Various lectures notes I have taken

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

July 2009
(While on Sabbatical at the University of Waterloo)

Contents

1 6 July 2009 **6**

1.1 Computational Logic and Pure Mathematics: Pure and Applied — Rob Arthan . . . 6

1.1.1 Linear Continuous Control Systems . . . 6

1.1.2 Opportunities and Issues for Automated Reasoning . . . 6

1.1.3 Decidability for Vector Spaces . . . 6

1.1.4 A Challenge . . . 7

1.2 Combining Coq and Gappa for Certifying Floating-Point Programs — Boldo/Filliâtre/Melquiond . . . 7

1.3 An implementation of branched functions — Jeffrey . . . 8

1.4 Producing “tagged PDF” using pdfTEX — Ross Moore . . . 9

1.5 Smart Pasting for ActiveMath Authoring — Libbrecht, Andrès & Gu . . . 10

1.6 Math Handwriting Recognition in Windows 7 and its Benefits — Marko Panić, Microsoft Serbia . . . 11

1.7 Understanding the (current) rôle of computers in mathematical problem solving — Bunt/Lank/Terry (Waterloo) . . . 12

1.7.1 What are the opportunities for design? . . . 13

1.8 A customizable GUI through an OMDoc documents repository — Heras *et al.* . . . 13

2 7 July 2009 **14**

2.1 Combined Decision Techniques for the ∃ Theory of **R** — Grant Passmore, Edinburgh . . . 14

2.2 Invariant properties of Third-order non-hyperbolic Linear Partial Differential Operators — Shemyakova . . . 15

2.3 A Groupoid of Isomorphic Data Transformations — Tarau . . . 16

2.4 Mathematical Equality and Pedagogical Correctness — Bradford, Davenport and Sangwin . . . 16

2.5 Conservative retractions of propositional logic theories by means of boolean derivatives. Theoretical foundations — Aranda-Corral, Borrego-Díaz & Fernández-Lebrón . . . 17

2.5.1 Future Work . . . 17

2.6 Abstraction-Based Information Technology — Jacques Calmet (by Skype) . . . 17
2.7 Proof reuse in a Mathematical Library — Noyer & Rioboo . . . 18
2.8 Reflecting Data: Formally Correct Results for Efficient (and Dirty) Algorithms — Dixon . . . 18
2.9 Calculemus Business Meeting . . . 19
2.9.1 . . . 19
2.9.2 . . . 19
2.9.3 . . . 19
2.9.4 . . . 19
2.9.5 Summary . . . 19
2.9.6 Elections etc. . . . 19
2.9.7 Any Other Business . . . 19

3 8 July 2009 20
3.1 Similarity Search for Mathematical Expressions using MathML — Yokoi (Tokyo) . . . 20
3.2 Improving Mathematics Retrieval — Kamali & Tompa, Waterloo 21
3.3 An Online repository of mathematical samples — Sorge *et al.*, Birmingham . . . 22
3.4 Digital Mathematical Libraries in France — Thierry Bouche, Grenoble . . . 22
3.5 Experimental DML over digital repositories in Jamap — Namiki it et al. . . . 23
3.6 Math Literate Computers — Dorothy Blostein, Queen's University 24
3.7 Document Interlinking in a Digital Math Library — Goutorbe (presented by Bouche) . . . 24
3.8 I2Geo — a web library for interactive geometric constructions — Libbrecht *et al.* . . . 25
3.9 Report on the DML-CZ project — Petr Sojka *et al.* . . . 26

4 9 July 2009 27
4.1 OpenMath in SCIEnce — Roozemond & Horn . . . 27
4.2 — Carlisle NAG/MathML . . . 27
4.3 OpenMath CDs for quantities and units — Collins . . . 28
4.4 Content Dictionaries for Algebraic Topology — Heras *et al.* . . . 28
4.5 Intergeo File Format — Libbecht *et al.* . . . 28
4.6 A Better Rôle System for OpenMath — Rabe . . . 29
4.6.1 Our proposal . . . 30
4.7 Semantics of OpenMath and MathML — Kohlhase . . . 31
4.7.1 A syntactic semantics . . . 31
4.7.2 OM-Models . . . 31
4.7.3 Difficulties . . . 32
4.8 The Evolving Digital Mathematics Network — Ruddy (Cornell) . 32
4.9 `wiki.openmath.org`: how it works and how to collaborate — Lange (Bremen) . . . 33

4.10 OpenMath Business Meeting 34

5 10 July 2009 **37**
5.1 28.5 years of Maple: ??? — Gonnet 37
5.1.1 "Option remember" and unique representation 37
5.1.2 "memory and GHz are cheap" 38
5.1.3 Use of C 38
5.2 38
5.3 Inplace arithmetic for univariate polynomials over algebraic number fields 39
5.4 Compact recognition of handwritten mathematical symbols — Golubitsky (UWO) 39
5.5 — ffitch 40
5.6 Lazy and forgetful polynomial arithmetic and applications — Paul Vrbic (SFU→UWO) 41
5.7 Criteria for Compactness in the Design of Maple — Geddes . . . 42

6 11 July 2009 **43**
6.1 The Characteristics of Writing Environments for mathematics — Gozli, Pollanen, Reynolds 43
6.2 Canonical forms in interactive assistants — Heeren & Jeuring . . 44
6.3 Some Drawbacks Appearing in Conversion of TEX Generated Documents to Adobe Acrobat PDF File Format — Pejovic, Mijajlovic 45
6.4 Representations for Interactive Exercises — Goguadze, presented by Libbrecht 46
6.4.1 Anatomy of an Exercise 46
6.5 Some Traditional Mathematical Knowledge Management — Ion (Mathematics Reviews) 47
6.6 OpenMath in SCIEnce: SCSCP and POPCORN — Roozemond & Horn 48
6.7 Using Open Mathematical Documents to interface Computer Algebra and Proof Assistant Systems — Heras 48
6.8 Content Management in ActiveMath — Libbrecht 49
6.8.1 Content Management and Aggregation 49
6.8.2 Imports 49
6.9 The FMathL Language — Schodl, Neumaier, Schichl 49
6.10 A Linear Grammar Approach to Mathematical Formula Recognition from PDF — Baker *et al.*, Birmingham 50
6.11 Confidence Measures in Recognizing Handwritten mathematical Symbols — Golubitsky & Watt 51

7 12 July 2009 **52**
7.1 A Saturated Extension of Lambda-bar-mu-mu-tilde — Mamane, Geuvers, McKinna 52
7.2 Finite Groups Representation Theory with Coq — Ould Biha . . 53

7.3 The MMT Language — Rabe 53
7.4 Natural Deduction Environment for Matita — Sacerdoti Coen, Tassi 54
7.5 MathLang Translation to Isabelle Syntax — Lamar, Kamareddine, Wells 55
7.6 Crafting a knowledge base of transformation rules: integration as a test case — Jeffrey & Rich 55
7.7 Software Engineering for Mathematics — Gonthier *et al.* 56
7.7.1 Diagnosis 57
7.7.2 Big operators 57
7.8 OpenMath Content Dictionaries for SI Quantities and Units — Collins 57
7.9 Integration Web Services into Interactive Mathematical Documents — Giceva, Lange, Rabe 58
7.10 Compensating the Computational Bias of Spreadsheets with MKM Techniques — Kohlhase[2] 59
7.11 Spreadsheet Interaction with Frames: Exploring a Mathematical Practice — Kohlhase 59
.1 Gonthier at Waterloo 62

Preface

There were a variety of conferences in the "Conferences in Intelligent Computer Mathematics" (Grand Bend, Ontario).

Since JHD dotted around between the various conferences, these notes are simplify in overall date order.

Chapter 1

6 July 2009

1.1 Computational Logic and Pure Mathematics: Pure and Applied — Rob Arthan

1.1.1 Linear Continuous Control Systems

Coming from avionics control systems — continuous data and time. Simulink etc. are great for modelling, but not reasoning. Block diagram models give *intensionality*, i.e. inputs versus outputs. These block diagrams can be designs for analogue computers, or *specifications*.

Qinetiq's ClawS tool takes Simulink diagrams, converts then into Z, and the Ada code is then verified against the Z via ProofPower. The next step is to reason abot more abstract models. Signals on wires are elements of vector spaces.

1.1.2 Opportunities and Issues for Automated Reasoning

We have a Hoare logic for these diagrams. We envisage assertions expressions in (possibly linear) first-order arithmetic. The language is expressive but decidable. He noted that real closed fields are decidable but very complex. Linear arithmetic is normally implemented over the rationals, but can be implemented over a field. Key is Fourier–Motzkin elimination: convert equations into upper and lower bounds, so works over decidable ordered field. Engineers want $\sqrt{2}$ and e etc. But these aren't as easy as one would like — Schanuel's conjecture etc. [MW96].

1.1.3 Decidability for Vector Spaces

It is a conservative extension to add a norm or an inner product. Some boundary between decidable and undecidable — see ArXiv paper (Arthan, Solovay etc.). Inner product spaces are decidable

For analysis (Harrison etc.) we want $\mathbf{R}$, therefore $\mathbf{C} \equiv \mathbf{R}^2$, so what about $\mathbf{R}^n$. We want a first-order theory with two sorts $\mathcal{R}$ and $\mathcal{V}$ (we need this: one-sorted theories where the reals are merely constants don't really work). Models are vector spaces, inner product spaces, normed spaces etc.

$$\dim_V \geq k \Leftrightarrow \exists v_1, \ldots, v_k \forall a_1, \ldots, a_k a_1 v_1 + \cdots + a_k v_k = 0 \Rightarrow a_1 = a_2 = \cdots a_k = 1 \quad (1.1)$$

similarly $\dim_V \leq k$.

Concept of an extreme point: Krein–Milman theorem implies that, in finite dimension, the unit disc is the convex hull of its extreme spaces. But there are infinite-dimensional counterexamples. Therefore normed spaces are more expressive, since $\exists$ a single sentence whose only models are infinitely-dimensional. There is a sentence `Peano` which defines $\mathbf{N}$.

Take the unit circle and "shave off" NE and SW elements at distance 1/1! from $w_1 = (0, 1)$ to w_2, distance 1/2! from w_2 to w_3 etc. This gives a consttruction for $\mathbf{N}$ (ArXiV).

1.1.4 A Challenge

Can we encode sin in a bounded concave γ? The answer is in fact affirmative, with $K = M = 1$, but he has no formal proof. Can do one (being refereed) with $K = 2$, $N = 9$.

Q–JHD Real Closed fields are difficult, but can one use such tools as an oracle?

A Paulson's Metatarski uses QEPCAD as an oracle. We get lots of variables, but not that many alternations, since all the components of a vector are quantified the same way.

Q What questions can't Simulink answer?

A Stability is a good example.

Q–Ion Do engineers really want e etc., or just approximations?

A Approximations make things harder! Also, engineers do expect $\sqrt{2}^2 = 2$.

1.2 Combining Coq and Gappa for Certifying Floating-Point Programs — Boldo/Filliâtre/ /Melquiond

There are problems of both range (exceptions etc.) and precision. Example of accummulation 1/10 second over a day (Patriot errors). In 1983, truncation in the Vancouver Stock Exchange caused a 50% drop in value; in 1987, inflation in the UK caused pensions to be off by £100M; 1995 Ariane 5 explsion. In 2007, Excel displays 77.1*850 as 100,000 — this last bug had only twelve failing instances.

There's also Caduceus/Why, a tool that takes annotated C code (with pre/post conditions) and generates verification conditions for Coq, Isabelle, PVS or automated ones like Simplify, Z3. Coq has a library for floating point, but ver little automation, Gappa is a tool for checking propoerties on real-bvalued expressions. Example of the correctness of integer division (positive integers ≤ 65535, using an 11-bit approximation to $1/b$ and intermediate reuslts in `BINARY80` — 3 lines in Gappa but several pages by hand. Second example is a toy cos near 0: precondition is trivial but post-condition is hard. For example, if $x < \frac{1}{32}$ then $|\cos(x) - (1 - \frac{1}{2}x^2)| < 2^{-23}$ where the parenthesisied term is evaluated in floating point.

So input to Caduceus, have a Coq goal in the Caduceus model, convert with the `why2gappa` tactic to a Coq goal in the Gappa model, then work in Coq/Gappa. This conversion converts things into interval bounds, Gappa's language. Typically 400 lines of pure Coq reduce to 35 lines (at the cost of doubling the time).

1.3 An implementation of branched functions — Jeffrey

Many algebra systems in the 1980s had simplifications of $\sqrt{z^2} \to z$ etc., which led to what many people thought were mistakes (and many didn't!). In Maple this is known as "the square root bug", though it's more general. This continues:

$$\arctan x + \arctan y = \arctan\left(\frac{x+y}{1-xy}\right) \tag{1.2}$$

is saved by

$$\text{Arctan}x + \text{Arctan}y = \text{Arctan}\left(\frac{x+y}{1-xy}\right) \tag{1.3}$$

What is $\arctan 1$:

- $\frac{\pi}{4}$
- a set
- a given value, but content-dependent.

Maple etc. now believe that these are unique values, so how to we deal with "nonentites" such as 1.2.

I contend that the problem is the *interface* to the function. If I solve $f(z) = u$ I get a `RootOf` construct, but if f is sin, I get an explicit arcsin. If f is a polynomial, then Maple will give me all n solutions, which can be forced from $z = \sin\frac{1}{2}$ by `allvalues:=true`. In particular periodic functions are treated differently.

