ISSAC 2021

Notes by J.H.Davenport

18 July 2021

Chapter 1

18 July 2021: Gerdt Workshop

FC pointed out that VG presented in Beijing 2019 the bid for ISSAC 2021 to be in Russia. Note that VG was genreal chair for 1993 ISSAC (Kyyiv). The workshop was organised by Daniel Robertz, a close collaborator of VG.

1.1 Thomas Decomposition: A brief History in Memory of VG: Domgming Wang

Shows a picture of VG lecturing on this at SMS 2018. [BGLHR12, LGM17].

1.2 Simple Decomposition and Simple Characterstic Decomposition: Chenqui Mou

"Simple Decomposition" is also "Thomas Decomposition". $x_1 \prec x_s \prec \cdots$. Triangular sets. A simple set is a triangular set with squarefreeness. The absence of multiplicity means that you can count multiplicity easily [BÏ14], and D5 applies for dynamic splitting. The radical of the idal is the intersection of saturated ideals. We clearly (JHD things he means globally) distinguish algebraic variables from transcendental ones ("unmixed"), and the algebraic side is equiprojectable [AV00]. Squarefree in characteristic 0 is g.c.d. for univariates, and generalises [BGLHR12], but not over $\mathbf{F}_p$: [GT96].

Concept of W-characteristic set [Wan16], based on a LEX GB.

1.3 Theory in CA⊆SC: Ernst Mayr

Reminiscences of VG and the founding of CASC.

Table 1.1: Data from [May21]

Example	1	2
vars	18	32
generators	11	21
GB	81	478
GB time	1.6 sec	22.1 min
Radical	66	??
Radical Time	6.13 min	∞

Our GB became 6 times larger, and the time to compute it 800 times more, but we can't compute the radical after four months of trying.

CM talked about upper bounds, but I have worked on lower bounds, and my constructions are very similar to this work. Binomial ideals are bad enough.

There is nothing better in practice than a good theory.

1.3.1 Q&A

Q–JHD Slides?

A Send e-mail. [JHD now has them.]

Q–TM I can't say anything precise, but by hand the computation of involutive bases is very similar to the Gebauer-Möller version of Buchberger, at least when I compute them by hand.

A I am looking at a formal definition, but there examples where, say, Maple works in 5 minutes, but involutive takes days, others when involutive is faster by $\times 20$.

1.4 Edneral

VG was one of the first to start CA in USSR. Used CDC 6500. Hearn visited Dubna in early 1980s and brought Reduce. VG got a JINR prize for this.

1.5 Nikolai Vavilov

Numerous reminiscences

1.6 Werner Seiler

Lagrange transformation: work in cotangent space (phase space) rather than tangent space. Dirac was first to look at singularities here. Note that the Dirac

"algorithm" is "notoriously subtle" [HenneauxTeitelboim1992]. "Existence follows by implicit function theorem" — not something we algorithmic thinkers want to hear. In fact, Dirac "algorithm" isn't an algorithm at all: VG wnate to make it one.

$$N_{DoF} = N - N_{\text{first constraints}} - \frac{1}{2} N_{\text{secondary constraints}}.$$

1.7 Amir Hashemi

Short visit to Dubna in 2011. Look at Lakshman's algorithm [LL91] to compute associated primes, then used a variant of FGLM in [Lak91]. But this isn't valid.

1.8 Ceria

Work I spoke about with VG. Bar code has rows, with segments in each row, such that there are no breaks under a bar, and all rows have the same total length. Associate the vertical rows with variables $1 \prec x_1 \prec \cdots x_n$.

1.9 Mora & Ceria

First met VG at Leipzig 1987. Need a concept of "effectively given ring". Then we can expend Pommaret ideas to this.

"Janet discovered his reduction immediately after talking with Hilbert".

1.10 Robertz

Picture of VG at CASC 2003 in Passau. Times of many meetings in Aachen, with or without Yuri Blinkov. Since Maple 2018 our Thomas decomposition has been available in Maple. Joint collaboration at ISSAC 2019.

