletalJSC2012]).

14.5 On the Complexity of Multivariate Interpolation with Multiplicities and of Simultaneous Polynomial Approximations — Nieger

Basic setting: Lagrange interpolation: fixed degree = # points−1. Suppose we said "only go through k of d points"? So let k be the degree and t the amount of agreement required. See [GuruswamiSudan] as Reed-Solomon codes.

[1] Dan Bernstein stated that there were errors in [GJV03]. AS seemed to accept this.

There is also "interpolation with multiplicities", done in two variables. $\forall i Q(x_i, y_i) = 0$ with multiplicity m. There are approaches based on structured linear systems [ZehGentnerAugot2011,RothRuckenstein2000], and on polynomial lattices [CH10, and others].

First reformulates as a univariate problem, then as a linear system. Use [BJS07] for this. In fact we have solved a slightly more general (modular) problem. $\tilde{O}(l^{\omega-1}m^2n)$. This extends to the multivariate case.

Q–EK I would call this implicitization, not interpolation.

A Depends on the discipline.

Chapter 15

Multivariate Polynomial Interpolation provides Surprising Combinatorial Insights: Zonotopal Algebra and Beyond — Holtz

Definition 17 Splines *are piecewise polynomial functions with given knots (breaks of polynomiality).*

What happens in higher dimension: CAGD patches etc. A box spline can be defined as its Fourier transform $\widehat{M}_x(y) = \prod_{x \in X} \frac{1-\exp(-ixy)}{ixy}$. In general X is a multiset in $\mathbf{R}^n$, also viewed as a matrix (? as the rows of).

Definition 18 *A* zonotype $Z(X)$ *is the image* $X([0,1]^{\#X})$ *of the unit cube* $[0,1]^{\#X}$.

Hence concepts of basis, and independent set. order X in an arbitrary way. B is said to be an *internal basis* if, for each $b \in B$, b in not the last element in $X \setminus \ldots$.

A long sequence of subsets is one that intersects every basis. $L(X)$ is the set of all long sequences. A short sequence is the opposite.

Theorem 28 (Dahmen–Micchelli,1984) *Define* $D(X) = \{p \in \mathbf{C}[t_1, \ldots, t_n] | q_y(D)(p) = 0 \forall y \in L(X)\}$. *Then* $\dim(D(X) = \#B(X)$.

Apparently the faces of the zonotope are determined by the hyperplanes coming out of the dual space P of D.

Theorem 29 ("If you take one thing away, ...") *For a finite set $\sigma \subset \mathbf{R}^n$ (not a multiset)*

$$Exp(\sigma) := \mathrm{span}\{e_a, a \in \sigma\}$$

where $e_a : \mathbf{R}^n \to \mathbf{R} : t \mapsto e^{a \cdot t}$. Then for each $t \in Exp(\sigma)$, we have $f = f_0 + f_1 + \cdots$ where f_i is a homogeneous polynomial of (total) degree j. Define $f_\perp$ to be the least non-zero f_j. Let

$$\Pi(\sigma) := \mathrm{span}\{f_\perp : f \in Exp(\sigma)\}.$$

Then the map $p \mapsto p|_\sigma$ is a bijection between $\Pi(\sigma)$ and $\mathbf{C}^n$.

There's also a theory, due to speaker and others, of external bases as well. Apparently useful X are the incidence graphs of matrices, coding the edge $i \to j$ as $e_i - e_j$. The Hilbert series of these various spaces are essentially the Tutte polynomials of the graph.

Bibliography

[BD02] R.J. Bradford and J.H. Davenport. Towards Better Simplification of Elementary Functions. In T. Mora, editor, *Proceedings ISSAC 2002*, pages 15–22, 2002.

[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.

[BF12] J.-F. Biasse and C. Fieker. A polynomial time algorithm for computing the HNF of a module over the integers of a number field. In *Proceedings ISSAC 2012*, pages 75–82, 2012.

[BJS07] A. Bostan, C.-P. Jeannerod, and É. Schost. Solving Toeplitz- and Vandermonde-like linear systems with large displacement. In C.W. Brown, editor, *Proceedings ISSAC 2007*, pages 33–40, 2007.

[BL00] B. Beckermann and G. Labahn. Fraction-free computation of matrix rational interpolants and matrix GCDs. *SIAM J. Matrix Anal. Appl.*, 22:114–144, 2000.

[BMdCS12] C.J. Brooks, A. Martín del Campo, and F. Sottile. Galois groups of Schubert problems of lines are at least alternating. `http://arxiv.org/abs/1207.4280`, 2012.

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

[CH10] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. `http://arxiv.org/abs/1008.1284`, 2010.

[CLO06] D.A. Cox, J.B. Little, and D.B. O'Shea. Ideals, Varieties and Algorithms. *Springer–Verlag*, 2006.

[CMMXY09] C. Chen, M. Moreno Maza, B. Xia, and L. Yang. Computing Cylindrical Algebraic Decomposition via Triangular Decomposition. In J. May, editor, *Proceedings ISSAC 2009*, pages 95–102, 2009.

[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.

[Cop96] D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In *Proceedings EUROCRYPT '96*, pages 178–189, 1996.

