CICM 2011: Conferences on Intelligent Computer Mathematics 2011

(Springer Lecture Notes in Artificial Intelligence 6824
http://www.springerlink.com/content/978-3-642-22672-4/)

(partial) Notes by J.H. Davenport — J.H.Davenport@bath.ac.uk

18–24 July 2011

Contents

Chapter 1

18 July 2011

1.1 Mathematical Proofs Based on Strong Geometric Intuition — Krystyna Kuperberg

Intuition is a way to get the idea of a proof, or to convey the idea of a proof to others.

1.1.1 Brouwer Fixed Point Theorem

Definition 1 *Let $f : X \to X$ be a continuous function. p is a* fixed point *of f if $f(p) = p$. X has the* fixed point property *if every such f has a fixed point.*

Theorem 1 (Brouwer, 1912) *The unit ball*

$$D^n = \{(x_1, \ldots, x_n) : \sum x_i^2 = 1\}$$

has the fixed point property.

Theorem 2 (Brouwer, 1912) *Let $H : \mathbf{R}^2 \to \mathbf{R}^2$ be an orientation-preserving homeomorphism of the plane with no fixed points. Then*

- $\lim_{n\to\infty} d((0,0), h^n(p)) = \infty$
- *h is conjugate to a translation.*

But in fact the second part is not true (see diagram). In fact the counterexample was already known, ... One problem is that thsi paper doesn't actually *define* what is meant by a translation.

Theorem 3 (Cartwright–Littlewood) *Let h be an orientation-preserving homeomorphism, and $X \subset \mathbf{R}^2$ be a compact connected set that does not separate $\mathbf{R}^2$. Then h has a fixed point in X. [CL51] [Ham54] [Bro77]*

Note that [Ham54] is much shorter, and [Bro77] is even shorter: one page including references. This is by use of the (correct part of) Theorem 2.

1.1.2 Covering Spaces

A covering space of a punctured plane is a punctured surface. Exercise: it may have a handle (which is a counter-example to a paper by Lickorish). There is a "maximal unwrapping", the universal covering space. The universal covering space of a punctured plane is (topologically) the plane.

Definition 2 *A set $X \subset \mathbf{R}^n$ is* cellular *if it is the intersection of a nested set of topological n-balls.*

Does a cellular set in $\mathbf{R}^n$ have the fixed point property? Open in $\mathbf{R}^2$, but false in $\mathbf{R}^n : n \leq 3$. [Bursuk1935] has the "double tornado" which is in $\mathbf{R}^3$ [Bing1969]

Definition 3 *Let X be a topological space, and $\phi : \mathbf{R} \times X \to X$ be a continuous function. h is a* dynamical system *if the following hold.*

- $\forall x \in X \ F(0, x) = x$.
- *For $s, t \in \mathbf{R}$ and $x \in X$, $\phi(s, \phi(t, x)) = \phi(s + t, x)$.*

1.1.3 Scottish [Café] Book problem 110

Let $f : \mathbf{R}^3 \to \mathbf{R}^3$ be continuous. Suppose that the orbit $\{f^n([])\}_n^\infty$ is bounded by 1. Must f have a fixed point.

Theorem 4 *There is a dynamical system on $\mathbf{R}^3$ with every trajectory of diameter less than 1 and no singular trajectories (no fixed points). [KuperbergReed1981]*

1.1.4 Discussion

Many useful points were made, which JHD was unable to take down as he was chairing

AT Rota suggested that a theorem which survives five years "really is" a theorem, so the Lickorish case is a counter-example to this meta-theorem!

KK Many people were citing [Lickorish19??], for years after it had been disproved.

***** JHD notes privately that the LMS JCM model supports this sort of "refutation management"

1.2 Workflows for the Management of Change in Science, Technology, Engineering and Mathematics — Autexier [ADD+11]

There is much formal mathematics online, but also Wikipedia etc. See also Polymath, PlanetMath etc. There are many links between these items — au-

thors are not aware of each other and of dependencies. We present two systems in (M)KM.

Planetary A "Web 3.0" system, with a Wiki front-end with user comments, discussions, contextual menus etc. Behind it there is an active document paradigm, with backgrounds OMDoc ontologies. The presentation is XHTML+MathML, entirely generated from the OMDoc. Editing is done in sTEX. We also use Miller's LATEXML.

The semantic markup lets us declare concepts, refer to them, delimit theorems, assertions etc. We can use this to do impact support in workflows.

- C1 Estimate total costs of changing a definition.
- C2 Changing a definition should trigger impact analysis — list of potentially-affected knowledge, cross-links with presentation documents, etc.
- C3 notification to other authors of affected knowledge

DocTIP Broker system. This maintains collections of documents. It mediates between connected systems.

One underlying idea is Semantic Document Impact (SDI) Graphs.

Have an OMDoc Document Meta-Model. Syntax, semantics concepts (Symbol, Definition, Theorem etc.) and relations (HasDefinition, HasProof etc.), and properties. A semantic concept may have more than one syntactic presentation.

Abstraction maps syntax to semantics,. Propagation derives properties of the model, and projects maps model properties into annotations to the syntax. Hence the key concept is "Change Aware Reasoning". The syntax changes are computed via sematic XML difference analysis. The reasoning is supported by graph-theoretic concepts.

Note that there's a lot of related activity in software change analysis, which uses code analysis tools, whereas we don't have the same level of semantics. Hence we are dependent on the sTEX markup. So the accuracy of the impact analysis is related to the accuracy of the manual annotation. Probabilistic impact analysis generates false positives and may trigger more impacts.

There is work to be done on scalability, and moving to a multi-user mode, which involves partial merges, and versioned links (see next talk). Also our "eager" impact analysis supports small changes well, but inhibits big changes.

1.3 Versioned Links — Kohlhase2

The MKM we see so far is mostly concerned with static knowledge (after all, mathematics is seldom invalidated, isn't it). Furthermore, mathematics is developed collaboratively (even if not at the paper level, certainly at the theory/community level). The previous talk explained some implementations. Our experience shows that change impacts can cascade into major activities. MK showed his introductory CS course's dependency graph. Renaming a symbol is

the trivial sort of change, but anything more complex is hard to automate, and is probably incompatible with global consistency.

The solution is versioned links.

- Impacted but unchanged objects link to the old version (which maintains consistency)
- we can then change dependent objects at will (which enhances coherence).

Note that citing [AS64] is a classic example of where we need versioned links into the paper literature.

- DLL hell in windows; version conflicts of shared macro packages `\usepackage{foo}[2001/06/13]` loads package `foo` f younger etc.
- Hyperlinks in Wikipedia should use dated links, but don't
- Regressions in theorem provers etc. (Mizar library committee), or HOL-light problems.

Hence our solution is versioned URIs (subject, predicate, object *and* the URI of the document it is referenced is). OMDoc 1.3 supports versioned links, and 1.6 .

There is a SigDOC paper we have written on this.

1.4 A Dynamic Generalised Parser — Kofler

We want to allow efficient incremental addition of new rules without recompiling the whole grammar/ We also need to be more general than LR(1) or LALR(1). Our approach in parallel multiple context-free grammars (PMCFGs). There is a problem of ambiguity (which needs semantic analysis). Note that simplicity is important, which we hope will lead to formal verifiability.

Top-down parsing chokes on left recursion. We use the "initial graph". This is a directed labeled multigraph on $\Gamma = N \cup T$. There is an edge from symbol $s \in \Gamma$ to category $n \in N$ iff there is a rule. Example of an incomplete grammar and corresponding graph. Neighbourhood $\mathcal{N}(s, z)$ is the set of edges from s which ultimately can lead to z.

This scheme has more conflicts than LR etc., but this is OK. We have an arbitrary token source (lexer, token buffer, even a hierarchical parser which returns these trees).

We would like to have customised parse actions. The long-term goal is error-correction (suggestions to the user) rather than just detection.

1.5 Large Formal Wikis: Issues and Solutions — Urban [ABMU11]

A *formal Wiki* is a distributed version control system (DVCS) with added features. We want it to be accessible via standard DVCS operations. The verifi-

cation policy is that the main branch should be correct.

Coqdoc is a fast HTML-izer for Coq, which is capable of symbol-linking and disambiguation. This turns out to be remarkably easy to add to our Mizar-based framework. Coq proofs are typically procedural, and so hard to read. We need proof explanation systems (Provila) and declarative proof mode.

So Coq/CoRN has practically the same tool-chain as Mizar/MML. Note that CoRN uses nested directories (unlike the Wikipedia world). There is also less parallelism in Corn than in MML (which is bad for fast refactoring, unlike MML).

There are issues with SSReflect, which is still a moving target. This also use a different binary from the Coq standard library (how on earth does one handle both in one Wiki?). This is a more anarchistic community than Mizar, and we have to accept this. Hence the Wiki has to support branches, as in a DVCS.

CoRN, despite being relatively small, takes a long time to recompile. Major ITPs only allow file-based dependencies. Hence we need to extract fine=grained dependencies, which is a lot of work (many people are sceptical). CoRN has been done (Lionel Mamame) as Coq kernel extensions. For Mizar (Alama *et al.*) we have a slow but robust micro-article approach, which is in partial use for the Mizar Wiki. This allows section editing (as in Wikipedia).

CoRN has 175K dependencies at the item level, but 2214K at the file level. Mizar 700K versus 21M. Parallel library-scale developments seem necessary. Compiler MML with HTML and intermediate files is 10GB. Hence standard copying is slow and space-inefficient. We need a copy-on-write filesystem (ZFS — stable but not Linux; BTRFS — new but usable). This is usable for both Coq and Mizar.

At the moment we only have anonymous editing, but some operations are resource-intensive, so we need access control. We use Gitolite, which is Git with SSH keys. There can therefore be different verification policies for different clones.

MK How do you handle the fact that Mizar only supports file-based dependencies? Snippets?

A Yes. This also allows minimisation, which is very important for the Presburger tactic, which imports over 200 lemmas automatically.

1.6 Isabelle as a Document-Oriented Proof Assistant — Wenzel [Wen11]

Urban was asking for more document-orientation with theorem-proving: this is a partial answer. The classic Isabelle/Isar view had the following.

+ Routine publishing of Isabelle theory and proof developments for the last 10 years (including these slides and the formal proceedings paper).

– Limited to batch processing.

– Limited formal content in the PDF.

The architecture of Isabelle/Isar is by now fairly standard — how do we make this evolve? There is a cultural gap between front-ends, XML+weakly structured data + Java? versus the back ends, plain text + λ-calculus + ML. His answer is to have a document model in the middle, with APIs connecting it to the front end and to the theorem prover.

There are problems with Unicode (UTF-8 in ML versus UTF-16 with JVM), semantic dilemmas between `03C6` "small Greek letter" versus `03D5` "the Greek ϕ symbol" and `1D711` "mathematical ital small phi". So we use a stable ASCII-based symbol notation , e.g. `\<forall>`. Markup can be

Universal such as the Scala type `Any`

Arbitrary such as an arbitrary Scala type parameter `A`.

often a concrete pair (String,Attribute) as in XML markup elements.

Therefore we have a robust text addressing giving a map of text ranges to markup.

The prover reports document semantic markup for text ranges, and the Scala layer reconstructs document tree structure. Side note — the Java is only twice as long as the ML.

XML has two problems.

- Not really a markup language: text is changed `<>\&`.
- Difficult to implement an efficient parser.

We therefore use YXML, which uses `005` and `006` (known as X and Y) so an open tag `<name>` becomes XYnameYattribute-value ... X, and the end tag XYX.

Lange We can reform old provers, such as Isabelle to support rich document content. Scala/JVM facilitates interaction with the prover/ML world.

\+ Some powerful JVM frameworks (e.g. jEdit) can be used to re-build formal document editor infrastructure.

1.7 Towards formal proof script refactoring — Whiteside [WAGD11]

Refactoring is improving the design of existing code while preserving semantics. The term was coined by Opdyke in 1992, but has been around for much longer in practice. A classic example is the refactoring of Eclipse for Java, but this also illustrates the pitfalls — many bugs.

Example: a script which proved $P \wedge Q \rightarrow Q \wedge P$. Showed three refactorings. Questions:

- What is *semantics preservation*?
- Can we prove reliability?
- What refactorings are available?

First give a semantics to proof scripts:

Definition 4 *prf is a proof of goal g if*

$$\langle p, prf \rangle \Downarrow \langle \mathcal{T}, \mathcal{L} \rangle$$

(where $\mathcal{T}, \mathcal{L}$ seemed to JHD to be the environment).

Note that some refactorings have preconditions. Example: rename o to n. Precondition: $n \notin$ names(proofscript). Then various transformation rules (fairly obvious) but note that the precondition *does* have an essential use. Other refactorings include unfolding tactics, backward to forward proof transformation, extract sub-proof as a lemma in its own right, procedural/declarative transformations.

