INFORMATION SOCIETY TECHNOLOGIES
(IST)
PROGRAMME

Project IST-2001-33562 MoWGLI

Report n. D0.d
Final Self-Assessment Report

Main Author:
A. Asperti

Contents

1 Project Meetings and Information flow

1.1 Project Meetings

During the second reporting period only one meeting has been held, at the École Polytechnique in Palaiseau, Paris, France. The meeting was held on December 14th, 2004. We had 12 participants, so subdivided: UNIBO (4), INRIA (2), DFKI (2), KUN (2), MPG (1), Trusted Logic (1).

We also had an informal MoWGLI meeting at the third International Conference on Mathematical Knowledge Management, Bialowieza, Poland, in September 2004.

In the context of MoWGLI, the Albert Einstein Institute organized a meeting on "Hermes and Semantic Authoring with TeX and MathML' in Golm-Potsdam, Germany, from October 26 October until October 27 2004.

As for personal mobility, Claudio Sacerdoti was invited to Trusted Logic on September 2004 to help in the installation of MoWGLI's prototype, and to provide technical assistance to the implementation of Trusted Logic's converter of Coq models into UML.

2 Work progress overview

2.1 Specific Objectives for the reporting period

According to the contractual workplan, the activity of the second reporting period has been mainly focused on the following Workpackages and Tasks:

WP0 Project Management
WP6 Testing and Validation (all Tasks)
WP7 Information Dissemination and Exploitation

During the final period we planned to perform the following activities:

1. refine of the overall architecture resulting from feedback of the validation phase (Tasks T6.1-T6.2);

2. finalize the advanced prototype of the LaTeX based authoring tool according to the experience of the validation phase (Task T6.3);

These activities were driven by the following three major pilot applications:

1. Formalization of a full undergraduate course in algebra or analysis for didactic purposes (Task T6.1, deliverable D6a).

2. Formalization of (part of) the process of loading, verifying and executing an applet into a smart card (Task T6.2, deliverable D6b).

3. Make maximal use of content marked-up articles in a solely electronic scientific physics journal (Task T6.3, deliverable D6c).

KUN, Trusted Logic and the Albert Einstein Institute have been respectively in charge of the three validation activities T6.1-3. UNIBO, DFKI and INRIA have been mostly working at the final prototype, tuning the application with the relevant feedback and solicitations provided by the other partners.

Figure 2.1 describes the main synergies between the different partners, in this phase of the project.

Final Mowgli Prototype
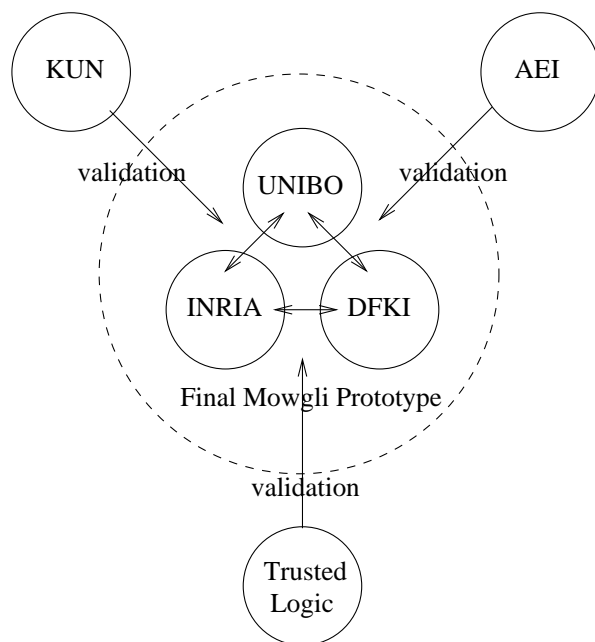
2.2 Overview of the progress

During the last year an extension in the duration of the project from the original 30 months to 36 months has been negotiated and accepted by the European Commission. The extension, that was motivated by a slight delay in the validation phase, has allowed to accomplish all the expected work and to delivered all prototypes and reports according to the new timetable.

2.2.1 An Interactive Algebra Course with Formalized Proofs and Definitions

The activity, mostly performed at KUN, consisted in the exploitation of MoWGLI technology for the electronic publishing *on the web* of a typical course notes in mathematics. In order to compare the result with a state-of-the-art digital document, we choose IDA, an interactive course on algebra, which has been developed at Eindhoven University of Technology (NL), for first year math. students.

