ICMS 2016 (Berlin)

Notes by JHD

11-14 July 2016

Contents

Chapter 1

11 July 2016

1.1 With Extreme Scale Computing the Rules have Changed: Dongarra

1.1.1 Overview of HPC

PFlop machines are current: there are 95 such systems in Top 500. There are three technologies:

- Commodity processors
- Commodity processors + accelerators (93 or 95)
- Lightweight cores: ShenWei, ARM, Knights Landing.

Note the shift in HPC deployment: half the Top 500 are in a variety of industries (finance, movies, databases). Intel is 91% of Top 500, with AMD a further 3%, so x86 is 94%. Top 500 benchmark: dense matrix to be solved by Gaussian elimination. We want the limiting case as #matrix tends to infinity. Over 24 years, we see doubling every 14 months (Moore's law plus added parallelism), where N=500 has gone from 59.7Gflops at the start, 286Tflops today = Σ in 2003. The gap from N=1 to N=500 is 6–8 years. JD gets 70Gflops from his dual core Haswell laptop. His iPhone is 4Gflops, which would have been in top 500 in 199?. Extrapolating $N = 1$ (which is a bumpy graph) shows Exaflops in 2020. The Chinese expect this, US expects 2023.

Sunway TaihuLight with SW21010 has 260 cores/chip, 10649000 cores in all, custom interconnect, used a $10^7 \times 10^7$ matrix to achieve Rmax=93, which is 74% of Rpeak. This machine is 15MW. In the US, a MWattyear is $1M, and that's just the computer, so add the cooling. On this basis, 6Gflop/watt, whereas most other machines are around 2. Chip is 1.45GHz. Chip has 4 core groups, each 64 processing cores and a control core. 8GB/group 22 flops/byte ratio[1]. Cabinet is 1024 nodes, and a system is 40 cabinets. 1.3 PB of DDR3 (slow, less power) memory. HPCG benchmark shows 0.3% of peak. Cost (including building) $280M. `http://bit.ly/sunway-2016`. 3 out of 6 finalists at 2016 Gordon Bell.

[1] JD wants 1. SMW queries this.

- MHD 15Pflops
- Molecular dynamics 14.7Pflops
- ??

HPCG benchmark is won by NSCC Guangzhou at 0.58 (1.1% of Rpeak), second is RIKEN at 4.7% of Rpeak, 3rd is Sunway. The gap between LAPACK and HPCG (in terms of %age Rpeak) is about $\times 20$. Shows how Intel has been adding flops/cycle, mostly in terms of vector lengthening. Notes also that fetcing from main memory on same node takes 167 cycles, i.e. 4000 flops on Skylake.

Lovely infographic of machines in Top 500. Note 167 China versus 165 USA (also wins in $\sum_{500}$ terms). ZIB's Konrad is #96 on the list.

1.1.2 JD's software history

EISPACK Algol translation, row-oriented

LINPACK Level 1 BLAS (VV), column-oriented

LAPACK Level 3 BLAS (MM)

SCALAPACK Distributed memory etc.

PLASMA/DPLASMA/MAGMA DAG/Scheduler, block data layout.

Classical Analysis of Algorithms may not be appropriate. Machines are over-provisioned in terms of Flops. Data movement is extremely expensive. Hence operation count is not as appropriate as it was.

Note that the zero-ing of a panel in SVD is a matrix-vecor, not matrix-matrix, operation. Hence half the algorithm is MM, half is MV. Since MM is $\times 22$ faster than MV, the MV dominates time-wise. Hence we are now looking at a two-stage algorithms

1. Reduce to banded (MM)
2. bulge chasing to tridiagonal (MV)

This takes $\frac{10}{3}n^3$ operations rather than $\frac{8}{3}n^3$, but is 6–7 times faster in practice. Notes also that "deep learning" tends to be matrix-matrix multiply, but lots of small matrices to be processed in parallel. Also these guys don't need accurate results, and can even make do with 16-bit (now appearing in hardware). This batched-matrix also comes up in sparse multifrontal metods etc. Hence we are loooking at a BLAS that does batched matrix operations. Gets $\times 3$ on Knights Landing with lots of matrices of sizes ranging from 32^2 to 500^2.

Lovely diagram showing activity on each core over time as LAPACK LU (fork-join parallelism) runs.

Also notes mixed precision. Some nVidias have $3\times$ for SP over DP. Can we use this? Can we do the bulk in 32-bit and use 64-bit to clean up? Let's rediscover iterative

refinement. See Wilkinson, Moler, Stewart, Higham. Can do $O(n^3)$ in SP and $O(n^2)$ in DP, but uses 1.5× the storage (since we need to refine against the original matrix). Doesn't work if the matrix is too ill-conditioned. Shows 1600 rather than 600 GFlops/sec on a mixed Kepler/Intel system.

1.1.3 Extreme scale

- Classical analysis doesn't explain everything
- Need latency tolerance in algorithms
- Need to reduce synchronisation
- Data movement takes both time *and* energy
- Need to think about mixed precision
- Autotuning is vital as machines get more complicated
- Fault tolerance (hard or soft) is needed.
- Bit-wise reproducibility is a major challenge: some of our colleagues don't understand this.

Q Are supercomputers like Audi/VW: tuned to pass the benchmarks?

A Couldn't agree more. Linpack is 40 years old. Things have changed (possibly because of LinPack)

Q Doesn't this also depends on funding: the guys with the money (DoE) have a certain shape of problems.

A Yes — people with money want 3D PDEs.

Q Moore's Law?

A This gives us more gates/chip, and may be slowing down.

Q Compile time or run time scheduling?

A OpenMP (latest version) — a mixture of compile and runtime.

1.2 Free Logic in HOL: Benzmüller & Scott

HOL can handle syntax and semantics for a variety of logics L: HOL is a metalogic: $\phi :=$. Classical HOL is Church's Simple Type Theory (JSL9140). Assume Henkin semantics (JSL1950). See [BenzmulleretalJSL2004].

Scott has found an inconsistency in Gödel's work. [6]. This is why the collaboration started.

The present King of France is bald.

Russell: False; Frege: doesn't denote; Hilbert–Bernays: the term can not be introduced because of existence/uniqueness not being satisfied. [Scott1967]

1. Bound individual variables range over $E \subset D$
2. E may be empty
3.

Hence in HOL we have a raw D_i for the type i, and E with a predicate. $\neg$ and $\rightarrow$ map, but $\forall x.\phi(x)$ maps to $\forall x E(x) \rightarrow \phi(x)$. $\iota x.\phi(x)$ maps to an if/then/else bottom construct. Becomes one slide of HOL. "=" is symmetric: if one side is defined, so is the other and the values are equal.

Various experiments. Second series had $\simeq$, no * (E may be empty). Consistent if all maps are defined, but inconsistent if defined map(s) exist. Third series (Scotts 1977/79) non-reflecxive equality, no * (E may be empty) is consistent.

Theorem 1 $(\exists x.\neg E(x)) \rightarrow \mathit{false}$

Informal proof in 10 lines. We had a verified publication, but Springer's re-production process may completely mess this up.

1.3 Agent-based HOL Reasoning: Steen

Based on Leo-III prover.

Examples 4CT [3, 19]; Kepler [21]; Gödel's Ontological Argument [Benzmuller-Wloltzenlogel Paleo IJCAI2016].

Cantor's surjective Theorem — no surjective function from a set to its power set. What is an appropriate formalization? [13].

$$\neg\exists F_{\iota\rightarrow(\iota\rightarrow o)}.\forall Y_{\iota\rightarrow o}.\exists X_\iota FX = Y$$

Leo-III uses specialists as independent agents, whihc can find a proof cooperatively. Based on a Blackboard model. Sequential loop, biut agents can execute non-blocking. Competed in CADE' ATP (CASC) competition. Didn't do very well, but not optimised (parameter settings especially). On this, took 1.8 seconds. Output is human-unreadable, but the speaker managed to highlight the key clause (diagonal argument).

Q Are the systems local?

A Yes, but of course they could be stubs that make an internet-based call.

1.4 Theorema 2.0: Maletzky

3000 formulae and 2500 proofs in reduction rings (Gröbner bases generalised). Revealed some weaknesses. Can't prove automatically, no support for higher-order reasoning as such, and difficult to keep track. Theorema aims fro automated proving, so users have to split theorems into lemmas. hence we've developed an Interactive Proof Stratgey in Theorema 2.0. So what's new? This is done via dialogue-windows.