Harder work ongoing is "generalise definition", where hard work is needed on the use of the definition.

MK Mostly independent of particular proof system/language. How much can be generalised?

1.8 Querying Proofs — Aspinall

Mechanised proof tools produce **big** proofs. What can we do with these? Check/reuse/transform/inspect. We propose *proof queries* to inspect proofs in a uniform way.

- Which axioms are used in the proof?
- Which witnesses are used for existentials
- Which tactic uses this axiom?
- Where does this subgoal come from?
- (for failed proofs) why does this tactic *not* apply?
- What were the goal inputs to tactic t?
- ...
- Is there a subproof which occurs more than once?
- Are there steps which have no effect.

Use the *hiproof* concept (as in last talk) which is an abstraction of a proof (tree), with hierarchy as a primary idea.Ideas such as labelling, sequencing . [MKM2009]

The idea is to generate paths $\mathbf{P}$, filter on these to select ones of interest, and select paths of proof trees using patterns. Start with the comprehension scheme $\{P \in \mathbf{P}(s)|\phi(P)\}$. This allows, e.g. "show all axioms", "show all tactics used recursively" etc.

1.9 planMP: Collecting Mathematical Practices for MKM — A. Kohlhase

We observe that MKM technologies are not as highly used as they should be (but note DLMF has > 1000 visitors/day). The problem seems to be adoption, to which we propose HCI methods. HCI methods are based on "the user", but HCI asks "who is the user"? We can give a very high-level list.

- Professional mathematicians
- Professional users (physicists etc.)
- mathematical educators
- mathematics students.

But in fact we don't really know who the user is/ what the user does in more detail. Hence we create mathematical personas, i.e.

> patterns in user and customer behaviours, attitudes, aptitudes, motivations, environments, tools, challenges. [Cooperetal2007]

A practice is defined as "what people actually do". Showed a photograph of a real blackboard, containing graphs of functions, graphs of object relationships, tables, formulae etc. The replacement has to be much more than an editor? `planMP` is a wiki for collecting mathematical practices. We note that the end-result of mathematics, published papers, is very different from the process of creating them. `http://planMP.kwarc.info`.

BM Libbrecht has a notation wiki [Lib10]. What is the relationship?

A Notation is certainly a practice. However, I would not like to be collecting these here.

PI Notation defines sub-communities.

Urban This seems very unstructured at the moment.

1.10 Interleaving strategies — Jeuring [HJ11]

There are many aspects to learning — we focus on two.

- "Learning by doing" — many exercises.
- "Learning by feedback": tutoring services are often delegated to domain reasoners.

A domain reasoner can generate steps (examples from Dutch high school, in ActiveMath). This will be used by at least 1000 students in Paderborn and Kassel this September. Also OpenUniversiteitNederland has "Exercise Assistant Online": showing "maybe you were trying to apply Dr Morgan, but forgot to ...".

- We use rewrite strategies for exercises
- A strategy describes valid sequences of rules
- View a strategy description as a context-free grammar
- Track intermediate steps by parsing.

Until now, we could not manage interleaving of strategies.

1.10.1 Strategies

Rewrite rules

- specially how terms can be manipulated
- can encode common mistakes ("buggy rules")

Rewrite strategies

- Guide the process of applying rewrite rules
- use a strategy language, similar to tactic languages, CFGs etc.

Views and canonical forms recognise structure etc.

Shows an example of achieving DNF. Naïve strategy; algorithmic strategy and expert strategy (algorithmic plus tautologies and contradictions). We can implement algorithmic, but the students complain that it long-winded and "they can do better".

$$negations := NonNot|DeMorganAnd|DeMorganOr$$

$$basics := constants|definitions|negations|\ldots.$$

$$dnfExhaustive := repeat(somewherebasics).$$

The tutoring services are generated automatically from these strategies, using 'empty' and 'first'. We want these to be observable and composable.

$$additionals := tautologies|contradictions$$

Note that

$$dnfExtra = repeat(dnfExhaustive|additionals)$$

isn't right because dnfExhaustive will already terminate.

1.10.2 Interleaving

Introduce || as an interleaving operator. Note there are $\frac{(m+n)!}{m!n!}$ interleavings of m and n objects. Allow a block construct $\langle \ldots \rangle$ inside which interleaving does not occur. This definition comes from the Algebra of Communicating Processes (ACP).

However, it is hard to use this for introducing tutoring services. 'empty' is easy: 'first' is the problem (given atomic blocks etc.).

There is the requirement to generate the parser. We therefore need an "interleaving parser".

Experiments with thousands of students will happen in September. `http://ideas.cs.uu.nl`. `mailto:J.T.Jeuring@uu.nl`.

1.11 Parsing and Disambiguation of Symbolic Mathematics in the Naproche System [CKS11]

NAtural language PROof CHEcking — a joint Bonn & Duisburg/Essen project. We study the semi-formal language of mathematics as used in journals and textbooks.

For every sentence in the text, the system parses the text, keeping track of context. Note that mathematical symbols are integrated into the ordinary text. Example [HW79, proof $\sqrt{2}$ is irrational]. See [**?**] and [Gan09]. The speaker claims this is inadequate, e.g. $[K : k]$ (as far as JHD recalls the claim is that $[\alpha : \beta]$ is essentially a single 'outfix' operator), $a \circ_G b$, multiplication by concatenation, applying functions to their arguments as in $f(x, y)$ (an amazing omission in [**?**]). Note in particular the ambiguity of $a(x + y)$, depending on whether a is a function-valued symbol. There are other issues, such as 2D-ness, so we parse normalised (always `a^{b}` not `a^b`) LaTeX.

In a proof system such as Naproche, presuppositions have to be checked for correctness. One possible approach for disambiguating symbolic expressions is to check presuppositions during the parsing process, which would mean outcalls to the prover from the parser: dodgy and expensive.

[Gan09] generated a type system which can carry this. However, the author has to write sentences purely to create types, which is unnatural.

In fact, a combined apporach can be used: a relatively simple type system can block most unwanted readings, and outcalls fix the rest.

1.11.1 Our type sytem

.

i individuals

o for formulae expressing propositions.

$[o, o] \to o$ for logical connectives

syntactic types — six of these

Fairly impressive examples, incluiding implicit introduction of function symbols "To each vertex x we associate an edge $g(x)$ such that ...". `http://www.naproche.net`

APS Have you look at type inference, e.g. for $a(x + y)$.

A But we might know nothing about a.

APS Might we use information from later on?

A Only from same sentence.

1.12 CICM Business Meeting

MK, as CICM Secretary, opened the meeting.

1. "We need a scribe" — JHD was volunteered.

2. Trustees' report
   MK, as CICM Chair, noted that CICM had been founded, as an organisation of organisations, at CICM 2010 (Paris). In answer to a question, this does not include workshops unless they become big enough to affiliate to CICM. There is a draft charter at `http://trac.mathweb.org/CICM/wiki/Charter`.

Q IFCOLOG?

A MKM was a member of IFCOLOG, and CICM is a member. They are a registered charity with a bank account, so can (and do) keep our funds.

3. Treasurer's report
   We are finalising the balance transfer from Birmingham for CICM 2008 (£1511.76). 2009 essentially broke even. 2010 (Paris) probably make a surplus of 2000–3000 Euros. The aim is to have a balance of 5000 Euros, for seedcorn and insurance, and the aim is to fund students out of any excess.

4. CICM Programme Chair's report
   JHD reported. He noted that, as well as the EasyChair statistics, he had computed statistics for the individual tracks. It was pointed out that EasyChair has a facility (but this has to be enabled from the start) to make this easier. JHD didn't know about this, but will include it in his summary notes.

   Josef Urban pointed out that the Systems and Projects track had yet really to happen (tomorrow/ Wednesday) and he urged people to attend these sessions. Note that Springer had changed their mind about the length (from 2 to 4 pages) and for the future we should get this right.

5. CICM Venue/Dates/Chair for 2012
   Bremen 2012 has been agreed in Paris. Beautiful campus setting (MKM 2005), 45 minutes train/tram from the Ryanair terminal! Nice and cool in summer, with less rain than you might think.

   Programme Chair is Johann Jeuring. The individual conference will nominate their Track Chairs, and the CICM Committee have ideas for Systems and Projects Chair, which has to be confirmed shortly.

   Dates have to be agreed (many people voiced constraints). Possibly early July.

6. CICM Venue 2013.
   JHD presented the Bath option. The only question was "what about the rain"? JHD noted that having a buffet lunch in the lecture theatre building (which was also Computer Science's new building) would reduce the *exposure* to the rain, though he made no promises about the amount of rain.

   Since ISSAC 2013 is at the end of July, early July seems like the obvious date.

7. AOB: MathUI
   It was noted that MathUI was not taking place this year. PL had proved unable to organise this for 2011 (and offering financial assistance, though possibly late, hadn't solved the problem). MK commented that CICM had been unfortunate with workshops this year, compared with six in Paris in 2010.

   It was noted that there was also no Doctoral Programme in 2011, unlike 2010 and 2008. This had been dependent on external funding. APS noted that getting such funding often took more than a year.

Chapter 2

Systems & Projects 19 July 2011

2.1 Formalisation of Formal Topology in Matita — Sacerdoti Coen

"New foundations should give new mathematics" "Classical logic hides mathematical richness, like a pair of sunglases". "Impredicativity hides the distinction between data types (computer representable) and abstract notions" — slogans of the Padova Logic Group.

The motivations are interesting, and non-standard.

- The mathematicians *are* confident of their results.
- But are they strictly only dependent on this framework?
- Are the notions so elementary to be easily understood by a machine — can we have a de Bruijn factor of 1?

There are several insights obtained

- The main formalised proof is a categorical dense embedding between two categories of generalized topological spaces (Basic Pairs and Basic Topologies) that generalizes the adjunction between topological spaces and locales.
- Calculus of Inductive Constructions (or even Luo's ECC) is not well suited — how do we *state* and prove that an instance of a large category is actually small.
- We have nmeeded the concept of an "overlap algebar"
- This has led to a new logic for Matita

2.2 MathScheme — Farmer [CFO11]

2.2.1 Objectives

- Significantly advance the capabilities of mechanized mathematics schemes;
- Tightly couple symbolic computation and formal deduction;
- Create a powerful, maintainable and widely usable system.

2.2.2 Challenges

- Merge axiomatic and algorithmic reasoning
- Reason about algorithms that manipulate syntax
- Design a scalable library of formalized mathematics
- CA is oriented towards users, and ITP towards developers
- Reflect the mathematical process

In particular, we learn from Maple and IMPS as exemplars. WE want to support multiple reasoning paradigms. We want to *safely* re-use other proejcts' work. We must leverage the structure in mathematical knowledge. Intend to use generative programming.

Key ideas

- Biform theories: concepts + transformers + facts, which represent both axiomatizations and interfaces.
- Chiron logic, which is a derivative of NBG set theory with types, undefined terms and a facility for reasoning directly about syntax.
- MathScheme language: a user-oriented high-level language for expressing biform theories.
- "Tiny theoreies"
- Applied Universal Algebra.

2.3 Project: LATIN – Logic ATlas and INtegrator — Rabe [CHK+11]

2.3.1 Goals

- We want to formalize and interrelate all foundational languages: logics, syntax, proof theory, model theory.
- Little foundations: systematic reuse of theorems across logics and semantic domains: building logics out of little components

2.3.2 Methods

- Proof-theoretical logical frameworks, based oon type theory, specifically LF/Twelf.
- Model-theoretical logical frameworks, based on set/caetgroy theory and specifically institutions.
- MKM-based throughout, specifically XML, OMDoc and MMT

So `and`, which is form→form→form, is combined with `andl`, which is (Proof A)→(Proof B)→(Proof $A \wedge B$).

2.3.3 Current state

700 little theories, propositional, first-order and higher order logic, comon, modal, linear and description logics. Can explicitly state the Curry–Howard correspondence *in* the system.

2.4 C99 in HOL, Isabelle and Coq — Krebbers [KW11]

`LangPop.com` shows C as the top-ranking language (second Java and third C++). But C99 is written in English with no mathematically precise formalism, and is incomplete and ambiguous.

```
in x=30, y=31;
\int *p=&x+1, *q=&y;
if(memcmp(&q,&q,sizeof(p))==0 {
  printf("%d\n",*p)
  }
```

This is actually defect report #260.

We will create a master formalism in Ott, and check in HOL4, Isabelle/HOL and Coq.

- Utterly precise formalisation of the standard
- Validate correctness of formal versions of subsets of C, suuch as Compcent
- Verify compilers

Related work include Norrish (C semantics, but only a subset); Xavier Leroy *et al.* have a verified C compiler (but only Compcent) in Coq; Ellison & Rosu have executable C semantics in Maude. `http:ch2o.cs.ru.nl`

2.5 Mizar items — Alama (by video) [Ala11]

This (presumably Mizar) has support for implicit forms of reasoning. The problem is that it's hard to work out exactly what an item depends on. The MML list of 100 theorems (Rudnicki) was shown. Shows Fermat's Little Theorem, and the 'requires' and 'supports' links, which *include* the implicit dependencies as well as those formally stated in the proof. These essentially build a dependency graph.

