Patrizia Gianni and teaching me/us about solutions (and some questions to think about)

James Davenport[1]
University of Bath
Fulbright Scholar at NYU
J.H.Davenport@bath.ac.uk

30 March 2017

[1]Thanks to Matthew England (Coventry), EPSRC EP/J003247/1, EU H2020-FETOPEN-2016-2017-CSA project $\mathcal{SC}^2$ (712689)

Timeline (as I saw/see it)

1965 Buchberger's PhD [Buc65].

1970 Buchberger's paper [Buc70].

1976 SIGSAM Bulletin [Buc76b, Buc76a]; JHD starts as research student with John ffitch.

1979 EUROSAM presentation/paper [Buc79].

JPff "What on earth did you make of that talk"?

JHD "Not sure, but it's not mediocre".

Axiom JHD joins what becomes the Axiom group at IBM.

Summer 1983

PG, BMT, JHD are all at IBM.

- By now the idea is sinking in that Gröbner bases are "a good thing", though JHD, at least, doesn't really understand them.
- However, a key ingredient is distributed polynomials and orderings
- We decide that $K_{\texttt{plex}(x,y,z)}[x,y,z]$ and $K_{\texttt{tdeg}(x,y,z)}[x,y,z]$ are different `Ring` structures
- (and do a lot of exploring of isomorphisms and their encoding)
- and experiment a lot (this was long before CoCoA etc.) especially with orderings and different orderings, homogenisations etc.
- I at least learned a lot, but a lot of questions remained: solutions, orderings etc. Also a definition of "usual".

Spring 1987

JHD is Programme Chair of EUROCAL 1987 (Patrizia does 1988, but turns it into ISSAC).
Two papers land on his desk (this is 1987, and "papers", "land" and "desk" are all meant to be taken literally: there was an extra desk in the office for EUROCAL papers)

[Gia89] P. Gianni *Properties of Gröbner bases under specializations*

[Kal89] M. Kalkbrener *Solving systems of algebraic equations by using Gröbner bases*

Different routes to a similar result: we publish both.
Only much later do I see this is connected with "lazy algebraic numbers and D5" [DDDD85]

So I/we now understand that Lexicographical bases are the answer to "solutions", at least in dimension zero, but others are faster.
Then [FGLM89] arrived, the preprint version of [FGLM93] (in the days before we really used arXiv!). We can now compute in an efficient ordering, and convert, at least in dimension zero.
Then the Gröbner walk [CKM97] arrived, valid in positive dimension.
[AGK97] claims the Gröbner walk is faster than FGLM, but `http://staff.bath.ac.uk/masjhd/JHD-CA/GWalkexample.html` shows the opposite in Maple.

Open Problem

Seriously compare the two approaches.

Positive Dimension

But what about positive dimension? If we have the Gröbner walk, we can compute a lexicographic Gröbner base, but then what? Does Gianni–Kalkbrener generalise? Surely it ought to. After all, we can always take slices.
Sadly, not: [FGT01].

Open Problem

So what exactly can we say/do in positive dimension?

Open Problem

How does this compare with regular chains?

What's usual (I) Polynomials in $\mathbf{Z}[x]$?

The old question we used to ask in 1983: what should we try to be fast on? A major challenge in computer algebra
"Almost all polynomials are irreducible", or more precisely $\forall d$

$$\lim_{H\to\infty} \frac{|\{\text{irred. polys of degree } d, \text{ coefficients} \le H\}|}{|\{\text{polynomials of degree } d, \text{ coefficients} \le H\}|} = 1$$

This makes it much harder to say anything about "interesting" polynomials.

Conjecture

"Almost all reducible polynomials are squarefree", or more precisely $\forall d$

$$\lim_{H\to\infty} \frac{|\{\textit{sqfr. red. polys of degree } d, \textit{ coefficients} \le H\}|}{|\{\textit{reducible polys of degree } d, \textit{ coefficients} \le H\}|} = 1$$

What's usual (II) Polynomials in ?[x]?