1.11 Misc

JHD Eurocal '85 and Liepzig '87.

Shaoshi Chen Met VG at Wu's 90th.

Zima JHD was chair of Leipzig, and VG made presentations for people who couldn't come, or couldn't speak.

JHD Thanks for the reminder, and yes, VG also started a tradition: I did Weispfennng at ISSAC 1993 (Kyyiv) and Hasemi at ICMS 2018 (Notre Dame).

Chapter 2

19 July 2021

2.1

Univariate. Given F and G, compute Euclidean Division: $F = GQ + R$. Dense algorithm is quasi-linear in degee D. Suppose $\#F, \#G \leq T$, ssize linear in $T \log D$. Examples of polynomials with same shape and very different-sized Q, R. Also example of coefficient blowup. [MP11] gives $\tilde{\mathcal{O}}(\#F + \#G\#Q)$.

Propose a polynomial-time probabilistic algorithm for exact division. Can test result quasi-linear [GGPdC20]. Will use sparse interpolation, repeatedly guessing the sparsity. If p is a random prime, most of the monomials in Q are still in $Q \pmod{X^p - 1}$ for "good" p. For this to work, we need G to be coprime with $X^p - 1$, but if $G(1) = 0$ never true. So use $X \mapsto \alpha X$.

Chapter 3

July 21

3.1 DEWCAD: Matthew England

CAD and QE.

Logic E.g. [BDE+16].

SMT approach.

CDCAC [ADEK21]

Lazard projection [MPP19] but needs a lot of reformulation.

3.2 Nikhil Balaji, Sylvain Perifel, Mahsa Shirmohammadi and James Worrell – Cyclotomic identity testing and applications

[**?**]: choose a prime $p > n^2$ and compute $f(\alpha) \pmod p$. [CKS99] solving "evaluating in $\mathbf{Z}$". Can we check if $f(\alpha) = 0$ in time $poly(||f||, ||\alpha||)$? Special case is n-th root of unity. [Pla78], but claim there's a P algorithm [CTV10].

3.3 Calcium: Johansson

RC numbers mixed success; Example SAGE. C library with Python interface. Nemo interface with Julia in the works. Rely heavily on multivariates in FLINT. But we need to know the ideal I, and may not: $\mathbf{Q}(\pi, e)$ and Schanuel's conjecture. Given a partial ideal, we can use numerical zero testing to prove non-zero.

Chapter 4

July 22

4.1 Haokun Li, Bican Xia, Huiying Zhang and Tao Zheng – Choosing the variable ordering for cylindrical algebraic decomposition via exploiting chordal structure

Example [DES98] variable ordering can be 512 or $> 10,000$.

Associated Graph [CP16]. Chordal completions, and minimal ones. PEO = Perfect Elimination Ordering. Table showing examples.

Combined degree and (m, d) (citing [BDE$^+$16]) and define various sets. Good example (slide 28) of how PEO helps. Table (slide 30) and Theorem (31) on gains. Example from [DES98] which has different possible orders.

4.1.1 Q&A

Q–JHD Thanks for crediting us, but it's really [McC85]. But are you showing that being chordal isn't enough: you need to follow the PEO.

A That's right.

4.2 Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations

See [LSED21]. Various references to block structure [BPR96, e.g.], but there's no complexity analysis, though it's a practical algorithm. Setting:

$$\exists \mathbf{x} \Psi(\mathbf{x}, \mathbf{y}) \Leftrightarrow \Phi(\mathbf{y}) : \text{with } n\ x_i;\ t\ y_i.$$

Note that Ψ is purely equational.

This [HSED12] is a critical point method. We require:

1. $\mathbf{f} = \{f_1, \ldots, f_s\}$ to generate a radical ideal[1],

2. $\mathcal{V}$ to be smooth and equiprojectable,

3. and a third condition on $\pi(\mathcal{V} \cap \mathbf{R}^{n+t})$ having non-zero measure in $\mathbf{R}^t$.

Actually just look for a weak algorithm only producing $>$ rather than $\leq$. The output is a Φ encoded by matrices.