At the moment, this only works on MML: we would like to .... See `mizar.cs.ualberta.ca`

2.6 Learning2Reason [KUT+11]

Joint project of Foundations and Machine Learning groups at Nijmegen.

2.6.1 Premise Selection

The first aim is to focus on Premise Selection in ATPs. The more premises we have, the harder it is to find a proof.

- Define features for first-order theorems.
- Use standard machine-learning tools from here.

2.6.2 Strategy Selection

In general, only the developer knows which strategies will be tried, and in which order. Can we do better? First experiments solve 20% more problems from the MPTP problem list.

2.7 EuDML demo — Bouche [BBNS11]

Tells the story of the animal on the road. `demo.eudml.eu` Is the animal on the road named EuDML a virtual library catalogue, a digital library, a toolbox etc.? Project started February 2010, for three years. Various data and content providers (hence metadata compatibility issues): currently 200K items.

There is an annotation component, which allows users to interact with documents.

2.8 A Symbolic Companion for Interactive Geometric Systems — Botana [Bot11]

It is possible to connect dynamic geometry systems (such as GeoGebra) to computer algebra, to do more that GeoGebra on its own. Gives an example (orthecentre) where GeoGebra gets a question right, but as the triangle's vertex

moves towards infinity, result becomes false in GeoGebra. Therefore connects GeoGebra to SAGE, and gets "generically true". Can also compute equations of non-linear objects, which is beyond GeoGebra's native capabilities.

2.9 Algebraic Topology — Heras [?]

The fKenzo system is a friendly interface to the Kenzo system (written in ACL2). Interface for GAP, interoperability between Kenzo and GAP, interface for ACL2. JHD observes that the menu-based system is a great improvement on ACL2 S-expressions. The "expert system" suggests usingthe Hurwitz theorem in the context demonstrated. GAP can then be used to give properties of the groups computed by Kenzo. To compute homology groups, GAP computes the resolution, and Kenzo then does the rest, for example.

As an application. he loaded some digital images and computed homology groups, e.g. number of connected components.

2.10 EgoMath2 as a search for mathematical searching — Mišutka [MG11]

This is built on EgopMath ideas. Major change in an augmentation algorithm with transformation rules and ordering. Augmentation seemed to JHD to be the addition of rules to the search space, such as α-equivalence. We use the `Wikipedia.org` English dump (rather than ArXiV as in EgoMath). We used LaTeX formulae and/or KWARC's latex2mathml, which is good at identifying variables. There are 250K formulae, which are stored in a database, but only after a lot of pre-processing (which turned out to be crucial — many `\,`, `\\`, `\mathbf` etc.)[1].

2.11 KREXTOR — Lange [Lan11]

"Linked Open Data" is a set of best practices for publishing and connecting structured data. This has "light-weight semantics": not good for automatic reasoning, but scales well. This is a "Web of Data" idea. Showed a diagram of the web, with Wikipedia as the hub.

The big question is "what can I reuse"? We currently have the following.

- e-Science data — with opaque mathematical models.
- statistical datasets — without mathematical derivation rules.
- publication databases[2] — without mathematical content.

[1] JHD has a query here. I can see discarding some of these, but Z is very different from $\mathbf{Z}$

[2] DBLP is one example.

Mathematical Knowledge is document-oriented, either textbook style or as in Mizar's articles. Web-of-Data is rather RDF-based. Hence Krextor which is an XML→RDF library. A major focus has been OpenMath CDs → RDF "vocabulary". Would like to interlink with [fST10]. Note that CDs don't currently identify the individual properties, so that `times` is labelled, but not its associativity property.[3]

2.12 The LaTeXML Daemon [GSMK11]

We are at the most informal end of the MKM spectrum. Note the size of corpora: Zbl and arXiv for example. LaTeXML is a "semantics-friendly" converter, achieving 95% of Zbl, and 70% of arXiv. Has HTML5+RDFa support. It is extensible in terms of packages[4].

2.12.1 Daemon extension

- This is efficient (Zbl spend most of its time loading and initialising,s ince documents are short).
- This made it scalable, and then allowed "on-the-fly" conversion. Needs to be flexible for differnt fora.

This is PERL5, with batch and RESTful APIs. It is public domain software.

[3] JHD's example.
[4] JHD presumes LaTeX packages.

Chapter 3

JHD's observations on demos/posters etc.

3.1 Conversation with Bruce Miller (NIST)

[fST10] has been updated to 1.0.2 — about six errata, and the same number of clarifications. JHD asked for a footnote clarifying that the Lambert W function is not elementary in the sense of [BCDJ08]. Note that [fST10] is based on the concept of permalinks, so that all links remain valid.

3.2 Re: The LaTeXML Daemon

ES asked whether the semantics of macros were preserved. Her example was

```
\def\binomial#1#2{\left(\begin{array}{c}#1\\#2\end{array}\right)}
```

BM replied that macros were expanded by default, and that the semantics (if any) were lost. But it is possible to tell the PERL that a certain macro is not to be expanded, and has certain semantics. In detail

```
DefMath('\binomial{}{}',
        '\left(\begin{array}{c}#1\\#2\end{array}\right)',
        meaning=>'binomial', cd=>"combinat1")
```

This could do with being better documented.

A further problem is "known ambiguity": this symbol might mean either this or that. JHD noted that people will tend to use two macros in this case.

3.3 Re Krextor

JHD noted that CL wanted links into components of OpenMath CD definitions, in particular FMPs and/or CMPs. CL replied that he wanted both, or,

even better, links to the pair. He had an (undocumented) proposal to add `<PROPERTY>` which would group CMP and matching FMP. One could have `<PROPERTY name="associative">`, or a child element which gave the name: he could handle either.

He currently uses the heuristic, based on the standard's suggestions, that a CMP and FMP occurring together are conceptually grouped. He currently just indexes them, e.g. "property 1". Real names (which generally exist in mathematics) would be a substantial improvement, as well as being more change-proof.

3.4 EuDML

PS demonstrated the search facility, typing in `$x^2+y^2$`. This is converted into (presentation) MathML, normalised and searched. In fact, the search is done both on the orignal formula $x^2 + y^2$ and the α-normalised form $\mathtt{id}_1^2 + \mathtt{id}_2^2$.

JHD asked about searching for `$\arccot(-1)$`, but arccot is not (currently) known to the search engine (in any form).

3.5 Mizar Items

JHD asked PR a question.

Definition 5 *ψ* depends on *ϕ (in the current Mizar world) if deleting ϕ means that the* current *proof of ψ ceases to be valid.*

Another proof of ψ might be derivable, of course.

3.6 Formal Topology in Matita [AMSC$^+$11]

We introduce a relation $\Vdash$ and look at examples where $x \Vdash P$ ($x \in C$, $P \in F$):

C	$\Vdash$	F
points	$\in$	basic open sets
programs	has	properties
data	has	approximations

$\Diamond P := \{o \exists x : x \Vdash o \wedge x \in P\}$: existential image. $\clubsuit P := \{o : \forall x : x \Vdash o \Rightarrow x \in P\}$ universal image of P. $\mathrm{Rest}\, P := \{x | \forall o x \Vdash o \Rightarrow o \in P\}$ universal counterimage of P, $\mathrm{Ext}\, p := \{x | \exists o x \Vdash o \wedge o \in P\}$ existential counterimage of P.

Then $\mathrm{Int}(P) = \{x | \exists o : x \Vdash o \wedge o \in \clubsuit P\}$, as a definition of 'interior' in terms of these operators. Similarly $\mathrm{cl}(P) := \{x | \forall o : x \Vdash oo \Rightarrow o \in \Diamond P\} = \mathrm{Rest}(\Diamond P)$ for closure. Define $A(P) := \clubsuit(Ext(P))$ and $J(P) := \Diamond(\mathrm{Rest}(P))$.

CSC observed that cl and A are saturation points on sets of points/opens, and Int and J are reduction operators.

Note that functions are not the rght concept here, since they are asymmetric in domain/codomain. We therefore use relations (JHD: couldn't you use bijections, going the other way? CSC: yes, but it doesn't work as well).

Basic topologies arise from dropping the points, and talking purely about the opens, and A and J. To formalize this, we need an operator which is logically dual to set inclusion.

$$A \subseteq B := \forall x : x \in A \Rightarrow x \in B.$$

So define

$$A \between B := \exists x : x \in A \wedge x \in B.$$

Classically, $A \between B \Leftrightarrow A \cap B \neq \emptyset$, but intuitionistically $\neg\forall\neg$ is weaker than $\exists$. Then an overlap algebra [Sambin] is a structure $(S, \subseteq, \between, \sqcap, \sqcup, \bot, \mathrm{T})$.

Chapter 4

19 July 2011

4.1 A Foundational View on Integration Problems — Rabe [KRSC11]

Computer algebar systems, deduction systems, MKM systems are becoming more powerful: how do we get them to owrk together. Consider system 1 communicating with system 2. A pragmatist would say "just send it, and hope for the best". The fundamentalist would want everything proved first, but we have to hope there's time left to get anything to run. We can split this into *a priori* (ytranslation of a library) versus "on demand". HOL in Nuprl [SchurmannStelh2004] is an example of *a priori*. The other question is "when is the integration verified". Dynamically (our work) or statically.

Our work is based on MMT and LF/Twelf. Ideally we have a communtig diagram with translations I and O. Suppose S_i defines natural numbers $\mathbf{N}_i$. It may be the case that $O(\mathbf{N}_1) \neq \mathbf{N}_2$. We might choose to do no correspondence (then $\mathbf{N}_2$ isn't used), prove isomorphisms individually that $O(\mathbf{N}_1) \equiv \mathbf{N}_2$, assume that $O(\mathbf{N}_1) = \mathbf{N}_2$ (which isn't true, so all we get are proof sketches, or filtering (our appraoch). Given a specification *Spec*, we have theopry morphisms μ_i which prove that S_i implements *Spec*, and partial theory morphisms η_i which invert μ_1.

Note that the MIzar library assumes the Tarski axiom right at the start, so niïve filtering with respect to a system without Tarski will essentially destry the Mizar library.

proof goal	proof
expression	simplified/decomposed expressions

4.2 Enumeration of AG-Groupoids — Sorge [DSS11]

Classification is a generla part of algebar research. Enumeration results are an important step towards classification. The less structure the obecjts have, the harder it is to enumerate! There has been previous work with Quasigroups and Semigroups.

Abel–Grassman groupoids: Algebraic structures closed under $\circ$ with

$$(a \circ b) \circ c = (c \circ b) \circ a \tag{4.1}$$

(note that these are not associative).

In general, from Groupoids (a.k.a. Magmas), we can go semi-groups, monoids, groups, or Quasigroups (Latin square property), Loops and then groups. AG-groupoids live between semigroups and quasigroups.

They have applications in the theory of flocks (physics and biology), geometry (as parallelogram spaces). AG-groupoids capture subtraction and division (with $x \circ y = y/x$ or $y - x$).

Quasigroups are enumerated up to order 11, IP-loops up to order 13, semigroups up to order 9 [KelseyDistler], and monoids up to order 10. These depend on symmetry breaking (either via Latin squares or associativity), which isn't available to us immediately.

We use the constraint solver Minion together with GAP to do the symmetry breaking, and can enumerate all AG-groupoids of order 6, and this gives us the Cayley tables. With the `loops` package of GAP, we can identify further sub-classes of Cayley tables.

For $|G| = n$, we have an n^2 Cayley table, and (4.1) is a constraint on these. But unfeasible without symmetry breaking. Use lex-leading as the symmetry-breaker[1]. For $n = 5$ drop from 3.7M to 31913, and greatly in time. 325 are associative and commutative, 121 are associative and non-commutative and the rest (31467) are neither (commutative and non-associative is impossible). Semigroups were checked with GAP, and $n = 5$ by one of the reviewers[2].

In $n = 6$ can get associative non-commutative AG-groupoids with are not AG*-groupoids (contradicting a previous paper).

An AG-band has $a \circ a = a$, and an AG-3-band has $(a \circ a) \circ a = a$. Again at $n = 6$ there are AG-3-bands which are not AG-bands.

Q. How do you know there's no hardware error?

A. Good faith in our constraint problem code: though the GAP code is more subtle and did have an error.

***** Note that the existence of counter-examples is independent of this question.

[1] This symmetry-breaking is complete, in the sense that no two produced are isomorphic. UNtil now, it was not known if it was practicable. I private commnication from Distler says that $n = 7$ has been done, but this seems the limit of this, or any known, method.