Hence I would like an *explicit* inverse notation, e.g. invsin etc. (including invexp and invsquare).

$$\text{invsin}_k(x) = (-1)^k \arcsin(x) + k\pi \tag{1.4}$$

etc. now become the standard formulae. Example of "honest" plotting.

$$\mathrm{Arcsin}(x) \pm \mathrm{Arcsin} y = \mathrm{Arcsin}\left(x\sqrt{1-y^2} \pm y\sqrt{1-x^2}\right) \tag{1.5}$$

has a corresponding formulation ??

A further example , showing that $\ln z$ and $\frac{1}{2}\ln z^2$ are actually different functions: we can write

$$\mathrm{invsin}_k z = -i \mathrm{invexp}_K(\mathrm{invsquare}(1-z^2,k)+iz) \tag{1.6}$$

where K has a complicated expression, but

$$\mathrm{invsin}_k z = \frac{-i}{2}\mathrm{invexp}_{\lfloor k \rfloor}\mathrm{invsquare}\left((1-z^2,k)+iz\right)^2) \tag{1.7}$$

when

Question: can anyone think of a good notation for fraction powers.

Q Weren't you a bit hard on mathematicians? It depends on the group.

A Inventing a labelling scheme for the roots of a polynomial equation is a tricky problem.

Q But computers need us to impose an order

A But the advantage of my notation is that I can write an equation that's true for all k.

Q–JC But `solve` doesn't compute solutions; it produces expressions that, if substituted in, *might* give zero.

A True.

1.4 Producing "tagged PDF" using pdfTEX — Ross Moore

[He gave a second talk later in the week, but I have merged the two]

ISO PDF is 15929, 2002; but there's been PDF/A[1] since 2005, which is actually (a subset of) PDF 1.4 (2001). There are five "standardised" forms of PDF, including PDF/X, which has seven sub-variants. PDF 1.7 became an ISO standard (32000?) in 2008. There's more coming: PDF/A.2 (2011?) .... Also PDF/UA (accessibility) is being worked on: the plan is for this to be ISO 32000-2 in the 2011/2 time-frame, which will include MathML 2.0.

The user interface is

- your usual TEXshop, MiKTEX etc.,
- your usual PDF browser, but *some* will get more out of it.

[1] Intended for archival use.

Adobe has “read out loud”.

Tagged PDF has been around since 1.4,: see §14.8 of the 1.7 specification. Note that tagging is optional. “All text shall be represented in a form that can be converted into Unicode[2] ... Word breaks shall be represented explicitly[3]; Actual content shall be distinguished from artifacts of layout and pagination[4].”

Note that tagged PDF requires a structure tree, which is quite a complicated object, of chapters, sections etc., but also a tree structure of pages etc. Items like paragraphs that straddle pages make for quite a convoluted structure. There’s also a “Rôle map”, a bit like a CSS style sheet, apparently on the lines of “I want these chapter headings to look like ...”. There also an “id tree” which lets you give names to individual pieces of the document.[5] The diagram related the four trees is extremely complicated (and has been quoted as a reason for not doing tagged PDF in pdfTEX).

Acrobat Pro (previous parts were also in Reader) allows export to XML. There’s a LATEX package to produce the corresponding metadata. Therefore the MathML could be in the PDF (as well as the appearance), and would be extractable. In his vision, every equation would also have its MathML (Presentation) version embedded in the PDF. It also supports various views of the data, e.g. in order of reading.

Summary — there’s an awful lot here.

1.5 Smart Pasting for ActiveMath Authoring — Libbrecht, Andrès & Gu

ActiveMath is a learning environment, with all the formulae in OpenMath. Authoring is done in XML, apart from the formulae, which is in “Qmath”, which isn’t TEX, since TEX doesn’t have the meaning needed for OpenMath. These semantics are needed for

1. Rendering depending on country and subject;
2. formula search;
3. cut-and-paste, e.g. into plotting tools.

Qmath is a linear syntax, with preceddence and binary operators, but takes advantage of Unicode.

$$C_1^n = \frac{n!}{1 \cdot (n-1)!} = n \tag{1.8}$$

with change to C_n^1 for Russians etc.

[2]TEX does not currently do this explicitly, and a “large closing bracket” actually has to be specified in four ways. It will take years to get the macros to do this automatically.

[3]TEX does not currently do this explicitly, an dthis has required changes to pdfTEX.

[4]In the demo, the tagged version did not read running heads etc., whereas the untagged version did, so that they suddenly (from the point of the listener) broke into the flow.

[5]In answer to a question, this is *not* related to the labels generated by `hyperref`.

Need a “smart paste”, to deal with TEX, Maple, Windows 7 “pen”, PlanetMath, Wikipedia (a TEX-like language), MathWorld etc. The WIRIS algebra systems has OpenMath tools. There is apparently a tool called BlahTEX, which does a good job on a range of TEX-like constructs.

This is all brought together with a pipeline, e.g. blahtex — webeq — David Carlisle's tools — ..., which offers alternatives, e.g. a specimen from (French) Wikipedia, looking like $\sqrt{2} \times \sqrt{2} = 2$, gives as alternatives $2 \times 2 = 2$ and $\sqrt{2} \times \sqrt{2} = 2$.

Pretty good with Wikipedia and MathWorld, *as along as* there are no indexed variables, mostly thanks to WebEQ. PlanetMath is largely jsmath, and there's some *very* wierd TEX. We believe we have pretty good “presentation to content” conversion.

1.6 Math Handwriting Recognition in Windows 7 and its Benefits — Marko Panić, Microsoft Serbia

Started as an extension of the “Tablet PC” group. Ter eis often a need toiput mathematics, but it is quite painful. amajor requirement was editable output, MathML. We also wanted reasonable responsiveness even on large formulae.

Aims to take a robust approach to identifying upper/lower case versions of the same letter.

Q What is the effort involved in adding a new symbol?

A Need samples of the handwritten symbol, and have to change the grammar. There can be knock on effects on performance, though.

Q Internationalisation?

A I have studied in Serbia, France and the US, and other team members bring other expertise.

Q What about long division?

A That's a collection of formulae, not a single formula, and thus is out-of-scope. But a good question.

Q Are the components accessible?

A Not currently.

Q–SMW How many samples?

A At least 100. We collected millions of pieces of ink.

Q This is ink, rather than scanned input?

A We rely knowing the on strokes, but not on other timing information. So it would not be trivial, but a lot easier than starting from scratch.

Q–ES (TI) We have seen it is a large system: can it be "cut down"

A It would be great to have the grammar modular, but we haven't done that. Custom function names can be added to the API, though, but they have to be written letter–by–letter.

Q Why Mathematica?

A We ended up working with Wolfram, but it is not exclusive, and we would also like to work with Maple etc. But the application has to be MathML-aware.

Q What about non well-formed expressions.

A A single class, e.g. ending in a plus, could be added, but the fundamental design is for well-formed expressions.

1.7 Understanding the (current) rôle of computers in mathematical problem solving — Bunt/Lank/Terry (Waterloo)

Really about computer algebra systems. Works on the "MathBrush' system at waterloo. Many people find this easier than, say, Maple.

As HCI people, we have to ask "what is the tool used for?". There are some laboratory evaluations [Oviattetal2006], expression entry techniques (where the pen wins, with 1-D keyboard coming second) [Anthonyetal2005], computer algebra systems [LaViolaetal2007].

We did a qualitative study on nine (3 professors, 3 postdocs, 3 graduate students) theoretical mathematicians[6]. Structured interviews with recordings and digital photographs. Did data analysis via open coding.

We sould CAS was the *only* application used in the course of the problem-solving process. LaTeX etc . were, of course, part of the communication process. Hva ehard evidence of increaing formality through the evolution of problem solving: ideation, Execution, Formalisation, Dissemination.

CAS for solving long tedious expressions. Use of words like "horrible". Also verifying hand-derived expressions. Some experimentaion and plotting.

CAS played a much more limited rôle than we expected. There were transcription problems, and the need to collaborate also intervened. It

[6]Since then, we have interviewed engineers, physicists etc., and are starting on people in companies.

was commonly stated that "hand-derived work provides better insight, facilitated pattern detection and keeps skills sharp".

Trust and reproducibility (especially for engineers) were major issues — "I tend not to trust the symbolic toolbox, even though the results are very rarely wrong".

In-place manipulations are common, and a legitimate technique, and this is not directly supported by computer algebra systems.

Errors in transcription (input and output) are a major problem. So does PenMath solve this? The speaker wonders whether this is a real problem — witness the way mathematicians master LaTeX. The interviewees *knew* that the research was part of a PenMath project.

Q–SMW Don't psychologists lie about the purpose of an experiment?

A Office of Research Ethics at Waterloo won't let us.

1.7.1 What are the opportunities for design?

1. Project Management — formalised notebooks etc. Specialised LaTeX styles.
2. Verifying as opposed to replacing?
3. Collaboration — large screen interaction is an under-researched area.
4. Flexible placement, electronic post–it, etc.

1.8 A customizable GUI through an OMDoc documents repository — Heras *et al.*

The system in Kenzo, a system in Algebraic Topology. The system is not particularly usable[7], and some operations cause errors, notably as a consequence of type errors, e.g. passing in the object rather than the simplicial group. For some processes, it is necessary to understandthec hain of commands. *But* many homotopy groups are only computable by Kenzo.

To integrate Kenzo with ACL2, as the theorem prover, we use XUL as the structure for our user interface programming. We use OMDoc documents to define that mathematical structures, and these are to be stored in an OMDoc repository.

The aession can be dumped out as an OMdoc, hence properly printed in the familiar notation. There is an OMDoc reader for ACL2 (for these objects, JHD assumed). This system integrates representation, computation and deduction.

[7]The system is written in Lisp, and this is the command interface.

Chapter 2

7 July 2009

2.1 Combined Decision Techniques for the ∃ Theory of R — Grant Passmore, Edinburgh

The basic problem is the high complexity, with respect to the number of variables, of the existing decision procedures. Combine

1. special fragment of CAD for topologically open sets
2. Gröbner bases.

RAHD, our tool in Common LISP, in integrated with PVS. It's really aimed at ∀ problems, by showing *unsatisfiability* of ∃.

QE for Real-closed fields (RCF) is doubly-exponential [DH88].

n dimension

m number of polynomials

d total degree

L bit-length.

In theory there are better algorithms than CAD/QE, but only in theory [Hon91]. Gave an overview of cylindrical algebraic decomposition (CAD) [Col75]. Expensive since the smaple points can be (vectors of) algebraic numbers. [McC93] if ϕ is an open predicate, then we can select rational sample points.

1. Split on-strict inequalities $p \geq 0$ into $(p > 0) \vee (p = 0)$.
2. Reduce to Distributive Normal Form (DNF)
3. For each clause C_i in DNF do
4. If C_i has equations, reduce the inequalities with respect to a Gröbner base for the equalities

5. Use McCallum open-CAD (QEPCAD-B).

Have a 4-variate case that was insoluble for QEPCAD-B or HOL/RealSOS, but took eight seconds in their system. Has 256 cases, of which 28 require Open-CAD. Also have a simple Positivstellensatz.

Hard to do good benchmarks, but have worked on producing a corpus, from NASA, Isabelle and HOL-light, kissing numbers. Compare their RHAD with QEPCAD-B, Redlog/Rlcad and Redlof/Rlqe. RHAD can solve many large problems that the others can't, but CEPCAD-B is much faster *when* it works. Redlog/Rlqe [Wei99] is faster where it is really applicable.

Q–JHD Variable ordering for QEPCAD-B?

A Essentially Brown's thesis.

Q What Gröbner-basis?

A Our own for ≤ 6 variables, then CoCoA. Also use CoCoA for computing radical ideals.

Q–Rioboo What about `RealSolving` and other parts of Marc's work.

A Not investigated.

2.2 Invariant properties of Third-order non-hyperbolic Linear Partial Differential Operators — Shemyakova

Bivariate case: $\hat{K} = K[D_x, D_y]$. If we have an operetor $L = \sum_{i+j=0}^{d} a_{ij} D_x^i D_y^j$, we associate a *principal symbol* $\sum_{i+j=0}^{d} a_{ij} X^i Y^j$. It is good if L factors into linears.

$$D_{xy} + a(x,y)D_x + b(x,y)D_y + c(x,y)$$

has at most two (incomplete) factorizations $(D_x + a) \circ (D_y + b) + h$ and $(D_y + b) \circ (D_x + a) + k$. The Darboux integration theorem says that there is a complete factorization iff $h = 0 \vee k = 0$, and hence his algorithm.

In general, if we write $L = L_1 \circ \ldots \circ L_s + R$ then R is *not* unique, but depends on the choice of L_i, and is not an invariant, and hence cannot be described in terms of generating invariants.

[ShemyakovaWinkler2008] solved the hyperbolic case, using [GrigorievSchwarz2004], which shows that the factorisation of the principal symbol determines the factorisation of L.

If the symbol is X^2Y, or X^3 then [ShemyakovaMansfield] we can determine the invariant (different in each case). Henc we have to consider *non-commutative* factorisations of the principal symbol. The properties of formal adjoints can reduce the number of cases to be considered. $L^{\dagger\dagger} = L$, $(L_1 \circ L_2)^\dagger = L_2^\dagger \circ L_1^\dagger$.

