CICM 2014 (and ADG 2014)

Partial notes by J.H. Davenport — `J.H.Davenport@bath.ac.uk`

7–11 July 2014

Contents

Chapter 1

OpenMath Workshop

1.1 Lars Hellström:

OM allows variadic operators, but how to state FMPs etc.? Claims can be solved by symbols in a CD.

Inspiration: TCL, as a scripting language. This is primarily a dispatch engine. The command procedure receives arguments, argv-like.

Core syntax can read variables, and use results of commands. Writing variables is via `set` command, also control flow. TCL is very variadic, so should be sufficient for OpenMath.

An entity can be an item or a (possibly empty) sequence of items. TCL uses `{*}`, "splode", and a word beginning with splode contributes a sequence, else an item. Splode was new in 2003, revised in 2006. One argument against its introduction was that it could be done via eval.

`list4#eval` sort of does the same as TCL's eval. But this would need an infinite sequence of axioms. This solved items 1-3 of [HKR11]. Doesn't cover variadic variable binding (TCL not a problem as variable bindings are semantic, not syntactic).

JWK: I want a way to treat a sequence as a single item - possibly a further symbol.

CR: maybe we should define these as operators on lists.

1.2 Michael Kohlhase: OpenMath Language Extensions

Note that OM2 is 10 years old, and is now firmly embedded in MathML3. There is a lot of experience with OM2 and lots of extension proposals. Note that OM's CD mechanism is akin to adding functionality to a programming language by libraries. **But** programming languages (JHD would say only “some”) allow extensions of syntax as well.

Therefore we present a language extension proposal, using [HKR11] as a running example. The semantics of LEDs (Language Extension Dictionaries) is given by translation into OM2. More formally, OM3 should be OM2 + bug fixes + LEDs.

An LED should

- Extend the syntax (RelaxNG)
- Specify the semantics (via translation)
- Equality ..., need to know what equality of these extended objects means.

Example: `OMNTH` and `OMNATS`.

SMW What do you gain by going this way.

A OM is not meant to be minimal, but useful.

Future How does an `OMOBJ` specify what LEDs it is using —not currently addressed. Binary encoding?

1.3 Michael Kohlhase: Records in Pragmatic OM

“My pet language extension proposal”. Note that OpenMath has gone for functionality rather than minimality (n-ary, integrals as binders etc.).

“A ring is a triple $\langle R, +, \cdot\rangle$ with ... ”, a triple *with named components*, e.g. “a ring is commutative is the multiplication operator is”.

LH Do you know of a textbook which goes into this (handling of tuples) formally?

A not as such.

Observations: record structures are syntactically similar to attributes, and his example (ab)uses `OMATP`, outside `OMATTR`, to give the names to the record elements. Note `OMATP` takes $2k$ arguments, with k implied equality symbols. However, this doesn’t allow selectors, and we should also have equalities: these β/η equalities can be done via the mechanism of the previous talk.

1.4 Lars Hellström: Literate Programming

OM2013: suggested that CDs could benefit from Literate Programming approach. Have a system where generating the literate document produces the `.ocd` as a side-effect.

CMPs, FMPs and Examples all work. Not all omel currently supported.

Should do STS in a similar way.

Can the community please pick a standard for notation specification! It should cover priority vs binding strength!

Improve rendering of omels. Currently good if you are trying to debug the XML, but not very readable.

Works via `\begin{OpenMathCD}{list4}` Etc. currently uses straight quotes and text ..., but a referee objected, and we could use fancy TeX commands, getting Unicode hex-escapes in the CML.

Users: me (addicted to LP), authors who are prepared to document, but who aren't necessarily familiar with XML technology. Also my students, for whom it reduces the learning curve.

JWK: did you consider Popcorn?

A: Popcorn parser in LaTeX is non-trivial

1.5 Rabe: MMT

This [MMT] may be the biggest OpenMath-based project. So what have I learned? This isn't a formal proposal

More that there's only four elements in the MMT grammar, with "complex object" unifying four of OpenMath's. Also, only a single "literal constructor".

MMT has no attributions, since contexts declare variables. Ignorable attributions should be extra-linguistic metadata.

MMT's complex object $c(\gamma; \Gamma; \overline{E})$. The semantics are purely those of c, the MMT constructor itself is purely structural.

1.6 Davenport

See slides at `http://staff.bath.ac.uk/Slides`

1.7 Formal OpenMath Business Meeting

1.7.1 Chair

MK was proposed by JHD seconded by JWK.

1.7.2 Secretary

JHD was proposed by MK and seconded by JWK

Minute checkers: JWK and CAR were proposed and seconded.

1.7.3 Annual Report

No income and expenditure. MS normally paid the domain registration fees, and he was thanked for doing this.

1.7.4 New Members

Moritz Schubolz was nominated as a new member, having worked on OpenMath for over three months.

1.7.5 Executive Committee

Christina Müller (Treasurer) was no longer active. MK nominated LH as Treasurer, who was willing, and JHD seconded. The Committee, as thus modified, was re-elected unanimously.

1.7.6 AOB

None.

1.8 Technical OpenMath Business Meeting

MK presented a report of the Standards Extension Committee. It was noted that synchronisation of OpenMath 2 with MathML 3 was an excellent idea, not to be sacrificed.

This report led to a useful debate.

Q Is there a concept of language binding, e.g. for GAP.

A Yes - phrasebook is the technical term. There is a GAP one, out of the Science project.

Q Is there any "why use MathML" documentation — how to persuade people not to use SVG?

A This isn't exclusively OpenMath's problem, but we should be part of the solution. There should be information on the MathML pages.

Q What are CDs for?

A That is for the author — largely mathematical objects.

Q' I was thinking of (specification for) function plots — general approval.

Q In a field, e.g. special functions, these should be written by the real experts in the field

A Agreed: that's the OpenMath philosophy. There's a description in the OM standard, and "On Writing OpenMath Content Dictionaries" [Dav00] and on `www.openmath.org/documents/`.

Q What about RDF?

A See Christoph Lange's work [Lan11, LID^{+}12, and his thesis].