1.4.1 Interaction

Example 1 (Drinker's Paradox) *In every non-empty pub there is someone such that, if he drinks, everyone else drinks as well.*

$$\exists_x x \in pub \Rightarrow (\exists_{x \in pub} drinks(x) \Rightarrow \forall_{y \in pub} drinks(y)).$$

Gets a dialogue window; selects case-based reasoning then gets a window to enter cases.

1.4.2 Rewriting

Theorema extracts rewrite rules from formulae. But only first-order rewriting is supported at the moment, as supported by Mathematica. Hence we have implemented higher-order via a compiler into Mathematica transformations. The α-equivalence checking etc are encoded into the transformation. Note, however, that decidability is undecided in general, so we only implement subclasses, but this turns out to be pretty sufficient in practice: only 2–3 of the 3000 are unsolved.

1.4.3 Theory Analysis

If I change something, I need to reprove various other formulae, but which? This can be hard across 3000 formulae. Hence a `TheoryAnalyzer` that generates the dependency graph from formalizations in Theorema 2.0.

Further work text-based as well as interactive guidance; higher-order uniification as well. Isabelle-inspired, want to automate common tasks, as well as proofs, e.g. constructing quotient domains.

Q-Benzmüller I really agree on needing two styles of assistance: we are at the other end, with only text, and would like the dialogue.

1.5 Automated Deduction in RingTheory

Based on Prover9; descendant of Otter. Under what conditions is a ring commutative?

Theorem 2 *If in some ring R $x^2 = x$, then R is commutative.*

Theorem 3 (Jacobsen) *If for any $x \in R$ there is $n(x)$ such that$x^{n(x)} = 1$, then R is commutative.*

Thre are three conditions.

1. Polynomial conditions.
2. Rings with derivations.

   Theorem 4 (Posner1957) *If $d(x)d(y) = d(y)d(x) = 0$ then R is commutative.*

3. Rings with involutions

With $n = 2, 3$ Pveror9 prove sin 3 seocnds, $n - 4$ 80 seocnds. For $(xy - yx)^n = xy - yx$, for $n = 2, 3$ prover9 takes 20 minutes. Also a counterexample to ??.

1.5.1 Near-rings

1. $(R, +)$ is a group, non necessarily abelian
2.
3.

Some results.

Also more general results, e.r. $(R, +)$ ust veing a cancellation (possibly abelian) semigroup.

1.5.2 Semirings

1. $(R, +)$ is a commutative monoid with identity 0
2. $(R, \cdots)$ is a monoid
3. Multiplication distributes over addition
4. Some cancellation laws

Theorem 5 (2 minutes Prover9) *If additive commutations are central in a CL-semiring R, then R is commutative.*

Theorem 6 (20 minutes Prover9) *Another result.*

a is Moore-Penrose invertible if $\exists b : aba = a; bab = b; (ab)^* = ab, (ba)^* = ba$. Can prove uniqueness.

Q Problem with displaying Prover9 proofs in readable form

A-Benzmüller Ω had such.

1.6 Automated Theorem Discovery in Elementary Geometry in Geogebra: Botana

Intoduction to dynamic geometry. Automatic proving is establishing if some given statement is true, while automatic discovery tries to establish *when* the statement is true, adding more clauses to the statement. This was initiated by Wu: [32]. Geometric statements become set inclusion statements. When $H \Rightarrow T$ is false, we want H_0 such that $H \wedge H_0 \Rightarrow T$ is true.

1. Assign numerical coordinates to each base point.
2. Solve the equations for all the constructed points.
3. Get the locus of P (one free point) such that the extra condition is satisfied.

The standard definition in dynamic geometry is that of the "tracer–mover" locus. [1].

Example 2 (Right triangle altitude theorem) *So when is this true for non-right triangles?*

Q *Any attempts to systematise geometric facts database?*

A *Some portuguese work.*

Ion *Also Kimberley's work.*

1.7 Efficient Knot discrimination via quandle coloring with SAT: Lisitsa

Is it possible to deform $\mathbf{R}^3$ continuously such that the knot is transformed into a trivial unknotted circle without passing through itself. We first need to translate this into a discrete code of the knot diagram. Hence the question is "is the knot ambient isotropic" to trivial. Hence we ask also about conversion of one knot into another. UD is decidable [Haken1961] and coNP [HassLacariasPippenger]. UD is in NP modulo GRH [Kuperberg2011]. KE is decidable [Haken1961] . Examples from Haken are impracticable. Monotone simplification algorothms are fast is practice but do not provide a decision procedure. Normal surface theorn [Burtonetal2012] provide efficient recognition of non-trivial knots. With crossing number ≤ 12 always is at most 5 minutes.

With Fish, as approach via quandles (2014).

Definition 1 *1.* $x \rhd x = x$ *for all* $x \in Q$

2. for all $x, y \in Q$*, there is a unique* z *with* $x = z \rhd y$

2' $(x \rhd y) \rhd y = x$

3. $(x \rhd y) \rhd z) = (x \rhd z) \rhd (y \rhd z)$

2' gives us an involutary quandle rather than a quandle.

Theorem 7 *The following are equivalent*

(*) J is knotted

U1 Q(K) is non-trivial

U2 IQ(K) is non-trivial

K1 There is a finite quandle such that $col_Q(K) > 0$

K2 There is a finite simple quandle such that $col_Q(K) > 0$

K3

We translate these into SAT or #SAT. Have boolean vaiables $v_{i,c}$ saying that arc i has colour c. Adequacy is clear: every colorig f of D by Q such that$f(\alpha_1 = 1$ corresponds to a unique solution o fthe SAT problm. Symmetry breaking by adding $v_{1,1} = 1$.

SQ 354 simple quandles of size ≤ 47

CQ 26 quandles ≤ 182.

Q1-Q3 small sets of quandles they have devised.

K10-K13 all prime knots wth croosing numbers $\leq$ index.

Used MiniSAT 2.2.0; #SAT 12.08, various Perl/Prolog scripts. Debian VM on Windows 7. GFor K12, eahc case is under 3.3 seconds, whereas Regina is in minutes. For #SAT, it seems that, averaged over quandles, the running time in K12 is small for knots, but there is a quite a vaiations for different quandles. His Q3 family of quandlres give 100% distinguishability Takes 6511 minutes for all knots in K12. But [Clark et al2015] claim 5000 seconds with very efficient parallelisation (sequential would be months: apparently 100K+ threads). How about parallel #SAT?

Q Can you distinguish figure 8 from its mirror? Jones can't.

A

1.8 Sage; Zhou

Parameter space anaysis. Suggest to compute one cell by metaprogramming, then complete the proof complex by wall-crossing search. This will be applied to cutting-plane theorems in integer programming.

Example 3 *Conisider* $\begin{pmatrix} a & b \\ b & \frac{1}{4} \end{pmatrix}$. *and for which* a, b *is this positive definite*

Example 4 *Maximise* $ax + by$ *across a linear space (Simplex), then how does this vary as* a, b *change?*

The set of parameters down a given branch of the program is a semi-algebraic set.

```
K.{x,y>= ParametricRealField([3/2,1/2])
a=2*x    % so a is 3
b=4*y    % so b is 2
c=x^2+y^2-4
sorted([0,a,b,c,])   % 0<a is true, but the side-condition is 2x>0
                              % 0<b  is true record -4y<0
      % 0>c since 0>-3/2  record x^2+y^2-4<0
     % answer is c<0<b<a with related conditions
```

But CAD is very slow if the number of inequalities is large. Given a complicated product, e.g. (JHD's interpretation) if we have $FGH > 0$, we know the signs of each at our test point, so we might take $F > 0, G < 0, H < 0$ instead.

Consider example 3. Test point $(1, 1)$. This is not p.d. But at $(\frac{2}{3}, \frac{1}{3})$ it is true. Used CAD implementation in Mathematica. This lets us find a point in a cell next to a given cell. Use breadth-first search to complete the space.

An example of "forward slope" functions, claims that the proof produced is "close to human". Verifies some proofs in the literature.

1.9 Problems of sequence in university entrance exmaination:

Part of Todai robot [4]. Tis project aims to unify AI, which has subduvided inthe 1980s and afterwards. And with developments elsewhere in computing. Note thatthere is a large corpus, and a good knowledge of human abilities.

Academic year begins in April. Mock exams June–December (help deicde where to apply). Jnauary has the Center test. n February examinations administered by indivudal universities.