By analogy with irreducibility, polynomials have few real roots [Kac43], $\frac{2}{\pi}\log(d+1)$. But this is not

$$\lim_{H\to\infty} \frac{\sum_{f\in S} |\{\text{real roots of } f\}|}{|S := \{\text{polys of degree } d \in \mathbf{Z}[x], \text{ coefficients} \leq H\}|} = \frac{2}{\pi}\log(d+1)$$

rather a result about uniformly $(-1,1)$ real coefficients.
A definition with better geometric invariance properties gives $\sqrt{\frac{d(d+2)}{3}}$: very different [LL12].

What's usual for ideals (I)?

Though I've never seen it stated as such, I believe that "almost ideals are 0-dimensional", more accurately "almost all generating sets generate 0-dimensional ideals", i.e. $\forall n, d$

$$\lim_{H\to\infty} \frac{|\{\text{0-dim } \langle n \text{ polys of degree} \leq d, \text{ coefficients} \leq H\rangle\}|}{|\{\langle n \text{ polynomials of degree} \leq d, \text{ coefficients} \leq H\rangle\}|} = 1$$

And if we have more than n polynomials, almost all generating sets are trivial.
But this poses the same problem, even assuming the correct definition of "interesting" is "reducible".

Open Problem

Are almost all reducible ideals 0-dimensional (in the sense above)?

What's usual for ideals (II)?

Open Problem

Are almost all reducible ideals radical (in the sense above)?

Open Problem (hard to state)

For a given n and dimension d, are almost all reducible ideals of dimension d radical (in the sense above)?

These would have interesting implications for the weak worst-case complexity (i.e. apart from an exponentially-rare subset: [AL15]) of Gröbner bases: [MR13] improves on [MM82]

Bibliography

B. Amrhein, O. Gloor, and W. Küchlin.
On the Walk.
Theor. Comp. Sci., 187:179–202, 1997.

D. Amelunxen and M. Lotz.
Average-case complexity without the black swans.
http://arxiv.org/abs/1512.09290, 2015.

B. Buchberger.
Ein Algorithmus zum Auffinden des Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Math. Inst. University of Innsbruck, 1965.

Bibliography

II


B. Buchberger.
Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystem (English translation in [Buc98]).
Aequationes Mathematicae, 4:374–383, 1970.


B. Buchberger.
Some Properties of Gröbner-Bases for Polynomial Ideals.
SIGSAM Bulletin 40(Nov. 1976), pages 19–24, 1976.


B. Buchberger.
Theoretical Basis for the Reduction of Polynomials to Canonical Forms.
SIGSAM Bulletin 39 (Aug. 1976), pages 19–29, 1976.

Bibliography

III


B. Buchberger.
A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases.
In *Proceedings EUROSAM 79*, pages 3–21, 1979.


B. Buchberger.
An Algorithmic Criterion for the Solvability of a System of Algebraic Equations.
In Gröbner Bases and Applications, pages 535–545, 1998.


S. Collart, M. Kalkbrener, and D. Mall.
Converting Bases with the Gröbner Walk.
J. Symbolic Comp., 24:465–469, 1997.

Bibliography


J. Della Dora, C. DiCrescenzo, and D. Duval.
About a new Method for Computing in Algebraic Number Fields.
In *Proceedings EUROCAL 85*, pages 289–290, 1985.


J.C. Faugère, P. Gianni, D. Lazard, and T. Mora.
Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering.
Technical Report LITP 89-52, 1989.


J.C. Faugère, P. Gianni, D. Lazard, and T. Mora.
Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering.
J. Symbolic Comp., 16:329–344, 1993.

Bibliography

V


E. Fortuna, P. Gianni, and B. Trager.
Degree reduction under specialization.
J. Pure Appl. Algebra, 164:153–163, 2001.


P. Gianni.
Properties of Gröbner bases under specializations.
In *Proceedings EUROCAL 87*, pages 293–297, 1989.


M. Kac.
On the Average Number of Real Roots of a Random Algebraic Equation.
Bull. A.M.S., 49:314–320, 1943.


M. Kalkbrener.
Solving systems of algebraic equations by using Gröbner bases.
In *Proceedings EUROCAL 87*, pages 282–292, 1989.

Bibliography

VI


A. Lerario and E. Lundberg.
Statistics on Hilbert's Sixteenth Problem.
http://arxiv.org/abs/1212.3823, 2012.


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


E.W. Mayr and S. Ritscher.
Dimension-dependent bounds for Gröbner bases of polynomial ideals.
J. Symbolic Comp., 49:78–94, 2013.