Use SafeyElDin–Schost algorithm. Use Jacobian criterion, and the $n - d$ minors of the Wronskian matrix. Then use Hermite quadratic forms [Wei98]. Minors of the H_i with grevlex order, and sample points [LSED20]. Get a sharp degree bound on the minors. Singly exponential in n.

We get better complexity analysis etc., but for generic systems. Could probably do more to exploit the characteristics of the Hermite matrix.

JHD "generic" = conditions 1–2?

A No: 1–3!

Q–TS Singly exponential even though you use GB?

A Because of genericity assumption.

4.3 Hormann

I am one of two non-Russian physical participants: excellent. Joint work with others and Chee Yap. Assume all roots are simple. Algorithm is based on bisection, and range functions for f, f'. If $0 \notin \text{range } f$, then we can discard the interval. If $0 \in \text{range } f'$, then there could be an inflection, so we split.

So what range functions? Maximum Taylor forms. [CL84] for Hermite interpolants. Reusing computations doesn't change complexity, but is useful in practice. Tree size is larger with Lagrange by $\times 3 - -5$.

4.4 David Braun, Nicolas Magaud and Pascal Schreck – Two new ways to formally prove Dandelin-Gallucci's theorem

We are in 3D projective incidence geometry. Every line in $\{a, b, c\}$ meets every line in $\{d, e, f\}$. Then DG is a statement about incidence. Th e DG theorem is that Pappus is equivalent to DG.

[1] This worries JHD. In examples like [BD07], the set of *all* polynomials generates the trivial ideal. *But* this paper is purely equational, so this doesn't apply directly: merely places limits on where we can go.

4.4.1 Wu

Since Pappus is true, we can only prove Pappus ⇒ DG. Translate the geometry into algebra. Prove goal is ideal of assumptions. Then use RegularChains in Maple. But choosing good coordinates isn't easy.

4.4.2 Combinatorics

Use a rank function. There are three matroid properties of rank. We have a closed-world assumption, and aim to generate a verifiable Coq script. Ther are 17 points. Pappus⇒DG is 20Kloc and 22 minutes, and 60K, 36 minutes in other direction.

4.4.3 Q&A

Q–EK Do we actually want to understand the proof, or just check it?

A Coq gives you that check.

4.5 Jasper Nalbach, Erika Ábrahám and Gereon Kremer – Extending the fundamental theorem of linear programming for strict inequalities

We use Simplex for LP, but SMT might require strict inequalities. [DDM06], but no proof for strict inequalities. So we need an equivalent of FT Linear Programming: D is satisfiable iff there is a max l.i. subset $V \subseteq C$ such that

$$\exists \alpha : \alpha \vDash \cdots .$$

We transform strict to nonstrict by adding ϵ. But this has real problems when extended. So make ϵ into a new unknown.

Q Have you tied this in SM-RAT?

A Yes.

Q Only one ϵ?

A Yes, and it makes the proof tricky

4.6 Andrei Matveiakin – Discovering multiple polylogarithm equations via symbolic computations

$\mathrm{Li}_w(x) = \sum \frac{x^l}{l^w}$. The multiple polylogarithms. 5-term equation for weight 2 by Abel, then weight 3

4.7 Nadia Heninger – Algorithmic Techniques and Open Problems in Cryptanalysis

[Hen21] Today, just before PQC, we have RSA, finite fields (DH/DSA) and ECDH/ECDSA. One important question is side-channel attacks/partial recovery.

4.7.1 Coppesmith/Howgrave-Graham

$e = 65537$ in practice. Given the top (or bottom) half of one factor, we can factor N in polynomial time. Practical demonstration in SAGE with LLL (dual method to [Cop96]). Better version by HG.

Theorem 1 *Given a degree d polynomial f, integer N, we can in time* $P(\log N, d)$ *find modulo divisors B of N satisfying* $f(r) \equiv 0 \pmod{B}$*, where ....*

Infineon smart cards and "the return of Coppersmith". $p = kM + (65537^a \pmod{M})$. Force recall of Estonian passports etc.