Center Multiple/grid-in choice. 530K applicants in 2014

Individual Tokyo 9400 apply, 3100 succeed. Gnerally more difficult.

1.9.1 Main flow

Problem Use natural language processing

ZF Use symbolic computation with a knowledge base

RCF Use QE.

Answer

1.9.2 sequence problems

Problem

ZF use symbolic computation and 1800loc Haskell

Solver

Example 5 (Translated from Japanese!) *Let a_i be a sequnce with $a_{n+1} = 3a_n + 60$, with initial term -27. Then $a - n = A^n - BC$. Let $S_n = \sum_{k=1}^{n} a_k$. Then $S_n = \frac{D}{E}(F^n - G) - (BC)n$ (A etc. unknown digits to be completed).*

So we have $S_{n+1} = S +_n +a_n$. Use Maple's `rsolve`. Then add initial values from problem. So $a_n = 3^n - 30$ etc., and we can determine A,B,C etc. Used 5 years of main and supplementary examinations, and 31 mock exams. Average score 13.6/20. 16 times we scored 100%. The robot took an open mock exam in June 2015 with 116,000 applicants for math/science. Held an open conference to report the results in November 2015.

Example 6 *Let*

Our solver got 18/20, not the last part of the question. We did well because assigning values to the sequences/series got the answers. The failure was a problem with NLP.

Q Is the NLP deep semantics, or pattern matching?

A Largely pattern matching.

Q Has this changed university policy?

A Not sure yet.

Q–PI What was your motivation? Curiosity, change university policy, ...

A To see what AI can do.

Q Allen institute has organised something similar.

A No relation (yet).

Chapter 2

12 July 2016

2.1 Towards an International Mathematical Knowledge Base: Watt

This conference is the closest to my heart: both "Mathematical" and "Software". I could talk about all sorts of things, but have chosen to talk about the future.

Mathematics does not date, or go stale. At least by comparison (not absolutely) the results are precise and clear. Hence it is more susceptible to machine treatment, and hence the GDML goal. ID at ICM2014 wanted to go beyond just a collection of PDFs. Hence IMU WG: 5 of the 8 of which are at this conference, which shows something.

1. "Is this result known" (expecting yes, and a reference).
2. "Is this result known" (expecting no, so my paper is new).
3. Identification of holes.
4. Conjecture generation.
5. Refactoring mathematics.
6. Certification.

2.1.1 Information → knowledge

Note that the distinction between "programme and data" is artificial: Kolmogorov complexity etc. So what is "knowledge"?

Plato Justified true belief.

Many perception, commnication and reasoning

Semiotics syntactics, semantics, pragmatics.

The CA system implementer implement rules, and needs to eplxain them to the user, hence code and documents should, at least match. If we look at documents, we are also concerned with metadata. Then there's the formalised mathematics point of view.

So where is math knowledge today? Indexes, reviews, Math genealogy. General summary works; Wikipedia, MathWorld etc. Tools/databases such as OEIS. Libraries of formal mathematics: Mizar, Archive of Formal Proofs etc.

2.1.2 How do we get knowledge from documents?

1. Assemble document collections
2. Capture page sets (note that a PDF is less informative than one might think: a "left brace" may in fact be several PDF characters).
3. capture metadata
4. semantic capture
5. knowledge tools

Mechanically. we the community are at the 3/4 boundary, with some manually-driven work at 5. Note the analogy with compilers. At some point, we move from the source program to an annotated tree with bindings etc. Then this become the primary object, and we use this to generate output(s), be they machine code, or test cases, or ....

2.1.3 Document analysis

Note [Sexton,Sorge] and [28]. But in the future born digital documents will be the majority. Good TEX versus bad TEX (example was { and } in different formulae. `(n+1)^2` (squaring the ')') versus `{(n+1)}^2` (squaring the expression).. Also semantics macros: `BesselJ` or `J` for example.

Various past projects: Maple, Aiom, Aldor, OpenMath, MathML, MONET [10], InkML. Note also Automath, Mathematical Vernaacular, ideas of Kamareddine and Gowers.

SMW notes the incrasingtrend in # Java standard libraries. from 1840 in Java 1.3 to 4240 in Java 8. Hence one needs to separate language from library. This is also vital for backwards compatibility. Typical language issues are scope. Granularity of libraries is a key issue.

"Semantic Capture" had a variety of meanings

1. Library Science
2. Document Analysis
3. Shallow capture — NLP etc.
4. Deep capture, formalised mathematics etc.

5. synthesis

Even "equation" is ambiguous [22]. Note that equation is 1391 (Chaucer) "=" is [26] and variables were Descartes (1637).

2.1.4 Notation selection

This case up even last week, at Waterloo, where we are developing on-line course content. $(ax)^{-\frac{1}{2}} + \text{atan}(x)''$ or $\frac{1}{\sqrt{ax}} + \cdots$ or .... Equally, same notation can mean different things: J_ν for example.

Shows his frequency charts as in [29], and claims that this lets you work out what a paper is about. Also n-gram frequencies. ωt is much more frequent that wt, which can help with disambiguation. Note MK's invention of "flexiformalism". Note that [31] claims the de Bruijn factor is about 4. "A little inaccuracy saves a world of explanation" [HH Munro — Clovis onthe Alleged Romance of Business].

Note that ThomsonReuters sold their IPR business for $\approx$ 10G$, so IP is valuable. But "All 10 of us were angry when Google yanked Math support from Chrome". Notes that the EU OpenMath project was funded under "Multimedia standards".

"One ring to rule them all" versus "big tent". Picture of Esperanto conference versus a larger Francophonie meeting, making his approach clear.

- Can afford to hand-annotate a small subset
- Rely on improvement of technology
- Approximation goes a long way ("this theorem is mostly true" doesn't help in mathematics, but probably does here).
- Future proof the data

We are chipping away at a grand challenge.

Q-BB Data versus programs: you said there wasn't a difference, but then analyse them differently.

A Of course, you analyse differently.

Q Google dropped MathML "for security reasons" — sounds strange.

A Yes.

Q What about the future, rather than existing literature. What should new authors do?

A The optimists would like to see much more author involvement, but many will continue in the old ways.

Q-JHD Have you done any experiments to classify documents based on [29]?

A No.

JHD Advertisment for my research student doing this.

SMW Great.

Q Would it helpto have a better language than TEX?

A Certainly, even just for reflow reasons.

2.2 Symbolic Floating Point: Plet

Defines IEEE FP (normalised, and assuming unbounded e). $x = (-1)^s \cdot m \cdot \beta^{e-p+1}$ where $\beta^{p-1} \leq m < \beta^p$. Round to nearest with tie-break to even.

Algorithm 1 (Kahan) *1.* $\hat{w} := RN(bc)$

2. $e := RM(\hat{w} - bc)$

3. $\hat{f} := RM(ad - \hat{w})$

4. $\hat{x} := RN(\hat{f} + e)$
computes determnant of abcd . $\frac{|\hat{x}-x|}{x} \leq 2ulp.$

[JLP2013a] shows this is optimal, but all calculations done by hand.

Let k be a symbolic variable, and $\mathbf{L} := \{ak + b, a, b \in \mathbf{Z}\}$. $\mathbf{E} := \{\sum_i c_i\beta_i, |c_i| \in \{1, \ldots, \beta - 1\}, i \in \mathbf{L}\}$.

Round to nearest precision p (symbolic, even)

$$f(p) : + \frac{2^{3p/2} + 5 \cdot 2^{p-1}}{2^{3p} + 2^{5p/2+1}}.$$

Write $p = 2k$. Domains are **SQ**, **SZ** and $\mathbf{SF}_p$. But some elements of **SQ** cannot be rounded.

$$f(p) := \frac{2}{3}(1 + 11 \cdot 2^{-p}). \tag{2.1}$$

When p is even, $f(p) \in \mathbf{F}_p$, $f(2k) \in \mathbf{SF}_{2k}$. When p is odd, $RN_{2k+1} = \cdots$ and the two cannot be unified.

Writes Algorithm 1 as a Maple procedure and evaluates the precision. Also evaluates (2.1) and is told about the cases. `https://hal.nia.fr/hal-01232159`.

Wants to extend to more operations, eg. $\sqrt{}$. Automatic search for bad cases.

Q–JHD Unnormalised numbers? Or is this a consqeuence of assuming unbounded mantissae?

A (Slightly vague)

Q–GMG Applications?