The overall idea was to borrow from IDA the macrostructure, meaning both the overall logical organization and the purely textual parts in natural language, adding a deeper semantic layer for mathematical definition, theorems and proofs. In particular, Coq has a large repository of formalized constructive mathematics (C-CoRN) covering basic algebra and analysis, and the goal was to relate IDA notions to the corresponding formal counterparts in C-CoRN, using then MoWGLI tools to render them on the Web.

An important part of the work consisted in integrating the style sheets that do the rendering. The other main effort consisted in integrating the formal repository C-CoRN with the missing notions (especially with examples). Finally, the constructive aspect of Coq (and

C-CoRN) involved a bit of extra work, as some of the statements in IDA are not constructively provable, and had to be revisited.

This activity provided a really valuable feedback to MoWGLI technology. On one side it proved that the idea of having a deep semantic content in real mathematical documents is feasible; on the other side it clearly stressed the lack of a good authoring environment for this kind of integrated documents. Although authoring was outside of the scope of MoWGLI, the effort required for the semantic enriching of the source document is still not adequate to the final gain for the user. We must not only study innovative services and appealing interactive functionalities exploiting the formal encoding but, especially, we must a find a way to cut down the actual cost of producing computer understandable information instead of computer readable one.

2.2.2 Smart Card Security

Trusted Logic explored the use of MoWGLI's prototype as a support for the certification of IT products based on the Common Criteria standard (CC). This international standard is presently recognized in several countries of the European Union, like France, Germany, Spain and the UK. Depending on the Evaluation Assurance Level claimed by the sponsor of the evaluation, some of those documents must be presented using an informal, semi-formal or completely formal languages. Informal documents are just text in English. Semi-formal documents are usually based on graphical specification languages, like for instance the Unified Modeling Language (UML). Formal documents are written using a language based on a formal calculus, like Coq.

According to this scenario, MoWGLI's technology has been evaluated along three possible axes:

1. Providing a Security Policy Model with semantic contents. This means a document that contains both English explanations but also the logical structure of the formal definitions of the security policy, that the Evaluator may directly check using a proof assistant.

2. As a tool for explaining the formal description of the product, that provides support for the exploration (hyperlinks, search tools) and the appropriate rendering of the formal definitions.

3. As a neutral exchange format for transforming formal models into semi-formal ones (composite evaluations) and to communicate with development teams.

The evaluation performed in point 1 and 2 above allowed to point out several weaknesses in the tested technology: installation was too complex, rendering was most suited for mathematics than software, some (meta)data and annotations are lost during exportation from coq sources, rendering could be improved (both in quality and complexity). Many of these points have been taken into account in the final mowgli prototype (Trusted Logic actively participated in this refinement process, implementing and correcting several software components).

The most interesting validation experiment was however the third one, exploring the interoperability potentialities offered by MoWGLI's XML encoding, using it as an exchange format between formal models. In this case, the translator enables to communicate formal models to development teams that use CASE tools based on UML or to link formal models to other UML models provided by the clients. The tool enables the automatic integration of formal models in Coq into the Rational Rose UML environment. Using the original technique

developed at Trusted Logic and described in deliverable D6b, UML diagrams can be used to have an overview (actually, a picture) of all the data-structures of the Coq model and the different relations linking those data-structures.

This experiment was a clear success and an important assessment of MoWGLI methodology.

2.2.3   Journal Interface

The task aimed to assess the usability of Hermes (Deliverables D4d and D4e) as a conversion and authoring tool for scientific document. In particular, it consisted in using the tool for a trial conversion of all the articles in Living Reviews in Relativity, which is an international, peer-reviewed, open-access electronic publisher of review articles in gravitational physics.

Hermes was originally intended to provide a way to convert mathematical expressions in MathML, but it then evolved into a semantic oriented, full document converter and authoring tool. The current implementation of hermes has the following components:

- a set of semantic helper macros, for LaTeX, $\mathcal{AMS}$-LaTeX and $\mathcal{AMS}$-TeX (the dlt.tex, dalt.tex and da.tex files available in the source distribution). These macros enable the author to add semantic layers to his documents, that is, authoring with, or constructing, his own semantic vocabulary, such as MathML-content, or, with minimal manual intervention, making his document renderable in a web browser using XML and MathML-presentation.

- a scanner, written in flex, which extracts from the resulting 'semantic dvi' file the tokens seeded by the macro collection above and sends them to the parser below (the 'hermes.l' file in the Hermes distribution);

- a parser, written in bison, which is a grammar that performs a semantic action when a structured set of tokens is recognized (the 'hermes.y' file in the hermes distribution); the semantic action is the creation of parts of the xml output; the parser and the scanner compile into a 'semantic dvi' translator called 'the Hermes translator'.