Middle bits is more complicated [HM08] and the bound is less good $p^{0.41}$. Bernstein et al. broke Taiwanese Smart Cards Digital Certificate (2013). Many unknown chunks now looks like $p^{0.3}$. Note that LLL is L_2 but we really want L_1. Also encodes algebraic relationships poorly.

4.7.2 Branch and Prune

Attacker knows some bits of p and q. This was my first paper, saw Coron's "10 reasons why a paper is rejected". The relevant case in practice is CRT-RSA. Bernsteinetal2017 . Libgcrypt wasn't constant time. But only leaker 40% of the bits, but could deduce more.

Copycat leaked sequence of branches in Euclidean binary GCD. [MVBH+20]

4.7.3 Hidden Number

See [DMH20]. This is about ECDSA. Partial information about nonces helps.

Q "ECDSA screws up less" — why?

A Probably because people are scared of elliptuc curves and go by the book.

Q Was RNG is Smart Cards screwed up on purpose?

A Hard to separate malice from incompetence.

Chapter 5

23 July

5.1 Comprehensive Characteristic Decomposition

$<$ a bloc term ordering in $\mathbf{K}[\mathbf{u}, \mathbf{x}]$. [KZH+13]: comprehensive Gröbner system if we partition $\overline{\mathbf{K}}^m$ into $\mathcal{A}_i$, and over each $\mathbf{u} \in \mathcal{A}_i$, $\mathcal{G}_i(\mathbf{u})$ is a GB.

A triangular set $\mathcal{T}$ is *normal* if every $\text{ini}(T_i)$ contains only free variables, and *regular* if $\mathbf{Z}(int(T_i))$ and ... have no common zeros. Then we have a *comprehensive triangular decomposition* if $\mathcal{T}_i(\mathbf{u})$ is a *regular* triangular set.

Consider pairs $\Gamma := (\mathcal{G}, \mathcal{C})$ where each $\mathcal{G}_i$ is a reduced LEX GB, and $\mathcal{C}_i$ is ....

Extend above idea to a (normal) comp. characteristic decomposition if we partition $\overline{\mathbf{K}}^m$ into $\mathcal{A}_i$, and over each $\mathbf{u} \in \mathcal{A}_i$, $\Gamma_i(\mathbf{u})$ is a (normal) characteristic decomposition.

5.1.1 Q&A

Q-RL You said Gröbner Walk "wasn't so slow"

A I don't remember the timings.

5.2 Signature-Based Buchberger over PIDs: Maria Francis & Thibault Verron

Need a *strong* GB for the two definitions to match. Usual problem of wasteful reductions. See [MMT92]. If $f = \sum h_i f_i$, then f has a representation as $\sum h_i e_i$ where the e_i are the standard basis.

5.3 mSolve: Mohammed SED+others

Input in $\mathbf{Z}/p\mathbf{Z}$ for $p < 2^{31}$ or $\mathbf{Q}$. Concentrate on zero-dimensional systems, losing multiplicities. Good algorithmic description of F_4 in `msolve`. Grevlex

only so far. Use hash tables to reduce active storage: one for the the basis and one for pre-processing results. CE had good LA routines. This always takes $> 90\%$ of the runtime, and sparse, and sparse probailitsic, seem competitive. Use generic staircase [MS03]. Two examples (noon7/8) where Maple is much faster. Seems to know why. We hope to make this available via Sage.

5.4 FGLM over Tate Algebras

Usual valuation, which is non-archimedean.

5.5 Generalised GB: Levin

Let K be in an inversive differential field with $\alpha_1, \ldots, \alpha_m$ automorphisms and their inverses (say σ). Partition σ into p sets.