For the second-order case, we have that $h^\dagger = k$ and $k^\dagger = h$, but for third-order case we have a sign-change, which complicates things.

This leads to a completely automated process for determining factorability (for order 3, two variables).

Q Have you used [named other packages]

A They don't allow *symbolic* coefficients in the operator, but I use them for experimentation.

2.3 A Groupoid of Isomorphic Data Transformations — Tarau

Analogies, and analogies between analogies, emerge when we we transport objects, and operation so them. This is a creative process, e.g. geometry and coordinates, Tring machines and combinators, types and proofs. So the aim is to automate the process of finding *computational analogies* and experimenting with them.

So we want a functional programming framework to encode isomorphjisms between data types. Gödel numberings are a key tool[1], which give us ranking/unranking operations. Isomorphisms form a groupoid, shown in Haskell notation. An `Encoder` of `a` is then `Iso a Root`. This gives an encoding of (finite) objects.

We have unranking anamorphisms (unfold operation) and ranking catamorphism (fold operation). The combination is a hylomorphism. This essentially-gives us the Ackermann encoding. Applied to permutations we get the Lehmer code.

We are looking at GMP for an implementation vehicle.

Q–Rioboo What about a prover?

A We are looking at Coq.

2.4 Mathematical Equality and Pedagogical Correctness — Bradford, Davenport and Sangwin

Q–Blostein What about students learning off marking each other's work?

A The importance of peer working comes out (since students will have different examples), but not peer marking as such — good point.

Q–Carette You *can* use an algebra system: nothing says you have to parse `+` as the algebra system's $+$.

[1] This presumably corresponds to the fact that he chooses `Nat` to be the root of is system.

A True — this was essentially the first conclusion point.

Q Wouldn't giving the students the rules and the makr scheme encourage *them* to think algorithmicaly?

A It might well, but we haven't done any field-testing yet.

2.5 Conservative retractions of propositional logic theories by means of boolean derivatives. Theoretical foundations — Aranda-Corral, Borrego-Díaz & Fernández-Lebrón

Given a theory T in a language Lm and $L` \subset L$. Then we want a conservative retraction T' defined over L'.

For example $KB? \models F$. Does $[KB, L'] \models F$? There are also applications to Description Logic Reasoning, where we can remove "irrelevant" concepts.

Map into the ring $F2[X]$, with $\wedge \to \times$ and $X \vee Y \to X + Y + XY$. Define

$$\partial_p F = \frac{\partial}{\partial p} F = \neg(F \leftrightarrow R\{P/\neg p\}) \tag{2.1}$$

We have an initial implementation in Haskell.

$$\Gamma \models F \Leftrightarrow \partial_{PV(\Gamma)}\Gamma \vdash F.$$

There may be ontologies whose union is inconsistent (example given),but where we can retract away some items (those common items in the languages which give rise to the inconsistency), and then the merge is consistent.

2.5.1 Future Work

- Full implementation
- Extension to multivalued logics
- extend to more expressive description logics
- Formal Cncent Analysis

2.6 Abstraction-Based Information Technology — Jacques Calmet (by Skype)

The goals of this talk are as follows.

- To show that the ideas behind calculemus can be exported to the whole world of language,

- To propose a new task for Artificial Intelligence.
- To outline some methodologies.
- To propose illustrative examples.

[McCarthyHayes1968].

The key lies in Virtual Knowledge Communities, where an agent prposes a topic, other agents join the topic, and information is shared. These have been in several different domains.

Q How does your vision direct the development of computer algebra systems?

A One of the challenges we have is to consider algebra, be it algebraic geometry or differential equations, in a topological context. Example is Kenzo, which requires much ability to use.

2.7 Proof reuse in a Mathematical Library — Noyer & Rioboo

FoCalize is a project to combine specification and implementation, which is UFOL (Unsorted First-Order Logic). $\mathcal{X}$ is variables, $x \gg_{Q(A).A} y$ mean sthat x is to the left of y in the quantified formula $Q(A).A$. In $Q_A.A \vdash Q_B.B$ we have an *oriented unifier* if it unifies in $\exists A\ \forall B$. This notation allows to prove that unform continuity implies continuity, but not *vice versa*

2.8 Reflecting Data: Formally Correct Results for Efficient (and Dirty) Algorithms — Dixon

Optimisations are the bugbear of correctness. Two traditional approaches: computational reflection (and various ways of doing this); Oracles (compute outside and verify inside), and this isn't always applicable. Example (Buchberger) normalise terms such as

$$S(a + S(b)) + S(c) \to S(S(S(a + b + c)))$$

which has an obvious linear-time algorithm of "counting S", but requires recursion on term structure. But we can't define this within our theorem-prover if it involves recursion on terms tructure, so prove it correct in an externalised version of our term structure, and prove them by induction.

Provably correct result, with only linear slowdown (representation mapping), and no need for extra trusted code.

2.9 Calculemus Business Meeting

2.9.1

2.9.2

2.9.3

2.9.4

2.9.5 Summary

Calculemus 2009 had 17 full submissions and 4 workshop papers: History $\in [10, 29]$. There were 24 abstracts, so 7 did not materialise. Each paper had three reviews, and there was (new this year) a rebuttal phase.

The following options had been discussed.

- Merge with AISC
- Move to every two years
- Joint with CICM in 2010 (and therefore AISC and MKM)

Ir had been suggested that we should co-locate with (alternately) a computer-algebra and a theorem-proving conference.

JC said that he liked the theory, but the practice did not seem to work out as well as one would like. VS suggested that co-location with CICM should be pursued for another year.

2.9.6 Elections etc.

We need

- A secretary
- Two Programme Committee chairs (one CAS, one TP)
- four trustees, two of which are automatic from the previous.

One suggestion for Trustee was Paul Jackson (Deduction).

2.9.7 Any Other Business

JC asked for ideas for PC chairs who could be approached, and the names of Catherine Dubois and David Delahaye emerged.

Votes of thanks were proposed, and carried by acclamation, to Stephen Watt and the CICM organisation for the local arrangements, and to the Programme chairs for this year (LD and JC).

Chapter 3

8 July 2009

This day was devoted to Digital Mathematics Library 2009 (DML) and PenMath, and JHD largely attended DML. At the start of DML, it was pointed out that published (research) mathematics only amounts to about 10^8 pages, and hence could be contained on one disc. But *isn't*!

3.1 Similarity Search for Mathematical Expressions using MathML — Yokoi (Tokyo)

Goal: build a search system for mathematical expresisons which returns *similar* ones. We recall that traditional search engines tergeting natural languages have problems with the unique structure of mathematical expressions. MathML has two representations — presentation tends to lead to wide trees, and content to deep ones.

[Adeeletal2008] has MathGo!, which works by generating keywords and throwing them at regular expression engines. [Otagirietal2008] use their own query language, and search using tree expressions.

[Ichikawa2005] proposed the concept of the subpath set, which deals with deep structure well, therefore (?!) I will use Content MathML in my project. He uses the Jaccard coefficient[1]:

$$J(t_1, t_2) = \frac{S(t_1) \cap S(t_2)}{S(t_1) \cup S(t_2)}. \tag{3.1}$$

40% of all symbols are `apply`, hence he rotates the trees to replace `apply` by its first child. "`apply` has no semantic information by itself". We have 155,607 expressions searched from `http://functions.wolfram.com`. With five queries, only one had the result show up in the top 100 when searching in presentation, and all appeared in content, but "apply-free" content markup defintely won, e.g. 6th rather than 17th for one expression.

[1] A questioner pointed out that this doesn't take account of the order of children, e.g. 2^x and x^2.

In conclusion he is worried that the similarity search may become the bottleneck in scaling up.[2] He currently doesn't take into account the *value* of the symbols.

3.2 Improving Mathematics Retrieval — Kamali & Tompa, Waterloo

There's a lot of mathematcal expressions on the web, but there is no search engine for them, unlike text, which is a mature field. One fundamental question is the definition of 'similarity'. Text has a large number of different words to choose from, whereas mathematics has fewer symbols, and the structure of the arrangement is more important.

Starting from Wikipedia and Wolfram, we crawled around 60GB, butthis gave us 4000 MathML (3000 from the W3C test suite!) expressions, but 300,000 TeX ones, mostly annotations on images, and therefore contain errors. This corpus is published. We translated the TeX into MathML. The vast majority have between 10 and 130 nodes.

The fundamental question is content versus presentation. Content handled synonymy and polysemy better, but this relies on common dictionaries. Most of what they saw was presentation, hence this is what we use.

Assign a weight (defaults to 1, but, as above, `apply` or `mrow` need lower weights) to each node, and the weight of a tree is the sum of the weights of the nodes. Two trees match is they have the same shape and corresponding nodes have the same labels. Write $T_1 \cap T_2$ for the set of all common parts. We are interested in the heaviest weight in this.

Some attributes, e.g. sin in $\sin x$ are significant, but i in $\sum_{i=0}^{n} x_i$ is not. We need rules to know which are which, but we should also allow publishers to declare this. We 'normalise' a tree by replacing insignificant values by tags.

Various definitions: mathematical equivalence, syntactic equivalence, identity, normalised-identity, and n-similarity (n seems to be same as J from (3.1?)).

Q–PL There is scope for a shared test suite.

***** A show of hands supported this.

Q Is there really any effective way of normalising?

A Not if one does not know the semantics

[2] In response to a question from PL, he doesn't seem to be using any standard 'inverted tree' libraries for the searching.

3.3 An Online repository of mathematical samples — Sorge *et al.*, Birmingham

We have a repository for handwriting recognition and OCR, which we are hoping to make online. We are inspired by benchmarks in other areas[3], but the only one here is Suzuki's Ground Truth Set, which is for OCR, rather than the formula recognition task we are working on.

We would like to build a repository of a range of forms (handwritten, scanned, electronically born), categorised at a range of subjects/levels. Need the following files.

sample TIFF, or eventually, InkML.

provenance including copyright.

source file, or rather a link, internal or external, e.g. PDF, PostScript, TIFF.

clip file containing the bounding box and position in glyphs in JSON format. "We have a tool to generate this".

Attribute file containing information about the type of sample and mathematics.

Annotations — a potentially unbounded number.

The key attribute is perfect/rendered/scanned/InkML, telling us about the information available. For mathematical field, we use the first two digits of 2000 MSC, where available.

Major open questions are quality assurance (tension between quality of data and difficulty of submission) and copyright (own research is easy: making it available to others is harder.).

3.4 Digital Mathematical Libraries in France — Thierry Bouche, Grenoble

Began with an overview of the physical mathematics library in Grenoble, and its anomalies (old books locked away) and features (new items). Se what would a Digital Mathematical Library be?

- a list
- a database
- a list of databases
- virtual shelves

[3]TPTP, SAT benchmarks.

- a database of databases
- a list of national Digital Mathematical Libraries[4]

French digital mathematical libraries contain:

- 1500 books (Gallica 1683–1939 has 740, which are generally 300 dpi monochrome, 214 with OCR text)
- 2000 theses (1500 Thèse en ligne[5]: 1929–current, mostly new), (450 NUMDAM 1913–1945; Thèses d'Etat only).
- 38000 serial items + 75,000 CRAS: NUMDAM is the big player, but Gallica has some generalist journals, e.g. *Journal de l'Ecole Polytechnique*.

† NUMDAM 30 journals and 28 seminars

† Gallica

- Miscellaneous: HAL and arXiV, NUMDAM/SMF, Boubakistas

* Patrimoine numérisé du Service de la documentation de l'université de Strasbourg has 139 books, and many other special cases.

There are various "unarchivable", e.g. *European J. Control*, which requires installing a special PDF reader, which only works for them, and displaces any other PDF reader.

He notes the IMU 2001 call, and quotes as examples the 2001 CEIC members, saying that there are different levels of completeness: sometimes to ArXiV versions, sometimes NUMDAM, sometimes author's own preprint, sometimes publisher's proof.

Q–JHD Is it the fact that the PDF is not the publishers, or the fact that the reader does not *know* that distresses you?

A It wasn't quite clear, but he seemed to be objecting to the fact that the documents were not the "official" ones.

A–Ion Sometimes, of course, you may get links to extended versions.

3.5 Experimental DML over digital repositories in Jamap — Namiki it et al.

MR says that 70,000 mathematical articles in 400 journals have been published in Japan. He says that Japan has lagged behind, but DML-JP (supported by

[4] We know there will not be *the* Digital Mathematical Library, and funding is easier to obtain on a national basis.

[5] Almost no quality control: in theory it's on behalf of the *individual*, not the institution, and there are several versions of some old ones

the Institutional Repositories project of NII[6]) is now a metadata-based DML for Japan. About 80 University libraries have now launched institutional repositories, supported by NII. It incorporates 27 journals.

After harvesting metadata via OAI-PMH, we load them into EPrints 3.1.1, transforming where necessary into EprintXML, from, say, `oai_dc`. This process includes about half of all articles published in Japan. The problem with `oai_dc` is th bibliographic information encoded in `dc:identifier`. We had to add `msc_p` (primary), `msc` and `mr` to the EprintXML format. They have a special gateway to map from MR numbers to journals in their system.

Various statistics are supported, including the HITS algorithm for connectivity between subjects (defined as MR 2-digits). Future work includes more collaboration with the DML community, and full-text in XHTML/MathML.

3.6 Math Literate Computers — Dorothy Blostein, Queen's University

[She admitted that her father was the Haken of [AH76], so using computers to interact with mathematics was in her blood.]