A For my thesis I wanted to do this n a proof assistant, so needed to be sure what I was doing.

2.3 A guide for Good Scientific Practice in Numerical Experiments:

1971 No numerical experiments. [Nitsche1971], but heavily used in numerical analysis.

1986 GMRES [SaadSchultz1986] 2/14 pages numerical experiments.

2010 More than 30% of numerical experiments.

> Science builds on previous results: either theorems or established methods. Often the first step in new science is to reproduce the old. This should be easy in numerical experiments.

But no standards. But see [5, 27] and `rcomputation.org`, `sciencecodemanifesto.org`. All science should be:

R Replicability.

R Reproducibility

R Reusability.

What does this mean for CBEx (Computer-Based Experiments). Want concrete rules, but nonexclusive becaus eof Open Source requirements.

R Replicability. That I myself can, next day or next year, reproduce the experiments. This shows robustness against statistical influences, and observer biases.

R Reproducibility. That another researcher, in a differnet computing environment, can reproduce the experiments. Note there is a general "reproducibility crisis", not just in computing,

R Reusability.

R Replicability. Requies basic documentation. Recommended: Automaion and testing.

R Reproducibility. Requires extensive documentation, and recommended is availability.

R Reusability. Requires accessibility, and recommended Modularity, Software Management and Licencing.

See ArXiV preprint.

Q What about R:=Readibility?

A Didn't want to be to prescriptive. But maybe it should be recommended.

2.4 Robust Construction of Voronoi Diagram: Kim

Tesselation, with $f(G, D, d)$: G generator set, D distance and d dimension. Usually $2 \leq d \leq 4$. Notes that applying weighting can change the topology of a VD. Traditional offsetting algorithms (in 2D) take $O(N^2)$, and their ideas $O(N)$.

Notes that VD in 3D have great applications in molecular dynamics. But hard to compute. Exact computation can lead to Voronoi vertices of degree > 3, whihc is unstable. We want a topology-oriented approach, after Sugihara et al. He had a TOI (Topoogy-Oriented Incremental) approach. [Sugihara1992] shows problematic cases. Because of convexity, T is non-empty, is a tree, and ∂V_c is connected.

Q-GMG VD's have many uses, buthwat abou tthese weighted ones?

A Mobile 'phone cells, where masts differ.

Q What happens when you make achoice basedon numerical evidence. So a weak evidence might drive you one way, which then conflicts with strong evidence.

A Not a problem. If I cannot find a red vertex to propagate from, then

2.5 3D-modelling and Pycao software: Evain

Example: working on my bicycle. Note that $\mathbf{R}^3$ has a more complicated symmetry group. We are inputtng via 2D tools. AutoCAD takes "your whole life" to master, but these are tools for professionals. Two clicks for a point in 3D, do we want movie precision or science precision? nterface with Numpy/Scipy. Want a coordinate-free description. See `Povray.obj` format, but it's a raytracer format. Our objective is "what is the shortest description". Hard, but we can do something in this direction. Use Mathematical affine geometry as the framework. Use Python as the tool.

Use "massic points" (?) a 4-vector. Can therefore write $p_1 - p_2$, and get type verification etc. Absolute and relative definitions $[p_1, p_2, p_3, p_4] \simeq [p_1, v, p_3, w]$ if $v = p_2 - p_1$, $w = p_4 - p_3$ can be handled by the compiler. `Tableleg1:=cube(tableLegDimensions)` etc.

The "box paradigm" is deeply embedded in our mind: the modelled world lives n a box.

Q Is the spftware available?

A On my website. Still needs work on the documentation. Uses Numpy for the computations.

2.6 Business Meeting

Chaired by Joswig. John Hauenstein appointed as Secretary. Kohlhase appointed as Web Chair. `icms-conference.org`.

Bid for next conference: Hauenstein/Sommese at Notre Dame. One of ND's features is the Studebaker museum, featuring one owned by Lincoln: aimed for banquet venue. Have to avoid football games in terms of pricing etc. Founded 1842; etc. Train to/from Chicago, or flights to various hubs. Dates to be decided after ISSAC 2016 decides dates of ISSAC 2018. Note that

2.6.1 New Journal

Aimed at the software should be the main part of the submission, and be assessed. It is hard to write a paper "the new version of", even tough there may be a lot of work involved,both mathematical and technical.

2.6.2 Software

MK noted that OpenDreamKit was building a suite of Docker mplementations from DockerHub was proving successful. He noted that writinga Docker install script was a good start in documentation.

2.7 Need Polynomial Systems be Doubly-exponential? England

"Doubly exponential" means doubly exponential in the number n of variables, not m the number of polynomials, or d degree.

GB are known, [23]. But note [24] shows that it's doubly exponential in r, the dimension.

Cylindrical Algebraic Decomposition: [14], but note [25] has moved the goalposts since our paper was written. Classically sign-invariant, but in fact what we want is truth-invariance for formulae. Note that our improvements [17] had to break away from

1. Projection polynomials are uniform;
2. Answers are in terms of sign-invariance.

Reduces the double exponent of m to be $n - \ell$ rather than n, where ℓ is the number of equational constraints, but not d. See [9]. Our CASC paper [18] used Gröbner bases to reduce the d exponent to be exponential in $d - \ell$. Require the constraints to be variable-by-variable (artefact of the proof) and primitive, which this paper shows to be inherent.

Q–JAA This is worst case — typical?

A–ME No.

A–JHD Well, it probably is typical case as far as d is concerned, but of cours ethe polynomial

2.8 New practical algorithms for implicitisation of hypersurfaces: Bigatti

$$\phi : K[x1, \ldots, x_n] \to K[t_1, \ldots, t_s]$$

`Implicit`$(f_1, \ldots, f_2)$:=ker(ϕ) by GB: neat but slow.

Hypersurface case (i.e. `Implicit`$(f_1, \ldots, f_2)$ is principal), e.g. $s = n - 1$. But not necessarily.

Let h be a new indeterminate, and work in $K[t_1, \ldots, t_s, h, x_1, \ldots, x_n]$, with $\deg(x_i) = \deg(f_i)$. Let $F_i = f_i^{hom}$. Let $J = \langle x_i - F_i \rangle$. The $J \cap K[h, x_1, \ldots, x_n]$ is prime, and its dehomogenisation is the Implicit ideal. Timings generally better, but not always.

Q What if the ideal isn't principal?

A In general, we kmow thi sfor extrinsic reasons. Not verified.

2.9 Fault-tolerant Rational Reconstruction: Abbott

Modular methods (or Hensel). Even my mobile has 4 cores, and moduar is well-adapted to parallelism. But

1. Bad reduction
2. How many primes?

Note that there's no homomorphism from $\mathbf{Q}$ to $\mathbf{F}_p$, because of $1/p$, so call primes which appear in denominators "ugly", and discard these *a priori*. Then usual good/bad decision. Badness is not necessarily decidable *a priori*. Direct or ElimTH from the previous talk will always terminate, but with answers with σ-smaller LT, or lwer-or-equal w-degree. $\leq$ means that we can't spot bad primes automatically. Key is [2, to appear in JSC].

Reconstructions is $< 1\%$ of total, so the real question is "how many primes". For balanced numbers, we are slightly worse than [7], once the numbers are unbalanced between numeratir.denominator, we do better. Whether or not there are bad primes doesn't seem to affect this comparison. [8] doens't seem to be applicable.

Q Suppose all primes are bad?

A That can happen, and we can be fooled.

2.10 NDEmathema: An Innovative Web-based Automated Symbolic Computing Platform for Nonlinear Differential Equations:

We have developed offline Maple programs to derive speicifc types of analytic solutions to certain nonkinear DE. Our platform is to be used online via a browser: supports

Chrome, Opera [most], and mobile devices. Chinese version only online so far: English later (she demoed a private copy). Two interfaces: integrated and independent. Input is linear, and output is 2D mathematics.

Each equation has as much information as [ossible, in particular a Maple worksheet is established. Shows example of KdV.

Q Looks like Maple.

A I also have Macsyma etc. versions.

Chapter 3

13 July 2016

3.1 Challenges in Open Source CA: Decker

- Methods from CA are now firmly established in the toolbox of the pure mathematician
- CA: group and number theory feeding into ...
- Now this national SFB (Decker heads)
- Four cornerstones: GAP (progrmaming language interesting in its own right); Singular; Polymake; ANTIC — a new system (nucleus, really) on number theory.