5.6 Pierre Lairez and Mohab Safey El Din: Computing the dimension of real algebraic sets

[Koi99, Vor99] [BPR06] $D^{O(\dim(x)\,\mathrm{codim}(X))}$.

dim(point)=0; $\dim(X \cup Y) = \max(\dim(X), \dim(Y))$, $\dim((0,1) \times X) = 1 + \dim(X)$ and these are sufficient. [Har80] for any semi-algebraic map $f : X \to \mathbf{R}$, ther eis a finite set $\Sigma \subset \mathbf{R}$ such that on any connected component I of $\mathbf{R} \setminus \Sigma$, any $t \in I$, $f^{-1}(I) \sim I \times f^{-1}(t)$. However, best known algorithm for computing Σ has $\#\Sigma = D^{2^{O(n)}}$.

For $x \subset \mathbf{R}^n$ real *algebraic* [not semi-algebraic] by polynomials of degree D, [BV07] $\#\Sigma = D^{O(n)}$. See also [SED05], which has no infinitesimals

Our algorithm is efficient in practice as $\#\Sigma <<$expected. Shows 10ksec, versus 200ksec for Maple's RT (where $\#\Sigma = 10$ against bound of c. 1000.

5.7 Closing

ISSAC 2022 in Lille.

Bibliography

[ADEK21] E. Ábrahám, J.H. Davenport, M. England, and G. Kremer. Deciding the Consistency of Non-Linear Real Arithmetic Constraints with a Conflict Driven Search Using Cylindrical Algebraic Coverings. *Journal of Logical and Algebraic Methods in Programming Article 100633*, 119, 2021.

[AV00] P. Aubry and A. Valibouze. Using Galois Ideals for Computing Relative Resolvents. *J. Symbolic Comp.*, 30:635–651, 2000.

[BÏ14] T. Bächler. *Counting solutions of algebraic systems via triangular decomposition*. PhD thesis, RWTH Aachen, 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.

[BDE+16] R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson. Truth table invariant cylindrical algebraic decomposition. *J. Symbolic Computation*, 76:1–35, 2016.

[BGLHR12] T. Bächler, V. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas decomposition of algebraic and differential systems. *Journal of Symbolic Computation*, 47:1233–1266, 2012.

[BPR96] S. Basu, R. Pollack, and M.-F. Roy. On the Combinatorial and Algebraic Complexity of Quantifier Elimination. *J. ACM*, 43:1002–1045, 1996.

[BPR06] S. Basu, R. Pollack, , and M.-F. Roy. Computing the Dimension of a Semi-Algebraic Set. *J. Math. Sci.*, 134:2346–2353, 2006.

[BV07] S. Basu and N.N. Vorobjov. On the number of homotopy types of fibres of a definable map. *J. Lond. Math. Soc. Ser. 2*, 76:757–776, 2007.

[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.

[CL84] H. Cornelius and R. Lohner. Computing the range of values of real functions with accuracy higher than second order. *Computing*, 33:331–347, 1984.

[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.

[CP16] D. Cifuentes and P. Parrilo. Chordal networks of polynomial ideals. `https://arxiv.org/abs/1604.02618`, 2016.

[CTV10] Q. Cheng, S.P. Tarasov, and M.N. Vyalyi. Efficient algorithms for sparse cyclotomic integer zero testing. *Theory of Computing Systems*, 46, 2010.

[DDM06] B. Dutertre and L. De Moura. A fast linear-arithmetic solver for DPLL (T). *In International Conference on Computer Aided Verification*, pages 81–94, 2006.

[DES98] P. Diaconis, D. Eisenbud, and B. Sturmfels. Lattice Walks and Primary Decomposition. *Mathematical Essays in honor of Gian-Carlo Rota*, pages 173–193, 1998.

[DMH20] G. De Micheli and N. Heninger. Recovering cryptographic keys from partial information, by example. `https://eprint.iacr.org/2020/1506`, 2020.

[GGPdC20] P. Giorgi, B. Grenet, and A. Perret du Cray. Essentially optimal sparse polynomial multiplication. In *Proceedings ISSAC '20*, pages 202–209, 2020.

[GT96] P. Gianni and B.M. Trager. Square–Free Algorithms in Finite Characteristic. *AAECC*, 7:1–14, 1996.