In people, understanding precedes literacy, and people learn to read before they learn to write. Computers are fundamentally different. Mathematics is a case of general two-dimensional notations, such as music, choreography etc. Mathematics is a natural languagethat has evolved over centuries, and has many dialects. "Is it worth the hassle with the I/O problems to get help from the computer"?

Four-colour theorem was one of the first applications — see above.

Graph rewriting proved very difficult for recognition, since it was necessary to order the rules in a non-transparent order.

There are 'hard' (e.g. layout of $\sum$) and 'soft' (e.g.where to break a line) conventions in notation: in general the soft ones aren't used and should be.

3.7 Document Interlinking in a Digital Math Library — Goutorbe (presented by Bouche)

The mathematical literature is, and always has been, a network, but the new digital infrastructure can make this *explicit*. We have good reference databases (Jahrbuch; MR/Zbl). We assume that the publication process, or some prior digitization/matching, or extraction from TeX, has given individual references as a text string, and we wish to locate the matching entry. Butthere may be typing errors, OCR errors, errors in numeric data such as page numbers etc., and the data may be incomplete (Physics style) or translated.

One it could try field-by-field comparison, as in (the first version of) MR, but the parsing process is dificult here. One could try character pased (Leven-

[6]JHD assumes this is the National Informatics Institute.

shtein distance etc.), which deals well with local errors, but not with reordering of fields. We actually use a token-based approach. Out of 412721 artciles, 376076 have distinct volume/first page/last page entries, which indicates the importance of matching numeric tokens.

All artciles in NUMDAM and Zbl are correctly matched. In general, we 75% of the total numebr of bibliographic items, rising to 85% in some journals. They tried *J. Differential Geometry* (from project Euclid) and got 89%.

Initial selection witha Boolean query, then check numeric data, then trigrams and then cross-check with Dice coefficients. Showed two examples, the second matched an article quoted in French (including French translation of journal title) with English original (pretty impressive!).

The main problems are missing numbers, or books, where the data in the database are very complete and the citation only has a small subset. Multiple editions and years are very hard to distinguish, and publication years are surprisingly often wrong.

Q–MD Any use of DOI/Crossref?

A NUMDAM is discussing whether to join Crossref, but there are financial implications. Also, what happens when we are digitising data which already have DOIs.

A–JSTOR A technical explanation of how they deal with this problem.

A It is not clear that our rights in NUMDAM include the right to assign DOIs.

A–MR We have a tool which we make freely available to publishers to help them get the MR numbers.

3.8 I2Geo — a web library for interactive geometric constructions — Libbrecht *et al.*

Interactive geometry tools are everywhere, and there is much on the web already. Currently one can't share between systems, or indeed between countries and languages, and there are questions of quality/trust.

This is an open-source project. For example a Luxembourg teacher can share a GeoGebra file, with explanation in French and some metadata. A Czech teacher might submit a search, but is using Cabri, and wants to know Use `curriki`, a large systems with every item given traceable long-term URLs with many resources. We have user profiles, which are part of the quality process. The metadata are very simple, and we intend to make it OAI-harvestable. The platform knows Czech, French, German, English, Dutch, Basque and Portuguese.

Annotations are made in Geoskills, which is a set of competencies organised an a multi-lingual OWL ontology. Quite impressive (triangle matches polygon, for example).

There is a simple review system, but the problem is "my quality, your quality" (X rates simplicity, but Y detests inconsistencies ...). They seem to have some ideas on this, and there is more work in progress.

3.9 Report on the DML-CZ project — Petr Sojka *et al.*

They have implemented a "similar articles" feature (details not clear to JHD), and are evaluating it. The project is `http:/dml.cz`, with some 11,000 articles.

Chapter 4

9 July 2009

4.1 OpenMath in SCIEnce — Roozemond & Horn

Want to link CAS to other programs. SCSCP is the protocol used to communicate between systems, encoding the mathematics in OpenMath, and indeed much of the protocol is in OpenMath — see new CDs later.

POPCORN provides an alternative linear notation which is much simpler to read (and write). Demonstration where muPAD locally takes 42 seconds to factor Swinnerton-Dyer(6), but MAGMA, at the end of of SCSCP and running in Kassel (!) takes 2 seconds.

Examples in GAP.

Numerous presentations of CDs, e.g. `matrix1`. JHD pointed out that the "encode the field once" paradigm had already been done in `polyd`. MK pointed out that "bridge FMPs" between say, `matrix1` and `linalg2` would be useful.

4.2 — Carlisle NAG/MathML

Hoping to get the "last call" draft of MathML3, which has much more explicit links to OpenMath, out in August. "Strict Content MathML" $\equiv$ OpenMath. `partialdiff` is a case where the translation is particularly horrible.

He also noted that the OpenMath CDs, as displayed on the website, could be changed to show a POPCORN equivalent.

Q–SCIEnce There are also problems with `calculus1`, which is interms of functions, whereas (most) CAS ae in terms of expressions.

A MathML3 does this by sticking `lambda` in all the appropriate places, but this should be regarded as an "idiom".

4.3 OpenMath CDs for quantities and units — Collins

Goals are consistency with existing standards (OpenMath and SI), and another name attached to this effort is PhysML. We need

- lack of ambiguity
- consistency and simplicity

Created `SI_BaseQuantites1` and `SI_BaseUnits1`[1], both of which are fixed in size. Also fixed are `SI_NamedDerivedUnits1` and others. Prefers *not* to have "metres/second" etc.

Note that SI has *defined* a nomenclature, and he shows a chart that should map to any type systems. His SI family defines functions like `dim`: quantity (or anything else, e.g. one can say "dim(metre)" as well as "dim(1 metre)", and indeed "dim(length)") $\mapsto$ dimension, `unit` (in the `SI_functions` CD): quantity $\mapsto$ coherent derived unit (again it applied to anything, so "unit(length)" = metre), `num`: quantity[2] $\mapsto$ number, so Q (but in SI) =`unit`(Q)×`num`(Q).

`kind` copes with dimensionless quantities that can't be added, e.g. angles and salinity, and, he claims, also copes with JHD's temperature issues.

Claims that, for fixed `dim`and `kind`, we have an Abelian group which makes mathematical sense, but not necessarily physical sense.

Also fundamental physical constants: Newton, Coulomb, Bolzmann, Planck and the speed of light.

Q–JHD Prefixes? And therefore do you have the "millikilogram"?

A `gram` is specifically added as a

4.4 Content Dictionaries for Algebraic Topology — Heras *et al.*

These are really Kenzo CDs, where Kenzo works with the main structures in (simplicial) algebraic topology. These are all *graded* structures, and a structure K is represented as $\mathtt{inv}_K$: $(x, n) \mapsto$`Boolean` as $x \in K^n$.

4.5 Intergeo File Format — Libbecht *et al.*

Interactive geometry is here, and there are many interactng communities. There is an `i2geo` platform (section 3.8), so the consortium is designing a file format. Claims that this is a legitimate object of discourse, showing a light-emitting illustration.

[1] Includin the kilogram, as opposed ot the gram.

[2] Here we don't have the overloading issue: "num(length)" is invalid.

We will send things as zip archives, with XML files describing the package: `intergeo.xml`. How to describe a construction.

- Simply as constraints: Line l is incident to P and Q: doe snot encode *behaviour*.
- functional: line l is constructed from P and Q — what happens if its multivalued?
- constraints *with output* — our solution. Therefore a construction is "initial conditions plus constraints".

A consequence is that there is an explosion of symbols. We want to use OpenMath to document all these symbols, using the CD structure to help manage the diversity. We will also use OpenMath to manage symbolic coordinates — already supported by some descriptive geometry systems.

Version1 is in GeoGebra, Cinderella and JXGraph, and many others are working on this (WIRIS, Geometrix, GeoPlan, TracEnPoche etc.).

Version2 is soon, Version3 at end of project (2010Q4?).

The big question is FMPs. Should allow, e.g.

$$\texttt{line\_by\_two\_points}(l, A, B) \leftrightarrow \texttt{line\_by\_point}(l, A) \wedge \texttt{line\_by\_point}(l, B)$$

Maybe we need quantified expressions, with special geometric quantifiers.

Typesetting is a problem: MathML seems too big, and currently each system has its own TEX, which leads to incompatibility. Symbolic coordinate input is necessary, and being worked on.

Q–SCIEnce Why the "fake OpenMath" rather than real OpenMath?

A POPCORN would be equivalnt. We don't need full OpenMath, since we don't have composability (an InterGeo constraint, not an OpenMath one).

Q–MK It would be nice to have an official XSLT that translated this "non-standard encoding" into the standard encoding.

4.6 A Better Rôle System for OpenMath — Rabe

The three stages of validation in OMDoc 2

1. XML validation
2. Construction validation, in particular rôle validation.
3. Semantic (mathematical) validation — type-checking, equality-checking etc.: expensive and foundation-depednent.

It is the second stage that concerns us.

The current system has function/binder/key/error/constant. Every symbol has rôle (possibly none). But anything (including keys and binders) can occur as constants, which seems eccentric. A composed object can occur as a binder[3], but not as a key. Why?

We can't use `plus` as a binder, but we can wrap this in a (possibly nugatory) attribution, and it is then illegal.

4.6.1 Our proposal

Four roles.

term mathematical objects (this would now be the default)

(semantic) attributions keys should be distinguished symbols

binders distinguished symbols

$$\frac{\vdash B : \texttt{binder} \quad \vdash T : \texttt{term}}{\vdash (\texttt{OMBIND} \quad B \quad vars \quad T) : \texttt{term}}$$

etc.

Also propose that a symbol has an arity in $\mathbf{N} \cup \omega$. An `OMA` whose first child has rôle R returns a temr of rôle R. We don't actually need a separate rôle for errors, since the presence of `OME` distinguishes it.

Hence the sub-concept of a *semantic rôle*, which would includ errors, but also, say, specified Booleans etc.

Q–DPC I would rather see binding as onlybeing λ, and $\forall$ as a function of signature `function`$\mapsto$`boolean`.

A Not sure how to relate the two definitions.

He showed a translation, and claimed that there are fewer well-rôled expressions, but those that we are losing are those we never wanted anyway. He stated that there was a compromise between sumplicity and validation.

Q What statistics do you have — have you tried the FMPs on the OpenMath website.

A We haven't implemented it, but I couldn't see any errors, since people tend to write well-rôled expressions.

A–MK

Q–DPC STS tells you arity, but also gives names for the slots. So there is a strong overlap.

A We haven't really looked at STS. The rôle system should be coarsest possible type system.

A–JHD STS distinguishes two kinds of ω: the ordinary lind and the `nassoc` kind.

[3]Used in JHD/MK's `forlalin`, for example.

4.7 Semantics of OpenMath and MathML — Kohlhase

Quoted flame review for [DK09] "OpenMath has no semantics . . . ". Fundamentally MK knows that is not true, but the reviewer has a point.

The question of the "meaning" of mathematical expressions has been studied in logic, with the "Grundlagenkrise" [Russell1901]. So these days e pick "foundations", e.g.

Sets axiomatic set theory — "everything is a set", typically ZFC, which used first-order-logic as its letalogic. Gödel's results imply that consistency and adequacy can't be proved.

Types The universe is stratified into terms and types, and we have typing judgements. The λ-calculus is typically the metalogic.

ZFC rules for mathematicians. So what about OpenMath?

- Operations. Every system has a phrasebook, and it's
- Objects. OpenMath objects are labellel trees (modulo α-conversion and flattenings).

XML, the binary encoding, and indeed strict content MathML, are merely encodings.

4.7.1 A syntactic semantics

Propose "OpenMath algebras".

1. The main parameter is the OM vocabulary T, the set of symbols of an OpenMath objects.
2. Rationalize the syntax of $OM(T)$, as openmath objects over T.
3. Define OM algebra (problems with interaction of binding and attribution)
4. Define an interpretation into $\mathcal{A}$.

   * This lets us show that α-conversion is sound.
5. Define the free OM algebra $I(T)$, which is initial, and α-conversion is complete.

4.7.2 OM-Models

An OM-logic is an OM vocabulary with $L := T$ and $=$, e.g. `logic1`, `relation1` and `quant1`. Then an OP-Theory Θ is $(T, \mathcal{A})$, where $\mathcal{A} \subset OM(T \cup L)$.

Then an OM-Model is a theory Θ (FMPs) where the interpretation of $=$ is Δ (the diagonal) and all the axioms of $\mathcal{A}$ are T.

Then an initial model is $I(T)/\equiv_\Theta$.

4.7.3 Difficulties

The classical treatment of binding structures has a context Γ, but we have to handle arbitrary binders, which we will handle via higer-order abstratc syntax.

Attributions themselves are not a problem, but what do we do if attributions are on the bound variables? It turns out that the concept of well-rôled terms terms removes some of the complication.

This is in fact independent of the foundation. However, the MathML CD group is heavily under-specified (necessarily so), so we should produce some more specified ones for particular domains, e.g. Peano.

Q–CSC This is just the usual game of quotienting by the logic, as always played in catgeory theory.

A We give you an extension mechanism — you bring a foundation and we extend it.

Q Doesn't this contradict the standard that says that all that is necessary is the name?

A Not as such, but it does make more explicit that a symbol with no FMPs has no intrinsic eaning.

Q–CAR Doesn't this mean that we have to look carefully at the foundational CDs.

