UNIVERSITY OF CAMBRIDGE

# Isaac Newton Institute for Mathematical Sciences

## *Annual Report for July 1995 - June 1996*

December 1996

# Contents



## Appendices

# 1 Director's Preface

The Newton Institute is now four years old and thousands of mathematicians from all parts of the world have been through its doors. Programmes have been run across a very wide spectrum of areas of science, and many scientists from fields outside mathematics have taken part in interdisciplinary meetings.

The Institute has now established its reputation world wide and financial support has been confirmed and extended. Although a definite pattern of 6-month programmes has been adopted, some pilot variations are being attempted and more variety in programme format is planned for the future. While top-level science remains the essential criterion in selecting programmes, greater efforts are now being made to increase the participation of young UK mathematicians.

As I hand over the Directorship to my successor, Professor Keith Moffatt, I would like to express my thanks to all those who have worked so hard to make the Newton Institute such a great success.

Sir Michael Atiyah, OM FRS
30 September 1996

# 2 New Developments 1995–1996

## 2.1 Programmes

*Semantics of Computation* and *From Finite to Infinite Dimensional Dynamical Systems* were the programmes which ran from July to December 1995. They were followed by *Dynamics of Complex Fluids* and *Computer Security, Cryptology and Coding Theory* which took place from January to June 1996. A total of 1287 visitors attended the programmes, including workshop and short-stay participants. Over 800 seminars were given at the Institute and over 250 papers have been produced or are in progress.

## 2.2 Direction

Sir Michael Atiyah will retire as Director on 30 September 1996.

Professor Keith Moffatt has been appointed as full-time Director of the Institute from 1st October 1996. He will be assisted by Dr Noah Linden as part-time Deputy Director and by Dr Colin Sparrow as Liaison Officer.

Professor John Wright resigned as Deputy Director on 31 March 1996. Sir Peter Swinnerton-Dyer served as Executive Director from June 1995 and will also retire on 30 September 1996.

## 2.3 Senior Fellow

Dr Andrew Wiles was elected a Senior Fellow of the Institute for the calendar year 1996. Dr Wiles arrived at the Institute in April 1996 for an extended visit.

## 2.4 Hewlett-Packard Fellows

Dr Colin Sparrow's period as Hewlett-Packard Senior Research Fellow came to an end on 30th June, and Dr Sandu Popescu was appointed as Hewlett-Packard Reader in Quantum Mechanics. He takes up his appointment (initially for 3 years) on 1st October 1996 and will foster the Institute's continuing relationship with HP's Basic Research Institute in the Mathematical Sciences, BRIMS (see § 9).

## 2.5 Seminars given by participants elsewhere in the UK

Visitors to the Newton Institute gave over 160 seminars in other institutions. Universities visited included: Bath; Bristol; Cambridge; Edinburgh; Exeter; Glasgow; Hatfield; Heriot-Watt; Hertfordshire; Imperial College, London; Kent and Canterbury; Lancaster; Leeds; Leicester; Manchester; Newcastle; Nottingham; Oxford; Queen Mary and Westfield, London; Royal Holloway and Bedford New College, London; Southampton; St Andrew's; Strathclyde; Sussex; University College, London; Warwick; West of England.

## 2.6 EPSRC/PPARC Rolling Grant

The Institute applied to the EPSRC and PPARC for renewal of its 'rolling grant' in September 1995 and, after review by an EPSRC panel, the grant (£2.28 million over 4 years) was renewed until March 2000. The next review will take place in 1997/98.

## 2.7 Sun Microsystems

Sun Microsystems agreed to provide the Institute, at a very substantial discount, with a multi-processor computing server (Enterprise 4000) and a Netra fast fileserver, as well as replacements for existing workstations.

## 2.8 NATO Advanced Study Institutes for Young Scientists

The programmes *From Finite to Infinite Dimensional Dynamical Systems* and *The Dynamics of Complex Fluids* received support of £45,610 and £48,078 respectively to fund conferences aimed at young scientists.

## 2.9 Isaac Newton Trust

The Isaac Newton Trust has generously agreed to make a loan of £1,000,000 to the Institute, the interest on this loan to be used for running costs. If the Institute can raise matching funds within a four-year period, then the loan may be converted into an endowment.

## 2.10 Gabriella and Paul Rosenbaum Foundation

The Gabriella and Paul Rosenbaum Foundation announced that it would extend its grant to the Newton Institute by two further years, the second such extension. The grant will now run to 1999.

## 2.11 Institute of Physics

The Institute of Physics renewed its funding to the Newton Institute, donating £17,000 over a two-year period.

## 2.12 Programme Sponsorship

Programmes running in 1995/96 attracted funds from a wide variety of sources. *Semantics of Computation* ran a workshop with the assistance of Harlequin Software. *From Finite to Infinite Dimensional Dynamical Systems* obtained additional workshop funding from LMS and workshop funding from the Wellcome Trust. *Dynamics of Complex Fluids* obtained programme funding from Unilever (£10,000) and Schlumberger ($15,000) and workshop funding from DSM (Netherlands) (£6,000), British Society of Rheology (£3,000) and ICI (£500).

## 2.13 European Postdoctoral Institute in Mathematics

The inauguration of the European Post-Doctoral Institute in Mathematics (EPDI), a joint venture between the Newton Institute, the Institut des Hautes Etudes Scientifiques (IHES) and the Max Planck Institut für Mathematik (MPM), took place in Bures-sur-Yvette on 13th October 1995. The Executive Director, Sir Peter Swinnerton-Dyer, attended on behalf of the Institute. The EPDI invited applications in January 1996 and the first recipients of EPDI awards were selected in March 1996 by an international scientific committee.

## 2.14 Royal Society/Japan Society for the Promotion of Science Scheme

The scheme, which is a joint venture between the Royal Society, the Japan Society for the Promotion of Science, the Research Institute in the Mathematical Sciences (RIMS) at Kyoto University and the Newton Institute, was in full operation during this year. Scientists from the Universities of Swansea, Cambridge, Durham, Edinburgh, Manchester, Bristol and King's College, London visited Japan and scientists from Japan visited various UK institutions which included the Universities of Swansea, Warwick, Cambridge, Liverpool and the Newton Institute.

## 2.15 Fellowships

The Rothschild Professors in 1995/96 were Professor D Scott (*Semantics of Computation*), Professor J Hale (*From Finite to Infinite Dimensional Dynamical Systems*), Professor LG Leal (*Dynamics of Complex Fluids*) and Dr G Simmons (*Computer Security, Cryptology and Coding Theory*). The Prudential Senior Visiting Fellows were Professor E Spiegel (*From Finite to Infinite Dimensional Dynamical Systems*) and Dr R Larson (*Dynamics of Complex Fluids*). The Institute of Physics Fellow was Professor V Entov (*Dynamics of Complex Fluids*). The Rosenbaum Fellows were Dr R Viswanathan (*Semantics of Computation*), Dr Y Yi (*From Finite to Infinite Dimensional Dynamical Systems*), Dr G McKinley (*Dynamics of Complex Fluids*) and Dr F Solis (*Dynamics of Complex Fluids*).

## 2.16 Cambridge University Press publications

Further monographs in the series *Publications of the Newton Institute* were published by Cambridge University Press. The two volumes, resulting from the *Epidemic Models* programme, were:

Vol 6 *Models for Infectious Human Diseases, their Structure and Relation to Data*, edited by Valerie Isham and Graham Medley

Vol 7 *Ecology of Infectious Diseases in Natural Populations*, edited by BT Grenfell and AP Dobson

Other volumes, resulting from the *Symplectic Geometry*, *Financial Mathematics* and *Semantics of Computation* programmes, are still in production.

## 2.17 Princeton University Press publications

Princeton University Press published *The Nature of Space and Time*, a series of lectures by Professor Sir Roger Penrose and Professor Stephen Hawking, together with an accompanying video. The book had sold 11,000 copies by the end of June 1996.

## 2.18 Sculptures

Three 'Borromean' sculptures by John Robinson, *Genesis*, *Creation* and *Intuition*, have been generously donated by Damon De Laszlo and Robert A Hefner III and are displayed in front of the building.

Figure 1: Sir Michael Atiyah with sculptor John Robinson at the inauguration of *Intuition* in February 1996

# 3 Participation

## 3.1 Participation Profile

During its fourth year the Institute has seen a further increase in the overall number of visiting scientists. A total of 1287 visitors was recorded for 1995/96, an increase of 269 on the previous year. This included 195 long-stay participants, each staying between two weeks and six months, (10 weeks on average) and 307 short-stay participants who stayed for two weeks or less. In addition there were 45 affiliated participants (listed in Appendix C), young people who accompanied visiting members and stayed for periods ranging from several days to the full six months. Within the four programmes there were 37 workshops in total. These were periods of more intense activity on specialised topics or pedagogical activities which attracted an additional 740 participants to the Institute. Undoubtedly there were others who attended occasionally for lectures, workshops or Institute seminars.

Four six-month programmes were held during 1995/96: *Semantics of Computation* and *From Finite to Infinite Dimensional Dynamical Systems* (July to December 1995) and *Dynamics of Complex Fluids* and *Computer Security, Cryptology and Coding Theory* (January to June 1996) Each programme had an average of 16 to 24 long-stay participants in residence at any one time (the Institute classes those participants who stay for more than two weeks as long-stay participants) and the total number of long-stay participants in each programme was between 42 and 61. The statistics for long-stay participants for the four programmes are given in the following table:

| Programme | Numbers | Average no. days | Average Occupancy |
|---|---|---|---|
| Semantics of Computation | 49 | 81 | 24 |
| Finite to Infinite Dimensional Dynamical Systems | 43 | 73 | 19 |
| Dynamics of Complex Fluids | 42 | 88 | 22 |
| Computer Security, Cryptology & Coding Theory | 61 | 42 | 16 |

The long-stay participants are listed in Appendix A and a chart showing the periods of their visits is given in Appendix B. A breakdown of numbers by nationality and country of residence is given in Appendix D, and Figs 2 and 3 below show the percentages of long-stay and short-stay participants broken down by country of residence. As might be expected, UK participation is significantly stronger for short visits and workshops.

A graph showing the age distribution of participants is shown in Appendix E. The median is 40 years with an interquartile range 34 years to 49 years. For workshops and short-stay visits the profile is younger. Detailed biographical records have not been compiled for all short-stay participants but an age survey at a typical workshop indicated an average age of 34.

## 3.2 Evaluation and Feedback

The Institute continues to collect information and to monitor its performance and achievements in various ways in order to improve its management and administrative procedures.

Biographical information on each visiting member is requested on acceptance of invitation. On departure, each participant is given a general questionnaire, inviting comments on the Institute's

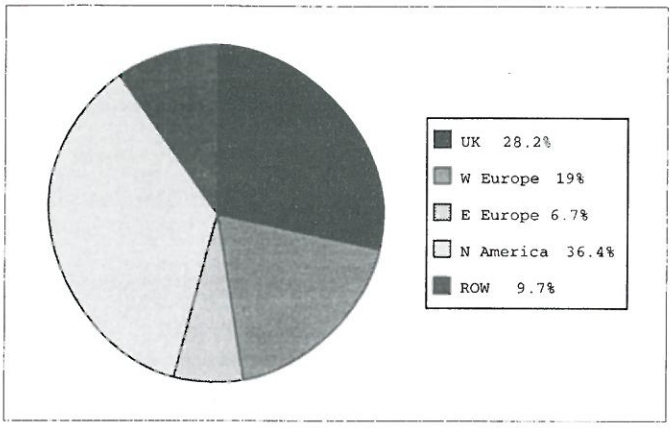



Figure 2: Countries of Residence of Long-Stay Participants

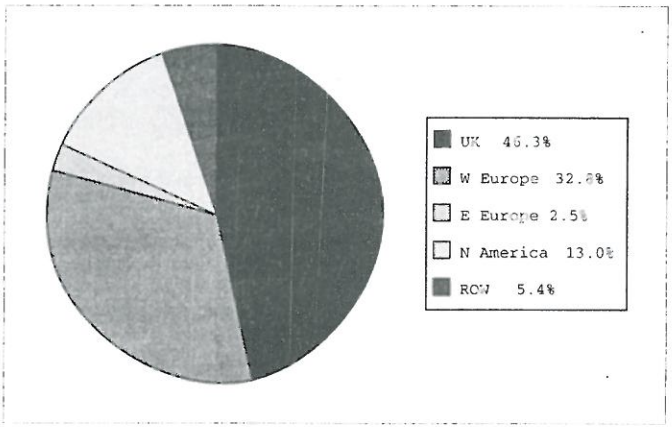



Figure 3: Countries of Residence of Short-Stay Participants

facilities, staff support, financial provision and coffee, tea and lunch arrangements. Participants are also asked to fill out a housing questionnaire. Conference participants are asked to complete a questionnaire requesting evaluation and comments on conference organisation, scientific content, and lunch and accommodation arrangements. These questionnaires are collated and discussed at regular staff meetings, where problems are identified and changes in procedure agreed. Where possible, improvements have been made, for example recent improvements to Seminar Room 1 (see § 13.3). This is seen as a continuing process.

The numbers of younger scientists attending lectures and seminars at the Institute is also monitored (although this relies upon them signing in at reception or being registered as affiliated participants). Numbers of women attending are recorded too. Each long-stay participant is required to write a report on his or her stay, giving details of work done and useful interactions during the visit, talks given in other academic institutions and publications produced or likely to arise out of the visit. These are followed up at regular intervals until publication details are received. On the whole the reports of participants have been positive and often very enthusiastic. A selection of extracts from those reports is quoted here:

**Semantics of Computation:**

I found the visit to Cambridge to be excellent. Most important was that (being from North America) this was the first time I was exposed to a number of my European colleagues over an extended period. It affected my thinking in a way that would have never occurred from just reading their papers...Mainly I found the time to be good for expanding ideas and attitudes; it will have an effect on the problems lasting long after the end of the programme. (Peter O'Hearn, Syracuse)

Relaxed and stimulating atmosphere. (S Brookes, Carnegie Mellon)

During this period most of the leading scientists in the field (from the whole world) visited the Institute and I had the opportunity to have discussions with a large number of them...an immensely stimulating and pleasant autumn. (Peter Dybjer, Chalmers)

The Institute has provided an ideal environment for discussing ideas with researchers from many different specialities, which has had a direct impact on my research. (Philippa Gardner, Edinburgh)

A conducive atmosphere for scientific research. (Robert Harper, Carnegie Mellon)

The Newton Institute provided the ideal working environment, both for the concerted study I needed and because of the collection of researchers who were either here full time or visited during the period of the programme. (CB Jones, Manchester)

The unique environment of the Newton Institute did indeed provide the right mixture of peace and stimulus so that I could fruitfully work out some of these ideas...It has been a great privilege to participate in this programme. (Achim Jung, Darmstadt)

The Institute's unique layout, aimed at fomenting contacts and research between visiting mathematicians is more than an architect's dream: it works. (Jim Lipton, Wesleyan)

The NIMS has offered a rare opportunity for comparing at length ideas developed in different areas. (D Sangiorgi, Edinburgh)

The most significant benefit that I reaped from the Semantics of Computation programme was the opportunity to be able to understand areas of study that I had not been exposed to before and to explore lines of investigation in these areas. (Ramesh Viswanathan, Stanford)

**From Finite to Infinite Dimensional Dynamical Systems:**

I am currently working in several research areas that originated or gained momentum from my visit at the Newton Institute. (Giorgio Fusco, Rome)

The scientific and administrative organization of both conferences was outstanding. (Darryl Holm, LANL)

I think that my visit here will lead to useful scientific cooperation in future. (Victor L'vov, Weizmann Inst)

My visit at the Newton Institute has been fruitful and I have enjoyed it. (Genevieve Raugel, Paris Sud)

This has proved to be a most stimulating and fruitful visit to the Newton Institute. (Jaroslav Stark, UCL)

As a young mathematician working on both finite and infinite dimensional dynamical systems, my research has been greatly benefited from such a stimulating programme... The visit also

provided me a unique opportunity talking with experts in the area of dynamical systems and differential equations. (Yingfei Yi, Georgia Inst)

**Dynamics of Complex Fluids:**

It was incomparable event for this important, challenging and extremely interdisciplinary branch of science. I have learned much more than in decades. (Vladimir Entov, Russian Academy of Sciences)

My time at the Newton Institute has been extremely enjoyable and very precious from a scientific standpoint. The atmosphere provided by the Institute for scientific interaction is unique. Participants are very accessible and the schedules have been arranged and publicised well so as to allow adequate discussion of a topic and enable all interested parties to join in. This has led to many very rewarding discussions and all participants have been extremely generous with their contributions and helpful comments. (Janette Jones, Durham)

I feel very fortunate to have been a participant at the Institute because I have benefited greatly from the programme on the Dynamics of Complex Fluids...It has been a rich six months. (David James, Toronto)

I have been absolutely delighted with my six month tenure at INI. Many thanks to all the people involved in the programme. (Roland Keunings, Louvain)

These visits in particular have stimulated some ideas on future research collaborations. Also, now being on first name terms with many of the leading names in this area of research will surely encourage further contact in the future. (Frank M Leslie, Strathclyde)

During my two-month stay at the Isaac Newton Institute, I have made substantial progress on a number of problems in polymer rheology, as a direct result of the concentration at the Institute of experts in the field. (Scott Milner, Exxon Research)

I found my (unfortunately too brief!) visit here extremely enjoyable. The atmosphere is almost ideal to work in, with easy access to people, well-coordinated meals, library and computer facilities, and best of all, great scientists to speak with. (Peter Olmsted, Michigan)

I participated in the programme on Dynamics of Complex Fluids from 19 February to 11 March 1996. The excellent conditions for scientific work in the INI enabled me to use this rather short period very fruitfully. (Serguey Shiyanovskii, Nuclear Research Inst, Ukraine)

The opportunity to mix with and talk with co-workers has been an exceptional one, and I am very pleased to have been invited to the program. (Roger I Tanner, Sydney)

My sabbatical leave at the Isaac Newton Institute has been a marvellous and fruitful experience. (LR White, Melbourne)

My time at the Institute has helped me open several new topics of inquiry to begin. (T Witten, Chicago)

**Computer Security, Cryptology and Coding Theory:**

I had a very good time at the institute and my stay in Cambridge has been very fruitful. (Mario de Boer, Eindhoven)

What will produce probably the richest results of this visit for me, were the numerous and fruitful conversations, both on professional and non-professional topics, that I had with some of the most prestigious people working in the computer security and cryptology fields who gathered in this programme. Of course, I had met most of them previously in conferences and other workshops,

but never in such a relaxed and friendly atmosphere. (Yves Deswarte, LAAS, CNRS)

I found the Newton Institute very stimulating for my work. (Markus Dichtl, Siemens)

I would like to thank all the staff of the Isaac Newton Institute for Mathematical Sciences for the nice working condition and excellent research atmosphere here. (Cunsheng Ding, Turku)

The Institute is an almost ideal work place...in that the support is excellent so we do not need to worry much about things outside work, the facilities are quite nice, the offices quiet, and we have wonderful colleagues to collaborate with. (Li Gong, SRI Intl)

The atmosphere at the institute was excellent for exchanging ideas. I believe the institute is a very important place promoting research in mathematics. (Tor Helleseth, Bergen)

All in all, this was a very worthwhile visit. (Sushil Jajodia, George Mason University)

The visit gave me inspiring ideas for further work. (Volker Kessler, Siemens)

I spent a very exciting and productive week at the Newton Institute and I seriously regret that my other duties did not allow me to stay longer. The discussions and new contacts will certainly have a positive influence on my future work in the field of Computer Security. (Marcus Kuhn, Erlangen)

My visit will significantly benefit my future technical work. (Carl Landwehr, US Naval Research Lab)

The entire staff of the Institute were both professional and friendly. They made me feel most welcome and certainly facilitated my research whilst there. (Ira Moskowitz, US Naval Research Lab)

This meeting provided an opportunity to discuss the explosive proliferation of outlets for computer security research, its diluting effect on the community, and plans to cope with it. (M Reiter, AT&T)

I had highly fruitful visit. I managed to learn and interact with many people from universities and industrial research and development. (Moti Yung, IBM)

The staff derive considerable satisfaction from such comments but they are far from complacent and are constantly striving to improve the Institute as a stimulating environment for research.

# 4 Young Scientists

We are keen to encourage the participation of research students and young post-docs. It is the policy of the Institute to make information about its workshops widely available, and experience over the last four years has shown that these workshops, especially those with an instructional element, are particularly valuable for young researchers. Research students on EPSRC or PPARC studentships should consult their Heads of Department concerning the possibility of support grants to attend such workshops; exceptionally, funding may be available direct from the Newton Institute for research students recommended by programme organisers.

During the year 1995/96, two NATO Advanced Study Institutes took place. These were aimed specifically at young people. The first, *From Finite to Infinite Dimensional Dynamical Systems* was part of the programme of the same name and the second, entitled *Theoretical Challenges in Complex Fluid Dynamics*, was part of the *Dynamics of Complex Fluids* programme. In addition there were three conferences also specifically for young people which were funded, at least in part, by the European Community. These were *Advances in Type Systems for Computing* which formed part of the *Semantics of Computation* programme; *Finite and Infinite Dimensional Dynamical Systems* which formed part of the *From Finite to Infinite Dimensional Dynamical Systems* programme and *Constitutive Relations and Their Application to Complex Flow Problems* which formed part of the *Dynamics of Complex Fluids* programme.

In total, 210 young people (defined as aged 35 years or less for males, 40 or less for females) were registered as attending these workshops. Of these, 16 were from Cambridge departments, 47 from institutions elsewhere in the UK, and 147 from institutions outside the UK. There were in addition many others who attended individual seminars but did not register for a workshop.

Figure 4: Young scientists at a poster session during the NATO ASI *Theoretical Challenges in Complex Fluid Dynamics*

# 5 Programme 13: Semantics of Computation

**July to December 1995**

Report from the Organisers: S Abramsky (Imperial/Edinburgh); G Kahn (INRIA); JC Mitchell (Stanford); AM Pitts (Cambridge)

## 5.1 Introduction

The capabilities and use of computer systems are increasing at an astonishing rate. Although improvements in computer hardware have provided the raw material for this spiralling development it is software which makes a computer useful. Complex software makes simple hardware powerful and contributes to the simplicity, speed and commoditization of digital devices. Unfortunately the cost of producing and maintaining software systems is vast in comparison to hardware costs, it is often hard to adapt a complicated piece of software to new uses, and worst of all (considering the many critical situations in which it is used) software is often unreliable. Consequently, over the last 30 years or so much effort has gone into the design of new programming languages, new methods of specifying and developing programs, and new formal systems for verifying properties of programs. These developments have sought to address several key issues. How to increase the level of abstraction in programming languages away from the details of particular computer architectures, in order to enhance portability and make code production simpler. How to increase modularity and code reuse in large computer programs. How to design languages that aid the use of formal proof to verify program properties, in order to increase assurance of code correctness and reliability in critical situations. And finally, how to do all these things for the complex, distributed systems that are at the forefront of current practice and which involve non-determinism, communication and concurrent actions. The programme aimed to refine the current mathematical techniques for the semantics of computation so that it is more capable of dealing with these issues. It also aimed to provide a framework for interaction between such fundamental research and the issues confronted by language designers and software engineers.

## 5.2 Organisation

In issuing invitations to participate in the programme, the organisers deliberately targeted three areas where current theoretical developments in semantics seemed especially likely to influence future language design and software engineering practice—namely object-based concurrent programming, projects to develop the next generation of advanced programming languages (such as ML2000), and semantic foundations of reactive systems. Activity was focussed on the first two areas during the first half of the programme, in an attempt to have the present and future needs of practitioners influence the shape of the theoretical work carried out. In particular, the first major event was a one week conference on *Themes in the Semantics of Computation* which mapped out a number of the themes to be addressed over the course of the programme, with particular emphasis on the interface between theory and practice.

A large proportion of the key researchers in all three target areas visited the Institute during the six months, for visits of at least a month, usually longer. For example, nearly the whole of the ML2000 design committee were present during August. Many of the participants commented upon the way in which the internal layout of the Institute fostered discussions and the forging of new research collaborations. Between the periods of workshop activity, there were informal twice

weekly seminars whose speakers included Institute participants, their affiliated graduate students and local participants. The organised activities of the programme centred around two one-week research conferences (on *Advances in Type Systems for Computing* in August and on *Games, Processes and Logic* in November) and five two- or three-day workshops on specialised topics. In addition the programme hosted an extremely well attended, week-long summer school on *Semantics and Logics of Computation* in collaboration with the ESPRIT project 'Categorical Logic in Computer Science', and a final conference on *New Connections between Mathematics and Computer Science* in collaboration with our sister programme and Hewlett-Packard's BRIMS. This quite high level of organised activity did not seem to affect unduly the productivity of the long-term visitors, who were able to be selective in what they attended in order to preserve periods of uninterrupted research. However, it did enable a large number of short-term visitors, mostly from the UK and Europe, to contribute and to benefit from activities of the programme. Extensive use was made of the Internet to circulate information about events. In particular, World Wide Web information pages about the programme were set up by Mitchell and maintained by him and Pitts (see *http://www.newton.cam.ac.uk/programs/sem-home/sem.html*).

In addition to funding received through the Newton Institute budget, the programme received funding for meetings from the CEC, the US Office of Naval Research, the London Mathematical Society, the EPSRC MathfIT initiative, Hewlett-Packard, and Harlequin Ltd.

## 5.3 Meetings

*Themes in the Semantics of Computation* (17–21 July, organiser: Abramsky)
This conference mapped out a number of the themes to be addressed over the course of the programme, with particular emphasis on the interface between theory and practice. A number of distinguished researchers (Freyd, Hoare, Jones, Kahn, Milner and Reynolds) gave keynote lectures in which they reviewed the current state of their art, and identified key problems to be addressed. Each of them had been invited to nominate two or three speakers on topics related to their theme; there were also some sessions of contributed talks during the week. It was a week combining intellectual stimulation with sobering reminders of how great a gap there can be between theory and practice. In particular the keynote talks and the frank and wide-ranging discussion which they provoked seemed to be greatly appreciated by participants.

*Advances in Type Systems for Computing* (14–18 August, organisers: Mitchell and Pitts)
This Euroconference consisted of invited lectures, contributed papers, and on-the-spot contributions to impromptu sessions that were organised during the meeting. There were a total of 73 participants (including 24 programme participants, 3 outside invited speakers, and 24 authors of contributed talks) who came from seven European countries as well as from the USA, Japan and fSU. The conference focussed on recent developments in the use of typing in computing, with particular emphasis on three related areas: extensions of the ML type system; types in object-oriented programming; and type theories for reactive systems. A surprisingly large fraction of the invited and contributed talks emphasised type systems for object-oriented programming. In fact, this active and vibrant area accounted for 6 of 12 invited talks and 12 of 22 contributed talks. As a result, the conference had an unexpectedly sharp focus, leading to repeated discussion of type systems for object-oriented programming during coffee breaks and free time.

*Summer School on Semantics and Logics of Computation* (25–29 September)
The first three months of the programme came to an end with a week-long summer school organised by P Dybjer (Chalmers) and Pitts, funded by the CEC ESPRIT project 'Categorical Logic in Computer Science'. The aim was to present a number of modern developments in

semantics and logics of computation in a way that would be accessible to graduate students. Lecture courses were given by Abramsky, T Coquand (Chalmers), M Hofmann (Darmstadt), M Hyland (Cambridge), E Moggi (Genova), M Nielsen and G Winskel (Aarhus), and Pitts. The school proved very popular, and was over-subscribed. The 106 participants were mostly graduate students and post-doctoral researchers, together with a small number of established academics. A volume based upon the lecture materials will be produced in the CUP Newton Institute Publication Series, edited by the two organisers. (Some participants also had the dubious pleasure of appearing as extras in the BBC Horizon documentary on Wiles' assault on Fermat's Last Theorem which happened to be filming at the time.)

*Games, Processes and Logic* (6–10 November, organiser: Abramsky)
There are long-standing connections between the mathematical theory of games and logic. For example dialogue games have been used in Proof theory. More recently, similar types of dialogue game have been applied to the semantics of computation, in a variety of ways. For example, they provide an intrinsic model of interaction between a system and its environment, with processes modelled as strategies. The workshop brought together researchers pursuing these various strands, to compare and contrast the different approaches, and to take stock of current progress and future directions. The range of the talks at the meeting, spanning ideas from category theory and logic through to a systematic treatment of abstract machines for functional languages and their connection with games, showed the very lively state of current research in this area. Close links to Linear Logic were in evidence throughout.

*New Connections between Mathematics and Computer Science (20–24 November, organiser: J Gunawardena)*
The interplay between mathematics and computer science has traditionally centred around areas in logic, category theory and discrete mathematics. In recent years new connections between mathematics and computer science have emerged from such unexpected quarters as algebraic topology, differential geometry, dynamical systems and operator algebras. The workshop brought together mathematicians and computer scientists from this programme and our sister programme on dynamical systems, together with a distinguished list of invited speakers, for a series of tutorials and discussions on these 'new connections'. The result was an eclectic, but extremely stimulating week. Financial support was provided by Hewlett-Packard, the London Mathematical Society and the MathfIT initiative of the EPSRC.

*Short Workshops*
The workshop on *Semantics for System Design* (10–12 July, organiser: CAR Hoare) stimulated discussion of the top-down approach to semantics for system design. The workshop on *Category Theory and Logic Programming* (18–19 September, organiser: J Lipton) featured talks on the categorical foundations of logic programming, categorical approaches to declarative programming and program synthesis, and foundations of relational computing. The workshop on *Linear Logic and Applications* (16-18 October, organiser: G Bierman) was focussed on a topic—Linear Logic—which in fact featured more or less explicitly in a surprisingly large number of the activities throughout the six months. The workshop on *High-level Concurrent Languages: Foundations and Verification Techniques* (2-4 October, organisers: M Hennessy and B Pierce) brought together programming language designers and concurrency theorists to share both ideas and problems, focussing on what can be achieved with present-day tools and techniques and on the search for better semantic foundations for such languages. The workshop on *Higher Order Operational Techniques for Semantics* (28-31 October, organisers A Gordon and Pitts) addressed current developments in operational techniques for the semantics of higher-order languages. These included operational techniques for proofs of properties of type systems and for program verification, using observational or contextual equivalence, (applicative) bisimulation,

and Hennessy-Milner logics. Sponsorship from Harlequin Ltd enabled the organisers to invite a number of key speakers who would not otherwise have participated in the programme. Since several of the techniques discussed during this workshop are not well represented in the literature, the organisers plan to produce a volume of surveys and selected research papers arising out of it.

## 5.4 Participation

The programme involved 51 long-term participants, whose average length of stay was eleven weeks, 13 of whom stayed five months or more. Several of these participants sponsored their graduate students as affiliated members of the programme. There were an additional 38 short-term visitors, and approximately 400 registrations for the various organised events. Of the long-term visitors 14 were from the UK, 13 from other EC countries, 22 from the USA, and 2 from other countries. Japanese research in this area was under-represented (the one long-term visitor who accepted an invitation from the organisers had to drop out at a late stage due to ill health). On the other hand, the relatively small amount of research relevant to the programme carried out in the fSU and Eastern Europe was reflected in the quite small numbers of participants from these countries. Seven of the long-term visitors were from industrial research laboratories, the rest from universities or national research laboratories. There were no deaths or marriages amongst the participants, but there was one birth.