[Har80] R.M. Hardt. Semi-Algebraic Local-Triviality in Semi-Algebraic Mappings. *Am. J. Math.*, 102:291–302, 1980.

[Hen21] N. Heninger. Algorithmic techniques and open problems in cryptanalysis (Slides at ISSAC 2021). `https://www.issac-conference.org/2021/material/slides/4-Heninger-AlgorithmicTechniques.pdf`, 2021.

[HM08] M. Herrmann and A. May. Solving linear equations modulo divisors: On factoring given any bits. *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–424, 2008.

[HSED12] H. Hong and M. Safey El Din. Variant quantifier elimination. *J. Symbolic Comp.*, 47:883–901, 2012.

[Koi99] P. Koiran. The Real Dimension Problem Is $NP_{\mathbf{R}}$-Complete. *J. Complex.*, 15:227–238, 1999.

[KZH+13] D. Kapur, Z. Zhang, M. Horbach, H. Zhao, Q. Lu, and T. Nguyen. Geometric Quantifier Elimination Heuristics for Automatically Generating Octagonal and Max-plus Invariants. *Automated Reasoning and Mathematics: Essays in Memory of William W. McCune*, pages 189–228, 2013.

[Lak91] Y.N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals. In T. Mora and C. Traverso, editors, *Proceedings MEGA 1990*, pages 227–234, 1991.

[LGM17] D. Lyakhov, V. Gerdt, and D. Michels. Algorithmic Verification of Linearizability for Ordinary Differential Equations. `https://arxiv.org/abs/1702.03829`, 2017.

[LL91] Y.N. Lakshman and D. Lazard. On the Complexity of Zero-dimensional Systems. In T. Mora and C. Traverso, editors, *Proceedings MEGA 1990*, pages 217–225, 1991.

[LSED20] H.P. Le and M. Safey El Din. Solving parametric systems of polynomial equations over the reals through Hermite matrices. `https://arxiv.org/abs/2011.14136`, 2020.

[LSED21] H.P. Le and M. Safey El Din. Faster one block quantifier elimination for regular polynomial systems of equations. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, pages 265–272, 2021.

[May21] E. Mayr. Theory in CA⊆SC: in memoriam Vladimir Petrovich Gerdt. *Talk at Gerdt workshop ISSAC 2021*, 2021.

[McC85] S. McCallum. An Improved Projection Operation for Cylindrical Algebraic Decomposition. In *Proceedings EUROCAL 85*, pages 277–278, 1985.

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

[MP11] M. Monagan and R. Pearce. Sparse polynomial division using a heap. *J. Symbolic Comp.*, 46:807–822, 2011.

[MPP19] S. McCallum, A. Parusiński, and L. Paunescu. Validity proof of Lazard's method for CAD construction. *J. Symbolic Comp.*, 92:52–69, 2019.

[MS03] G. Moreno-Socías. Degrevlex Gröbner bases of generic complete intersections. *Journal of Pure and Applied Algebra*, 180:263–283, 2003.

[MVBH+20] D. Moghimi, J. Van Bulck, N. Heninger, F. Piessens, and B. Sunar. CopyCat: Controlled Instruction-Level Attacks on Enclaves. *In 29th USENIX Security Symposium (USENIX Security 20)*, pages 469–486, 2020.

[Pla78] D.A. Plaisted. Some Polynomial and Integer Divisibility Problems are NP-Hard. *SIAM J. Comp.*, 7:458–464, 1978.

[SED05] M. Safey El Din. Computing Sampling Points on a Singular Real Hypersurface Using Lagrange's System. Technical Report 5464 INRIA, 2005.

[Vor99] N.N. Vorobjov Jr. Complexity of computing the local dimension of a semialgebraic set. *J. Symbolic Comp.*, 27:565–579, 1999.

[Wan16] D. Wang. On the Connection Between Ritt Characteristic Sets and Buchberger–Gröbner Bases. *Math. Comput. Sci.*, 10:479–492, 2016.

[Wei98] V. Weispfenning. A New Approach to Quantifier Elimination for Real Algebra. *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 376–392, 1998.