Notes at Conferences on Intelligent Computer Mathematics 2010

Partial notes by JHD
J.H.Davenport@bath.ac.uk

CNAM, Paris
5–10 July 2010

Abstract

If you read nothing else, read footnote 1 on page 10 to learn that, in Excel, 'paste' is *function application*.

The "impact police" might be amused by note 3 (page 57).

Updated 16.7.2010 to include some factual corrections by DPC to the OpenMath discussion (at which he was unable to be present).

Contents

Chapter 1

5 July 2010 — AISC 2010

1.1 A mathematical model of the competition between acquired immunity and virus — Mikhail Kolev

Good mathematical model can reduce the number of actual experiments required. The interactions between the infections and immune cells are highly nonlinear.

1.2 How to correctly prune tropical trees — Loddo

This turned out to be really about Minimax games. Many problems can be solved with a *non-deterministic* search. Tropical trees are a generalization of min-max games. They support "tropical α-pruning".

We believe that 'divide and conquer' helps. Example — non-deterministic parsing, as in `1+2+3`.

1.3 Artificial Intelligence Techniques on Biological Structures — Alexiou

1.4 Invited: The Challenges of Multivalued "Functions" — JHD

See `http://staff.bath.ac.uk/masjhd/Slides/AISC-handout.pdf`. In brief, JHD said that there were many views of such functions, including the Bourbakist, the multivalued, the Riemann surface, the branch and the differential algebra views.

MK asked whether we couldn't produce 'active' texts, that let a reader interacts with the text in *his* view.

JHD thought that this would be wonderful, but that, in view of his comments on the difficulty of inferring the views, such texts would need to be explicitly constructed.

SMW noted that the interval community also grapples with the problem of assigning consistent meanings[1] to symbols, and with set-valued objects.

JHD agreed, sand said perhaps what we could learn from them is that they do not *ask* for set equality: rather for set inclusion.

1.5 Automated Reasoning and Presentation Support for Formalizing Mathematics in Mizar — Urban (& Sutcliffe)

This work aims at providing a bridge between Mizar, ATPs and SystemOnTPTP (Sutcliffe). The input is a Mizar 'article', which can be XMLised (which in turn gives the HTML form). This can be done before an MPTP (Mizar Proof for Theorem Provers) format is exported. So, for example, clicking on a 'by' keyword causes translation to ATP format and a side-window explaining the results, e.g. "status countersatisfiable". Hints can be provided. The main gap is a suitable metasystem for ATP over large libraries.

1.6 Structured Formal Development with Quotient Types in Isabelle/HOL — Lüth

We think of a "design tactic" as formalising design knowledge. One difference might be a deep/shallow encoding. We are not interested in meta-theorems, hence we are *shallow*. We note that software development is *structured*, which similar to the "Little Theories" approach. Therefore we need to add structuring operations.

Isabelle has `theory` which `imports`. We want theory morphisms. We do this by *proof term transformation*, which is conservative over the logic kernel.

[1] JHD's classic example is that, if $x, y \in [0,1]$, then $x(1-y) \in [0,1]$, but $x(1-x) \in [0,0.25]$.

1.7 From matrix interpretations over the rationals to matrix interpretations over the naturals — S. Lucas

Motivations: proofs of termination. To $x \in \mathbf{Z}$, we associate $\mu_n(x)$ as $\frac{x}{n} I_n$ if $n|x$, and xI_n otherwise[2]. But there is no matrix representation of *all* unit fractions this way. Consider the nilpotent matrix J_n where $(J_n)_{i,j} = \begin{cases} 1 & j = i+1 \\ 0 & \text{otherwise} \end{cases}$. So J_2 might represent $\frac{1}{2}$. But J_2^2, which should represent $\frac{1}{4}$, is 0. So represent $\frac{1}{2}$ by $\begin{pmatrix} J_4 & J_4 \\ 0_4 & 0_4 \end{pmatrix}$ and so on.

There was a theorem dealing with transformation of *bounded* constraints.

1.8 Krawtchouk Polynomials, Matrices and Transforms — Feinsilver

One way of thinking of these is "symmetric functions of bitstrings".

As an example, $\begin{pmatrix} 4 & 2 & 0 & -3 \end{pmatrix}$ becomes (row of sums; row of differences) $\begin{pmatrix} 6 & 2 & -3 \\ 2 & 2 & 3 \end{pmatrix}$ becomes (row of sums — twice; row of differences) $\begin{pmatrix} 8 & -1 \\ 4 & 5 \\ 0 & -1 \end{pmatrix}$ becomes (row of sums — thrice; row of differences) $\begin{pmatrix} 7 \\ 9 \\ -1 \\ 1 \end{pmatrix}$ and this is the corresponding Krawtchouk vector.

1.9 Some Notes on "When does $\langle T \rangle$ equal sat(T)" — Li

Let $\tilde{K}$ be the algebraic closure of K (e.g. complexes). Let $\overline{S}$ be the Zariski closure of S in K^n. Note the concept of a triangular system (with parameters). $\text{sat}(T) = \text{Ideal}(T) : J^\infty$ where J is initials (JHD missed definition). Let $\text{Zero}(P/Q) = \{z \in \tilde{K}^n : p(z) = 0, q(z) \neq 0 \forall p \in P, q \in Q\}$.

We say p is **weakly primitive** if either $\text{lc}(p)$ is invertible and $|C(p)| = 1$ or, for any β such that $\text{lc}(p)|\beta b$ for all $b \in C_{\text{red}(p)} \ldots$. We introduce new concepts of **C-weakly primitive** and **C-primitive**.

[2] JHD worries about the ambiguity of this.

Chapter 2

6 July 2010 — AISC

2.1 The Dynamic Dictionary of Mathematical functions — Salvy

The project is formally three years old, but in fact some underlying ideas were at MKM 2001 (the first MKM) in Linz.

> Special functions: functions that have been met sufficiently often to deserve a name.

2.1.1 Background

Among the most cited documents in mathematics are [AS64] and [PBM83]. Both are the works of humans and contain mistakes, as, unfortunately[1], does [GR94].

Since these works were compiled, the world has changed, and computer algebra has arrived, and the Web has changed the way we interact with information. Notice also the NIST DLMF [Loz01, fST10].

Our system *generates*, rather than stores, its formulae, and can produce proofs. Our system is no surprise to those used to computer algebra systems, but there is no syntax to learn!

This is written in DynaMoW: Dynamic Mathematics on the Web — note that the computation tells you the **structure** of the document, e.g. the number of singular points, rather than just "filling in the slots". He demonstrated the proof that arctan is odd, and the source code that generated this.

2.1.2 Symbolic Computation

What does it mean to say that a traditional CA system "knows about exp"? Currently, it means bits of code scattered all over the system. We note that

[1] These are JHD's notes. JHD *thinks* that what was intended is that [GR94] conatins far more mistakes, which indeed his experience.

polynomials represent their roots better than radicals. More recently the same is being seen for linear differential or recurrence equations.

The major tools are:

1. Effetcive Majorant series
2. Efficient evaluations of truncated sereies
3. time complexity quasi-linear w.r.t. precision

Where necessary, the *user* has to specify an analytic continuation path. This lets one compute monodromy: he demonstrated integrating arctan round 0, to compute π.

We use algorithms for the hypergeometric case [Zei90] extended to the D-finite case [Chy00].

2.2 A Revised Perspective on Symbolic Computation and Artifical Intelligence —Calmet & Campbell

Calmet: Another title would be "why computation; why AI"? At the founding AI Meeting (Dartmouth, 1956) mechanizing mathematics *was* on the agenda. He claims that the DISCO conference was an attempt to integrate CA and CS, but that conference series has died.

Ontologies are everywhere (see success of Wolfram Alpha), but also a health warning. We aimed at a knowledge warehouse (KOMET porject) but these proved very hard to maintain. Hence a federated solution seems desirable.

Chapter 3

6 July 2010 — Compact Computer Algebra

3.1 Compensating the Computational Bias of Spreadsheets — Kohlhase[2]

In some sense this work is making computation *less* compact. If computer algebra has millions of users, spreadhseets have hundreds of millions. But most users deny they are programming, and ignore software engineering (even those, like the audience, who otherwise know it). Apparently there's a conference (in London this year) exclusively on spreadsheet errors.

Spreadhseets (and Maple worksheets etc.) are **active** documents, unlike most mathematics. Hence we need **semantic documents**. The key *implicit* concept is the functional block, e.g. `B17` might be a formula involving earlier `B` cells, and this can be pasted (i.e. re-applied)[1] to columns `C` etc.

Therefore need an *intention* layer, and a real ontology For the spreadsheet contains 27 theories about quantities, units and basic accounting. 20 union theories for our company semantics (mostly trivial). Also a dozen general mathematics theory, which are certainly re-usable.

By "semantic bias", we mean that ontology, provenance and interpretation are absent, and the bias is towards computation only (in fact, the same bias is also present in computer algebra systems). A pre-requisite would be a certain amount of semantic transparency.

Q.–JHD You said that this level of semantics was probably not needed for grade books, I have been looking at my[2] 1.5MB grade book, with comments to Senate minutes, Maths Teaching Committee decisions etc., and

[1] JHD admits that he had never thought of 'paste' as being function application, but, now that the point is made, he feels like M. Jourdain, who had been spekaing prose all his life without realising it.

[2] XX10190

I disagree

A. I can live with that.

3.2 MathPASS: A Remedial Mathematics System with Concept Checking — Wei Su (and Paul Wang)

This is a drill-and-practice system used in remedial mathematics at KSU[3] — 100 teachers and 6000 students, with about 1.2M assignments taken. A typical question is "expand $\left(\frac{\cdots}{\cdots}\right)^{-2}$".

The model is based on 'experts' creating question prototypes, and the teacher selecting from these. Over 400 have been created. Examples would be

Description	Prototype	Instantiation
same denominator	$\frac{A}{B}+\frac{C}{B}$	$\frac{1}{7}+\frac{2}{7}$
denominator divides	$\frac{A}{B}+\frac{C}{D}\ (D\%B=0)$	$\frac{1}{4}+\frac{7}{12}$

MathPASS is written in JavaScript and MathML.

Mathematical Answer Checking protocol (MACP) is an access protocol for communcation between service and client. Service might be a CAA system or other implementation. It is based on REST (Representation of State Transfer). The request data and service response are encoded in JSON. The current service is Maxima to verify expression equivalence. He showed the data format of an MACP query and response. There is a mixture of (presentation) MathML and infix notation (JHD wasn't sure of the distinction), but later on there was also some MathML Content. The system distinguishes the two (extensions `.mmlp` and `.mmlc`).

When can we say if an answer is "right"?[4] Obviously the answer is wrong if the computed result is not CAA-equivalent. But we have hundreds of e-mails from students saying that the answer is correct, but the system graded them as wrong. Equally there are teachers who say that answers marked as right should have been marked as wrong. Suppose $\frac{5}{6x^5+y^8}$ is **the** correct answer: what do we then do about $\frac{5}{6}\frac{1}{y^8x^5}$, or $\frac{5x^{-5}}{6y^8}$?

There are two classes of "correct answers" — simplest form and special syntax form. This isn't a complete distinction, but seems to be helpful in evaluating the answer and resolving the issue of partial credit.

3.2.1 Full simplification form

Questions in this category include expansion etc. We work as follows:

[3] Kent State University — Paul Wang's institution.

[4] The speaker seemed ignorant of the discussion of this question in [BDS09].

1. judge algebraic equivalence in CAS
2. convert answer to canonical form
3. judge whether it is equal to the simplest form
4. assign grades.

