VISIT TO ICOT

4–27 February 1993

Dr John Slaney
Centre for Information Science Research
Australian National University

I visited ICOT for a little over three weeks, in order to pursue existing research collaborations with members of the Theorem Proving group. Dr Mark Grundy of the Centre for Information Science Research accompanied me on this visit, as he did on our last visit in May 1992. This time, in addition to working at ICOT itself, we were able to visit research groups in Kyoto, Nara and Numazu in order to learn of their work and to explain our ICOT collaboration to them.

This visit took place under the Memorandum of Understanding signed in 1992 by ICOT and the Australian National University. So far, the only Australian group directly involved is ours, the Automated Reasoning Project, but it is hoped that other departments of the ANU will follow us in becoming active collaborators with ICOT researchers.

* * *

The project occupying most of my research time on this visit involved the use of the theorem prover MGTP/G (Model Generation Theorem Prover, Ground version) and the rather comparable program FINDER (Finite Domain Enumerator) which I am currently upgrading in the light of what I have learned from MGTP and other systems. The principal Japanese collaborator in this work was M. Fujita, recently of ICOT and now returned to his company Mitsubishi. Others involved were Professor F. Bennett of Mount St. Vincent University, Halifax, Nova Scotia and Professor M. Stickel of SRI who has visited ICOT in the past.

Applying our automated reasoning software to problems in finite algebra, we have discovered many previously unknown facts concerning quasigroups. A quasigroup is a cancellative groupoid, that is, an algebra with a 'multiplication' operation whose 'multiplication table' is a Latin square. So every row and every column of the table is a permutation of the groupoid elements. As algebras, these structures may satisfy or fail to satisfy further conditions such as equations. The idempotent ones in particular satisfy the general equation $x^2 = x$ for each element x. Many interesting relationships hold between finite quasigroups and certain other structures such as classes of edge-coloured graphs or some types of block designs. These give rise to particular conditions which the quasigroups in question have to satisfy, and the question then arises for which numbers n is there a quasigroup with exactly n elements satisfying the condition. For example, one of the most interesting conditions is the equation $(yx.y)y = x$. It has been proved that there is a quasigroup of which this equation is true of every odd-numbered order but not of every even-numbered one. For example, although there is such a quasigroup of order 4 (i.e. with 4 elements) and also one of order 8, there is none of order 6. We were able to show, using MGTP and later confirming the result with FINDER, that there is none of order 10, which had been an open problem. The computation which

established this result was not at all trivial, requiring several hours of processor time on PIM-M with 256 processors. We also obtained the new results that there is no idempotent model of the above equation of order 12, and Professor Stickel showed that there is no idempotent model of order 13, a result we have since confirmed. The same problem for orders 14, 15 and 16 remains open.

In the first stage of our joint research on this topic, including the visit to ICOT just before FGCS'92, we mainly investigated the equation above. In July 1992 Fujita-san and I were able, with support from ICOT and the ANU, to visit Professor Bennett in Canada, where we discussed our work with him and received much helpful information on the mathematics of the problem set. He also suggested to us a number of closely related problems on which we might work. In the second stage of our research, we investigated seven suitable problems, one of them being that of the above equation and the other six somewhat similar. On all of the problems, we were able to confirm already known (non-trivial) results for some orders, and on three of them we obtained several new results. One of the new results was positive: the existence of a previously unknown structure. This is an idempotent quasigroup of order 9 satisfying the equation $xy.y = x.xy$ known as Schröder's first law. The existence of this structure was used by Professor Bennett to solve about half of the open existence problems concerning this law. We wrote a joint paper (with Professor Bennett) during Fujita-san's visit to the ANU in October 1992 in which we summarised the methods used and the results to that date. The paper will appear in the proceedings of IJCAI-93.