GAP Intelligent GAP objcets and algorithms

```
grp:=PSL(2,5);
a:=random(grp);
b:=random(grp);
Group(a,b);
```

Singular Rational parametrization of (genus zero) curves, which may do blowups, normalization, integral bases.

- More and more abstract tools are being made constructive. Quotes proof of FLT (though JHD couldn't see relevance)
- Interface diagram: far from complete, but at least connected (though not as a digraph). GAP can call any other, though Antic via Singular ratherthan direct.

Question 1 (Mumford; Montreal 1980) *Can a computer classify all surfaces of general type with* $p_g = 0$.

Theorem 8 (Bogomolov–Miyaoka–?? Inequality) *A minimal surface of geeral type with* $p_g = 0$ *has* $1 \leq K^2 \leq 9$.

Example 7 ($K^2 = 1$; Numerical Godeaux Serfceces) *It is known that $\pi_1(X)^{ab}$ is cyclic of degree at most 5, and there are constructions for each order. It is conjectured that there is precisely one of each order, and $\pi_1(X) \cong \pi_1(X)^{ab}$.*

Needs computations with GB over number fields.

Shows a graph of Singular citations by field and year from `https://zbmath.org`. They come from many areas, not just the "core" areas. Need "resolution of singularities", which is highly parallel, whereas most (current) algorithms are sequential — a great challenge.

ANF/Modular/CRT Gröbner bases. Choose primes, then factor the minimal polynomial, to geta two-level split (and reconstruction).

3.1.1 Parallelism

Coarse More natural for us.

Fine Far from clear how this would work for us given the memory management issues.

GAP has some HPC

Singular Hired from GAP, and now working on a parallel version

Polymake has ideas in this area.

Antic new: needs to think about this challenge.

Example 8 (Singular; coarse) *Let commands be computing a GB, first by lex, then by tdrl.*

```
parallelWaitFirst(commands,args);
  [1] empty list
  [2] 11
parallelWaitAll(commands,args);
  [1] 55
  [2] 11
```

Theorem 9 (Hironaka, 1964) *Every curve over characteristci 0 K can be resolved by a finite number of blowups.*

We actually geta tree of charts — how does one make this parallel?

Fraunhöfer in Applied Mathematics at Kaiserslautern, which has a parallelism methodology based on Petri nets: trying to work with them.

Example 9 (De Rham Cohomology) *Use Weyl algebra to compute this. Implemented in Singular.*

Example 10 (Sheaf Cohomology) *Done via a constructive version of Bernstein–Gel'fand–?? correspondence. Made constructive via ??*

Example 11 (`homalg` example) *Baraket's dream to construct low rank vector bundles on projective spaces using* `homalg`.

Chevie Useful,but part Maple and part (ld) GAP; needs reimplementing.

Atint Tropical Geometry. Under development.

Future Closed connection, using Julia as a connection language

Databases Small Group in GAP. Graded Ring Database by Gavin Brown/Alexander Kasprzyk.

Challenge Generic concepts to make such databses easier to access to connect.

Phylogenetics The strand symmetric model reflects the symmetry of DNA. Computing invariants of this model on "three loaf claw tree" was open. Hilbert-driven GB in singular took 26 days and produced a 416812 element GB. Were beaten to this by an American mathematician who had a better subdivision.

Docker might be the answer to making these software images easier to use. Also jupyter notebooks.

Q SAGE?

A We are a smaller tent than SMW's. SAGE is up-down communication, whereas we are thining of peer-to-peer

Q–SMW Versions etc.

A–Joswig Use Jenkins for continuoous integration.

Q

A

3.2 GBLA — A Groebner Basis Linear Algebra Package: Eder

Note that the matrix formulation is already close to triangular. Dynamic column swapping destroys the monomial ordering, but can do a static re-ordering before GE provided we invert afterwards. A 'non-pivot' columm is one with no leading non-zeros. Sort all pivot columns to front. Then do pivot rows at the top. Then the upper-leftis always upper-triangular, and hence its elements corrspond to knwon GB rows. Then reduce the lower left to zero. Then reduce lower right. A very large matrix shows a lot o fblocking structure. F4 computtaion of Katsura-1, degree 6. 21Kx22K, 24M nonzeros (5%).

$\begin{matrix} A & B \\ C & D \end{matrix}$ where A is sparse UT, C is sparse. Multiply by A^{-1} to make A identitiy, which makes B denser. Says he has OpenMP implementations in 16-bit primes, and FP, which scale well to 32 cores at least. We have a huge matrix database: > 500 matrices

and 280GB. `http://hpac.??`. The sparseness is non-random — if $m_{i,j} \neq 0$ then its neighbours are morely likely to be non-zero. Hence we do a multiline TRSM step.

GBLA has two matrix formats, and can also convert to/from Magma. If a row is a scalar multiple of another, then the second format allows for this. Takes 1/3 the memory (really matters!).

FL implementation requires *a priori* memory allocation. Speeds up to 16 cores, but barely to 32. GBLA0.2 seems to scale well up to 32 cores (often $\times 20$, smetime sonly $\times 10$). Our one-core implementation is comparable to Magma 2.20 on small-medium sizes, and $\times 2$ or more on bigger examples. Note that Magma is using FP, and we are using medium primes (hence JHD notes the memory bandwidth requirement of Magma would be twice as great).

1. Optimize GBLA for FP and 32-unsigned arithmetic.
2. New version open source C library GB to get a F4 implementation
3. Firststeps to CPU/GPU heterogeneous implementation.

3.3 CGS Real QE: Fukasaku

A GCS is a set of pairs (GB, side-conditions on parameters). CGS-based QE was introduced in [30]. This is efficient when $\#F$ is large, but the problem is large $\#Q$. Needs Multivariate Real Root Counting MRRC. Let I be a -dim ideal. Let $A_I = R[\mathbf{x}]/I$. Consider this as a vector space and let $\{t_i\}$ be a basis. Let $\theta^I_{q,i,j} : A \to A : f \mapsto ht_it_jf$.

Theorem 10 *One of these is satisfied*

(i) $I' = \langle 1 \rangle$. *Then no roots*

(ii) *Otherwise* p_i *and* q_j *are invertible in* $A_{I'}$. *Then these are satisfied.*

(1) *Sign*$(M_1^J) \neq 0 \Leftrightarrow \#\{??\}$

(2)

Note that GBs compute zero-dimensional tests and the representation matrices of $\theta^I_{q,i,j}$. Then if I has parameters, we get CGS. Sign(M_1^J) is computed by Descartes rule on characteristic polynomial.

Definition 2 *Let* $S \subset \mathbf{R}^m$. *Definite a partition of* S, *each* S_i *is called a segment and is identified with its defining formula.*

Definition 3 *A CGS has* $\{S_i\}$ *a partition of* $\mathbf{R}^m$ *and* $G_i|_a$ *is a GB* $\forall a \in S_i$.

1. $\exists \mathbf{X} \phi$
2. Introduce new $Y_1, \ldots, Y_t, Z_1, \ldots, Z_u$.

3. $\{(S_i, G_i)\}$ a CGS of $\langle \ldots \rangle$.

4. ...

Five examples (all purely existential). In general has smaller formulae then the others (one counterexample is RC/Maple). `http://www.mi.kagu.tus.ac.jp/~fukasaku/??`.

Q-JHD Your examples were purely existential.

A Yes, that's the formalism we can deal with.

Subsequently, JHD was referred to `http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-20160509/benchmark/computation-time/`.

3.4 Software Library for Triangular Decompositions: Mou

$R := K[x_1, \ldots, x_n]$ with $x_i < x_2 < \cdots$. Hence triangular in terms of greatest variables. Various formalisms: characteristic, regular normal, simple (i.e.squarefree), irreduciable.

Definition 4 *Given $F, G \subset R$, compute a finite set of (T_i, U_i) with that the union of the zeros of these are the ....*

Aimed to release today, but integration problems: real soon now. As an application, can prove geometric theorems automatically. Can also do ordinary differential version of charsets. We can decompose algebraic varieties into irreducible components. `sisys` module can deal with requirements: regular chains etc.

`GEOTHER` proves geometric theorems, e.g. Simson's under five side-conditions: A, B, C not collinear; AC non-isotropic, BC non-isotropic, $AB \not\perp BC$, $AC \not\perp AB$.