Simplest Natural Numbers, Simplest Primary etc., are defined.

3.2.2 Special Syntax Form

Examples are multiplication of polynomials, sum or difference of logarithms etc. This kind of answer should not be simplified as above. These are defined in terms of a Mathematical pattern language. An example is `2+x^$` (`$` being a pattern-matching variable).

Further work would include adding geometry questions to MathPASS.

Q. (Bastiaan Heeren?) Do you allow questions such as "write the equation of a line" etc. Also, for easy questions it is important to get the answer in the correct format, but for more complex questions this is less important: can you handle this gradation?

A. The first question was not clearly understood (nor the second).

3.3 Demonstration of MathEdit — Wei Su

A browser-based Visual editor for Mathematical Expressions. `http://mathedit.lzu.edu.cn`. It's a template-based editor, and apparently the list of templates *is* extensible. Generated MathML *and* OpenMath, LaTeX. There is also a linear syntax. which constructs a similar template-like creation.

Seven lines of code will embed MathEdit in a web page.

Q.–MK Is the MathML extensible?

A. It is Open Source code.

3.4 Compact CAS: behind the scene — Watt & Smirnova (double speaker)

What do we mean by compact? In real analysis, we mean closed and bounded, and this really applies to CCA as well. In topology we mean that we can have finite subcovers.

Inspired by this, we note that general CAS have problems with intermediate expression swell, and are generally open-ended, and *can be* very large.

In CCA, we tend to want output size to be bounded by some multiple of input size. One problem we face with hand-held devices is the limited size of

the keypad. Apparently[5] the U.S. requires `ABC` keyboards rather than `QWERTY`. Pen-based interfaces are coming. She claims that there is a spectrum: keyboard ⇒ mouse ⇒ pen ⇒ voice, with increasing usability **and** ambiguity.

But do we not want such manipulation as well, e.g. dragging terms around an equation. We could also use a CAS for validation, so that $\frac{\partial F}{\partial 2}$ bcomes corrected to $\frac{\partial F}{\partial z}$.

We should have more suppport for mathematics, e.g. equation line/page breaking (this can be done for joint English/Arabic, so why can't we do maths?). "Compact" really means 'bounded ambitions'. It also allows **complete** handling of restricted sets of problems.

Q.–MK It seems to me that 'compact' means 'embeddable', at least for you.

A. Not necessarily, but most of the constraints we have mentioned (human-targeted, accessible, good housekeeping, well-defined error reporting, how to fail with grace etc.) are useful (even necessary) for embeddability.

[5]This is JHD's undestanding of what was said, but this may be a *de facto* requirement rather than *de jure*.

Chapter 4

6 July 2010 — Calculemus

4.1 Reducing expression size using rule-based integration — Jeffrey (& Rich)

DJJ pointed out that ADR is the prime mover. `http://www.apmaths.uwo.ca/~arich` describes the rule-based mathematics he is promoting. Their test suite amounts to 9428 problems, with Maple 13 being optimal on 60.2% ('messy' 28.2% and unable 8.9%, with 'invalid' at 2.9%), Mathematica on 74.8% ('messy' 23% and the rest pretty small). All the rules are available on the above-mentioned URL. The programs (`Rubi`) are currently written in Mathematica.

At CICM 2009 [RJ09], we had a three-fold classification:

1. Lookup tables
2. Rule-based
3. Algorithmic (not being displaced, but should be kept for the really hard problems).

Fateman, changing his mind since 1979, "there's no arguing with success".

How does this work? A rule consists of **N**ecessary conditions, **T**ransformation rule and **S**implification conditions. The implementer can pay special attention to

1. Reducing output size/complexity
2. Raising the aesthetic level of the results (in particular making the results as symmetric as possible between inverse trig and inverse hyperbolic)
3. reducing the number of steps required
4. increaing the ratio of integrals solved to database size (knowledge density).

Consider $\int \frac{x^m dx}{(1+x)^{12}}$ for different m.. Both Maple and Mathematica have a simple(ish) curve, whereas Rubi has a major dip at $m = 10$, and in $0 < m < 10$ we choose the smaller of the alternatives.

Similarly consider $J(m, n, p) = \int (x-a)^m (x-b)^n (x-c)^p \mathrm{d}x$. There is an m-reduction rule as $J(m, n, p) \to \frac{1}{b} J(m-1, n+1, p) - \frac{a}{b} J(m-1, n, p)$, but this can be pretty inefficient.

Q.–ES How do you know which rule to apply?

A. *In principle* the N+S pairs are mutually exclusive. However, we currently have no tools for verifying this.

4.2 Symbolic Domain Decomposition — Watt (& Carette, Sorge, Sexton)

The main idea is that many problems are defined on a domian which is the union of parts. We want to express these conditions symbolically to avoid the combinatorial explosion. We do this with hybrid sets (multisets with negative multiplicity) and work with a single generic case, and claim that this unifies a number of previous ideas.

SMW interested in symbolic polynomials

VS/AS interested in symbolic matrices. Particularly interested in D^2+L+L^T etc.

Consider $f(x) = \begin{cases} 2(a^2-a) & x < a-1 \\ x^2 & \text{otherwise} \end{cases}$ — delaing with this is hard. Consider $U = [a_1, \ldots, a_{h-1}, b_h, \ldots, b_n]$ and $V = [c_1, \ldots, c_{k-1}, d_k, \ldots, b_n]$. Then$U + V$ is a mess.

$$[U+V]i = \xi_{i,1,k}[a_i + c_i] + \xi_{i,k,h}[a_i + d_i] + \text{third term}$$

where ξ is the appropriate choice function (0 or ± 1)..

What is really going on is that we have an asscoiate operatorwith an inverse,and we're abusing this **Z**-module structure to do our book-keeping. The same abuse takes place when we integrate over oriented volumes. This also has problems where the function being integrated might not be defined.

4.2.1 Hybrid sets

"We might need to take things out before we put them in". Use $\otimes$, $\ominus$ and $\otimes$ rather than $\cup$, $\cap$ and$\backslash$. Can define hybrid functions, which can be, essentially, joined. "Essentially, this is pieces with functions, rather than functions with pieces". Can therefore get hybrid partitions.

Consider Let A_1 be evens and A_2 be odds. Let B_1 be negatives a,d B_2 be non-negatives. Can represent this as **three** sets:

$P_1 = A_1$

$P_2 = B_1 \ominus A_1$

$P_3 = B_2$

More generally, $m + n$ parts rather than mn.

Symbolic structured matrix arithmetic is one application. This gives us a single expression for a generic case, which makes the structure clear, and the result has linear size, and has linear evaluation time.

Q.–Salvy Could this be applied to `assume`?

A. We hadn't thought of that, but it's a good question.

4.3 A formal quantifier elimination for algebraically closed fields — Cohen & Mahboubi

"Computer Algebra systems allow us to formalize, encode mathematical objects, and compute [with them]". Our language will involve the four arithmetic expressions and the Boolean operators. No quantification on predicates, functions or families. Since we can't do this, we can't write that any non-constant polynomial has a root. Hence we add an **axiom schema** for this to the field axioms. This can be formalised in Coq. Hence we need a program `q_elim` **and** a prof of its validity. It is sufficient to have `proj` that eliminates x from $\exists x \phi$. We can furthermore assume

$$\exists x \wedge_i p_i(x) = 0 \wedge \wedge_j q_j(x) \neq 0.$$

This looks trivial in terms of gcd etc., but gcd is not first-order. Hence we use continuation-passing style. We have the procedure, and its proof. Unfortunately, it does not run in reasonable time[1], since division, gcd etc. are naïve. We would like to use this trick for real closed fields as well.

4.4 Formally verified conditions for Regularity of Interval Matrices — Paşca

Introduction to interval arithmetic, e.g. $-pi \times \sqrt{2} \in [-4.473, -4.4274]$. **IR** is the set of intervals $x = [\underline{x}, \overline{x}]$. An interval is **thin** if $\underline{x} = \overline{x}$, otherwise thick. However, we only have machine numbers, hence need $\diamondsuit$ as our rounding operator.. There is much use of interval arithmetic in proof assistants. Use x_c for the centre of x, i.e. $(\underline{x} + \overline{x})/2$.

[1] According to a subsequent conversation GG/JHD, this isn't the point. Continuation-passing produces a natural style for the algorithm and its proof, and it is then much easier to prove subsequently that a more efficient algorithm is equivalent to this one, rather than (GG contrasted this talk with the SCHUR talk later) prove an efficient algorithm correct from first principles.

4.4.1 Interval linear algebra

Would like to use interval analysis in robotics. There is a two-phase method

1. Check that the associated interval matrix is regular (all matrices in this interval are non-singular)
2. Need **bounds** for the solution set (which may be larger, as a box, than the true interval solution, which might be star-shaped for example.

By solution, we mean $\Sigma(A,B) := \{x : \exists a \in A, b \in B : Acx = b\}$, but in fact we will compute $\diamondsuit\Sigma(A,B)$.

Theorem 1 $\Sigma(A,B) := \{x : Ax \cap B \neq \emptyset\}$.

Note that in Coq we will need a **proof** that $\underline{x} \leq \overline{x}$ as well. Note that $-x + x \neq 0$ if x is thick, hence we don't have a ring. In particular, this means we can't re-use the Coq libraries of matrices for our interval matrices.

Need to use Rayleigh quotients, and the Perror-Frobenius theorem (for a real nonnegative matrix, there is a real nonnegative eigenvector corresponding to the spectral radius — largest eigenvalue in absolute value).

4.4.2 Regularity

Criterion 1 *A is regular iff* $\forall x, 0 \in Ax \Rightarrow x = 0$.

Criterion 2 *another one*

But these are of little use in practice.

Criterion 3 *In terms of A_c*

But would like a criterion in terms of $\diamondsuit$ arithmetic.

4.5 Formal proof of SCHUR conjugate function

SCHUR is a 20-year old C (automatically translated from Pascal!) program, but notw under GPL. It is in algebraic combinatorics. We will extract one key —C function, try to prove it, then deduce some general principles. Our tool is Frama-C/Jessie (a successor of Caduceus). Jessie generates verfication conditions from first-order logic annotations (Hoare logic).

The combinatorial objects and integer partitions, which can be represented by Ferrers diagrams. They have an important rôle in group representation tehory. Given a partition λ, we can build a Young tableau by numbering the boxes under increasing conditions. For a semi-standand Young tableau T of shape λ, if X^T is the product of all x_i for integers i appearing in T, then the Schur function is

$$s_\lambda(\mathbf{x}) = \sum_{T \text{ of shape } \lambda} X^T.$$

A common function is that for computing the conjugate of a permutation, e.g. $(3, 2, 1, 1, 1) \to (5, 2, 1)$ (draw the boxes). The naïve implementation is pretty inefficient. The efficient version is 15 lines of uncommented C, with two nested loops. It is implicit that no integer overflow is allowed. Needs four lines of preconditions (one of which is the output array is pre-initialised to 0 — not evident), a side-effect declaration, and a post-condition. The loop invariants alone double the size of the program.

Among the conclusions was that some versions of CVC3 (one of his four checkers: none of them will prove all the assertions, but `simplify` does the most) actually have bugs. Would like to go further, e.g. Littlewood–Richardson coefficients, Kostkas numbers etc.

Q. How much did the code grow?

A. It's hard to say — many of the predicates were placed in separate files, and should be reusable.

Q. Did you find Frama-C restrictive — many of your assertions look very like the algorithms.

A. This is probably inevitable when trying to prove some-one else's algorithm.

4.6 Calculemus Business Meeting

SMW chaired the meeting, and described the agenda. JHD took the minutes by default.