Q–JWK There are questions of what tool — MK was proposing XSLT, but what about XSLT2.

A Good question. But specifying from scratch would be a PhD project in itself.

1.8.1 Extended OpenMath

MK described the following. OM2 described a certain kind of labelled trees as OM2OBJ, and the standard specifies certain rules (e.g. α-conversion). The CDs specifies more rules, so that it is **legal** (not compulsory) to apply associativity to '+', translate $\sin 0$ to 0, etc. If we extend OpenMath by some extension mechanism, then we get new objects (OM3OBJ). What then is their relationship and equality.

Proposal 1 *That there should be an OpenMath Extension Proposal, possibly based on a revised version of [Koh14]. JWK would write up his alternative. This would be continued by e-mail.*

Proposal 2 *That OpenMath should adopt MathML-3 (Content) as an alternative encoding, and mandated DPC*[1] *to propose the relevant extensions to the standard to document this.*

Proposal 3 *LH (and JHD) had called for a standard "notation" mechanism. MK to document and circulate the Bremen notation mechanism, which can generate Presentation Math-ML. JWK was very interested in this project.*

[1]Post-Meeting Note. JWK was looking at upgrading the Java OM-LIP (RIACA) library to support this: he and DPC should liaise.

Chapter 2

Yves Bertot: A naïve view of Homotopy Type Theory and its relation to the Calculus of Constructions

2.1 Conjunction

Note that there is growing complexity in mathematics, e.g. [FT63] was250 pages. Also discontent, Voevodsky[1], Hales. Hence an interest in computer verification of proof: one promising approach is the Curry–Howard isomorphism.

We need

- A language for the objects of discourse
- Verification algorithms, for well-formed and verifying that the proofs respect the rules of logic
- Variety of choices: LCF style *proofs are in the same language) or Intensional Type Theory.

$A \to B$ — " a proof of A should construct a proof of B". A [pair of] proofs of A and B is a proof of $A \wedge B$.

Hence with dependent types, we can use proofs as certificates. Hence the proof language is itself a programming language, and we might be able to be extract algorithms. This raises new questions.

- If (a, p) and (a, p') are certified values, are they equal?
- Are proofs relevant

[1] "I now know that a paper I published 10 years ago is wrong."

- What is “equality of proofs”?

2.1.1 What is this thing called Equality?

`A:x=y` is a type. This is an inductive type with a single constructor`refl`.

2.2 Intensional Type Theory

$\forall A : Type \forall x : A.$ is necessary. Also

$$\forall P : A \to Prop.P(x) \Rightarrow \forall y : Ax = y \Rightarrow P(y)$$

(everything true of x is also true of y).

This is not the same as saying “identical” [HoffmannStreicher1998].

2.3 Paths in homotopy theory

“$X = Y$” is “X goes to Y”. A topological space is a contraction where

- There is a centre of the contraction
- ...

A Groupoid is a special kind of category where every morphism is an isomorphism. The abstract definition of equivalence relations. If p_1 is a proof that $x \sim y$ and p_2 that $y \sim z$, then $p_1 \bullet p_2$ is a proof that $x \sim z$. Symmetry is denoted by $^{-1}$: o_1^{-1} is a proof that $t \sim x$. Reflexivity is an element 1. We need various coherence laws. This is like a group, but $\bullet$ is partial. A higher groupoid is where the properties of $\bullet$ are stated as proofs of equivalence in another groupoid. An ∞-groupoid is the limit of this process.

In homotopy theory, paths form an ∞-groupoid. In type theory, proofs of equality form an ∞-groupoid. Hence we get a new correspondence: types as topological spaces. Many proof of homotopy theory can be modelled directly in type theory. Topological structures can be modelled by adding new paths around points.

Examples of topological spaces: interval, circle)one point and a non-trivial part, or two points and two paths)[2], the sphere (two points, and for every point on the equator (circle) a path from A to B via this point (meridian); or a base point and ...). Types of paths are themselves topological spaces.

2.3.1 Suspension of a structure A

Two points X and Y, and for every point in A, a path from X to Y.

bool is the suspension of the empty set.

[2]These are the same by homotopy equivalence.

circle is the suspension of bool

Sphere is the suspension of the circle

etc.

2.3.2 Should you be afraid?

Homotopy type theory looks at the microscopical level. Continuity of real numbers lives at another level.

It distinguishes types where all points have trivial type spaces (called hsets) and for them UIP holds. Hedberg theorem: datatypes with decidable equality are hsets. For instance `nat`. Also distinguishes types with at most one element. For them, proof-irrelevance holds.

2.3.3 What are the gains?

Synthetic homotopy type theory

Understanding of quotients (a systematic approach to adding equations)

Advantages of hsets are already exploited in `ssreflect`.

The univalence theorem (isomorphic types are equal) is very powerful.

Q How much of this is type theory, and how much is category theory?

A We only use the basic concepts of category theory.

Chapter 3

Doctoral Programme

3.1 Ieuan Evans: Pachinko Allocation Model Applied to Mathematical Document Classification

3.1.1 Current

Started looking at OCR-based recognition, but moved more into document classification. What is the content behind "$(0,1)$" — depends on context. For example "continuous" is a clue that it means the open interval, and so on.

Pachinko is an unsupervised topic allocator. Latent Dirichlet Allocation is a common alternative. A *topic* is a probability distribution over words. The LDA model allows multiple topics within a document, and words can occur in several topics.

Pachinko. Each word has a super-topic label, a topic label and an integer label. LDA is the special case with only one supertopic. This has been used to classify mathematical documents based on words. We are also doing this on symbols, with the own distribution. **Note** that there is only one distribution of supertopics.

Why have I done this. Partly because topics, such as set theory, are common, and that wants to be a single cluster. Conversely, calculus (one word topic) has two notational conventions (deisme versus dotage). But this allow reuse of existing techniques/tools.

3.1.2 Future

These find **anonymous** topics. We would like to assign based on, say, MSC, hence we will train on a supervised category (ArXiV). Supervised LDA exists but in several variants.

Q–MK You said "refine then model", then do experiments. Shouldn't it be the other way round?

A It's much easier after I have labelled tree.