A Indeed, and we should not have put `ge` etc. into `relation1`, so perhaps we need `relation0`.

4.8 The Evolving Digital Mathematics Network — Ruddy (Cornell)

Been involved in project Euclid for the past 10 years, and also responsible for the digital repository, and otehr publishing services. Euclid was a repsonse to the late 1990's "serials crisis", with funding by the Andrew W. Mellon foundation. Early development 1999–2002; project launched in 2003, with 19 journals. Initially focsed on current serial content. Digitization of journal back issues began in 2002: now digitised 50K journal articles, and approx 1.2M pages of content; 68% of which are open access. So far this year have added nine journals (mostly U.S.) andtwo monograph series. Expect to add three Japanese journals (Hokkaido, Kyoto, Tsukuba) and Cornell Historical Mathematical Monographs.

Not for profit organisation., selling hosting services etc., with a variety of business models. It's now co-run with Duke University Press, which has brought skills not at Cornell Library. In particular, they do actual print.

There's a mission statement for DML (2003) on the Cornell website. There were some obstacles.

- No significnat funding

- very (overly?) ambitious
- An approach that called for centralised planning

What we have is an increasing numbers of autonomous systems, with little networking (other than what one finds via Google). Central planning is clearly dead, though.

Need to lobby publishers for greater access to metadata. This collaboration in network services grows in unpredictable ways. There's a balance between openness and risk.

Q Is paper copy still part of archiving: in 1990s the LoC decided that paper was the answer to the acid paper problem.

A It depends.In the digital world, the issue has changed. There are now digital preservation institites etc. Most Librarians are "I'm worried by this, but I have no alternative".

A-floor There is a certain amount of "I'll keep X if you keep Y" arrangements.

Q–SMW It is alleged that if yu go to a library and open a random journal randomly, you are the first person to have looked ta *that* page. This isn't a very Web 2.0 world.

A I see very little advanced networking at this level.

A–JSTOR Our statistics are that every year, 80% of articles are read[4]. JSTOR attempts to have two paper copies stored in different locations (continents!).

4.9 `wiki.openmath.org`: how it works and how to collaborate — Lange (Bremen)

The intention is to provide a browsable view, and some editing facilities, the latter with permission management. There could be other spaces as well. The basic system is SWiM — Semantic Wikis in Mathematics.

There can be additional information in parallel files, types as in STS, XLST for translation into presentation inot MathML, etc. Once a CD is official, the *meaning* of a symbol cannot change. Traditionally, files are stored in the OpenMath SVN repository, and people check out copies, discussion is done on mailing lists, or via TRAC. Unfortunately, TRAC and SVN are on different servers, and there is no linkage.

He presented three use cases.

1. Minor edits - e.g. fixed a typo. Traditional use is

[4] JHD queried this later. It is true, much to the JSTOR man's surprise. Of course, JSTOR has 5000 institutional subscribers, and is pretty selective about the journals it covers.

2. More major revisions, e.g. some-one notices that an FMP is wrong: reported on the mailing list, general discussion occurs, and then there's a fix, with, at best, a comment “fixed as in e-mail”.

3. Fixing nottaion. Have to find out the erroneous symbol, then check out the corresponding notation file, fix it, and then regenerate the document showing the bug.

[LangeonzalezPalomoMathUI08] SWiM supports structured outlines, with explicit attachment of metadata. The XML is organised into tables, with a toolbar which allows adding new items. Currently use our own syntax, but should consider switching to POPCORN. So about the use cases.

1. Each wiki page, i.e. each fragment of a CD, is viewed in the Wiki as a separate component, so when the Cd is reassembled for the SVN, the log message will now say precisely which fragment was changed.

2. There is discussin atthe granularity of the CD, and the discussion is categorised: issue/position/argument/decision . . . . The discussions are represented as an RDF graph. CD structures are also represented in an RDF graph extracted from the XML. There is an RDF query language, and he demonstrated “all symbols for which ther eis an issue but no decision”.

   Quite often we have common solutions to common problems, and we would like to implement a wizard-like interface. Currently running a survey to decide what common themes there are.

3. One click to the symbol, one more to the notation definition (and this will be sped up — see section 7.9 and the previews are shown in the wiki window.

The discussion feature is the only one really used so far. There were 90 posts, 69 of which fitted into the argumentation ontology. The main missing concept was “question”. 54 of the posts were atthe CD levle, which indicates that it should be easier and clearer how to post about individual symbols.

It is currently far too hard to add a new symbol to a CD, because of the granularity of the SVN. Interoperation at this level is important. There is currently no e-mail notification.

Needs to change the underlying base wiki (old one discontinued) to KiWi. Also TNTBase is a successor to SVN for XML documents, and if that were hosted on the same machine life would be much easier.

Q Moving away from SVN would be an issue for many.

A TNTBase is compatible with SVN.

4.10 OpenMath Business Meeting

Kohlhase opened the OpenMath Business Meeting. The agenda was agreed.

1. Kohlhase was elected to chair the meeting

2. Davenport was elected as Secretary: Carlisle and Ion were elected as minute checkers.

3. Annual Report. The last Business Meeting was in February 2008 in Barcelona. There has been some progress on OpenMath 3, but most people's efforts have been absorbed by MathML 3 (which has an imminent deadline). It was asked whether the MathML 3 work wasn't a useful contribution to OpenMath 3. Kohlhase stated that it was, but had not produced any formal OpenMath 3 material *as such*.

   Davenport was thanked for organising this workshop.

   The financial report (Watt) is that there have been no transactions. It was asked who the signatories of the account were: Watt and the Founding Presider (Mika Seppälä).

4. New members: the membership rules were explained. Davenport suggested Joseph Collins, and Dan Roozemond and Peter Horn were also suggested. These were added to the roll. Chris Rowley was apparently missing, so he was added.

5. Executive Committee. The current membership is listed in Table 4.1. The committee was formally discharged from its obligations from the past year.

Table 4.1: 2008/9 OpenMath Executive

Michael Kohlhase	Chair
Mike Dewar	Vice-Chair
Olga Caprotti	Secretary
Stephen Watt	Treasurer
Marc Gaëtano	Member-at-Large
Professor Mika Seppälä	Member-at-Large

6. Election of a New Committee. Watt indicated his wish to resign from the Treasurer's rôle, and Christine Müller was proposed, seconded and elected. The rest of the Committee was re-elected. Libbrecht was thanked for his work as webmaster. Davenport was thanked for his work as CD Editor.

7. OpenMath 3. There was no specific OpenMath3 news to report (see item 3).

8. CD (management) issues. It was proposed that the 'alignment' CDs in Carlisle's talk, and interval changes in Davenport's talk, be adopted. This was agreed, and the changes will go live before the end of the Grand Bend meeting.

   Davenport asked for exceptional authority to make minor changes, in consultation with the Executive Committee, in order to facilitate alignment.

Watt proposed to delete the word 'minor'. The motion, as amended, was carried. The proposal to add `integral_defined` to `calculus1` would be reviewed by Carlisle and Kohlhase.

Davenport explained the process to make CDs official: an "in principle" decision at this meeting, the nomination of reviewers, and then a review report to him.

Watt asked about the two sets of units/dimensions CDs (Collins and Davenport) that had been presented. These two authors were charged with writing a reconciliation report, and Bruce Miller and Christoph Lange were nominated as reviewiers.

The SCIEnce project stated that the `scscp1` and `scscp2` CDs were probably not stable enough for consideration. It was pointed out that the `polyd` etc. family were still only `experimental`.

Davenport and Rowley were appointed reviewers to take `order1` (probably under a better name) forward.

It was pointed out that `matrix1` was rather short of FMPs. Davenport proposed that we agree the need for a CD in this area, encourage the authors of `matrix1` to add the appropriate FMPs, and nominate reviewers. Ion and Davenport were appointed reviewers.

`polynomial4` interacted with the existing, `experimental`, `poly` group. Horn and Davenport were charged to look at this area.

The Algebraic Topology CDs would be contributed to the repository as `experimental`.

Davenport would submit the `existsuniquely` and `forallin/existsin` elements of his paper for consideration. Carlisle and Watt would act as reviewers.

Questions were asked about the openness of the review process. It was suggested that the review process be made more public — both the fact that CDs had entered into review (with the names of the reviewers), and the formal review report. This was agreed. It was note dthat this would also ensure the website better reflected the activity of the Society.

9. Any Other Business. It was suggested that a plan should be adopted for the next (23rd) workshop. Watt reported on the likely plans for CICM next year, which would be decided in the next few days. It was proposed that the Executive Committee be given authority to fix the next OpenMath workshop in line with the appropriate scientific meetings. This was approved.

Kohlhase declared the meeting closed at 18:07.

Chapter 5

10 July 2009

Elena Smirnova opened the Compact Computer Algebra Workshop, with an account of the history of the workshops, which goes back to 2008.

She also pointed out that we are talking, not merely about compact computer algebra as small things in themselves, but also as small components of larger systems.

5.1 28.5 years of Maple: ??? — Gonnet

The S^2T measure says that, if S is the auxiliary storage available and T is the time used, then one can prove results of the form: *every* algorithm to solve problem X has $S^2T = \Omega(n^2)$. But in fact, I saw a paper by Borodin which shows that $ST = \Omega(n^2)$ is the right measure for sorting.

An $O(n^2)$ hidden bug is when an algorithm, or the kernel, has an $O(n^2)$ algorithm when $O(n)$ is possible — generally occurs when adding to the end of a list repeatedly. These problems are *not* picked up by standard testing. In the kernel, we picked this up and added `append` to the kernel, but never really exposed it to users. Mike Monagan removed most (? all) of the $O(n^2)$ bugs in the kernel.

5.1.1 "Option remember" and unique representation

"Option remember" was known as "memoisation" in previous systems. Is built into Maple, and therefore fast: supported by hashing, and therefore $O(1)$. Note that it relies on unique representation and *vice versa*. The xample he quoted was `diff(tan(x),x$100)`, i.e.

$$\frac{d^{100}\tan x}{dx^100},$$

which without remember "takes forever.[1]

[1] JPff solved this problem on the fly using Reduce, but JHD pointed out that Reduce expands, and Maple does not.

The general rationale is that there are highly repeated parts in mathematical expressions.

This has some good consequences, but also produces odd results, e.g. the fact that the first occurrence determines the order. “I admit that this is a tough decision, but I would make the same decision again”.

Q–GHG How often is it used today?

A–JC A lot in the core, but newer DAG types have been added, and they don’t make as much use of it.

5.1.2 “memory and GHz are cheap”

A system which uses memory efficiently is *always* ahead of one that doesn’t. Memory costs time: paging, garbage collection etc.

5.1.3 Use of C

Maple’s predecessor (Wama) and early Maple, were encoded in B, a predecessor of C and successor of BCPL. Later Maple could be compiled into either, via a pre-processor called Margay. This was fairly early in the evolution of C itself, and we had to write in the lowest common denominator of early compilers. This caused a great deal of grief in the early days — “why abandon LISP, the father of computer algebra”.

Originally Maple was “fast to start”, as was commented on by Ritchie. This is important for “calculator use”, and can be contrasted with Axiom[2].

5.2

To reduce the number of multiplications for small matrices with large entries. Example is holonomic functions. We hae improved upper bounds for matrices of sizes up to $30 \times 30 \times 30$. We currently know

- $\omega \approx 2.807$ (Strassen: 7 multiplications for (2,2,2))
- $\omega \approx 2.84$ (Laderman: 23 for (3,3,3))
- (Hopcroft–Kerr based on (3,2,3))
- $\omega \approx 2.3$ (Coppersmith-Winograd: only asymptotic)

Encode each algorithm, and name it $(a, b, c)_L$ for an algorithm of length L. So Strassen is $(2, 2, 2)_7$. We can apply this to a $(4, 4, 4)$ problem, and this gives us $(4, 4, 4)_{49}$. This is the “nice” case, where we have exact division, e.g. Strassen to $(3, 3, 3)$. Padding to $(4, 4, 4)$ and laziness with the zeroes is possible, but tedious by hand, hence we have implemented `Optimizer` to systematize this.

[2] He did not name Axiom, but the evidence was clear.

They have run this up to $(30, 30, 30)$. This also includes Pan/Kaporin's idea to do two matrix multiplications simultaneously. Their table beats (except in one case) previous tables by [Probst1980] and [Smith2002]. Example improvements are: the first is (9,9,9) is 512 rather than 529, and (13,13,13) is 1450 rather than 1580.

The implementation is GMP/NTL. Even for bitlength 1000, they don't beat naïve, but for 10,000 they do. They also beat for polynomials, and linear recurrence problems.

Q–SMW Have you considered special structures of matrices?

A No, we haven't, there are too many cases.

5.3 Inplace arithmetic for univariate polynomials over algebraic number fields

$L_p = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$, there each α_i is defined by a minimal polynomial m_i in $\mathbf{Z}(\alpha_1, \ldots, \alpha_{i-1})[x]$. GCDs over these univariates are the bottleneck for multivariates. Monagan's `RECDEN`, in the Maple kernel since 2004, does arithmetic in $L_p[x_1, \ldots, x_m]$. `RECDEN` uses a vector representation at each level: degree d followed by (pointers to) $d + 1$ coefficients. This representation can turn over a lot of storage. Therefore we pre-allocate a chunk of memory and work privately within it, as in Monagan's `modp1` package.