All the currently published articles in the Living Reviews in Relativity collection have been converted to XML+MathML. They served also as a testbed for constructing the Hermes macros corresponding to the major LaTeX packages used.

The conversion process involved the following steps:

1. validate the original sources: compiling the original sources into dvi

2. validate the sources with the insertion of the corresponding Hermes macro collection: compiling the modified sources into semantic dvi;

   this is the step where Hermes detects unbalanced mathematical expressions and author intervention is needed to fix the sources

3. parse the semantic dvi with Hermes and output the result into an xml file, encoded in Unicode UTF-8, which contains enough semantic information for making it archivable in a library.

4. convert the library xml file into a media dependent xml file (currently, the Hermes distribution comes with an xslt stylesheet which converts a typical scientific article into

an XHTML+MathML renderable on screen and printable in a pdf); the quality of the rendering depends on the fonts and the implementation of the MathML rendering engine.

The overall result of the sample conversion can be reached and browsed through the Hermes website, hosted by Max-Planck-Institut für Gravitationsphysik (Albert-Einstein Institut), Golm, Germany, at `http://www.aei.mpg.de/hermes`.

Living Reviews in Relativity was particularly satisfied by this achievement.

2.3   Deliverables

The following is the list of Deliverables for the final period, covered by this report.

n.	Deliverable Title	WP no.	Lead Partic. month	Estim. person-	Type	Secu- rity	Deliv. month
0.d	Final Self-Assessment Report	0	UNIBO	1	R	Pub	end
6.a	Validation 1: Education	6	KUN	16	R	Pub	end
6.b	Validation 2: Smart Card Security	6	TL	9	R	Pub	end
6.c	Validation 3: Journal Interface	6	MPG	14	P	Pub	end
6.d	**Final MoWGLI Prototype**	6	UNIBO	12	P	Pub	end
7.b	Technological Implementation Plan	7	MPG	1	R	Pub	end
R =Report, *P* =Prototype, Pub=Public							

3   Dissemination of Results

3.1   MoWGLI presentations

Also during the last year the Dissemination of Results progressed well. The following is a list of the main talks and presentations (without publication) held at national and international events. Publications in conference proceedings and journals are listed in the next section.

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", Workshop on Web Enabling Technologies, Trieste, Italy, April 2004

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", Heinz Nixdorf Center for Information Management in the Max Planck Society (ZIM), Munich, Germany, March 2004

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", Workshop New Developments in Electronic Publishing of Math, Stockholm, Sweden, June 2004

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", Romanian Academy in Iasi, library of the Romanian Academy in Iasi, Central University Library in Bucharest, Iasi, Romania, September 2004

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", Workshop on Hermes and Semantic Authoring with TeX and MathML, Golm, Germany, October 2004

- R. Anghelache, "Hermes: A content oriented LaTeX to XML conversion/authoring tool", presentation for the TexDocC Group, Duisburg, Germany, February 2005

- A. Asperti. The HELM and MoWGLI Projects. Lecture at the national conference of the Italian Association for Logic and its Applications. Pisa, february 2005.

- H. Barendregt, "The Automath Heritage", Automath symposium, Eindhoven, May 26 2004.

- H. Geuvers, "Some drinks from the Automath source", Automath symposium, Eindhoven, May 26 2004.

- I. Loeb, L. Mamane, "Interactive algebra course with formalised proofs and definitions", Niii-colloquium, Nijmegen, Nov 8 2004.

- B. Spitters, "The C-CoRN project and program extraction", Programming Logic Seminar (Chalmers, Sweden), 17 May 2004

- B. Wegner, Plenary lecture at APPOPT 7, University of Leon, Nicaragua, March 2004

- B. Wegner, Key note talk at the International Conference of Mathematics and Applications, University of Kuwait, Kuwait, April 2004

- B. Wegner, Guest Lecture at Steklow Institute of Mathematics, Moscow, Russia, April 2004

- B. Wegner, talk at the special session on electronic publishing at the joint meeting of the American Mathematical Society and the Sociedad Matemtica Mexicana, Houston, USA, May 2004

- B. Wegner, talk at the special session on electronic infrastructure for mathematics in Africa at the Pan-African Congress of Mathematicians, Tunis, Tunisia, September 2004

- B. Wegner, Guest lecture at Chiangmai University, Thailand, October 2004

- B.Wegner, Plenary talk at International Conference on Discrete Mathematics and Applications, Chonqing, China, October 2004

- B. Wegner, Invited talk at the meeting of the Latvian Mathematical Society, Riga, Latvia, November 2004

- B. Wegner, Talk at the Seminar on Coding Theory, Bankya, Bulgaria, December 2004

- B. Wegner, talk at Mat.es 2005, Valencia, Spain, February 2005

- B. Wegner, plenary lecture at the Bolivian Congress of Mathematics, Cochabamba, Bolivia, February 2005

- F. Wiedijk, "When will it happen?", Automath symposium, Eindhoven, May 26 2004.