Q–AS What about compound words.

A sin is one word, but that's as far as it does. These are all "bag of words" models.

Q–JWK "i" versus "j"?

A Two clusters of symbols in the same super-topic, I hope.

3.2 Washington Secundo

Barendreght's variable convention: terms are α-congruent, and bound variables are taken to be different from free ones. One solution is de Bruijn indices, another is locally nameless.

Prolog uses First-order Abstract Syntax, there is Higher-order Abstract Syntax (Coq, PVS). Nominal Abstract Syntax is in NRT in Coq, and Nominal Isabelle. Free and bound variables

Q New approach, or old ideas.

A Mixture. Nominal is very superficial in Coq.

3.3 Algebraic Algorithms for Numerical semigroups

Based n previous word "On the enumeration of the set of saturated numerical semigroups with fixed Frobenius number".

Submonoid of $\mathbf{N}$, such that it's complement in $\mathbf{N}$ is finite. Example are "boxes of doughnuts". The last number you can't get is the Frobenius number. Let $d(a) = \gcd\{x \in A :\leq a\}$. S is saturated if, for all $s \in S$, $s_d - s) \in S$.

An F-saturated sequence is a saturated sequence such that there is a $(d_1, \ldots)$-semigroup with Frobenius number F. Type 1: $\gcd(F+1, d_2) = 1 \wedge F \not\equiv -$ (mod d_2) and Type-2 otherwise.

Algorithm 1 - brute force.

Theorem, then algorithm 2. This only gives the groups, not the sequences. Algorithms 3 and 4 compute these for types 1 and 2 respectively, for an input F. Theorem in paper shows limits on length.

Algorithm 3 takes all second elements, the up to the limit builds possibilities for Type 1. Complexity for stage n is $O(TF^{n-2}$ where T is the size of the magic set. Algorithm 4 similar for Type 2. Run these two, then Algorithm2 to find the sequences.

Implementations in GAP. Original dies well before 100, now does thousands easily.

Chapter 4

Notion of Proof

4.1 Kinyon: Loops and Automated Deduction

Dedicated to William McCune.

Tools are Automated Theorem Provers: McCune's Prover9 (descendant of Otter), Hillebrand's Waldmeister, also SAT solves etc.

Definition 1 Quasigroup $(Q, ., /, \backslash)$ *with equation that say that they interact as multiplication/division. The alternative definition, mathematically neater ("Multiplication is a Latin square"), tends to make provers introduce Skolem functions.*

Definition 2 *A* loop *is a quasigroup with an identity.*

Best known non-associative examples are Moufang loops, e.g. octonions.

The left and right translations are permutations. Call the group generated $\mathrm{Mlt}(Q)$. Those that fit the identity are $\mathrm{Mlt}(Q)_1$, the "inner multiplications", which correspond to inner automorphisms.

Definition 3 Automorphic loops *are those where* $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$

Definition 4 *A loo is* diassociative *if every subloop which can be generated by no more than two elements is associative.*

Every Moufang loop is diassociative (a consequence of Moufang's Theorem). Is the converse true? Yes for commutative loops [Osborn1958] — large manual proof.

First time took a week elapsed time to get an Otter proof (actual overnight run), with Prover9 now taking a minute. Proof unreadable to a human — "The Humanisation Imperative".

> If a proof can be reasonable translated into a human form, then we should do so.

Found a human-readable proof , which nevertheless contains a step no human would probably have discovered. Hence the machine-generated proof was vital.

A technical result is that, in . . . , the product of squares is a square.

We often get Prover9 proofs that are several thousand steps long. Often (not always, and counterexamples are more common than I would like) stating a lemma one discovers automatically will shorten the proof.

Q Would you be happy understanding "the idea of the proof"

A Yes, but I don't know how to express that.

Q Is heavy computing the main requirement?

A Not really: software is the main problem now.

Example - smallest nonassociative Moufang loop has order 81 — can't be found by brute force.

Chapter 5

Calculemus

5.1 England: Problem Formulation ...

Lots of background (to appear in [BCD+14]). Various heuristics to decide how to choose which?

In RC-TTICAD, the order in which the problem is written down matters. All previous heuristics are essentially commutative[1], so don't help. O a small example, ranges from 25 to 81 cells.

Generated 100 random system. The average TTICAD had 2108 cells in 37 seconds, median 15?? in 6 seconds. Hence ∃ outliers. All heuristics do better than the average in cell count, but heuristic 2 costs more than it saves in time. Heuristic 1 is almost 3 and certainly helps.

Q Adjacency

A Good question

5.2 Huang: Applying machine learning to choose the variable ordering for CAD

"CAD is the key tool for computational geometry". Various heuristics. Our examples were all 3-variable NLSAT examples. Used both unquantified (T/F) and quantifier-free variants. Used QEPCAD to count number of (intermediate) cells. For each example, coded each heuristic with +1 (found best order) or −1 (otherwise). Used SVM-Light and Matthews correlation coefficient

$$MCC := \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP) \cdots}}.$$

[1] JHD's phrasing

Want to look at a wider class of examples, and also look at more features. Currently also analysing only QEPCAD: should look at the selection across implementations.

Q How long does it take?

A Building the data, and training are expensive, but running is very cheap.

5.3 Formal Reliability ...

Given by Umair Siddique.

These pipelines are thousands of kilometres around the world, and their reliability analysis is difficult: cost, availability and environment: just look at Deepwater Horizon. To complicate matters, some of these pipelines are ageing.

Want a reliability analysis, done this way

1. Partition into reliability blocks
2. Analyse each $R(t) = Pr(X > t) = 1 - Pr(X \leq t) = 1 - F_x(t)$ where X is a random variable denoting failure time.
3. compose results (based on series/parallel block diagram). Series = multiply the $R(t)$ values, parallel multiply the complements.

- Pencil/paper(+ texts) — error prone
- Computer simulations, which are not exhaustive
- Therefore neither is guaranteed.

For formal methods, we have the choice between Theorem Proving and Model Checking. Note that we have to deal with continuous variables.