Our representation is conceptually that of `RECDEN`, but has no pointers: rather a long vector with internal offsets. The maximum anount of working storage is bounded as 6 (multiplication), 12 (division), 14 (gcd) times the input size.

Timings show that for multiplcation is generally slower than MAGMA[3] ($\approx$ 5), but faster than `RECDEN` ≈ 100. For GCD is is faster than MAGMA (≈ 5), and faster than `RECDEN` ≈ 300. There is a special case code for α_1 being quadratic, using a variant of Karatsuba.

5.4 Compact recognition of handwritten mathematical symbols — Golubitsky (UWO)

There is a speed/accuracy/memory trade-off, and we have a larger alphabet but less vocabulary information than traditional text. But symbols are genrelaly better segmented than in text. The real questionis the choice of the distance metric. The key question is the distance metric: two traditional solutions.

Euclidean — faster, especially if we represent the curves parametrically and compute distance in this space. Legendre–Sobolev seems ot be the best, especally as we can compute it dynamically,

[3] MAGMA is sub-quadratic here.

Elastic Matching — more accurate, but indeed it is not clear at all how tocompute it, and most people only compute approximations.

Manhattan — Euclidean, but replace $\sum(a_i - b_i)^2$ by $\sum |a_i - b_i|$. We only need one byte per coefficient (think of the resolution required to recognise a single character), so can pack them: $(-63 \ldots 63)$ in 1's complement. Have a six-instruction sequence to compute this — speedup of $3\times$ in 32-bit and $5\times$ in 64-bit. It performs slightly worse (10%) than Euclidean.

In practice we use Manhattan to produce the "short list" of ten candidates. For characters without allomorphs, "intermediate" characters are convex. This means that, for the ten candidates, we use a "convex hull of nearest neighbours" algorithm: expesnive, but not often used.

To reduce memory, we can define the significance of X as a sample of C as the number of samples from *other* classes for which X is the nearest element of C. Many have significance 0, which lets us complress our database of 45,000 characters to 1MB, with 2.52% error rate. If we halve the space, the error rate only goes to 2.80%.

Q Fateman was looking at this.

A–SMW That was **printed** recognition, which has a more uniform alphabet, but no time element/ discrete curve knowledge.

Q–Suzuki There was too much in this paper. The Manhattan distance itself could be a paper.

A–SMW That's the nicest complaint I've ever heard.

5.5 — ffitch

> The past is another country: they do things differently there. (L.P. Hartley *The Go-Between*

The algebra system came to life in order to solve *one* problem: Delaunay's orbit of the moon. The moon is going round the (static) earth, perturbed by the sun. Energy of the moon is "15 page formula followed bya full stop". There are six variables, and six angles. The entire universe of discourse is

$$\sum P(a, b, c, d, e, f, g, h) \cos / \sin(iu + jv + kw + lx + my + nz), \tag{5.1}$$

where P is a polynomial, and $u, \ldots, z$ are the symbolic angles. (The otehr two aviables are there "to help with substitution".) Division is not on the agenda.

Description (eulogy) of Titan. Since all exponents are *clearly* ≤ 31, we can fit all exponents into one 48-bit word. A coefficient was 48-bit numerator and denominator, and reduced lazily. They were store di increasing total degree order in a polynomial. Again, the arguments of sin / cos were packed, and a bit at the bottom of the pointer tothe polynomial coeficient told you which was sin or cos. This is a canonical system, and linearisation of trigonometric products was automatic.

Steve Bourne's PhD was on the Hill formulation, which is in Cartesian coordinates, and has larger coefficients and complex numbers. There was also a programming language. Variables were single-letters (`I-T` were integers, the rest algebraic), multiplication by juxtaposition etc. One feature was that it was an explcit return system, and there was an explciit distinction between destructive (e.g. addition, differentiation) and non-destructive (e.g. multiplication) operations. Writing `B:` rather than `B` meant that B could be destroyed, and therefore need not be copied.

My PhD was concerned with relativity, gravity waves etc., so we wrote a third system. This has more elementary functions, but it re-used the polynomial system. It was written in a language like theuser one, which was compiled into machine code for integer operations, and 'half-word-code' interpretations for algebra systems.

Later versions of CAMAL allowed an arbitrary number of variables (fixed for any run), arbitrary exponent limits (again fixed). Also arbitrary-precision arithmetic. Showed benchmarks from SIGSAM Bulletin, showing CAMAL as probably the fastest, and almost certainly the smallest, in terms of data space. Speed was never in the CAMAL design: "time is infinite, but memory is finite", and was a by-product.

As a later experiment he coded CAMAL's Fourier series in Reduce, and beat Reduce by a large margin (20+). But still did not beat (even in absolute time) the CAMAL of the early 1970s.

CAMAL was designed to solve problems. Samll memeory forced us to us etight data structures, but the styles of expression were limited. Gröbner bases in CAMAL (ACN 1999) were perfectly competitive.

5.6 Lazy and forgetful polynomial arithmetic and applications — Paul Vrbic (SFU→UWO)

The goal of lazy polynomial arithmetic is to extract the nth term of $f \times g$ etc using as few terms of f and g as possible. Johnson's heap multiplication still uses the whole of g, so we develop a truly lazy heap system.

Based on JPff's `:`, we allow for "forgetful polynomials", where one acces destroys the other terms. This can be done for $+$, but not $\times$. Equally, in division the divisor can't be forgetful, but the dividend can be. For example, in Bareiss we have lots of $\frac{A\times B-C\times D}{E}$, and we can treat the numerator, and hence the two products, forgetfully. Example of a degree 8 Toeplitz, where the product has 57000 terms, butthe quotient only 800. Similar in sub-resultant PRS, 427K versus 15K.

Managed to implement in C (showed data structure, where the method is a field in the constructed polynomial). Still slowed than `sdmp` in Maple, but that's because they chain equal terms in the heap.

5.7 Criteria for Compactness in the Design of Maple — Geddes

In 1980, we had a Honeywell timesharing, with 200KB as "very large". ALTRAN had a maximum limit of 100 digits: he fell foul of this in GCD. Quoted at length from [CGGG83], in particular Macsyma was impossible at Waterloo. The 1983 kernel was 100KB. Data structures as dynamic vectors (directly, rather than via lists, so models the structures in his book [GCL92] directly).

Library functions were interpreted, from a language which users could read. Choice of good algorithms was essential: mentioned GCDHeu and extensions. Also claimed that modular/lifting was far beeter than PRS: four-line polynomial and two-line polynomial has one-line answer but pages-long intermediate answers via sub-resultants.

Q–Rioboo I agree completely — why is there so much C now?

A I'm not sure: it wasn't our original style. But now we can have 'external' C, whereas then there was C only if it was in the kernel.

Chapter 6

11 July 2009

6.1 The Characteristics of Writing Environments for mathematics — Gozli, Pollanen, Reynolds

Two basic problems in the variety of the

Text multigraph, digital pen, palette-based editors.

Layout commands, digital pen, palettes.

Se we wanted to compare BrEdiMa (nested one-dimensional choices from a palette) and XPress (direct-acces to a 2-D area), which both used a palette-based solution to the symbol problem. Use a whiteboard as a baseline for comparison.

7 volunteers, each doing 2 sessions (e.g. solutions of the quadratic, sums and products[1]) with the 3 environments. Hypothesis is that $\frac{A}{B}$ would be written as:

Structure-based first the fraction bar (provided by the palette) then A and then B;

Unit-based A then the fraction bar and then B.

Crudely speaking, the whiteboard and XPress gave unit-based approaches, and BrEdiMa a structure-based. On average, the software editors took six times as long as the whiteboard, with 50% more "events". BrEdiMa had more, and more time-consuming, deletion events, e.g. typing in the numerator and *then* realising that they need a fraction and having to start afresh.

Overall behaviour similar between the two editors, but detailed behaviour very different.

Q I am disappointed that youdidn't use, say, Mathematica, which lets one make an existing expressions into a numerator.

[1] In answer to a question, the subjects were given a piece of paper and told to reproduce it. One listener complained that this biased the experiment.

A We were testing with novices.

Q Was it a time trial?

A We used our usual instructions: "Go as quickly as you can without sacrificing accuracy for speed".

Q Surely you should be trying bigger expressions: the great advantage of computers is "cut-and-paste".

A That's where we want to go next.

6.2 Canonical forms in interactive assistants — Heeren & Jeuring

The environment was the DWD Math Environment — he showed an applet for solving linear equations. There's a palette of available operations. This tool is in practical use in Dutch high-schools, but the only feedback is right/wrong. One could enhance it with

worked examples

hints "try distributive law"

comments , e.g. "this step is correct, but doesn't get you any closer".

He then showed a version which used their service — apparently DWD, ActiveMath and MathBox all have bindings to their service. This sort of work is often done by a CAS, but a CAS does not provide the sort of fine control that is needed. Instead we will use a strategy language [MKM08], written in Haskell, with components like `seq` and fixed-point (repeat until done). Questions that come up include

- adaptability (to the learner)
- granularity

Their solutions is a "view": a pair of a matching function $A \to B \cup \texttt{failed}$ and a building functions $B \to A$. So

$$3x - (1 - x) \underset{match}{\to} [3x, -1, x] \underset{build}{\to} 4x - 1.$$

Showed a lcm finding routine, programmed by pattern matching. This matches $\frac{a}{b} + \frac{c}{d}$, but not $\frac{a}{b} - \frac{c}{d}$: this could be fixed by a new clause, but we end up with combinatorial explosion. Hence we need to "match in the presence of algebraic laws". *But* the choice of laws depends onthe subject, e.g. we would not to match inthe presence of distributivity for 10-year olds.

Views compose. He stated that (JHD things he meant that this was in the context of the linear solving apllication) Associativity is implicit, order is preserved where possible, combination of like constants is implicit, distributivity is not assumed.

"Views" allow one to hide the details of the abstraction, makes the rules explicit, correspond to a particular level of detail. Multiple views can coexist in a strategy specification.

Q–CAR Not sure how to put this, but are you were working with actual teachers.

A At the Dutch Open University, we do have educational specialists with whom we work, but also we are providing a "back-end" tool to environments, and many of the pedagogical questions belong there.

6.3 Some Drawbacks Appearing in Conversion of TEX Generated Documents to Adobe Acrobat PDF File Format — Pejovic, Mijajlovic

Started looking at digitizations of the *Publictaions de l'Institut Mathématique*, but are also archives for some other publications. We now have over 2000 papers in PDF, in a mixture of retyped and scanned. `http://elib.mi.sanu.ac.rs`, but would like to increase the visibility, therefore we wanted to add this to Google via WebMaster, but the quality of the indexing was poor.

One problem was that we had used a variety of TEX→PDF tools, basically because we came to this from typesetting, and indexing issue shad been ignored in favour of visual appearance. Hence we a re regenerating all the TEX-originated PDFs, sometimes enhancing the LATEX source. Now use pdfLATEX, with the `cmap` package.

PDF/A-1b Provides most of what we want (but nt Unicode), where conformance can be verified.

improved PDF/A-1b Forces Unicode, satisfies all our requirements, but conformance can be verified, though not easily.

PDF/A-1a Would be noice, but is still "work in progress", and so not ahcievable at the moment.

Have also tried reading with a book reader, but it has problems with reflowing. We found it necessary to document the process of generating PDF from TEX files. We have come to the conclusion that it is reasonable to impose some restrictions on what we archive in repositories.

Q–RM Very interested in readers, since they seem to be a "disruptive technology". Why were we looking

A

Q Shouldn't you be using XHTML+MathML if you wanted to show up in Google?

A Well, we do show up in Google

floor Doesn't Google currently do PDF beter than XHTML (general laughter).

6.4 Representations for Interactive Exercises — Goguadze, presented by Libbrecht

We want authoring, generation and hybrid.

6.4.1 Anatomy of an Exercise

A task dscription, with interaction and feedback, where feedback can lead to a new task, etc. There are normally many paths.

For example, differentiate $x \mapsto 2x$. This might be correct, or lead to $2 \cdot x'$, which leads to correct via a longer path.

We claim that some automation is possible — many feedback routes can be generated. Transitions can depend on tutorial strategy, and can be adapte dto the learner's situation (but the model in IMS 1.2 is inadequate). We need tasks to have metadata, and the feedback has to be typed, e.g.: procedural (do this next), conceptual, product and meta-cognitive. Transactions need to be enriched. There is the typical "syntactic, numeric and semantic (i.e. CAS)" as levels, but this is not rich enough for us.

We therefore propose a system of queries to evaluate student answers. Better annotations allow different feedback strategies, and different presentation strategies. Also delayed feedback — let the student do several steps before getting back to him.

Future work includes fully generated exercises, domain-specific exercises, the authoring of tutorial *strategies*, as well as mashup-powered interactivity.

Q–Ross Meyer We have had several such presentations (e.g. Davenport): what standardised markup can we use?

A QTI version 2 (v1 was basically MCQs) is about the only standard we have, and it has almost no implementations. It requires mathematical evaluation, hence hard.

Q–MK Is any of this specific to mathematics?

A Good question. The special input is one.

Q–CAR Is this available?

A It should be — I need to check the details.

6.5 Some Traditional Mathematical Knowledge Management — Ion (Mathematics Reviews)

[Associate Editor of Matematical Reviews since 1980]. MR is based in an old brewery!

There's a lot of mathematical knowledge, some of which is common, some of which is not, and some of which was common and is no longer (e.g. 6/8– = $\frac{1}{3}$£1.