4.6.1 Report on Calculemus 2010 — RR

RR stated that Delahaye has done most of the work, and, in line with the call at previous meetings for "new blood", he should give the report. DD then reported.

16 papers were submitted, but two withdrawn. of the 14, seven were selected as full papers. There was also a paper transferred to PLMMS. This does raise questions about overlap of Calculemus/MKM/PLMMS/ etc. LD reported that last year (there wasn't an AISC last year) was 10 out of 17. It was noted that Calculemus (as a conference) had survived the demise of Calculemus (the EU project), which was itself remarkable.

RR said that SMW had helped him with the finances for CICM. There will be 110 paying registrants for CICM, up from last year's 80[2]. He attributed this rise to the addition of AISC this year, but MK thought that moving back to Europe might also have helped. One problem had been that the registration site could not be openened as early as RR had hoped, which meant that 'early bird' registration has to be open for longer than was desirable. RR stressed his

[2]But SMW noted that 80 mas the per-day maximum, and 110 was the total number of distinct people at 2009.

willingness to help next year's organisers with the administrative history. SMW reported that 2009 had sold 433 lunches, which was one crude estimate. MK asked whether CICM would break even, and RR thought that, once promised grants had rolled in, this would happen.

MK moved a vote of thanks to RR, LR and the team, which was passed by acclamation.

4.6.2 Calculemus constitution

SMW opened the discussion by noting that the coincidence of Calculemus and MKM at RISC–Hagenberg in 2007 had led to an informal confederation in 2008 and 2009. SMW's experience (as local organiser in 2009) was that the administration through several distinct steering committees had been difficult, and the pain did not seem worth it.

RR reported that the 2008 system of separate registration had been a mess, and he was grateful to SMW for suggesting that 2010 adopt the 2009 system of global and *per diem* registration. He would strongly recommend this for the future.

The MKM and Calculemus trustees had discussed the formation of a more formal combined institution. MK displayed the proposed constitution for CICM, and mentioned LD's addition of a common submission date (for full papers). There would be one general programme chair, chairs for each tracks[3] and an overall programme committee. One question for DML has been the fact that CICM has archival proceedings but DML does not. However, MK noted that Calculemus has 'emerging trends' papers, and MKM has presentation-only papers, so this did not seem insuperable.

He opened the meeting for comments. WW asked about workshops. RR reported that Springer were unhappy about adding new components to the proceedings. SMW stressed that there were two different aspects: proceedings and meeting organisation. As far as the organisation was concerned, he rather thought that the Organising Committee should incorporate a representative from each workshop, as had happened in 2009.

This proposal was adopted *nem. con.*

Trustee nomination SMW noted that the ratio of trustees to accepted papers was rather high for some existing meetings, and we should consider whether separate trustees were necessary. MK said that it was unwise to do two changes at once, though he would be delighted to propose the abolition of separate trustee boards once CICM was established. This was seconded by several others, and SMW was glad to let the proposal lie on the table.

Calculemus trustees should be nominated to the meeting secretary (JHD). In line with tradition, these are due by the end of the meeting, which JHD interprets as **15 July 2010**.

[3] Calculemus, MKM, AISC if they were involved, and possibly DML.

4.6.3 Meetings for 2011/12

It was the wish of the trustees to move to a system where we had plans two years in advance. WW noted that organising a conference could be fun as well! Expressions of interest for either 2011 or 2012 should be given to SMW or MK.

Chapter 5

7 July 2010 — Calculemus

5.1 Sone Considerations on the Usability of Interactive Provers — Asperti (& Sacerdoti Coen)

5.1.1 Historical Considferations

One of the first examples is Jutting's [Jut77] forrmalisation of [Lan30].

How can we measure progress:

1. Compilation time
2. de Bruijn fatcor
3. formalisation cost

none of which are quantifiable and intrinsic.

How long to verify [Lan30]?

1979 13 minutes

2002 0.6 second

This factor of 2^{12} is no more (indeed possibly less) than we would expect from processor speedup. Indeed application 'improvements' absorb handware improvements like sponges!

What about the de Bruijn factor?

- For [Jut77], This has been measured as 3.9 (or 3.7 if zipped).
- Mizar's CCorn is 4.0 (Wiedijk),
- elementary proof of the prime number theorem (5.2–17.8),
- analytic prime number theorem (Harrison) 9.0,

- Bertrand's postulate [AR09] 17.7.

What about formalisation cost?

- For [Jut77], about 1 week/page.
- Hales [Hal08] quotes the same.
- Wiedijk (unpublished) quotes 1.5, which matches [AR09].

OK, so none of these are improving, *but* we can deal with more complex mathematics [Gon08, Hal07]. a pessimistic interpretation would be that this is due to external factors. His conclusions are that the de Bruijn factor is already low — the real problem is the formalisation costs, which needs an order-of-magnitude improvement, e.g. to 1 page/day. To do this we need to improve usability. We claim that these programs are *interactive* theorem provers, but there is in fact not much dialogue.

5.1.2 Future Perspectives

On one example[1], 1182 theorems, he had 33% use of `apply`, 16% `rewrite`, 13.3% `assumption`[2], 11.4% `intros`, 7.4% `cases`, 5.1% `simplify` and the rest less. There were 22 tactics/theorem.

He had a cruder classification: `rewrite` and `apply` use **global** knowledge (amounting to 49%), while all teh rest are local. Mostbresearch is focused on the local aspects, but these are *not* the points where we expect machine help.

In Matita [SCT09], with some automation, the number iof applications goes from 629 to 148, and so on. He would like to promote the study of automation with large knowledge bases. he quoted the Constable programme (1986) "The natural growth for a system like Noprl tends towards increased inetlligence. ... Hence there is an impetus to give the system more knowledge about itself".

Q.—DZ Have any **new** results been proved this way?

A. AA: no. Floor — some cases in specialised algebra. Also GG's proof of the four-colour theorem [Gon08] is genuinely *different* from the previous methodology.

Q.—LD How do we know if we're making progress? Your work is good but needs formalisation. Also, it's not fait to say that there has been little progress in systems: Isabelle 2 has *much* better search techniques for examplel

Q.–MK Has anyone measured the *human* de Bruijn factor: the time it takes a human to understand a piece of mathematics. It probably takes me 1 day/page to read *research* mathematics. After all, some of this must take place during teh formalisation process.

[1] This provoked substantial debate. In particular, it wasn't clear to GG where 'forward chaining' appeared.

[2] This is basically redundant — saying 'I have done it'.

A. Not that I know.

5.2 — Rubio

Our aim is to formalize smome algorithms implemented in Kenzo. This can compute homology groups The frist milestone was a mechinised proof og the Baic Perturbation Lemma (in Isabelle/Coq). Now being attempted in by Coquand and Spiwack. We need a hierarchy of (graded and infinite) data structures. We build on CoRN (but use setiods without apartness). We use the formalisation of Modules by Pottier, which we have extended to graded strcutres.

Definition 1 (Sergeraert) *A r*eduction *is a 5-tuple* (TCC, BCC, f, g, h) *with* $f : TCC \to BCC$*,* $g : BCC \to TCC$ *and* $h : TCC \to TCC$ *with compatibility constraints.*

From this, we can build the **effectie homology** data structure. But computing with instrances of infinite type is in general undecidable.

5.2.1 Conclusions

- We have formalised a hierarchy of data structures
- Provided some proofs and some instance sof the structures
- We can relate computing and deduction.
- we are ready to rebuild using new formalizatuin tehcniques in CoRN and.or ssreflect.

Q. ssreflect is very much at the decidable end[3], so how will you use it?

A. Future work.

5.3 A Unified Formal Description of Arithmetic and Set-theretic data types — Tarau

Axiomatizaions of various formal systems are generally expressed in classical or intuitionistic predicate logic. We will use λ-calculus and type teory as porovided by Haskell. Type classes are seen as (approximations of) axiom systems.

We represent **N** as bitstrings by removing the bit indicating the leading power of 2 from $n + 1$, hence 1=`0`, 2=`1`, 3=`00` etc. Hereditary finite sets are represented by the Ackermann mapping. Claimns that arithmetic is O(size).

[3]Seconded by GG.

5.4 What are the rules of elementary algebra — JHD (& Sangwin)

See `http://staff.bath.ac.uk/masjhd/Slides/CICM2010-Sangwin-handout.pdf`.

5.5 Evolution of Documents — Lange *et al.*

Claims that Web 2.0 should allow collaboration on **content**. Mathmatical content is typically hierarchical. Therefore we want users to be able to

- customise the display
- customise the notation C_n^k or $\binom{n}{k}$ etc.

We use Wolfram Alpha as our test case. Rely on SCIence to produce the interoperability architecture.

5.5.1 Wolfam Alpha

Was launched in May 2009. Is intended to merge CAS and a proof engine. We nnat to embed its capabilities in our JOBAD. We could do this by scraping (but the images are deleted rapidly, etc.), but in fatc there is also an API. MathDpox provides our OpenMath $\leftrightarrow$Mathematica translator, but the reverse connection needs more work, so we currently just display the output.

Q. Is it possible to embed the OpenMat?h

A. Not inside the PDF, only at top level.

A.—JHD Ross Moore has incorporated MathML inot individual formulae of a PDF, so it should be possible to do more.

Q.—BM Obviously you pucked a simple example for the demonstration: in real life, one would have a lot of context.

A. Good question.

5.6 Demonstrations

5.6.1 Visualising Data Type Isomorphism — Tarau

In Mathematica (not Haskell this time).

5.6.2 The FOCalize environment: Certifying polynomials — Rioboo

History: FoC, FoCaL, Zenon, ...

All statements must ultimately be Coq proofs. We now have structural induction in Zenon. Many statements end up being curried.

Q. How do the times compare?

A. One has to compare systems with a consistent algorithm, which is a problem. It compares reasonably with Axiom.

5.7 Mathematical Formulae recognition and logical structure analysis of mathematical papers — Suzuki

5.7.1 The OCR Problem

He characterised major problems as the following.

- variety of rare symbols
- detection of Fonts
- Segmentation of touched and broken characters
- stabe structural analysis of mathematical formulae against misrecognition of characters
- Distinction between noise and small symbols.

Detection of structural data (author, ttitle, section, theorem itemization etc.). This is currently done with line characterizatipn, but we need stronger tools.

5.7.2 Formula Recognition

Based on a lot of data, defined a 'cost functon' for each possible link between adjacent symbols e.g. alphabetic folloed by raised digit). Then want the minimum-cost spanning tree. Since this is NP-hard, use beam search.

5.7.3 Bulk digitisationn

In this case, an adaptive method is efficient, incorporating some manual checking (? and training). The `InftyReader` oftware can be downloaded from `http://www.inftyproject.org`. Also a 'Pro' version, and the `BatchInfty` product.

We still have problems with old (lower-resolution) scans, and old books produced in typescript (subscripts aren't smaller). We also need to improve logical structure analysis (even with manual correction).

Q.—AS You have placed a great deal of emphasis on speed — is this really important.

A. Essentially the choice is P/NP.

D.—SMW Is there any analysis of how well your systems performs on different areas of mathematics.

A. We haven't thought about this, yet.

Chapter 6

7 July 2010 — Doctoral Programme

6.1 So the thesis is going well: what else should I do with the work I've done? — JHD

See `http://staff.bath.ac.uk/masjhd/Slides/Doctoral-handout.pdf`. This referred to [McD81, PP05]

6.2 Managing geometric knowledge in Textbooks

Wants an electronic geometry textbook as his thesis project. He is interested in

- sharing
- modifying
- querying

geometric content.