?? 2002 Discrete probability analysis

Hasan 2007 Continuous probability analysis

Abbasi 2010 Reliability Analysis

2011 [Mhamdi], [Höltzl] two formal methods.]

Example: 60 segments. Abut 100 lines of HOL (on top of tools).

5.4 Lisitsa: Detecting unknots via equational reasoning

Diagram of a potential knot — is it an unknot? In fact the *culprit unknot*.

Question 1 *Is it possible to transform* $\mathbf{R}^3$ *continuously such that ....*

Consider the projection on the plane (as in examples), and in a discrete representation. Represented as Gauss Codes. [Haken1961] showed this is decidable. Known to lie in coNP [Hassetal1999], and GRH implies it is NP [Kuperberg2011]. So the theoretical question is whether it is in PTIME. We are more concerned with practical methods. Reidemeister moves capture knot equivalence. But this leads to NEXPTIME. [Dynnikovetal2000] is a practically fast (in theory EXPTIME) recognition process, but doesn't lead to a decision procedure. [Butronetal2012] uses normal surface theory, and provide efficient recognition of non-trivial knots. Recognises every non-trivial knot with crossing number ≤ 12 in ≤ 5 minutes. Hence we would like to do better.

Definition 5 *An* involutory quandle *satisfies three properties of* $\triangleleft$ *[he quoted* $\triangleright$*]*

1. $\forall a, b \exists ! c : a = c \triangleleft b$
2. $(a \triangleleft b) \triangleleft c) = (a \triangleleft c) \triangleleft (b \triangleleft c)$
3. $\triangleleft = \triangleleft^{-1}$ *(involutory).*

This is a knot invariant, and is trivial iff we actually have an unknot.

We convert the task of triviality detection into a theorem-proving one: can we deduce that all variables are equal. So start a prover and a disprover.

10 crossings: Regina average 47 seconds, and us 1230 seconds. But up to countermodels with sizes $\leq 15 - -17$ takes$<$ 11s, and in 70% of the time we outperform Regina. Which unknots can be untangled by a particular class of Reidemeister moves? If only 1,2,3 we can build an equational proof from the sequence of moves.

5.5 Wegner: Patent Analysis

Current procedures by lawyers produce a big backlog, and have big problems with decisions based on emerging technologies. also the decisions have a lack of precision. A patent analysis is based on

- text of patent application
- applications "prior art"
- "pertinent skill" as defined by standard literature
- And the text of SPL — Substantive Patent Law (we use US Law 35 USC) This represents 10 tests. Other SPLs would be similar.

The questions revolve around the "inventive concepts". These should be embedded in a mathematical and logical framework.These consists of a legal part and a creative part.

A concept C is represented by a map MC from its domains DC to its values VC. We consider binary concepts. In IES/FSTP the assignment of T/F will follow from the text of the application. An equivalent description ...

Let CA and CB be two sets of concepts with sets covering the concepts A and B. T transformation is a bijection TCACB from A to B. In general this isn't a map from CA to CB, but induces a relation. Use "concept transformations" to extend/restrict concepts. Note, however, that our explanation has be to cast in terms of the text of the original document. Three levels of analysis.

1. original document
2. binary aggregate disclosed concepts
3. binary elementary disclosed concepts

Some of the ten tests are automatically taken into account in this encoding: the first four are implied by the disaggregation into elementary concepts. The next three are about novelty/obviousness (note that mathematics is not patentable) but a key test is "not idempotent from prior art"

5.6 Cerna: A Tableaux-Based Decision Procedure for Multi-Parameter Propositional Schemata

Most of the subclasses of the class of propositional schema are unsatisfiable.

Theorem 1 ([Aravantinosetal2011]) ...

Have a concept of "Limited Schemata", where the scopes of variables are controlled. Propositional symbols only occur in the scope of at most one free parameter. Concept of a "relatively pure" literal.

5.7 Johansson: Hipster: Integrating Theory Explanation in a Proof Assistant

Theory Exploration Paradigm — Buchberger(2000) [BDJ$^+$01, probably]. Proof by induction as a case study. Often need extra lemmas (themselves proved by induction). Quite often it's necessary to generalise.

Previous work was HipSpec is an inductive prover for Haskell. It generates equational conjectures (tested, not proved). It applies [structural] induction, then call off-the-shelf FO-provers.

HipSter is Isabelle/HOL (translated into Haskell). Uses the conjecture generation from HipSpec. Currently only equational conjectures.

Demo: exploring a theory about binary trees (data at leaves only). Finds two (useful) lemmas, plus many discarded ones. Apparently "useful" = "needed induction to prove". Claims this greatly helps Sledgehammer.

Q But Haskell is not Isabelle.

A In theory we could go wrong if a conjecture is true in Haskell's semantics, but not Isabelle's. However, all the *proving* is done in Isabelle.

5.8 Tahane: Formalization of Complex Vectors in Higher Order Logic

Complex vectors are used to describe manifolds etc. One application is electromagnetic field computation. How does one verify such a computation. Obviously a complex vector is a vector with complex numbers, but in practice they are thought of *interchangeably* as pairs of real vectors.

Work flow as follows.

1. Type definitions.
2. Basic operations.
3. Vector space, functions `flatten` and `unflatten` to go to/from $\mathbf{R}^n \oplus \mathbf{R}^n$.
4. Vector product ($n = 3$ only).
5. Infinite summation (based on real vectors).

5.8.1 Application: Light

A vector field is a time-varying function of space.

```
type: emf = point -> time -> complex* x complex*
```

Monochromatic plane waves are `emf` satisfying the wave equation and various physical constraints. The fields must be orthogonal to the direction of propagation. The simplest device is a plane interface, but even this translates into a dense page of code. Then the law of reflection becomes a (provable) theorem!

Q Quantum mechanics?

A Possible,and we have done some of this.

Chapter 6

Weisstein: Computable data,mathematics, and digital libraries in Mathematics and Wolfram—Alpha

I've been in this area since AltaVista/NCSA Mosaic. Note that DML is

- currently a hot topic
- Good in terms of long-term validity of the papers being looked at
- Not amenable to Google as MathSearch is an unsolved problem.