It is claimed that the Oshango bone is a table of small prime numbers, but there is no documentation, and access isn't great. Cuneiform bullae from Mesopotamia seem to contain multiplication tables beyond the need of commerce.

Around 1900, Valentin started a project for all mathematics, and had around 250,000 paper slips (alas now lost in bombing of Berlin), never published despite several attempts. Répertoire Bibliographique des Sciences Mathématiques (1885–1912) tried to make a catalogue on index cards. Royal Society Catalogue of the Scientific Literature of the 19th Century — 19 volumes, now digitised, but not reduced to a database. An international effort foundered in 1914. Paul Otlet and Henri La Fontaine collected and catalogued a significant amount — Otlet designed a highly advanced index card machine[2], allowing users to annotate relationships etc. At the end, they had even envisaged television supporting remote users. They even had a 'pay-per-card' service, but it didn't really work out (World War II). Their Mundaneum is now open as a museum, and there is a recent Flemish documentary.

Arund 1945, Vannevar Bush had $10,000 from IBM and NCR to develop "fast microfilm searching", and Shannon worked on this early on.

The database is from 1940, TeX from 1984 (Mike Doob submitted the first such). 2,500,000 items. 1980 40,000 item, 2007 80,000 items (MR staff has, if anything, gone down in this period). People claim that literature is growing exponentially, but this is *not* the fit: total database grows cubically (he showed a very convincing graph). The mean number of authors has been growing slowly, and 2006 was the year in which the number of 2-author papers passed single-author papers.

MSC 2010 has just been finished (joint MR/FIZ) — see `http://msc2010.org`. It has nearly 6000 rank-3 nodes. [SmirnovaWatt2008] can classify into MC by symbol frequency. We are working with the Mathematics Genealogy project. There are groups looking at the structure of the graph. There are also issues of classification through compression, and plagiarism detection[3], via BLAST or Déjà Vu.

Mathematical archives are a growing interest (note that Leibniz wrote 40,000 letters)[4]. Jeremy Leighton John (Nature June 2009) said that "archives in the wild have the potential to be on incalculable value".

[2] Aimed at "millions of 3×5 index cards".
[3] Ion's own view is that this is noise.
[4] Apparently there is a "curator of eManuscripts" at the British Library.

The lesson of history is to keep trying, we have to collaborate, tools can be useful, and we have to keep sharpening them.

6.6 OpenMath in SCIEnce: SCSCP and POPCORN — Roozemond & Horn

Overview of the SCIEnce project.[5] SCSCP is a lightweight, OpenMath-based, protocol for communication between engines.

All the semantics of OpenMath is in the Content Dictionaries. Thre are two representations of OpenMath — XML and binary, neither of which are particularly (human) readable. Hence POPCORN, Possibly Only Possible Convenient OpenMath Representation Notation. Various POPCORN converters: $\leftrightarrow$ XML and binary, $\rightarrow$ LaTeX.

Many systems speak SCSCP/OpenMath: MuPad, GAP, Maple, TRIP (a celestial mechanics system) and KANT. There are both Java and C libraries.

6.7 Using Open Mathematical Documents to interface Computer Algebra and Proof Assistant Systems — Heras

Kenzo can do things no other system can, *if* we believe it: hence the goal of integrating with ACL2. We have a mediator providing access to Kenzo. ACL2 is an interactive theorem prover. OMDoc will represent formulae, statements and theories. We have five kinds of OMDO cdocuments

* Kenzo

1. Definition of Mathematical Structure

2. Logic to Interact with Kenzo

3. Presentation for the GUI — makes much use of `OMFOREIGN`

* ACL2: OMDoc content dictionaries correspond to ACL2 encapsulations, and they have a tool to map.

4. Interaction with with interpreter.

5. Presentation for the GUI

These all live in a common document repository[6]. It would be nice to integrate with other theorem provers, provided they can interface with OMDoc.

[5] Kassel is in the project as a replacement for Paderborn, and bring the MuPad knowledge.

[6] MK asked what sort of repository, but didn't get a very coherent reply

6.8 Content Management in ActiveMath — Librecht

Authoring is about writing content, which is in several sources, which ae then exploited by delivery engines. ActiveMath is a web-based mathematics learing environment. The content is in OMDoc, with formulae in OpenMath. It supports storing documents in "small items", such as 'axiom', 'definition', with many cross-references.

6.8.1 Content Management and Aggregation

Re-use is important. OMDoc is great for this, but we *don't* want cut-and-paste, rather we want to incorporate content collections (by reference!). We have a tool to do this aggregation.

6.8.2 Imports

We want to keep references short, so this becomes an issue of namespace management. We have a tool to support this. There are also issues of metadata inheritance. Inheritance properties are written in the DTDs.

Q–DPC How does one evaluate manegement tools.

A I have ideas, but no formal idea. We use SVN for version control.

6.9 The FMathL Language — Schodl, Neumaier, Schichl

A formal system for specifying numerical problems for global optimization. We want the systm to choose the "best" solver. One year into a three-year project, but it seems pretty promising.

The semantic matrix is a sparse matrix with each column and row representing a concept. So[7] $M_{x\in,\mathbf{N}}$ =true would indicate that $x \in \mathbf{N}$. We translated TPTP[8] into this formalism, and then produced a LaTeX file for each.

We then tried the problems from the OR-library. We extracted the essential parts and represented in a semantic package (by hand). We hen produce a LaTeX file as above, and compare (by eye) with the original.

The "semantic Turing machine" operates on a semantic matrix, and has an assembler language rather than a transition description. In particular, there is a universal one, which needs less than 300 lines of code.

This is much simpler than parsing natural language. We took a 450-page set of lecture notes (in German), which has a 1500 word vocabulary, and a simple

[7]There were questions here, which confused me. He seemed to change his mind, and indicate $M_{M_{x,\in},\mathbf{N}}$.

[8]Thousands of Problems for Theorem Provers.

morphological grammar with about 1000 productions. From this, we have an (almost) automatic translation of these lecture notes into English.

6.10 A Linear Grammar Approach to Mathematical Formula Recognition from PDF — Baker *et al.*, Birmingham

The OCR problem for mathematics is much harder, and the dictionary-checking approach does not work. Fonts and typefaces are also important. (Most) PDF fiels contain characters names, font metrics and character placement commands, but spatial information is insufficiewnt for mathematical formula recognition.

We (manually) clip into TIFF, and have software which will produce bounding boxes. The PDF extractor produces character names, font names and sizes etc., but one visual character, as in $\sqrt{\quad}$, may be made of several PDF characters. We have a function that reverses this encoding, based on the special character names. Equally, a single PDF character, such as `i` may correspond to two apparent glyphs.

[Andeson1968]: a PhD producing a 2D grammar for mathematics. It requires carefully typeset notation, and perfect character input[9], and is restricted, but very efficient. We have taken this, and added many more rules, e.g. matrices and case statements. We also have LaTeX and MathML output.

Demonstrated some examples. They took 128 examples from two books. One could not be parsed, and two gave wrong LaTeX. 18 had slight rendering differences, but no semantic loss. Some of the examples were pretty hard, e.g. $\int\sqrt{\sum\ldots}$. One of the wrong examples was a matrix of differential operators, which was so squeezed that the rows ran into each other, and the matrix recogniser failed.

Are looking at comparing the LaTeX output with the original, to check for gross errors. We also intend to collaborate with the infty project to automate the clipping. In general, this works with most PDfs originating from LaTeX.

Q Explain the diagram showing bounding boxes.

A PDF's bounding boxes are far too large, since they interact with font information, which we don't have. Hence we tend to trim them so as not to interact.

Q–PL You just produce presentation?

A I doubt we can produce full content, but we could do better. At the moment $(x+1)^2$ regards the bracket itself as squared, not the whole

Q–SMW How deeply nested are the `mrows`?

A (At least in LaTeX), we produce text with not too many `{}`.

[9] Generally hard, but using PDF rather than OCR is important here.

A–VS I wrote the MathML, and that does deeply nest the `mrows`. But $a+b\times c$ is a single `mrow`.

Q–CAR To what extent are you *assuming* the LaTeX→ Distiller route?

A We looked at a PDF from Word, and could make neitehr head nor tail of it.

6.11 Confidence Measures in Recognizing Handwritten mathematical Symbols — Golubitsky & Watt

We have recognition at 97.5%, and to improve we need to look at context.

So the idea is to recognise the symbol, as various options with probabilities, and prdict the symbol from context with the same output, and merge. Our methodology was support vector machines.

Standard symbol recognition has an ensemble of linear SVMs. If $\xi_{i,j}$ is the confidence of a vote for C_i over C_j, we can compute the probability that C_i won incorrectly over C_j.

Our symbol recognition is based on distance of the symbol from the (convex hulls of) reference clusters. It's not trivial to translate this methodology.

Then we produce a graph of "quality of confidence measures", i.e. retrospectively is their confidnce correct?

Q–JHD You haven't said mcu about the context-predictor, but it's likely to give several symbols with similar probabilities, e.g. a 3D geometry text might have x y and z as equal favourites.

A We don't yet know how to do this, but are working on it.

A–SMW That's where we're going.

Q More data sets?

A–SMW We're tried two so far, and their envelopes are so similar that trying more is not our highest priority.

Chapter 7

12 July 2009

7.1 A Saturated Extension of Lambda-bar-mu-mu-tilde — Mamane, Geuvers, McKinna

Aim: to use $\overline{\lambda}\mu\tilde{\mu}$ for proof authoring, exchange and a language to talk about prof transformations.

Hypotheses are named.

$$\Gamma \vdash \alpha : A \to B, \beta : A \to V$$

and "assume $A(x)$" is ambiguous in intent: henc eintroduce the concept of a focus:

A logical system is usually minimal, but we actually want greater richness, especially if we want to compare/translate proofs.

This link has been done for Isabelle/Isar (subset), PVS, Mizar, and Coq/Czar. But we still need to implement and automate.

Q This is a multi-conclusion sequent calculus: is it classical or intuitionistic?

A Classical, but ne can build an intuitionistic logic in it.

Q To what extent can these translations, e.g. Mizar, be automated.

A We don't have a Mizar parser, but with one it should be automatable.

Term	v	::==	$x \vert \lambda x : T.v \vert \mu alpha : T.c$
Environment	E	::==	$\cdot \vert v \circ E$
Terminaml Environment	e	::==	$\alpha \vert \overline{\mu} x : T.c$
Command	C	::==	$(v \vert E \vert e)$

7.2 Finite Groups Representation Theory with Coq — Ould Biha

We want to us proof assistants to "program" mathematics. The Feit–Thompson theorem is long (255 pages) and complex, covering a variety of areas, including representation theory, the goal of this project. We actually use Cuq-SSreflect. Coq's logic is, by default, intuitionistic, and a proposition is as object of type `Prop`. It has dependent types, also coercion (both as $\mathbf{N} \to \mathbf{Z}$ and `Ring`→`AbelianGroup`).

SSrelfect is the extension that was first used for the four-colour theorem. It has a new language for tactics, which leds to shorter proof scrips and has integrated small-scale reflection: Boolean ⇔ decidable logical proposition. Also many libraries, originally developed for the Four-Colour Theorem, but "types with decidable equality" and "finite types" will be useful.

A representation is an akgfebar homomorphism $\phi : A \to M_n(F)$. We also need (finitely-generated) modules, and various kinds of sub-structures. Shoiwed a diagram of linear algebra librraies, built on the `ssralg` library, which provides `Zmodtype`, `Ringtype` and `Fieldtype`.

We use packaging and inheritance heavily, and this design seems to work.

Maschke Theorem is a key result in representation theory. We have a Coq proof (he showed the first of three screens of proof). The next steps are Wedderburn's Theorem and character theory.

7.3 The MMT Language — Rabe

MMT arose i the development of OMDoc. MMT is the evolution of OMDoc's fragment for formal theories:

- simple, expressive module system
- foundation-independent
- web-scalable.

We have a graph o ftheories, with orphisms (tructurs, also known as imports, and views). So `monoid` is imported into `cgroup` and `ring`, and `integer` has views of both `cgroup` and `monoid`. By comparison with OMDoc 1 the structures (i.e. imports) are named, and this, apparently minor, change has major consequences. Hence `ring` can decide which copy of `monoid` it is talking about, e.g. whether it is talking about the additive or multiplicative identity.

Logics and foundations are represented as theories. MMT yields module-level semantics relative to the foundation's semantics. The validation of OMDoc documents occurs in three stages:

XML simple and well-supported;

MMT the intermediate stage, which picks up undeclared variables etc.;

semantic needs theorem-proving, type-checking etc., and is foundation-dependent.

Q–RR How do you tell whether you want a *new* copy or not?

A This is a question for the programmer.

Q–JC But what about the carrier type?

A The carrier type is a tricky thing: should it be in the logic or in the theory? Here we put it in the logic.

Q–JC Putting it in the logic makes it hard to use two-sorted algebras.

A Use two-sorted logic!

Q–PL These are always the same examples — monoid etc.

A We do have others.

7.4 Natural Deduction Environment for Matita — Sacerdoti Coen, Tassi

An unexpected consequence of re-electing Berlusconi is that we now teach a first-year first-semester course on logic, which has to include interactive theorem-proving. Can't use two tools: one for natural deduction and logic itself. So we need to *prevent inference* at the student level, but *enable* it at the quick (batch) correction of exercises by the teacher. Also need a simple textual interface, and a palette for syntax learning and speeding the input phase.