## 5.5 Achievements

As might be expected, the programme resulted in the strengthening of some existing research collaborations and the forging of several new ones. At least two edited books will be published in connection with the programme (one containing the material presented at the Summer School on *Semantics and Logics of Computation* and the other arising out of the workshop on *Higher Order Operational Techniques for Semantics*). Groups of participants also collaborated on some short "survey and open problems" papers summarising particular areas of interest to the programme, details of which will be made available via the programme's Web pages.

We briefly highlight below some of the scientific achievements of the programme.

*Simplified Standard ML*
The programming language ML (Milner *et al*) was originally devised as a programmable metalanguage for machine-assisted proof. From those origins have grown a number of mature languages used and supported not only within academic research, but to a certain extent commercially: both AT&T in the US, and Abstract Hardware and Harlequin in the UK are investing in ML development. Amongst existing flavours of ML (indeed, amongst all programming languages, sad to say) Standard ML is unusual because a fully formalised definition of its semantics was produced in tandem with the design of its syntax. One important development of the programme was that Harper, MacQueen, Milner, and Tofte formulated a revision of Standard ML, called Simplified Standard ML (SSML). This is intended to correct a number of errors in the existing semantic definition and, more importantly, eliminate some of the more problematic constructs in favour of much simpler mechanisms that have emerged from research in the last few years. Subject to agreement with industrial and academic collaborators and the user community, the authors expect to announce the definition of SSML during the first half of 1996.

*ML2000*
The purpose of the ML2000 project is to design a programming language that extends Standard ML to include support for higher-order modules, object-oriented programming and concurrency, whilst preserving the nice properties of the original language. The project is an informal collaboration between a group of researchers, most of whom participated in the programme. Substantial progress was made on the design of the so-called "internal language" of ML2000. This is a polymorphic typed lambda calculus which serves as the target of the elaborator (which translates from the full, "external language" by eliminating derived forms and performing type reconstruction) and as the source language for the compiler proper (which translates the internal language into machine code). The definition of the internal language is a very important step which essentially determines the semantic structure of ML2000. A key issue in its design is how best to treat object-oriented programming. By bringing together such a concentration of experts on this topic, the programme enabled the ML2000 team to work through difficult questions about this issue much more rapidly than would otherwise have been the case. A draft design of the internal language has now been produced by Cardelli and Harper.

*Typed Object-Oriented Programming*
Type systems for programming languages with object-oriented features are a topical and important area since this style of programming provides one promising approach for improving software productivity. Scientific progress on the underlying type systems of object-oriented languages aids our understanding of software development, leading to improved programming languages and more effective program-development tools. Such progress has been hampered by the lack of a clear analysis of what are the **fundamental** features of the object-oriented style and how they are related to each other. The discussions produced by the *Advances in Type Systems for Computing* conference went a long way towards providing such an analysis for concepts such as 'subtyping' and 'inheritance'. By bringing together experts on object-oriented languages, on type systems, on concurrency theory, and on operational semantics, the programme also fostered several promising assaults on the hard area of verification methods for such languages. For example Jones, Hodges, Pierce, and Sangiorgi began to develop bisimulation-based methods to prove correctness of Jones' concurrency-introducing transformation rules in his object-based design language; and Gordon and Rees were able to contribute operationally-based methods for equivalence of objects to the extensive work Abadi and Cardelli are carrying out on primitive object calculi.

*Semantic Foundations*
The programme brought into sharp focus a couple of trends which are taking place in the mathematical foundations of program semantics.

First, the programme emphasised the huge and rather surprising way in which Girard's Linear Logic has pervaded the subject. Three varied examples from the many which featured in the programme: the work of Lincoln, Mitchell and Scedrov on classifying computational complexity classes; the work of O'Hearn-Reynolds, Pitts and Stark on using relational parametricity to reason about properties local variables; and the work by Abramsky, Hyland and others on the game-theoretic analysis of computation. One particularly intriguing aspect of this last example is the connection which was made during the workshop on *Games, Processes and Logic* between the work of Joyal on free bicompletions of categories, and that of Blass on game semantics for Linear logic. This opened up the challenging problem of finding a good game theoretic representation of Joyal's construction, whose solution would represent a significant advance in this field. This stimulated subsequent work by Hyland and his co-workers at Cambridge.

Secondly, the methods of Scott-Strachey denotational semantics are increasingly being replaced by more refined, 'intensional' methods. Three examples of this phenomenon whose development

was fostered by the programme are: Abramsky's use of categories of dialogue games to give a model of Algol-like languages treating local state in an abstract, 'process-theoretic' manner; the work of Gardner, Milner and Power on Milner's 'Action Calculus' framework for describing and classifying different types of interactive process; and the development by Birkedal, Harper, Mitchell and Pitts of operationally-based logical relations for proving properties of recursively typed languages. The last example was but one of a number of program verification methods discussed at the lively workshop on *Higher Order Operational Techniques for Semantics* which combine ideas from denotational semantics with operationally-based techniques originally developed in the context of concurrency theory.

*Theory-Practice Interaction*

One of the ambitions of the programme organisers was to provide a framework for interaction between fundamental research and the issues confronted by language designers and software engineers. The developments to do with ML described above were an important contribution to such interaction. Some other examples which developed during the programme are: the use of theoretically-motivated programming features (such as constraint- and object-based methods) by Cardelli, Saraswat and others for programming multi-user, content-based applications on the Internet; the conversion of proofs in the mathematically precise form of lambda terms into humanly intelligible proofs in natural language being developed by Kahn; and the development by Gunter of a new theoretical model for representing dependencies between software configuration items and its application to a collection of examples which have emerged as important problems in configuration maintenance for substantial projects.

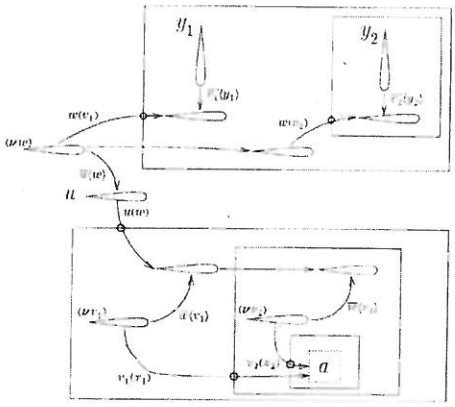



Figure 5: A graphical representation of an action in the $\pi$-calculus, a formalism for expressing processes that evolve through the concurrent communication of names of processes. [R. Milner]

# 6 Programme 14: From Finite to Infinite Dimensional Dynamical Systems

**July to December 1995**

Report from the Organisers: P Constantin (Chicago); JD Gibbon (Imperial); J Hale (Georgia Tech); C Sparrow (Cambridge)

## 6.1 Introduction

In general terms, the programme concerned itself with global dynamical aspects of systems with many degrees of freedom. To this end, it brought together experts in both low dimensional dynamics and PDEs, as well as those who study other high dimensional problems such as lattice dynamical systems, delay differential equations, and high but finite dimensional systems. Many participants had particular interests in dynamical phenomena that are relevant in a variety of these areas, such as pattern formation, scaling phenomena, or existence and properties of attractors. Major sources of examples of systems of interest are nonlinear and statistical physics (incompressible fluids, convection, condensed matter) and biological systems; these all featured often in the programme, which attracted experts in these areas and in relevant numerical methods. Overall, we felt the programme had a good balance between mathematics and its applications.

Figure 6: Striped roll patterns with dislocations from an experiment with chlorite-iodine-malonic acid reaction [Reproduced by kind permission of Q Ouyang and H Swinney]

It became apparent over the course of the programme that there were two main clusters of long-term participants; those with a more physical (but not necessarily less mathematical) interest in fluids, turbulence, the Euler and Navier-Stokes equations etc, and those interested primarily in developing a dynamical systems approach to more well-behaved infinite dimensional systems. Both groups made considerable progress and spawned numerous collaborative endeavours. We were fortunate both that there were many participants with interests broad enough to encompass aspects of both these approaches, and that almost all participants made an enormous effort to understand and benefit from ideas and techniques very different from their own. Indeed, the primary aim of the programme was to develop a common understanding and mathematical language needed to fill in the large gaps between the areas where expertise is already well-developed, and it will only be possible to judge the ultimate success of the programme in this area in several years time. Certainly those of us on the programme were enormously impressed by the willingness with which almost all participants participated in this common endeavour, to their mutual benefit and, hopefully, to the ultimate benefit of the subject. As one participant wrote, 'I believe we will all approach our problems in a different way in future. This may not be apparent in the short run, but it will be clear in the long run to those that attended.'

## 6.2 Main areas of scientific activity

Several main scientific directions emerged from the programme which cut across fields and workshop topics, and many interesting collaborations developed between experts in different areas. Some of these are described below.

1. Open systems: bifurcations, dissipativity and finite dimensionality in the presence of continuous spectra. This is an emerging area of research which contrasts with the inertial manifolds type of finite dimensionality that occurs with a discrete spectrum. Aspects of the topic were discussed formally, for example, in the ASI lectures of Collet and Holmes, and in other talks by Spiegel and Feireisl. There was also much useful informal discussion in this area: the field is at a stage in which questions are beginning to be formulated.

2. Dependence of dynamics upon parameters, especially under singular perturbation: semicontinuity of attractors, inviscid limit (Hale, Constantin, Raugel, Mahalov, etc). The question of the inviscid limit has been one of the central issues in fluid mechanics for many years. The problem is essentially open in the case of bounded domains because a deep understanding of turbulent boundary layers at a mathematical level is still lacking. Recently there has been some progress in the study of the inviscid limit for non-smooth vorticity in the whole plane. The study illustrates the non-universal features of 2D turbulence and presents challenges to the existing equilibrium statistical mechanics descriptions based on microscopically constrained mean field theories. (See below). Mahalov presented results regarding averaging over fast modes in stratified rotating fluids.

3. Universality: scaling in statistical and nonlinear physics, normal hyperbolicity in nonlinear dynamics of PDEs and ODEs. This theme was discussed in the workshop organised by Procaccia, and in the talk of Bates, for example. The hope that a statistical description of complex high dimensional dynamical systems can be accomplished is based on the idea of the existence of universality classes, for which certain determining characteristics are constant. Such classes are hoped to be defined by scaling exponents of structure functions. The persistence of normal hyperbolic structures in PDE is a potentially useful tool for the realisation of the idea that a classification of statistical properties of complex high dimensional dynamical systems is possible. L'vov and Procaccia made considerable progress in their physical theoretical attempt to describe the scaling exponents arising in strong fluid turbulence. Pomeau described his critique of weak turbulence theories.

4. Statistical description of dynamics: coupled lattice maps (Bunimovich), statistical physics of vortices in two dimensional incompressible fluids (Constantin). Following original approaches by Onsager, Montgomery, Joyce, Kraichnan and others, more recently Jonathan Miller and R. Robert proposed mean field theories based on equilibrium statistical mechanics of vortices in the presence of infinitely many constraints. Independently, Caglioti, P.L. Lions, Marchioro and Pulvirenti have analysed the Onsager, Montgomery, Joyce few constraints theories. The predictions of these theories are that the statistical behaviour of 2D decaying turbulence is described for inviscid time scales by certain nonlinear PDEs; the fact that these PDEs depend on frozen microscopic constraints that are very sensitive to viscous perturbation (see above) presents a challenge to the mean field picture. The parallel approaches of Majda and Constantin to this puzzle have been clarified during the programme. Majda has given evidence for the robustness of the few constraints theories, if one asks for very rough ($L^2$) correlation. Constantin gave evidence for the divergence from the inviscid limit in the case of infinitely many constraints.

5. Role of singularities in fluids. This became one of the central themes of the programme, and featured in the workshop organised by Constantin, and talks elsewhere by Pomeau, Gibbon,

Moffatt and others. The question of the existence and role played by putative singularities in incompressible fluids was addressed numerically by Kerr, Sulem, Krasny, and theoretically by Pomeau, Gibbon, Moffatt, Constantin and others. The need for geometrical-analytical criteria has emerged as a common ground.

6. Finite Dimensional Dynamics. It was inevitable given the participants that there would be some progress in purely finite dimensional problems. Rand & Pinto made considerable progress in their work on moduli spaces and rigidity for maps; Stark & Broomhead continued their work on geometric approaches to time series; Yi's work on the bifurcations of quasi-periodic solutions was of interest to many participants; and Afraimovich presented results on multipliers for homoclinic orbits.

7. Biological applications. A specialist workshop (see below) brought in many experts towards the end of the programme, but applications from biology made frequent appearances throughout the programme. Indeed, the first seminar of the programme (Glass) was on cardiac dynamics, and biology was a constant source of problems and examples (in for example, pattern formation, and in the symmetry workshop). Interaction between those with biological concerns and mathematicians was facilitated by Rand's 6 month stay at the Institute.

In addition to the collaborations mentioned above, there were many others, some of which were apparent to all at the programme, and some of which happened more quietly but are reported in participants individual Final Reports. A few of these, selected more or less at random, are: Titi & Gibbon produced the best estimate to date for the 3d Navier-Stokes attractor dimension; Procaccia & Gibbon started a collaboration on vortex tubes in turbulence; Doering & Constantin improved a theory that reproduced the correct Nusselt vs Rayleigh number scalings across a wide range of the latter; Bates, Fife & Nishiura started joint work on the dynamics of micro-structures; Titi & Collet completed a paper on determining modes for the Ginzburg-Landau equation in unbounded domains; and Feireisl & Polacik started an intense collaboration on the asymptotic behaviour of time-periodic reaction-diffusion equations.

## 6.3 Organisation

The programme proposal was constructed after extensive consultation with the Dynamical Systems community in the UK and elsewhere. Given this beginning, it was natural that the programme would develop in two directions: first, a coherent strategy of concentration on specific areas of interest to the organisers and other long-term participants; second, as a vehicle for the wider dynamics community. The first direction is mainly that described in the introduction above, and many of our workshops, particularly the smaller ones, were firmly focussed in this direction, with workshop participant invitations targeted at experts who could be expected to interact in an intense way on particular topics. The second direction was represented by our willingness to 'host' workshops on topics that were somewhat peripheral to the main direction, but which drew in large numbers of dynamical systems and other UK and international participants. We feel strongly that the two directions were complimentary rather than contradictory, and that the programme benefited from both.

One consequence of this dual approach was that the Institute became very busy, and at times very crowded. This caused difficulties for the administration, and very occasionally for the participants. It was perhaps unfortunate that the parallel programme, Semantics of Computation, was also one of the more active of recent programmes, so that between us there were few weeks of 'quiet' in the Institute. In general, however, we felt that the programme went as planned and was an organisational as well as scientific success. We are very grateful to the staff who worked

so hard to make it a success, and to the participants who were almost entirely sympathetic to the need to squeeze and share in periods of very high occupancy.

The programme was widely advertised, in particular as the world wide web and majordomo e-mail systems came on-line. It appears that interested persons in Cambridge, the UK, and internationally felt well-informed about the activities of the programme.

We were pleased to obtain additional financial support for workshops as detailed in the section below, and are grateful for support from the Cambridge Philosophical Society for K Wiklund, and for the Rosenbaum Fellowship which allowed Y Yi (Georgia Tech) to spend a fruitful 6 months with the programme. We were happy to welcome three Japanese visitors supported on the RIMS exchange scheme; they made substantial useful contributions to the programme.

Prof Jack Hale held the Rothschild Visiting Professorship for the duration of his stay at the Institute. Several participants secured connections of one kind or another with Cambridge Colleges. In particular, Profs Hale and Constantin held Visiting Fellowships at Emmanuel and Clare Hall respectively.

Our major organisational failure was to secure the long-term participation of various UK experts who had expressed an early interest in the programme. This seems to be a structural difficulty – such persons often have serious responsibilities in their own universities, and projected visits of several months slowly shrink to weeks and finally days as events overcome them.

## 6.4 Seminars, Workshops and Conferences

The programme structure was built around a NATO ASI, a large research Euroconference and by a series of workshops. Two organisers (Gibbon, Sparrow) were present for the whole programme. Hale arrived in July, Constantin in August, and both left in November. Activities most closely related to the central themes of the programme took place in the period August to October. Outside this period workshops were organised on related but more peripheral themes. In chronological order the organised activities were:

*Regular seminars.* During non-workshop weeks we held regular seminars on Tuesdays and/or Thursdays. These were mainly attended by participants and local Cambridge mathematicians, though they were widely advertised. In particular, during July and August a series of excellent introductory seminars by organisers Hale and Gibbon explored techniques and results in a range of areas that were to be covered in more depth later in the programme. These seminars set the constructive tone that was to dominate attempts throughout the programme to speak a common mathematical language, and were of great benefit to those long-term participants who arrived early enough to attend.

*Workshop: Finite Dimensional Dynamics,* 24-28 July. This meeting, organised by P Glendinning & C Sparrow, started the transition from finite to infinite by concentrating on one and two dimensions. We were able to bring together many experts in one-dimensional dynamics (e.g. Strien, Nowicki), and other high-points included the talk by Ya Pesin. The week included a preview of what was to come, with talks by D Levermore (Arizona) and his co-workers. We were able to support many of the European short-term visitors to this workshop from external sources.

*NATO ASI,* 21 Aug - 1 Sep. This meeting, organised by P Glendinning (DAMTP), was in many ways the high point of the programme. Nearly every lecture series was excellent, and lecturers, students and programme participants all benefited enormously. Two or more lectures were

given by each of Ball, Bunimovich, Carr, Collet, Constantin, Coullet, Cvitanovic, Glendinning, Hale, Holmes, Procaccia and Rand, covering between them most of the themes and applications discussed elsewhere in the programme. The ASI proceedings should be excellent and will be published by Kluwer. Funding of approximately 40K was obtained from NATO, and we are able to support additional students from external sources.

*Euroconference,* 4 Sep - 15 Sep. This two week research meeting was organised by J Robinson (DAMTP) and followed immediately after the NATO ASI. Many students stayed on for this meeting, as did other short-term programme participants. The meeting complemented the ASI nicely, and included sessions organised by T Mullin (Oxford) from experimentalists. We were able to supplement the Euro conference support for this meeting with further contributions from external sources.

*Workshop: Singularities in PDEs,* 28 Aug - 1 Sep. P Constantin organised this small discussion meeting that focussed on a theme central to the interests of many programme participants. Circumstances outside our control obliged us to hold this workshop in parallel with the second week of the ASI, but this has advantages as well as disadvantages. The meeting was intense and well-organised with a good balance of mathematics, numerics and more physical approaches.

*Workshop: Inertial Manifolds, Approximate Inertial Manifolds, and Nonlinear Galerkin Methods,* 9-13 October. This meeting was organised by E Titi and was attended by about 40 short-term visitors including many leading experts in the field. This is a fairly 'mature' area, and many discussions were focussed on detailed technical matters. With hindsight, a shorter meeting more focussed on connections with the other themes of the programme might have been even more useful, but the meeting was in any case a success.

*Scaling phenomena in nonlinear physics,* 16-20 October. This very small workshop (organised by Procaccia) focussed on one theme of the programme, and involved a core of programme participants and a very small number of short-term visitors. There were few formal seminars, which left time for several intense, extended and fruitful discussions.

*Pattern Dynamics,* 23-27 October. Organised by Rand, Fife, Glendinning and Hale. This meeting explored different approaches to understanding Pattern Formation in high dimensional systems. The organization of this workshop was a little late, but attracted a high-quality of participant and generated much discussion; everyone learnt something. It was attended by most programme participants and about 12 experts imported for the duration of the workshop or a little longer.

*Dynamics and Symmetry,* 30 Oct - 3 Nov. This meeting attracted about 40 participants, and was organised by D Chillingworth (Southampton). The concentration of mathematicians was high, and the meeting might have benefited from more applications. It did, however, provide a useful summary of where we have got to using symmetry in low dimensional problems; there is room to develop many of the ideas further for high dimensional problems, and this led to useful discussions. We were very grateful to receive additional funding (2K) from the LMS in support of this workshop.

*Piecewise Linear PDEs,* 16-17 November. This short and small meeting was organised by Doole and Hogan from Engineering Mathematics, Bristol. The problems addressed are interesting and do not receive enough mathematical attention. The approach adopted was noticeably different from the rest of the programme, but hard work led to interesting and informative discussions.

*Current Issues and Controversies in Biological Dynamics,* 27 Nov - 1 Dec. This meeting was organised by D Rand (Warwick) and consisted of 2 days on Virus and Immune System Dynamics, a day each on Pattern Formation in Biological systems, and dynamics in Ecology and Epidemics,

and ended with a day for discussion. The meeting attracted approximately 40 participants, and generated (or encouraged) many interesting discussions and disputes. We were grateful to receive financial support (2.5K) from the Wellcome Trust for this workshop.

*Accuracy and error control in ODE and PDE systems,* 4-5 December. A small workshop of about 12 participants organised by D R Moore (Imperial), fell into the straight numerical analysis tradition. It would have been interesting to tie this workshop into the main theme of the programme more solidly, but the time available was very short.

*PDEs and low order models,* 6-8 December. This workshop, organised by Proctor, Rucklidge and Weiss from DAMTP, attracted approximately 35 participants mainly interested in low dimensional ODE models derived from or with similar behaviour to various PDEs. Highlights included the lecture by Busse, and welcome interaction between the dynamics community in DAMTP and those participants who had not yet departed.

*Other activities.* In addition to the above we held a reasonably well attended *LMS Spitalfields Day* on Saturday November 11th, at which Hale, Gibbon, Constantin and Titi talked to a largely general audience. In many ways it was odd to hold this event so late in the programme, but by so doing we were able to illustrate that participants with very different approaches had drawn close enough together during the course of the programme to give four talks in a common language that made a coherent and scientifically satisfying whole. Participants in the programme also enjoyed and benefited from interacting with the participants in the workshop *New Connections between Mathematics and Computer Science,* 20-24 November, organised by Jeremy Gunawardena of BRIMS somewhere in the literal and metaphorical space between our own programme and the Semantics of Computation programme. Constantin and Fife gave talks in the Institute's Monday seminar series.

# 7 Programme 15: Dynamics of Complex Fluids

**January to June 1996**

Report from the Organisers: TCB McLeish (Leeds); JRA Pearson (Cambridge); K Walters (Aberystwyth)

## 7.1 Introduction and Objectives

Many fluids of industrial, biological and environmental importance (e.g. molten plastics, salad dressings, whole blood, sinovial fluid, clay and cement slurries, volcanic lavas) respond in a complicated fashion when deformed. the reasons for this complexity can be traced back to their molecular structure, which may itself b very elaborate, to microscopic supramolecular structures into which they assemble themselves and to the fluid mechanical forces that act between molecules and structures.

Many theories and explanations for their behaviour have been developed, using the techniques of statistical mechanics, thermodynamics and continuum mechanics. However many of these theories only cover part of this complex behaviour and are not readily applicable to industrial, medical or geomechanical problems, where quantitative predictions are required.

The key concept for constitutive behaviour is a mathematical model embodying physical insight into the behaviour of a particular material. Covering the full range of behaviour of most systems involves modelling on a wide range of length and time scales. Much of the difficulty experienced in seeking complete explanations of behaviour is connected with passage from smaller to larger length scales; in embedding the rheological equation of state into the conservation equations governing mass, momentum and energy. Most of the mathematical problems that arise involve non-linear differential, integro-differential and integral equations: a full range of analytical and numerical techniques has to be employed to obtain solutions.

The aim of the Programme was to bring together experts in all these approaches; to confront the assumptions of one group with the predictions of another; to discover what underlying problems were preventing progress and whether an extension of conventional approaches could overcome this; to widen the horizons of all.

## 7.2 Organisation

Invitations were sent in 1994 to leaders in the field all to spend from 3 to 6 months at the Institute. Some were prevented by other commitments from making other than short visits, but the response from all was very enthusiastic. Several suggested other younger invitees. As a result a broad and balanced representation of specialities and backgrounds was achieved.

To encourage concentration on particular topics over shorter periods, a skeleton structure was agreed, which had obvious advantages for short-term visitors wishing to be brought up-to-date in specific areas. The sequence chosen was:

| | |
|---|---|
| January | Polymeric systems |
| February | Surfactants and liquid crystals |
| March | Colloids |
| April/May | Constitutive modelling and boundary-value problems |
| May/June | Computational issues |

The idea was to start with particular materials, emphasising their constitutive properties, rheological behaviour and associated problems. Molecular and structural theories would be to the fore. This was to be followed by consideration of more generic, continuum mechanical theories, suitable for description of complex flows of complex fluids. The last phase was intended to cover the solution of continuum flow (boundary value) problems by analytical and computational means, revisiting the individual materials insofar as computational issues arise in predicting their constitutive behaviour from structural models.

This proved to be helpful; fortunately this arrangement was not intended to be exclusive and so some activity continued throughout on all topics.

Frequent seminars (sometimes 4 in a week), both formal and very informal, were arranged and attended by most participants in residence. These ensured that short-term visitors rapidly made their presence and interests felt. Much of the detailed personal work done by participants during the Programme stemmed from issues raised at seminars.

Most significant in determining attendance was the choice of workshops, meetings and study groups which were advertised in advance. Much care was given to issuing special invitations to workers on the fringe of the subject whose approaches and insights would be valuable to core participants and vice-versa. Again we had a remarkably enthusiastic response. The restriction to about 100 proved a positive advantage.

Much use has been made of the www and e-mail and special thanks are due to CJS Petrie in this context; he also organised a one-day symposium in *Celebration of A Complex Fluid Career*, that of one of the organisers (JRAP).

## 7.3 Meetings

*Workshop on Unresolved Experimental Dilemmas* (8–12 January)

This meeting was intended to provide "food for thought", to describe new observations and phenomena that could usefully be investigated theoretically. It proved to be outstandingly successful in that it provided the basis for much of the new work carried out, and influenced the subjects discussed in seminars, throughout the Programme. It had a strong international flavour, but was fully representative of U.K. work. A poster session was necessary to accommodate all presentations. The proceedings will appear in the Journal of non-Newtonian Fluid Mechanics.

*NATO-ASI on Theoretical Challenges in Complex Fluids* (24 March–4 April)

This remarkable workshop drew a particularly high-calibre team of lecturers from seven countries, and a full complement of students from over 15 countries, both within and without NATO. The principle aim was to present an overview of current molecular and microstructural theories of complex fluids, focussing particularly on entangled polymers, colloids, surfactants and liquid crystals, and trying to point out similarities and differences in approach. Close link with experiments was ensured by incorporating an experimental presentation at each stage of the workshop. The gentle pace of four lectures per day allowed extended discussion periods, which were particularly memorable for their high creative quality. Several research projects can be traced back to the ASI. A full social programme, both formal and informal supported the atmosphere of international co-operation.

*Euroconference on Constitutive Relations and their Application to Complex Flow Problems* (15–19 April)

This workshop covered continuum models for bulk behaviour of viscoelastic fluids (mainly polymeric systems), liquid crystals, foams, emulsions, suspensions and granular media. Models based on Brownian dynamics and various meso-scale structures were described. Special attention was given to near boundary effects that at a continuum level appear as boundary (interfacial) conditions. Examples of the solution of boundary-value problems by analytical or computational methods were given.

*Joint INIMS/DSM Symposium on Rheology/Chain Structure Relationships in Polymers* (14–15 May)

This symposium brought together a large number of industrial and academic workers, the latter mainly composed of participants on the Programme. It was a useful opportunity for the former to explain the interests and constraints of industry and for the latter to explain how their models could be useful.

Three other associated or jointly organised meetings took place outside the Institute.

*Royal Society of Chemistry Colloid and Interface Science Group Conference on Colloidal Aspects of Complex Fluids* (Cavendish Laboratory 26-28 March)

*Drilling Fluids Workshop* (Schlumberger Cambridge Research 11-12 April)

*The Royal Society - Unilever Indo - UK Forum on Dynamics of Complex Fluids* (Cavendish Laboratory 24-28 June)

This provided a suitable finale for the Programme. Session topics included polymers, self-assembled systems, particulate dispersions, visco-plasticity and complex flows, and this reflected the spread of interests of the Programme. There was a deliberate emphasis on computer simulations. The proceedings will be published by Imperial College Press.

## 7.4 Participation

The Programme attracted over 70 participants of whom a core of 20 spent over 3 months at the Institute. They ranged from recently retired Professors to research students and young post-doctoral workers. The Americas, Europe, Asia and Australasia were all represented; special funding facilitated the participation of several eastern Europeans whose characteristic broadly based ways of thinking about shared problems provided a welcome stimulus.

Participants came from a range of disciplines in the physical sciences, engineering and mathematics, but in practice had no difficulty in sharing the common language of traditional applied mathematics and mechanics. There were differences in emphasis and objectives: some concentrated on the characterisation and modification of materials, some on their behaviour in industrial processes, while some were most concerned with mathematical niceties. The extent to which everybody sought to appreciate the interests of others was most gratifying.

## 7.5 Achievements

Because of the very wide spread of interests and activities, this report on the achievements of the Programme has inevitably to be a rather personal account. Speaking to other participants

made clear to us all that everybody has benefited significantly from the chance to work in a lively environment and many have carried away with them a range of ideas and problems to pursue in the future. Each of us has our own list of those moments when the significance of some part of other people's work dawned on us. not surprisingly these moments sometimes came during the re-presentation of earlier work, the importance of which had been heightened by more recent investigations. Advances were evolutionary rather than revolutionary.

*Polymer melts*

Most early work on modelling the rheology of polymer melts was based on long flexible chains of equal length. Only more recently have the effects of branches been systematically and rigorously included; significant developments occurred during the course of this programme, much of it provided by UK workers. Polymers now come as stars, combs and pom-poms, each with its own constitutive relation cast in the style of the celebrated Doi-Edwards equation. Polydispersity has been included. It is not clear what consequences these new ideas will have for process modelling.

Fiber spinning experiments based on screw extrusion and carried out over a range of temperatures, output rates and spin-line lengths, for both linear and branched polyethylenes, were shown to exhibit remarkable similarity, leading to a single grand master curve for each material. This unexpected result led to a re-examination of the predictions of existing model equations and suggested potential simplifications of these models. It was noted that axial stresses dominated in both die and free fiber and that die swell appeared to be representable as a discontinuity linking two kinematically distinct flows (one a non-uniform extensional flow, the other a non-uniform simple shear flow). Velocity profiles were consistent with the simple notion of a purely elastic region followed by a strongly viscous region.

*Polymer solutions*

These continue to be the favoured system for much experimental work, particularly because they often show constant shear viscosity in uniform steady simple shear flow. Observations have been compared with a series of visco-elastic models which come equally from continuum mechanics and statistical mechanics; these include the Upper Convected Maxwell model, the Oldroyd (8-constant) model, the FENE (finite extension non-linear dumbbell) and FENE-P models, the Phan Thien-Tanner and Giesekus models; the simplest forms of these models relate to monodisperse systems (polymer chains of equal length) though addition of contributions to the stress tensor allow for poly-dispersity.

It has long been known that uniaxial or biaxial extensional flow provide unique and sensitive tests of rheological models; recent experiments reported during the programme have enabled far more sensitive comparisons to be undertaken; significant improvements in understanding the relations between elastic and viscous behaviour in extensional flow were described (see above); a consistent explanation of the apparent success of single-mode (relaxation time) models in matching experimental observations in multi-mode systems was put forward. Increases in computing power have allowed far more detailed simulations (described below) can be undertaken, even for the apparently simple case of uniaxial extensional flow. These have helped to explain the prediction of paradoxically short lengths for the "fully extended" dumbbells in the FENE models.