Notes, with approval, the Sloan report [Nat14].

Wolfram Alpha is updated every week. It's a "knowledge engine", not just a search engine. Over 1M queries/day. The logs *are* looked at by humans. Enough human input into the database (partly based on this feedback), e.g. "meaning of life".

Uses Mathematica 10 (now "the Wolfram Language") as the computational engine. This now has "free from input", which is basically Alpha-like input,e.g. "population of Coimbra" returns a number which could be factored. "Angular momentum of a pendulum" return a genuine Mathematica formula, which is "tagged" (JHD couldn't quite see what the tags were).

Examples such as "flags of all African countries (with tooltips)" in two lines. But doesn't have any support for movies.

Can produce diagrams showing correlations between things in the database, e.g. chemical elements occurring together etc.

6.1 eCF Project

Funded by Sloan. In the "continued fractions" area, and organised at the 'result' level, rather than the 'paper' level. We think this should be a prototype area for a DML. There were 7K articles/books and 150K pages. The mining was done by hand, as was the encoding. Now have same conventions and notation. We think this is the first comprehensive table of identities in this area. Also links to the "people" (i.e. author) database. Can also ask "what sort of theorems apply to ...".

Currently running at 250 hits/day — not great by world standards, but not bad for mathematics.

The tagging is time-consuming. We know (now) that we can automate parts of it. But it would take all mathematicians in the US working for three years to do the whole of mathematics.

Q–MK "Math for the people" or a land grab?

A Needed Sloan funding, but Stephen is genuinely interested in this — see MathWorld.

Q How does this scale? Are there links from your database back to the original papers etc.?

A Current thinking is in terms of "papers", whereas this database is in terms of results. This will probably require a mind-shift. This requires "math annotation", a different field from text annotation. At the moment it will tell you which paper it came from, but there isn't a direct link. In general Wolfram Alpha currently quotes sources at the macro level, but working on micro-sourcing.

Q Support for multiple human languages?

A Not economically feasible for us. The Chinese Government are funding a Chinese version (with appropriate geographical adjustments).

Chapter 7

CICM Business Meeting

MK, as CICM Secretary, opened the meeting. He noted that we had now gone to one business meeting, rather than one per day, as in Bath.

7.1 Scribe

JHD as usual.

7.2 Trustees

CICM is an organisation-of-organisations, and has 3 (?+AISC) members; Calculemus, MKM and DML. It is governed by a Steering Committee (SC).

MK is not standing for re-election as Secretary after CICM 2015: the Steering Committee will need to nominate a replacement.

CICM 2015 will be in Wastington DC (Bruce Miller & Abdou Youssef). The SC has nominated a Programme Chair for 2016, but yet tobe confirmed. We have track Chairs for 2015: S&P Florian Rabe, MKM Cesary Kaliszek. DML and Calculemus yet to nominate.

7.3 Treasurer

2008/10/11 made a surplus (5380euros). There is a surplus from 2012, but MK is still fighting the admin. 2009 and 2013 (Bath) broke even. We have decided that we will underwrite up to 5,000Euro for student travel. Local organisers should still endeavour to raise such funds locally (as 2013 and 2014 did). The 2015 organisers noted that Washington DC was an expensive place.

In response to a question, MK noted that historically student bursaries have been linked to the doctoral programme.

Figure 7.1: Acceptance Rates

Main tracks:	2014		2013		2012	
Calculemus	8 / 14	57%	5 / 12	42%	7 / 9	78%
DML	6 / 8	75%	6 / 8	75%	2 / 3	67%
MKM	12 / 16	75%	7 / 18	39%	14 / 19	74%
S&P	9 / 14	64%	12 / 16	75%	11 / 12	92%
Overall	35 / 52	67%	30 / 54	56%	34 / 43	79%

Figure 7.2: e-book downloads (of chapters=papers)

	2008	2009	2010	2011	2013	2013
CICM 2008	1336	1528	1374	598	616	2277
CICM 2009		1398	1183	596	370	2294
CICM 2010			1135	755	370	1563
CICM 2011				440	621	1693
CICM 2012					802	3686
CICM 2013						6748

7.4 Programme Chair

Report on accptance rates etc.: see Figure 7.4. Springer were generally helpful.

Reported on e-book downloads from CICM 2008 onwards (2008 supplied by SA).

He was asked a question about “conditional acceptance”. JHD noted that the “shepherding” process had worked in the past, occasionally leading to rejection. MK noted that a named shepherd (rather than straight ‘conditional’) was essential.

JU noted that the “invited speakers” process was not very formal, but had worked. Also, the “best paper” process was rather late. SMW said that the announcement from Maplesoft was somewhat late. In response to a show of hands, the feeling of the meeting was in favour of having “Best Paper” awards.

PS noted that `electionbuddy.com` had worked well for DML.

7.5 Local Organisers

PQ reported on 81 registrants, We had four workshops plus the doctoral programme, which also funded five students.

He felt that ”Base+day” was confusing, having seen that now from both sides. He had had to send 20 chasing e-mails.

Finance had proved tricky, with some expected sources not coming up. But Research Centres had stepped in — thanks. He expected to break even. He had set fees based on three tiers: doctoral programme (free), students and general.

Thanks wer due to Serge Autexier forthe website.

7.6 CICM 2016

Two bids were proposed, both aiming at July 2016.

7.6.1 Białystok

Białystok is in the centre of Europe. The university was founded in 1997. Białystok is the birthplace of Esperanto! Historical monuments and decent hotels at reasonable events. Social events could be in Białowieza or the Mazury Lake District. Venue would be the new (but now finished!) CS Building.

Białystok is 200km from Warsaw, with direct buses from Warsaw airport.

7.6.2 Innsbruck

Innsbuck is also in the centre of Europe (!): 2 hours by train from Munich[1]. Small airport in Innsbruck itself. Old city centre and University building (Gröbner bases!), but CS has a new building. Winter Olympic venues. The university has 27,500 students.

7.6.3 Discussion

The SC favoured Białystok, who had already bid two years ago, but would encourage Innsbruck to bid again. The meeting was in favour.