Demonstration. Creates a demonstration. The book is created hierarchically: first a chapter, then a section, then a theorem. The theorem has both natural and formal representations. There is a diagram, which *seems*[1] to be generated from the formal description — GeoGebra is used for the drawing. The system is multi-lingual, and one can change the language (he demonstrated English and Chinese) dynamically.

A typical relation might be `on.circumcircle(...)`. There is an inheritance behaviour for properties of geometric objects. Importing from other books will

[1] There are tt autoprove and `autodraw` buttons.

warn about unimported dependencies (the author then has to choose *where* they should be imported to in the new structure, but the system tracks logical dependencies and warns for inconsistenicies in the order). Cited some work by Dongming Wang, apparenly about degeneracy constraints.

6.2.1 Conclusions

We can

- construct such textbooks dynamically
- Maintain consistency and dependencies.

JHD's remarks. The demonstration was a little clunky: there was no need to start from a blank sheet. "here's one I prepared earlier" works. It wasn't clear to what extent the diagram was automatically produced. The relationship with Dongming's work wasn't clear.

Q. Is there an automatic way to add content, e.g. from a PDF book?

A. No — the content must be written via the interface.

Q.–CL I am impressed by the richness of the features, buw what is the research question? Also, what is/will be the user evaluation. I was late in realising that I needed to do an evaluation.

A. He haven't really done much evaluation yet.

Q.—VS What is the interaction with Paul Libbrecht's ActiveMath?

A. I don't know — VS will introduce.

Chapter 7

7 July 2010 — Digital Mathematics Libraries

7.1 PD Enhancement Tools for a Digital Library — Hatlapatka & Sojka

He showed a slide showing great compression. JBIG2 gives a standard (ISO/IEC 14492) forcompression of bi-level images. It is good for scanned text. It doe smulti-page compression, and a symbol copding for text. It segemnts each page into regions. This has been supported in PDF since 1.4 (Acrobat 5). A similar tool is used in DjVu.

Our tool is Pdfjblm. This is a PDF re-compressor. It recompresses the bi-levle images in PDF dcuments. Uses the open-souce JBIG2 encoder tha the library Leptonica for manipulating images. This cojmpares all templates (representtaive symbols) with the same size for finding equivalence. Two templates are considere equivalent if there is not a big enough accumulation of differences.

When from 1.424 kB to 1.128 with pdfJbl, 733 with pdfsizeopt.py, and 618KB after both.

7.2 Metadata editing and Validation in a Digital Mathematical Library — Růžička *et al.*

The metadata editor was developed as part of DML-CZ. It's a client-server web application. One source of articles is retro-digitisation, others come from retro-born digital and source format documents. From retrodigitisation sources, one has to separate pages into articles. Harmonisation of author names is performed.

"The viability of a digital libary rests with new acquisitions emerging mainly in the form of born-digital publications". Therefore there is need for validation of incoming metadata. The TEX appearing in metadat has to be validated. The

ditors themselves need feedback, so this has to be an on-line application.

The metadata is XML, so we can use the XML schema to generate the editor (via a Perlscript which generates javascript). This runs in the end-user's browser, and generates a form that matches the XML Schema. As part of Eu-DML we have internationalised and localised this editor (via HTTP/1.1 `Accept-Language` header, but not all browsers support this, or IP address localisation tools — again not perfect).

7.3 Implementing Dynamic Visualisatution —

DML-CZ has 28,000 articles in 11 journals, 5 proceedings series and 28 monographs. How is this browsed and searched? There is a standard search interface — this presentation is about an alternative. One sign of the screen shows the classical 'list of artucles' view. If one clicks on an author or article here, one gets a visualisation of the graph from that author/artuicle, with 'mouse-over' for nodes or edges in the graph. One can zoom in/out on this graph. What relationships to display?

- Structural (article in a series) – probably the least useful.
- semantic (classification)
- mixed (e.g. same author)

The technology is an RDF graph returned by a SPARQL query from the Joseki RDF server. We add MSC classification, as in `http://msc2010.org`.

7.4 Data Enhancement in a DML — Růžička *et al.*

The quality of a DML depends on the quality of the data it offers, but the viability depends on new acquisitions. Our first approach was complex, based on CEDRAM. This was basically too complex for a small editorial office. Not all editors are ready to use LaTeX. We now have a two-phase process. Journal-dependent article processing (which also geneates `article.dml.tex`). This is input to the second phase, which is journal-independent, and is processed by TRALICS.

```
\documentclass{dmlcztralics}
...
```

TRALICS is a LaTeX to XML translator which is the most indeispensable part of the system.

```
<article>
  <title lang="eng"> ,,, </title>
  <author> .. </author>
</article>
```

In particular, theere is no need for BibTeX. the metadata is generatwed *at the same time* as the article is processed. Since TRALICS supports MathML, we get this as well.

PDF is a very widely used framework. Thanks to podfTeX, PDF is also the *de facto* standard. The `ActualText` command of the PDF language is used to mark the region of the mathematical expression inside the LaTeX dcument. We use `\pdfliteral` at the beginning and end of every mathematical environment. Alas, simple redefinition of ASM-LaTeX is not possible.

Q.—JHD How doe sthis work compare with Ross Moore's?

A.—PS This is much simpler than what Ross is doing. We just redefine the environment to grab the source code and place it in the PDF.

Q.—TB Much of text processing you are doing is macro-based: is this the right direction given the nature of TeX's macros?

A. JHD: there didn't seem to be much of a discussion here.

Chapter 8

8 July 2010 — Plenary

8.1 — Carette

We are not talking about a robot that will do "all of mathematics": want we want is tools that can automate the automatable part, to "leavemore time for thinking". CA vendors will try to sell us a racing car (the fact that it looks like a car, but is actualy held together with duct tape, is embarrassing), whereas what we want is a tool kit.

8.1.1 Expressions are Syntax

This has been known by mathematicians for so long that they seem to have forgotten it. Furthermore, some expressions are meaningless. `diff` operates on expressions: $\frac{\partial}{\partial x}$ acts on functions $\mathbf{R} \to \mathbf{R}$.

8.1.2 Duplication is Evil

But we need many flavours to please the user.

8.1.3 Non-choices

Efficiency, correctness, abstraction, modularity and usability are now non-negotiable. I can do any pair, but the triples are still ard.Our tools are rowing: denotational semantics, code generation, polymorphism, first-class syntax (Unicode — see Agda), universal algebra, type theory etc.

We have to use structure. Universal Algebra will tell us how to define `sub`xxx, free structures etc.

Generic and Generative programming started out in computer algebra, but essentially died out there, and has been taken over by the C++ people. Maple has 80 different implementations of Gaussian Elimination and LU Decomposition, mostly for "efficiency" reasons. Essentially, what has to happen is that these inner loops have to be generated, not written. Did this in MetaOCAML,

and in some cases the generated code was *identical*. He showed an instantiation example — pointing out that we often get type errors, or errors at generation time, rather than run-time errors. However, it is worth noting that the design space for LU-decomposition is $\geq$ 24-dmiensional.

On a more trivial level, logging code just disappears whe not wanted.

Note also that the way this is structured lets us *design* partial evaluators..

Using biform theories, in Chiron, we can try to say that the evaluation of `diff` is $\frac{d}{dx}$, but "is" means "is equal to where one or the other is defined". It's also not often true, unless we have a precondition of 'differentiable'.

Q.—LD This all looks very difficult and abstract.

A. As long as it's only the system developer (i.e.myself) who suffers, I don't mind!

Q.—SMW In the context of Gaussian elimination, how do you handle movement at run-time within the design space?

A. This is possible, as another design variant.

Q. When will you allow further developers?

A. Once their pain pain becomes bearable.

8.2 Can we make mathematics universal as well as fully reliable — Cartier

Claim that we are at a turning point.

8.2.1 Unicity and Universality of Mathematics

There is a long debate over Pure/Applied (in his opinion a futile distinction), and many departments of mathematical science**s**. Look at the history Greece/Europe, or China (much more algorithmic) and India. Unitf of notation is prely a stepping-stone here.

8.2.2 Encyclopedias

Descartes, Diderot, etc. Then the 19th century traidtions of "Traité d'Analyse": Cauchy first, then Jourdan Goursat etc. Felix Klein and the German encyclopediac tradition. This inspired Bourbaki[1]. The founding fathers of Bourbaki, Weil, H. Cartan, went to Germany. This was more ambitious, not merely an exposition of what was already known, but a formal demonstration of unicity, under a collective authorship. Like many Encyclopedias, it is unfinished. There is a fundamental reason for this — even if one claims *not* to create mathematics, the mere act of thoughtful exposition *is* creation.

[1] Note that in some institutes, 50% of a class might have been killed in WW1.

8.2.3 Big problems

Hilbert's (1900) list of 23 problems. These are not all ofthe same genus — e.g. 6th problem: "axiomatize physics". 3rd problem asks: given that two polygons have the same area iff there is a dissection which reassambles to them (i.e. there is a purely combinatoric definition of area), can this be generalised to polyhedra. Also four colours theorem, the fact that, though we can't prove the Riemann hypothesis itself, the work of Weil/Grothendieck/Deligne is fundamental. Add Finite Simple Groups, Fermat's "Theorem' etc.

8.2.4 Institutional Challenges

Big prizes, e.g. Clay Millenium Prize, King of Sweden prize and Poincaré. The rôle of academies has been decreasing.

8.2.5 "Giant" Proofs

These may be large because of computers, but not necessarily so: the Wiles+... proof of Fermat is effectively in the thousands of pages. The Grothendieck/Deligne work is enormous as well, but locally easy. The four-colour theorem is inprinciple simple, but enormusly detailed. The classification of finite simple groups is (except for some explicit constructions) a human proof, but Kepler conjecture includes a human reduction of 600 papers, and the *Annals of Mathematics* editors felt obliged to publish a disclaimer. This reduction is then followed by a computer computation whose correctness is far from clear.

These giant proofs are basically a new feature of mathematics, which leads to the following.

8.2.6 Industrialisation

Big teams of papers, with continued collaboration (much aided by the Internet), reliance on coplex computer systems (e.g. PARI).

8.2.7 Data Sets and Experimental Mathematics

These are used instatistics, where samples can be replaced with exhaustive analysis. Mentioned [AS64]. One of his students has a 4MB polynomial — can't be printed.

8.2.8 How to guarantee Mathematics?

This trend to giganticism has changed mathematics. One has proof assistants, onion rings of proof, and so on.

8.2.9 New Foundations

Of course there was the aim of foundationalism. HOLight is the first reformulation since [WR10]. I have always been convinced that type theory is more suitable than set theory, and HOLight's intensional view is very exciting. This also inspired new views of infinity: there is "very large" between the genuinely finite and the truly infinite.

Q. Will we need to accept "probably true" as well as the old certainties.

A. I expect so, but haven't given it enough thought.

Q. But these 'large' proofs a re getting smaller.

A. These are still not getting to the point where we can understand **why** the results are true.

Chapter 9

8 July 2010 — OpenMath

9.1 Towards OpenMath Content Dictionaries as Linked Data — Lange

"Lnked Data" is a set of best practices for publishing and connecting data. Berners-Lee proposes the following principles.

- Use URIs to identify data.
- use HTTP URIs, which can therefore be dereferenced.
- Provide useful (machine-understandable) information at these URIs. In practice, this is often RDF, but needn't be.
- Links to other related things to improve information disovery.

