my file

SCIENCE AND ENGINEERING RESEARCH COUNCIL
RUTHERFORD APPLETON LABORATORY

INFORMATICS DIVISION

SOFTWARE ENGINEERING GROUP NOTE 101

Software Engineering Research at RAL

issued by
D A Duce
13 February 1986

DISTRIBUTION: F R A Hopgood
R W Witty
D A Duce
C P Wadsworth
Personnel

(see next page)

Software Engineering Research at RAL

The Software Engineering Group at RAL has a research section whose activities are in the general areas of formal specification and verification. Another section of the Group plays an important role in the management of the Alvey Software Engineering Programme. The Group is part of the Laboratory's Informatics Division, which includes MMI and IKBS Groups with similar mixtures of research and national programme management functions.

Dr R W Witty is leader of the Software Engineering Group. The staff in the research section are at present:

Dr D A Duce (Deputy Group Leader)
Dr C P Wadsworth
A D B Cox
D R Gibson
P M Hedlund
A J J Dick (Atlas Research Fellow)

The overall SEG research theme is "Quality Certification of Software Products". Within this theme, the main research interest of the Group is in Formal Specification, the development and application of machine-assisted proof systems and the role of formal proof in software development. Individual activities are outlined below.

Formal Specification

David Duce holds a research grant under the Alvey Software Engineering Programme entitled 'Specification of the Graphical Kernel System (GKS)'.

GKS became an ISO standard on 15 August 1985, and has been a British Standard for some time. The document describing GKS is some 245 pages in length; the style of the description is mainly English narrative. It is difficult for a potential implementer to get to grips with the standard from this document. David Duce, together with Julian Gallop and Dale Sutcliffe at RAL, were editors of the GKS document. Other RAL staff have participated in the design, and subsequently the implementation, of GKS. The aim of this project is to apply formal techniques for the description of system designs techniques to GKS.

Initial work has been carried out with the Vienna Development Method (VDM), and more recently comparative studies with other formal techniques have been started. This work has resulted in a number of publications.

A complementary activity, looking at the emerging 3D Graphics Standards, GKS 3D and PHIGS, is funded by SERC's Computer Science Committee.

Theorem Proving

Chris Wadsworth is starting a new project in collaboration with UK universities and industry to develop a theorem proving capability for an integrated project support environment (IPSE).

Although mechanical theorem proving has been quite heavily studied in the past, it has yet to become a practical tool in methodologies and support environments for software development. Existing theorem provers operate essentially in isolation, are not integrated with other formally based programming tools, and have concentrated largely on mechanical techniques. At the same time, even the best of current interactive systems.eg Boyer-Moore, IOTA and LCF, provide only limited support for the user's role in proof construction. Such systems are at their best as "semi-automatic" proof checkers, when the user has a good idea in advance of how a proof can be found.

The principal aim of the work proposed is to investigate concepts and techniques for theorem proving tools which combine man's strengths (insight, experience, "leaps of intelligence", problem-specific knowledge and heuristics) with machine strengths (accurate, repeatable symbol manipulations, large storage), and to extend the scope, practice, and acceptability of theorem proving in the production of verified software. Particular objectives, jointly with the other collaborators, are:

a. to develop the theorem proving capability for an IPSE,

b. to understand the requirements for integration with other components in project/programming support environments,

c. to investigate new approaches to proof construction designed for advanced interactive use on large, high-resolution displays,

d. to consider evolution to a distributed delivery environment in which the computational power of mainframes is linked with the interactive convenience and flexibility of advanced terminals or single-user workstations, and

e. to achieve a design which is readily portable between alternative delivery environments.

Equational Reasoning

Jeremy Dick's research concerns theorem-proving with equations based on a technique called the Knuth-Bendix completion algorithm. In this approach, equations are considered as rewrite-rules, and can actually be used to perform computations. There are many important applications of such work in computer science, especially in proving properties of program specifications, modelling the execution of functional programs, transforming programs into more efficient but equivalent ones, and compiling techniques.