7.7 Steering Committee

We would like to organise and simplify the CICM self-governance structure.

Mailing lists currently one per track — should probably have one unified one. This would be done immediately.

Current structure Every track with trustees, a steering committee, of delegates per track and *ex officio* members (Treasurer, PR, Secretary). It was noted that no track had actually done trustee elections this year.

Proposed new structure Member communities to phase out their trusee organisation. Track delegates to be elected by popular vote of track members[2]. Track chairs to be selected by SC based on community nomination to delegates.

Proposal 4 *The SC to work up a formal proposal on these lines, to be discussed in the business meeting of 2015. Since this was in North America, there should be an indicative electronic vote of the whole membership (e.g. via `electionbuddy.com`) prior to the 2015 meeting.* **Carried unanimously**

[1] Zürich is also relatively close.

[2] MK wanted to keep the definition informal. JHD suggested that we should issue some guidance

7.8 S&P track

The systems side of this was very successful, with strong refereeing by eager young referees. MK claimed that the Projects side of this suffered by comparison, and many papers were rejected on the grounds that they were “not systems”.[3]

Q How does “Projects” fit with “Work-in-Progress”

A MK: I think I can see a difference.

SMW I am worried about the acceptance rates. This can’t just be “publishing my grant proposal”.

JHD The CfP and refereeing instructions need to be clear, and consistent with each other, in time for the first CfP for CICM 2015.

JU [Publications in] These proceedings have no value in Poland or the Czech Republic any more [for academic evaluation purposes]. We should maybe think about a journal spun out of CICM.

SMW If they are formally in a separate track, we should maybe not place the projects in the archival proceedings.

JHD Agreed, especially since the “informal” proceedings have become more substantial, currentlythrough CEUR-WS.

Many expressed varied views.

JHD/SMW It is quite difficult to get EasyChair to give different instructions to referees in one track, so running two EasyChair tracks (even if it was publically one track) might make the Track Chair’s life easier and improve the focus of the refereeing.

There was a proposal from the SC to split the track formally, but the vote was tied 12–12. JHD therefore proposed

> In the light of the views expressed, the 2015 Programme Chair and S&P should work together to ensure that the S&P track applied appropriate refereeing criteria, and that the criteria were clear at the Call-for-Papers stage. This *might* mean the use of two EasyChair tracks internally.

This was approved with no objections.

[3]However, a post-meeting analysis revealed the following.

	2013	2014
All	75%	64%
All Systems	70%	67%
All Projects	83%	60%
Unconflicted Systems	50%	63%
Unconflicted Projects	100%*	60%

$*n = 1$.

Having seen this, MK withdrew his claim.

7.9 Any Other business

Rename the conference as "Conference on Intelligent Computer Mathematics" (i.e. drop the final 's' on Conferences) — carried.

Chapter 8

Automated Deduction in Geometry 2014

8.1 JHD

8.2 Streinu: Star Unfolding Polygons

Question 2 (Standard) *Cut the surface of a convex polyhedron P along a tree T and immerse the resulting bounded and connected surface in the plane.*

Question 3 (Star Unfolding) *Cut along the shortest paths and unfold.*

Mathematica demo.

Take a planar polygon with $2n$ vertices, alternatively labelled s and v vertices. Sum of all s-angles is 2π. Note we do not require convexity (but all examples in the literature are)

Question 4 *Do all such polygons arise from cutting a convex polyhedron along a shortest-path tree?*

In fact the answer is negative. We need the v-vertices to be placed on perpendicular bisectors of s-vertices.

Definition 6 *A (ridge point) is one with multiple distinct paths to the source. The ridge points form a* ridge tree*.*

When unfolded, there is a (defined, but I missed this) relation to a Voronoi diagram.

Question 5 *Do all flap polygons arise from cutting a convex polyhedron along*

In fact the answer is negative

Theorem 2 *A flap polygon arises from a shortest path unfolding iff the v-vertices lie on the actual Voronoi edges (not on other bisectors, or on extensions of the edges).*

This leads to algorithms for verification.

8.3 Current Status of I2GATP common format

An XML-format for Conjectures in geometry. DGSs and GATPs and repositories of geometric constructions. We would like to see a looser coupling of tools, and wider availability of their corpora. In 2010 we had the Intergeo (I2g) for format

+ supports constructions

− doesn't support conjectures, proofs etc.

Hence I2GATP, an extension of I2G. There are four XSD files:

`information.xsd` S is the TGTP database. Name, description, references bibrefs etc.

`intergeo.xsd` This is the I2G file.

`conjecture.xsd` This is the "work in progress" This is a GCLC Area method format file.

`proofinfo.xsd` Mirrors the TGTP information.

The container is a ZIP file (as the Intergeo container).

8.4 Automated Natural Language Geometry Theorem Proving using QE

Came from Todai[1] Robotics project: can a robot pass the University of Tokyo Entrance Exam? This is an NII Grand Challenge 2011-21. The exam is a two-stage exam, the first being multiple choice. Subgoal is a high score on this part by 2016. Use

Collins CAD Can do $n \leq 5$

Virtual Substitution Can do ≤ 10 where applicable (linear)

Sturm-Habicht sequences for sign-definite conditions: can do $d \leq 8$.

[1] Acronym, in Japanese, for Tokyo University!

Table 8.1: Formulating Example 1

Parameter	Human	Robot
variables	5	19
Quantifiers	2	16
Atomic formulae	2	24

Example 1 (Hokkaido entrance 2011) *Let* l *be a line created by* $\forall t(t+2, t+2, t)$ *in the* xyz *space. Let* S *be the sphere centred at* $C(a, b, c,)$ *and* $O(0, 0, 0)$, $A(2, 1, 0)$ *and* $B(1, 2, 0)$ *be three points on* S*. Find the conditions on* a, b, c *when* S *and the line have common points.*

There are two approaches

Template-based

Compositional approach to natural language semantics. Appropriate for CA/QE

There are two problem types: “compute/solve” and “prove”. For grammar, we use Combinatory categorical Grammar [Steedman2001], and Japanese CCG) [Bekki2010]. For Discourse Representation Structure [KampReyle1993]. For the example, we get five existential, one over S (i.e. (a, b, c)). Consider Table 8.1

Decompose problem into separately soluble parts, using VS and S–H. Complicated algorithm based on a suitable size heuristic.