*Singularities, asymptotics, change of type, instability*

The mathematical richness of solutions to the sets of elliptic/hyperbolic equations describing the slow flow of Maxwell-type fluids formed a notable, even if limited, part of the programme. The re-entrant corner flow problem, linked to stress boundary-layers on the smooth solid surfaces forming the corner, is now basically resolved; the significance of change-of-type within the flow fields is now commonly recognised and its consequences satisfactorily allowed for in simulations

of seemingly "innocuous" flows, e.g. past a sphere or cylinder. Detailed prediction of lip vortices for converging flows is now largely satisfactory.

Equally fascinating have been the recent studies of instability (symmetry breaking, bifurcation, Hadamard instability) in flow and material behaviour, several of which were presented during the programme. For a generation brought up on Newtonian liquids, described by two constitutive parameters (density and viscosity), with inertial non-linearities providing the cause of instability and secondary flow, the effect of visco-elastic non-linearities can be counter-intuitive and more complex. The purely visco-elastic analogue of Taylor-Couette instability, for example, which has been analysed through the first bifurcation into the weakly non-linear regime, was shown to provide a rich range of further instabilities.

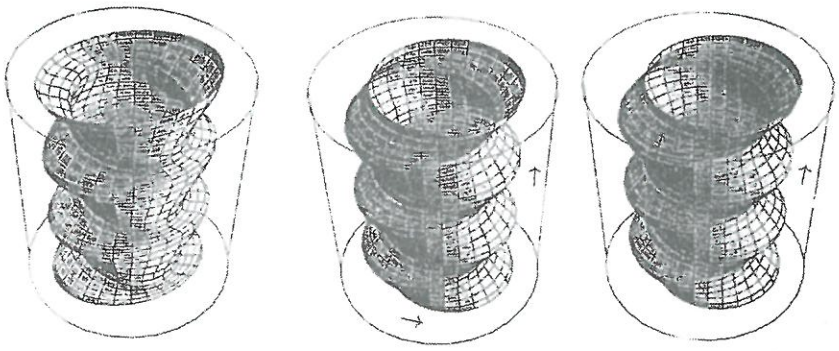


Figure 7: Interface instabilities in core-annular flow.
(a) axisymmetric bamboo waves (b) corkscrew waves (c) snake waves [Y Renardy]

Of particular interest were the many cases of flows involving deformable interfaces, many of which were carefully re-examined. Draw resonance in fibre spinning, drop formation due to Rayleigh instability and the associated persistence of thin filaments formed during drop growth or plate separation, rolling up of interfaces during co-extrusion along tubes or channels (as in lubricated transport along pipes), effects of heat and mass transfer on otherwise static systems, and fingering or 'printer's ink' (flow under rollers) instability were all revisited. The asymptotics of fibre rupture using long-wave approximations, which can be significantly altered by elasticity, proved to be a very topical issue. Apparent slip at solid or deformable boundaries provided another rich topic. Diffusive and other boundary-layer effects on a structural length scale lead to complex constitutive description for the boundary conditions applied at the continuum level, and strike conventional fluid mechanicians, brought up on the no-slip condition and Prandtl boundary-layer theory, as alien and almost indecently empirical. For colloid scientists and biologists, it is almost the reverse: for them the interfaces are the source of material behaviour and organic diversity.

*Granular media*

Here one problem dominated attention during the programme: that of predicting the stress state within a pile of grains resting in limiting equilibrium after being formed by pouring or by collapse of a supported column on release. Are there simple physical guiding principles which remove the need for details elasto-visco-plastic description? Or is conventional application of continuum deformation theory for homogeneous bodies, with full tensor constitutive models, the best way forward? What role can be played by (ensemble averaging of) discrete grain computations? This particular example illustrated just how varied are the ways of seeking scientific insight and

making engineering predictions, at the highest professional level, a lesson not lost on even the most experienced workers.

*The role of computation*

The most important question addressed in this context concerned the need for continuum constitutive relations when undertaking quantitative calculations for stress and velocity fields, assuming that molecular and meso-scale descriptions of material behaviour exist. The answer would seem to be that hugely parallel (or repetitive) simple calculations for individual fluid elements can be undertaken for a statistical ensemble almost as easily as can those for discretised forms of continuum representations; furthermore that there is more flexibility in introducing variations into the elemental constitutive models than in making equivalent changes in the continuum constitutive models. This of course raises the further question of how accurate the elemental models are in the first case, and whether such averaged calculations will provide the sort of generic results on results on material flow behaviour that are the outstanding successes of rational mechanics.

Successful calculations, predicting drag reduction for polymer solutions and providing detailed velocity and stress fields for unidirectional flow in pipes, were reported at the Euroconference. This extension of direct modelling of turbulence near transition was a major achievement. Also remarkable were some of the molecular dynamical and Brownian dynamical calculations reported for non-Newtonian fluids, emulsions and suspensions.

No specific attributions have been given above so as to emphasise the collective nature of the Programme. The interested reader can readily deduce the authors of much of the work described by reference to the titles and abstracts of talks given at the several meetings and seminars organised in connection with the Programme.

# 8 Programme 16: Computer Security, Cryptology and Coding Theory

**January to June 1996**

Report from the Organisers: R Anderson (Cambridge); P Landrock (Aarhus); RM Needham (Cambridge)

## 8.1 Introduction

Over the past fifteen years, the quest for dependable computer systems has fuelled rapid advances in cryptology and coding theory. Previously, these techniques had been principally used to protect military communications; the emphasis has now shifted to designing systems that will perform reliably despite the presence of noise and of attacks by criminals or other opponents.

Cryptology is used increasingly to secure electronic payment networks, distributed operating systems, utility meters, car alarms and mobile phones, while mobile communication is just one of the new applications facilitated by coding theory. There has been significant interaction between these disciplines, with coding techniques being used to attack stream ciphers and explore the limits of authentication systems.

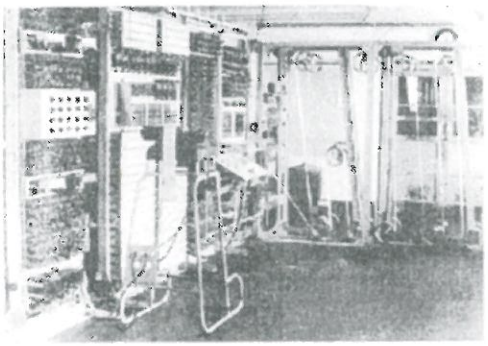


Figure 8: Colossus was the world's first electronic valve programmable logic calculator. Ten of them were built and used for codebreaking at Bletchley Park during World War II

Cryptology also draws on many other mathematical disciplines, especially number theory, combinatorics, finite field theory, algebraic geometry and statistics. Mathematics in turn has benefited greatly from cryptographically motivated research programmes; the best known example of this may be the progress made on factoring algorithms.

The link with engineering is much stronger than with many other mathematical sciences. Incorporating cryptographic and coding techniques into systems turns out to be much more complex than early researchers anticipated, and many subtle errors can occur during protocol design and implementation. This has prompted research on the use of formal methods in system design, and to broader questions of the how the technical and human aspects of system reliability can be integrated.

For these reasons, the programme aimed to promote a cross-fertilisation of ideas between the various mathematical, computer science and engineering aspects of the field. Our goal was twofold: to refine and focus the current mathematical techniques, and to help security engineering mature as a discipline based solidly on the mathematical sciences.

## 8.2 Organisation

There are relatively few people whose research spans the whole of computer security, cryptology and coding theory, but many who work across one of the boundaries. For this reason we structured the programme as a logical progression, starting with coding and moving through

conventional encryption algorithms, computational number theory, public key techniques, formal methods and protocols, computer security and finally security engineering. In this way we aimed to provide continuity for the programme, even if the number of people who attended all of it was relatively small.

A large proportion of the key researchers in all of our target fields visited the Institute during the six month period. The average stay was over a month, and many stayed longer. Most of the participants attended at least one of the four conferences that were held at the Institute, and which will be described in greater detail in the next section; there was also a one-day workshop on formal methods, organised by Ross Anderson and Mike Gordon, and regular Tuesday seminars organised by Peter Landrock. We also had less formal seminars on many Friday mornings at which participants described work in progress, and a dinner once a week (which alternated between colleges and local restaurants). Participants' spouses were taken in hand by Shireen Anderson, Marianne Landrock and Kosa Golić, who organised regular local outings.

However, we deliberately resisted the temptation to overfill the formal part of the programme, and left most of the time free for research.

## 8.3 Conferences

Four international conferences were held during the programme. Two were part of established series, while two were the first of their kind, and were designed to bring together people working in emerging fields. The proceedings of the first conference have already been published; the second and third are at the printers'; while the proceedings of the fourth are awaiting a decision of which of two publishers should be awarded them.

*Fast Software Encryption*: From the 21st to the 23rd February 1996, we hosted the third international conference on fast software encryption. The importance of this topic comes from the fact that cryptology is undergoing a shift not just from military to commercial systems but also from algorithms implemented in custom hardware to software systems that must run on a range of PCs and other platforms. This means using different techniques. In addition, the development of differential and linear cryptanalysis techniques in the early 1990's had broken many of the existing block ciphers, while various correlation attacks had disposed of most of the stream ciphers. So new ideas are needed, and many scientific advances are coming from the design and analysis of the next generation of algorithms.

The conference was ably chaired by one of our participants, Dieter Gollmann, and attracted some 60 participants. Highlights included an attack by Hans Dobbertin on a hash function in wide use; a theoretical framework presented by Mitsuru Matsui for the design of strong block ciphers, that has since led to an encryption chip from Mitsubishi; a new way of combining software encryption with smartcard key management, by Matt Blaze; and several new encryption and hashing algorithms.

The proceedings have been published as Springer Lecture Notes in Computer Science volume 1039.

*Security Protocols*: Cryptographic protocols are used in distributed computer systems to authenticate both subjects and objects, to distribute encryption keys, and to protect transactions for value against fraud. Cambridge has made significant contributions to this field since its inception by Needham and Schroder in 1978; and for the last three years, an annual conference had been held on the subject in Cambridge in the week following Easter.

One of the most powerful tools available to the protocol designer is public key cryptography; this was invented just after Easter 1975, and so the fourth conference on cryptographic protocols, which was held at the Institute from the 10th to the 12th April celebrated its coming of age. The keynote speaker was Whitfield Diffie.

Whereas previous events had tended to focus on the management of keys in distributed computing systems, this event had a strong emphasis on electronic payment mechanisms — there were six papers directly on this topic, ranging from the Cambridge 'Netcard' project to a talk by Adi Shamir on the 'Micromint' system he has developed with Ron Rivest. Other talks reported progress on supporting services such as key certification, digital notarisation and secure timestamping. This change in emphasis not only reflects the recent enormous surge of public and business interest in the commercial prospects of the Internet; it also ensured that this conference made a timely contribution to a growing and important field.

The proceedings should appear in the next few months in Springer's Lecture Notes in Computer Science series.

*Information Hiding*: While preparations for the programme were already underway, we realised that there were at least five different research communities doing work on hiding information, and that they were mostly unaware of each others' existence.

Firstly, recent moves towards the digital distribution of films, music and other intellectual property have raised the question of how the ownership of digital objects can be established. One candidate technology is watermarking — embedding hidden copyright notices in digital objects — but these watermarks must be hard for pirates to find and remove. Secondly, a number of teams have been working on anonymous communications, digital cash, online elections and making mobile communications hard for third parties to trace. Thirdly, computer security researchers and system builders have worried for over twenty years about covert channels — channels which arise when users of a shared resource (such as a computer operating system) can signal to each other by modulating the system's performance.

Fourthly, there is steganography, in which people try to conceal the existence of messages, often in other messages. An example is when a prisoner of war spells out a message in Morse Code in the dots and dashes on the letters $i$, $j$, $t$ and $f$ in a letter home. Finally, a number of essentially physical means of unobtrusive communication have been developed over the past fifty years or so, mainly at the instigation of the military; a typical example is spread-spectrum radio.

It struck us that bringing these research communities together could be both timely and effective, so a workshop was organised for the 30th May to the 1st June as part of the programme.

The response far exceeded our expectations. The workshop was attended by some 70 people; we had eighteen refereed papers and three rump session talks, as well as invited talks from David Kahn on the history of steganography and Gus Simmons on the history of the subliminal channel. We not only managed to get the various research communities talking to each other, we even managed to get them to agree on a common terminology — a harmonisation that would probably have been impossible if the workshop had happened even six months later than it did.

Many of the participants remarked that this event was likely to be remembered as one of the landmark conferences that mark the birth of a new academic discipline. Its proceedings should be published shortly by Springer Verlag.

*Personal Information*: The fourth of our conferences was organised at rather short notice. It was called in response to rapidly growing concern, in both Britain and the USA, about the safety and privacy of electronic medical records. It was held on the last two days of our programme — the

21st and 22nd June — and was sponsored by the British Medical Association, whose President, Sir Terence English, attended on the first day and presided at the conference banquet.

This workshop was truly interdisciplinary. It brought together mathematicians, computer scientists and engineers with doctors, nurses, philosophers and representatives of patients' groups with a view to creating a common understanding of the security problems that will have to be tackled in order to realise the benefits that computer networking can bring to medicine, in a safe and ethical way. This does not just mean affixing digital signatures to medical records, so that subsequent users can be satisfied of their authenticity; it means building systems that enshrine and enforce the principle of patient consent to the disclosure of information — in other words, systems that pass control of the confidentiality function from the centre (where it resides in a conventional organisation) to the end users.

In addition to posing new policy problems, this raises many interesting technical issues concerning the tradeoffs between privacy and safety, which must be much better understood than at present before the role of clinical discretion (and thus the administrative burden on clinical staff) can prudently be cut.

This conference was a great inspiration to those who attended, and unlike many has had tangible political effects. In the UK, there is now a growing consensus between the BMA and the Department of Health on how to proceed with the introduction of information technology into clinical care. This is a welcome advance from the status quo ante, which had been marked with public rows over confidentiality. The conference also gave strong support to US medical privacy lobbyists, which contributed to recent legislation forbidding insurance companies from discriminating on the basis of genetic tests.

It has also enabled the UK medical privacy community to forge strong links with counterparts in Europe, and this will no doubt lead to collaborative projects in the future. As with the information hiding conference, there is a feeling that the Newton Institute meeting may come in time to be seen as the birthplace of a new discipline — medical informatics security.

We are about to decide whether the proceeding should be published by IOS Press (who publish a series of books on medical informatics) or Springer (who publish most cryptologic and related proceedings). The decision should be made by the end of October, and the book published early in the new year.

## 8.4 Conclusion

In addition to the programme's highly visible contributions made through these conferences, it gave participants an opportunity to catch up with new work in related fields. For example, during January we hosted over a dozen researchers in coding theory, and our initial view had been that we should explore whether recent work in algebraic geometry codes would be relevant to cryptology. Indeed it is — recent German work in function fields enables apparently secure public key cryptosystems to be constructed using single-precision arithmetic; however, the main contribution of this session was to communicate recent research in turbo codes that has still not appeared in the literature in an accessible form. Turbo codes provide much better practical performance than other error correction systems, although we do not yet possess a complete theory of why this should be so. Exploring this, and possible applications to cryptanalysis and elsewhere, is an exciting opportunity for researchers.

A number of research collaborations have started between people who previously considered their areas of interest to be disjoint, and we have no doubt that these collaborations will continue.

One of our long-stay participants, Tom Berson, summed up this contribution of the programme in 'Cryptobytes' as follows:

> I do expect that we will see published over the next two years perhaps two hundred papers which give credit to time spent at the Isaac Newton Institute ... I am certain that the professional collaborations furthered at the Institute during the first six months of 1996 will constructively enhance the nature of cryptologic research for many years to come.

Tom's prediction is already coming true. In our capacity as conference and journal referees, we are beginning to see a healthy flow of papers which acknowledge work done at the Isaac Newton Institute, or cite discussions held with colleagues there. This confirms to us that the programme in Computer Security, Cryptology and Coding Theory was indeed worthwhile, and we are very grateful to the Institute for giving us the opportunity to arrange it.

# 9 Hewlett-Packard's Basic Research Institute in the Mathematical Sciences (BRIMS)

## 9.1 Senior Research Fellow

Hewlett-Packard continues to fund a Senior Research Fellowship at the Institute. The holder during the period 1 January 1995–30 June 1996 was Dr Colin Sparrow. From 1 October 1996 the position will be held by Dr Sandu Popescu. The Senior Research Fellow spends 8 weeks per annum at BRIMS (near Bristol), and the rest of the time is based at the Institute.

## 9.2 Interaction with BRIMS

The Institute's association with BRIMS continued to develop during the year. In November 1995 Dr Jeremy Gunawardena (Scientific Director of BRIMS) organised a very successful workshop *New Connections between Mathematics and Computer Science* at the Institute, in conjunction with the two programmes (*From Finite to Infinite Dimensional Dynamical Systems* and *Semantics of Computation*) running at the time. In the same month, the Institute hosted a one–day meeting organised by BRIMS on *Stochastic Networks*. Throughout the year a number of programme participants visited BRIMS to give seminars or for discussions, and BRIMS staff members and post–docs participated in Institute programmes and workshops.

## 9.3 Fellowship Report

Dr Sparrow writes: 'My Research Fellowship was enjoyable and rewarding. There is now considerable mathematical acitivity in BRIMS, and it is an exciting place to visit on a regular basis. As well as continuing with my own research in Dynamical Systems, I began a fruitful collaboration (which continues) with Jeremy Gunawardena on the dynamics of non-expanding maps, which has applications to discrete event systems, and therefore to network and hardware design.'

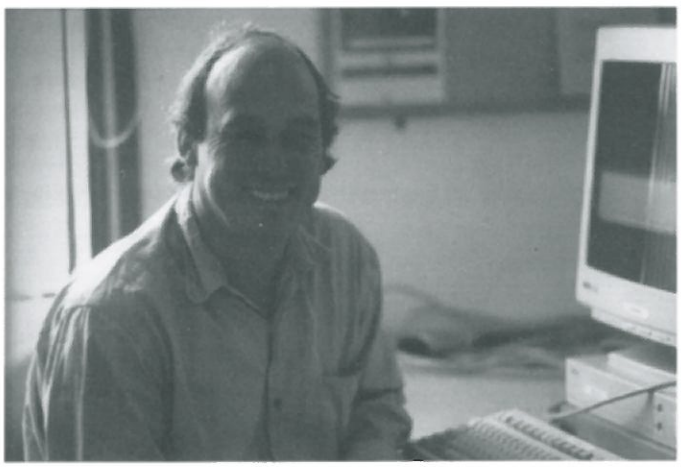


Figure 9: Colin Sparrow, Hewlett-Packard Senior Research Fellow from January 1995 to June 1996

# 10 Scientific Planning and Future Programmes

## 10.1 Programme structure and organisation

The scientific planning for each programme is the responsibility of a team of three or four organisers appointed by the Management Committee following input from the programme proposers and the Scientific Steering Committee.

Programmes are selected about two years before they are scheduled to begin. The first task of the organisers is to identify leading workers who are willing to commit themselves to participating in the programme for an appreciable period. A wider group can then be approached in successive tranches. In the period between eighteen and six months before a programme starts the budgets for travel and subsistence are committed in this way. Six months before the programme starts budgets are usually over-committed by between 5% and 10%. Naturally there will then be subsequent changes and withdrawals due to unforeseen circumstances, leaving flexibility in the budget to enable some invitations to be issued just before and during the programme.

A typical structure for a programme is to begin with a conference having some instructional content, to have two or three more specialised workshops towards the middle of the programme, focusing on particular aspects of the programme or closely related areas, and perhaps to end with some more general meeting summarising the state of the art. Such a model is not rigidly imposed and programmes vary quite considerably in their actual structure. Of those which took place in 1995/96, *Dynamics of Complex Fluids* followed closely the pattern outlined above whilst *Semantics of Computation* and *From Finite to Infinite Dimensional Dynamical Systems* deviated from it (particularly in the case of the latter programme) in that they contained a much larger number of workshops.

In addition to the workshops which serve to widen UK participation in the programmes, the organisers are strongly encouraged to organise less formal special days, short meetings or intensive lecture series which can attract daily or short-term visitors, so further increasing the impact of the Institute on the UK mathematical community.

All of this is against the background of regular series of seminars in each programme. During the year 1995/96 there were over 800 lectures and seminars given in the Institute. A list of these seminars, which perhaps more than anything else illustrates the scope of the Institute and the intensity of its activities, is given in Appendix G.

A list of publications produced, or in production, by participants is included in Appendix F. This shows that the number of publications notified to the Institute in 1995/96 was over 250.

Partcipants at the Institute have given over 160 seminars in departments outside Cambridge (an increase of at least 20 on the previous year). These are listed in Appendix G. UK universities and other institutions at which visiting members have talked during 1995/96 include: Bath; Birmingham; Bristol; British Meteorological Office; Cambridge; Edinburgh; Exeter; Glasgow; Hatfield; Hertfordshire; Heriot-Watt; Hewlett-Packard Basic Research Institute in Mathematical Sciences, Bristol; Imperial College, London; Kent; Lancaster; Leeds; Leicester; Manchester; Newcastle; Nottingham; Oxford; Queen Mary and Westfield, London; Royal Holloway and Bedford New College, London; St Andrew's; Strathclyde; Southampton; Sussex; University College, London; Warwick; West of England.

After discussion in both Scientific Steering and Management Committee meetings concerning programme structure and duration it was decided to conduct an experiment during the second

half of 1996 when there will be one substantial six-month programme *Mathematics of Atmosphere and Ocean Dynamics* together with two six-week programmes *Mathematics of Plankton Population Dynamics* a(in July/August) nd *Four-Dimensional Geometry and Quantum Field Theory* (in November/December) running alongside it. It has also been agreed that, with effect from 1999 two six-month programmes and three four-month programmes will run in parallel each year.

## 10.2 Scientific Policy

The Director is advised on the scientific work of the Institute and, in particular, on the selection of programmes by the Institute's Scientific Steering Committee. The scientists on this committee, with the exception of the Director, come from outside Cambridge. The Committee consists of the Director; three persons appointed by the General Board on the recommendation of the EPSRC; one person recommended by the General Board on the recommendation of the Particle Physics and Astronomy Research Council (PPARC); two persons appointed by the General Board on the recommendation of the LMS, six persons appointed by the General Board after consultation with the Councils of the Schools of the University and national scientific bodies (the Royal Society; the Royal Society of Edinburgh; the Royal Statistical Society; the Institute of Physics; the Royal Academy of Engineering; the Institute of Mathematics and its Applications and the Edinburgh Mathematical Society) and one additional person co-opted at the discretion of the Committee.

The membership of the Scientific Steering Committee on 30 June 1996 was:

| | | |
|---|---|---|
| Professor Sir Christopher Zeeman, FRS | Oxford University | GB *Chairman* |
| Sir Michael Atiyah, OM, FRS | Newton Institute | Director |
| Professor Sir Michael Berry, FRS | Bristol | GB |
| Professor J-M Bismut | Orsay | GB |
| Professor M Cates | Edinburgh | GB |
| Professor S Donaldson, FRS | Oxford | GB |
| Professor TWB Kibble, FRS | Imperial | PPARC |
| Professor J Moser | ETH Zürich | GB |
| Professor TJ Pedley, FRS | Leeds | GB |
| Professor BD Ripley | Oxford | EPSRC |
| Professor AFM Smith | Imperial College | EPSRC |
| Professor JF Toland | Bath | LMS |
| Professor CTC Wall, FRS | Liverpool | LMS |

Professor J Ball was also a member of the Committee during 1995/96. Professor Sir Michael Berry and Professor BD Ripley reached the end of their terms of service on 31 December 1995 but were both re-appointed for a further four years.

The Committee is required to meet once per year but in practice meets twice per year, usually in October and May.

The Scientific Steering Committee perceives its role as involving both the consideration of proposals received and the stimulation of proposals in the areas of mathematical sciences which it considers to be potentially particularly suitable for the Institute. The Institute advertises its willingness to receive proposals in a variety of ways which have included the annual distribution of a poster containing a "Call for Proposals" (the current version of which is included in Appendix I) to over 500 departments and institutions concerned with mathematical sciences in the UK and abroad, and publicity by email and World Wide Web. At meetings the Committee

regularly considers in which areas it should stimulate proposals and the Director, Director or individual Committee members then assume responsibility for taking action in particular areas.

It is the intention of the Scientific Steering Committee that the Newton Institute should be devoted to the Mathematical Sciences in the broad sense. The range of sciences in which mathematics plays a significant part is, of course, too large for an Institute of modest size to cover adequately. In making the necessary choices important principles are that no topic is excluded a priori and that scientific merit is to be the deciding factor. One of the main purposes of the Newton Institute is to overcome the barriers presented by normal departmental structures in Universities. In consequence, a relevant criterion in judging the "scientific merit" of a proposed research programme is the extent to which it is "interdisciplinary" (although it is not the intention to exclude strongly focused proposals). Usually this will involve bringing together research workers with very different backgrounds and expertise. There must, however, be a clear common ground on which all can focus and each programme has to have a substantial and significant mathematical content and a broad mathematical/scientific base. A further main criterion should be that the subject area is in the forefront of current development.

Because of the wide base of support for the Newton Institute in the research councils and elsewhere, the Institute's programmes should as far as possible represent an appropriate balance between the various mathematical fields. Such considerations, however, are secondary to the prime objective of having high quality programmes. If there are no exciting developments, actual or potential, in a particular field, it would be inappropriate to run a programme simply to maintain a balance.

## 10.3 Future programmes

The Institute began its scientific work in July 1992 with its first two programmes on *Low-dimensional Topology and Quantum Field Theory* and *Dynamo Theory*; since then fourteen further programmes on *L-functions and Arithmetic*; *Epidemic Models*; *Computer Vision*; *Random Spatial Processes*; *Geometry and Gravity*; *Cellular Automata, Aggregation and Growth*; *Topological Defects*; *Symplectic Geometry*; *Exponential Asymptotics*; *Financial Mathematics*; *Semantics of Computation*; *From Finite to Infinite Dimensional Dynamical Systems*; *Dynamics of Complex Fluids* and *Computer Security, Cryptology and Coding Theory* have been completed. On the advice of the Scientific Steering Committee, the following programmes have now been selected for 1996-1998:

**Mathematics of Atmosphere and Ocean Dynamics**
July to December 1996
*Organisers: JCR Hunt (UK Met Office), ME McIntyre (Cambridge), J Norbury (Oxford), I Roulstone (UK Met Office)*

Weather forecasts are routinely computed for up to 10 days ahead, based on large quantities of wind, temperature and humidity data that are collected continuously and used to modify the computations. The data are of course insufficient to determine the exact state of the atmosphere. Since they are very expensive to obtain there is a premium on their optimal exploitation. Therefore it is of the highest importance for numerical weather prediction to identify the dominant processes and flow features that determine how the large scale weather patterns develop. By then ensuring that the continuous assimilation of data is consistent with these features the accuracy of the forecasts is greatly increased. Ocean modelling is beginning to develop similar data assimilation techniques. Recent exchanges of ideas between mathematicians and atmosphere-ocean dynamicists has brought a new geometric global viewpoint to these problems, in particular a

new appreciation of how fluid-dynamical conservation laws, for example potential vorticity, connect with the symplectic geometric structure of the underlying equations of motion. A major challenge for the programme will be to bring ideas from geometry, analysis and the theory of dynamical systems to bear on the practical and urgent problems of weather forecasting, ocean and climate modelling.

**Mathematical Modelling of Plankton Population Dynamics**
29 July to 6 September 1996
*Organisers: J Brindley (Leeds), M Fasham (Southampton), J McGlade (Warwick)*

Plankton play a key role in ocean-atmosphere dynamics. Their effects range from alterations on a local scale of the structure of the sea-surface temperature and mixed layer depth, to ocean basin-wide emissions of potentially important climatological gases such as dimethyl sulphate, up to global fluxes of atmospheric carbon. These effects occur over a wide range of spatio-temporal scales and via a number of different biophysical processes. The programme will bring together mathematical and numerical modellers with biological oceanographers to review, improve and develop models, addressing particularly the needs to understand the spatio-temporal scale distribution of plankton behaviour and its relationship with the physical dynamics of the ocean-atmosphere system. Within the six-week programme will be embedded a specialist meeting attended by much larger number than the core participants, focussing on the effects of physical forcing on plankton populations and the consequences for fisheries.

**Four-dimensional Geometry and Quantum Field Theory**
4 November to 13 December 1996
*Organisers: Sir Michael Atiyah (Cambridge), IM Singer (MIT)*

This six-week programme will focus on the exciting recent developments centering around a remarkable duality in four-dimensional space-time. This formally interchanges Electricity and Magnetism and works in certain non-abelian gauge theories. It has major implications for the understanding of strong interactions in physics and in four-dimensional geometry.

**Representation Theory of Algebraic Groups and Related Finite Groups**
January to June 1997
*Organisers: M Broué (Paris), RW Carter (Warwick), J Saxl (Cambridge)*

There is a famous theory due to Hermann Weyl for the characters of the finite dimensional irreducible representations of simple algebraic groups over the complex numbers. In finite characteristic no analogous formula has been proved, but there is a conjecture due to Lusztig which expresses the irreducible characters as linear combinations of the Weyl characters. This is related to certain characters of affine Kac-Moody algebras, and also to the representations of certain quantum groups - the latter being at the moment a rapidly developing branch of mathematics. Other related themes include subgroup structures of the corresponding groups of Lie type.

**Non-Perturbative Aspects of Quantum Field Theory**
January to June 1997
*Organisers: DI Olive (Swansea), P Van Baal (Leiden), P West (King's College, London)*

Recent results of Sen, Seiberg and Witten have made increasingly plausible the idea of a quantum transformation between the weak and strong coupling regimes of certain spontaneously broken supersymmetric gauge theories in space-time of four dimensions. The relevant ideas encompass and unify many topics studied intensively over recent years by particle physicists including QCD and the theory of instantons, solitons and their quantisation, conformal field theory, Yang-Baxter equations, the s and t duality of string theory and the mirror symmetry of Calabi-Yau manifolds. The new results have also already had an impact on pure mathematics, for example in

the understanding of the Donaldson classification of four manifolds. The aim of the programme is to explore the idea of electromagnetic duality, to gain new insights into fundamental physics (for example, the issue of confinement in QCD, and the improved formulation of unified string theories), and into pure mathematics.

**Disordered Systems and Quantum Chaos**
July to December 1997
*Organisers: J Keating (Bristol), DE Khmelnitskii (Cambridge), IV Lerner (Birmingham), P Sarnak (Princeton)*

The quantum properties of disordered systems have been the focus of considerable attention in many branches of physics, principally nuclear physics and condensed matter physics. Recently it has been recognised that many of the same phenomena also occur in deterministic systems which possess only a few degrees of freedom, but which are chaotic in the classical limit. Even more surprisingly, the theories developed in these areas also have natural counterparts in a number of topics in mathematics; for example, in the study of spectral properties of random operators and random matrices, in the theory of Fourier integral operators, in harmonic analysis (specifically in the theory of the Riemann zeta-function and related L-functions). In the past few years an extremely stimulating and productive cross-fertilisation between the above fields has slowly been developing. The aim of the programme is to accelerate the already significant rate of progress on some of the important common problems which occur, in different guises, in each area. The main topics upon which the programme will focus are localisation, fluctuation statistics, and trace formulae; with a particular emphasis on their role in the theory of mesoscopic systems.