During the last twelve months, he has built on theoretical and practical work achieved as a PhD student at Imperial College. His main practical goal has been to develop further a rewrite-rule laboratory (mechanical theorem prover) called ERIL (Equational Reasoning: an Interactive Laboratory) to the point where it can be made available as a tool on the Alvey infrastructure machines; this goal is almost complete. At the same time, he has been able to considerably clarify much of the theoretical basis for ERIL, particularly with regard to a special form of polymorphism involving hierarchical types and overloaded operators.

Jeremy Dick holds an Atlas Fellowship in association with St Cross College, Oxford.

Standard ML

The section has actively followed the development of the new Standard ML. Chris Wadsworth was actively involved in the design of the new language. The standard is a consolidation of tried-and-trusted developments in the ML community since the original language was designed for the Edinburgh LCF project.

Principal additions are: the data constructors and pattern matching facilities of HOPE, exception values, a richer and more systematic set of definition constructs, a module facility based on the latter, and I/O handling. The language has Alvey backing and it is expected to be used in software development in the section.

Mikael Hedlund is working on converting ML/LCF to Standard ML. The new parser and typechecker are complete and he is now working on the rest of the system (code generator and run-time support). The aim is to ensure that LCF, as the largest application of ML to date, is fully available for Standard ML. (The modules facility is not needed for LCF and is not being implemented in the first instance.)

Facilities at RAL

The Laboratory has an excellent computing environment for research. Mainframe support available includes an Atlas 10 (a large IBM compatible machine) running the Amdahl UTS Unix system and an IBM 3081. There are a large number of VAX 11/750 machines running Unix, a Pyramid 90X, a number of Prime and GEC minicomputers and a large number of PERQ, SUN and Whitechapel workstations. The systems are linked either through ethernet or Cambridge Ring local area networks, or the X25 network. The Laboratory has good communications with UK universities and sites abroad, through the JANET network and PSS. All staff have access to an office automation system.

Good typesetting facilities are regarded as essential to the smooth progress of the section's research projects. A variety of output devices is available, ranging from the book quality IBM 4250 electro erosion printer, to Apple Laserwriters. The Unix troff suite of formatting programs is used to drive these devices.

The Laboratory also has an excellent computing library and strong links with research groups in UK and overseas universities.

There are several active seminar programmes in the Labratory. Staff are encouraged to travel to conferences, workshops and training courses, and to develop links with other research workers, both in the UK and abroad.

Opportunities

There are immediate opportunities to work with David Duce in the GKS formal specification projects, and with Chris Wadsworth in the theorem proving project.

Opportunities also exist to do new research which is complementary to the section's research projects described here.

Senior members of the section may propose their own research projects. Collaboration with other groups, both in academia and industry, is encouraged.

Members of the section are able to undertake research work full time, and do not have other commitments such as teaching duties or user support.

Publications

1. D A Duce, E V C Fielding and L S Marshall, 'Formal Specification and Graphics Software', RAL-84-068.

2. D A Duce and E V C Fielding, 'Better Understanding through Formal Specification', RAL-84-128, accepted for publication in Computer Graphics Forum.

3. D A Duce and E V C Fielding, 'Formal Specification - A Simple Example', to appear in ICL Technical Journal, May 1986.

4. D A Duce and E V C Fielding, 'Formal Specification - A Comparison of Two Techniques', RAL-85-051.

5. D A Duce, 'Concerning the Specification of User Interfaces', Computer Graphics Forum 4 (1985), 251-258.

6. D A Duce and E V C Fielding, 'Towards a Formal Specification of the GKS Output Primitives', accepted for Eurographics '86, August, 1986.

7. D Gibson and D A Duce, 'GKS and Text Processing', Computer Graphics Forum, 4 (3), 1985.

8. R J Cunningham, A J J Dick, 'Rewrite Systems on a Lattice of Types', Acta Informatica, 22, pp149-169, 1985.

9. A J J Dick 'ERIL - Equational Reasoning: an Interactive Laboratory', RAL-86-010.

10. C P Wadsworth, 'Report on the IOTA Programming System and other Japanese Advanced Research', RAL-84-090.

Copies of these publications are available on request.

seg2/seg 101/lv