W-characteristic sets: combpine reduced LEX GB, to get W-characteristic sets. [Wang2015, Theorem 3.9]. Then each G_i is equidimensional, and the corresponding C_i can be transformed into a Ritt characteristic set. $\mathrm{sat}(C_i) = \langle C_i \rangle \Leftrightarrow \mathrm{sat}(C_i) = \langle G_i \rangle$.

See `http://epsilon.cmou.net`.

Q Your Simson's had the first two points at $(-x_1, 0)$ and $(x_1, 0)$. What happens if you make then generic.

A One could do, but we always want to make this sort of choice to reduce free variables.

3.5

Solvable polynomial ring, $\mathbf{Q}(x, y, z, t; Q_x)_{/\mathcal{I}}\{r; Q_r\}$. Not commutative variable,s but with commutator relationship. Java sstem, wth `mfac.addSolvRelations`(commutators) etc. b equals $(b * a^{-1}) * a = f$, but b has four terms, and f has 150. Hence we need reduction to lower terms. Can have parametric coefficient rings.

Can ask questions about the Ore conditions.

Theorem 11 *Noetherian rings satisfy Ore.*

Can be computed [Apel].

Common divisor algorithm. Compute left/right content by recursion, then make primitive. Then regard as univariates and use Euclid with pseudo-remainder (which need computation of Ore conditions). These Ore conditions are still pretty expensive (syzygies on multivariates).

3.6 Integration: Introduction: Koutschan

Tables were around long before computers.

3.7 Computer algebra tools for integrals: Raab

[JHD was sitting outside the packed lecture theatre, only able to listen]. Distinguish definite from indefinite. Note that indefinite integrals are easy to verify (differentiate), but defnite ones can be harder.

In general special functions satisfy lots of identities with respect to their parameters, which help.

Talks about the parallel approach, with a suitable Ansatz on the denominator and the degree bounds in the numerator. [15, 16].

3.8 A Discussion of the Practical Issues of Computing Integrals in Maple: Roche (& May)

1. Sanity checks and dealing with `x=x[1]...x[2]`. Some work with `assume`. Deals with inert functions.

2. Maple is an inside-out evaluation model, whereas for integration, the bounds, say, can help, and also for nested (as opposed to multiple-integral syntax) integrals. Expressions versus procedures. Spot floating point and send to `evalf/int`. Convert float/rational as required.

3. Dispatch to definite/indefinite solver as appropriate.

4. Defnite has a long list of methods tried in a predefined order. `ftoc` uses Fundamental Theorem of Calculus, but `ftocms` uses multiseries for the limits. There was a bug which caused the same integral to be evaluated twice (renaming `assume`'d variables screwed memo). These need to handle the "discontinuities of the integral"[1] issue. We still have problems with this. `method=` lets you choose. Note also `infolevel[int]:=5`..

[1] JHD: essenially branch cut problems, I suspect.

Indefinite also has a range of methods. Have recently fixed some "only valid on $\mathbf{R}$" bugs. I've worked on making `assume/is` more efficient, and making sure that `remember` gets it right. Various statistics on how often methods are successful. For defnite, `ftoc` has a very low success rate.

3.9 Recent Developments in the RUBI Integration Project: Jeffrey (& Rich)

When Mathematica came out, people decried it, saying "rule-based systems don't work". See what happened there. Also, Rich wants to try this on integration. Claims that "Rubi does it better", producing not just an integral but a "better" one, which might be measured by:

1. Size of integral (as an expression);
2. Continuity;
3. Real versus complex;
4. Aesthetics.

These are not always compatible. Conside $\int \frac{x^n}{(1+x)^{12}}$. Note that Rubi's answer is sometimes different (by a constant) from Maple's, to give smaller results. $\int \frac{(x^2+2)dx}{x^4-3x^2+4}$ is in Mathematica $\arctan\left(\frac{x}{2-x^2}\right)$ even though it's not continuous, because "that's what calculus professors want", even though it has singularities.

Rubi is in Mathematica: pattern, conditions (necessary and desirable) and rule. 6000 rules and a test suite of 55000. There are so many rules partly to get special cases "right". A lot of the rules are also really trigonometric simplification rules. For example, if you start[2] with $3\sin(x)^2$, and `expand` it, there is no way of getting that form back.

3.10 Davenport

See `http://staff.bath.ac.uk/masjhd/Slides/JHDIntegrationatICMS-handout.pdf`

3.11 Integration in terms of exponential integrals . . . : Hebisch

FruCAS is an advanced computer algebre sytem forked from Axiom, about 30% of the mathematical code (via `wc`) is new.

1. Improvements to integration
2. Limts via Gruntz's algorithm [20].

[2]This was JHD's notes at the time. Reading it through, I am not sure I believe this. I can, though, believe $3\sin^2 x\cos^2 x$.

3. nows about most classical special functions

4. a "guessing" package

5. computations in quantum probability

6. noncommutative GB.

From Axiom we had probably the best Risch algorithm. But there algorithm still isn't complete, and there is no rule fallback. Porting Rubi would be difficult, as the transformed form is not Rubi-relevant. Note that there's work such as [11, 12], but considered impractical. $\mathrm{Ei}(x-x_0)' = \frac{exp(x-x_0)}{x-x_0}$: analogous to exponentials as log is to rational functions.

```
integrate(exp(x)/(x^2-2),x)
```

$\frac{\mathrm{Ei}(-\sqrt{2}+x)e^2-\mathrm{Ei}(\sqrt{2}+x)}{2\sqrt{2}e^{\sqrt{2}})}$ The result may appear as li, as in $\mathrm{li}(xe^x)$. erfi is a special case of incomplete Γ, so can produce this when relevant.

$$(x^2+2)e^{\frac{x}{x^2+2}} + \mathrm{Ei}(\frac{x}{x^2+2})$$

can be produced where no other system does this.

(Unlike original Axiom) I move trigonometric into complex exponentials.

3.11.1 Theory

Differential fields. If $v' = u'/u$ we say that u is an exponential element and v a logarithmic element. For example, if θ is Lambert W, then θ/x is an exponential element, and $-\theta$ is the corresponding logarithmic element.

Theorem 12 *Th egroup of logarithmic elements under addition modulo additive constants iin a finite rank free abelian grou. Same for the multiplicative group of elementary elements.*

Theorem 13 (Liouville Generalised) *If Gamma-elementary,* $f = v_0' + \sum c_i \frac{v_i'}{v_i} + \sum c_i v_i' \frac{u_i}{v_i} + \sum c_i v_i' w_i u_i$. *Only algebraic extension is the constants and the* w_i.

Q Is this complete?

A In theory, yes. Implementation has gaps.

3.12 Method of Brackets: Jiu

$\int_0^\infty f(x)dx$ integrate din terms of series, with only six rules.

Definition 5 $\phi(n) := \frac{(-1)^n}{n!}$

List of siz rules, which comes from Ramanujan's Master Theorem.

Theorem 14 (RMT)

$$\int_0^\infty x^{s-1}\left\{a(a)-\frac{a(1)}{1!}x+\cdots\right\}dx=a(-s)\Gamma(s). \tag{3.1}$$

1. Apply the rule
2. Keep track of s
3. Inex=#sums-#brackets

Q Complete?

A I have a counter-example, where the analytic continuation in (3.1) doesn't work. .

Chapter 4

14 July 2016

4.1 UniMath — a library of mathematics formalised in the univalent style: Voevodsky

More about the style than the GitHub where the library is. Saw a course in Oxofrd "Constructive Mathematics", which was really about algorithms. UniMath is a library of constructive mathematics (Brouwer-style) rather than necessarily algorithms.

Various uses.

1. Verify a complicated proof
2. Explore constructive ramifications of a classical area
3. teaching tool to see what rigorous proofs are

Aim is to have a language readable by humans and computers. Recently had a new colleague, and both I and the computer can read his files.

But to explain UiMath I must explain "univalent", and this is work in progress. Formal part starts with ZF. Bourbaki viewed mathematics as operations on sets. But it's hard to connect to our intuition. I think of well-founded rooted trees. It is then possible to indue ZF structure on obecjts like quotients. So we haven't quite decided on what is the formal language, hence I am talking about the intuitive side.

Element-level mathematics works iwth numbers etc. Then there is set-level mathematics. Higher-elvel mathematics as we know it now is category theory. It works with structures or colelctions whose elements are sets with structure.

It is "standard" that the category of sets do not form a set, etc., because "there are too many sets". Also, two sets can be "equal" in more than one way, depending on what one means by "equal". Equality should "preserve all mathematical properties".