[2] Who used MAZE-4, and also pointed out an error in the classification, which was traced to an error in the GAP code.

4.3 MKM Business Meeting

SA, as MKM Secretary, opened the meeting.

1. "We need a scribe" — JHD was volunteered.

2. Track Chair's report
   This was the first time MKM had been a CICM track, rather than a separate conference. We used EasyChair multitrack, which worked, and solved conflict issues well. We had a 1-week reburttal period, but would recommend that next year we don't send the scores. We collected the PC discussions into summary reviews, which was successfull. We used shepherding for three papers, two of which were eventually accepted.

   The major issue was the low number of submissions (22), and acceptances (9, with 8 further work-in-progess papers). The trustees should reflect on this.

   The MKM best paper award was presented to Whiteside *et al.*: Towards Formal Proof Script Refactoring.

3. MKM in CICM
   The MKM Trustess have unanimously approved the CICM Constitution. This states that the constituent organisations (e.g. MKM) are represented by a delegate[3]. We propose to add to the MKM Charter

   > The MKM trustees appoint a standing delegate to the CICM Steering Committee. This delegate is **mandated** to vote on items that require a unanimity of CICM Steering Committee only in a sense that has the approval of an absolute majority of the MKM Trustees.

   The meeting approved this amendment (23-1 with 2 abstentions).

4. CICM 2012
   This will be in Bremen, with overall Programme Chair John Jeuring. The Trustees have selected Makarius Wenzel as MKM Track Chair.

5. CICM Venue 2013.
   JHD had presented the Bath option at the CICM Business Meeting, but other suggestions (to the CICM Steering Committee) were welcome.

   Since ISSAC 2013 is at the end of July, early July seems like the obvious date.

6. Trustees
   Claudio Sacerdoti Coen would be replaced by Makarius Wenzel. A trustee should be elected to replace Petr Sojka. Lionel Mamame had already

[3]Currently WMF, but he is also CICM Treasurer, so the MKM Trustees will nominate another delegate once the MKM Trustee election for 2011 is over.

agreed to run the election for trustee. Nominations were Bruce Miller (APS/JHD).

Nominations would close at the end of this conference, with manifestos circulated by August 20 to LM, and election in September 2011.

7. Any Other Business
   Manfred Kerber commented that the reduction in papers had already been mentioned. SA stated that they would try to get the announcement and call for papers out as soon as possible. BM commented that refereeing was a subjective art. This led to some discussion.

   It was noted that everyone's job, not just PC members, to encourage submissions. MK noted that PI had commented that, some years ago, we had a wishlist of things that "should be done". The systems and projects track today had answered many of these items.

Chapter 5

20 July 2011

5.1 — Hales

Want to emphasise some of the "pre-formal" aspects of the project .

Conjecture 1 (Kepler) *The densest packing on congruent balls in* $\mathbf{R}^3$ *is achieved by the 'cannonball' packing.* Formulated in 1611 in a book presented to his patron. The motivation was a study of the snowflake (six-fold symmetry) and the honeycomb, which is rhombic dodecahedra, which tile space, and a cannonball in each cell gives the packing.

Proved 1998, but not published until 2006 ("We will publish your paper when you have convinced us it is correct!"), hence the interest in formalising the proof. WE estimated Flyspeck at 20 person-years, and is probably 75–80% complete.

- The text part of the proof is an unpublished 300-page manuscript. This is being done by a team of researchers. Today's talk.
- First computer program (graph theory) is now done, with Nipkow.
- Linear Programming — see Friday.
- Verification of non-linear inequalities

  A big surprise for me has been how much effort is needed before any formalisation takes place.

5.1.1 Preformalisation

This is essentially Bourbakization.

Conjecture 2 (Variant on Fejes Tóth 1953) *Let 14 nonoverlapping balls of diameter 1 be given with centres* P_i*:* $0 \leq i \leq 13$*. Let* $a = 7/\sqrt{27} \approx 1.347$*. Is* $\sum_{i=1}^{13} P_0P_1 \geq 12 + a \approx 13.347$*?*

Theorem 5 (L12; New=June 2011) *Essentially this with 13.26*

Theorem 6 (Kepler) *There's a new proof (Theorem 9), different from 1998*

Theorem 7 (Fejes Tóth's full contact conjecture (1969)) *In 3-space a packing of equal balls such that each enclosed ball is touched by 12 others consists of hexagonal layers.*

Note that the corresponding theorem in the plane is trivial/

Theorem 8 (K' Bezdek's strong dodecahedral conjecture) *In very packing of congruent balls in* $\mathbf{R}^3$*, the surface area of every Voronoi cell is at least that of the circumscribing regular dodecahedron.*

This implies the weak dodecahedron conjecture, proved in 1998 and published last year.

Theorem 9 (New) *L12 implies all the other.*

5.1.2 Graph Generation

[BauerNipkow] classified the planar graphs (c. 3000) that arise in the original proof. The new proof has 25,000[1], and this has now been done (August 2010). This found a bug in literally 1 of the 25,000 graphs produced by TH's initial code. This Isabelle proof still links to be linked to HOL Light.

5.1.3 Linear Programming

S. Obua did the "basic cases", which covers 92% of the graphs, but only about 3% of the linear programs. The linear programs were never written up for publication, and consist essentially of 3GB of raw data.

5.1.4 Remaining Code

This is testing of (about 500) nonlinear inequalities, done with a gradient descent program, developed at University of Maryland. The basic method is explicit Taylor approximations There's 7K of C++ code and 7K of test code. The main control structures (about half the 7K) have been ported into 1K of OCAML (with HOL backquoting!).

The inequalities were generated (heuristically) in Mathematica, to analyse what inequalities *might* be used to make the linear programming work, and were tested (non-rigorously) by the Maryland code. They are then converted into C++, which goes into rigorous interval arithmetic verification. This still needs to be formalised.

[1] "This was the part that was easy to formalise, so I've moved more effort into this."

Uses John Harrison's symbolic differentiation code in HOL[2], transformation in HOL of the inequality. For a single inequality (taking 2 second) needed to subdivide into 7481 sub-cells on each of which Taylor could prove the result.

Uses Harrison's `REAL_RING` For example gives a one-line proof of isogeny between elliptic curves. Needs this as elliptic curves are the Riemann surfaces he needs for simplifying radical expressions.

The original C++ code took three months to run, which is now done to 10 hours. Moving this into a formal proof system is therfore now conceivable (not trivial!).

5.1.5 Proof strategy revisited

The new strategy was adopted in 2009 (based on a paper by C. Marchal). The 300-page text has been formalised apart from the last 500 lines (and all the integration). There are 14,00 theorems in HOL Light, 30% of which are from Flyspeck.

Why these 500 lines?

- 50 lines integrate fans and polyhedra. This requires combining the work of John Harrison (polyhedra) and Vietnamese work on fans.
- 200 lines — properties of packings in $\mathbf{R}^3$ — delayed by `CHEAT_TAC` utilisation (now disabled!).
- 200 line son local fans — the informal proof wasn't completed until June 2011.
- 50 lines — student went to a PhD programme in Germany.

The text part is a TEX book which tracks (semi-manually?) the

Example: perimeter estimate for convex spherical polygons ($\leq 2\pi$). "Obvious" by deformation, but hard to formalise. In fact, he uses dual polygons, and the statement is that the area of the dual polygon is ≥ 0! The cost is that of introducing the whole duality concept, but the proof is ultimately more formalisable.

Another example is the Euler theorem for planar graphs and/or polyhedra. Which proof should we pick? I don't have homology or homotopy, but I do have measure theory. Therefore uses a proof based on the approximate equivalence of the Euler formula and the fact that 4π is the sum of the areas of the triangles in the triangularisation of the sphere.

Note that there are many such "design" decisions which need to be made. The proof of Fermat's Last Theorem has many such as well.

MK What are your thoughts on educating the next generation of mathematicians.

[2]The difference from standard computer algebra is that this keeps track of the assumptions under which the derivative is valid.

A I tried to organise a bunch of mathematicians to look at Fermat's Last Theorem, but they would all rather be looking at new theorems!

APS Has this changed your sense of aesthetics in mathematics?

A Yes, but it's hard to articulate. It has increased my appreciation of computation.

JJ When was the original paper published?

A 2006 (but the editors were never convinced!).

JJ As a computer scientist, "pre-formal" corresponds to the early (pre-formal) stages of design.

A Possibly, and maybe there are tools we could use.

Q Would you still use HOL Light?

A I liked the small kernel. I could prove my first theorem more easily. Strong support for real analysis. I admire Gonthier's structure in Coq, and I am coming to appreciate the power of dependent types.

Q How much have you formalised of differential geometry.

A I don't do any differential geometry, or even surface integrals.

DA What do you plan to do with the proof when it's finished?

A There's a lot that can learned from this. Machine Learning can learn a lot from these libraries (this, HOL Light, etc.).

MK Your original motivation was correctness. What do you see as the consequences?

A Raise the awareness of formal proof. We can do by machine what referees were not able to do by hand.

Q You've done a lot of refactoring. Is this because of what was available? Systems tend to be developed 'bottom-up', while your work was 'goal-directed'.

A Yes: availability did drive the refactoring. I could have developed homology formally, but chose to change the proofs instead.

CSC Traditionally we have gone from concrete proofs to abstract proofs: are you reversing this?

A Probably, but I need to think about this.

5.2 Extending OpenMath with Sequences — Horozal

OpenMath has variables x, symbols c, applications $@(E, S)$, bindings $\beta(E, \Gamma, S)$, attributions $(E\ k\ V)$, and literals (numbers) n.

Currently sequences are indirectly built by flexary operators $@(+, 1, 2, 3, 4)$. Multirelations such as $x < a \in S \subseteq T$ are common in mathematics. We could have a multi-relation operator, and write $@(M, a, <, a, \in, S, \subseteq, T)$. How would we axiomatise this.

- $@(M(x, r, y) - r(x, y)$
- $@(M(x, r, y, t) - r(x, y) \wedge @(M, y, t)$ but this only works with sequence variables.

Hence we add S_E (sequence expressions) to the OpenMath language. Example $[i^2]_{i/\leq n}$ would generate a sequence, and their sum is $@(+, [i^2]_{i/\leq n}$.

The paper has inference rules for sequence expressions, e.g. for selection

$$\frac{S \to E_1, \ldots, E_n, I \ldots I \qquad X \to n}{S_X \to E_n}.$$

The concrete syntax would be `<OMSV name="ζ"/>`.

We can add a CD to OpenMath which can simulate these, and make a translation from our primitives into this to allow interoperability. This would have symbols like `seq` etc.

CSC Gonthier has a much more expressive set of sequence variables in a paper. [BGOBP08]

AT How much are multirelations used in practice?

MK There are 200 occurrences in my 500-page text (excluding the $a < b < c$ cases, i.e. only counting mixed ones).

Q Does it only make sense to have sequences starting at 1: they might start elsewhere.

A This is the simple primitive — there is a trade-off between generality and simplicity, which could be argued.

BM What would be the implications for Content MathML?

A We have a matching proposal here.

5.3 Combining Source ... — Horozal[HIJ+11]

The LATIN project (section 2.3) is background. This is a multi-author project, so there are implications for collaborative authoring, change management etc. It is also hard to present such work — interactive documents would make this easier. How do we query: XQuery, SPARQL etc.?

Note that these challenges are similar to those in traditional software engineering: source languages, documentation, programming tools etc. Our source files are basically ASCII, but we need to combine all five dimensions. source/content has been done, RDFa combines presentation and relation aspects, etc.

Our representation is one directory per dimension

source physical files

content OMDoc organised into folders by logical identifiers

presentation XHTML rendering of the content

narration outline of the source documents with links into the content.

relational representation of the content in the OMDoc ontology

Use MMT URIs: `namespace?theory?symbol` (inspired by OpenMath), which should be canonical for mathematical knowledge items. We compile the source files to get the rest (JHD thinks), and the whole structure can be packed in a `.mar` mathematical archive. The "theory graph" is automatically generated.

This is a first design for such a structure, but we have already found it very useful in our own work.

PI Is this an updated version of the "mathematicians' workbench" of EMT? Who else can try it?

A:MK You can build the tree with any tool, and make the archive with ZIP.

5.4 FLOS Licensing the Mizar Mathematical Library — Mamame [AKN+11]

Note that MML started in 1989[3], with the copyright centralised in SUM (the association of Mizar Users: a Polish body). But there was no licence.

The border between formal and informal content is pretty (e.g. IBM Watson) blurred. Code is generally licensed under GNU GPL (though there are variants etc.). Documents seem to be mostly "creative commons". As recently as 2009, Wikipedia changed its licence, which demonstrates that the world is still in flux.

We therefore suggest that SUM keeps the copyright, to allow for a relicensing decision. What about patents? They forbid re-implementation from a published specification, but there is no difference for us. Hence we propose to ignore the issue.