**Neural Networks and Machine Learning**
July to December 1997
*Organisers: CM Bishop (Aston), D Haussler (UCSC), GE Hinton (Toronto), M Niranjan (Cambridge), LG Valiant (Harvard)*

Research in machine learning has advanced significantly in recent years, stimulated in part by the emergence of a range of successful, large-scale applications. Examples include optical character recognition, classification of sleep stages from EEG signals, cervical smear screening, and real-time tokamak plasma control. At the same time there have been many impressive developments in the theoretical foundations of this field, arising from several complementary approaches. Concepts from statistical pattern recognition have been used to formulate a general framework for machine learning based on statistical inference. Parallel developments in computational learning theory have led to a characterisation of computational and sample-size requirements for learning problems, while also resulting in powerful new algorithms. In addition, concepts from information theory, differential geometry and statistical mechanics have been exploited to give alternative insights into neural networks. The principal aims of this programme are to promote greater inter-disciplinary collaboration between researchers with different theoretical perspectives, to strive for a more unified mathematical framework for neural networks and machine learning, and to stimulate the development of new algorithms for practical applications.

**Dynamics of Astrophysical Discs**
January to June 1998
*Organisers: JCB Papaloizou (QMW); JE Pringle (Cambridge); JA Sellwood (Rutgers)*

Many astrophysical systems, over a vast range of length scales, consist of matter organised in differentially rotating, centrifugally supported discs. Such systems include planetary rings, protostellar discs (which provide the environment from which planets may form), close binary star systems, and normal and active galaxies. Understanding the structure and evolution of astrophysical discs is therefore of central importance in astronomy. Discs may sometimes be

modelled as collections of discrete particles, and this leads to the study of collisionless many body problems. Other studies require that the disc be treated as a differentially rotating turbulent fluid possibly containing a magnetic field. The effects of self-gravitation may also need to be taken into account. The mathematical problems that arise usually involve the solution of differential or integro-differential equations. The programme will bring together experts from relevant areas in astrophysics and mathematicians and scientists familiar with appropriate analytic methods and numerical simulation techniques.

**Arithmetic Geometry**
January to June 1998
*Organisers: J-L Colliott-Thélène (Orsay); J Nekovář (Cambridge); C Soulé (IHES)*

The origin of this subject was the study of solutions of Diophantine Equations - that is the solutions in integers or rationals of systems of algebraic equations. In recent years it has become clear that many important problems in apparently diverse branches of pure mathematics cannot be fully understood except in terms of number-theoretic ideas. Such branches range from algebraic geometry through automorphic functions to representation theory. One aspect of these connections is the so-called Langlands Programme; another is Wiles' recent proof of Fermat's Last Theorem which was first announced during a previous Newton Institute programme. Arithmetic Geometry is at the moment one of the most central areas of Pure Mathematics and perhaps the most active area of all.

**Biomolecular Function and Evolution in the Context of the Genome Project**
July to December 1998
*Organisers: P Donnelly (Cambridge), W Fitch (Irvine), N Goldman (Cambridge)*

There is a long and productive history of interplay between genetics on the one hand and mathematics and statistics on the other. The "molecular revolution" over the last 15 years, and in particular the impetus of genome projects, has transformed the field to one with an abundance of data and a paucity of relevant mathematical models and techniques. By 1998, the maturation of genome projects will make data on DNA, proteins, gene duplications and gene arrangements on the chromosomes widely available. As a consequence of recent advances in computational statistics, vast improvements in the quality of statistical analyses of these data are possible. They will have a profound impact on the practice of biological research, and, ultimately, medical diagnostics and preventive medicine. The driving force of the present programme is the opportunity offered by genome sequence research to understand biomolecular function and evolution at a much more complete level than hitherto possible and to sustain recent progress in a number of relevant mathematical areas. Problems in analysing the flood of molecular genetic sequences and structures raise a range of challenging biomathematical research topics. This inter-disciplinary programme will bring together mathematicians and computer scientists working on subjects such as probabilistic modelling, stochastic processes, geometry, statistical data analysis, computational complexity, neural networks, genetic algorithms and expert systems; and molecular biologists working in medical and biological fields.

Further programmes, listed below, have been agreed. More details will be available in the near future.

**Nonlinear and Nonstationary Signal Processing**
July to December 1998
*Organisers: WJ Fitzgerald (Cambridge), RL Smith (North Carolina), PC Young (Lancaster)*

**Turbulence**
January to July 1999
*Organisers: GF Hewitt (Imperial College), N Sandham (QMW), PA Monkewitz (Lausanne), JC Vassilicos (Cambridge)*

**Mathematics and Applications of Fractals**
January to April 1999
*Organisers: RC Ball (Cambridge), KJ Falconer (St Andrews)*

**Complexity, Entropy and the Physics of Information**
May to August 1999
*Organisers: A Albrecht (Imperial), RM Salovay (Berkeley), W Zurek (LANL)*

**Singularity Theory**
July to December 2000
*Organisers: VI Arnold (Moscow and Paris IX), JW Bruce (Liverpool), D Siersma (Utrecht)*

# 11 Fund-Raising and Grant Aid

## 11.1 EPSRC

The Institute's rolling grants from the EPSRC for both scientific and administrative salaries and associated overheads, and for travel and subsistence for participants were reviewed in the autumn of 1995 and spring of 1996. New levels of funding (totalling £2.28 million over 4 years have been agreed and the grants have been extended until March 2000.)

## 11.2 Hewlett-Packard

Hewlett-Packard continue to fund a Hewlett-Packard Senior Research Fellow with full 100% overheads. The first Hewlett-Packard Senior Research Fellow is Dr Colin Sparrow. He was appointed from 1st January 1995 until 30th June 1996. His successor will be Dr Sandu Popescu who will take up his appointment on 1st October 1996.

## 11.3 Isaac Newton Trust

The Isaac Newton Trust continued to provide the Institute with £200,000*pa* as a contribution to overheads for 1994/95. In addition, it made a contribution of £10,000 towards the salary of the Librarian and Information Officer. The Trust has announced that it will continue to support the Newton Institute beyond the period of its present grant, which ends in June 1997, and will do this by means of a loan or endowment.

## 11.4 St John's College

St John's College donated the sum of £150,000 to the Institute in 1995/96 being the fourth instalment (of five) of its funding to offset the rent of the Newton Institute building.

## 11.5 NM Rothschild and Sons

The donation by NM Rothschild and Sons enabled the appointment of four Rothschild Distinguished Visiting Professors was in 1995/96: Professor Dana Scott (*Semantics of Computation*); Professor Jack Hale (*From Finite to Infinite Dimensional Dynamical Systems*); Professor Gary Leal (*Dynamics of Complex Fluids*) and Dr Gus Simmons (*Computer Security, Cryptology and Coding Theory*).

## 11.6 Leverhulme Trust

The second instalment (of three) of £55,000 was paid by the Leverhulme Trust to the Institute to provide travel and subsistence for scientists from Eastern Europe and the former Soviet Union with associated costs.

## 11.7 Centre Nationale de Recherches Scientifiques (CNRS)

CNRS donated its fourth contribution of 400,000FF to the Institute towards subsistence and travel costs for French participants (in particular those from CNRS laboratories) and related costs.

## 11.8 Gabriella and Paul Rosenbaum Foundation

The Institute received the fourth instalment of a grant which was extended from three years to five years from the Gabriella and Paul Rosenbaum Foundation. The $70,000*pa* donation funds the salary of four young American scientists attending the Institute's programmes. The recipients in 1995/96 were Dr Ramesh Viswanathan (*Semantics of Computation*); Dr Yingfei Yi (*From Finite to Infinite Dimensional Dynamical Systems*); Dr Gareth McKinley and Dr Francisco Solis (*Dynamics of Complex Fluids*). The grant has now been extended again for a further two years (ie July 1997 to June 1999) at the increased rate of $80,000*pa*.

## 11.9 NATO Advanced Study Institutes (ASIs)

Successful applications were made to NATO by the organisers of the programmes on *From Finite to Infinite Dimensional Dynamical Systems* and *Dynamics of Complex Fluids* for support to fund conferences, aimed at young scientists, under the NATO ASI programme. These conferences were awarded £45,610 and £48,078 respectively.

## 11.10 European Union

The Institute continued to use its funding from the European Union's Human Capital and Mobility Fund to fund Euroconferences on its programmes. Thus conferences within the programmes *Semantics of Computation*; *From Finite to Infinite Dimensional Dynamical Systems* and *Dynamics of Complex Fluids* were each funded from the 90,000 ecu awarded for the Newton Institute Euroconferences Series Two.

## 11.11 Prudential Distinguished Fellowship

The year's instalment of £25,000 from the Prudential Corporation was the final one of four, given to be spent on distinguished visiting fellows and associated costs. In 1995/96 the fellows appointed were Professor E Spiegel (*From Finite to Infinite Dimensional Dynamical Systems*) and Dr R Larson (*Dynamics of Complex Fluids*).

## 11.12 London Mathematical Society (LMS)

LMS awarded the sum of £10,000 to the Institute in 1995/96. This was the fourth instalment (of five) given to fund short-term participation of UK mathematicians. The Institute was also granted additional support for a workshop on the *From Finite to Infinite Dimensional Dynamical Systems* programme and support for Spitalfields Days.

## 12.3 Summary Accounts for 1994/95 and 1995/96

| Category | 94/95 | 95/96 |
|---|---|---|
| **Expenditure** | | |
| Consumables | 101,831 | 98,439 |
| Computing | 41,839 | 37,326 |
| Library | 23,538 | 15,754 |
| Institute Rent | 184,000 | 184,000 |
| Scientific Costs | 543,217 | 558,771 |
| University Overheads | 34,838 | 34,335 |
| Staff Costs | 296,834 | 291,437 |
| Depreciation/Reprovision of Equipment | 140,000 | 90,000 |
| Miscellaneous | | 42,815 |
| **Total** | 1,366,097 | 1,352,877 |
| **Income** | | |
| Grant Income | 1,303,151 | 1,248,070 |
| Workshops | 38,874 | 49,269 |
| General Income | 32,982 | 44,210 |
| Housing | 2,833 | 7,714 |
| **Total** | 1,377,840 | 1,349,263 |
| **Income less Expenditure** | 11,743 | (3,614) |

**Notes**

*[i]* Grant income for 1995/96 breaks down as follows:

| | |
|---|---|
| EPSRC Salaries | 259,604 |
| EPSRC Travel and Subsistence | 225,988 |
| Newton Trust | 210,000 |
| St Johns College | 150,000 |
| Hewlett-Packard | 98,000 |
| Rothschild | 55,383 |
| CNRS | 50,655 |
| Rosenbaum | 45,155 |
| Prudential | 25,000 |
| Leverhulme | 43,093 |
| Leibniz | 28,573 |
| Information Systems Committee | 16,119 |
| Royal Society | 12,299 |
| LMS | 10,000 |
| Institute of Physics | 10,000 |
| Jesus College | 5,000 |
| Thriplow Trust | 2,200 |
| Cambridge Philosophical Society | 1,000 |
| TOTAL | 1,248,070 |

full-time. Professor Moffatt will be supported by a part-time Deputy Director, Dr Noah Linden, who was previously Assistant Director.

Figure 10: Lynne Stuart, Administrative Assistant from 1992 to 1996

Lynne Stuart, who was an early employee of the Institute when she joined as Principal Secretary in 1992, left in April 1996 to marry and join her new husband in the United States. Lynne was upgraded to Administrative Assistant in the Director's Office in July 1993 and was replaced in that position (now known as Administrative Officer in the Director's Office) by Wendy Abbott, former Housing Officer in May 1996. Wendy was succeeded as Housing Officer in June 1996 by Sharon Allen.

Andrea Le Core took up the post of Librarian and Information Officer in September 1995.

Michael Sekulla succeeded Florence Leroy as Conference and Programme Secretary in July 1995. Mike had previously worked for the Institute in a temporary capacity.

As usual the Institute could not have run without the assistance of many other staff working as temporary or casual employees. In the year 1995/96 these have included: Elsie Batchelor; Heather Dawson; Michael Goddard; Jane Hartwell; Penny Hunter; Simone Marshall; Siobhan Miller and Peter Wren.

The staff of the Institute on 30 June 1996 was:

| | |
|---|---|
| Director | Sir Michael Atiyah OM, FRS |
| Executive Director | Professor Sir Peter Swinnerton-Dyer FRS |
| Assistant Director | Dr Noah Linden |
| Institute Administrator | Ann Cartwright |
| Administrative Officer | Wendy Abbott |
| Computer Systems Manager | Mustapha Amrani |
| Deputy Computer Systems Manager | Neil Dunbar |
| Librarian & Information Officer | Andrea Le Core |
| Housing Officer | Sharon Allen |
| Accounts Clerk | Sarita Haggart |
| Conference & Programme Secretary | Michael Sekulla |
| Secretary | Tracey Hibbitt |
| Receptionist & Catering | Teresa Secker |
| Cleaner | Clive Dean |

## 13.3 Building

The Institute's building contains two seminar rooms with flexible seating (the larger, Seminar Room 1, holding between ninety-six and one hundred and fifty people and the smaller, Seminar Room 2, between thirty-six and fifty), a library, thirty offices (eighteen double and twelve single), General Offices (for administration), an office for the Director and common areas.

For use in the seminar rooms, the Institute possesses four GBI 5000 overhead projectors, three Kodak Carousel 35mm slide projectors and a GEC CRT projector (mounted onto the ceiling in Seminar Room 1) which can project European and USA videos (in PAL, SECAM and NTSC formats) and the output, in monochrome or colour, from a SunSPARC station, an HP, a Macintosh

Quadra or a PC. In each seminar room there are six chalkboards and two overhead projector screens. In Seminar Room 1 there is also a central screen which can be raised and lowered automatically from the lectern. It can be used for the CRT projector, one or two slide projectors (which can be controlled from the lectern) or an overhead projector.

The library, seminar rooms and administrative offices are grouped around a ground-floor common area and the scientists' offices which are on the mezzanine and galleried first and second floors, surround the mezzanine common area. Throughout the building there are places for discussion grouped around chalkboards. As with the rest of the Institute's facilities, the building has been designed with a view to quickness of assimilation, which is of prime importance given the relatively short average stay of participants compared with that in a normal university department.

Figure 11: The Institute's ground floor common area

Improvements have been made to various aspects of the building in 1995/96. Windows at the top of the building have been modified so that they can be opened by a remote control mechanism. This significantly improves the ventilation of the common areas.

The control system for the audio-visual facilities in Seminar Room 1 has been upgraded.

Further measures have also been taken to improve the security of the building, including additional security cameras.

Three new sculptures by John Robinson, generously donated by Damon De Laszlo and Robert A Hefner III, have been installed at the front of the building. They are entitled *Genesis*, *Creation* and *Intuition*. The first to be installed was *Intuition* and this was unveiled by Sir Michael Atiyah on 14th February 1996. *Creation* and *Genesis* will be unveiled on 4th October 1996.

## 13.4 Computing

A number of meetings took place between the Institute and SUN Microsystems UK with regard to a heavily discounted upgrade of the existing SUN computing resources. These negotiations were completed at the beginning of the Institute year 1996/97, and the new computers were installed during September/October 1996. This upgrade has radically improved the existing computer facilities at the Institute, bringing them up to an appropriate level.

The Institute's scientific computer network (as at December 1996) consists of 10 Hewlett-Packard 700 series workstations, 26 Sun workstations and 15 Apple Macintosh Quadra 700s with the recent addition of 1 Ultra Sparc 1 workstation, 14 Sparc 5 workstations, 1 SUN Enterprise 150 NFS server and 1 SUN Enterprise 4000 computer server.

This provision allows each participant who has been allocated designated office space to be provided with a computer for use during his or her visit. Participants who do not fall into this category may use the 24-hour computer facilities in the terminal room, subject to demand.

The most common use of the facilities are electronic mail, accessing remote machines, word-processing (using TEX) and symbolic manipulation. The following software is available on all SUN workstations: Mathematica, Matlab, Maple, TEX, LATEX, Rerduce, S-Plus, Emacs, elm, pine, MH, netscape, Perl, C, C++, FORTRAN, Tcl/Tk... A complete list of software can be found on WWW page, URL

**http://www.newton.cam.ac.uk/computing/software.html**

All Mac Quasars 700 are installed with the following software: Mathematica, Eudora, NCSA Telnet, Fetch, Textures, Microsoft Word 6.01, Claris Works, Mac Write, Mac Draw, Netscape and 3 licences for Matlab.

AU/X has been phased out on all the Mac Quadras. All Quadras 700 have been upgraded to Mac OS 7.5.1. Xinet K-Ashare (Installed on Turing) and CAP (Installed on Newton) will allow Mac users to access their home directories on the UNIX system. All files saved in the home directories will benefit from daily backup. Eudora has been installed as the main mailing agent. 15 licences of Textures version 1.7.6 have been purchased and installed on all the Macs. This will provide TEXand LATEXfor Mac users. In addition to these programs, all Macs are now installed with Mathematica, Claris Works, Microsoft Word, NCSA telnet, fetch and Netscape.

A new heavy-duty HP 5SI/MX printer was purchased and installed. This printer now offers high speed (24 pages per minute) and high quality (600 DPI). It will be the main printer for the participants. The printer is fitted with a duplex unit which allows printing on both sides of the paper. The Laserwriter II has now been installed in room M2 for the Institute Accounts Clerk to print confidential documents; pay slips etc.

Due to the popularity of Matlab with DCF participants, two extra licences have been purchased. This means that we now have 4 concurrent licences for combined use on the SUNs and HPs.

Several software packages were upgraded or added to UNIX in order to improve the existing provision. These include: LATEX2e, Sendmail 8.6.12 and MH (email agent) on both Suns and HPs. All SUN Sparc workstations (except Bohr) were upgraded to the latest version of SunOS (version 4.1.4).

Majordomo, a software package that automates the maintenance of mailing lists, was also added to the system. This allows users to add and to remove themselves from lists, obtain information about lists, obtain files through email, etc. The weekly seminar list is distributed via an email list, and there is also a list for each programme. This is proving to be an effective way to

communicate news and views between participants on the same programme.

## 13.5 Library

In September 1995 Andrea Le Core took up the post of Librarian and Information Officer, which now includes additional responsibility for maintaining and disseminating information about the Institute via conventional and electronic means.

The bookstock in the library is increasing steadily and is now approaching 4000. In addition there are 76 periodical titles, many with quite extensive backruns. Plans have therefore been approved to install a mezzanine gallery in one section of the library, substantially increasing the amount of shelving to meet the increasing demands of an expanding collection. It is hoped that building work will start towards the end of 1996.

Over the period 1995/96 250 loans were recorded. This decrease from the previous year may be partly due to the fact that for a short period between librarians the library was staffed part-time, making it more difficult to keep track of self-service loans. This is borne out by the fact that the lowest number of loans was recorded during this period. In addition, the needs of participants do vary between programmes, and it was observed those taking part in the four programmes during 1995/96 tended to make greater use of the library for reference to journals and as a place to study than for borrowing books.

The archive of papers and preprints produced by participants continues to grow steadily, and of the 264 papers notified to the Institute this year (listed in Appendix F), 75 have so far been deposited in the library. This number is expected to increase during the year, as participants complete work on papers begun at the Institute.

## 13.6 Housing

The Institute provides housing for its participants in eleven flats (Mordell Court, Chesterton) and a listed building containing six study bedrooms (1 Chapel Street, Chesterton), both of which are rented from St John's College, and an average of twelve privately-owned houses and flats.

For a single person, prices vary from £15 to £18 per night, with accommodation ranging from single study bedrooms to self-contained one-bedroom flats. For accompanied participants prices range from £20 to £28 per night - the price reflects the size of the property and the length of stay.

All the accommodation that the Institute has arranged is fully furnished and of good quality and the rent charged includes council tax, water rates, maintenance and standing charges for utilities. The prices reflect the fact that, in order to be able to guarantee accommodation for its relatively short-stay members, the Institute often has to rent properties for periods when they will be unoccupied, therefore the rent charged to members must cover these voids. The rent charge must bear a sensible relation to the subsistence allowance paid by the Institute, £30 per day in 1995/96. This allowance is primarily designed to cover the accommodation and basic food costs for a single person. It should also cover the cost of accommodation for a participant accompanied by his or her family, though not in this case the food costs as well.

Due to natural programme breaks and the fact that the visit period for participants varies considerably causing inevitable voids, it is difficult to get the average occupancy rate above 275 days per year. The housing office is in effect a small business with an annual turnover of

£200,000 which has to run at very close to zero margin, neither making a profit nor being an appreciable drain on the Institute's finances.

## 13.7 Publicity

The Institute has continued to publicise its activities widely. Posters announcing conferences and workshops are distributed to specially targetted mailing lists of UK, EU and overseas departments. They are also sent out to the appropriate programme email lists (see 5.2), to which there are over 500 individual subscribers in total. The weekly list of seminars is distributed to a separate email list which has nearly 200 subscribers, as well as being sent as a poster to many UK departments and individuals who have requested it in this format. The Institute's Call for Proposals was as usual sent to over 500 departments, as well as to many past participants and other individuals connected with the Institute. A copy of the current Call for Proposals document is given in Appendix I, together with instructions for the submission of a proposal.

All publicity information is also available on the Institute's World Wide Web server (URL **http://www.newton.cam.ac.uk**) which attracts a round 16,500 'visitors' per week. In addition to workshop and seminar infomation, the Web site includes general information about the Institute including background, scientific policy, relationship with other organisations such as BRIMS (Hewlett-Packard's Basic Research Institute in the Mathematical Sciences), how to contact staff and participants and information about each programme. The organisers of the *Semantics of Computation*, *Dynamics of Complex Fluids* and *Computer Security, Cryptology and Coding Theory* programmes produced their own Home Pages in addition to those produced by the Institute, providing news and programme information from the point of view of those directly involved.

The Institute continued to receive publicity in the national and local press, including a major article in the *Times* about the *Computer Security, Cryptology and Coding Theory* programme and articles in the local press reporting on the work of that and *The Dynamics of Complex Fluids* programme, as well as the unveiling of John Robinson's mathematical sculpture *Intuition*. Andrew Wiles attracted the attention of the local press during his visit to the Institute as Senior Fellow and and was also the subject of the BBC Horizon documentary *Fermat's Last Theorem* (part of which was filmed at the Institute) broadcast on 15th Jan 1996. Reviews of Hawking and Penrose's *The Nature of Space and Time* (see § 2.17) appeared in *Scientific American* and *Nature*.

## 13.8 Merchandise

Institute merchandise continued to sell well. *Semantics of Computation* T-shirts had sold out by the end of the programme, and the new generic Newton Institute T-shirt proved popular enough to re-stock in a wider variety of sizes and colours. Fermat's Last Theorem T-shirts continue to be in steady demand (telephone orders are received from all around the country) three years after Andrew Wiles' celebrated lecture at the Institute. Other items available are mugs, pens, postcards and Christmas cards. To order any of these items, please contact Andrea Le Core, Librarian and Information Officer (email a.lecore@newton.cam.ac.uk).

# A Long-Stay Participants

Please note that in the tables within this section, a long term participant is defined as one whose visits total 15 days or more.

## A.1 Semantics of Computation

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Abadi, M | DEC Systems Research | Italy | USA | 8th Aug - 2nd Sep |
| Abramsky, S | Imperial College | UK | UK | 9th Jul - 15th Dec |
| Brookes, S | Carnegie-Mellon University | UK | USA | 3rd Jul - 1st Oct |
| Bruce, KB | Williams College | USA | USA | 1st Aug - 31 Oct |
| Cardelli, L | DEC Systems Research | Italy | USA | 12th Aug - 9th Sep<br>23rd Oct - 27th Oct<br>28th Oct - 31 Oct |
| Constable, R | Cornell University | USA | USA | 26th Sep - 19th Oct |
| Dybjer, P | Chalmers Technical University | Sweden | Sweden | 30 Jul - 15th Dec |
| Freyd, PJ | University of Pennsylvannia | USA | USA | 16th Jul - 22nd Jul<br>7th Aug - 18th Aug<br>16th Sep - 29th Sep<br>20th Nov - 27th Nov |
| Gardner, PA | University of Edinburgh | UK | UK | 2nd Oct - 22nd Dec |
| Gunawardena, J | BRIMS | UK | UK | 17th Oct - 15th Dec |
| Gunter, C | University of Pennsylvania | USA | USA | 10th Aug - 15th Dec |
| Harper, R | Carnegie Mellon University | USA | USA | 12th Aug - 12th Nov |
| Hennessy, M | University of Sussex | Ireland | UK | 29th Aug - 10th Sep<br>18th Sep - 5th Oct |
| Hoare, CAR | University of Oxford | UK | UK | 5th Jul - 21st Jul |
| Hyland, JME | DPMMS, Cambridge | UK | UK | 6th Jul - 15th Dec |
| Ionitoiu, C | Technical University of Timisoara | Romania | Romania | 23rd Sep - 30 Sep<br>4th Nov - 10th Nov |
| Jagadeesan, R | Loyola University | India | USA | 6th Jul - 28th Jul |
| Jay, CB | Imperial College | Australia | UK | 1st Nov - 30 Nov |
| Johnstone, PT | DPMMS, Cambridge | UK | UK | 6th Jul - 15th Dec |
| Jones, CB | University of Manchester | UK | UK | 6th Jul - 15th Dec |
| Jung, A | Technische Hochshule Darmstadt | Germany | Germany | 1st Oct - 17th Dec |
| Kahn, G | INRIA | France | France | 2nd Jul - 30 Sep |
| Lincoln, P | SRI International | USA | USA | 14th Aug - 1st Sep<br>8th Oct - 20th Oct |
| Lipton, J | Wesleyan University | USA | USA | 6th Aug - 25th Sep |
| MacQueen, DB | AT & T Bell Labs | USA | USA | 7th Aug - 16th Nov |
| Milner, R | University of Edinburgh | UK | UK | 6th Jul - 15th Dec |
| Mitchell, JC | Stanford University | USA | USA | 1st Jul - 15th Dec |
| Moggi, E | University of Genoa | Italy | Italy | 6th Jul - 30 Sep |
| Montanari, U | University of Pisa | Italy | Italy | 21st Jul - 19th Aug |
| O'Hearn, P | Syracuse University | Canada | USA | 1st Oct - 7th Dec |
| Ong, C-HL | University of Oxford | Singapore | UK | 1st Aug - 30 Sep |
| Pierce, B | University of Edinburgh | USA | UK | 9th Jul - 15th Dec |
| Pitts, AM | Computer Lab, Cambridge | UK | UK | 6th Jul - 15th Dec |
| Power, AJ | Univeristy of Edinburgh | Australia | UK | 1st Nov - 30 Nov |
| Pratt, V | Stanford University | | USA | 6th Nov - 24th Nov |
| Reynolds, J | Imperial College | USA | UK | 1st Jul - 4th Sep |
| Riecke, J | AT & T Bell Labs | USA | USA | 1st Oct - 16th Dec |
| Robinson, EP | University of Sussex | UK | UK | 9th Jul - 15th Aug |

*continued on next page*

*continued from previous page*

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Sangiorgi, D | University of Edinburgh | Italy | UK | 1st Oct - 12th Dec |
| Saraswat, V | Xerox | India | USA | 21st Jul - 30 Aug |
| Sassone, V | Aarhus University | Italy | Denmark | 28th Oct - 30 Nov |
| Scedrov, A | University of Pennsylvannia | USA | USA | 31 Jul - 18th Dec |
| Scott, DS | Carnegie Mellon University | USA | USA | 15th Jul - 15th Oct |
| Scott, PJ | University of Ottawa | Canada | Canada | 1st Aug - 15th Dec |
| Sieber, K | Universität des Saarlandes | Germany | Germany | 4th Jul - 31 Jul |
| Stoughton, A | Kansas State University | USA | USA | 6th Jul - 31 Jul |
| Tennent, RD | University of Queens | Canada | Canada | 6th Jul - 31 Jul |
| Viswanathan, R | Stanford University | India | USA | 6th Jul - 15th Dec |
| Winskel, G | University of Aarhus | UK | Denmark | 6th Aug - 11th Aug<br>22nd Aug - 29th Dec |

## A.2 From Finite to Infinite Dimensional Dynamical Systems

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Afraimovich, V | Georgia Inst of Technology | Russia | USA | 21st Jul - 18th Aug |
| Baesens, C | Université de Bourgogne | Belgium | France | 16th Aug - 17th Dec |
| Bates, P | Brigham Young University | UK | USA | 20th Aug - 19th Dec |
| Bellettini, G | Univesity of Pisa | Italy | Italy | 9th Oct - 31 Oct |
| Broomhead, D | UMIST | UK | UK | 22nd Jul - 6th Aug<br>27th Aug - 15th Sep |
| Bunimovich, L | Georgia Inst of Technology | Russia | USA | 16th Aug - 15th Sep |
| Chillingworth, D | University of Southampton | UK | UK | 3rd Sep - 16th Sep<br>22nd Oct - 3rd Nov |
| Collet, P | Ecole Polytechnique | France | France | 21st Aug - 19th Oct |
| Constantin, P | University of Chicago | USA | USA | 21st Aug - 16th Nov |
| Cvitanovic, P | Niels Bohr Institute | Denmark | Denmark | 15th Aug - 30 Aug |
| Doering, CR | Los Alamos National Lab | USA | USA | 14th Aug - 15th Dec |
| Elgin, J | Imperial College | UK | UK | 20th Aug - 14th Sep<br>30 Oct - 10th Nov<br>20th Nov - 23rd Nov |
| Feireisl, E | Mathematial Institute AS CR | Czech Republic | Czech Republic | 15th Aug - 30 Sep<br>30 Oct - 10th Nov |
| Fife, P | University of Utah | USA | USA | 3rd Jul - 11th Aug<br>19th Aug - 13th Dec |
| Fusco, G | University of Rome | Italy | Italy | 24th Aug - 31 Oct |
| Gibbon, J | Imperial College | UK | UK | 14th Jul - 17th Dec |
| Glendinning, P | Queen Mary and Westfield College | UK | UK | 6th Jul - 17th Dec |
| Hale, J | Georgia Inst of Technology | USA | USA | 1st Jul - 30 Nov |
| Holm, D | Los Alamos National Lab | USA | USA | 21st Aug - 20th Sep |
| Holmes, P | Princeton University | UK | USA | 22nd Aug - 9th Sep |
| Keane, M | | USA | Netherlands | 22nd Jul - 26th Jul<br>16th Oct - 27th Oct |
| Kerr, RM | NCAR Boulder | USA | USA | 26th Aug - 22nd Sep |
| L'vov, VS | Weizmann Institute | Russia | Israel | 30 Sep - 31 Oct |
| Mackay, R | Université de Bourgogne | UK | UK | 16th Aug - 17th Dec |
| McGlade, J | University of Warwick | UK | UK | 27th Jul - 7th Sep<br>27th Nov - 1st Dec |
| Mierczynski, J | Technical University of Wroclaw | Poland | Poland | 20th Aug - 16th Sep |
| Moore, DR | Imperial College | USA | UK | 2nd Oct - 15th Dec |
| Nishiura, Y | Hokkaido University | Japan | Japan | 18th Nov - 8th Dec |
| Ohkitani, K | Hiroshima University | Japan | Japan | 10th Jul - 8th Aug<br>27th Aug - 2nd Sep |
| Polacik, P | Comenius University | Slovakia | Slovakia | 1st Aug - 10th Oct |
| Procaccia, I | Weizmann Institute | Israel | Israel | 21st Aug - 1st Sep<br>27th Sep - 27th Oct |
| Rand, DA | University of Warwick | UK | UK | 20th Jul - 15th Dec |
| Raugel, G | Université de Paris Sud | France | France | 18th Sep - 15th Oct |
| Robinson, JC | DAMTP, Cambridge | UK | UK | 6th Jul - 12th Dec |
| Sharkovsky, A | Ukrainian Academy of Sciences | Ukraine | Ukraine | 1st Aug - 30 Sep |
| Sparrow, CT | Newton Institute | UK | UK | 6th Jul - 17th Dec |
| Spiegel, E | Columbia University | USA | USA | 15th Sep - 15th Dec |
| Stark, J | University College London | Czech Republic | UK | 6th Jul - 20th Sep |
| Suhov, YM | DPMMS, Cambridge | Russia | UK | 13th Nov - 17th Dec |
| Takei, Y | University of Kyoto | Japan | Japan | 8th Oct - 4th Nov |
| Tereshko, VM | Moscow State University | Russia | Russia | 20th Aug - 15th Sep |
| Titi, ES | UC Irvine | Israel | USA | 19th Aug - 15th Dec |
| Yi, Y | Georgia Inst of Technology | China | USA | 10th Jul - 17th Dec |