Perhaps this is "the Semantic Web as it should have been". But current linked data sets, often statistical data, contain very little mathematics. The example shown was the number of geese in the isle of Wight in 2008. These data sets may have growth rates, densitie stec., i.e. *derived values*, which is practice a re currently hard-coded.

$$HDI = \frac{1}{3}\left(LE + \frac{2}{3}ALI + \frac{1}{3}GEI + GDP\right)$$

would need to be a formula in a CD which could be dowloaded. But this doesn't currently work.

- Use URIs — not many CDs have `cdbase` defined.
- Use HTTP URIs well — this is true for the 'official' ones.
- Provide machine-readable information: unfortunately what you get is non machine-readable HTML.
- Link to other things — most links are to [AS64], but should be linked to the DLMF, and probably into DBpedia.

9.1.1 Technical flaws

- No MIME type specified. We ought to be able to use HTTP content negotiation. `application/openmath+xml` should be supported.
- "It is important to stress that it is not CDs themselves which are being transmitted, but some 'mathematics' whose definitions are held within CDs" discourages publishers from making machine-understandable CDs available.
- Weak semantics of FMPs — this has been discussed for many years, but little progress has been made. RDF linked data has pretty weak semantics, e.g. "see also" links.
- No way to link to non-OpenMath objects, such as DLMF.
- There are issues to do with `#` versus `/` URIs.

One possibility would be to have OpenMath entailment rules for SPARQL, or simply SPARQL extension functions.

Q.—JWK A service might have private CDs (as in SCIence), which are obtained by a service.

JHD This is related to CL's comments that linked data might even be useful on an Intranet as well as in the woder world.

A. Agreed.

Q.—MK SB tried to transform CDs to RDF, and at that point concluded that it wasn't worth it.

A. But that was 1998, and certainly at that time RDF was not useful.

JHD Probably 'Overtaken By Events'.

Q.—MK Of course, if one uses OMDoc CDs, all this already works.

A. We have made some progress in publishing **OMDoc** as linked data, which is easier, but many of the problems were generic.

JHD How much is `openmath.org`, how much is the CDs stored there, and how much is the standard?

A If PL were here, hacking `openmath.org` would be relatively trivial.

9.2 OpenMath Meeting

[Incorporating clarifications from DPC]

9.2.1 MSC

PDFI reported that the 2010 Mathematical Subject Classification will be available as URI's from `http://msc2010.org`. JHD noted that this was related to CL's comments about "see also" links. PDFI said that links to CDs could be placed in the MSC site, and JHD noted that an example would be Bessel functions.

9.2.2 MK's 'state of the world' report

He noted that this was essentially a 'post MathML-3' report. He noted that MathML3 should be a true W3C recommendation in the next couple of months. At MathML-2 there were essentally two standards for content mathematics, despite the efforts of DPC etc. to write converters. There were just too many edge cases. Content MathML is now (MathML-3) split into 'pragmatic'[1] and 'strict', and 'strict' is in 1–1 correspondence, syntax and semantics, with OpenMath.

```
<OMS cd="relation1" name="eq"/>
```

becomes

```
<csymbol cd="relation1">eq</csymbol>
```

(one slight advantage of the latter is that Firefox, for example, will now show `eq`). The old MathML-C⇒OpenMath is now known as `p2s` (Pragmatic⇒Strict)[1].

As far as MK knows, the only remaining anomaly is over `cdbase`.

Q. Why was `DefinitionURL` deprecated in MathML (by declaring it to be pragmatic-only).

A. It's a consensus-based process!

A.—DPC (later) it's not deprecated (you can't deprecate something that was never there): the attribute isn't in Strict MathML because it isn't in OpenMath.

MathML `DefinitionURL` in general (if it doesn't point to a CD) corresponds to an OpenMath annotation using a symbol "definitionurl" in some CD and a OMstring to hold the URI. In the case that the definitionurl is of the form uri-of-cd`#symbolname` then it just corresponds to the usual `OMS cd=... name=...` attrbutes.

This rewrite is built into the MathML → Strict rewrites, and so there will never be a `definitionURL` in the resulting strict MathML, so the schema for Strict Content MathML doesn't need, and doesn't have, this attribute.

[1] DPC points out that the word 'pragmatic' is no longer used in the MathML 3.0 draft. The standard now states, in the introduction to Chapter 4 "Finally, Section 4.6 *The Strict Content MathML Transformation* summarizes the algorithm for translating arbitrary Content Markup into Strict Content Markup".

In OpenMath, `cdbase` can be inherited from any parent, which is the same as MathML. OpenMath defaults to `http://www.openmath.org/CD`, but MathML says that it is inherited from the mathematics embedding mechanism. Note that MathML does **not** specify the embedding mechanism. PDFI pointed out that the default therefore depended on whether one used `OMA` or `csymbol`. JHD pointed out that the MathML construct meant that one could not (naïvely) cut-and-paste MathML-Strict in a way guaranteed to preserve semantics.

DPC subsequently comments as follows, though.

> There is no difference between MathML and OpenMath here. In the XML encoding of OM the OM standard says (`http://www.openmath.org/standard/om20-2004-06-30/omstd20html-3.xml#sec_xml-desc`)
>
> > If a symbol does not have an explicit `cdbase` attribute, then it inherits its `cdbase` from the first ancestor in the XML tree with one, should such an element exist.
>
> The "XML Tree" wording was not accidental, and it allows for this attribute to be inherited from outside the openmath elements from a containing document element, just as in MathML.

9.2.3 MK's proposals

MK felt that we should work towards a new normative standard.

1. Make Content MathML (both strict and pragmatic) into OpenMath encodings. Technically speaking, they already are, since the standard says that any representation of OpenMath *is* OpenMath.

   Q. Should there be a reference translator (Strict⇔OpenMath)?

   A. DPC has such things, so really the only question is whether they are normative.

   A.—DPC (later) I don't think there needs to be a reference translator (we never had an official reference translator between XML and binary encodings for example). The current CD presentation includes the translator, you'll see "strict content mathml" in the xhtml view even though the CD file only has OM.

   JWK But won't this break lots of tools etc.?

   CL OWL, for example, has several encodings, and the ugliest (RDF triples) is actually the lowest-common-denominator standard.

   JWK This comes down to how the OpenMath Society wishes to promote itself.

   All This is clearly an important discussion to be held on the mailing list.

   MK's (incomplete) set of issues would be the following.

(a) `cdbase` (see above).

(b) Strict Content MathML as an encoding — what is the canonical one, and what happens to tools.

(c) Weaknesses of the FML language — as came up in the `multirelation` CD.

CL This is handled in some languages by allowing indexed access to arguments as well.

(d) OM compliance (missing even from OpenMath 2).

MK also felt that we should address the OpenMath infrastructure, which is too static and does not support linked data for Content Dictionaries.

9.3 OpenMath Business Meeting

1. **Election of a President of the Meeting.**
   MK was proposed and elected by acclamation.

2. **Election of a Secretary of the Meeting.**
   JHD was proposed and elected by acclamation.

   Election of Minute Checkers.
   JWK[2] and PL[3] were proposed and elected by acclamation.

3. **Annual Report on Activities.**
   OpenMath 3 has stalled, since all effort was diverted to MathML3. There has been little interest in the OpenMath workshop **as such**, but there has been a "Content Mathematics Training Camp", and there is much OpenMath activity at CICM

   Financial Report.
   No transactions to report.

4. **New Members.**
   CL felt that many members of the Content Mathematics Training Camp would be eligible for membership. Urs Hölzer and Constantin Jucovschi were nominated and elected.

5. **Acceptance of Reports.**
   The reports were accepted and the Executive Committee was discharged.

6. **Executive Committee.**
   The current list was displayed, subject to the replacement of Stephen Watt as Treaturer by Christine Müller. The Committee was re-elected.

   CL proposed, and it was seconded, that the Committee should be asked to consider their involvement and rôle within OpenMath, **before** the next

[2] Approval message `20100710131829.GB78466@stack.nl`.
[3] Approval message `CE160F60-2D03-486B-B13A-D0D5881954AE@activemath.org`.

meeting. **MK**

7. **OpenMath 3 Working Group.**
   MK proposed JHD, CR proposed MK, and MK proposed CL. He proposed that the Committee should be the editors of the new standard. They should be prepared to 'mine' the old OpenMath 3 drafts, but this should be a new activity. CL suggested that SCIEnce had to be represented. This was agreed, with JWK as the interim member until SCIEnce could be formally approached. PL was nominated. JHD suggested that DPC should be considered.

   CL asked what could be learned from the MathML experience, of three editors and twenty authors. It was noted that this *had* worked. CR therefore proposed that MK and JHD be nominated as the editors of the new draft OpenMath standard, with right to co-opt authors and editors as appropriate. JCo seconded this and it was passed *nem. con.*[4] **MK/JHD**

8. **OpenMath Infrastructure.**
   It was noted that `http://www.openmath.org` was too static, probably needed to support linked data (see CL's presentation earlier in the day), and probably support Wiki-style editing (though **not** for CDs themselves, which JHD as Content Dictionary Editor strongly agreed with).

   PL pointed out that the OpenMath Infrastructure mailing list (`infrastructure@openmath.org`) was basically unused. It was also the case that the previous OpenMath website had been the victim of many attacks, and security was an important issue.

   After some debate, it was suggested that PL, CL, CJ and JH should resurrect the mailing list and start discussing the future of OpenMath infrastructure, including the website. **Named**

The meeting closed at 12:53.

[4] *Nemine contradicente*: post-classical Latin "nobody speaking/voting against".

Chapter 10

8 July 2010 — Programming Languages for Mechanized Mathematics Systems

10.1 `transalpyne`: a language for automatic transposition — De Feo

Matrices represented by computer programs. Blakc box model: represent A by $b \mapsto A.b$. Application is Power iteration to find the largest eigenvalue — as used in page rank [BP98] and in [Wie86]. If we have straight-line programs, we can transpose them. Power projection $l \mapsto \sum_{i>0} l(\sigma 6 i) X^i$ is the transpose of modular composition.

Givne transposition is useful, why automatic transposition? The author spent three weeks (one mistake took him a month to find subsequently) to do the transposition.. This was origiannly discovered in electrical network theory [Bor56]: see also [BS83]. Any time we want to transpose, we end up linearising a circuit with multiplication nodes. We also need to lieanise `for` and `if`. Can we automatically deduce any possible linearisation of a program. Type inference can help. Define `L` and `S` as the linear ans scalar types. Then plus can be either `L->L->L` or `S->S->S`, 1 has to be `S`, 0 can be either `S` or `L` etc. We extend Hi9ndlet–Milner type inference to handle lists of acceptable unifications. So what does `transalpyne` allow?

```
type Ring R
type Module(R) M
def (linear M A, const m)f(linear M Z, const M z,n):
```

together with `int`, `bool`, `if`, `let`. Automatic transposition consist of keeping the

scalar computations where they are, and running the linear parts backwards. However, we may break taiil recursion, which is a problem. This increases space complexity, but not time. **If** we trust the user, memo-isation can preserve complexity of recursion. We have an (almost) complete Python implementation.

10.2 LEMA: Tpowards a language for reliable arithmetic — Thévery

We want to generate automatically certified and efficient numerical code (typically in C). For example, given a mathematical function, we need to choose a 'good' polynomial approximation, a 'good' evaluation scheme etc. For the first, there is a specialised algebra system Sollya and for the evaluation (which has to take account of parallelism), we use CGPE. GAPPA is the tool that produces a formal proof. We also use Maple and Coq. Lema converts the problem description into the internal library format. LEMA has to be sufficiently expressive to capture the function, with values on special inputs, types (and their associated arithmetics), target platform capabilities. We also need to handle data generated with external tools.