Our database of exam papers (half of all, rest kept for testing) is 47% RCF (rest probability theory or combinatorics). Manually-constructed FOFs solve 40, semi-automatic 23

8.5 Kovács: The portfolio prover in Geogebra 5

Claims that ADG software is mature enough to use in the classroom. Want

- Easy to use
- support for “rewording” a problem
- multilingual
- multiplatform
- fast.

Also

- support discovery/verification
- support proving (ATP)

- support traditional classroom values, e.g. not revealing the solution too early; distinguish conjecture from proof; KISS.

Activities

- Per theory framework
- Experiments
- Controlled discovery with questions
- uncontrolled discovery (automated)
- verifications
- collecting relationships
- obtaining readable reports
- Confirmation

Want to add the R-prover.

Q What is the state of the prover-choosing heuristics?

A Not clear to JHD.

8.6 Janičuć: Solving Geometric Construction Problems Supported by Theorem Proving

Goal: construct a geometry figure that meets certain constraints. Focus on ruler/compass triangle constructions. No previous approach addresses correctness proofs. Each phase (except construction) is abut theorem proving of the form

$$\forall X(\Phi(X) \Leftrightarrow \exists Y \Psi(X,Y)).$$

8.7 Detecting dependencies in geometric constraint systems

Typically, when a dependent constraint is entered, the "whole system goes yellow". How do we explain **what** is wrong.

Has a concept of a redundant constraint being "in special position", but SolidWorks is unreliable in this case. Quotes various papers on the combinatorics of rigidity theory. Constraints can be Coincidence, Angle or Distance (which she abbreviated to "cad" — somewhat confusing). The special positions are when the determinant of a "pure condition" matrix vanishes. There are both generic dependencies and these special position ones. $O(nm)$ algorithm for the first, $O(n^3)$ for the second.

Q

A

Chapter 9

Teaching Tiles

Showed a decorative tile(18th century), with the Magdeburg hemispheres experiment.

Then showed a tile showing a geometric figure "Fig 46, P. 29"[1] with a geometric construction. Article in Expresso, 6/11/1983 "O mistério dos azulejos didácticos". The traditional view is that 16th century was a "golden age", then expulsion of Jesuits and a dark age followed by major educational reforms ("Pombal" (?) reforms). Also mentioned tiles in private collections, some more astronomical rather than plane geometric.

Modern views are more complicated.

Cristóvâo Vlávio (1538–16??) published a 16-book explanation of Euclid,using an Axiom that parallel lines are equidistant.

We have 20 tiles (20 × 20 cm) reproducing diagrams from Elementa geometricas of A Tacquet (161–) First edition 1654. All tiles state figure and proposition, but again not book number. Some figures are definitions, some important results, and some just comments of the editor[2].

Diagram of what was almost a catalogue of tiles: two diagrams for book 1, also book 5. Also two tables for Archimedean figures.

Some tiles came from Bishop's palace, and the Bishop was also rector of the University. There was a decree that every philosopher should have available the first 6 books, and Tacquet's version was recommended. A report (1836) on Bahia (Brazil) said "not many years ago it could still be seen in the refectory of the [Jesuit] college of this city that the tiles adorning the walls contained mathematical propositions and proof so that their students, seeing them, would master them, . . . "

Also showed a hydrostatics tile, but the source isn't known. One of a comet, probably 1662 Halley's.

[1] Clearly Proposition 29 of Book 1, but why no book number.

[2] e.g. "How to trisect a right angle".

9.0.1 Exhibition: Meeting of China and Portugal

Note that the science was mostly jesuitical. We have one copy of the book with all the diagrams missing — probably went to the tile-maker.

When Pombal restored the buildings, he destroyed all Jesuit symbols.

Chapter 10

Dumas: Certified Proofs of programs involving exceptions

Example 2 *Gaussian elimination modulo a composite number, with dynamic evaluation.*

One of the tricky points is to preserve the work already done, when we split. Easy way, programming-wise, is to throw an exception when inverting, catch it in Gaussian elimination and then catch outside the inner loop.

How do we handle exceptions in the syntax, either explicitly ($\to$ *Type* $\oplus$ *Exception*) or implicit. We write (in type declarations for functions) $^{(0)}$)/1/2 (or use colours) to distinguish pure/raises exceptions/catches & raises (or at least propagates) exceptions. Also need to distinguish strong equations (identical including exceptions) from weak (if neither side raises an exception, then result is the same). Operations `tag` and `untag` (for moving to/from exceptions). Inside $f : X \to Y$, `throw` (JHD thinks notionally) returns a Y, but also throws the exception (`tag`ged). `catch` is more complicated.

Theorem 3 *This is sound: five statements, such as commutativity of different* `catch`*es*

This system is Hilbert–Post complete: consistent and no consistent pure (exception-free) exceptions.

Formalization in Coq of the exception effect. Roughly doubles the size of the proof (4 pages of LNCS-style maths, 8 of Coq).

Tried 2×2 rank programme. IMP imperative program syntax 49 source LOC, 14 variables, 1 exception (fairly simple), but 1215 tactics and 2GB and 9 minutes in Coq.

Q–RR With Marc MM with LexTriangular we did something similar, but returning a split. This does not go outside the type system

A

10.1 Secundo: formalizing a Named Explicit Substitution Calculus on Coq

Towards a formalisation of PSN for λex-calculus. An Explicit Substitution (ES) Calculus extends λ-calculus by extending the grammar to internalise the substitution operator. Note the choice of names (but α-equivalence), or de Bruijn indices (unreadable by humans). Have a mixed approach: bound variables via de Bruijn, but free by name: known as *locally nameless*.

λex-calculus has four rules. Needed to create a specialized induction principle over bodies of λ-terms. To prove PSN, we need to prove many-step reduction (several pages of Coq). Need to prove it's deterministic. We can simulate one step of the β-reduction, and have perpetuality (subject to a hypothesis).