## A.3 Dynamics of Complex Fluids

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Balan, C | Polytechnic Univ, Bucharest | Romania | Romania | 3rd Apr - 21st Apr |
| Brady, JF | CIT | USA | USA | 5th Jan - 30 Apr |
| Cantelaube, F | Université de Rennes I | France | France | 6th Jan - 30 Jun |
| Cates, M | University of Edinburgh | UK | UK | 8th Jan - 20th Jan<br>1st Feb - 15th Feb<br>20th Mar - 4th Apr<br>22nd Apr - 14th Jun<br>24th Jun - 28th Jun |
| Davies, AR | Univ Wales, Aberystwyth | UK | UK | 2nd Jun - 29th Jun |
| Doi, M | Nagoya University | Japan | Japan | 16th Mar - 12th Apr |
| Entov, VM | Russian Academy of Sciences | Russia | Russia | 6th Jan - 29th Jun |
| Goddard, J | UC La Jolla | USA | USA | 11th Jan - 30 Jun |
| Hamley, IW | University of Leeds | UK | UK | 14th Mar - 16th Mar<br>8th May - 25th May |
| Harlen, OG | University of Leeds | UK | UK | 8th Jan - 12th Jan<br>29th Jan - 2nd Feb<br>14th Apr - 20th Apr |
| Hinch, EJ | Trinty College, Cambridge | UK | UK | 6th Jan - 30 Jun |
| James, DF | University of Toronto | Canada | Canada | 7th Jan - 13th Jan<br>15th Jan - 21st Jun |
| Jones, JL | University of Durham | UK | UK | 11th Mar - 15th Mar<br>24th Mar - 4th Apr |
| Joseph, DD | University of Minnesota | USA | USA | 24th Mar - 19th Apr |
| Keunings, R | Université Catholique de Louvain | Belgium | Belgium | 6th Jan - 30 Jun |
| Larson, RG | AT & T Bell Labs | USA | USA | 3rd Jan - 31 May<br>19th Jun - 30 Jun |
| Leal, LG | UC Santa Barbara | USA | USA | 6th Jan - 3i Mar |
| Leonov, AI | University of Akron | Russia | USA | 7th Jan - 22nd Jan |
| Leslie, FM | University of Strathclyde | UK | UK | 8th Jan - 12th Jan<br>27th Jan - 23rd Feb |
| Lobanov, YY | Joint Inst for Nuclear Research | Russia | Russia | 2nd Jun - 22nd Jun |
| Marrucci, GP | University of Naples | Italy | Italy | 8th Jan - 12th Jan<br>24th Mar - 4th Apr |
| McKinley, GH | Harvard University | UK | USA | 6th Jan - 30 Jun |
| McLeish, T | Univertsity of Leeds | UK | UK | 4th Jan - 30 Jun |
| Mehta, A | SN Bose Nat Centre of Basic Sci | India | India | 11th Apr - 27th Apr |
| Milner, ST | Exxon Research & Engineering | USA | USA | 18th Mar - 17th May |
| Pearson, A | Schlumberger Cambridge Research | UK | UK | 6th Jan - 30 Jun |
| Petrie, CJS | University of Newcastle upon Tyne | UK | UK | 7th Jan - 13th Jan<br>14th Apr - 19th Apr<br>17th Jun - 21st Jun |
| Podneks, V | University of Leeds | Russia | Russia | 8th May - 25th May |
| Poon, WCK | University of Edinburgh | UK | UK | 8th Jan - 12th Jan<br>1st Mar - 4th Apr |
| Ramaswamy, S | Indian Inst of Science | India | India | 24th Mar - 20th Apr |
| Renardy, Y | Virginia Polytechnic Inst | USA | USA | 6th Jan - 29th Jun |
| Renardy, M | Virginia Polytechnic Inst | USA | USA | 6th Jan - 29th Jun |
| Semenov, AN | University of Leeds | Russia | Russia | 15th Mar - 4th Apr |
| Shiyanovskii, SV | Inst for Nuclear Research | Ukraine | Ukraine | 19th Feb - 11th Mar |
| Solis, FJ | Chicago State University | Mexico | USA | 5th Jan - 22nd Jun |
| Tanner, RI | University of Sydney | Australia | Australia | 14th Apr - 29th Jun |
| Topracioglu, C | University of Patras | UK | Greece | 1st Mar - 30 Apr<br>20th May - 22nd Jun |
| Townsend, P | Univ Wales, Swansea | UK | UK | 4th Jun - 28th Jun |

*continued on next page*

*continued from previous page*

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Wagner, MH | University of Stuttgart | Germany | Germany | 7th Jan - 20th Apr |
| Walters, K | Univ Wales, Aberystwyth | UK | UK | 3rd Jan - 30 Jun |
| White, LR | University of Melbourne | Australia | Australia | 1st Feb - 29th Jun |
| Yarin, AR | Israel Inst of Technology | Israel | Israel | 2nd Apr - 25th Apr |

## A.4 Computer Security, Cryptology and Coding Theory

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Abadi, M | DEC Systems Research | Argentina | USA | 9th Apr - 26th Apr |
| Anderson, R | Computer Lab, Cambridge | UK | UK | 2nd Jan - 21st Jun |
| Berson, TA | Anagram Lab | USA | USA | 8th Feb - 3rd Jun |
| Bezuidenhoudt, SJ | ESCOM | France | South Africa | 30 May - 22nd Jun |
| Burmester, M | Royal Holloway and Bedford | UK | UK | 1st Apr - 13th Apr<br>26th May - 1st Jun |
| Davenport, JH | University of Bath | UK | UK | 11th Mar - 29th Mar |
| DeBoer, MA | Eindhoven University of Technology | Netherlands | Netherlands | 2nd Jan - 31 Jan |
| Deswarte, YAL | LAAS-CNRS | France | France | 27th May - 16th Jun |
| Dichtl, M | Siemens AG | Germany | Germany | 10th Feb - 10th Mar |
| Diffie, W | Sun Microsystems | USA | USA | 20th Feb - 15th Mar<br>10th Apr - 22nd Apr<br>20th May - 2nd Jun<br>16th Jun - 25th Jun |
| Ding, C | University of Turku | China | Finland | 1st Feb - 29th Feb |
| Golic, J | Queensland University of Technology | Australia | Australia | 12th Jan - 22nd Mar |
| Gollmann, D | Royal Holloway and Bedford NC | Austria | UK | 20th Feb - 2nd Mar<br>13th May - 5th Jun |
| Gong, L | SRI International | USA | USA | 21st May - 25th Jun |
| Hansen, JP | Aarhus University | Denmark | Denmark | 2nd Jan - 26th Jan |
| Helleseth, T | University of Bergen | Norway | Norway | 14th Jan - 14th Feb |
| Hirschfeld, JWP | University of Sussex | UK | UK | 2nd Jan - 29th Jan |
| Jajodia, S | George Mason University | USA | USA | 1st Jun - 22nd Jun |
| Job, V | Marymount University | USA | USA | 2nd Jan - 30 Jan |
| Johansson, BTE | University of Lund | Sweden | Sweden | 20th Jan - 17th Feb |
| Kaliski, BS | RSA Data Security Inc | USA | USA | 8th Mar - 22nd Apr |
| Kemmerer, RA | UC Santa Barbara | USA | USA | 21st Apr - 11th May |
| Klapper, A | University of Kentucky | USA | USA | 19th Feb - 13th Mar |
| Klove, T | University of Bergen | Norway | Norway | 2nd Jan - 16th Feb |
| Knudsen, L | Katholieke Universiteit Leuven | Denmark | Belgium | 30 Jan - 23rd Feb |
| Korjik, VI | University of Telecommunications | Russia | Russia | 11th Feb - 25th Feb |
| Lam, K-Y | National University of Singapore | UK | Singapore | 12th May - 15th Jun |
| Landrock, P | University of Aarhus | Denmark | Denmark | 2nd Jan - 22nd Jun |
| Landwehr, CE | US Naval Research Lab | USA | USA | 2nd Jun - 22nd Jun |
| Lee, ES | Computer Lab, Cambridge | Canada | UK | 1st Apr - 21st Jun |
| MacKay, DJC | Cavendish Lab, Cambridge | UK | UK | 15th Jan - 30 Jan |
| Mao, W | Hewlett-Packard Labs, Bristol | China | UK | 31 Mar - 21st Apr |
| Massey, J | Swiss Federal Inst of Technology | USA | Switzerland | 12th Feb - 9th Mar |
| Matsui, M | Mitsubishi Electric Corp | Japan | Japan | 25th Jan - 9th Mar |
| Matsumoto, T | Yokohama National University | Japan | Japan | 24th Mar - 9th May |
| McCurley, K | Sandia National Laboratories | USA | USA | 10th Mar - 31 Mar |
| McEliece, RJ | CIT | USA | USA | 21st Jan - 10th Feb |
| McKee, JF | DPMMS, Cambridge | UK | UK | 11th Mar - 4th Apr |
| McLean, J | US Naval Research Lab | USA | USA | 20th Apr - 1st Jun |
| Meadows, CA | US Naval Research Lab | USA | USA | 13th May - 30 Jun |
| Millen, JK | MITRE Corporation | USA | USA | 25th May - 9th Jun |
| Morris, R | National Security Agency (Retired) | USA | USA | 10th Apr - 22nd Jun |
| Naor, M | Weizman Inst | Israel | Israel | 5th Apr - 20th Apr |
| Needham, RM | Computer Lab, Cambridge | UK | UK | 8th Jan - 21st Jun |
| Nyberg, K | Finnish Defence Forces | Finland | Finland | 18th Feb - 3rd Mar |
| Okamoto, T | Nippon Telephone & Telegraph Corp | Japan | Japan | 25th Mar - 19th Apr |
| Pellikaan, R | Eindhoven University of Technology | Netherlands | Netherlands | 5th Jan - 11th Jan<br>15th Jan - 19th Jan<br>23rd Jan - 26th Jan |

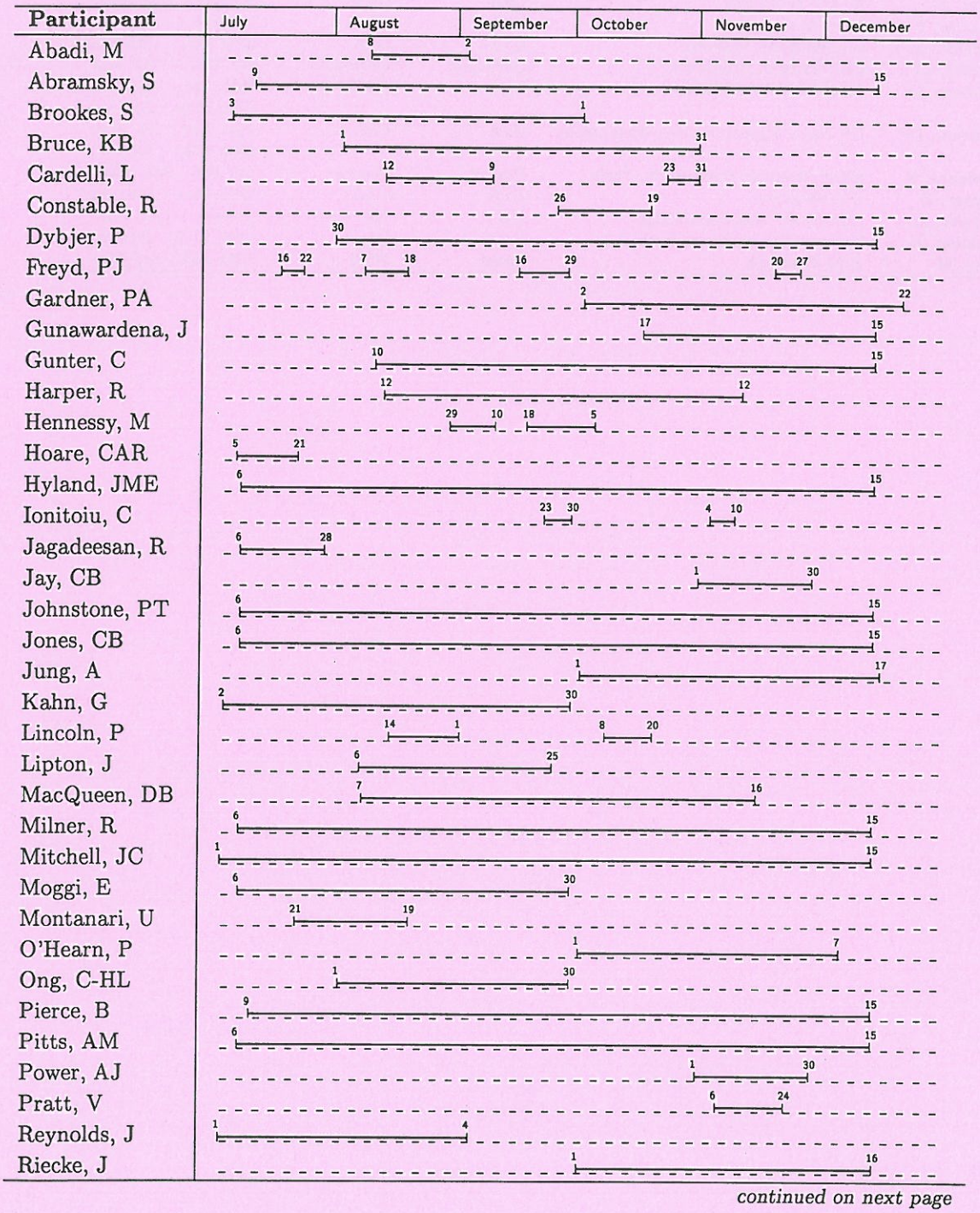
*continued on next page*

*continued from previous page*

| Name | Home Institution | Nationality | Country of Residence | Dates of visit(s) |
|---|---|---|---|---|
| Pfitzmann, B | University of Hildesheim | Germany | Germany | 30 Mar - 24th Jun |
| Pomerance, C | University of Georgia | USA | USA | 11th Mar - 31 Mar |
| Preneel, B | Katholieke Universiteit Leuven | Belgium | Belgium | 30 Jan - 9th Mar |
| Reiter, M | AT&T Bell Labs | USA | USA | 31 May - 23rd Jun |
| Rogaway, P | UC Davis | USA | USA | 1st Apr - 15th Apr |
| Schneier, B | Counterpane Systems | USA | USA | 20th Feb - 10th Mar |
| Schnorr, CP | University of Frankfurt | Germany | Germany | 4th Mar - 14th Apr |
| Simmons, G | Sandia National Labs | USA | USA | 25th Jan - 12th Mar<br>27th May - 2nd Jun |
| Syverson, PF | US Naval Research Lab, Washington | USA | USA | 21st Apr - 4th May<br>28th May - 8th Jun |
| Vaudenay, S | Ecole Normale Supèrieure, Paris | France | France | 5th Feb - 8th Mar |
| Wagner, D | UC Berkeley | USA | USA | 27th Mar - 14th Apr |
| Wheeler, DJ | Computer Lab, Cambridge | UK | UK | 1st Feb - 21st Jun |
| Yahalom, R | Hebrew University of Jerusalem | Israel | Israel | 29th Mar - 27th Apr |
| Yung, M | IBM Research | Israel | USA | 13th Feb - 3rd Mar |

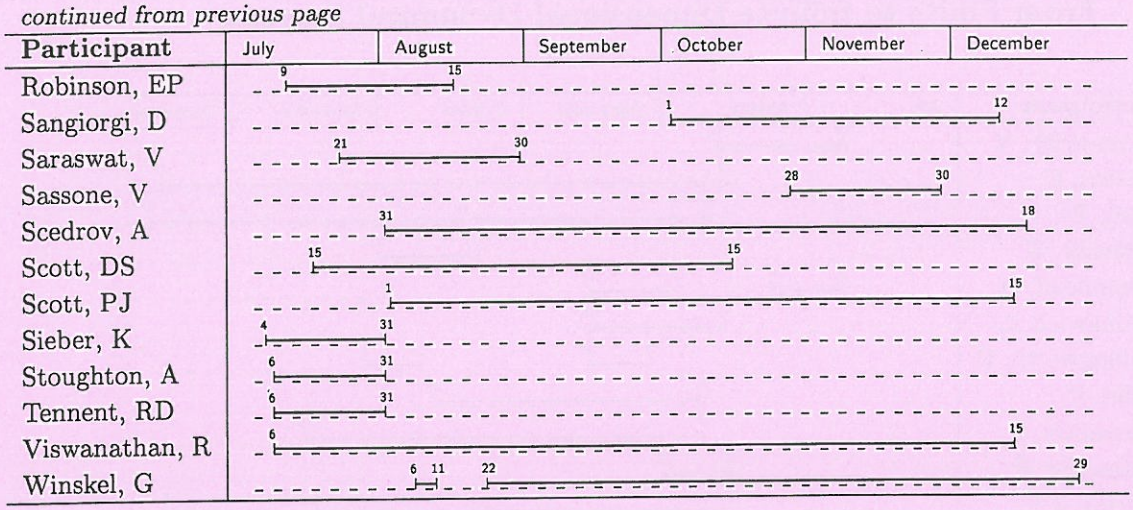
# B Chart of Visits of Long-stay Participants

## B.1 Semantics of Computation

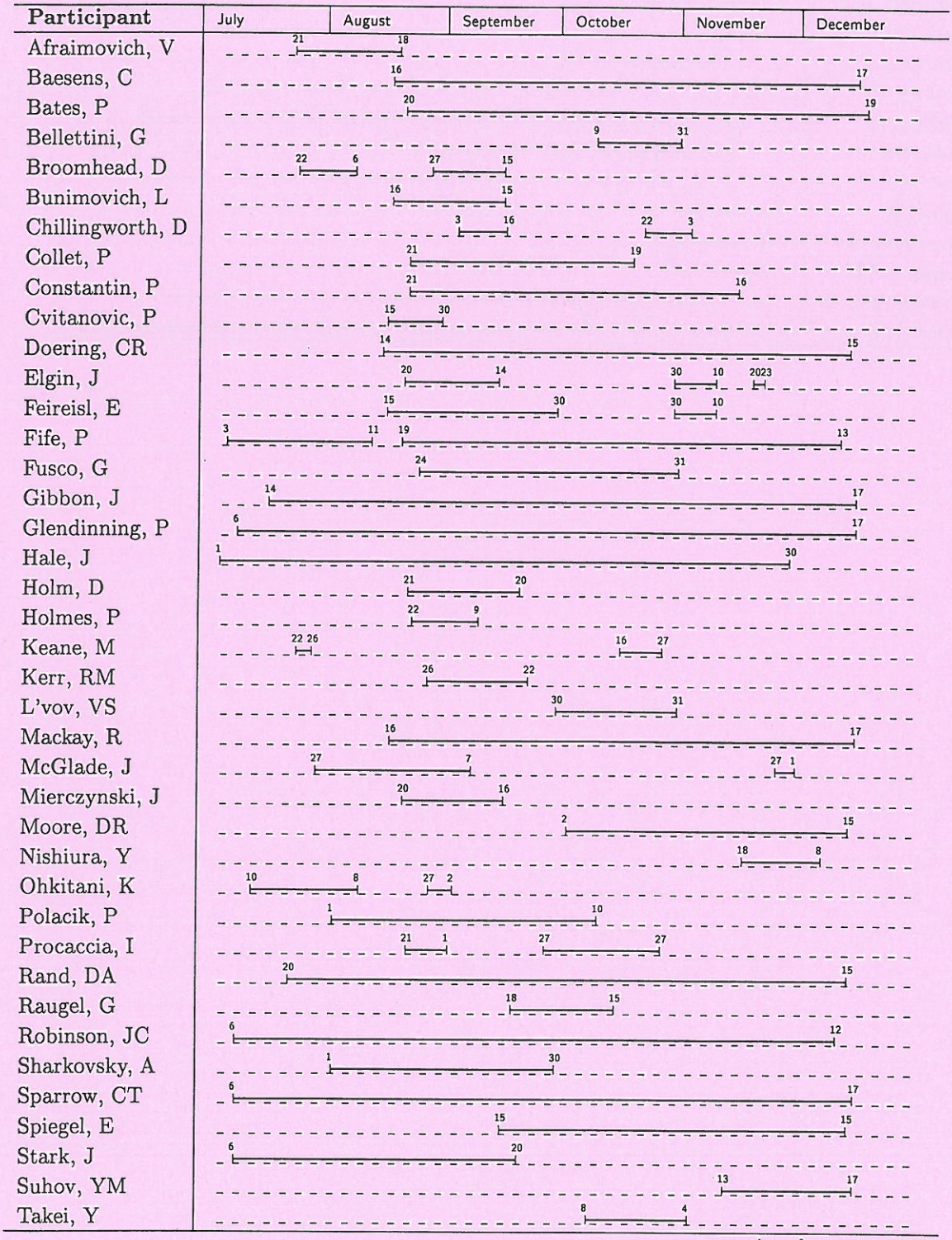



*continued on next page*

*continued from previous page*



## B.2 From Finite to Infinite Dimensional Dynamical Systems

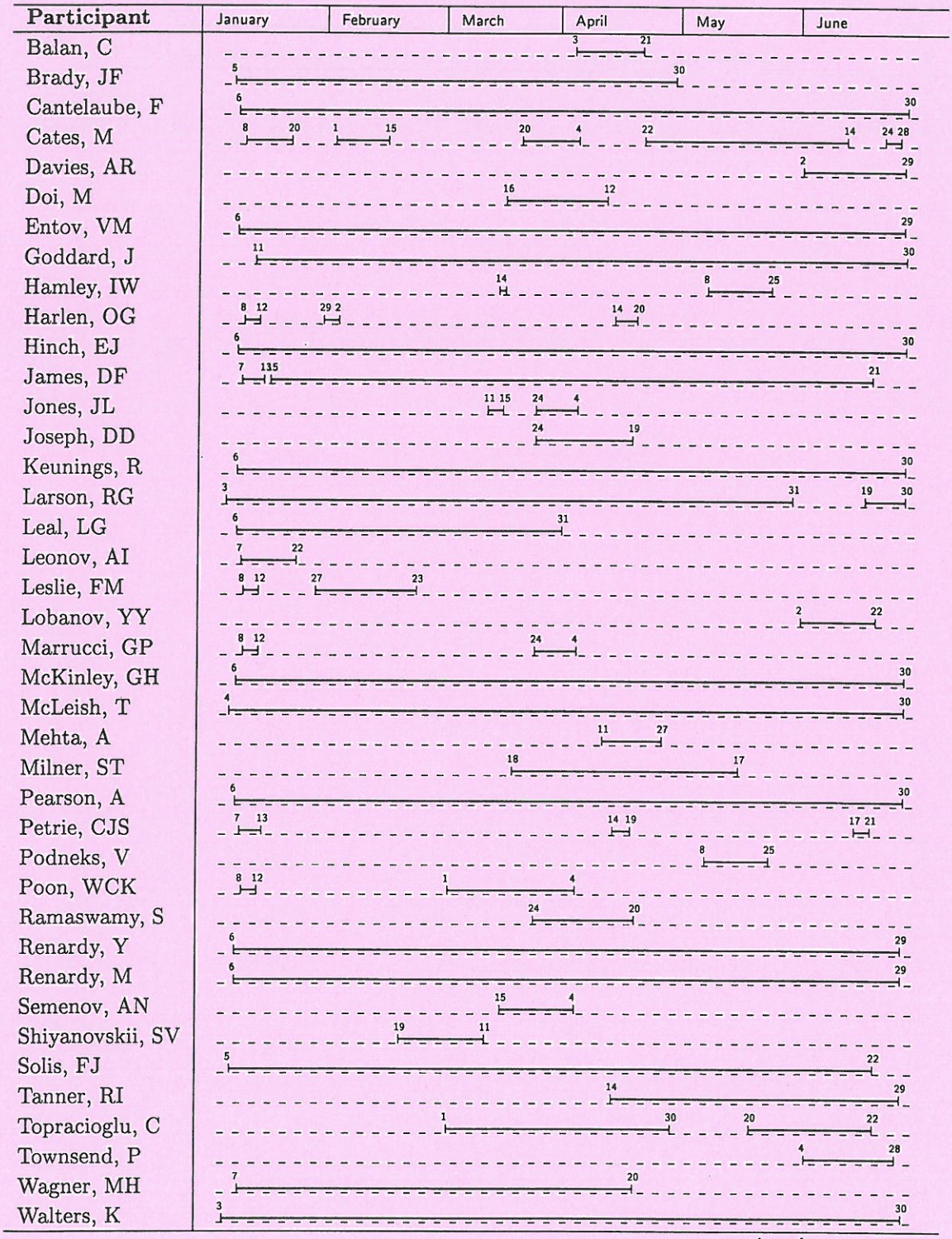



*continued on next page*

*continued from previous page*

| Participant | July | August | September | October | November | December |
|---|---|---|---|---|---|---|
| Tereshko, VM | | 20 | 15 | | | |
| Titi, ES | | 19 | | | | 15 |
| Yi, Y | | 10 | | | | 17 |

## B.3 Dynamics of Complex Fluids

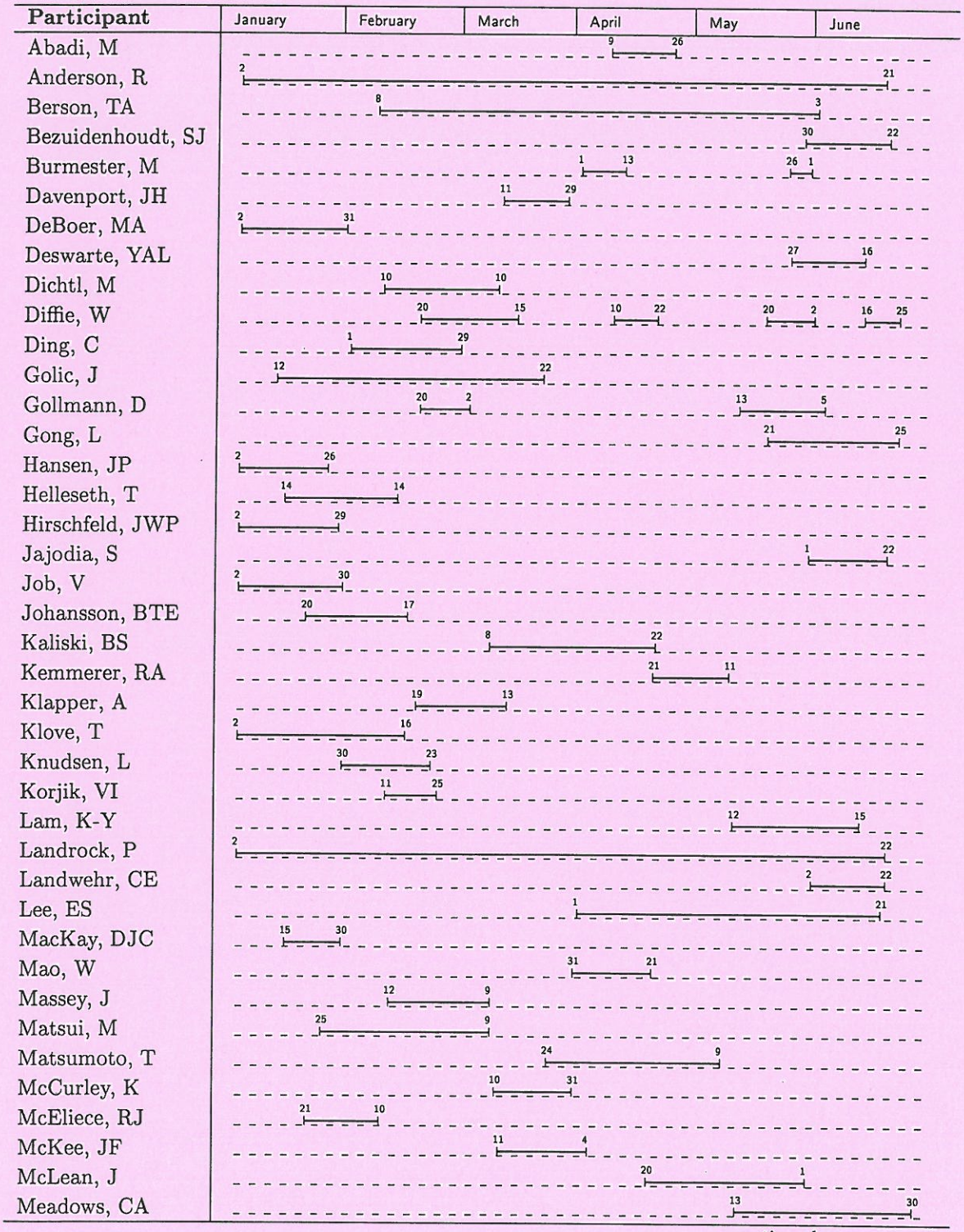



*continued on next page*

*continued from previous page*

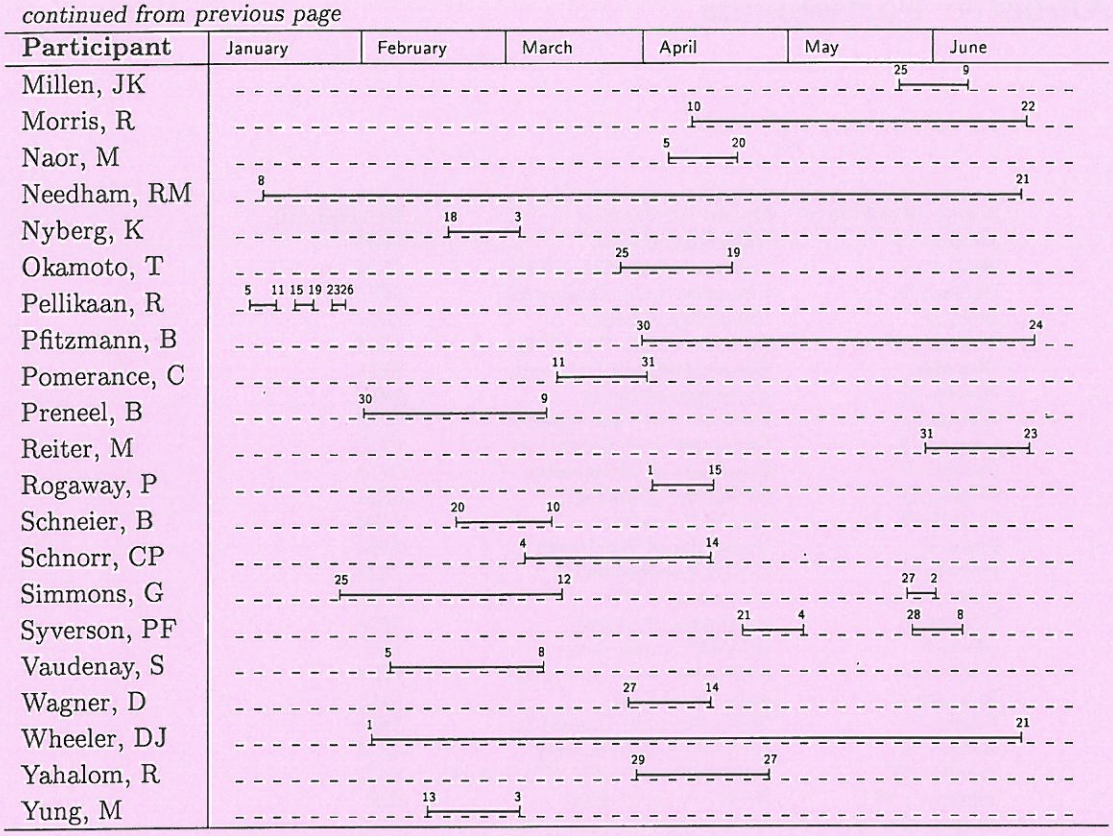
| Participant | January | February | March | April | May | June |
|---|---|---|---|---|---|---|
| White, LR | | 1 | | | | 29 |
| Yarin, AR | | | | 2 | 25 | |