We chose to develop LEMA as an XML document (using Content MathML for the mathematics).

Q.—JC Do you know about the Coconut project (IBM Power/PC)?

A. Couldn't find out too much about it — JC to prod the authors.

10.3 The PIDE project — Wolff

Proof Integrated Development Environment for an Asynchronous Isabelle environment. The most widely used interface is Emacs/proofGeneral. It looks pretty outdated. We aim to overcome these shortcomings and build a Formal Methods tool platform. ProofGeneral is an untyped Lisp implementation with a Linear Text model (buffers), with all the limitations this imposes. Proofs are more structured than linear scripts imply. We would like prover independence, platform independence, support for asynchronous proof processing, and extensibility for domain-specific visualisation.

Holger Gast has a PIDE-Netbeans implementation. It is synchronous, but has refined protocol logs, and **cut and paste finally works**.

Makarius Wenzel has an asynchronous candidate, with refined tooltips.

We envisage that the eventual implementation will support a nonlinear document mode, rather an DAG on netepads, each of which is a DAG on atoms. 'Notepad' goes back to ideas of the author from 15 years ago, and can be modified both by the user and the prover. This should be a persistent data type. DAGs on versioned notepads fits into modern versioning systems. In the future this parallel asynchronous model could extend to specialised provers as well as Isabelle. This will require attaching proof logs as an attribute of a notepad.

Makarius's work is funded by this project,as in the current attempt to put I3P on the Isabelle/Scala layer. We can conclude that a true document model is needed. See `http://bitbucket.org/pide/pide/wiki/Home`, where one can find the PIDE manifesto.

10.4 Recent Developments in ΩMEGA's Proof Search Programming language — Autexier

The context is that we have mathematical knowledge, theory, proofs and proof search, and services, such as verification, suggestions, corrections, explanations. Applications would be text writing and tutoring.

Humans work at the level of assertions and strategies ("by polynomial fatorization"). Strategies are declarative or procedural, and refer to other strategies and assertions. In ΩMEGA,**inferences** are used to operationalize assertion-application. Inferences can be applied deeply. They can be annotated with application directives. There is a "Proof data Structure" PDS. It allows different layers of granularity, and alternatives. Scripts can be apply-style or declarative (as in Mizar).

10.4.1 Demonstration

`axiom setequaldef`etc.

```
prove "A intersection B = B intersection A"
apply setequaldef
apply intersectiondef
```

Then it asks us which goal to apply to, and so on. Having finished, we can ask to have the proof shown to us, eitehr textually or as a graph.

Q.—JC You repeat yourself to prove the two halves of this assertion. Can this be avoided?

A. Currently don't have the right sort of meta-variables.

Strategies are specified by the user, and are procedural. We need to annotate them, which ony works partly for synthesised inferences (we need a good syntax here). If we load strategies (such as closure over axioms), we get an immediate proof (which is identical to the previous one we spelled out).

There are also declarative tactics. We need to add granularity control to the proof script.

10.5 PLMMS Business Meeting

LD said that there weren't many submissions. Are we aiming for archival publications or demonstrations? He said that we could stay a workshop, or be absorbed into Calculemus?

Q. What differentiates PLMMS?

A. It the only one which is *exclusively* programming languages and mathematical systems.

JC Nowhere else would I sit next to MW!

JHD We were competing for archival publication with Calculemus itself, so I would like to see a demo-focused workshop.

BW But in that case we should find a way of archiving the demonstrations, e.g. as videos.

MW I never really undestood the scope of Calculemus.

LD Should we press to have this topic included in Calculemus? We could still have a video/demo track within Calculemus

This proposal was carried. **LD to e-mail Calculemus**

Chapter 11

8 July 2010 — MKM 2010

11.1 Proofs, proofs, proofs — Kerber

Quoted Hardy on thenature of proof. "unexpectedness, inevtability and economy". The deias are lost once we get lost in the swamp of 'forall-introduction' and so on.

> Historically speaking, it is of course quite untrue that mathematics is free from contradictions; noncontradiction appears as a goal to be achieved, ot as a God-given quality wthat has been granted to us once for all. Since the earliest time, all critical revisions of the principles of mathematics as a whole, or of any branch in it, have almost invariably followed periods of uncertainty — [Bourbaki, 1954]

What acceptance do we want in education? We want to

- Teach the concept of proof (to an acceptable level)
- joint development
- teach mathematical concepts
- let students find relationshps

We should, following [P45], distinguish plausible reasoning from demonstrative reasoning.

How do we support plausible reasoning? [McC97] solution of the Robbins conjecture. Independent checking was possible, because the proof object could be communicated. Diagrammatic reasoning is also quite important, and difficult to communicate (even over Skype-like conferencing).

"Mathematics is a motley of techniques of proof" — Wittgenstein.

11.2 CICM Business Meeting

1. **Election of a President of the Meeting.**
   MK was elected by acclamation.

2. **Election of a Secretary of the Meeting.**
   JHD was elected by default.

3. **Report on CICM 2010.**
   RR reported on this. The attendances were 7 invited/ 85 regular and 32 students (2009 7/50/32). We have (in Euros) collected 33K, and estimate expenses at 42K, with 10.5K on grants due in. There should be a small surplus to carry forward.

   MK proposed a vote of thanks to RR, which was carried by acclamation.

   RR said that we should thank the local organisers and the students who helped on the registration desk.

4. **Presentation of a Draft CICM Constitution.**
   MK outlined the background: accidental co-location in Linz in 2007, deliberate co-location (VS) in Birmingham in 2008, and Grand Bend (SMW) in 2009. The administrative burden in 2009 had been disproportionate to the size of the meeting. The trustees of MKM and Calculemus have been discussing this problem, and produced a draft constitution, which he showed. It wasn't clear that AISC[1] would join immediately, but that DML might wish to join. This would be a multi-track conference (using EasyChair's facility), with a joint submission date for the archival tracks — workshops, emerging trends tracks etc. could still have their own dates.

   Q.—MKe This seems like an excellent way forward if no-one objects.

   Q.—JAC AISC would probably like the freedom to associate or not.

   MK I take it that we should *not* specify the number of tracks precisely.

   PDFI It should be made explicit that this mechanism supports the (very important) workshops side of CICM.

   MK Agreed.

   Q. I am unhappy about moving papers between conferences, since authors decide which track they want.

   SMW My experience has been that this flexibility is useful.

   AA It could be argued that we should go for one conference, without tracks etc.

   MK The conferences *currently* prefer their identity. But it is true that the identities could be better defined.

[1] Recall that AISC is biennial.

MK proposed the draft constitution, subject to adding a common closing date, and representation of the workshops on the steering committee. This was carried, with three abstentions and no-one against.

5. **CICM Secretary and Programme Chair for 2011**
   MK explained that there was a bootstrap problem. MKe suggested that the three committees should jointly meet and decide the officers. It was proposed that

   - the Calculemus and MKM Trustees, and AISC Steering Committee, should collectively nominate the CICM Secretary
   - Each group should nominate its initial CICM Trustee
   - The CICM Trustees should collectively nominate the CICM Programme Chair
   - Each group should nominate its own track Programme Chair

   This proposal was approved after no-one spoke against it.

6. **Progress on CICM 2011**
   RR re-iterated his willingness to pass on his advice to the organisers of future CICMs. In his experience it was possible to organise CICM in one year.

   AA presented his interest in holding CICM in Italy. He had organised MKM 2003 in Bertinoro (near Bologna) but this time he proposed Sardinia[2]. His suggested site was close to Olbia airport (and therefore reachable). The site he has in mind has rooms of the right size. However, it would be advisable to organise it outside the "high season". Bertinoro would be more flexible about dates.

   MK reminded people that RR had suggested that 2012 should be planned for. SMW volunteered MK to organise it "near Bremen", and MK said that it should be possible, but he was still looking at venues etc.

The meeting closed at 19:40.

Note: see also footnote 3 (page 57) for an update on the (lack of) legal status of CICM.

[2]The website of his proposed venue is `http://www.aironehotel.eu`.

Chapter 12

9 July 2010 — Colloque Thérèse Hardin

12.1 The Genesis of Synchronous Functional programming in the Team SPI — Pouzet

In general, many of the bugs we found in critical embedded software were actually in the specifications rather than in the implementations. Therefore our system (Lustre) was designed to to take (linear) equations directly from the mathematical model. This user Kahn's model for the semantics of process networks commnicated by unbounded FIFOs (e.g. Unix pipe). It has

+ simple semantics

+ modular — a nework is a continuous function

+ supports asynchronous distributed execution

+/− Time invariance — there is no explcicit timing, but it is impossible to state that two events happen at the same time.

This lends itself to a kernel with minimal primitives: e.g. function, application, fix-point, constants and variables, unitary delay (`fb`='followed by') selection (`x when h` where `h` is a Bollean sequence), and merge. But there are sone 'synchronicity monsters' which must be barred at compile time.

We can have synchronous clocked streams, i.e. an explicit representation of absence. We extended Lustre into Lucid Synchrone (1996–), which had to be a conservative extension. This was the start of a fruitful collarboration with the SCADE team at Esterel Technologies, and many features of our work arrived in SCADE 6.

Can we move from syncrhony to relaxed synchrony? See `www.lri.fr/~plateau`. A 'real-life' example of this is insertion of a standard deifnition

image in an HD one — for example what size buffer is needed, what is the delay introduced in the video processing chain? The exact results are (delay) 9.598 (versus our model's 11.995) and 192K (versus 193K).

12.1.1 Postscript

Subsequently, JHD spoke with TH and the speaker. She stated that the whole strucure is based on dependent types, with the type structure carrying the burden of checking that the time constraints are met. Even in finite cases, checking this fully can be very dificult, so we over-estimate, which leads to the over-estimates in the previous paragraph.

12.2 Subsequently

JHD got involved in a meeting with Elsevier, so missed the next few atlks.

Chapter 13

9 July 2010 — Mathematical Knowldge Management

13.1 — Zeilberger

He asked that people not use latops during the talk. JHD will try to transcribe his notes later.

13.2 Towards Automatic Formalization of Informal mathematics with mathNat — Raffalli (& Humayoun)

Mathematical English is universally accepted by all mathmeaticians, and is (mostly — modulo symbols, 'let' etc.) a subset of English. Trivial translation from formal proofs to English is easy, but is not easily acepted by a human reader/ The linguists will say that parsing is easier than *good* text generation (not least because 'good" is undefined).

Our goal is to define

1. a small subset of mathematical English with some rich linguistic feaures;
2. a formal language MathAbs for mathematical text that keeps the structure and
3. a parser (1)⇒(2).

He showed a proof that $\sqrt{2}$ is irrational.

He then showed the MathAbs equivalent. MathAbs is parametrized by the language used in `hint` and `assume` constructs. He claimed that this is *nt* natural deduction.

The sentence-level parser is written using Ranta's GF. The output of this is fed to a Haskell program, whihc uses a 'zipper' to buildthe MathAbs parse tree. It uses a context for all expressions, hypotheses etc., and uses this to solve anaphora (the most recent object in the context which meets akll the constrainbts, as in "these integers")/ We also have to distinguish collective/dsitibutive reading, as "x and h are equal "(resp. positive). Anaphora inside expressions is non-trivial: "if $x = y$, then it is positive" — 'it' means x, and some other examples.