10.2

10.3

Chapter 11

Silve: What can International comparisons say about the Importance and Limitations of Using Computers to Teach Mathematics in Secondary Schools?

What do other countries do: doesn't automatically translate, but is informative. There is a lot of propaganda as well: "easy" is common. Logo is the most famous teaching language. There is no consensus about teaching programming in schools. Remember turtles? Portugal has a lot of interactive whiteboards in schools, mostly purely decorative!

Malaysia 10M children to use Google Apps

Australia no more laptops in schools

Portugal 100 schools with one laptop/pupil — sold/trained by vendors.This will fail.

Minister All calculators are bad in the first six years of school, but his statements are contradictory

Finland This year new exam allowing symbolic calculators in examinations. Need to wait and see.

French Minister (Chemist, 1999) "mathematics is in devaluation: there are calculators to do calculations, and soon to draw curves".

BBC "do doctors understand test results".

What are the principles to follow? Are we (becoming) ICT salesman? To transform an artefact into a useful instrument, we need a human (with appropriate culture) to operate it.

There is opposition to PISA, but I see this as giving us data, which we should be using. It's a very careful (albeit not perfect) experiment, and the data are available. I'll quote three studies.

1. Digital Reading [OEC11, based on PISA 2009]. Korea clearly top, but NZ and Australia came second and third. Digital and classical reading are closely correlated, but not perfectly. In these three, also Ireland, Sweden, Iceland and Macao, the students are digitally better. There is powerful evidence that "digital natives" do not know how to operate effectively in the digital environment. Using a computer at home is related to digital reading performance in all 17 countries. That is not always true for computers at school. Moderate users score better than both extremes! More intensive use of computers at schools is correlated with native scores, but at home positively correlated.

2. "Are the new millennium learners making the grade" [OECD 2010]. "With the right skills and background.more frequent computer use can lead to better performance". "Teacher training,both initial and in-service, is crucial ...".

3. PISA 2012 used computers as part of the assessment, and PISA 2015 will do more. "Competencies relating mathematics and ICT" (e.g. Piechart with wizard). "There is a high degree of consistency in student performance on items delivered on paper and by computer", **but** Shanghai scored 50 points higher (massive) on paper that with calculator.

Singapore Primary "Advances i technology have changed the way we teach and learn mathematics"

1. Achieve a better balance between computation skills and problem-solving skills
2. Widen the repertoire of T&L approaches to include investigations
3. Help students with learning difficulties

USA Common Core Note this is bottom-up, not federally-pushed. "5: Use appropriate tools strategically" (examples quoted range from protractor to CAS).

S. Korea "If cultivation of calculation ability is not the objective, use calculators ...". Samsung is proposing tablets, controlled by the teacher. "This allows learning outside the classroom".

ICMI Study 17, 2010 "Making technology legitimate and mathematically useful requires modes of integration ..., requires ways of thinking that are not the same as pencil and paper ..." "The slow progress is due to [various sound reasons]". "Implementation of mathematics afforded by digital technologies is more likely to occur when and where there is a shared vision among political leaders, ... [a square in all]".

Personal Final year exam has graphing calculators, and one question which *needs*them. On a Casio, the default graphing window did not catch the graph.

Final questions:

1. What about numerical methods? Should bisection be taught in elementary schools?

2. When should we introduce CAS?

3. When should we teach programming/coding? Is not an algorithm a mathematical structure?

Note that PISA shows clearly that technology is beneficial. Conway 1997: "We have to embrace technology. I don't mean just tolerate it; embrace it an d celebrate it. dots I see mathematics departments rethinking their entire curricula. Otherwise we are out of business.."

Chapter 12

12.1

12.2

12.3

12.4

12.5

12.6

12.7

12.8

Bibliography

[BCD+14] R.J. Bradford, C. Chen, J.H. Davenport, M. England, M. Moreno Maza, and D.J. Wilson. Truth Table Invariant Cylindrical Algebraic Decomposition by Regular Chains. In *Proceedings CASC 2014*, pages 44–58, 2014.

[BDJ+01] B. Buchberger, C. Dupré, T. Jebelean, F. Kriftner, K. Nakagawa, D. Vasaru, and W. Windsteiger. The TH∃OREM∀ Project: A Progress Report. In M. Kerber and M. Kohlhase, editors, *Proceedings Calculemus 2000*, pages 98–113, 2001.

[Dav00] J.H. Davenport. On Writing OpenMath Content Dictionaries. *ACM SIGSAM Bulletin 2*, 34:12–15, 2000.

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

[HKR11] F. Horozal, M. Kohlhase, and F. Rabe. Extending OpenMath with Sequences. *Intelligent Computer Mathematics Work-in-Progress Proceedings (Ed. by A. Asperti et al.) Vol. UBLCS-2011-04. Technical Reports of University of Bologna. University of Bologna*, pages 58–72, 2011.

[Koh14] Michael Kohlhase. Openmath language extensions. In Matthew England, James H. Davenport, Andrea Kohlhase, Michael Kohlhase, Paul Libbrecht, Walther Neuper, Pedro Quaresma, Alan Sexton, Petr Sojka, Josef Urban, and Stephen Watt, editors, *Joint Proceedings of the MathUI, OpenMath and ThEdu Workshops and Work in Progress track at CICM (CICM-WS-WiP)*, number 1186 in CEUR Workshop Proceedings, Aachen, 2014.

[Lan11] C. Lange. Krextor — An Extensible Framework for Contributing Content Math to the Web of Data. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 304–306, 2011.

[LID+12] C. Lange, P. Ion, A. Dimou, C. Bratsas, L. Corneli, W. Sperber, M. Kohlhase, and I. Antoniou. Reimplementing the Mathematical Subject Classification (MSC) as a Linked Open Dataset. In J. Jeuring *et al.*, editor, *Proceedings CICM 2012*, pages 455–459, 2012.

[Nat14] National Research Council. Developing a 21st Century Global Library for Mathematics Research. *The National Academies Press*, 2014.

[OEC11] OECD. PISA 2009 Results: Students On Line. *Digital Technologies and Performance (Volume VI)*, 2011.