We could have gone for an external UI to Matita, or a new plug-in for Matita, but instead we decided to implement *in* Matita, and it works, with the only code change being to add palettes. I claim Matita is the most MKM-friendly interactive theorem prover. It manages a web-distributed, inconsistent library. It has advanced indexing and searching. It uses XML technologies. Three levels of representation:

Semantics (CIC)

content OMDoc+MathML

Presentation BoxML and MathML

Matita has a MathML-Presentation based user interface, which unfortunately has no support for trees[1]. Much of the mapping is done by XSLT. It has to support conversion into semantically-invalid CIC, and back into presentation.

[1]Am trying to persuade MathML to move on this!

7.5 MathLang Translation to Isabelle Syntax — Lamar, Kamareddine, Wells

[Some of this depends on colour, and the proceedings are black/white, so there was a handout, or one can go to his (Lamar's) home page.]

Problem of the hour: go from "normal" mathematician's text to Isabelle etc. text is wrapped in boxed of various colours, so "arithmetic (denoted $a + b$)" is a declaration, a and b are "place-holder" variables, the use of + is a definition, and so on. Once annotated, this text can be used for a variety of uses, including text-to-speech, but the focus of this is to use it for Isabelle.

The template does become a proof sketch, but the rules may *not* be in the right order for Isabelle — it wasn't clear to what extent this mattered. We still need to automate the identification of missing rules.

Q–CSC Why go direct to Isabelle, rather than OMDoc which has translations to Isabelle and more.

A "Proof of concept".

Q–MK How long does it take to annotate text? And to validate it?

A We currently have very little automation, and it might to take hours. We have a checker that verifies some of this.

7.6 Crafting a knowledge base of transformation rules: integration as a test case — Jeffrey & Rich

Fateman (1991) and Carette (2009) are sceptical about rule-based integration. Although we justify this knowledge base (approximately 1300 rules) by computation, the database is also a repository of knowledge. We also have a database of 5841 examples: 1070 rational, c. 1200 algebraic etc. There is then an automatic check, which classifies outputs as optimal/messy/inconclusive. Note that in 'messy' we include cases where one needs to add a constant of integration in order to get simplification, and cases where unnecessary algebraics are introduced.

We are 99% optimal, versus Mathematica's 70% and Maple's 64%[2]. A general feature is that giving a symbolic exponent gives very different results which do not then simplify when integers are substituted in.

We wish to emphasise that this is merely an *example* for repository-based mathematics. The rule database[3] consists of a transformation rule (generally

[2]Including some failures on rational functions. RR was very surprised by this, and subsequent investigation by him showed that it was a case of `simplify` being unable to show correctness.

[3]Currently in Mathematica syntax, but this is not vital.

containing parameters), conditions, which may be necessary ($n \neq -1$), or conditions under which the rule is *useful* — a rule is only useful if you know when to use it. Aesthetically, we use the trig/hyperbolic symmetry, which generally leads to shorter results as well. Note that this is *not* a complete compilation of all integrals we have seen — redundant entries have been eliminated, and the 'utility conditions' have been heavily optimised.

Q–SMW Performance?

A–DJJ We currently do linear search through the database in Mathematica, and are about 5 times as fast as Mathematica's own integrator.

A–AR A tree-based matcher is on the agenda.

7.7 Software Engineering for Mathematics — Gonthier *et al.*

See also section .1. This talk was advertised with the following abstract.

> While the use of proof assistants has been picking up in computer science, they have yet to become popular in traditional mathematics. Perhaps this is because their main function, checking proofs down to their finest details, is at odds with mathematical practice, which ignores or defers details in order to apply and combine abstractions in creative and elegant ways. This mismatch parallels that between software requirements and implementation. In this talk we will explore how software engineering techniques like component-based design can be transposed to formal logic and help bridge the gap between rigor and abstraction.

[A joint Microsoft/INRIA project]. Formally proved the Four-Colour Theorem. Now interested in the classification of finite simple groups, justified by Jordan–Hölder.

Theorem 1 (Classification) *All finite simple groups belong to one of 16 classes, except for 26 sporadic.*

JHD has stated that this was 30,000 pages, but I have heard recently that it was 6,000. Feit–Thompson is one of major items on the way.

There has been nothing substantial in formal proof since 2005/6, though Hales is working on Kepler (with an army of vietnamese postgraduates). Computers are math-illiterate (see section 3.6), and even if we fix this, they will still be *functionally* math-illiterate. I claim that Software Engineering deals with complexity, and will help with this. Language design is part, but not one I will talk about. Instead I will talk about components.

first-order logic	mathematics
Fixed Symbol Set	Definitions
Free terms	formation rules
Context-free	"Abus de notation"
Axioms and Theorems	Axioms and Theorems **and Exercises**
Herbrand unification	Interpretation and Computation

7.7.1 Diagnosis

Let's compare first-order logic with mathematics. Therefore I conclude that mathematics is a typed higher-order language.

This leads to "the library problem". The caller has to adopt to the library's calling convention. The solution is for the library to publish metadata describing its servive, and the caller to read this and build an interface.

I claim that mathematicians exploit (higher-order) types to express intent. Group modules, group algebras and matrix algebras are all equivalent, but authors choose the 'right' one.

`bool` is concrete and computable (e.g. truth tables), whereas `Prop` is abstract and provable. Need constructs to move between them.

For the Four-Colour Theorem,

```
variable cf::config
Definition cfreducible: Prop :=
Definition check_reducible: bool :=
Lemma check_reducible_valid: check_reducible ->  cfreducible
```

7.7.2 Big operators

Want to be able to use the Leibniz determinant formula for the determinant. This needs inferred notation, i.e polymorphism with dependent records.

Q–DPC How important are depenbdent types.

A We need them for the group interfaces based on sets.

Q Does your approach to finiteness extend to concepts like "finite dimensional"?

A You need a theorem that it is basis-invariant, but then you pick a basis, and the problem is finite.

7.8 OpenMath Content Dictionaries for SI Quantities and Units — Collins

My guiding principles:

- Lack of ambiguity;

- Convenience;
- Simplicity (hard to separate form above);
- Distinguishing Presentation from Content.

Seven `SI_???` CDs and `FundamentalPhysicalConstants`.

The chart was introduced: the items in the box are SI-defined. The base units are a generating set for the coherent derived units, some of which are named.

The U.S. Navy uses Joint METOC Brokerage Language (JMBL), e.g. `kilogramsPerMeterCubedTimesMtersPerSecond`.

Claims that rules like "right application of units", "left application of prefixes", "unicity of prefixes" are all presentation issues. What we normally call "abbreviations" are called "symbols" by SI, and again this is, he asserts, a presentation issue. By analogy, "division" in OpenMath only has one name, not 'vinculus', 'solidus' etc.

Introduces dim, unit, num, and (unstandardised) kind. A Real Scalar Coherent Quantity is a product of **R** and the abelian group of coherent derived units. There are CDs for derived quantites corresponding to each named derived unit, and 'gram' added to the CD of named derived units for completeness. There are also defined (e.g. litre) and measured (e.g. electronvolt) off-system units

The Planck units are used by certain physicists, but "their magnitude makes them unsuitable for everyday use". I have not completely resolved the issues of types, but believe it should model my diagram. The `unit` operator can

Korean Air 6316 (cargo flight) crashed 15 April 1999 from Shanghai to Seoul, cnfusing metrs (tower) and feet (altimeter).

Q–CL How does this differ from JHD?

A Our differences are small — I am focusing primarily on SI.

Q–BM UnitsML?

A The UnitsML team at NIST are interested in collaboration.

7.9 Integration Web Services into Interactive Mathematical Documents — Giceva, Lange, Rabe

Most mathematics on the web is not interactive. ActiveMath, for example, is a counterexample. The (non-mathematical) web 2.0 has examples like Craig's List and Google Maps being combined into a "Mashup" housing map. JOBAD: **J**avaScript API for **O**MDoc-**B**ased **A**ctive **D**ocuments — `http://jomdoc.omdoc.org/wiki/JOBAD`. A key service is the rendering service: currently OpenMath → MathML, but which needs to be given more user control. We use `maction` for alternative display, and use fine-grained parallel markup. An example with an ‘abbreviation’ attribution. One service is the [Str08] unit conversion service, which can be selected for a number multiplied by a unit.

The fine-grained cross-linking (presentation → content) is needed to support cut-and-paste. Can use `<maction type=elision` to indicate a bracket that is not conceptually needed because of precedence, but which the author may wish to show.

We have no fixed access model (REST versus XML-RPC versus SOAP).

7.10 Compensating the Computational Bias of Spreadsheets with MKM Techniques — Kohlhase[2]

It has been estimated (how?) 1.9×10^8 spreadsheets in active use. *But* there is almost no software engineering or documentation support. [Winograd2006] is the classic example. A spreadsheet is an active document. Apart from the ‘legend’ cells, all cells are in functional blocks. Every cell has a formula, which may be a numeric constant. Although formulae are designed in blocks (the intended functions from a family of cells), each formula is logically separate in Excel. In general there are no types, and no explanation for the origin of data. There is no explanation for what Excel means by `+`.

We have an ontology that “understands” concepts like ‘revenues’, and also has enough types to know that years are AD etc. 27 general accounting, quantities etc. theories, 20 specific to the company, 12 underlying mathematical ones. The ‘bias’ of the title is a ‘semantic bias’, against recording the **intention**. Note that this is not restricted to Excel (apparently similar ideas work in Excel, though JHD fails to see how), and they are looking at Computer-Aided Design.

7.11 Spreadsheet Interaction with Frames: Exploring a Mathematical Practice — Kohlhase

Framing is understanding a new object in terms of already understood objects.

Bibliography

[AH76] K.I. Appel and W. Haken. Every Planar Map is Four-Colorable. *Bull. A.M.S.*, 82:711–712, 1976.

[Asc00] M Aschbacher. Finite Group Theory, 2nd edition. *Cambridge University Press*, 2000.

[BG94] H. Bender and G. Glauberman. Local Analysis for the Odd Order Theorem. *LMS Tracts in Mathematics 188*, 1994.

[CGGG83] B.W. Char, K.O. Geddes, M.W. Gentleman, and G.H. Gonnet. The Design of MAPLE: A Compact, Portable and Powerful Computer Algebra System. In *Proceedings EUROCAL 83 [Springer Lecture Notes in Computer Science 162*, pages 101–115, 1983.

[Col75] G.E. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. In *Proceedings 2nd. GI Conference Automata Theory & Formal Languages*, pages 134–183, 1975.

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

[DK09] J.H. Davenport and M. Kohlhase. Unifying Math Ontologies: A tale of two standards (extended abstract). In L. Dixon *et al.*, editor, *Proceedings Calculemus/MKM 2009*, pages 263–278, 2009.

[FT63] W. Feit and J.G. Thompson. Solvability of Groups of Odd Order. *Pacific J. Math.*, 13:775–1029, 1963.

[GCL92] K.O. Geddes, S.R. Czapor, and G. Labahn. Algorithms for Computer Algebra. *Kluwer*, 1992.

[Gor83] D.M. Gorenstein. The Classification of Finite Simple Groups. *Plenum Press*, 1983.

[Hon91] H. Hong. Comparison of several decision algorithms for the existential theory of the reals. Technical Report 91-41, 1991.

[McC93] S. McCallum. Solving polynomial strict inequalities using cylindrical algebraic decomposition. *Computer J.*, 36:432–438, 1993.

[MW96] A. Macintyre and A. Wilkie. On the decidability of the real exponential field. *Kreiseliana: About and Around Georg Kreisel*, pages 441–467, 1996.

[Pet00] T. Peterfalvi. Character Theory for the Odd Order Theorem. *LMS Tracts in Mathematics 272*, 2000.

[Str08] J.D. Stratford. OpenMath-based Unit Converter. *B.Sc. Dissertation*, 2008.

[Wei99] V. Weispfenning. Mixed Real-Integer Linear Quantifier Elimination. In S. Dooley, editor, *Proceedings ISSAC '99*, pages 129–136, 1999.

.1 Gonthier at Waterloo

He spoke informally at Waterloo on the afternoon of 13 July 2009. His main versions of the proof are in [BG94, Pet00], rather than the original [FT63]. He noted that both [Gor83] and [Asc00] contain numerous errors: serious but not fatal in *context*.

One significant theorem [BG94, Theorem 3.6], which concludes that the group in question must have p-length 1, *has* been completely proved in Coq. Another key theorem, that if $G \subset \mathrm{Hom}(\mathbf{F}_p^2)$ with $|G|$ odd, then $G^{(1)}$ is a p-group, has not yet been proved because of the amount of field theory required.

Most of the groups M under consideration[4] are Frobenius groups, i.e. transitive permutation groups on a finite set, such that no non-trivial element fixes more than one point and some non-trivial element fixes a point. It is a result that, if the conjugates of U (which happen to be a group less the identity) fix most of M, thenthe rest of M is nilpotent.

To do character theory, one needs algebraic numbers. In fatc it's a theorem of Brouwer that only $|G|$-th roots of unity are needed, but of course we would have to *prove* this, which actually needs general algebraic numbers. Furthermore, we need an embedding into $\mathbf{R}$, since some inequalities are fundamental to the proof, and this is therefore much more than an abstract field-theoretic construction.

[4]JHD arrived part-way through, so "consideration" was not well-defined for him.