The third stage of this research was the period from November 1992 to January 1993 during which MGTP, FINDER and the program of Professor Stickel were all used to attack new cases of the original seven problems together with some new ones such as those concerning 'incomplete' Latin squares which are Latin squares with some subsquare missing. Many new results were obtained, including several positive existence results. The most significant of these were new idempotent structures of order 12 satisfying respectively Stein's third law $xy.yx = y$ and Schröder's second law $xy.yx = x$. These two results complete the solution of the finite existence problems for a number of constructions including some classes of $n^2 \times 4$ orthogonal arrays, certain tournament designs, equivalent objects in graph theory and the like. Another joint paper, with Professors Bennett and Stickel, is planned and will be submitted to a mainstream mathematics journal.

During my visit to ICOT, we have continued to generate minor new results such as negative solutions to a range of further problems concerning incomplete Latin squares, but our main aim has been to understand the generation algorithms better for the purpose of improving their efficiency. This is slow work and so rather more of a long-term aspect of our project, but we feel that it may eventually be the most important outcome of what we are doing. We have discussed such matters several times during these three weeks, and conducted many small-scale experiments. No final conclusions about the algorithms have been reached, but we feel that we now have a better understanding of the computational techniques and we expect the programs to continue to improve during the next few months. My program FINDER is currently being substantially revised for a new release, and will incorporate insights gained from the work at ICOT.

A talk entitled *Solving Problems in Finite Algebra with MGTP/G and Similar Automated Reasoning Systems* was given to the Parallel Theorem Proving group on 16

February 1993. This was a report on the general problem of finite constraint satisfaction problems, on some specific features of FINDER which are not found in MGTP/G and on the quasigroup results themselves.

* * *

A related but distinct aspect of the research collaboration between ICOT and the ANU is the work being done on first order Horn clause theorem proving. This work in turn has two parts. We are interested in the problem of parallelisation of theorem provers such as MGTP/N, and we are interested in helping such theorem provers to control their search for proofs by reference to semantic information. The former problem is rather hard, though significant progress on it is being made by the ICOT group led by R. Hasegawa which developed MGTP/N and which is now looking at ways of improving its performance. We discussed parallel theorem proving a little with our ICOT colleagues, but that was not the main focus of our research during this visit.

The idea of using interpretations as a source of information to make theorem provers more efficient is quite old. At least three such uses of semantic information interest us particularly. Firstly, when searching for a proof of some goal in a theory, we may use models of that theory to eliminate many possible sub-goals. If they are false in an interpretation which models the axioms of the theory, then clearly they are not theorems and hence are not derivable, and hence need not be explored as possible lemmata. Theorem proving programs written by the ANU group have been using this 'goal deletion' technique for many years. Secondly, in trying to construct proofs by forward chaining, whether or not the goal is the empty clause, we may make use of interpretations in which the goal is false. Some of the axioms of the proof are also false, of course. When choosing a formula from which to generate logical consequences, we may give some weight to selecting one which is false in the interpretation. This 'false preference strategy' can speed up proof searches for difficult theorems by some orders of magnitude. Thirdly, there is a well known result called the semantic resolution theorem which states that for any model M, if there is a resolution derivation of the empty clause from a given set then there is one in which no two formulas which are both true in M are ever resolved together. Usually some trivial interepretation such as "make all literals false" is used for this purpose, but better results may come from choosing to work with a special purpose interpretation tailored to the problem in hand. Now a model generator like MGTP/G or FINDER may be used to make up appropriate interpretations once our theorem prover has begun to derive clauses which can be fed to the model generator as axioms. In this way, a system can be built in which theorem prover and model generator help each other towards an efficient solution to their problem.

We have already built such a system by combining FINDER with the prover OTTER from Argonne National Laboratory. This program, SCOTT (Semantically Constrained Otter) is rather powerful in comparison with OTTER itself. Now it is striking that MGTP/N is very similar to OTTER, and that MGTP/G is capable of the same kind of model search as FINDER, so the idea of putting the two MGTPs together in a SCOTT-like way is an attractive one. For one thing, both varieties of MGTP, unlike SCOTT, are designed for parallel execution. My colleague Dr Grundy will report on current work directed towards this goal. I have not been working especially on semantically constrained MGTP during this visit, though I have of course discussed it with a number

of individuals and given two talks on the subject. The first was my presentation to members of the Sharp Corporation IT Research Laboratory in Nara, and the second, entitled *SCOTT: A Model-Guided Theorem Prover*, was presented to members of the International Institute for Advanced Study of Social Information Science of the Fujitsu Corporation's laboratory complex at Numazu. That group like the Sharp group, has participated in ICOT and was particularly interested to hear of the joint research project between ICOT and the ANU and of the current work on MGTP.