Note that if you have a very liberal licence, anyone can import you, but you can only import from very few people and *vice versa*.

[3] Thus essentially predating the big open-source movement.

5.4.1 Aims

- Not hinder "legitimate science" — translation, archiving, APIs, data mining, search engines, benchmarking APIs, etc.
- Power to object to non-"open science", but therefore "ask and you shall be allowed" model.

Note that `gpl-violations.org` now gives constructive proof that open-source licences *are* enforceable — see the GNU/Objective C issue.

The assignment to SUM has a "doomsday clause" — SUM loses copyright (default to distributed copyright) if it "goes evil". The licence is based on the FSF Europe's FLA: the major change is that SUM *may* grant commercial licences.

Q Have you studied the enforceability under various jurisdictions?

A We trust FSFE's lawyers!

JU Bob Moore said "why not public domain", but the concept does not exist in many European jurisdictions.

Q What happens if SUM gives a commercial licence, then goes evil?

A Ask a lawyer!

5.5 Indexing and Searching Mathematics in Digital Libraries — Sojka [SL11]

We assume a vast DML — Zbl expects to add 140K papers this year. Search is the key to this knowledge. Google etc. shows that text/keyword search is largely solved. Mathematics search is basically a failure so far.

5.5.1 Prior Art

- MathDex (formerly MathFind) indexes n-grams on MathML. There are multiple fields for different constructs (numerators, superscripts etc.). Currently password-protected.
- EgoMath2 (section 2.10) — based on full-text EgoThor. α-equivalence supported.
- Search tool offered by Springer over their LaTeX sources, but basically string matching in LaTeX, with no formula structure. 3M formulae.
- LeActiveMath — string tokens from OMDoc with OpenMath semantics.
- DLMF — equation source, but only in their special markup[4].

[4] BM pointed out that it doesn't actually *require* this markup. But the search engine is admittedly tied up with the whole DLMF engine currently.

- MathWeb — supports Content MathML and OpenMath, uses substitution trees. α-equivalence supported.

Our proposal is MIaS (Math Indexer and Searcher). TEX or MathML input. α-equivalence supported.

5.5.2 Implementation

We need (in this order) ordering, tokenization (including extraction of subformulae), variable unification and constant unification. Note that unification is not always done (as JHD understands it, both the unified and un-unified are stored, but a non-unified match scores higher).

The initial weight of a formula is 1/(number of nodes). This adapts as we goes (showed a complicated worked example). Implementation is in Lucene 3.10. We has 439K documents, with 158M input formulae and 2.9G indexed items. Index time was 23 hours (not totally unreasonable). Average query time is 469ms.

Note that this is joint math+text searching-friendly, as shown in the demonstration.

Q Why `id1` as well as the named version?

A We get lower weight for unified matches.

MK Do you collect queries? We need a corpus of queries as well as a database of formulae.

A Vague answer.

Q How do you manage this 64GB index?

A Currently stored on one machine.

BM Does "relaxation" mean what DLMF does, i.e. $\sin^2 + \cos^2$ itself should match $\sin^2$`<junk>`$+ \cos^2$?

A Not currently.

A The main cost in the index is the hit-list and weights, hence it grows essentially linearly with database size.

Chapter 6

DML — 20 July 2011

Largely short communications.

6.1 Towards a Digital Mathematical Library: On the Crossroad — Sojka

There are various possible directions for mathematical publication: to quote but two: High-Energy Physics and Biomedical.

6.2 DML-CZ: current state — Jiri ??

About 3330Keuro project Finished December 2009. 11 Journals, 6 conference proceedings (including DML itself), 300K pages from 10K authors. One of the main outcomes is the metadata editor. We also have a well-established retro-digitisation process. There's a similarity-search engine (in fact three different algorithms, and three lists are presented. Many negotiations with publishers so that they will either use our tools (producing our metadata) or at least not get in our way. Unless the French, we don't actually publish journals.

When the project ended, we had to become self-sustaining. There is a good split of tasks among partners. After 18 months of this operation, we can say that we have general acceptance, and a new journal has been added, a book series on mathematical history, and the collected works of eminent Czech mathematicians[1]. According to Google Analytics we get 400 accesses/day, which seems quite good.

Need to distinguish between the 'working copy' and the public version of DML-CZ. The metadata editor has been internationalised, and is available in and beyond the EuDML project. The funding model which currently works is charging publishers *pro rata*.

[1] One so far. This has challenged the metadata model, and we have working papers etc., which do not fit into the original scheme. There are also copyright issues.

JP I had a project with Springer, but after five volumes they just 'pulled the plug' citing incompatibility of policy. We will try again.

A WE had the same problem with *Math. Slovakia*, but they switched to Springer and had to cancel their agreement with us. We also have two journals published by CRAS, but distributed by Springer. They wouldn't let us do a sensible "moving wall" ($\leq$ 1997 was offered!)), but we insisted, and they did.

6.3 Update on bdim: the Italian digital mathematical library — Zelati

`www.bdim.eu`. Aims:

- To raise the money for retrodigitization (not very successful to date).
- To give Italian mathematics journals a common repository and diffusion
- To integrate with the international effort for DML
- To integrate with the Italian national digital library.

Bull. UMI[2], Rendiconi di Trieste, Le Matematiche, Rivisti di Matematica (Parma), Ricerche di Matematica (Napoli), Rendiconti Lincei $+\cdots$ have signed up. "MathJax works very well'. Plain text searching is supported.

Q When Fedora, while DML-CS uses DSpace?

A It does the job!

6.4 Time-stamping Preprint and Electronic Journal Management — Namaki

Many universities offer local preprint services, but the security of thee may be at risk. Readers trust the publishers' version as the official one. How do we do this in paperless publication? It is difficult to distinguish a copy from the original. So we use the National Time Authority to feed our Time Stamping Authority, which issues timestamp to a long-term signature server (this and the certification server are run by NII), and this signs the digital hash of the PDF. This is maintained by the publisher (e.g. Hokkaido University). The timestamp technology is RFC 3616 and ETSI TS 101 861. While we can combine electronic signatures and timestamp technology there are problems with the compromise of the hash algorithm or the leakage of the private key. Hence we propose to combine with long-term signatures: RFC 3126. Call this ES-C. We then put a timestamp over ES-C (call this ES-X) add an archive timestamp, to get ES-A.

[2]Serie 3 (1946-1967) digitised. at 600dpi in line with Numdam.

The final output (from Hokkaido,.say) is a Full text PDF with a long-term signature which guarantees the time of creation of the original. He showed a validation example.

JHD Does Hokkaido go back to NII for each PDF?

A Yes, to guarantee the timestamp of that PDF. The entire PDF is transmitted.

PS Does Hokkaido also post with Euclid? What problems does this cause?

A Yes, and no problems.

6.5 Towards a flexible author name disambiguation framework — Dendek

6.5.1 Motivation

Binding between an author and his articles, and problems with mapping an author's is across libraries. The same author may have different names, there are OCR errors, poor handling of diacritics etc. Articles by the same authors tend to have common attributes. We need to train these affinity measures, then have an infrastructure into which to put them.

Definition 6 *An* author *is a human who writes articles.*

Definition 7 *A* contribution *is an author's signature on a paper: hence an article will be several contributions, in general.*

Definition 8 *A* shard *is a group of contributions which have common features.*

Definition 9 *An* identity *is a group of contributions believed to be by the same author.*

Definition 10 *A feature compares two contributions with respect to some field (e.g. year of publication), with a value in* $[-1, 1]$.

For example, e-mail address returns 1 is the same, but only -0.1 if different. Different languages (not English) scores -1, same language (English) scores $+0.05$, but same language otherwise scores $+0.1$.

Definition 11 *The* weight *is a measure of the feature's importance.*

Definition 12 *The product of feature and weight is an* atomic affinity

Definition 13 *The sum of all the atomic affinities is the* total affinity

6.5.2 Framework

These are the stages.

1. data import
2. contribution decomposition
3. affinity calculation. This is naïvely an $O(N^2)$ process, so we resort to hashing. Note that the hash function must place all the contributions by an author into the same shard. Some features (e-mail) are highly polarised. Some are flat ($= / \neq$), others have a graph structure.
4. clusterization — using a standard algorithm.
5. result persistence (in a database.

JP There's a lot of information in the collaboration graph which you are not using.

A Mistake — it's a feature in the list, with 0.7 with one common co-author, 1 if more than one.

JHD Isn't this recursive?

A Yes - we just use an approximation here.

PI Isn't there a problem with the shard requirement: Hilbert vs Gilbert, transliterations etc.

A Yes — future work.

PI Also, there are 11 I.I. Ivanov's.

A Keywords should help here.

6.6 Workflow of Metadata Extraction — Tkaczyk

We want to extract metadata (titles, authors and affiliations, abstract, *parsed* bibliographic references etc. from documents. Sometimes there are documents without metadata (scanned), and sometimes it's of poor quality.

MARS uses TIFF images

[Flynnetal] ...

We use PDF.

We build a tree structure (pages and characters[3]), analyse[4]Currently a top-town XY-cut algorithm, but intend to replace by a Docstrum-based bottom-up approach. and enhance the contect, and then extract the metadata.

Citation extraction is currently based on a heuristic based on digit/punctuation frequency occurrence (!). We plan to enhance this one. After this, there is citation parsing. This is done with a Hidden Markov Model based on a training set. Viterbi's algorithm is used. There are 48 features here (relative fractions of digits, upper case letters etc.), particular words ("and", "vol") and so on.

Q Citation blocks are a modern occurrence: how do you cope with older papers?

***** This seemed to come as a surprise to the speaker.

TB I am very sceptical about training in this context.

A We need a very diverse training set.

TB This has its own problems.

APS To what extent is the inaccuracy of iText a problem?

JB Do you have problems with tables?

A Haven't really encountered these as yet.

ES How do you do the segmentation in citations (e.g. author/title/journal).

***** Quite some confusion here: we tokenise into words, and then use a HMM to decide classification author/title etc.

6.7 The EuDML Schema v1.0 — Bouche

`http://www.eudml.eu/eudml-metadata-specification`. A public well-specified EuDML schema is needed

- for content providers
- for the search engine
- for the user interface (what and how to display)
- for metadata enhancers toolsets (input and output!)
- for content dump

Supported items include (− exclude)

- A multivolume work

[3]Uses iText library.
[4]

- A book, namely
  * a single volume from a multivolume work
  * a monograph (possibly a dissertation)
  * An edited book (possibly conference proceedings), containing articles/chapters with their own authors
- A part of a book (chapter/conference article)
- Journal article. (80% of the whole for mathematics — 90% if we add conference articles)

– Any text not persistently and formally published (preprints)

– Papers not generally accessible online

– version control for documents

– complicated author/contributor structure for documents

– licensing, access barriers, DRM issues.

We base ourselves on NLM JATS (Journal Archiving and Interchange Tag Suite), which originated in PubMed, and is used, for example, in JSTOR, and at EDP Sciences (one of our partners). It is MathML-ready. It allows parallel versions of the same content encoded differently. `http://dtd.nlm.nih.gov/archiving`.

However, we needed to add new first-class items. Conversely, it is too generic in other ways, and we have an "EuDML application profile". Formulae are encoded using `<alternatives>`, with generally MathML and TEX codings.

JP What is the authority for the name space `mr-item-id`?

TB Me![5] More seriously, we have a list of these, such as DOI.

JP What is the IPR position of these metadata records?

TB We discussed this yesterday. I believe that this should be freely available.

6.8 DML Panel

JHD participated, so couldn't take notes. The question asked was, essentially, "what would make people want to use a modern DML such as EuDML". The following major points emerged.

JHD

VS

[5] JHD remarks that we are looking at the authority for the *names* of the tags, not the values.

Chapter 7

21 July

7.1 Towards Reverse Engineering of PDF Documents — Baker

It's quite easy to find the relevant PDF document, but much harder to work with the document: screen readers, reflow, cut and paste, and in fact there's no `pdf2latex`. This is in fact more a feature of current PDF production tools, rather than inherent in PDF. In principle, PDF analysis offers more than reverse OCR, in that Unicode names, fonts, sizes, baselines *may* be available. Character spacing is vital in mathematics: xy versus x^y. Our previous work includes character (glyph) extraction via PDF→TIFF, merging this with PDF analysis, linearisation and parsing.

Our improvements include full automation (allowing for large scale conversion), and further structural analysis include mathematics segmentation. Projection Profile Cutting (PPC) was used for line and column extraction, which is efficient and offers good results on many layouts. Lines are parsed with an LALR parser, separating display mathematics from text (possibly including mathematics) via heuristics.

Showed a whole page, original and reconstruction. Main problems were recognition of headings (fonts correct, but spacing wrong), and lined-up multi-lined equations weren't lined up correctly. Also JHD observed that the hyphen at end-of-line was not correctly parsed[1].