Since two sets can be equal in different ways, "therefore" two abstract sets do not form a set. Therefore there are even small collections that are not sets, and this is made precise for us by "h-level". If T is a collcetion, we say "a:T" to mean that a is an element of T. Let `Id T a a'` (or $Id(T, a, a')$) be the collection of equalities between elements a

and a' of T. A collection has h-level 1 is any such `Id T a a'` has precisely one element. In classical mathematics, there is the empty set and the set with one element.

h-levle 2 if such an `Id T a a'` is either empty or has exactly one element. The collection T that has two two-element sets has every `Id T a a'` having two elements, therefore this is at h-level 3. This given us a straightforward induction on n to define h-level n. But hwat of $n = 0$. The collection that consists of one two-element set has h-levle 3.

Hence we need to use homotopy theory. A collection of h-levle 0 is represented by a *contractibe* homotpy type and `Id T a a'` by the space of paths between points a and a' of T. A collectio of h-lelve 1 will then be a homotopy type that is contractible or empty, and a collecyion of h-level 2 by a homotopy type that is homotopy equivalent to a discrete set. This representation is very useful for intuition, but not so from a foundation perspective. Collections of h-level 0 then can be faithfully defined in Martin-Löf type theories. There are things that don't have finite h-levels, e.g. 2D sphere. In Martin-Löf we might say (and this is key)

$$\texttt{Definition iscontr(T:Type):=} \sum(x:T), \prod(y:T), \texttt{Id T y x}$$

which is Coq we see as

```
Definition iscontr(T:UU) :=
     total2(fun x:T => forall (y:T), paths y x)

Definition isaprop

Theorem isapropiscontr (T:Type)  := isaprop(iscontr T)
```

show stat .... This has the same form as the ML notation. It can be proves in UniMath assuming the Univalence Axiom,

Q You put homotopy theory as the start, but deciding contractibility is undecidable.

A It is at the top of the intuitive understanding, not the formalisation.

Q I don't like "collection": why not type?

A A collection is part of a museum, and a museum has a great deal of structure.

4.2 Coq for HoTT: Sozeau

Universes are the type of types. `Type@{0}<Type@{1}<....` This avoids Type:Type paradox. $id_\ell : \prod(A : Type@\{\ell\}), A \to A$. $\Rightarrow_\ell$ is quantified at the definition level, and is instantiated. Chpoces in Coq.

1. Keep with Russell's typical ambiguity (i.e. do inference)
2. Allow user annotations

3. Cumulativity, constraint-based
4. Unification is complete ($\neq$ algebraic universes), important for automation
5. Rely on state-of-the-art constraint checkingg
6. cuulativity and inductive types.
7. ArXiV1112.0784.
8. Local and global type-in-type options for experimenting, but definitions using type-in-type are flagged/tainted.
9. Why generalisaed rewqriting when we have Id-elimination? Becaus eId is not the only interesting relation, and even witha univalent equality, Id-ewlim is not enough.

4.2.1 Rewriting in Type Theory

Move from substitution to congruence. Built-in substitutipn (Leibiz equality/J-eliminator.

$$\prod A(P : A \to Type)(xy : A), Px \to x = y \to Py$$

Applies to any context, but iterated rewrites give large proof terms. Congruence:

$$ap : \prod AB(f : A \to B)(xy : A), x = y \to fx = fy$$

Applies at top level only, but produces smaller proof terms, and generalised to n-ary and parallel rewriting. Still liited to $=$.

So we want to apply .... This gives us generalised rewriting on any relations, and multiple signatures for a given constant. Thisgives us "poor man's quotients" and reasoning on setoids (type+equivalence relation), and bisummulations.

Rewriting is just one instance of reasoning up to monotonicity/logical relations. See `coqrel` library ([J.Koenig CoqPL'16]). Transfer is a librray to transfer theorems along such relations.

```
Class Related ..
```

becomes a key definition We then egenralise the logical relatio to dependent types.

4.3 Inductive sets in UniMath: Ahrens

Now "from natural numbers to the lambda calculus'.

4.3.1 UniMath

Goal a core language of dependenet types. Rich enough to formalise matheatics. Simple enough to allow for a proof of (equi-)consistency. Ib pratcice it's a fragment of Calculus of Inductive Constructions implemented in Coq.

Inhabitation $a : A$

Dependent Type $x : A \vdash B(x)$

Sigma type

...

Do not have: recorddtype, general inductive types, general HTTs.

Librraies for foundation, category theory etc.

4.3.2 What are inductive types

Types of tree-like data. Need a notion of a signature. Specifies shape of trees by specifyingthe type of nodes and the number of subtrees. Twqo notions

Binding

Matthew–Uustalu A function: $H : [C, C] \to [C, C]$ and a complication forgetful function. So $H(F) := F \times F + F \circ \mathit{option}$ for lambda-calculus.

We construst M+U signatures form binding signatures; the datat type (functor on Set) speified bya binding signature. Hence a model (substitution system of a M+U signature on this data type. Hence a monad form every substitution system.

We construct initialalgebaras of $F : C \to C$ (Asámek) as colimits. These comes form coproducts and coequalizers. The substitution operation comes fro a Generlized Mendler Iteration. Asserts the noque existence of a morphism making some diagram commute. This comes with a suitable fusion law.

The binding signature of ML TT is more than one slide's worth.

4.4 The HoTT/HoTT Library in Coq: Designing for Speed: Gross

How should theorem provers work? Example of currying equivalence: functoriality etc. takes 17sec, but conguence takes 2m46s. 5sec with Unique Identity Proof. Hence we need to be very careful. See `https://github.com/HoTT/HoTT`.

4.4.1 HoTT/HoTT Library

Basic type formers and their identity types. h-levels, object classifier. Many examples of HITs from the book: circule, interval, suspensions, flattening, truncations, quotiens. $\pi_1(S^1) = \mathbf{Z}$.

Q–VV What do you mean by circle? Quite a debate

Large Type Theory diagram

4.4.2 What make sthem slow

Lots of repetition, lots of unnecessary work. Also using a slow langauge (when you could use Python!). Graph of duration of tactics as a function of term size, but semed hard to understand. The biggest culprit in term size is nested arguments. The user can have better abstraction barriers.

Q Does Coq have sharing?

A Yes, doesn't help, because the type checking isn't cached.

```
Record Graph:=(V:Type; E:V->V->Type }
Record IsGraph (V:ype) (E:V->V->Type:={}
```

Second is much slower.

Also took a proof assistant fix. 4m52s to 28s

4.5 Ion

Materials EuDML, ArXiV, IMU Proceedings, JSTOR, Euclid, HatheTrust.

Cataloguing zbMath, MathSciNet, Beebe

Reserach Data

Authority, Trust and Provenance trustchains etc. We currently don't sign papers.

Crowd Sourcing Research Gate, Google Scholar, LinkedIn medneley, Bibsonomy.

Classification MSC, now in SKOS.

Semantic Intermediate Abstraction Language

Note that the Fields Workshop white paper says little, because of the issues in Section 2.1. Might formalised abstracts be a useful stepping-stone? Atiyah etc. Mathematician's Workbench, based on ISO 12083, towhich MathML was a response. Now OpenDreamKit.

Q When?

A Something this year: quite what, and takeup, are interetsingquestions. Note that it took TEX 15 years to take off.

4.6 Buchberger

Inthe 19th century, we had "methods", precursor of algorithms. GDML group former after ICM 2014.

Theorema: human readable. automated generation. Able to work at object level and meta level. 2001 organised the first (MK)M conference. Contrast with Hazewinkel's M(KM). Lists EuKIM consortium. Knowledge Infrastructure for Mathematics. Contrasts coarse grain (papers) and fine-grain (formula). Need a particular branch of mathematics with a specific logic to attach detailed semantics. But muost people don't care: hence flexiformal.

Should have a Kernel Portal, able to access the exitsing mathematical sources. It will need an KB of knowledge sources. Also access to Knowledge processing Tools. So who does the portal? Nobody — it's all in our heads. Ask Stephen Wolfram to do it. Publical cooperative effort. Note that portals are the future: look at Uber, Ali Baba, Apple App Store, each of which are the largest in the world, but actually don't have anything.

Q The portals you cite are all private. You said that mathematics was a social business, but where is this reflected?

A These portals have no theory of their social interatcion, but it happens.