## B.4 Computer Security, Cryptology and Coding Theory




*continued on next page*

*continued from previous page*



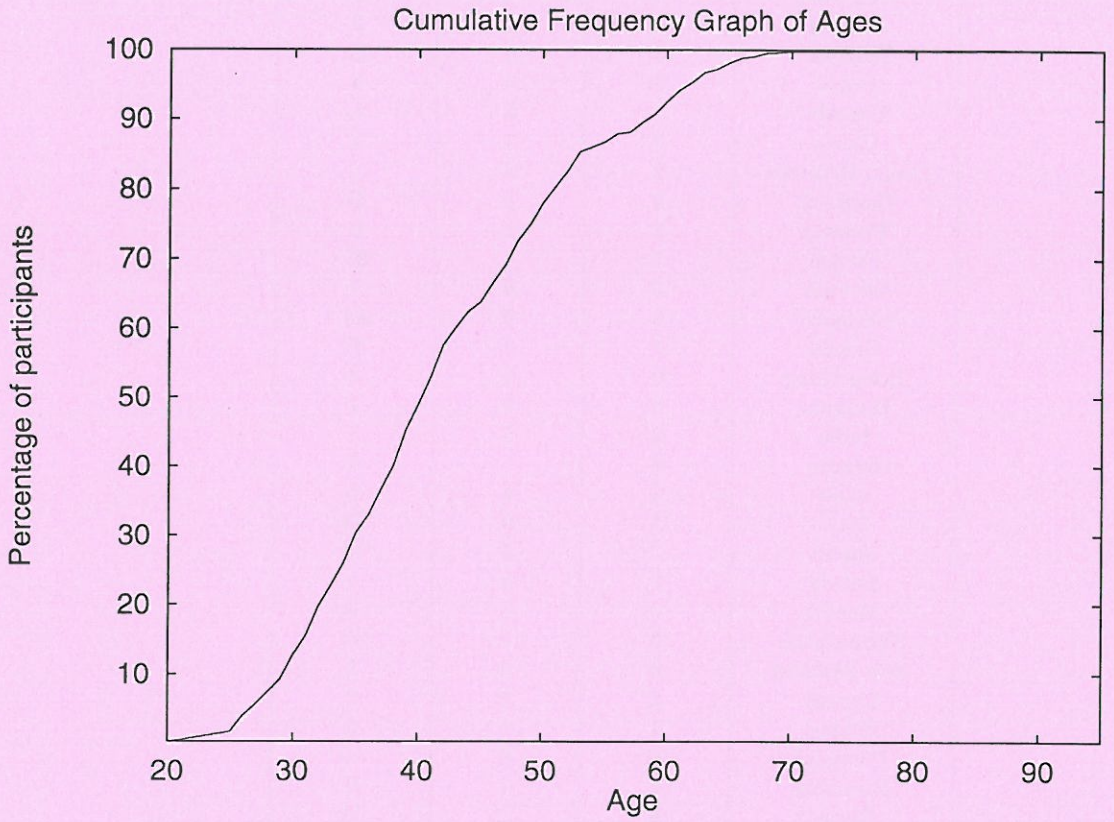
# C Affiliated Participants

| Name of Affiliate | Home Institution | Programme |
|---|---|---|
| Archieri, D | University of Pisa | SEM |
| Beatriz, A | Computer Lab, Cambridge | SEM |
| Benton, N | Computer Lab, Cambridge | SEM |
| Bick, D | University of Leeds | DCF |
| Bierman, G | Computer Lab, Cambridge | SEM |
| Birkedal, L | Carnegie Mellon University | SEM |
| Bisliko, G | University of Leeds | DCF |
| Biswas, S | University of Pennsylvania | SEM |
| Chuang, S | Computer Lab, Cambridge | CCC |
| Collette, P | University of Manchester | SEM |
| Cubric, D | DPMMS, Cambridge | SEM |
| Finkelstein, S | McGill University | SEM |
| Fiore, P | University of Edinburgh | SEM |
| Furnet, C | INRIA Rocquencourt | SEM |
| Gadducci, F | University of Pisa | SEM |
| Gianna, B | University of Genoa | SEM |
| Glass, K | DPMMS, Cambridge | FID |
| Gordon, A | Computer Lab, Cambridge | SEM |
| Heritage, C | Imperial College | FID |
| Hilken, B | Computer Lab, Cambridge | SEM |
| Hodges, S | University of Manchester | SEM |
| Jakobsen T | Technical University of Denmark | CCC |
| Johnston, M | DAMTP, Cambridge | FID |
| Karpelevich, F | Moscow Inst of Transport | FID |
| Kegelmann, M | Technische Hochschule Darmstadt | SEM |
| Kennedy, A | Computer Lab, Cambridge | SEM |
| Kohei, H | University of Manchester | SEM |
| Laing, C | DAMTP, Cambridge | FID |
| Martin, U | University of St Andrews | SEM |
| Murray, R | DPMMS, Cambridge | FID |
| Nestman, U | FAU Erlangen-Nürnberg | SEM |
| Nikander, P | Helsinki University of Technology | CCC |
| Nobuko, Y | University of Manchester | SEM |
| De Paiva V | Computer Lab, Cambridge | SEM |
| Price, G | Computer Lab, Cambridge | CCC |
| Rees, G | Computer Lab, Cambridge | SEM |
| Rosolini, G | University of Genoa | SEM |
| Rydehead, D | University of Manchester | SEM |
| Schalk, A | Computer Lab, Cambridge | SEM |
| Selinger, P | University of Pennsylvania | SEM |
| Sewell, P | Computer Lab, Cambridge | SEM |
| Stark, I | Computer Lab, Cambridge | SEM |
| Sutherland, C | Computer Lab, Cambridge | CCC |
| Wagner, K | Computer Lab, Cambridge | SEM |
| Yamaguchi, H | University of Manchester | SEM |
| Zeng, C | Brigham Young University | FID |

# D Nationality and Country of Residence of Participants

| Country | Long-stay | | Short-stay |
|---|---|---|---|
| | Residents | Nationals | Residents |
| Argentina | 0 | 1 | 0 |
| Australia | 3 | 5 | 14 |
| Austria | 0 | 1 | 9 |
| Belgium | 3 | 3 | 21 |
| Brazil | 0 | 0 | 6 |
| Canada | 3 | 5 | 5 |
| China | 0 | 3 | 2 |
| Czech Republic | 1 | 2 | 2 |
| Denmark | 5 | 4 | 35 |
| Finland | 2 | 1 | 6 |
| France | 7 | 7 | 91 |
| Georgia | 0 | 0 | 1 |
| Germany | 6 | 6 | 65 |
| Greece | 1 | 0 | 9 |
| Hong Kong | 0 | 0 | 2 |
| Hungary | 0 | 0 | 1 |
| India | 2 | 5 | 5 |
| Ireland | 0 | 1 | 3 |
| Israel | 5 | 6 | 6 |
| Italy | 5 | 9 | 38 |
| Japan | 7 | 7 | 13 |
| Latvia | 0 | 0 | 1 |
| Mexico | 0 | 1 | 4 |
| Netherlands | 3 | 2 | 43 |
| New Zealand | 0 | 0 | 2 |
| Norway | 2 | 2 | 2 |
| Poland | 1 | 1 | 6 |
| Portugal | 0 | 0 | 10 |
| Romania | 2 | 2 | 0 |
| Russia | 6 | 11 | 14 |
| Singapore | 1 | 1 | 0 |
| Slovakia | 1 | 1 | 1 |
| South Africa | 1 | 0 | 1 |
| Spain | 0 | 0 | 12 |
| Sweden | 2 | 2 | 3 |
| Switzerland | 1 | 0 | 9 |
| Taiwan | 0 | 0 | 1 |
| Turkey | 0 | 0 | 2 |
| UK | 55 | 48 | 506 |
| USA | 68 | 55 | 137 |
| Ukraine | 2 | 2 | 1 |
| *Unknown* | 0 | 1 | 3 |
| Total | 195 | 195 | 1092 |

# E Cumulative Frequency Graph of Ages



# F Papers Produced by Participants

Please note that this list includes publications produced or in preparation during 1995/96.

| Authors<br>*Title* | Programme |
|---|---|
| Abdelguerfi M, Kaliski B, Patterson W<br>*Public-key security systems - introduction* | CCC |
| Afraimovich V, Hale J<br>*Synchronization phenomena in a system of coupled oscillators (book)* | FID |
| Anderson R<br>*A security policy model for clinical information systems* | CCC |
| Anderson R, Ding C, Helleseth T *et al*<br>*Democratic secret sharing with geometric codes* | CCC |
| Anderson R, Preneel B, Vaudenay S *et al*<br>*The Newton channel* | CCC |
| Balan C<br>*Rheologic model for the material fluid behaviour* | DCF |
| Bates P W, Fife P, Gardner R *et al*<br>*The existence of travelling wave solutions of a generalised phase field model (book)* | FID |
| Bates P W, Ren X<br>*Heteroclinic orbits for a higher order phase transition problem* | FID |
| Bates P W, Fife P, Gardner R *et al*<br>*Phase field models for hypercooled solidification* | FID |
| Bates P W, Fife P, Ren X *et al*<br>*Travelling waves in a convolution model for phase transitions* | FID |
| Bates P W, Chen X, Deng X<br>*A numerical scheme for the two phase Mullins-Sekerka problem* | FID |
| Bates P W, Lu K, Zeng C<br>*Persistence of normally hyperbolic invariant manifolds for semiflows in Banach space* | FID |
| Belletini G, Fusco G<br>*The dynamics of V=H-$\bar{H}$: motion of a small drop on a fixed suface* | FID |
| Berson T A<br>*The art of information warfare (working title)* | CCC |
| Berson T A, Knudsen L, Gollmann D<br>*Truncated differentials of SAFER* | CCC |
| Berson T A, McLean J<br>*Almost any channel may contain a hidden channel* | CCC |
| Brady J, Morris J F<br>*Microstructure of strongly sheared suspensions and its impact on diffusion and rheology* | DCF |

| Authors / *Title* | Programme |
|---|---|
| Brookes S<br>*The essence of parallel Algol* | SEM |
| Bunimovich L<br>*Dynamical systems* | FID |
| Campillo A, Farran JI<br>*An algorithm to compute weight functions for decoding* | CCC |
| Cates M<br>*Of micelles and many layered vesicles* | DCF |
| Cates M, Mao Y, Lekkerkerker H<br>*Theory of the depletion force due to rods* | DCF |
| Cates M, Wittmer J P, Claudin P<br>*Stress propagation and arching in static sandpiles* | DCF |
| Christianson B, Harbison W S, Lomas M<br>*Why isn't trust transitive?* | CCC |
| Collet P, Glendinning P<br>*Nonlinear dynamics of extended systems* | FID |
| Collet P, Titi E<br>*Determining modes for dissipative extended systems* | FID |
| Constable R L, Buss E<br>*Constructive type theory* | SEM |
| Constantin P, Doering C<br>*Convection* | FID |
| Curien P<br>*Abstract machines for dialogue games* | SEM |
| Cvitanic J<br>*Nonlinear financial mathematics: hedging and portfolio optimization* | FIN |
| Dåmgard IB, Pfitzmann B, Pedersen T P<br>*On the existence of statistically hiding bit commitment schemes and fail-stop signatures* | CCC |
| Davenport J<br>*Proving and certifying polynominal irreducibility* | CCC |
| Davenport J<br>*Galois groups and the simplification of polynomials* | CCC |
| Davies A R, Anderssen R S<br>*On the direct recovery of partial viscosities from oscillatory shear measurements* | DCF |
| Dawson E, Golic J, Khodkau A *et al*<br>*Cryptanalysis of the summation generator with three input shift registers* | CCC |
| De Boer M A, Pellikaan R<br>*Some results on improved geometric Goppa codes* | CCC |

*continued on next page*

*continued from previous page*

| Authors | Programme |
|---|---|
| *Title* | |
| Diffie W, Massey J, Schneier B *et al*<br>*Initial cryptanalysis of RC4* | CCC |
| Doering C, Constantin P, Titi E<br>*Rigorous estimates of small scales in turbulent flows* | FID |
| Doering C, Constantin P<br>*Variational bounds on energy dissipation in incompressible flows III: Convection* | FID |
| Dybjer P, Cubric D, Scott P<br>*The Yoneda embedding and solutions of word problems* | SEM |
| Dybjer P<br>*Representing inductively defined types by Welladenys in Martin-Löf's type theory* | SEM |
| Dybjer P, Coquand T<br>*Intuitionistic model construction and normalization points* | SEM |
| Elgin J<br>*Multifractality of the Lorenz equations* | FID |
| Entov V, Alexandrou A N<br>*A two-phase model for semisolid metals processing* | DCF |
| Entov V, Hinch J E<br>*Effect of spectrum of relaxation times on capillary thinning* | DCF |
| Entov V, Alexandrou A N<br>*On the steady-state advancement of fingers and bubbles in a Hele-Shaw cell filled by a non-newtonian fluid* | DCF |
| Entov V, Barsoum M, Shmaryan L E<br>*On capillary instability of jets of magneto-rheological fluids* | DCF |
| Feigenbaum J, Blaze M, Lacy J<br>*Managing trust in medical information systems* | CCC |
| Fife P<br>*Recent advances in the theory of hypercooled solidification* | FID |
| Fife P, Kielhofer H, Maier S<br>*Doubly periodic solutions of nonlinear elliptic equations and applications to the Cahn-Hilliard theory of phase separation* | FID |
| Fife P<br>*A nonlocal analog of similinear parabolic differential equation* | FID |
| Fife P, Penrose O<br>*A phase field model for diffusion induced phase transitions* | FID |
| Fife P, Bates P, Wang X<br>*Travelling waves in a nonlocal model for phase transitions* | FID |
| Fife P<br>*Recent developments in phase field theory* | FID |

| Authors / *Title* | Programme |
|---|---|
| Fife P, Wang X<br>*A nonlocal model for phase transitions: interfaces in higher dimensions* | FID |
| Fife P<br>*Clines and material interfaces with nonlocal interaction* | FID |
| Fusco G, Bates P, Fife P<br>*Nucleation in the context of the Cahn-Hilliard equation: existence of multi-spike stationary solutions* | FID |
| Garcia A, Stichtenoth H<br>*Asymptotically good towers of function fields over finite fields* | CCC |
| Gardner P<br>*A name-free account of action calculi* | SEM |
| Gardner P<br>*The expressive power of higher-order action calculi* | SEM |
| de Gennes P-G<br>*Injection threshold for a branched polymer inside a nanopore* | DCF |
| Gibbon JD<br>*Recent results on the Navier–Stokes equations* | FID |
| Gibbon JD<br>*A voyage around the Navier–Stokes equations* | FID |
| Gibbon JD<br>*Analysis of the 2d and 3d Navier–Stokes equations* | FID |
| Gibbon, JD<br>*An estimate of the attractor dimension for the 3d Navier–Stokes equations* | FID |
| Gill AJ, Kibble TWB<br>*Quench induced vortices in the symmetry broken phase of liquid $^4He$* | TOP |
| Glendinning P, Swinnerton-Dyer HPF<br>*Bifurcations from infinity in the Nosé equations* | FID |
| Glendinning P<br>*The critical orbit closure and irrational rotations for unimodal maps* | FID |
| Glendinning P<br>*Bifurcations and rotation numbers for maps of the circle associated with flows on the torus and models of cardiac arhythmias* | FID |
| Glendinning P, Swinnerton-Dyer HPF<br>*Bifurcations from infinity* | FID |
| Glendinning P, Robinson J<br>*From finite to infinite dimensional dynamical systems* | FID |
| Glendinning P, Sparrow C<br>*Shilnikov's saddle node bifurcation* | FID |

| Authors / *Title* | Programme |
|---|---|
| Glendinning P, Laing C<br>*Bifocal homoclinic bifurcations* | FID |
| Glendinning P, Perry L<br>*Melnikov analysis of chaos in a simple epidemiological model* | FID |
| Glendinning P, Laing C<br>*A homoclinic hierarchy* | FID |
| Glendinning P<br>*Differential equations with bifocal homoclinic orbits* | FID |
| Golic J<br>*Linear statistical weakness of RC4* | CCC |
| Golic J<br>*In the computation of low-weight parity checks* | CCC |
| Golic J<br>*Cryptanalysis of the alternating step generation* | CCC |
| Golic J<br>*Cryptanalysis of a stream cipher known as A5* | CCC |
| Golic J, Menicocci R<br>*Correlation attacks on up/down and stop/go cascades* | CCC |
| Golic J<br>*On conditional correlation attacks on combiners with memory* | CCC |
| Gollmann D<br>*Fast software encryption (proceedings)* | CCC |
| Gollmann D, Geiselmann W<br>*Correlation attacks on cascades of clock controlled shift registers* | CCC |
| Graessley W<br>*Polymeric liquids and networks* | DCF |
| Gruska D<br>*Process algebra for shared resources* | SEM |
| Gunawardena J<br>*New connections between mathematics and computer science: report, abstracts and bibliography of a workshop* | SEM |
| Gunter C<br>*Abstracting dependencies between software configuration hems* | SEM |
| Hale J, Raugel G<br>*Perturbations of invariant manifolds* | FID |
| Hansen J P<br>*Zero-dimensional schemes and codes - cohomological methods* | CCC |
| Hansen J P, Jensen H E<br>*Error-separating polynominals of low degree* | CCC |

| Authors / *Title* | Programme |
|---|---|
| Harper R, Cardelli L<br>*ML2000 design note 1: internal language* | SEM |
| Harper R, Mitchell J<br>*A CHAM-like semantics for objects* | SEM |
| Harper R, Birkedal L, Pitts A *et al*<br>*Constructing relations over recursive types in an operational setting* | SEM |
| Helleseth T, Klove T, Levenshtein V<br>*The Newton radius of codes* | CCC |
| Helleseth T, Johansson T<br>*Universal hash functions from exponential sums over finite fields and Galois rings* | CCC |
| Hirschfeld J W P<br>*Projective geometries over finite fields (book - 2nd Edition)* | CCC |
| Hirschfeld J W P, Korchmáros G<br>*The number of rational points on an algebraic curve over a finite field* | CCC |
| Hoare CAR, Jifeng HE<br>*Unifying theories - the challenge for computing science* | SEM |
| Hoholdt T, Pellikaan G, Van Lint JH<br>*Algebraic geometry codes* | CCC |
| Hu H<br>*Simulation of particle motion in viscoelastic fluids* | DCF |
| Hyland J M E<br>*Game semantics (proceedings)* | SEM |
| Jakobsen T, Knudsen L R<br>*Breaking ciphers of low nonlinear compexity* | CCC |
| Jay C B<br>*A functional type system* | SEM |
| Jay C B, Clarke D G, Edwards J J<br>*Exploiting shape in parallel programming* | SEM |
| Job V, Johnston C<br>*A finite field valued wavelet transform* | CCC |
| Jones C B, Collette P<br>*Enhancing the tractability of rely/guarantee specifications in the development of interfering operations* | SEM |
| Jones CB<br>*Accommodating interference in object - based formal designs* | SEM |
| Jung A<br>*Ten years of mathematical structures in denotational semantics* | SEM |

| Authors | Programme |
|---|---|
| *Title* | |
| Jung A | SEM |
| *Domain theory in logical form for continuous domains* | |
| Jung A, Sünderhauf P | SEM |
| *Uniform approximation of topological spaces* | |
| Jung A, Sünderhauf P | SEM |
| *On the duality of compact US open* | |
| Jung A | SEM |
| *A note on Hechmann's probabilistic power locale* | |
| Jung A | SEM |
| *Lawson-compactness for the probalistic powerdomain* | |
| Kaliski B, Lomas M | CCC |
| *IEEE P1363: A standard for RSA, Diffie-Hellman and elliptic curve crytography* | |
| Keane M, Gunawardena J | FID |
| *Existence of cycle times* | |
| Kelsey J, Schneier B, Walker J | CCC |
| *Distributed procturing* | |
| Kerr R | FID |
| *Velocity and spatial scaling of singular Euler dynamics* | |
| Kerr R | FID |
| *Rayleigh number scaling in numerical convection* | |
| Keunings R | DCF |
| *On the Peterlin approximation for finitely extensible dumbbells* | |
| Klove T, Svirid Y | CCC |
| *Diffuse difference triangle sets* | |
| Knudsen L R, Lai X, Preneel B | CCC |
| *Attacks on fast double length hash functions* | |
| Korjik V, Yavolev V | CCC |
| *Constructive algorithms of coding and decoding on wire-tap channel coding* | |
| Kuhn M | CCC |
| *Tamper resistance - a cautionary note* | |
| Kuhn M | CCC |
| *Cipher instruction search attack on the bus encryption security microcontroller DS500ZFP* | |
| Landrock P | CCC |
| *A new realisation of electronic negotiable instrument* | |
| Landrock P | CCC |
| *Security and confidentiality issues relating to the electronic data interchange of clinical data* | |

*continued on next page*

*continued from previous page*

| Authors<br>*Title* | Programme |
|---|---|
| Landrock P, Nissen K<br>*Cryptology (book)* | CCC |
| Landwehr C<br>*Requirements for a wireless identification system* | CCC |
| Larson R, McLeish T C B<br>*Molecular constitutive equations for a class of branched polymers: the pom-pom polymer* | DCF |
| Larson R, Mather P T<br>*The shear-flow properties of liquid crystals* | DCF |
| Larson R<br>*Normal stress differences in shear-thickening suspensions* | DCF |
| Leonov A, Padovan J<br>*A scaling theorem for effective computations of 3D unsteady flows by nonlinear viscoelastic constitutive equations of differential type* | DCF |
| Leslie F<br>*Continuum theory for liquid crystals* | DCF |
| Lincoln P<br>*Intuitionistic second order linear logic* | SEM |
| Lincoln P<br>*Authenticated agreement* | SEM |
| Lobanov Y<br>*On some method of numerical integration in functional spaces* | DCF |
| Loskutov A Y, Tereshko V M, Vasiliev K A<br>*Predicted dynamics for cyclic cascades of chaotic deterministic automata* | FID |
| Loskutov A Y, Tereshko V M, Vasiliev K A<br>*Stabilization of chaotic dynamics on one-dimensional maps by a cycle parametric transformation* | FID |
| Loskutov A Y, Rybalko S D<br>*Suppression of chaos in families on one-and two-dimensional maps* | FID |
| MacKay D, McEliece RJ, Neal R<br>*Good error-correcting codes based on very sparse matrices (revision of an earlier paper)* | CCC |
| MacKay D, Peto L<br>*A hierarchical dirichlet language model* | CCC |
| MacQueen DB<br>*Semantics of higher-order models* | SEM |
| Mao W<br>*Lightweight micro-cash for the Internet* | CCC |
| Mao W<br>*Blind certification of public keys and off-line electronic cash* | CCC |

| Authors / *Title* | Programme |
|---|---|
| Mao W<br>*On cryptographic techniques for on-line bankcard payment transactions using open networks* | CCC |
| Matsui M<br>*On Walsh spectrums of power functions* | CCC |
| McKee J F, Pinch R G E<br>*Old and new deterministic factoring algorithms* | CCC |
| McKinley G H, Pakdel P, Oztekin A<br>*Geometric and rheological scaling of purely elastic instabilities* | DCF |
| McKinley G H, Jamés D F, Muller S J<br>*Continuum and molecular properties from the modeling of ideally-elastic dilute polymer solutions* | DCF |
| McKinley G H<br>*Inter-relation between shear and extension properties of dilute solution models* | DCF |
| McKinley G H, Spiegelberg S<br>*Elastic instability in filament stretching devices* | DCF |
| McKinley G H<br>*Elastic instability and extensional rheology of polymer solutions* | DCF |
| McKinley G H, James D F, Muller S J<br>*Molecular and continuum models for ideally elastic dilute polymer solutions* | DCF |
| McKinley G H, Crook S, Mackley M R *et al*<br>*The Ovaici necklace and other instabilities in the cold extrusion of chocolate* | DCF |
| McLean J<br>*Using non-interference to analyze cryptographic protocols* | CCC |
| Meadows C, Lam K Y<br>*Reasoning about electronic payment protocols* | CCC |
| Meadows C<br>*A survey of confidentiality modes (working title)* | CCC |
| Mehta A, Luck J M, Bhattachaijee J K<br>*Some analytical results on noisy nonlinear coupled equations* | DCF |
| Melvin P, Morton H R<br>*The coloured Jones function* | LDT |
| Mestl, Lemag C, Glass L<br>*Chaos in high-dimensional gene and neural networks* | FID |
| Michor P, Dubois-Violette M<br>*More on the Froelicher Nijenhuis bracket in non-communicative geometry* | GGR |

*continued on next page*

*continued from previous page*

| Authors / *Title* | Programme |
|---|---|
| Milner S, Fredrickson G H<br>*Time-dependant reactive coupling at polymer-polymer interfaces* | DCF |
| Milner S<br>*Contour-length fluctuations and crossover to reptation* | DCF |
| Milner S, McLeish T, Adams C<br>*A parameter-free theory of star polymer dynamics* | DCF |
| Morain F<br>*Memoire d'habitation* | CCC |
| Morain F<br>*Algorithms for computing isogenies between elliptic curves* | DCF |
| Moreno O, Moreno C<br>*Report on exponential sums and applications* | CCC |
| Moskowitz I S, Kang M, Montrose B *et al*<br>*A case study of two NRL pump prototypes* | CCC |
| Naor M, Shamir A<br>*Visual cryptography II - improving the contrast via the cover base* | CCC |
| Nishiura Y, Ohnishi I<br>*Spectral comparison between 4th and 2nd order conservative equations with nonlocal terms* | FID |
| O'Hearn P, Riecke J, Rosolini G *et al*<br>*Domains and denotational semantics: history, accomplishments and open problems* | SEM |
| Okhitani K, Yamada M<br>*Inviscid and inviscid-limit behavior of a quasi-geostrophic flow* | FID |
| Okhitani K<br>*A successive approximation of the Taylor-Green vortex* | FID |
| Oliva W M, Fusco G<br>*Systems of repelling particles: formation of symmetric structures* | FID |
| Ong L<br>*On full abstraction of PCF* | SEM |
| Pedersen TP, Pfitzmann B<br>*Fail-stop signatures* | CCC |
| Petrie C J S, Pearson J R A<br>*Fibre spinning; corotational models (working title)* | DCF |
| Petrie C J S, Walters K<br>*Three-dimensional presentation of external flow data* | DCF |
| Pfitzmann B, Waidner M<br>*Properties of payment systems - general definition sketch and classification* | CCC |
| Pfitzmann B<br>*Trials of traced traitors* | CCC |

*continued on next page*

*continued from previous page*

| Authors / *Title* | Programme |
|---|---|
| Pfitzmann B, Schunter M<br>*Asymmetric fingerprinting* | CCC |
| Pfitzmann B<br>*Digital signature schemes - general framework and fail-stop signatures* | CCC |
| Pierce B C, Cardelli B<br>*Comparing object encodings* | SEM |
| Pierce B C, Turner<br>*Pict: a programming language based on the pi-calculus* | SEM |
| Pinch R<br>*On-line multiple secret sharing* | CCC |
| Pitts A M, Dybjer P<br>*Semantics and logics of computation (proceedings)* | SEM |
| Pitts A M<br>*Reasoning about local variables with operationally based logical relations* | SEM |
| Pitts A M<br>*Operationally based theories of program equivalence* | SEM |
| Pitts A M, Gordon A D<br>*Higher order operational techniques in semantics (book)* | SEM |
| Podneks V E, Hamley I W<br>*Landau-Brazovskii theory for the $Ia\bar{3}d$ phase* | DCF |
| Poláčik P, Feireisl E<br>*Asymptotic behaviour of solutions of time-periodic parabolic equations on $\mathbb{R}$* | FID |
| Poon W C K<br>*What is a liquid?* | DCF |
| Poon W C K, Warren P B<br>*Phase transition kinetics in colloid-polymer matrices* | DCF |
| Power J<br>*Elementary control structures* | SEM |
| Ramaswamy S, Lahiri R<br>*Sedimenting colloidal crystals: unsafe at any speed?* | DCF |
| Renardy M, Coward A V, Renardy Y *et al*<br>*Temporal evolution of periodic disturbances in two-layer Couette flow* | DCF |
| Renardy M<br>*A degenerate parabolic-hyperbolic system modeling the spreading of surfactants* | DCF |

| Authors / *Title* | Programme |
|---|---|
| Renardy M<br>*Reentrant corner behaviour of the PTT fluid* | DCF |
| Renardy M<br>*High Weissenberg number boundary layers for the upper convected Maxwell fluid* | DCF |
| Renardy M<br>*Qualitative correlation between viscometric and linear viscoelastic functions* | DCF |
| Renardy Y, Joseph D D, Chen K<br>*Core-annular flows* | DCF |
| Renardy Y, Coward A V, Papageorgious D *et al*<br>*Advances in multi-fluid flows* | DCF |
| Renardy Y<br>*Pattern formation for oscillatory bulk-mode competition* | DCF |
| Renardy Y, Coward A V<br>*Small amplitude oscillatory forcing on two-layer plane channel flow* | DCF |
| Renardy Y<br>*Patterns at the onset of salt finger formation for surface warming* | DCF |
| Renardy Y, Schmitt R W<br>*Linear stability analysis of salt fingers with surface evaporation or warming* | DCF |
| Renardy Y<br>*Snakes and corkscrews in core-annular flow of two fluids* | DCF |
| Renardy Y, Coward A V<br>*Thin-film evolution of core-annular flow of upper convected Maxwell liquids* | DCF |
| Reynolds JC, O'Hearn P<br>*From Algol to polymorphic linear lambda calculus* | SEM |
| Riecke J G, Reppy J<br>*Programming language design and implementation* | SEM |
| Robinson J C<br>*Asymptotic completeness of inertial manifolds* | FID |
| Robinson J C<br>*Finite-dimensional behaviour on global attractors* | FID |
| Robinson J C<br>*Flow normal hyperbolicity and inertial manifolds* | FID |
| Rogaway P<br>*The security of DESX* | CCC |
| Safavi-Naini R<br>*Authentication systems with arbetration* | CCC |