Did a comparison with infty [BSSS11]. Chose 2 pages each from 5 articles. In general their tool did better, but $\sum_{i=0}^{m} a_i x^i$ does not do well, as m and $i = 0$ are split off by the PPC. This has led to a `pdf2latex` tool, and `pdf2mathml` is in development.

ES The summation problem did not occur in the comparison old versus new?

[1] JHD observed subsequently that *some* PDF generators will place the unhyphenated text in the PDF as well.

A True, that's because the summands were tall enough that the equivalents of $i = 0$ etc. were not split off by PPC.

Q Also, if you ran this, do you get a "canonical" form for a mathematical expression?

A We actually have two drivers, a "sane" one and a "spacing-compliant" one. The first one would generate a canonical form for searching.

7.2 Web Interface and Collection for Mathematics Retrieval —

Claims that the main motivation is search — we are the "Google generation". Our experience with Google Scholar shows that not handing mathematical expressions in citations causes severe problems. There's a paper by Kováčik & Rákosník, which has mathematics in the title, which appears as 20 items in GS. There have been several attempts to solve the problem.

Springer has LaTeXSearch., which he demonstrated with $x^2 + y^2$, but this is basically string search in LaTeX sources.

WebMIaS is our system (see section 5.5).

We tested this on the MREC collection of hundreds of thousands of mathematical documents. which we believe should be used as a standard corpus for benchmarking such engines, analogous to TREC[2]. There are > 158M formulae, formed from arXiv documents which converted successfully (possibly with warnings).

We needed several steps of pre-processing to improve the possibility of matching two equal expressions encoded in different ways. UCML (Universal Maths Conversion Library), whose main purpose is MathML→Braille, and is in XSLT, is also used for our canonicalisation.

MIaS allows LaTeX input for ease-of-use. Note that the system seems to scale well, and we would like to move to MathML-C support as well in the future.

MK If you used LaTeXML rather than TRALICS, much of this need for canonicalisation would go away.

A But we wanted to allow direct MathML input as well, and we can't force the user to type the number of `<mrow>`s that are needed.

ES At which step do you apply commutativity?

A Unification.

PI As a member of MathML, we would like to compare the outputs of TRALICS, LaTeXML, `pdf2mathml` etc.

[2] `trec.nist.gov`.

MK There was a paper on this at DML two years ago: we should probably update this.

JP There was a drop-down box for "form of input" — unnecessary.

Q Do you index every subformula in a large multi-line formula?

A Yes (including a

7.3 Using discourse analysis to interpret object-denoting mathematical expressions — Wolska

Consider a^{-1} — what is it? This is relevant to syntactic parsing, semantics parsing and formula search. Is that really -1 or is "-1" a decoration as in a'? Claims that discourse analysis is needed to do this. Focus is on "object-denoting mathematical expressions", i.e. a single identifier with sup/super scripts. This is analogous to word sense disambiguation in NLP. Here it is normally done by comparison with a "gold standard",i.e. a reference lexical resource.

The corpus is 10,000 arXiv documents parsed with LaTeXML. These were pre-processed with tokenisation, word-stemming, domain-term identification (based on [Frantzietal2000] algorithm and n-gram statistics[3]) and identification of symbol declaration statements (based on [Kozarevaetal2008]'s *anchored patterns* approached). On a test set of 374 statements have 89% precision and 77% recall.

There was no suitable taxonomy (confirmed by reviewer). We wanted a single interpretation for simplicity, with not too many categories, and not a hierarchy. We built one based on MSC (5000 subareas) and Cambridge Mathematical Thesaurus (4500 concepts, with explicit broader/narrower categorisation, but hierarchical). Automated processing gives 341 unique concept names from MSC, 170 of which were also found in CMT. This gave, for example: Algebraic Object: Set: Monoid: Group.

Hence seven categories: Algebraic Object (general); Algebraic Object (Mapping/Function); four more; Method or Process. Based on this, we manually classified the $171 = 341 - 170$ ones.

For each target mathematical expressions

1. We create lexical context sets

local co-text

global declaration candidate in document, plus declarations.

2.

[3]Not yet evaluated in our context — original application was biomedical, where it was validated.

Then for each of local and global context C, we compute the similarity between C and each class in the taxonomy. The similarity is a weighted sum, where weighting is recency for local context[4] and position (first occurrence is highest weight) for global context[5].

The corpus of 200 simple MEs were split into 7 annotation sets, 4 of which were double-annotated (only seven disagreements). Showed the instructions for the annotators, which emphasised the importance of annotation in context. The process (but not the corpus) is language-independent.

Most MEs can be immediately disambiguated based on shallow syntactic analysis of the co-text. Therefore we can build basic NLP tools here. **But** tight collaboration with domain experts is a complete pre-requisite.

MK We are trying to organise the linguistics of mathematics — a new field.

WS This is very limited — you should be looking at phrases.

A But one has to begin somewhere.

Q Wikipedia/PlanetMath?

A PlanetMath is a wonderful resource, but I wish there were guidelines for authors, as it is incoherent at the link level. One also doesn't know what is a noun phrase/ verb phrase etc. Wikipedia articles tend to start with a definition, but there is a lot of pre-processing required here.

Q Standard stemming tools have problems with mathematics.

A Ours (?what?) seems OK, but I agree.

7.4 EuDML — Bouche [BBNS11]

Aim to assemble as much of the digital mathematical corpus as possible, with a view to

- helping preserve it over the long time;
- making it available online (not interested in stuff which will not be eventually free: moving walls[6] permitted);
- being an authoritative and enduring digital collection
- growing continuously with publisher-supplier new content
- being augmented with sophisticated search interfaces and interoperability services

[4] Standard technique in computational linguistics.

[5] Things tend to be declared at first appearance!

[6] Every year an archival copy (metadata and full text) is transferred, ingested and indexed. Full text links point to the publisher's site (and access control), until the wall moves past the item, then to the EuDML copy.

- being distributed.

Ultimately would like to drop "European".

Would like a website with personal work spaces, allowing searching and browsing of collections. We plan a (batch) service turning citations into links, and this provides added value for new text, as references turn into links.

Note that preservation is important, and is a task that has traditionally been assigned to libraries and publishers. There's little direct profit in preservation! Current state:

235K items; 185K journal articles, 45K chapters/conference contributions, 2500 books, 300 multi-volume works;

2M pages;

***** Both retro-digitised and born digital material.

7.4.1 Project Manager — Borbinha []JB

Note that this is *not* a research project in the EU's eyes. I'm a computer scientist. Note that we are in mid-project, with a mid-term evaluation in September.

PI *Europeana*?

A This is funded by the same programme as EuDML. Their aims are to set up new services based on existing technology. Their projects tends to have hundreds of partners/sub-partners/.... Note that EuDML could be viewed as an aggregator for Europeana.

MK Is there a collections of URLs to access the LaTeX produced.

TB We don't produce LaTeX as such, more LaTeX-producing tools. As regards the LaTeX of the papers, this is not necessarily available as a result of the moving wall.

TB The list of resources will be itself available as an EuDML query.

APS The core of the project is aggregation, and the tools are, formally, a by-product.

JP Encouraged to hear that you are committed to machine interfaces as well as human interfaces. RESTful interfaces and Json are not new technologies any more.

Q Why you, not JSTOR? "You are talking about libraries, but the key is STORage".

TB My opening slides showed the benefits of EuDML, against Springer and LMS.

Q You should force European publishers to deposit with EuDML.

JHD When LMS set up the "electronic only" JCM 14 years ago, we printed one paper copy to force the British Library to archive it, since it would not *at that time* do digital archiving. Legal deposit of digital materials is not even born, let alone in its infancy — you should be pressing the European Parliament, not EuDML.

TB The latest version of TRALICS has a TEX to MathML converter: install TRALICS and mail me for the incantation. He also demonstrated the linker, and showed it picking up a cited translation (in EuDML) for an article that wasn't. However, he gets NUMDAM metadata, not EuDML metadata (which doesn't exist yet).

MK You have this TRALICS-based LATEX→MathML — can you please wrap it compatibly with the LATEXML daemon so that people can do plug-and-play.

CL How do I get the RDF metadata?

TB There is no RDF metadata currently.

JB The project proposal predated the successful arrival of "linked data". We need to discuss the whole RDF issue.

JP Is something like the Bernouilli society, an international society based in the Netherlands, "European" enough for you? We currently use Project Euclid.

A The answer seemed to be yes, and JP was willing to go and ask the appropriate authorities.

7.5 DML Business Meeting — Sojka (chair)

PS took the chair at the DML Business Meeting. It was confirmed that DML had no formal charter, but the voting members were thos epresent at this meeting.

1. **DML Joining CICM?**
   He suggested that DML should become a CICM member. He felt that the increased visibility (LNCS etc.) would be a major positive point. DML had hitherto been fairly "hand-to-mouth". Carried *nem. con.*

2. **CICM Delegate.**
   TB was proposed, and this was agreed with only TB voting against.

3. **DML track chair at CICM.**
   TB proposed PS, and this was carried.

4. **Future "Yellow Book"?**
   PS noted that CICM allowed arXiv-etc. deposits, so we could continue depositing such versions in the DML archive.

5. **Mailing List?**
   JP called for a DML mailing list. MK offered `dml@cicm-conference.org`.

JB[7] announced that the EU had just called, asking thatEuDML present at the Information Society Open Day on 19 September. It also looks as if costs for direct digitization will be allowed in Framework 8 Projects (unlike EuDML itself).

[7] EuDML Project Manager.

Chapter 8

22 July

8.1 Why is the linguistics superstructure needed — Trybulec

Let $f : P_1 \to P_2$. Assume $P(f^{-1}(A)) = P(A)$, i.e. that f^{-1} is measure-preserving. Then f is not measure-increasing. However, note that, information-theoretically, proving a theorem is useless, since it does not add to the information. This problem was considered by S. Ulam and J. Conway (see game of life)!

Note that the Post Correspondence Problem (PCP) is unsolvable [Pos46], but semi-decidable. What about fixed k. It is decidable for $k = 2$ [Ehreneuchte-tal1982], but undecidable for fixed $k \geq 7$. [Matatiyasevich]

Let P be PCP, and S is set of possible solutions,

Theorem 10 $\exists_{e \in P} Inf_{\mu_2}(f(e) > \mathrm{Inf}_{mu_1}(e)$, *i.e. information* has *increased.*

8.1.1 Predicate Calculus

Theorem 11 $\exists n : \inf(proof_n) \geq \mathrm{Inf}(th_n) - \log_2 g(n)$ *where* $g : NAT \to RAT$ *such that* $g(n) < 1/2^{A(n,n)}$ *(A=Ackermann).*

Let v|Phi be the set of formulae,a nd P the set of proofs. $f : \Phi \to NAT$ with.$f(\phi) = \min_{pfits\phi} |p|$. Then f is not computable.

Hence, while theorems are undecidable, theorems and proofs are decidable. In fact, all one needs is the *length* of the proof, because then one can enumerate! But the length is not a very useful hint, if we start thinking about complexity rather than just decidability. When AT was asked, as part of [Wie03] for a proof that $\sqrt{2}$ is irrational, he could produce a 1-line proof in Mizar, since Mizar already had a proof that $\sqrt{p}$ is irrational. Hence we need to consider the length of the unfolded proof (see Alama's work).

Claims that we ned a theory of "obviousness" — not well developed.

Associativity of addition $a + (b_c) = (a_b) + c$ becomes $S[b, c, x] \wedge S(a, x, z) \wedge S(a, b, y) \Rightarrow S(y, c, z)$ Mizar insists that we quantify the variables x, y, z — one would normamly use $\forall$. But addition is unique, so $\exists$ is acceptable, or, worse, a mixture!

If we have a simple language (pure predicate calculus), then we need a powerful inference engine, but if we allow a more powerful language (in this case, functors), then we need a less powerful engine. Note that $((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r))$ becomes a four line expression when we define $p \Leftrightarrow q := (p \rightarrow q) \wedge (q \rightarrow p)$.

As another example, if one is being formal about the definition of a group homomorphism, we should let $G_1 = (A_1, +_1)$, $G_2 = (A_2, +_2)$ and then every theorem about $+$ has to be reproved for $+_1$ and $+_2$, etc. Types get round this problem (but see work of Lamport).

We should/could use qualified quantifiers. Notes that the LUTIN logic copes quite nicely with undefined terms, but it is occasionaly necessary to state explicitly that a term is undefined.

Life is easier with adjectives, such as "finite" (rather than 'finiteset", "finiteggroup" as nouns, JHD thinks).

Quotes the Boolos inference, which essentially encodes the Ackermann function, and has normlaly been seen as very different for theorem provers. [BenzmullerBrown2007] shows quite short proofs, and AT could do it in four slides, even though straight expansion gives $A(4, 2) \approx 10^{17,000}$-long terms.