4.7 Mathematical Videos and supplementaries in TIB's AV Portal: Runnworth

Like a YouTube for science. Heriate of Göttingen Archive. Try to contact athors/actors and get the legal rights if possible. Interviews are very popular. We try to do metadata enrichment.

1. DOI assignment
2. scene recognition
3. text recognition
4. speech recognition
5. visual concept detection
6. named object detection
7. ...

Mathematics is a big problem for film. need to deactivate OCR, for example. But these are the most active communities. Mathematics crops up everywhere.

1. Visual simulatin data

2. video abstracts

3. conference recording (including discussions etc)

4. lecture recordings. Much of this has handwriting recognition challenges. Additional materials might be LaTeX script, but also the homework that goes whit it.

There is a button to add links, but we only link to open access (and into our Library's system). Much of the linking is manual currently: needs much automation.

Q How do you find information: automatically? I note that Google relies, essentially, on people buidling links.

A Possibly, but computerised speech recognition, at least for English and German, is better than humans now. That's not true of Hungarian.

4.8 Mathnet-Ru: Chebukov

Shows a graph of growth of material held. We have videos in the database. Notes that a journal atricle live sina well-structured world.

Q Anything special formathematics?

A No, but we use HD. Russian 'text from speech' is not very good.

Q Statistics?

A We count views, but not correlations between them, or length of views.

4.9 Border basis for polynomial system solving and optimization: Mourrain

$R := K[x_1, \ldots, x_n]$, $I = (f_1, \ldots, f_s)$ and compute $A = R/I$. We have a Monomial Server, Normal Form Storage, and algebraic algorithms which communicate with them.

Let B be a set of monomials connected to 1: $\{1 \in B; \forall m \in B \setminus \{1\} \exists m' \in B, i \in [1,n] s.t. m = m' x_i\}$. $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$, and $\partial B = B^+ \setminus B$.

Definition 6 *A* border basis *of R for I is a set of relations of the form $f_\alpha = x^\alpha - \sum_{\beta \in B} \lambda_{\alpha,\beta} x^\beta$ for $\alpha \in \partial B$, such that $\langle B \rangle \cap (f_\alpha) = \{0\}$.*

Each $x^\alpha \in \partial B$ yields a rewriting rule. These are constructed by saturation: reducing the commutation polynomials. $C(f_{\alpha_1}, f_{\alpha_2}) - x_{i_1} f_{\alpha_1} - x_{i_2} f_{\alpha_2} \in \langle B^+ \rangle$. Claims it's numerically more stable, akin to pivoting in LA.

Polynomial optimisation: border basis of the minimiser ideal, and the minimizer points. Real radical: take $f = 0$.

Moment relaxation. Compute a linear functional σ given by its moments such that

- $H_\sigma^{S,S'} = (\sigma_{\beta+\beta'} \succeq 0$
- $\langle \sigma | p \rangle = \sum_\alpha \sigma_\alpha p_\alpha = 0$ for $p \in F$
- $\langle \sigma | f \rangle = \sum_\alpha \sigma - \alpha f_\alpha$ is minimal.

Borderbasix is a package of Mathemagix. needs Linalg, etc.

Comparisions for Katsura-n, Cyclic-n (5,6,7) over $\mathbf{F}_{32051}$, and some examples over $\mathbf{Q}$.

Bibliography

[1] M.Á. Abánades, F. Botana, A. Montes, and T. Recio. An algebraic taxonomy for locus computation in dynamic geometry. *Computer-Aided Design*, 56:22–33, 2014.

[2] J.A. Abbott. Fault-Tolerant Modular Reconstruction of Rational Numbers. `http://arxiv.org/pdf/1303.2965.pdf`, 2013.

[3] K.I. Appel and W. Haken. Every Planar Map is Four-Colorable. *Bull. A.M.S.*, 82:711–712, 1976.

[4] N.H. Arai, T. Matsuzaki, H. Iwane, and H. Anai. Mathematics by Machine. In K. Nabeshima, editor, *Proceedings ISSAC 2014*, pages 1–8, 2014.

[5] D.H. Bailey, J.H. Borwein, and V. Stodden. Set the default to 'open'. *Notices A.M.S.*, 60:679–680, 2013.

[6] C. Benzmüller and B.W. Paleo. The Inconsistency in Gödel's Ontological Argument: A Success Story for AI in Metaphysics. In *Proceedings IJCAI 2016*, pages 936–942, 2016.

[7] J. Böhm, W. Decker, C. Fieker, and G. Pfister. The Use of Bad Primes in Rational Reconstruction. `http://www.mathematik.uni-kl.de/~pfister/Artikel/badcrt210612.pdf`, 2012.

[8] C. Bright and A. Storjohann. Vector rational number reconstruction. In *Proceedings ISSAC 2011*, pages 51–58, 2011.

[9] L. Busé and B. Mourrain. Explicit factors of some iterated resultants and discriminants. *Math. Comp.*, 78:345–386, 2009.

[10] O. Caprotti, J.H. Davenport, M.C. Dewar, and J.A. Padget. Mathematics on the (Semantic) NET. *Semantic Web: Research And Applications*, pages 213–224, 2004.

[11] G.W. Cherry. Integration in Finite Terms with Special Functions: the Error Function. *J. Symbolic Comp.*, 1:283–302, 1985.

[12] G.W. Cherry. Integration in Finite Terms with Special Functions: the Logarithmic Integral. *SIAM J. Computing*, 15:1–21, 1986.

[13] A. Church. A formulation of the simple theory of types. *J. Symbolic Logic*, 5:56–68, 1940.

[14] 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.

[15] J.H. Davenport. On the Parallel Risch Algorithm (I). In *Proceedings EUROCAM '82 [Springer Lecture Notes in Computer Science 144*, pages 144–157, 1982.

[16] J.H. Davenport and B.M. Trager. On the Parallel Risch Algorithm (II). *ACM TOMS*, 11:356–362, 1985.

[17] M. England, R. Bradford, and J.H. Davenport. Improving the Use of Equational Constraints in Cylindrical Algebraic Decomposition. In D. Robertz, editor, *Proceedings ISSAC 2015*, pages 165–172, 2015.

[18] M. England and J.H. Davenport. The complexity of cylindrical algebraic decomposition with respect to polynomial degree. *To appear in Proc. CASC 2016*, 2016.

[19] G. Gonthier. Formal Proof — The Four-Color Theorem. *Notices A.M.S.*, 55:1382–1393, 2008.

[20] D. Gruntz. On Computing Limits in a Symbolic Manipulation System. *ETZ Zuerich Dissertation 11432*, 1996.

[21] T.C. Hales, M. Adams, G. Bauer, D.T. Dang, J. Harrison, T.L. Hoang, C. Kaliszyk, V. Magron, S. McLaughlin, T.T. Nguyen, T.Q. Nguyen, T. Nipkow, S. Obua, J. Pleso, J. Rute, A. Solovyev, A.H.T. Ta, T.N. Tran, D.T. Trieu, J. Urban, K.K. Vu, and R. Zumkeller. A formal proof of the Kepler conjecture. `http://arxiv.org/abs/1501.02155`, 2015.

[22] S. Marcus and S.M. Watt. What is an Equation? In *Proceedings SYNASC 2012*, pages 23–29, 2012.

[23] 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.

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

[25] S. McCallum, A. Parusinski, and L. Paunescu. Validity proof of Lazard's method for CAD construction. `https://arxiv.org/abs/1607.00264`, 2016.

[26] R. Recorde. *The Whetstone of Witte*. J. Kyngstone, London, 1557.

[27] V. Stodden, D.H. Bailey, J. Borwein, R.J. LeVeque, W. Rider, and W. Stein. Setting the Default to Reproducible: Reproducibility in Computational and Experimental Mathematics. `http://icerm.brown.edu/html/programs/topical/tw12_5_rcem/icerm_report.pdf`, 2013.

[28] M. Suzuki. Infty (2011). http://www.inftyproject.org, 2011.

[29] S.M. Watt. Mathematical Document Classification via Symbol Frequency Analysis. In S. Autexier *et al.*, editor, *Proceedings AISC/Calculemus/MKM 2008*, pages 29–40, 2008.

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

[31] F. Wiedijk. The De Bruijn Factor. http://www.cs.kun.nl/~freek/notes/factor.pdf, 2000.

[32] W.-T. Wu. Basic Principles of Mechanical Theorem proving in Elementary Geometries. *J. Syst. Sci. and Math. Sci. (Beijing)*, 4:207–235, 1984.