* * *

The research collaboration between the ANU's Automated Reasoning Project and ICOT began in a small way with a visit to the ANU by several ICOT researchers immediately after IJCAI'91. At that point we in the ANU became aware in some detail of ICOT's work, and were also able to communicate some of the ideas which we were then developing. Two PSI-II workstations were contributed to the ANU by ICOT (though they were never used because of installation problems). The first real collaboration was on the demonstration which we helped prepare for FGCS'92; the Memorandum of Understanding was signed a little later, when some PSI-III machines were installed in Canberra. Speaking personally, I should say that while it is good for us to have access to the ICOT hardware, which is indeed being used, the far more important aspect of our collaboration from the viewpoint of my research has been the personal contact with ICOT scientists. From the initial slight exchange of information less than two years ago, our work together has grown into one significant joint project, producing fine results and publications, and another very interesting investigation into theorem proving which may in the longer term help to change the ways in which we think about automatic reasoning systems. Such an outcome could not have been predicted at the start, so praise is due to those groups and individuals who helped set up the structures to make it possible. These include not only the ICOT management, but also MITI and the participating companies.

In my report on our previous visit to ICOT last year, I commented on the excellent way in which such mundane but important matters as accommodation, travel, local information, insurance and the rest had been provided, and particularly thanked Iwata-san and his staff for their efficient and most thoughtful work in this regard. He is no longer with ICOT, but his successor Kazuo Narita, assisted again by Kumiko Karakawa, continues to make ICOT all that we could wish our host to be. Thank you.

[1] J. Slaney, *SCOTT: A Model-Guided Theorem Prover*, Technical Report TR-ARP-4/92, Automated Reasoning Program, Australian National University, Canberra, 1992.

[2] M. Fujita, J. Slaney & F. Bennett *Automatic Generation of Some Results in Finite Algebra*, Technical Report TR-ARP-5/92, Automated Reasoning Program, Australian National University, Canberra, 1992. Proceedings of IJCAI'93 (forthcoming).

[3] J. Slaney, *FINDER: Version 2.0 Notes and Guide*, Technical Report TR-ARP-1/92, Automated Reasoning Program, Australian National University, Canberra, 1992.

THE AUSTRALIAN NATIONAL UNIVERSITY

Curriculum Vitae: J.K. Slaney

Senior Research Fellow
Centre for Information Science Research
Automated Reasoning Project

November 10, 1992

A. Personal Details

Name: John Keith SLANEY

Date of birth: 18 November 1953

Nationality: British
Australian resident

Current post: Australian National University — Senior Research Fellow
Automated Reasoning Project — 1988–1996

Address: Automated Reasoning Project, CISR
Australian National University,
GPO Box 4, Canberra, 2601.

John.Slaney@anu.edu.au

B. Education

Undergraduate: King's College — 1973–1976
University of Cambridge

Examinations: Philosophy Tripos Ia. Class: I
Philosophy Tripos Ib. Class: I
Philosophy Tripos II. Class: I

Degree: B.A. (1976) M.A. (1980)

Postgraduate: Australian National University — 1977–1980

Thesis: Computers and Relevant Logic: a Project in Computing Matrix Model Structures for Propositional Logics

Degree: Ph.D. (1980)

C. **Employment**

1980–1981	University of Durham Department of Philosophy	Postdoctoral Scholar
1981–1982	St. Andrews University Department of Logic & Metaphysics	Lecturer (temporary)
1982–1983	University of Queensland Department of Philosophy	Postdoctoral Fellow
1983–1990	University of Edinburgh Department of Philosophy	Lecturer (tenured)