*continued on next page*

*continued from previous page*

| Authors | Programme |
|---|---|
| *Title* | |
| Sangiorgi D, Pierce B | SEM |
| *Polymorphic bisimulation* | |
| Sangiorgi D, Fiore M, Moggi E | SEM |
| *A fully-abstract model for the $\pi$-calculus* | |
| Sangiorgi D | SEM |
| *An interpretation of typed objects into $\pi$-calculus* | |
| Saphiannikova M G, Darinskii A A, Dyakonva N | DCF |
| *Computer simulation of dilute polymer solutions in transient elongational flows* | |
| Saphiannikova M G, Darinskii A A | DCF |
| *Computer simulation of dilute polymer solutions in oscillatory elongational flow* | |
| Scedrov A, Lincoln P, Mitchell J C | SEM |
| *Linear logic proof games and optimization* | |
| Schneier B, Kelsey J | CCC |
| *Automatic event-stream notorization using digital signatures* | |
| Schnorr C | CCC |
| *Security of $2^t$ root identification and signatures* | |
| Semenov A N, McLeish T | DCF |
| *Relaxation of fluctuations in entangled polymer mixtures* | |
| Semenov A N, McLeish T | DCF |
| *Coupling between polymer density fluctuations and polymer dynamics at high molecular weights* | |
| Sharkovsky A N, Fedorenko A D, Fedorenko V V *et al* | FID |
| *Farey's rule for stable periodic waves in a transmission line* | |
| Sharkovsky A N, Fedorenko A D, Fedorenko V V *et al* | FID |
| *Coexistence of periodic orbits for one class of discontinuous maps* | |
| Shitikara MV, Rossikhin Y | FID |
| *Analysis of free damped vibrations of a hereditarily elastic functional calculus oscillator* | |
| Shiyanovski S, Kuksenok D, Ruthwandl R | DCF |
| *Topological defects in nemadic filled with colloid particles* | |
| Shiyanovskii S, Kuksnok O V, Ruhwandl R W *et al* | DCF |
| *Topological defects in a nematic filled with colloid particles* | |
| Shreve S, El Karoui N, Jeanblanc-Picque M | FIN |
| *Robustness of the Black and Scholes formula* | |
| Solis F J, Tao L | DCF |
| *Lacunarity of random fractals* | |
| Solonnikov V | DCF |
| *The Stokes and Oseen asymptotics in the problem of a steady motion of two immiscible liquids* | |

*continued on next page*

*continued from previous page*

| Authors | Programme |
|---|---|
| *Title* | |
| Spiegel E | FID |
| *Cosmic lacunarity* | |
| Spiegel E | FID |
| *Bifurcation of species* | |
| Spiegelberg SH, McKinley GH | DCF |
| *Stress relaxation and elastic decohesion in filament stretching rheometers* | |
| Sridhar T, Orr N | DCF |
| *Stress relaxation in extension* | |
| Stoughten A | SEM |
| *Porgi: a proof or refutation generator for intuitionistic propositional logic* | |
| Takei Y | FID |
| *On the connection formula for the first Painlevé equations* | |
| Tanner R I, Walters K | DCF |
| *Rheology: an historical perspective* | |
| Titi E, Ferrari A | FID |
| *A note on the Beale-Kato-Majda result for analytic solutions of the 3-D Euler equations* | |
| Titi E, Berkooz G, Lumley JL | FID |
| *Well-posedness for spatially localized models of fluid flow* | |
| Titi E, Ferrari A | FID |
| *Gevrey regularity for nonlinear analytic parabolic equations* | |
| Titi E, García-Archilla B, Novo J | FID |
| *Postprocessing the Galerkin method: a novel approach to approximate inertial manifolds* | |
| Titi E, Levermore CD, Oliver M | FID |
| *Global well-posedness for models of shallow water in a basin with a varying bottom* | |
| Titi E, Levermore CD, Oliver M | FID |
| *Global well-posedness for the lake equations* | |
| Titi E | FID |
| *Rigorous estimates of small scales in turbulent flows* | |
| Vaudenay S | CCC |
| *Hidden collisions on DSS* | |
| Viswanathan R, Mitchell J | SEM |
| *Effective models of polymorphism, recursion and subtyping* | |
| Viswanathan R, Abadi M, Cardelli L | SEM |
| *An interpretation of objects and object types* | |
| Wagner D | CCC |
| *How to build a hidden trapdoor in your block cipher* | |

| Authors | Programme |
|---|---|
| *Title* | |
| Wheeler D | CCC |
| *Transactions using bets* | |
| White L R, Landman K A | DCF |
| *Optimized pressure filtration throughput of suspensions exhibiting compressive yield stress* | |
| White L R | DCF |
| *Slumping of materials with a shear yield stress - a plastic flow approach* | |
| Wolper J | CCC |
| *Codes from Schubert varieties* | |
| Wolper J | CCC |
| *The topology of Hamada's Formula (P=2)* | |
| Xing C | CCC |
| *Drinfeld module of rank 1 and curves with many rational points* | |
| Yarin A L, Lifoosky E, Shapiro M | DCF |
| *Theory of rheological behaviour of highly concentrated suspension under the conditions of strong impact at the free surface* | |
| Yarin A L, Gottlieb O, Roisman I V | DCF |
| *Chaotic rotation of small particles shaped as a triaxial ellipsoid in simple shear flow* | |
| Yi Y | FID |
| *Almost automorphy and skew-product semiflow Part I: almost automorphy and almost periodicity* | |
| Yi Y, Shen W | FID |
| *Almost automorphy and skew-product semiflow Part II: skew-product semiflow* | |
| Yi Y, Shen W | FID |
| *Almost automorphy and skew-product semiflow part III: application to differential equations* | |
| Zimmermann K H | CCC |
| *On a class of Hecke-modules as linear codes* | |

**Total number of papers within this table: 264**

# G Seminars and Lectures

## G.1 Semantics of Computation

| Name | Seminar Title | Date Presented |
|---|---|---|
| C Martin | *Relations and predicate transformers* | 10/07/95 |
| J He | *From algebra to operational semantics* | 10/07/95 |
| R Tennent | *What is data refinement* | 10/07/95 |
| P Gardiner | *Power simulation is the weakest reasonable preconguence* | 11/07/95 |
| D Naumann | *Transformer semantics and higher order programs* | 11/07/95 |
| C Hoare | *Unifying theories* | 11/07/95 |
| C Hoare | *The sequential calculus* | 12/07/95 |
| G Kahn | *Semantic ideas for building and maintaining programs: progress and problems* | 17/07/95 |
| A Stewart | *Reasoning about data parallel array assignment* | 17/07/95 |
| G Smith | *Polymorphic variables* | 17/07/95 |
| C Hoare | *Unified theories of programming* | 17/07/95 |
| R Milner | *Interaction vs. evaluation* | 18/07/95 |
| D Walker | *Confluence of processes and systems of objects* | 18/07/95 |
| M Tofte | *Using types to express properties of interaction with a store* | 18/07/95 |
| P Freyd | *Between mathematics and computation: problems and perspectives* | 18/07/95 |
| D Benson | *Sketches and modules* | 18/07/95 |
| J Reynolds | *The interaction between semantics and programming language design* | 19/07/95 |
| R Tennent | *Semantics and language design for algol-like languages* | 19/07/95 |
| P Wadler | *Theory and practice in the design of Haskell* | 19/07/95 |
| C Jones | *Some practical problems and their influence on semantics* | 20/07/95 |
| B Pierce | *Linearity and the pi-calculus* | 20/07/95 |
| M Sintzoff | *Programs, proofs and dynamical systems* | 20/07/95 |
| K Honda | *Presenting processes* | 20/07/95 |
| R Jagadeesan | *Computing with continuous change* | 20/07/95 |
| P Wegner | *Interaction machines: semantics and expressive power* | 20/07/95 |
| V Yodaiken | *The sequence function tree presentation of automata feedback products, & its application to real-time computation* | 20/07/95 |
| A Yonezawa | *Theory and practice of concurrent object-orientated programming* | 21/07/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| U Reddy | *Object-based semantics* | 21/07/95 |
| L Paulson | *A concrete final coalgebra theorem for ZF set theory* | 21/07/95 |
| M Kwiatkowska | *Towards a fair powerdomain* | 21/07/95 |
| S Brookes | *Fairness revisited* | 21/07/95 |
| B Jay | *A fresh look at parametric polymorphism* | 21/07/95 |
| E Moggi | *Monadic semantics of CCS-like calculi* | 21/07/95 |
| R Jagadeesan | *Verifying safety properties of Esterel programs and an application to telecommunications* | 26/07/95 |
| K Sieber | *Full abstraction via logical relations* | 28/07/95 |
| U Montanari | *Checking bisimilarity for finitary history-dependent systems* | 02/08/95 |
| H Sondergaard | *Semantics-based analysis of (constraint) logic programs* | 04/08/95 |
| GC Wraith | *Finitary categories and cancellation* | 07/08/95 |
| J Adámek | *From Scott domains to Scott-complete categories* | 07/08/95 |
| T Plewe | *Localic triquotient maps are effective descent maps* | 07/08/95 |
| M Jibladze | *Another nonstandard NNO* | 07/08/95 |
| P Taylor | *On the general recursion theorem* | 07/08/95 |
| R Milner | *Control structures: a model of interaction* | 07/08/95 |
| D Pavlović | *Convenient categories of processes and simulations, I: modulo strong bisimularity* | 07/08/95 |
| A Heller | *Homological algebra as generalized homotopy theory* | 07/08/95 |
| G Janelidze | *Galois correspondence for commutative rings* | 07/08/95 |
| E Badouel | *Dualities between nets and automata induced by schizophrenic objects* | 07/08/95 |
| Y Kawahara | *Relational set theory* | 07/08/95 |
| H Kleisli | *How the group algebra of a topological group should be constructed* | 07/08/95 |
| P Buneman | *Languages for collection types* | 08/08/95 |
| S Soloviev | *Proof of a conjecture of S MacLane* | 08/08/95 |
| A Asperti | *Effective applicative structures* | 08/08/95 |
| JME Hyland | *The S-replete construction* | 08/08/95 |
| M Zawadowski | *On model completion of the first order theories of varieties of algebras arising from logic* | 08/08/95 |
| RAG Seely | *Proof theory for linear logics without negation* | 08/08/95 |
| V Trnková | *Representability and local representability of algebraic theories* | 08/08/95 |
| Y Diers | *Characterization of categories of algebraic sets* | 08/08/95 |
| A Obtulowicz | *The levels of monadicity over graphs, generalized algebraic theories, and hierarchical specifications* | 08/08/95 |
| G Winskel | *An introduction to sequentiality* | 09/08/95 |
| AK Simpson | *The convex power domain in a category of posets realized by cpos* | 09/08/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| MP Fiore | *Lifting as a KZ-doctrine* | 09/08/95 |
| R Backhouse | *Categorical fixed point calculus* | 09/08/95 |
| I Moerdijk | *Homotopy types of spaces and of topoi* | 10/08/95 |
| M Tierney | *On the theory of path groupoids II* | 10/08/95 |
| D Pronk | *Groupoids representing sheaves on orbifolds* | 10/08/95 |
| FJ De Vries | *Projection spaces: a simple domain to solve equations* | 10/08/95 |
| S Abramsky | *Typed realizability* | 10/08/95 |
| SD Brookes | *A category-theoretic treatment of a parallel Algol-like language* | 10/08/95 |
| T Altenkirch | *Categorical reconstruction of a reduction-free normalization proof* | 10/08/95 |
| A Pultr | *Completion: strictness vs. functoriality* | 10/08/95 |
| MC Bunge | *The symmetric monad on TOP* | 10/08/95 |
| M Hasegawa | *Decomposing typed lambda calculus into a couple of categorical programming languages* | 10/08/95 |
| A Scedrov | *The work of Moez Alimohamed: a characterization of lambda definability in categorical models of implicit polymorphism* | 10/08/95 |
| J Pradines | *Calculus of fractions revisited: a geometrical insight* | 10/08/95 |
| MP Fourman | *A proposed categorical semantics for ML modules* | 11/08/95 |
| JR Otto | *V-comprehension and P-space* | 11/08/95 |
| VCV de Paiva | *Lineale-valued sets* | 11/08/95 |
| GM Kelly | *A sufficient condition for flexibility of a 2-monad* | 11/08/95 |
| DB Verity | *Surface diagrams, associahedra and weak n-categories* | 11/08/95 |
| J Rosický | *Quantaloids and concurrent computation* | 11/08/95 |
| J van Oosten | *Fibrations and calculi of fractions* | 11/08/95 |
| J Lambek | *Relations in categories* | 11/08/95 |
| M Abadi | *Interpretations of objects and object types* | 14/08/95 |
| G Castagna | *Covariance and contravariance: conflict without a cause* | 14/08/95 |
| S Vorobyov | *Hierarchical approximations to Fsub* | 14/08/95 |
| D Remy | *The case of typechecking with constraint types: typing record concatenation* | 14/08/95 |
| A Letichevsky | *The means of typing in APS* | 14/08/95 |
| L Cardelli | *On subtyping and matching* | 15/08/95 |
| S Nishizaki | *Typed lambda calculus with first-class environments* | 15/08/95 |
| V Saraswat | *Default timed concurrent constraint programming* | 15/08/95 |
| A Kind | *Type inference with generic type schemes* | 15/08/95 |
| J Palsberg | *Type inference with subtyping* | 15/08/95 |
| P Scott | *Linear logic and games* | 15/08/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| K Bruce | *Subtyping is not a good match for OOL'S* | 16/08/95 |
| K Laufer | *Extending the Hindley/Milner systems with existential and universal polymorphism* | 16/08/95 |
| A Gordon | *Bisimilartiy for a first-order calculus of objects with subtyping* | 16/08/95 |
| S Smith | *Constrained type inference for object oriented programming* | 17/08/95 |
| A Compagnoni | *Subtyping dependent types* | 17/08/95 |
| B Pierce | *Linearity and pi-calculus* | 17/08/95 |
| M Muller | *Type diagnosis for a higher-order concurrent constraint language* | 17/08/95 |
| D MacQueen | *The design space for parametric modules* | 18/08/95 |
| T Sheard | *A dependent type system for program generators* | 18/08/95 |
| A Kennedy | *An extension of ML with dimension types* | 18/08/95 |
| S Aditya | *Functional abstractions in a strongly-typed, imperative language* | 18/08/95 |
| M Tofte | *Region inference for higher-order functional languages* | 18/08/95 |
| R Harper | *ML 2000* | 18/08/95 |
| V Saraswat | *Non-monotonicity in synchronous programming: a model for instantaneous defaults* | 25/08/95 |
| C Fournet | *Towards a distributed pi-calculus: The reflexive CHAM and the join-calculus* | 30/08/95 |
| K Bruce | *The search for a 'good' static-type discipline for object-oriented languages* | 13/09/95 |
| PJ Scott | *Linear lauchli semantics and full completeness theorems* | 15/09/95 |
| D Pym | *Functorial Kripke models of the lambda pi-calculus* | 18/09/95 |
| J Harland | *Some remarks on proof-theoretic notions of operational equivalence* | 18/09/95 |
| P Freyd | *Allegories* | 18/09/95 |
| J Power | *A proposed semantics for logic programs* | 19/09/95 |
| J Lloyd | *Integrating functional and logic programs* | 19/09/95 |
| J Lipton | *Categorical logic programming* | 19/09/95 |
| P Freyd | *The internal logic of cartesian categories* | 19/09/95 |
| B Pierce | *Using types to compare objects and ADTs* | 20/09/95 |
| A Pitts | *Operationally-based theories of programme equivalence I* | 25/09/95 |
| M Hofmann | *Dependent type theory; syntax, semantics, and applications I* | 25/09/95 |
| M Nielsen | *Models for concurrency I* | 25/09/95 |
| E Moggi | *Metalanguages and applications I* | 25/09/95 |
| M Hyland | *Game semantics I* | 25/09/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| T Coquand | *Computational content of classical logic I* | 25/09/95 |
| E Moggi | *Metalanguages and applications II* | 26/09/95 |
| T Coquand | *Computational content of classical logic II* | 26/09/95 |
| M Hyland | *Game semantics II* | 26/09/95 |
| S Abramsky | *Semantics of Interaction I* | 26/09/95 |
| T Coquand | *Computational content of classical logic III* | 26/09/95 |
| M Hofmann | *Dependent type, syntax, semantics, and applications II* | 26/09/95 |
| S Abramsky | *Semantics of interaction II* | 27/09/95 |
| T Coquand | *Computational content of classical logic IV* | 27/09/95 |
| A Pitts | *Operationally-based theories of program equivalence II* | 27/09/95 |
| M Nielsen | *Models for concurrency II* | 28/09/95 |
| A Pitts | *Operationally-based theories of program equivalence III* | 28/09/95 |
| S Abramsky | *Semantics of interaction III* | 28/09/95 |
| M Hofmann | *Dependent type theory; syntax, semantics, and applications III* | 28/09/95 |
| E Moggi | *Metalanguages and applications III* | 28/09/95 |
| M Hyland | *Game semantics III* | 28/09/95 |
| M Hofmann | *Dependent type theory; syntax, semantics, and applications IV* | 29/09/95 |
| M Nielsen | *Models for concurrency III* | 29/09/95 |
| M Nielsen | *Models for concurrency IV* | 29/09/95 |
| E Moggi | *Metalanguages and applications IV* | 29/09/95 |
| M Hyland | *Game semantics IV* | 29/09/95 |
| S Abramsky | *Semantics of interaction IV* | 29/09/95 |
| R Milner | *Applying the pi-calculus* | 02/10/95 |
| G Boudol | *Relating lambda-calculus and pi-calculus* | 02/10/95 |
| S Prasad | *Interprocess communication as cut elimination* | 02/10/95 |
| U Nestmann | *Correctness of encodings* | 02/10/95 |
| K Honda | *Idioms for insteraction* | 02/10/95 |
| A Jeffrey | *Monadic types for the semantics of concurrent functional programming* | 03/10/95 |
| S Peyton-Jones | *Concurrent Haskell* | 03/10/95 |
| J-J Levy | *Distributed pict* | 03/10/95 |
| J Niehren | *Functional computation in a uniformly concurrent calculus with logic variables* | 03/10/95 |
| D Sangiorgi | *Proof techniques for bisimulation* | 04/10/95 |
| U Montanari | *The weak late pi-calculus semantics as observation equivalence OR Checking bisimilarity for finitary pi-calculus* | 04/10/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| P Sewell | *Observational equivalence for pict* | 04/10/95 |
| C Priami | *Non-interleaving semantics for mobile processes* | 04/10/95 |
| D Cubric | *On the semantics of the universal quantifier* | 11/10/95 |
| R Constable | *Expressing computational complexity in type theory* | 13/10/95 |
| J-Y Girard | *Light linear logic* | 16/10/95 |
| V de Paiva | *New models of intuitionistic linear logic* | 16/10/95 |
| P Scott | *Linear Lauchli semantics* | 16/10/95 |
| A Scedrov | *Optimization problems in propositional linear logic I* | 16/10/95 |
| N Benton | *Mixing intuitionistic logic and intuitionistic linear logic* | 16/10/95 |
| A Barber | *DILL - A dual context intuitionistic linear logic* | 16/10/95 |
| G Plotkin | *Second-order type theory, parametricity and recursion* | 17/10/95 |
| P O'Hearn | *From algol to polymorphic linear lambda-calculus* | 17/10/95 |
| D Pym | *What is a linear logic programming language?* | 17/10/95 |
| J Mitchell | *Optimization problems in propositional linear logic II* | 17/10/95 |
| Y Lafont | *Phase semantics and decision problems in linear logic* | 17/10/95 |
| P Baillot | *Intensionally fully abstract model of PCF and geometry of interaction* | 17/10/95 |
| L Regnier | *Relating innocent games and Krivine's environment machine* | 17/10/95 |
| S Abramsky | *Game semantics for idealized parallel algol* | 18/10/95 |
| F Davey | *The localisation of copy* | 18/10/95 |
| B Mitchell | *An internal/external environment model of linear logic* | 18/10/95 |
| P Lincoln | *Optimization problems in propositional linear logic III* | 18/10/95 |
| A Schalk | *Lineale-valued sets* | 18/10/95 |
| T Brauner | *Fixpoints and fixpoint objects in a linear category* | 18/10/95 |
| G Bellin | *Braided proof nets for MLL with MIX* | 18/10/95 |
| A Jung | *Domain theory in logical form for continuous domains* | 25/10/95 |
| J G Riecke | *Kripke logical relations and PCF* | 27/10/95 |
| C Talcott | *Reasoning about equivalence of higher order actor programs* | 28/10/95 |
| D Aspinall | *Subtyping dependent types* | 28/10/95 |
| L Cardelli | *Operationally sound update* | 28/10/95 |
| A Gordon | *Bisimilarity for primitive objects* | 28/10/95 |
| M Felleisen | *Modeling allocation is important* | 28/10/95 |
| I Stark | *Reasoning about state in ML* | 28/10/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| A Pitts | *Operationally-based logical relations for idealized Algol* | 28/10/95 |
| D Howe | *Adding equivalence classes to untyped lambda-calculi* | 29/10/95 |
| D Sands | *Improvement theory and its applications* | 29/10/95 |
| K Honda | *Composing processes* | 29/10/95 |
| D Sangiorgi | *Behavioural equivalences for higher-order process calculi* | 29/10/95 |
| N Yoshida | *On reduction based process semantics* | 29/10/95 |
| A Jeffrey | *Monadic types for the semantics of concurrent functional programming* | 29/10/95 |
| M Tofte | *A co-inductive proof of the soundness of region inference* | 29/10/95 |
| D MacQueen | *Higher-order modules: semantics to implementation* | 29/10/95 |
| J Tiuryn | *Untyped lambda-calculus with input-output* | 30/10/95 |
| S Smith | *The coverage of operational semantic techniques* | 30/10/95 |
| J Mitchell | *Labeling techniques and typed fixed-point operators* | 30/10/95 |
| R Harper | *Typed closure conversion* | 30/10/95 |
| C Jones | *Fixing the semantics of some concurrent object-oriented concept: SOS and proofs* | 01/11/95 |
| S K Biswas | *Dynamic slicing in higher-order program* | 03/11/95 |
| R Milner | *Introduction to action calculi* | 06/11/95 |
| P Gardner | *Representing lamdba-calculi using Milner's action calculi* | 06/11/95 |
| J Power | *A categorical view of control structures* | 06/11/95 |
| H Herbelin | *Bohm trees and games, weak head reduction and interaction between strategies* | 06/11/95 |
| F Lamarche | *The correspondence between game semantics and proof nets* | 06/11/95 |
| W Hodges | *Imperfect information and compositionality* | 07/11/95 |
| P O'Hearn | *On passivity and activity in Algol* | 07/11/95 |
| M Huth | *Finite but unbounded delay in Milner's SCCS* | 07/11/95 |
| O Jensen | *PCF and the join-calculus as action calculi* | 07/11/95 |
| V Danos | *Relating games and abstract machines* | 07/11/95 |
| L Regnier | *Reversible and irreversible computation* | 07/11/95 |
| C Stirling | *Games for modal mu-calculus and model-checking* | 08/11/95 |
| J Mitchell | *Games, linear logic and complexity* | 08/11/95 |
| A Scedrov | *Optimization problems in propositional linear Logic* | 08/11/95 |
| M Hyland | *Introduction to dialogue games and innocent strategies* | 09/11/95 |
| L Ong | *A Curr-Howard style semantics of classical proofs via lambda-mu categorical and game-semantic characterizations* | 09/11/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| P Scott | *Proofs as processes* | 09/11/95 |
| P Baillot | *AJM strategies and geometry of interaction* | 09/11/95 |
| G McCusker | *Games and full abstraction for FPC* | 09/11/95 |
| I Mackie | *Interaction nets with state* | 09/11/95 |
| V Pratt | *Games, processes and logic from the Chu perspective* | 10/11/95 |
| D Pavlovic | *Interactions and dualities* | 10/11/95 |
| H Hu | *From free lattices to free bicomplete categories* | 10/11/95 |
| S Abramsky | *Games and duality* | 10/11/95 |
| V Sassawt | *Towards a calculus of nets* | 10/11/95 |
| P Dybjer | *An introduction to reduction-free normalisation* | 15/11/95 |
| M Kegelmann | *Factorization systems on domains* | 17/11/95 |
| A Bloch | *Discrete computations and smooth Hamiltonian and gradient flows* | 20/11/95 |
| A Edalat | *Dynamical systems, measures and fractals via domain theory* | 20/11/95 |
| P Panangaden | *Formal Feynman diagrams and proof normalization in linear logic* | 20/11/95 |
| P Siwak | *Filter automata and their particles* | 20/11/95 |
| J Gunawardena | *Digital circuits and nonexpansive maps* | 20/11/95 |
| S Smale | *Blum-Shub-Smale theory* | 21/11/95 |
| M Shub | *Complexity and Bezout's theorem* | 21/11/95 |
| J Sakarovitch | *On the writing of numbers* | 21/11/95 |
| S Tsarev | *Factorization of linear ODEs: old (mathemtical) results and their modern computer echo* | 21/11/95 |
| Y Baryshnikov | *Complexity of trajectories in rectangular billiards* | 21/11/95 |
| E Goubault | *Scheduling problems and homotopy theory* | 22/11/95 |
| S Rajsbaum | *Algebraic topology and distributed computing* | 22/11/95 |
| Y Lafont | *Homological methods and word problems* | 22/11/95 |
| V Pratt | *Computational and dynamical interpretations of mathematical structures* | 22/11/95 |
| M Manthey | *Distributed computation and the twisted isomorphism* | 22/11/95 |
| M Atkinson | *The combinatorics of abstract data types* | 22/11/95 |
| U Martin | *The princess and the plumber: the role of mathematics in computer science* | 22/11/95 |
| J-Y Girard | *Geometry of proofs* | 23/11/95 |
| G Mascari | *Dynamics of computational processes* | 23/11/95 |
| J Baez | *n-categories in logic, topology and physics* | 23/11/95 |
| P Freyd | *Computer science contradicts mathematics* | 23/11/95 |
| M Sintzoff | *Invariance termination and time refinement in structured dynamical systems* | 23/11/95 |
| R Josza | *Quantum computation and Shor's factoring algorithm* | 23/11/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| P Giblin | *Recent work of Izumaya and Sano on affine differential geometry in the plane* | 24/11/95 |
| B Dubuc | *From curve complexity to perceptual grouping* | 24/11/95 |
| H Heijmans | *Theoretical aspects of morphological image processing* | 24/11/95 |
| G Sapiro | *Geometric flows: theory and applications in computer vision and image processing* | 24/11/95 |
| P Olver | *Differential invariants in computer vision* | 24/11/95 |
| B Jay | *The functorial type system* | 29/11/95 |
| J Mitchell | *Classes = objects + data abstraction* | 08/12/95 |
| A Carbone | *Some combinatorics behind proofs* | 11/12/95 |
| P-L Curien | *Abstract machines for dialogue games* | 13/12/95 |
| C Gunter | *Abstracting dependencies between software configuration items* | 14/12/95 |