In fact, checking the mathAbs proof did not work, basically because the proof tended to be formally incomplete.

13.3 Integrating multiple sources to answer questions in Algebraic Topology — Heras *et al.*

In pratcice we may consolut soures, perform computations, check results against tables,a nd very conjectures with a proof assistant. How do we mechainise the mangement of these sources. We have two CAS (Kenzo and GAP[1]), a theorem prover (ACL2) and a rule based system (HES — Homotopy Expert System): uses RuleML and OMDoc files.

Archietcure is inspired by the broker model.: known here as Mediator There is certain existing interoperability: Kenzo↔GAP (uses SCSCP), Kenzo↔ACL2 ()in terms of OMDoc documents) and Kenzo↔HES (e.g. to compute a homotopy group, HES needs to knwo homology groups, computed by Kenzo .

He gace a demonstration, which seemed to show a well-integrated inerface. Claimed that the user does not know *in which ystem* his computations are being performed. One example was an Eilenberg–MacLane group via GAP and Kenzo.

We have integarted computation and reasoning tools, with OpenMath playing a key rôle.

Q.–PLWhy haven't you pubished your OpenMath CDs?

A. Lack of time.

13.4 Dimensions of Formalit: A Case Study for MKM in Software Engineering — Kohlhase *et al.*

The SAMS project is about safety components for autonomous mobule service robots and to get it certified as SIL-3 component. A naïve implementation means

[1] With the HAP Library.

that one can't drive through doors!. Hence we need a smarter implementation of the safety zone. The aim is to implement in Misra-C, verify the safety properties in Isabelle, and submit to the certification agency (TÜV). This actually has been done.

Used the V-model discipline, with all the constraints that this implies. The Isabelle basically checkied the implemented code against verification code, but the whole of the V was not verified. The whole verification project (9 person-years) had produced 251 LaTeX files, 61 Word documents, 33 Isabelle theories and 40 `.c` files. One key observation was that the levels of formality varied widely across the range of documents, There's quite a lot of geometry/physics in the informal part. We therefore user STeX, which is semantic pre-loading of TeX documents. Semantic macros like `\union{a,b,c}` $\rightarrow a \cup b \cup c$; we mark up the discourse structure `\begin{proof}[id=Wiles]`.

We can run LaTeX over this to generate documents, but also Bruce Miller's tool to generate a bunch of XML. One problem is that definitions in SAMS are often in tables, which is not allowed in OMDoc. Hence STeX had to be extended with a "table of definitions" construct. There are lots of cross-references in the V-model documents. The aim was to mark these up as OMDoc metadata: `\SemVMrel[cd=reqspec,refid=R12,rel=refines]`, and this is particularly important for change management. Use [LK09] to generate these RDFa relations.

STeX structures could be object structures, project structures, collection structures and organizational structures, which live in four, fairly independent, ontologies. The enormous XML files are read by an RDF harvester, which can be queried by SPARQL. He showed an example for a SPARQL query "find a substitute for an employee".

This case study shows that this *does* work. It does deal with the logical mathematical structure. We needed a flexible metadata scheme for secondary relations.

MK has learned that 'linked data' really works, and gracefully embeds MKM techniques in the real world. Doing it essentially inside LaTeX was very important in practice. However, this is only one of many aspects. Mathematics is only one part of reality.

Q.—BM Did you speak to the original authors?

A. There was quite a lot of work to be done adding hidden arguments, such as "this time t depends on v", to the input documents. We now have a much greater confidence in the correctness of the mathematics *as do* the original authors.

Q.—PDFI Why didn't you/they place all this in a database?

A. You should see the [low] level of sophistication of their technology in practice: emailed copies of Word documents!

13.5 Adapting mathematical Domain Reasoners — Heering (& Jeuring)

Part of the Mathbridge project. mathematical learning envornments typically offer ea wide range of interactive exercises. Exercise-specific parts are often delegated to specific *domain reasoners*. Showed various reasoners, including "Exercise Assistant Online", which showed a nice teacher-written piece of text explaining the student's mistakje (misapplying De Morgan). Some of his examples came from a tool that comes with a textbook which is used in 50% of Netherlands schools.

Customisation taken place at many levels.

1. Learners — level of expertise
2. Teachers — specific requests how an exercsie shouod be solved; good understanding of learner's capabilities; tailor exercises at a high level
3. learning environments, e.g. creating new execises by combining existing parts, or integrate with other components such as the ActiveMath student model
4. domain reasoners

An example was that the teacher wanted "completing the square", but this wasn'tin the textbook.

We need rewrite rules, (incluing buggy rules), rewrite stratgeies (which we define in a strategy language, similar to theorem provers' tactic languages), and views/canonical forms, which define notationalconventions. Claim that these three concepts correspond to the mathematical knowldeg appearing in textbooks. We need a representation for each concept, to communicate the internal structure. There are challenges in makingthe exercise parts transparent: cost and excessive flexibility (too easy fro the teacher to create a faulty exercise).

Rewrite rules map easily onto OpenMath FMPs. Rewrite stratgies are written in a simple DSL. We can tehrefore *remove* part of a strategy, *collapse* a sub-strategy into a rule etc. Representations of canonical forms is the trickiest part. Confluent sets of rewrite rules is one possibility. We are not yet clear on the best way forward. `http://ideas.cs.uu.nl`.

Q.—MK I can believe that *you* can customize it — how about the teachers.

A. Of course, teachers don't communicate directly with the domain reasoner, but rather with the leanring environment, hence we need a major GUI effort, which has yet to be done.

Q. If you provide an authoring tool, you have to provide a debugging environment — where is it?

A. The learning environment is the debugging environment — there was some scepticism here.

Q.—WMF Do you have a strategy for "when students can do what"

A. Generally called a tutorial strategy, which is often thought of as being orthogonal to the strategies we have described.

13.6 STEXIDE: An Integrated Development Environment for STEX Collections — Jucovschi & Kohlhase

OMDoc is great, but you want to consume it, rather than write it. MK showed a dependency graph of the various theories introduced in his CS course. There are a **lot** of STEX macros in this. Editing this with classic tools has both local and global problems — we focus on the latter.

The local problem he mentioned was `x\in A` should be `\inset{x}{A}` (but of course there are a lot of these). The expansion factor is probably only 2 (better than others), but still tedious. Hence STEXIDE as a project to make STEX easier to use. CJ demonstrated STEX an an eclipse plugin. It knows which symbols are defined, alomg with their descriptins from the corpus. This list is accessed by the auto-complete facility, which is context-sensitive. The aim is to keep the architecture fairly tool-indpendent, e.g. MK would like it for CATL. Would like a tool that applies new `\symdef`s to existing documents. Future work would include supporting interplay between MKM formats.

Q. Does this plugin do syntax checking — e.g. matching `begin`/`end`, also nuymber of arguemnstetc.

A. That's in the 'import' tool.

Q—PL. Where is the index?

A. There is a local index, but the gloabl index (RDF store) is future work.

Q. Why does the rewite of `\in` have to be done this way — cam't you just post-process.

A. In general presentation LATEX is ambiguous, so there may be more than one alternative necessary. Post-processing doesn't scale.

PL I agree with MK.

sectionNotations around the world: Census and exploitation — Libbrecht MathBridge is meant to cover Austria, Finland, France, Germany, Hungary and the Netherlands. Hence there are serious natural language issues, as well as notational issues. According to MathML:

en C_m^n

de $\binom{n}{m}$

ru C_n^m

others ${}_nC_m$

This appears not to be the case, though textbooks disagree[2]. There is very little done in this respect, and, for example, Wikipedia and PlanetMath disagree.

Our census will use Wiki infrastructure, but should be based on widely-used sources – online where possible (Google books have been helpful), or scans. The aim is one page per mathematical meaning. Showed the gcd page, e.g. 'ggT' in German. 'pgcd' in French etc. (also arabic).

Constructing and validating the census was non-trivisl: people object, and respnd by sending in Word documents with unicode problems. So we need sources. There are differences by language such as the gcd exanple, but also by country (half-open intervals) and culture 9evennumbes, notably the thousand separator)..

We believe it's complete for the six countries plus Arabic, and is complete for the MathML core CDs. It is not even clear what to call the culture: "grade-school number theory in German". There are also issues of completeness of notations. for example the notation for times of divide. Another question is preferred variable names: a line might be l in English, d in French and g in German.

`http://wiki.math-bridge.org/dislay/ntns/`

Q.–DZ What about history of notation?

A. That would be a great deal of work.

JHD But it would be nice to be able at least to add this, e.g. the correct attribution of "Landau O" is to [Bac94]. There are issues of copyright of a scan from a book [PL said that most of their Finnish sources came from a single formula book], but a single page should count as fair dealing under copyright law — it's essentially a quotation.

13.7 MKM Business Meeting

AS announced that there was an MKM 'Best Paper' award wich was presented to Kohlhase, Rabe & ???.

1. **Election of a Secretary of the Meeting.**
   JHD was elected by default.

2. **Report by Trustees.**
   Nothing except the discussion on the future of CICM.

3. **Report by Treasurer (WMF)**
   MKM's share of the CICM 2008 surplus, £1045, is currently held by Birmingham. CICM 2009 is not finalized, but is likely to break even. It is expected that CICM 2010 will yield a small surplus.

[2]He now has an example of a textbook using the "Russian" notation.

4. **Election of Trustees.**
   The terms of MK and SA come to an end at this meeting. One vacancy is one of the PC co-chairs, which would be, by mutual agreement, AS. MK and JHD would accept nominations until the end of CICM. If necessary, Mamane will run a Condorcet-compliant election. MK nominated SA for re-election. MK himself would *not* be willing to stand again. AS nominated PDFI.

5. **Report on MKM 2010.**
   PDFI and AS reported. EasyChair was an excellent support. 32 submissions and 16 acceptances. The Proceedings operation went well. We got a change in the copyright agreement from Springer, allowing authors to host archive version of their papers, which was a success.

   Q. Will you explain the recipe for getting this change?

   A. PDFI feels that MKM's change *can* be quoted as a precedent to Springer, since they seem happy with this. AS has the source of the revised copyright agreement, which he can give to those interested.

   All Applause to the organisers for this excellent innovation.

   Q. How does the submission and acceptance rate compare with previous years?

   A. It's not "out-of-line", but there are enough confounding factors: AISC and location.

6. **Presentation of a CICM Constitution.**
   MK explained that this was essentially the third CICM (plus CICM-0 at RISC in 2007). Calculemus has accepted the proposal. AISC will not formally decide, but might join CICM in 2012. DML might wish to join.

   So the question is whether MKM wishes to join CICM, which was formally accepted by the CICM Business Meeting yesterday.

   Q.—BM Each component will deal with its own Track Chair and (nominees for) Programme Committee [MK: Correct]. How about the overall CICM level? What happens if one party has many more trustees than the other?

   A. This won't arise in practice. The `all-trustees` process is only being invoked for bootstrapping, and currently numbers are roughly equal.

   MK proposed that MKM join CICM. This was carried *nem con.*

   MK reported that the MKM Trustees had met at lunch in anticipation of this vote. They had selected Florian Rabe for the MKM Track Chair for CICM 2011. The MKM funds referred to above would be used (along with Calculemus' share) as endowment for CICM[3].

[3] MKM is not in itself a legal body, so this rôle is performed by IFCoLog (`www.ifcolog.net`). IFCoLog have agreed that CICM, which is also not a legal body, can be a part of IFCoLog, and JHD has been invited (and has accepted) to join the Board of IFCoLog (and seems subsequently to have been promoted to the Council). MK is already on the Executive Board.