[Cop97] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptology*, 10:233–260, 1997.

[Cop01] D. Coppersmith. Finding Small Solutions to Small Degree Polynomials. In J.H. Silverman, editor, *Proceedings CaLC 2001*, pages 20–31, 2001.

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

[Dix82] J.D. Dixon. Exact Solutions of Linear Equations Using p-adic Methods. *Numer. Math.*, 40:137–141, 1982.

[Gen09] C. Gentry. Fully homomorphic encryption using ideal lattices. *Symposium on the Theory of Computing (STOC)*, pages 169–178, 2009.

[GGL05] A. Größlinger, M. Greibl, and C. Lengauer. Quantifier Elimination in Automatic Loop Parallelization. In *Proceedings A3L*, pages 123–126, 2005.

[GJV03] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the Complexity of Polynomial Matrix Computations. In J.R. Sendra, editor, *Proceedings ISSAC 2003*, pages 135–142, 2003.

[GK06] S. Gerhold and M. Kauers. A Computer Proof of Turán's Inequality. *J. Inequalities Pure Appl. Math. article 42*, 7, 2006.

[Har77] R. Hartshorne. Algebraic Geometry. *Springer-Verlag*, 1977.

[HG97] N.A. Howgrave-Graham. Finding Small Roots of Univariate Modular Equations Revisited. *Cryptography and Coding (Ed. M. Darnell)*, pages 131–142, 1997.

[HG98] N.A. Howgrave-Graham. *Computational Mathematics Inspired by RSA*. PhD thesis, University of Bath, 1998.

[HRS12] J. Hauenstein, J. Rodriguez, and B. Sturmfels. Maximum Likelihood for Matrices with Rank Constraints. `http://arxiv.org/abs/1210.0198`, 2012.

[HS10] J. Hauenstein and F. Sottile. alphaCertified: certifying solutions to polynomial systems. `http://arxiv.org/abs/1011.1091`, 2010.

[JdM12] D. Jovanović and L. de Moura. Solving Non-Linear Arithmetic. In *Proceedings IJCAR 2012*, pages 339–354, 2012.

[Kah87] W. Kahan. Branch Cuts for Complex Elementary Functions. In A. Iserles and M.J.D. Powell, editors, *Proceedings The State of Art in Numerical Analysis*, pages 165–211, 1987.

[Kal83] E. Kaltofen. On the Complexity of Finding Short Vectors in Integer lattices. In *Proceedings EUROCAL 83*, pages 236–244, 1983.

[KLYZ12] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *J. Symbolic Comp.*, 47:1–15, 2012.

[Laz91] D. Lazard. A New Method for Solving Algebraic Systems of Positive Dimension. *Discrete Appl. Math.*, 33:147–160, 1991.

[LLJL82] A.K. Lenstra, H.W. Lenstra, Jun., and L. Lovász. Factoring Polynomials with Rational Coefficients. *Math. Ann.*, 261:515–534, 1982.

[MM99] M. Moreno Maza. On Triangular Decompositions of Algebraic Varieties. Technical Report TR 4/99, 1999.

[MS03] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comp.*, 35:377–401, 2003.

[Ren92a] J. Renegar. On the Computational-Complexity and Geometry of the 1st-Order Theory of the Reals.1. Introduction — Preliminaries — The Geometry of Semi-Algebraic Sets — The Decision Problem for the Existential Theory of the Reals. *J. Symbolic Comp.*, 13:255–299, 1992.

[Ren92b] J. Renegar. On the Computational-Complexity and Geometry of the 1st-Order Theory of the Reals.2. The General Decision Problem — Preliminaries for Quantifier Elimination. *J. Symbolic Comp.*, 13:301–327, 1992.

[Ren92c] J. Renegar. On the Computational-Complexity and Geometry of the 1st-Order Theory of the Reals.3. Quantifier Elimination. *J. Symbolic Comp.*, 13:329–352, 1992.

[Rum10] S. Rump. Verification Methods: Rigorous Results using Floating-Point Arithmetic. In S.M. Watt, editor, *Proceedings ISSAC 2010*, pages 3–4, 2010.

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

[SEDZ09] M. Safey El Din and L. Zhi. Computing rational points in convex semi-algebraic sets and SOS decompositions. http://arxiv.org/abs/0910.2973, 2009.

[Sey93] Martin Seysen. Simultaneous reduction of a lattice basis and its reciprocal basis. *Combinatorica*, 13(3):363–376, 1993.

[SKP11] J. Schöberl, C. Koutschan, and P. Paule. EP2378444 — Method, device and computer program product for determining an electromagnetic near field of a field excitation source for an electrical system. https://register.epo.org/espacenet/application?number=EP10159805, 2011.

[Str69] V. Strassen. Gaussian Elimination is not Optimal. *Numer. Math.*, 13:354–356, 1969.

[vdH97] J. van der Hoeven. Lazy Multiplication of Formal Power Series. In W. Küchlin, editor, *Proceedings ISSAC 1997*, pages 17–20, 1997.

[YWL13] Z. Yang, M. Wu, and W. Lin. Exact Safety Verification of Interval Hybrid Systems Based on Symbolic-Numeric Computation. http://arxiv.org/abs/1302.5974, 2013.