8.1.2 The power of ...

See 5.2. Notes ambiguity: is $1 + \cdots + (2n + 1)$ equal to $\sum_{i=1}^{2n+1} i$ or $\sum_{i=1}^{n} 2i + 1$? Mizar has syntactic sugar: `a[1]&...&a[n]` (these are `...` in the Mizar language) as syntactic sugar, but this doesn't work by itself. We actually need a corresponding inference rule, relating Mizar's `...` to meta-level ..., which is being done in Mizar. The next direction is "multivariables".

MK You've been working on Mizar for 35 years, but still want to extend the langauge. Wher will this end?

AT I don't know.

JU Does this not need AI-style parsing etc.?

AT I am not sure?

PI There are energy costs of computation — can we work with this?

AT I am not sure?

MK The group in Munich have been looking at 'polynomial simulation', and this idea should possibly be looked at again.

Table 8.1: Origami specifictaion: equilateral triangle in square — Eos

```
lemma equilateral triangle:
fixes E F G H J K :: point
  and k l m n :: line
assumes a1:"k = fold2 A D"
  and a2: "E= intersect k A D"
  and ...
  and a7 : "m \in fold5 D I A"
  and ...
shows "dist A J = dist J K"
  and "dist J K = dist A K"
```

8.2 Formalizing Origami Proofs — Kaliszyk [KI11]

This is part o fthe "computer algebra is proof assistants" theme. There are efficient computation issues, such as his FormMath (also relationships with Cylindrical Algebraic Decomposition). ISSAC is a CA system in Isabelle. There are issues with computer algebra, e.g. Maple's `sub(x=infinty,2*x-x);` and `int(1/(1-x),x)` versus `int(simplify(1/(1-x)),x)`.

In ISSAC `y/y` gives `y*inv y` which can only be simplified under a suitable assumption.

8.2.1 Origami

Ancient Japanese art, which is an alternative for "ruler and compass" in Euclidean geometry. Used in (at least some) Japanese high schools. Eos [Ida] is a system for visualizing these in Mathematica. See table 8.1.

We wish to translate the computational part in HOL. We use John Harrison's implication of Gröbner [Har07]. We did the proof half-manually, moving equations between assumptions and the goal for rewriting in other assumptions, which was troublesome, and ended up with a 5-variable real QE problem (20m seconds). Note there is cylindrical algebraic decomposition [Mahboubi] — speaker not sur eof the status.

8.2.2 Axioms ()in Progess)

```
deinfition fold1 :: point => point => line where
  fold1 P Q == THE I P Z I = P /\ Q Z I = Q
```

where `Z` is the incident operator.

`fold5` is more complicated (see $\in$ in table 8.1). We have challenges over the secpification language, indeterminancy, and combining decision procedures.

JU How difficult are these problems — undecidable?

A Dedicable isn't good enough: we actually want practicable!

8.3 Retargeting OpenAxiom to PolyML: Towards an Integrated Proof Assistants/CAS Framework — Dos Reis [DRML11]

`www.open-axiom.org`. Note that OpenAxiom is supported by 5 Lisp systems, none of which work for me. I was going to start again, when MW pointed me at PolyML. Clearly everyone wants dependable computer mathematics. We wanted a *typed* CAS (Axiom is the obvious family).

Most prior work interfacing CAS and theorem provers is in Maple, but this is, for him, a *symbolic* system, working on ASTs, rather than a CA system. It's alos generally been pretty loosely coupled. Shows an example of

```
integrate(1/(x^3*(a+b*x)^(1/3)),x))
```
(8.1)

from the Axiom book, but claims that this hides many assumptions about `a` and `b`.

Note that AXIOM data types are **huge** cyclic data structures, so we need to avoid copying these.

```
\iBasicTYpe: Category ...
   =
  ~=
```

Hence `SemiGroup`, `LeftLInearSet`, and `Integer` belongs to these, which is a typical cause of cycles. This cyclicity gives real problems for proofs of correctness. There's also a problem with the number of packages that get loaded in, for example, (8.1). These are strong arguments for coupling the deduction and computer algebra in a single address space.

Types seem complicated, but they are indispensable: [Dav02] shows that equality is very type-dependent.

Note that Axiom uses LISP as a virtual machine[1], so can be replaced with PolyML, which is the common runt-ime for Isabelle/HOL Light etc. We will keep the compiler written in BOOT, but try to prove things about it in Isabelle.

JHD (8.1), which returns a result in `Union(Expression(Integer),...)`, actually hides no assumptions. The assumptions are made *when* we convert that expression to a function. This emphasises the importance of types, since the assumptions are made at type conversion time.

A True.

JC "integration" is an operation from functions to functions, but "closed form integration" is an operation from "expressions denoting functions" to same. This is the difference.

[1] The speaker quotes various comments by "a very angry JHD" in the Axiom source dealing with this layering.

8.4 Supporting Structured Generic Programming with Automated Deduction — Katzen

Our target audience is the practical programmer. Axiomatic programming is structured generic programming that expresses and uses axioms directly in code. [StepanovMcJones]

Example of why there's a problem here. He uses the `find` from STL. First case is OK, second case instantiates OK (even though naively type-incorrect) but produces an "instantiation error".

Have a user-defined concept "BinaryOperation", and can feed this into `power`, getting exponentiation with `*`, but multiplication with `+`. A more complex example has a user-defined concept "Iterator", and various developments, such as "Random Access Iterator".

Have currently translated code from 7 of the 12 chapters of [StepanovMcJones], which requires formalising $\forall^n$ and $\exists^n$.

Q The new C++ standard has a "typed template" concept.

A–GDR There are some issues with this, and this approach gives a list of implicit equations, which should be simpler than the C++ proposal.

8.5 The MathScheme Library: Some Preliminary Experiments — Carette [CFJ+11]

Three experiments in Abstract Theories, Concrete Theories and Applied Universal Algebra.

1. Abstract Theories. Every time I look at systems, I see so many "redundant" lines (except in Axiom). Hence we use "tiny theories" to ensure that each line is only typed once. But even here, with 200 theories in 250 lines, we had code duplication. Furthermore, we should have re-done this with `Partial`, and so on.

2. Concrete Theories (Implementations). E.g.

```
Bit := combine Bit_And, Bit_Or, ....
```

3. Applied Universal Algebra. I am interested in the constructions, rather than the theorems. "homomorphism", "substructure" etc.

```
MonoidTerm := Theory { type MTerm = &Monoid }
```

   Axiom is basically one-sorted, and we are not, which helps.

```
MonoidH:= Homomorphism(Monoid)                    (8.2)
```

   expands to seven lines, making the point about duplication.

MK You seem to be optimising the 10% code, rather than the proofs. Is this worth it?

A I'm working on this, so I clearly think it's worth it! More seriously, I should get re-use of the proofs, so *should* save here as well. Watch this space!

Q Axiom is very circular.

A There's a difference between the base theory of groups, say, and the enriched theory.

Q What language do you use?

A Currently using Chiron. Note that (8.2) is actually quite subtle, and needs this power.

8.6 Certified exact real arithmetic in Coq — Krebbers [SK11]

The Kepler conjecture (section 5.1) is a good example of why this is needed. We can approximate by the rationals, or indeed any set that is dense in the rationals. [O'C08] tried to do this, which is based on metric spaces and the completion monad. However, it uses Coq's **Q**, and this is an inductive type, not related to the machine arithmetic. Hence we wish to build our implementation on top of an abstract interface (good programming, but rare in theorem proving!). In fact we will use the dyadic rationals $n \cdot 2^e$ using Coq's machine integers. We are other performance improvements: range reductions and improved computation of power series.

We [SpittersvanderWeegen] need solid implementations of

- type and type class inference
- widening etc.

We use type classes, which are very similar to Axiom's categories, and have been a great success in Haskell and Isabelle. These have recently been added to Coq as well. We define *operational* type classes, e.g. `RingPlus` (with an infix shorthand), and, separately, properties as predicate type classes. Then `Ring` is a combination of operational type classes and properties.

On top of this, we have added libraries for constructive order theorem, additional operations such as shifting, support for undecidable structures (such as the reals), explicit casts and more implementations for abstract interfaces. This works for the basic rational operations.

For the operations we use power series. We don't have exact division, so we implement via two streams computing numerators and denominators. We actually use range reduction to $(-2^{-50}, 0)$ (alternating sum!) for exp. This Coq implementation is about 100 times faster that [OConnor2008]. We can

also think of `native_compute` by compiling to OCAML. We have observed no performance penalties in Coq from the type classes methodology.

JC You're still 100 times slower than standard computer algebra.

A One step at a time.

8.7 Incidence Simplicial Matrices Formalized in Coq/SSReflect — Heras [HPDR11]

Digital Image → Simplicial Complex → Chain Complex → Homology. This is currently done in Kenzo: how do we formalise this?

A Chain complex is a pair of sequences $C_* = (C_q, d_q)_{q \in \mathbf{Z}}$. The image $B_q = \operatorname{im} d_{q+1} \subset C_{q+1}$ etc. The d_n can in fact be expressed as matrices, and diagonalisation will give you the homology groups. In fact, the incidence matrices turn out to be the easiest thing to work with.

CSC These matrices are very sparse — how to you represent them?

A Currently as functions $(i, j) \to a_{i,j}$. Also the main cost in Smith normal form, and we don't know of a sparse algorithm for this. .

8.8 View of computer algebra data from Coq — Komendantsky [KKL11]

We started with GAP, but this work is more general. We use SCSCP which transfers OpenMath. In GAP we have `openmath.g` and `scscp.g`. This requires non-trivial package/tactic installation. SCSCP was developed for CAS, so Coq is a challenge. At the moment we only have Coq as a client, not server. Note that there is quite a lot of related work in TP/CAS interfacing, e.g. [CO00].

In our OpenMath, polynomial rings are only transmitted one by means of `id=` constructs. In Coq we use the packed class methodology (orthogonal to the type class method described earlier). A child class can have n parents. We then have a mixin with `viewin`:OM→ $T_\perp$ and `viewout`: $T \to OM_\perp$. We use "unification hints" in Coq, which are automatically generated for us.

Example uses GAP to compute roots of univariate polynomials. Another example is Bisimilar automata. GAP produces a non-minimal one for his example, but GAP can't prove the two are bisimilar, but we can call Coq to do this.

Work in progress includes a GUI for view construction in Calculus of Inductive Constructions XML.

CSC What is your trust model?

A We cannot do general reasoning about computations in GAP. There is no model of the GAP programming language to use in Coq.

8.9 Efficient Formal Verification of Bounds of Linear Programs — Solovyev [SH11]

Related to section 5.1, but more general. The primal problem is to maximise $c^T x$ subject to $Ax \leq b$. The dual problem is to minimise $y^T b$ subject to $y^T A = c^T, y \geq 0$.

- Formally prove all constraints of the original problem.
- Numerically approximate (relax) the original problem. An approximation that loosens the domain and tightens the range implies the original inequality. $x - y \leq \sqrt{3}$ subject to $0 \leq x \leq \pi$, $\sqrt{2} \leq y \leq 2$ then we approximate (JHD disagreed with the details here). We actually relax to decimal numbers.
- Compute an approximate dual solution of the related problem (with an external solver). In Flyspeck we use `GLPK`. Take a decimal approximation $y_1^{(p)}$ of R with p decimal digits, then get $A^T y_2^{(p)} = A^T z - (v - v_e) + (w - w_e) = A^T y_1^{(p)} - e = c$. If $b^T y_2^{(p)} \leq K$ we are done, if not we use a higher precision.
- Construct a formal proof certificate
- Formally verify the relaxed problem and the original problem. So $y^T Ax = c^T x$ and $y^T b \leq K$. The problem here is that $n \approx 1000$. Hence we need sparse vector arithmetic in HOL Light.

In the implementation, a special routine creates approximated inequalities of the given precision from proved inequalities which contain transcendental constants.

To make this run faster, we use

- Integer arithmetic (rather than rational numbers): multiply by 10^{p_1} or 10^{p_2} as appropriate.
- HOL Light represented in binary (quite literally), with constants BIT0 and BIT1. Move to an arbitrary base, storing all the theorems about addition of digits in a has table.

  $14 + 7 = D4(D1(0)) + D7(0) = D1(SUC(D1(0) + 0) = \cdots = D1(D2(0))$.

  Moving to base 256 from binary got a factor of not quite 2.

JC Have you profiled the code? It doesn't look as if arithmetic is the bottleneck.

JHD It seems odd to use base 256 for this arithmetic, but decimal elsewhere.

8.10 Using Theorema for Formalization of Theoretical Econimics — Kerber & Windsteiger[KRW11]

These proofs in theoretical economics are typically undergraduate-level, but are error-prone.The aim is true automation (or at least minimisation of user interaction). Game theory is a major tool.