MK forgot to report, but he and JHD have added it here for completeness, that at the same Trustees meeting WMF was appointed as MKM Trustee on the CICM Steering Committee.

The meeting closed at 19:20.

Chapter 14

10 July 2010 — MIPS

14.1 Apros Proof Tutor

`http://www.phil.cmu.edu/projects/apros` is a course with a pedagogical empahsis on teh cinstruction of proofs. We are trying to use *dynamic tutoring* of proof construction via an automated *Proof Tutor*. This is working fro pure logic, and we are working on an extension for set theory.

> Proofs are not mere collections of atomistic processes but have a complicated internal structure.

He wishes to make this bi-directionality formal via the "intercalation calculus". he would also like to extend the concept by appealing to the meaning of mathematical concepts, and to use lemmas. The real question is what actual structure of mathematical proofs and their strategy.

Chapter 15

10 July 2010 — Mathematical User Interfaces

15.1 Intelligent Summarising and Browsing of Mathematical Expressions

JHD presented Ivelina Stoyanova's work — see `http://staff.bath.ac.uk/masjhd/Slides/Stoyanova-handout.pdf`.

Q. Why not make this available via a parameterised URL, where the [OpenMath] browser took the OpenMath in the URL?

A. Why don't you e-mail Ivelina with the suggestion, and tell her how the linkage would work.

15.2 The Methods of Improving and Reorganizing Natural Deduction proofs — Kaç

We often merge together two deductions into one reasoning. If the first has steps $\alpha_1, \ldots, \alpha_n$ and the second has $\beta_1, \ldots, \beta_n$, then we can create a proof $\alpha_1 \wedge \beta_1, \ldots, \alpha_n \wedge \beta_n$, but this is unreadable. Solving this problem involves understanding the dependency graph. h ethen considered the following

> In every group of people one can point to one person in the group such that if that person drinks,very person in that group drinks

which has a proof by cases. His methods make proofs slightly shorter (c. 1%) but slower to verify (c. 5%). Claims there are 755K unnecessary references in the Mizar ;ibrary, and 39K unnecessary statements.

Q. Are these tools available to Mizar users?

A. Not yet — tehre are some dependencies that need to be resolved.

Q.—PL Could be a web service?

15.3 An Interface for Math e-learning on Pen-based Mobile Devices — Fujimote (& Watt)

We regard this as technology for the genral classroom, not a specialised computer laboratory. In a PC lab,, when the tecaher says "lets plot the graph of this function", the class stops for several minutes. We therefore think the hand-held stylus device is appropriate for the classroom.

Some years ago I developed AsirPad (described in first MathUI). This showed useful potential, but AsirPad had no way to support mathematics quizzes. So we buit a Web-based Support System based on the Nintendo QS. iT provides a quiz, visualises the results, and sends messages to the tecahers. He did an experiment with Eulerian circuits among grade 6 students. Japanese students are very shy of expressing results publically, so this worked.

But this didn't scale, so we used Moodle. However, the screens are too rich for mobile devices. Hence we produced Moodle Lite (which runs off the same database as Moodle, so the teacher can prepare and view results on full Moodle). Moodle has a TEX filer, also jsMath and ASCIIMathML. Unfortunately Nintendo doesn't support jsMath, nor indeed MathML, so we used ASCIMathML alsongside Bruce Miller's MathML CSS (Bruce Miller).

For input, we could use DragMath (but it's in Java) or BrEdiMa, which is in JavaScript. For graphs, we use GnuPlot. The quiz element, which he deomnstrated, seems to be purely multiple-choice. One problem currently is that the drawing action (for user graphical input) is recognased as page scroll. We need a CA tool, e.g. Maple T.A. and STACK. Implementing this is future work.

15.4 :orenzen Dialogue games

Dialogue games based on Proponent and Oppnent. payers attak or defend statements that have already been made.

Particle rules say what moves are available base don the structure of forumulae

Structural rules govern the overall shape of the group.

It will turn out that termination may depend on whether we have classical or intuitionistic logic. Structral rules are

1. Proponent may assest an atomic formula only after Opponent has asserted it,

Table 15.1: Particle Rules

Formula	Attach	Defence
$\alpha \wedge \beta$	?L	α
	?R	β
$\alpha \vee \beta$	?	α or β
$\log \alpha$	α	—-
$\alpha \to \beta$	α	β
$\exists x \alpha$	?	$\alpha(c)$
$\forall x \alpha$		

2. A player may defend against only the most recent unresponded attack
3. An attack may be answered at most once
4. As assertion made bya Proponent may be attacked at most once.
5. Opponent must repsond to Proponent's immediately previous move.

Theorem 2 *[Fel85] Proponent has a winning strategy for the same that starts with ϕ iff ϕ is intuitionistically valid.*

This proof is constructive, in that it builds a proof from a strategy or v.v. `http://www.dialogical-logic.info`, based on UnCommonWeb. Shows that

$$((P \to Q) \to P) \to P \tag{15.1}$$

(Pierce's formula) goes into an infinite loop here, because it is not *intuitionistically* valid.

15.5 Demonstration Introductions

15.5.1 MathDox Formula Editor — Knopper

Wanted a content input tool *without* plugin. Has an optional palette. Use an HTML canvas with jsmath. The latest version has

1. dynamic off/on for palette;
2. support for n-ary infix
3. `mu` now displays as μ etc.;
4. Better integral parsing

15.5.2 MathML test suite — Libbrecht

1400 expressions. A typical examplewould be $\sqrt{2}$. `http://www.w3.org/Math/testsuite`. Note that, while this is intended as a browser conformance test, the MathML is exportable for use elsewhere.

15.5.3 MathEdit — su Wei

`http://matheit.lzu.edu.cn/mathedit`. Seems to be palette based, but, with the cursor on the y in $\sqrt{x-y}$, he was able to use a short-cut key to replace the y by a fraction having y as numerator. Desigmed to be easily embedded into a web page. There is apparently a Braille version, though there were questions from thfloor about its precise operation.

15.5.4 Tiddlywiki and MSC2010 — Ion

There is a tiddlywiki version of this MSC2010. Note that some of the SC have mathematics in their name. This works, and is editable. He also showed a tiddlywiki geometry wiki with changeable diagrams.

15.5.5 DLMF— Miller

Note that [AS64] Equation number ws very important, so DLMF equation numbers are also permalinks. They also, where appropriate, refer to the original number.

15.5.6 — Wenzel

Showed a proof checker (Isabelle/Scala) running in the background while he typed into his editor (jEdit). The point is that this is genuinely real-time, whereass Mizar-mode for emacs typically is not.

Bibliography

[AR09] A. Asperti and W. Ricciotti. about the formalization of some results by Chebyshev in number theory. *LNCS 5487*, pages 19–31, 2009.

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

[Bac94] P. Bachmann. Die analytische Zahlentheorie. *Teubner*, 1894.

[BDS09] R.J. Bradford, J.H. Davenport, and C.J. Sangwin. A Comparison of Equality in Computer Algebra and Correctness in Mathematical Pedagogy. In J. Carette *et al.*, editor, *Proceedings Intelligent Computer Mathematics*, pages 75–89, 2009.

[Bor56] J.L. Bordewijk. Inter-reciprocity applied to electrical networks. *Appl. Sci. Res. B.*, 6:1–74, 1956.

[BP98] S. Brin and L. Page. Anatomy of a large-scale hypertextual web search engine. In *Proceedings of the 7th International World Wide Web Conference*, pages 107–117, 1998.

[BS83] W. Baur and V. Strassen. The Complexity of Partial Derivatives. *Theor. Comp. Sci.*, 22:317–330, 1983.

[Chy00] F. Chyzak. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Math.*, 217:115–134, 2000.

[Fel85] W. Felscher. Dialogues, strategies and intuitionistic provability. *Ann. Pure Appl. Logic*, 28:217–254, 1985.

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

[Gon08] G. Gonthier. Formal Proof - The Four-Color Theorem. *Notices A.M.S.*, 55:1382–1393, 2008.

[GR94] I.S. Gradshteyn and I.M. Ryzhik. Table of Integrals, Series and Products (ed A. Jeffrey). *5th ed.*, 1994.

[Hal07] T.C. Hales. The Jordan curve theorem, formally and informally. *Amer. Math. Monthly*, 114:882–894, 2007.

[Hal08] T.C. Hales. Formal Proof. *Notices A.M.S.*, 55:1370–1380, 2008.

[Jut77] L.S.v.B. Jutting. *Checking Landau's "Grundlagen" in the AUTOMATH System.* PhD thesis, Eindhoven University of Technology, 1977.

[Lan30] E. Landau. Grundlagen der Analysis. *Leipzig*, 1930.

[LK09] C. Lange and M. Kohlhase. A Mathematical Approach to Ontology Authoring and Documentation. In J. Carette *et al.*, editor, *Proceedings Intelligent Computer Mathematics*, pages 389–404, 2009.

[Loz01] D. Lozier. The NIST Digital Library of Mathematical Functions Project. In *Proceedings MKM 2001*, 2001.

[McC97] W. McCune. Solution of the Robbins Problem. *J. Automated Reasoning*, 19:263–276, 1997.

[McD81] D. McDermott. Artificial Intelligence Meets Natural Stupidity. *Mind Design*, pages 143–160, 1981.

[Pól45] G. Pólya. How to solve it. *Princeton University Press*, 1945.

[PBM83] A.P. Prudnikov, Yu.A. Bryčkov, and O.I. Maričev. Integrals and series of special functions. *Nauka*, 1983.

[PP05] E. Phillips and D. Pugh. How to get a PhD: a handbook for students and their supervisors. *Open University Press*, 2005.

[RJ09] A.D. Rich and D.J. Jeffrey. A Knowledge Repository for Indefinite Integration Based On Transformation Rules. In J. Carette *et al.*, editor, *Proceedings Intelligent Computer Mathematics*, pages 480–485, 2009.

[SCT09] C. Sacerdoti Coen and E. Tassi. Natural Deduction Environemtn for Matita. In J. Carette *et al.*, editor, *Proceedings Intelligent Computer Mathematics*, pages 486–492, 2009.

[Wie86] D.H. Wiedemann. Solving Sparse Linear Equations Over Finite Fields. *IEEE Transactions on Information Theory*, 32:54–62, 1986.

[WR10] A.N. Whitehead and B. Russell. Principia Mathematica. *Cambridge University Press*, 1910.

[Zei90] D. Zeilberger. A Fast Alogorithm for Proving Terminating Hypergeometric Identities. *Discrete Math.*, 80:207–211, 1990.

Appendix A

Dramatis Personæ

AA Andrea Asperti — Università di Bologna

SA Serge Autexier — DFKI Bremen

JAC John Campbell — University College London (emeritus)

JC Jacques Carettte — McMaster University

DPC David Carlisle — NAG Limited

JCo Joseph Collins — USNA

JHD James Davenport — University of Bath

WMF Bill Farmer — McMaster University

PDFI Patrick Ion — American Mathematical Society/MathReviews

MKe Manfred Kerber — University of Birmingham

MK Michael Kohlhase — Jacobs Universität Bremen

JWK Jan Willem Knopper — TU Eindhoven

CL Christoph Lange — Jacobs Universität Bremen

PL Paul Libbrecht — Saarbrücken

BM Bruce Miller — NIST

AS Alan Sexton — University of Birmingham

VS Volker Sorge — University of Birmingham

SMW Stephen Watt — University of Western Ontario

MW Makarius Wenzel — Munich

BW Burkhardt Wolff — Munich