- F. Wiedijk, "Integrating procedural and declarative proof", Small TYPES workshop "Types for Mathematics / Libraries of Formal Mathematics", Nijmegen November 1-2 2004

- S. Zacchiroli. Web Searches in Hypertextual Electronic Libraries of Mathematics. Workshop on New Developments in Electronic Publishing of Mathematics, Stockholm, Sweden, June 2004

3.2   Publications

Scientific and technological aspects of the Project have been presented to International Conferences, testifying the high technical quality of the work performed so far. The following is a list of main scientific publications related to MoWGLI for the final reporting period:

1. A. Asperti, M. Selmi, "Efficient Retrieval of Mathematical Statements", Proceeding of the Third International Conference on Mathematical Knowledge Management, LNCS 3119, Bialowieza, Poland, September 2004

2. L. Cruz-Filipe, F. Wiedijk, "Hierarchical Reflection", in Konrad Slind, Annette Bunker, Ganesh Gopalakrishnan (eds.), Theorem Proving in Higher Order Logics, Proceedings of TPHOLs 2004, Springer LNCS 3223, 66-81, 2004

3. L. Cruz-Filipe, H. Geuvers, F. Wiedijk, "C-CoRN, the Constructive Coq Repository at Nijmegen". In: Andrea Asperti, Grzegorz Bancerek, Andrzej Trybulec (eds.), Mathematical Knowledge Management, Proceedings of MKM 2004, Springer LNCS 3119, 88-103, 2004

4. L. Cruz-Filipe, "Constructive Real Analysis: a Type-Theoretical Formalization and Applications". PhD thesis, Radboud University Nijmegen, 2004. Promotor: Prof.dr. H.P. Barendregt, copromotor: Dr. J.H. Geuvers

5. E. Melis, G. Goguadze, "Towards Adaptive Generation of Faded Examples", proceedings of International Conference on Intelligent Tutoring Systems, LNCS 3220, pp. 762–771, 2004

6. M. Niqui, "Formalising Exact Arithmetic: Representations, Algorithms and Proofs", PhD thesis, Radboud Universiteit Nijmegen (2004). Promotor: Prof.dr. H.P. Barendregt, copromotor: Dr. J.H. Geuvers.

7. M. Niqui, Y. Bertot, "QArith: Coq Formalisation of Lazy Rational Arithmetic", In S. Berardi and M. Coppo and F. Damiani (Eds.), Post-Proceedings of TYPES 2003 Workshop, Torino, Italy, LNCS 3085, Springer-Verlag (2004).

8. L. Padovani, C. Sacerdoti Coen, S. Zacchiroli, "A Generative Approach to the Implementation of Language Bindings for the Document Object Model", in the Proceedings of the Third International Conference on Generative Programming and Component Engineering (GPCE'04), LNCS 3286, pp. 469–487, Vancouver, Canada, October 2004

9. L. Padovani, R. Solmi, "An Investigation on the Dynamics of Direct-Manipulation Editors for Mathematics", in the Proceedings of the Third International Conference on Mathematical Knowledge Management (MKM 2004), LNCS 3119, pp. 302–316, Białowieza, Poland, September 2004

10. L. Padovani, "A Math Canvas for the GNOME Desktop", in the Proceedings of the 5th annual GNOME User and Developer European Conference (GUADEC 2004), Publication Series No 107, Agder University College, Kristiansand, Norway, June 2004

11. L. Padovani, "Interactive Editing of MathML Markup Using TeX Syntax", in Proceedings of the International Conference on TeX, XML, and Digital Typography, held jointly with the 25th Annual Meeting and of the TeX Users Group (TUG 2004), LNCS 3130, pp. 125–138, Xanthi, Greece, August/September 200

12. M. Pollet, V. Sorge, M. Kerber, "Intuitive and Formal Representations: The Case of Matrices", in Proceedings of the 3rd International Conference on Mathematical Knowledge Management, LNCS 3119, pages 317–331, 2004