$\mathcal{X} \equiv \{\{x_i\}_{i\in I} | x_i \geq 0, \sum_{i\in I} x_i = 1\}$. A power function π satisfies

WC if $C \subset C' \subseteq I$ then $\pi(C, x) \leq \pi(C', x)\ \forall x \in \mathcal{X}$ (monotonicity)

WR if $y_i \geq x_i\ \forall i \in C \subseteq I$ then $\pi(C, y) \geq \pi(C, x)$ and

SR If $\emptyset \neq C \subseteq I$ and $y_i > x_i \forall i \in C$ that $\pi(C, y) > \pi(C, x)$ (strong monotonicity constraint).

WW then showed the corresponding formalisation (except everything written in terms of $\geq$).

Similarly define domination and a *core* as the set of undominated allocations.

Definition 14 *A set of allocations $S \subseteq \mathcal{X}$ is a* stable set *iff it satisfies*

internal stability $S \cap D(S) = \emptyset$

external stability $S \cup D(S)\mathcal{X}$.

These combine to give $S = \mathcal{X} \setminus D(S)$ and the core belongs to any stable set.

The Theorema is more complex here, as there are hidden parameters in the definition of domination.

$WIP_\pi[C, x] = \sum_{i\in C} x_i$ is the "wealth is power" view. Under this, the three-player game (with certain assumptions such as anonymity) has nine stable points: $(1, 0, 0)$ etc., $(\frac{1}{2}, \frac{1}{2}, 0)$ etc. and $(\frac{1}{2}, \frac{1}{4}, \frac{1}{4})$ etc. Existing work in economics had a pseudo-code "algorithm". The Theorema code looks rather different here, since the pseudo-code is in terms of if/then/else, which is case distinction in Theorema. Theorema might not be able to decide, e.g. if $M = \emptyset$, so the Theorema code looks like three-valued logic. In fact we had to help Theorema with two lemmas here.

$SIN_\pi[C, x] = \sum_{i\in C}(x_i + \nu)$ is the "strength in numbers" argument. If $\nu > 1$ then money is almost irrelevant, and we have a stable set. $0 < \nu < 1$ is different. These are shown with (assisted) Theorema. We did detect a mistake in the original algorithm. We plan to use the underlying Mathematics to compute solutions of sets of equations. In this context Theorema's mixture of reasoning and computation seems appropriate for the subject. This has been well-received by the economists (invitation to present at a research student summer school).

8.11 Calculemus Business Meeting

JC, as Calculemus Secretary, opened the meeting.

1. "We need a scribe" — JHD was volunteered.

2. Track Chair's report — WMF
   15 PC members (six new to this). We used rebuttal, summary reviews as needed, final reviews.n 15 submissions (and also three which were withdrawn), with 9 acceptances. In addition three were work-in-progress.

APS At MKM it was commented that maybe having unified submission dates was a problem. It was confirmed that this is impossible with an EasyCair multi-track.

3. Calculemus in CICM
   The Calculemus Trustess have unanimously approved the CICM Constitution. This states that the constituent organisations (e.g. Calculemus) are represented by a delegate. We propose to add to the Calculemus Charter

   > The MKM trustees appoint a standing delegate to the CICM Steering Committee. This delegate is **mandated** to vote on items that require a unanimity of CICM Steering Committee only in a sense that has the approval of an absolute majority of the Calculemus Trustees.

   The meeting approved this amendment unanimously.

MK This means that all four (AISC, MKM, DML and Calculemus) have accepted the Charter.

4. CICM 2012
   This will be in Bremen, with overall Programme Chair John Jeuring. The Trustees have selected Gabriel Dos Reis as Track Chair.

5. CICM Venue 2013.
   JHD had presented the Bath option at the CICM Business Meeting, but other suggestions (to the CICM Steering Committee) were welcome.

   Since ISSAC 2013 is at the end of June, early July seems like the obvious date.

6. Trustees
   There are currently twelve trustees (many more than MKM), and this is based on two track co-chairs every year, whereas there is now only one track chair. JHD's term expires, and he is on far too much already. The trustees propose to extend MW until 2013, and this will mean a single new election this year. JHD vigorously seconded this proposal, which again was carried unanimously.

7. Trustee Election
   The following had been nominated: JC, VS and JR, but it had tobe checked that they were willing to stand.

8. AOB
   IT was noted that the Calculemus track had been spread across the week, and it was asked that this be reconsidered. **JJ**

Bibliography

[ABMU11] J. Alama, K. Brink, L. Mamane, and J. Urban. Large Formal Wikis: Issues and Solutions. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 133–148, 2011.

[ADD+11] S. Autexier, C. David, D. Dietrich, M. Kohlhase, and V. Zholudev. Workflows for the Management of Change in Science, Technologies, Engineering and Mathematics. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 164–179, 2011.

[AKN+11] J. Alama, M. Kohlhase, A. Naumowicz, P. Rudnicki, Urban.J., and L. Mamane. Licensing the Mizar Mathematical Library. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 149–163, 2011.

[Ala11] J. Alama. mizar-items: Exploring fine-grained dependencies in the Mizar Mathematical Library. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 276–277, 2011.

[AMSC+11] A. Asperti, M.E. Maietti, C. Sacerdoti Coen, G. Sambin, and S. Valentini. Formalization of Formal Topology by means of the interactive theorem prover Matita. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 278–280, 2011.

[AS64] M. Abramowitz and I. Stegun. Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, 9th printing. *US Government Printing Office*, 1964.

[BBNS11] J. Borbinha, T. Bouche, A. Nowiński, and P. Sojka. Project EuDML — A First Year Demonstration. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 281–284, 2011.

[BCDJ08] M. Bronstein, R. Corless, J.H. Davenport, and D.J. Jeffrey. Algebraic properties of the Lambert W function from a result of Rosenstein and Liouville. *J. Integral Transforms and Special Functions*, 18:709–712, 2008.

[BGOBP08] Y. Bertot, G. Gonthier, S. Ould Biha, and I. Pasca. Canonical Big Operators. In O. Ait Mohamed, C. Mu noz, and S. Tahar, editors, *Proceedings TPHOLs '08*, pages 86–101, 2008.

[Bot11] F. Botana. A Symbolic Companion for Interactive Geometric Systems. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 285–286, 2011.

[Bro77] M. Brown. A short short proof of the Cartwright–Littlewood theorem. *Proc. AMS*, 65:372–372, 1977.

[BSSS11] J.B. Baker, A.P. Sexton, V. Sorge, and M. Suzuki. Comparing Approaches to Mathematical Document Analysis from PDF. *To appear in ICDAR 2011*, 2011.

[CFJ+11] J. Carette, W.M. Farmer, F. Jeremic, V. Maccio, R. O'Connor, and Q.M. Tran. The MathScheme Library: Some Preliminary Experiments. `http://arxiv.org/abs/1106.1862`, 2011.

[CFO11] J. Carette, W.M. Farmer, and R. O'Connor. MathScheme: Project Description. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 287–288, 2011.

[CHK+11] M. Codescu, F. Horozal, M. Kohlhase, T. Mossakowski, and F. Rabe. The LATIN Logic Atlas. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 289–291, 2011.

[CKS11] M. Cramer, P. Koepke, and B. Schröder. Parsing and Disambiguation of Symbolic Mathematics in the Naproche System. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 180–195, 2011.

[CL51] M.L. Cartwright and J.E. Littlewood. Some fixed point theorems. *Ann. Math.*, 54:1–37, 1951.

[CO00] O. Caprotti and M. Oostdijk. How to formally and efficiently prove `Prime(2999)`. In M. Kerber and M. Kohlhase, editors, *Proceedings Calculemus 2000*, pages 116–127, 2000.

[Dav02] J.H. Davenport. Equality in computer algebra and beyond. *J. Symbolic Comp.*, 34:259–270, 2002.

[DRML11] G. Dos Reis, D. Matthews, and Y. Li. Retargeting OpenAxiom To Poly/ML: Towards an Integrated PA and CAS System. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 15–29, 2011.

[DSS11] A. Distler, M. Shah, and V. Sorge. Enumeration of AG-Groupoids. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 1–14, 2011.

[fST10] National Institute for Standards and Technology. The NIST Digital Library of Mathematical Functions. `http://dlmf.nist.gov`, 2010.

[Gan09] M. Ganesalingam. *The language of mathematics*. PhD thesis, Cambridge, 2009.

[GSMK11] D. Ginev, H. Stamerjohanns, B.R. Miller, and M. Kohlhase. The LaTeXML Daemon: Editable Math on the Collaborative Web. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 292–294, 2011.

[Ham54] O.H. Hamilton. A short proof of the Cartwright–Littlewood theorem. *Canad. J. Math.*, 6:522–523, 1954.

[Har07] J. Harrison. Automating elementary number-theoretic proofs using Gröbner bases. In F. Pfenning, editor, *Proceedings CADE 21*, pages 51–66, 2007.

[HIJ+11] F. Horozal, A. Iacob, C. Jucovschi, F. Rabe, and M. Kohlhase. Combining Source, Content, Presentation, Narration, and Relational Representation. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 212–227, 2011.

[HJ11] Heeren and J. Jeuring. Interleaving Strategies. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 196–211, 2011.

[HPDR11] J. Heras, M. Poza, M. Dénès, and Rideau.L. Incidence simplicial matrices formalized in Coq/SSReflect. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 30–44, 2011.

[HW79] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers (5th. ed.). *Clarendon Press*, 1979.

[KI11] C. Kaliszyk and T. Ida. Proof assistant decision procedures for formalizing origami. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 45–57, 2011.

[KKL11] V. Komendantsky, A. Konovalov, and S. Linton. View of computer algebra data from Coq. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 74–89, 2011.

[KRSC11] M. Kohlhase, F. Rabe, and C. Sacerdoti Coen. A Foundational View on Integration Problems. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 107–122, 2011.

[KRW11] M. Kerber, C. Rowat, and W. Windsteiger. Using Theorema in the Formalization of Theoretical Economics. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 58–73, 2011.

[KUT+11] D. Kuehlwein, J. Urban, E. Tsivtsivadze, T. Heskes, and H. Geuvers. Learning2Reason. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 298–300, 2011.

[KW11] R. Krebbers and F. Wiedijk. A Formalization of the C99 Standard in HOL, Isabelle and Coq. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 301–303, 2011.

[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.

[Lib10] P. Libbrecht. Notations Around the World: Census and Exploitation. In S. Autexier *et al.*, editor, *Proceedings CICM 2010*, pages 398–410, 2010.

[MG11] J. Mišutka and L. Galamboš. System Description: EgoMath2 as a tool for mathematical searching on Wikipedia.org. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 307–310, 2011.

[O'C08] R. O'Connor. Certified exact transcendental real number computation in Coq. In O. Ait Mohamed, C. Mu noz, and S. Tahar, editors, *Proceedings TPHOLs '08*, pages 246–261, 2008.

[Pos46] E. Post. A variant of a recursively unsolvable problem. *Bull AMS*, 52:264–268, 1946.

[SH11] A. Solovyev and T. Hales. Efficient formal verification of bounds of linear programs. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 123–132, 2011.

[SK11] B. Spitters and R. Krebbers. Computer certified efficient exact reals in Coq. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 90–106, 2011.

[SL11] P. Sojka and M. Líška. Indexing and Searching Mathematics in Digital Libraries (Architecture, Design and Scalability Issues). In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 228–243, 2011.

[WAGD11] I. Whiteside, D. Aspinall, G. Grov, and L. Dixon. Towards Formal Proof Script Refactoring. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 260–275, 2011.

[Wen11] M. Wenzel. Isabelle as Document-oriented Proof Assistant. In J.H.Davenport *et al.*, editor, *Proceedings CICM 2011*, pages 244–259, 2011.

[Wie03] F. Wiedijk. Comparing Mathematical Provers. In *Proceedings Mathematical Knowledge Management 2003*, pages 188–202, 2003.

Appendix A

Dramatis Personae

APS	Alan Sexton	Birmingham
BM	Bruce Miller	NIST
CL	Christoph Lange	Jacobs University, Bremen
CSC	Claudio Sacerdoti Coen	Bologna
ES	Elena Smirnova	TI
JB	José Borbinha	EuDML
JC	Jacques Carette	McMaster
JHD	James H. Davenport	Bath
JJ	Johan Jeuring	Utrecht
JP	Jim Pitman	Berkeley
JU	Josef Urban	
MK	Michael Kohlhase	Jacobs University, Bremen
MW	Makarius Wenzel	INRIA
PI	Patrick Ion	AMS (emeritus)
SA	Serge Autexier	DFKI
TB	Thierry Bouche	Grenoble/EuDML
WMF	William M. Farmer	McMaster
WS	Wolfram Sperber	Zentralblatt