13. C. Sacerdoti Coen, "Mathematical Libraries as Proof Assistant Environments", in Proceedings of the Third International Conference on Mathematical Knowledge Management, Lecture Notes in Computer Science (LNCS) 3119, ISBN:3-540-23029-7, 332-346, 2004

14. C. Sacerdoti Coen, S. Zacchiroli, "Efficient Ambiguous Parsing of Mathematical Formulae", in Proceedings of the Third International Conference on Mathematical Knowledge Management, Lecture Notes in Computer Science (LNCS) 3119, ISBN:3-540-23029-7, 347-362, 2004

15. C. Ullrich, P. Libbrecht, S. Winterstein, M. Mühlenbrock, "A Flexible and Efficient Presentation-Architecture for Adaptive Hypermedia: Description and Technical Evaluation", in Proceedings of the 4th IEEE International Conference on Advanced Learning Technologies (ICALT 2004), pages 21–25, 2004

16. F. Wiedijk, "Formal Proof Sketches", In: Stefano Berardi, Mario Coppo and Ferruccio Damiani (eds.), Types for Proofs and Programs: Third International Workshop, TYPES 2003, Torino, Italy, Springer LNCS 3085, 378-393, 2004.

4 WorkPackages evaluation

The activity of the last year has been mostly focused on testing and validation. As already mentioned, all these tasks provided a really valuable feedback that helped to improve the technology and tools under development within MoWGLI. So, from the internal perspective, all the tasks have been of great value.

Testing and Validation had however also the role of evaluating the actual relevance of the project's achievements. As any FET Project, MoWGLI was strongly innovative and ambitious in its goals: we presume to have achieved what we promised in the contractual workplan, but the relevance of these results was, a priori, unclear.

Form this point of view, the self assessment paramteres and criteria adopted in report D0a were particularly severe.

For the education Task T6.1, we may only claim that the results are *satisfying*, in the sense that the course notes (deliverable D6a) are usable by students (as the original IDA course already was), but nothing more. In fact, the few additional 'semantic' functionalities offered to the final user (links to formal proofs, automatic checking, some searching features,

dependency graphs, etc.) are more oriented to professionals involved in formalization activities than students. However, MoWGLI proved that a complete description of mathematical documents at a deep semantic and logical level is feasible, and the potentialities offered such such an encoding for education are still far from being understood.

The relevance of results is more evident in Task T6.2 (Smart Card Security). The aim of the task was to improve the presentation of the formalization of some security properties related to the code embedded into a smart card. The tools have been concretely used to prepare presentations to the the client company commissioning the certification work. The client particularly appreciated the overall description of the Coq formalization in terms of UML diagrams, since it was a representation language they already knew. In this case, the emphasis put by MoWGLI on XML as a neutral, platform independent, intermediate language suitable for interoperability purposes simplified the translation from Coq to UML and proved to be extremely successful.

As for Task T6.3 the aim was to demonstrate how an electronic scientific journal could benefit from the exploitation of MathML markup in journal articles. The minimal achievement was the ability of publishing the journals on the web, and this was clearly achieved. Another criteria prospected in deliverable D0a was the number and quality of enhanced functionalities such an encoding could pave the way to. As in the case of education, this is still a weak point of MoWGLI achievements.

The technology developed for content-based authoring of scientific document (Hermes) has proved to be usable, allowing the conversion from LaTeX to XML+MathML of all the current articles of Living Reviews in Relativity (an international, peer-reviewed, open-access electronic publisher of articles in gravitational physics). However, the translation work has been performed by a professional employee of the publisher, and it failed in the goal convincing new authors to directly use the Hermes system of macro for new submissions (that would require extra-work from their side not justified by any immediate gratification). In fact, the cost of creating semantically rich, machine understandable encoding of the information remains the main bottleneck of content-based systems.

On the other side, Hermes has been adopted by several editors or research groups external to MoWGLI, testifying the success of the tool. The most important is Zentralblatt für Mathematik (Berlin-Karlsruhe, Germany), that uses Hermes as a component of a web server answering user queries from their reviews database. Prof. Antal M. IVÁNYI, of the Faculty of Informatics of Loránd Eötvös University, Budapest, Hungary, is using Hermes to convert a small number of fundamental books in computer science, in a government funded project. Similarly, Prof. Günter Törner, from Duisburg University, Germany, plans to use Hermes in a project for archiving TeX documents in the mathematical domain, called TeXDocC.