*Total number of seminars within this table: 263*

## G.2 From Finite to Infinite Dimensional Dynamical Systems

| Name | Seminar Title | Date Presented |
|---|---|---|
| J Hale | *From finite to infinite* | 13/07/95 |
| L Glass | *Nonlinear dynamics of reentrant tachycardias* | 18/07/95 |
| J Hale | *From finite to infinite: Seminar II* | 20/07/95 |
| T Mestl | *Dynamics of high-dimensional piecewise-linear biological networks* | 20/07/95 |
| V Afraimovich | *Conventional multipliers for homoclinic orbits* | 24/07/95 |
| T Nowicki | *Uniform hyperbolic structure of unimodal maps* | 24/07/95 |
| D Levermore | *Multi-dimensional generalizations of subharmonic Melnikov Theorems* | 24/07/95 |
| S van Strien | *On the notion of an attractor* | 24/07/95 |
| D Rand | *Rigidity & flexibility of pseudo-Anosov & other transversally laminated surface dynamics* | 25/07/95 |
| C Sparrow | *Dynamics of non-expansive maps* | 25/07/95 |
| S Luzzatto | *Critical & singular dynamics in the Lorenz equations* | 25/07/95 |
| J Robinson | *Asymptotic equivalence of ODEs* | 25/07/95 |
| K Horsch | *Attractors for Lyapownov cases of the complex Ginzburg-Landau equation* | 25/07/95 |
| M Oliver | *Analyticity and low-dimensional behaviour of solutions to the complex Ginzburg-Landau equation* | 25/07/95 |
| Y Pesin | *Multifractal analysis of dynamical systems; physical evidence & mathematical background* | 26/07/95 |
| A Quas | *Non-ergodicity of $C^1$ expanding maps* | 26/07/95 |
| P Glendinning | *Rotational Cantor sets for unimodal maps* | 26/07/95 |
| Y Yi | *Bifurcation from non-periodic solutions of differential equations* | 27/07/95 |
| T Hall | *Dynamical implications of compact invariant sets for surface homeomorphisms* | 27/07/95 |
| H Bruin | *Unimodal maps without invariant densities* | 27/07/95 |
| D Sands | *Misiurewicz maps are rare* | 27/07/95 |
| A Pinto | *The moduli space of smooth conjugacy classes of expanding maps in one dimension* | 28/07/95 |
| D Broomhead | *$\Sigma\Delta$ modulators* | 28/07/95 |
| J Gibbon | *Introduction to the Navier Stokes equation, and estimates for attractor dimension* | 01/08/95 |
| K Ohkitani | *On two dimensional Euler and Boussinesq flows* | 01/08/95 |
| J Gibbon | *Introduction to the complex Ginzburg-Landau equation and estimate for attractor dimension* | 03/08/95 |
| P Fife | *Dynamics of phase-separation* | 03/08/95 |
| J Gibbon | *Some introductory remarks about the Euler equations* | 08/08/95 |
| V Afraimovich | *Simple solutions in lattice dynamical systems* | 10/08/95 |
| P Polacik | *Effects of positivity and symmetry on dynamics of scalar parabolic equations* | 10/08/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| CR Doering | *Energy stability and turbulent energy dissipation* | 05/09/95 |
| ES Titi | *On the minimal number of determining nodes for dissipative evolution equations* | 06/09/95 |
| JC Robinson | *Some closure results for inertial manifolds* | 06/09/95 |
| J Stark | *Invariant manifolds and the stability of recursive filters* | 06/09/95 |
| P Bates | *Persistence of normally hyperbolic invariant manifolds for semiflows in Banach spaces* | 06/09/95 |
| T Mullin | *Physically relevant symmetries in fluid flows* | 07/09/95 |
| P Lucas | *Convective flow at low temperatures* | 07/09/95 |
| G King | *Particle paths in non-axisymmetric Taylor-Couette flows* | 07/09/95 |
| P McClintock | *Zero dispersion phenomena in nonlinear oscillators* | 07/09/95 |
| J McGlade | *Dynamics of plankton* | 07/09/95 |
| G Pfister | *Routes to chaos in Taylor-Couette flow* | 07/09/95 |
| M Gaster | *Transition to turbulence in a boundary layer* | 07/09/95 |
| L Bunimovich | *Transport coefficients from first principles* | 08/09/95 |
| G Fusco | *Finite dimensional dynamics of interfaces for some models of phase separation* | 08/09/95 |
| M Proctor | *Shearing and streaming in nonlinear convection* | 08/09/95 |
| D Holm | *Hamiltonian dynamics of wave mean-flow interaction* | 08/09/95 |
| S Metens | *Morphogenesis in reaction-diffusion systems* | 08/09/95 |
| A Rucklidge | *Chaos and global bifurcations in magnetoconvection* | 08/09/95 |
| P Fife | *Models for phase transitions with nonlocal interactions, and their analysis* | 08/09/95 |
| J Hale | *Dynamics of numerics* | 11/09/95 |
| Q Tang | *Global attractors and inertial manifolds for the Ginzberg-Landau model of superconductivity* | 11/09/95 |
| A Humphries | *Upper semi-continuity of attractors under approximation by variable time stepping numerical methods* | 11/09/95 |
| C Budd | *Adaptive mesh methods for PDEs as dynamical systems* | 11/09/95 |
| M Groves | *The steady water-wave problem as a dynamical system* | 11/09/95 |
| J Mierczynski | *Strongly monotone dynamical systems with first integral* | 11/09/95 |
| M Carter | *Diffraction of reaction diffusion waves: Eikonal approximation using conformal maps* | 11/09/95 |
| M Zimmermann | *Sil'nikov saddle node interaction near a codimension 2 bifurcation: laser with injected signal* | 11/09/95 |
| J Cervero | *Ermakov systems* | 11/09/95 |
| J Sepulchre | *Static disorder in an infinite network of bistable units* | 11/09/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| N Weiss | *Spatio-temporal structures in nonlinear magnetoconvection* | 11/09/95 |
| C Elliott | *Some time dependent free boundary problems* | 12/09/95 |
| A Champneys | *New multi-modal solitary & generalised solitary waves and their connection to solitons* | 12/09/95 |
| A Sharkovsky | *Ideal turbulence: self-structuring, cascade process of coherent structures formation and self-stochasticity* | 12/09/95 |
| C Beck | *Probability densities in fully developed turbulence* | 12/09/95 |
| N Cancrini | *Rigorous results on the UV stability for the KPZ equation* | 12/09/95 |
| S Merino | *Positive periodic solutions for semilinear reaction diffusion systems on $R^N$* | 12/09/95 |
| G Mandelbaum | *Chaos in fundamental interactions* | 12/09/95 |
| M Grinfeld | *On the structure of the global attractor of the viscous Cahn-Hilliard equation in one space dimension* | 12/09/95 |
| B Buffoni | *The existence of infinitely many multi-humped solutions of the capillary-gravity wave problem* | 12/09/95 |
| E Feireisl | *On the long time behaviour of solutions to semilinear evolutionary equations on unbounded domains* | 12/09/95 |
| Y Pomeau | *Singularities in the evolution of a perfect three dimensional incompressible fluid* | 13/09/95 |
| J Elgin | *Multifractality of the Lorenz attractor* | 13/09/95 |
| D Broomhead | *Dynamical systems, time series and filters* | 13/09/95 |
| Y Yi | *Almost automorphic dynamics of differential equations* | 14/09/95 |
| D Chillingworth | *Bifurcation from a critical circle with degeneracies* | 14/09/95 |
| C Sparrow | *Bifurcations from infinity in the Falkner-Skan equation* | 14/09/95 |
| Z Zheng | *The dynamics for generic one-parameter families of maps* | 14/09/95 |
| V Rothos | *Study of 2 degree of freedom Hamiltonian systems around an elliptic fixed point in complex time* | 14/09/95 |
| S Luzzatto | *Non-uniformly hyperbolic flows* | 14/09/95 |
| M Odyniec | *Nonlinear methods in circuit design* | 14/09/95 |
| A Pinto | *Renormalisation and the moduli space for diffeomorphisms of the circle* | 14/09/95 |
| G Lythe | *Deriving ordinary stochastic differential equations from stochastic partial differential equations in a pattern formation system* | 14/09/95 |
| P Glendinning | *Creation of periodic orbits in the Nosé equations* | 14/09/95 |
| R Kerr | *The role of singularities in the Euler equations* | 15/09/95 |
| D Rand | *Constructing all Anosov surface diffeomorphisms with a smooth invariant measure* | 15/09/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| P Constantin | *Direction of vorticity* | 15/09/95 |
| G Raugel | *Long-time asymptotics of perturbed fronts for a KPP system* | 03/10/95 |
| E Spiegel | *Bifurcations with continuous spectra* | 03/10/95 |
| J Gibbon | *Small scales in the 2-D Navier-Stokes equations* | 09/10/95 |
| J Robinson | *Convergent inertial manifolds for some approximate schemes* | 09/10/95 |
| C Jones | *Nonlinear difference schemes for barotropic ocean models* | 09/10/95 |
| M Chen | *Nonlinear Galerkin method in the finite difference case: 'incremental unknown' method* | 09/10/95 |
| B Birnir | *The homogenization of the Navier-Stokes equations, and applications* | 09/10/95 |
| L Dettori | *A nonlinear Galerkin method in the collocation case* | 10/10/95 |
| I Chueshov | *Approximate inertial manifolds of exponential order for semilinear parabolic equations subject to white noise* | 10/10/95 |
| A Mahalov | *Global attractors for 3D rotating turbulence* | 10/10/95 |
| B Nicolaenko | *Inertially stable algorithms for Navier-Stokes turbulent flows* | 10/10/95 |
| B García Archilla | *AIM-postprocessed Galerkin and the nonlinear Galerkin method* | 11/10/95 |
| R Bronstering | *Some computational aspects of AIMs and finite differences* | 11/10/95 |
| M Trummer | *Some effects of space-discretization on inertial manifold computations* | 11/10/95 |
| G Nabh | *Nonlinear Galerkin methods in the finite element case* | 12/10/95 |
| A Milani | *Global existence and asymptotics for quasilinear parabolic equations* | 12/10/95 |
| G Lord | *Attractors and inertial manifolds for finite difference approximations of the complex Ginzburg-Landau equation* | 12/10/95 |
| P Fabrie | *Uniform convergence of inertial set under time discretization for a model of natural convection in porous medium* | 12/10/95 |
| M Jolly | *Computations on inertial manifolds* | 13/10/95 |
| A Doelman | *Breaking the hidden symmetry in the Ginzburg-Landau equation* | 13/10/95 |
| P Bates | *A Hartman-Grobman theorem for semiflows in Banach space* | 13/10/95 |
| G Sell | *A new approach to inertial manifolds* | 13/10/95 |
| V L'vov | *Scaling in wave turbulence with weak interaction* | 16/10/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| K Moffatt | *Cusp singularities in free surface flows* | 16/10/95 |
| P Constantin | *Scaling of structure functions in turbulence* | 17/10/95 |
| V L'vov | *Scaling in strong hydrodynamic turbulence* | 17/10/95 |
| E Spiegel | *Empirical evidence for a cascade* | 17/10/95 |
| C Doering | *Energy stability and bounds on turbulent transport* | 18/10/95 |
| J Vassilicos | *Anomolous diffusion of isolated flow singularities and of fractal or spiral structures* | 18/10/95 |
| J Dold | *Propogation of a nonlinearly anti-diffusive combustion interface* | 19/10/95 |
| I Procaccia | *Interface growth and analytic methods: example of flame propogation* | 19/10/95 |
| Y Pomeau | *Scaling in decaying weak turbulence* | 19/10/95 |
| G Bellettini | *Fattening for forced mean curvature flow in 2D* | 20/10/95 |
| P Bates | *Interfacial dynamics for generalized phase-field systems* | 23/10/95 |
| C Beck | *Coupled map lattices simulating quantum field theories* | 23/10/95 |
| J Carr | *Coarsening dynamics* | 23/10/95 |
| C Elliott | *Numerical solution of interface motion via phase field equations* | 23/10/95 |
| Y Pomeau | *Crumpled paper* | 24/10/95 |
| W Pesch | *Complex spatio-temporal patterns in Rayleigh-Benard convection* | 24/10/95 |
| P Coullet | *Bifurcation of excitable waves and their collisions properties* | 24/10/95 |
| W van Saarloos | *Streamers in dielectric breakdown as a pattern formation problem* | 24/10/95 |
| G Fusco | *Nucleation in the context of the Cahn-Hilliard equation: existence of multi-spike stationary solutons* | 24/10/95 |
| E Meron | *Front transitions, spiral-vortex nucleation and complex patterns* | 25/10/95 |
| J Ockendon | *Phenomonology of vortices and dislocations* | 25/10/95 |
| J Hale | *Synchronization through diffusivity* | 26/10/95 |
| A Carvalho | *Localized large diffusion in reaction diffusion problems* | 26/10/95 |
| W Shen | *Travelling waves in lattice dynamical systems* | 26/10/95 |
| M Herrero | *Singularity formation in a chemotaxis model* | 26/10/95 |
| H Chate | *Non-trivial collective behaviour in extensively chaotic dynamical systems* | 27/10/95 |
| E Presutti | *Metastable phenomena in Ising systems with Kac potentials* | 27/10/95 |
| A Newell | *Defects are self-dual solutions of the regularized Cross-Newell phase diffusion equation* | 27/10/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| J Mallet-Paret | *Pattern formtion, spatial chaos, and traveling waves in lattics differential equations* | 27/10/95 |
| B Fiedler | *Meandering spirals* | 30/10/95 |
| W Oliva | *Formation of symmetries in systems of repelling particles* | 30/10/95 |
| M Silber | *Hopf bifurcation to three-tori in a problem with symmetry* | 30/10/95 |
| R Lauterbach | *Symmetry-breaking perturbations for periodic solutions* | 30/10/95 |
| M Golubitsky | *Symmetry detectives* | 31/10/95 |
| J Lamb | *Symmetric omega-limit sets in reversible flows* | 31/10/95 |
| D Armbruster | *Dynamics of cellular flames* | 31/10/95 |
| I Melbourne | *Steady-state bifurcation with Euclidean symmetry: rigour and universality in the Ginzburg-Landau equation* | 31/10/95 |
| K Gatermann | *Recursive detectives* | 31/10/95 |
| P Ashwin | *Attractors for dynamics with invariant subspaces* | 31/10/95 |
| S Robertson | *Symmetry types of convex bodies* | 31/10/95 |
| M Field | *Cycling chaos* | 01/11/95 |
| J Furter | *Singularity theory and forced symmetry-breaking* | 01/11/95 |
| A P Dias | *Instant chaos is chaos in slow motion* | 01/11/95 |
| C Leis | *Hopf bifurcation with spherical symmetry: invariant tori and connecting orbits* | 01/11/95 |
| P Chossat | *Symmetry-breaking dynamics from the orbit-space point of view* | 02/11/95 |
| A Rucklidge | *Heteroclinic cycles between chaotic sets; two examples from models of 3-dimensional convection* | 02/11/95 |
| S Maier-Paape | *Hexagonal and rectangular patterns for the Cahn-Hilliard equation* | 02/11/95 |
| J Brooke | *Spatial symmetry-breaking via an intermittency mechanism* | 02/11/95 |
| E Feireisl | *Attractors for some nonlinear wave equations on unbounded domains* | 02/11/95 |
| E Knobloch | *Turing instability in three dimensions* | 02/11/95 |
| I Stewart | *Speculations on speciation* | 03/11/95 |
| P Aston | *Classification of steady state/steady state mode interactions* | 03/11/95 |
| D Armbruster | *Dynamics of cellular flames* | 03/11/95 |
| I Hoveijn | *Versal deformations and normal forms for reversible & Hamiltonian linear systems* | 03/11/95 |
| T Bridges | *Instability of toral patterns* | 03/11/95 |
| J Hale | *From finite to infinite dimensional dynamical systems* | 11/11/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| J Gibbon | *Attractors for the Navier-Stokes equations* | 11/11/95 |
| E Titi | *Inertial manifolds and degrees of freedom for dissipative systems* | 11/11/95 |
| P Constantin | *The Euler and Navier-Stokes equations* | 11/11/95 |
| PJ McKenna | *Periodic and travelling waves in a nonlinearly suspended beam* | 16/11/95 |
| F Zanolin | *Periodic solutions of piecewise linear ODEs* | 16/11/95 |
| JA Sherratt | *Piecewise linear models in mathematical biology* | 16/11/95 |
| GW Desch | *Elastic and viscoelastic rods* | 16/11/95 |
| U an der Heiden | *Piecewise linear delay differential equations* | 16/11/95 |
| CJ Budd | *Piecewise linear PDEs arising from quantum and other effects in nonlinear electrostatics* | 17/11/95 |
| WA Green | *Wave propagation in layered solids* | 17/11/95 |
| SJ Hogan | *Piecewise Linear DEs: Closing Discussion* | 17/11/95 |
| L Floria | *Josephson junction ladder; a benchmark for nonlinear concepts* | 24/11/95 |
| L Segel | *From verbal to mathematical theories in immunology* | 27/11/95 |
| A McLean | *Competition amongst lymphocytes* | 27/11/95 |
| M Kaufman | *Toxicity and neuroendocrine regulation of the immune response* | 27/11/95 |
| S Gupta | *The maintenance of strain structure in recombining infectious agents* | 27/11/95 |
| C Bangham | *Immunological control of a persistent virus infection (HTLV1)* | 27/11/95 |
| M Nowak | *Viral dynamics and immune responses* | 28/11/95 |
| A Perelson | *Modeling HIV-1 dynamics in vivo* | 28/11/95 |
| E Szathmary | *AIDS progression as a problem in 'ecology* | 28/11/95 |
| R de Boer | *Is HIV-1 a predator, a prey, or both?* | 28/11/95 |
| S Bonhoeffer | *HIV and HBV dynamics in vivo* | 28/11/95 |
| M Kerszberg | *Putting molecular flesh on the theoretical backbone: the case of Morphogen gradient interpretation* | 29/11/95 |
| L Wolpert | *Pattern formation in limb development* | 29/11/95 |
| J Sherratt | *Mathematics as a tool for studying developmental patterns* | 29/11/95 |
| J Lewis | *Delta-Notch signalling, lateral inhibition and the genesis of fine-grained pattern* | 29/11/95 |
| E Szathmary | *The origin of the genetic code: no longer 'notoriously difficult'?* | 29/11/95 |
| B Grenfell | *Measles: The movie* | 30/11/95 |
| D Rand | *Fluctuation driven dynamics. Infection, diversity and persistence* | 30/11/95 |
| J Brindley | *Mathematical models of plankton dynamics* | 30/11/95 |
| H Metz | *The potential for evolution towards stability in simple population dynamics* | 30/11/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| Y Nishiura | *Turing patterns and micro-structures* | 01/12/95 |
| CT Elliott | *Numerical solution of a mean field model in superconductivity coupling a hyperbolic equation to an elliptic equation* | 04/12/95 |
| PK Jimack | *Stability of the moving finite element for a class of parabolic partial differential equations* | 04/12/95 |
| M Berzins | *Spatio-temporal error control for time-dependent PDEs* | 04/12/95 |
| J Norbury | *Some math problems in weather prediction* | 04/12/95 |
| AT Hill | *The inheritance of dissipativity by linear multistep and Runge-Kutta methods* | 04/12/95 |
| M Baines | *Multidimensional upwinding and grid adaption* | 05/12/95 |
| E Suli | *Posteriori error analysis and adaptivity for time-dependant problems* | 05/12/95 |
| J Butcher | *Runge-Kutta methods: a century of accurate computations* | 05/12/95 |
| RW Wright | *Continuation for singularly perturbed two-point boundary value problems* | 05/12/95 |
| DR Moore | *Accurate interpolants for the solutions of ODE systems* | 05/12/95 |
| P Metzner | *Oscillatory patterns in rapid directional solidification* | 06/12/95 |
| A Skeldon | *Super hexagons and twisted squares: some new stability results for spatially periodic patterns* | 06/12/95 |
| SP Decent | *Sideband instability and modulations of Faraday waves* | 06/12/95 |
| RB Hoyle | *Fronts between different wavenumber states in a non-variational Ginzburg-Landau equation* | 06/12/95 |
| H Herrero | *Fronts between hexagons and squares in a generalized Swift-Hohenberg equation* | 06/12/95 |
| A Mancho | *Bifurcation in a six dimensional model for the Kuramoto-Sivashinsky equation* | 06/12/95 |
| S Cox | *Long-wave models for anisotropic convection in Langmuir circulation* | 06/12/95 |
| J Elgin | *Multi-fractal formalism for ODEs and PDEs* | 06/12/95 |
| M Lücke | *Convection in binary gas mixtures: pattern selection as a nonlinear eigenvalue problem* | 06/12/95 |
| P Drazin | *Low order behaviour of the Proudman-Johnson equation* | 06/12/95 |
| F Busse | *New steady convection patterns in fluid layers heated from below* | 06/12/95 |
| E Knobloch | *Linear and nonlinear dynamo waves* | 07/12/95 |
| SM Tobias | *Low-order models and PDE simulations of the nonlinear solar dynamo* | 07/12/95 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| DW Hughes | *The suppression of chaos in nolinear dynamo models* | 07/12/95 |
| N Seehafer | *Bifurcations in a magnetofluid with helical forcing* | 07/12/95 |
| G Sarson | *Mean-field dynamo models under imposed boundary heterogeneities* | 07/12/95 |
| MR Proctor | *Subcritical squares and $\sqrt{2}$:1 resonance* | 07/12/95 |
| A Pumir | *Bursts of energy and enstrophy in homogeneous turbulent shear flows* | 07/12/95 |
| A Craik | *Second-harmonic resonance of capillary-gravity waves with Faraday excitation: properties of truncated equations* | 07/12/95 |
| NO Weiss | *Looping the loop in thermosolutal convection* | 07/12/95 |
| J Kurths | *Generalized entropies in a turbulent dynamo simulation* | 07/12/95 |
| T Mullin | *Convection in molten gallium* | 07/12/95 |
| AM Rucklidge | *Global bifurcations in three-dimensional convection* | 08/12/95 |
| B Malomed | *Anomalous dynamical chaos in a system of truncated Euler equations* | 08/12/95 |
| J Massaguer | *Bands of instability in two dimensional thermal convection* | 08/12/95 |
| J Elezgaray | *The Kuramoto-Sivashinsky equation: statistics of the large scales and models of the local dynamics* | 08/12/95 |
| P Manneville | *Phase turbulence in the two-dimensional complex Ginzburg-Landau equation* | 08/12/95 |
| E Spiegel | *Patterns of propagating pulses* | 08/12/95 |

*Total number of seminars within this table: 294*

## G.3 Dynamics of Complex Fluids

| Name | Seminar Title | Date Presented |
|---|---|---|
| G McKinley | *Unresolved problems in the complex flow of dilute polymer solutions* | 08/01/96 |
| D James | *Entanglements in dilute polymer solutions* | 08/01/96 |
| B Van den Brule | *Phenomena observed in particle settling in non-Newtonian media* | 08/01/96 |
| J Nieuwkoop | *Extensinal-flow experiments using a new extensional-flow device* | 08/01/96 |
| G Homsy | *Some unsolved problems in th flow of elastic liquids* | 09/01/96 |
| L Woodcock | *Why do Brazil nuts come to the top; the equipartition principle and the flow of granular materials* | 09/01/96 |
| J Ferguson | *Measurement and interpretation on non-equilibrium extensional flow* | 09/01/96 |
| L Leal | *Experimental results for polymeric solutions in mixed-type flows, and comparisons to model predictions* | 09/01/96 |
| T Sridhar | *Stress relaxation in extensional flows* | 09/01/96 |
| M Renardy | *On the mechanism of drag reduction* | 09/01/96 |
| A Keller | *A singularity in the melt flow of polyethylene with wider implications for polymer melt rheology* | 09/01/96 |
| M Denn | *Problems in polymer-melt extrusion* | 10/01/96 |
| J Meissner | *Open problems in polymer melt shear flows* | 10/01/96 |
| J Higgins | *Interactions of rheology with thermodynaics - effects of flow on polymer-polymer miscibility* | 10/01/96 |
| M Wagner | *Elongational viscosity of polymer melts measured at constant strain rate, constant stress and constant force* | 10/01/96 |
| M Mackley | *Slippery fluids and plastic flow* | 11/01/96 |
| F Baaijens | *Failures in predicting stress and velocity fields for the flow around a confined cylinder* | 11/01/96 |
| A Ryan | *Rhelogy of crosslinking polymerisations* | 11/01/96 |
| W Poon | *Viscosity and structural relaxation in concentrated hard-sphere colloids* | 11/01/96 |
| R Richards | *Surface and viscoelasticity of polymers at the air-water interface* | 11/01/96 |
| C Petrie | *Mathematical problems associated with the dynamics of complex fluids* | 11/01/96 |
| Y Renardy | *Spurt and instability in a two-layer Johnson-Segalman liquid* | 11/01/96 |
| D Durand | *An unresolved problem in the dynamics of complex fluids* | 11/01/96 |
| H Winter | *Time resolved rheometry* | 11/01/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| F Leslie | *Unresolved aspect of flow f nematic liquid crystals* | 12/01/96 |
| A Windle | *Banded structures and related microstructures in sheared LCPs* | 12/01/96 |
| H Fishcer | *Banded structures and LCPs* | 12/01/96 |
| R Larson | *Director tumbling inliquied crystalline polymers* | 12/01/96 |
| P Goldbart | *Dynamical problems in networks* | 17/01/96 |
| G McKinley | *Free-surface effects in filament stretching flows* | 25/01/96 |
| C Petrie | *Logistics of rheological constitutive models I* | 25/01/96 |
| C Petrie | *Simple ideas for complex fluids* | 25/01/96 |
| TCB McLeish | *Constitutive equations for branched polymers* | 30/01/96 |
| O Harlen | *Follow-up/new results on kinematics of filament stretching devices* | 01/02/96 |
| M Wagner | *Single integral constitutive equations for polymer melts* | 02/02/96 |
| M Renardy | *Classifications of instabilities in complex fluid flows* | 06/02/96 |
| ME Cates | *Onions/surfactants and other topics?* | 07/02/96 |
| M Wagner | *The rheotens experiment: Do rheologists understand fibre spinning?* | 08/02/96 |
| M Renardy | *Classifications of instabilities in complex fluid flows continuation* | 08/02/96 |
| J Brady | *Colloids under stress* | 09/02/96 |
| J Brady | *Viscous response in concentrated colloidal systems* | 13/02/96 |
| PD Olmsted | *A model for non-equilibrium transitions in nematic liquid crystals under shear* | 15/02/96 |
| R Larson | *Molecular modeling and simulation of semi-flexible chains* | 20/02/96 |
| V Entov | *Cohesive fracture and yield phenomena in a fluid* | 22/02/96 |
| EJ Hinch | *Dynamical consequences of a relaxation time spectrum* | 27/02/96 |
| S Shianovskii | *Spontanaous and induced chirality of nematic with flexible molecules* | 28/02/96 |
| V Entov | *Fracture-related topics* | 29/02/96 |
| P Coveney | *Domain growth and surface tension in 2d binary immiscible fluids* | 05/03/96 |
| E Boek | *Simulating the rheology of dense colloidal systems using DPD* | 05/03/96 |
| A Schlijper | *Simulation of polymers in solution* | 05/03/96 |
| C Marsh | *Theoretical aspects of DPD* | 05/03/96 |
| P Warren | *Dissipative continua* | 05/03/96 |
| R Larson | *Videotapes of single DNA molecule stretching* | 07/03/96 |
| G Capaccio | *Rheology round table with BP* | 08/03/96 |
| W Poon | *Metastability and gelation in colloid polymer mixtures* | 08/03/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| T Witten | *Simulations of entanglements in polymer melts - consequences for double reptation* | 12/03/96 |
| T Witten | *Physics of coffee stains* | 13/03/96 |
| J Rallison | *Lubricaton theory for a fibre suspension* | 14/03/96 |
| J Hinch | *Instability of a high-speed submerged elastic jet* | 14/03/96 |
| H Winter | *Time-resolved rheometry, possibilities and limitations* | 14/03/96 |
| R Keunings | *Simulation of polymer flows with kinetic theory models* | 14/03/96 |
| M Johnson | *Lubrication of piston rings with Newtonian oils* | 14/03/96 |
| G Maitland | *The life history of a filtercake, and other stories* | 14/03/96 |
| J Sherwood | *Friction between a drillstring and a bentonite filter cake* | 14/03/96 |
| G Astarita | *Thermodynamics of granular media* | 14/03/96 |
| J Benbow | *Effects of liquid phase rheology on particulate paste properties and the need for a predictive theory of surface defects* | 14/03/96 |
| C Petrie | *A theology of complex fluids* | 14/03/96 |
| A Pearson | *A note on the rheotens experiment* | 14/03/96 |
| I Hamley | *Rheology of cubic phases* | 15/03/96 |
| G Leal | *Leal's Swansong (in 3 movements); observations on entangled polymer solutions, conc. suspensions and maybe Doi models for LCPs* | 19/03/96 |
| M Wagner | *Double step strain deformations and molecular dynamics of polymer melts* | 21/03/96 |
| J Davenport | *Proofs and certificates of polynomial irreducibility* | 22/03/96 |
| S Edwards | *The challenge of theories of dynamics* | 25/03/96 |
| J Candau | *Experimental windows onto dynamics* | 25/03/96 |
| M Rubinstein | *Polymers: the nature of entanglements* | 25/03/96 |
| M Rubinstein | *Linear chains - reptation and fluctuation* | 25/03/96 |
| P Pusey | *Experimental challenges in colloids* | 26/03/96 |
| J Brady | *Introduction to theory of colloidal dynamics I* | 26/03/96 |
| T McLeish | *Polymers: effect of complex topologies* | 26/03/96 |
| M Rubenstein | *Polymers: theories of constraint release* | 26/03/96 |
| T McLeish | *Polymers: nonlinear response* | 27/03/96 |
| A Semenov | *Polymers: concentration fluctuations I* | 27/03/96 |
| J-F Berret | *Rheology of micelles* | 27/03/96 |
| P Callaghan | *NMR microscopic flow imaging* | 27/03/96 |
| G Floudas | *Microphase separation in nonlinear block copolymers* | 27/03/96 |
| J Goveas | *Dynamics of the lamellar-cylindrical transition in block-copolymer melts* | 27/03/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| R Lahiri | *Nonequilibrum phase transitions in sheared colloids* | 27/03/96 |
| N Spenley | *Theory of shear banding* | 27/03/96 |
| M Evans | *LC phases and defects on genus 1 and 2 surfaces (mostly 1)* | 27/03/96 |
| M Zapotocky | *Phase ordering and disclination dynamics in nematics* | 27/03/96 |
| J Palierne | *Rheology of complex fluids at acoustic frequencies* | 27/03/96 |
| A Semenov | *Polymers: concentration fluctuations II* | 28/03/96 |
| S Ramaswamy | *Self-consistant fields in colloidal dynamics I* | 28/03/96 |
| J Brady | *Introduction to theory of colloidal dynamics II* | 28/03/96 |
| S Ramaswamy | *Self-consistent fields in colloidal dynamics II* | 28/03/96 |
| J Brady | *Colloids: simulation and scaling results* | 29/03/96 |
| S Ramaswamy | *Anomalons dissipation dense emulsions* | 29/03/96 |
| J Candau | *Surfactant complex fluids and worms* | 29/03/96 |
| M Cates | *Linear dynamics of wormlike surfactants* | 29/03/96 |
| M Cates | *Wormlike surfactants - nonlinear dynamics* | 30/03/96 |
| F Lequeux | *Mechanical properties of foams* | 30/03/96 |
| C Toprakcioglu | *Surfactant cubic phases* | 30/03/96 |
| G Marrucci | *Rheology of polymer liquid crystals I* | 01/04/96 |
| M Doi | *Dynamics of domains and textures I* | 01/04/96 |
| S Milner | *Polymers: shear and phase transitions I* | 01/04/96 |
| G Fredrickson | *Block co-polymers - introduction* | 01/04/96 |
| G Marrucci | *Rheology of polymer liquid crystals II* | 02/04/96 |
| M Doi | *Dynamics of domains and textures II* | 02/04/96 |
| G Fredrickson | *Block co-polymers - shear effects* | 02/04/96 |
| S Milner | *Polymers: shear and phase transitions II* | 02/04/96 |
| R Larson | *Shear and transition in liquid crystals I* | 03/04/96 |
| D Roux | *Shear and phase diagram of surfactants I* | 03/04/96 |
| R Larson | *Shear and transition in liquid crystals II* | 03/04/96 |
| D Roux | *Shear and phase diagram of surfactants II* | 03/04/96 |
| M Cates | *Viscoelasticity of smectic dispersions* | 04/04/96 |
| D Roux | *Shear and phase diagram of surfactants* | 04/04/96 |
| G Fredrickson | *Flow-modification of diffusion-reactions* | 04/04/96 |
| DD Joseph | *Steep wave front on extrudates* | 15/04/96 |
| VM Entov | *One dimensional dynamics of jet or spin-line flows* | 15/04/96 |
| DF James | *Constitutive models for dilute polymer solutions* | 15/04/96 |
| PS Hammond | *Continuum models for high Reynolds number liquid-liquid flows* | 15/04/96 |
| JM Rallison | *Dissipative stresses in polymer solutions* | 16/04/96 |
| A Nadim | *A hydrodynamic approach to the rheology of polymeric solutions modelled as dumbbells in time-periodic shear flow* | 16/04/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| MH Wagner | *Shear followed by elongational flow: constitutive equations for melt spinning* | 16/04/96 |
| RI Tanner | *The variations on and durability of single-integral models for fluids and soft solids* | 16/04/96 |
| E Beris | *Dynamics of liquid crystals* | 16/04/96 |
| JF Brady | *Modelling viscous suspension flows* | 16/04/96 |
| CJS Petrie | *Simple initial - and boundary - value problems; the way their structure is affected by choice of constitutive equation* | 16/04/96 |
| E Shaqfeh | *Using Brownian dynamics to develop constitutive equations: Brownian vs viscous stresses in transient linear flows* | 16/04/96 |
| AR Davies | *Viscoelastic boundary layers in Oldroyd-type models* | 17/04/96 |
| Y Renardy | *Hopf-Hopf and steady Hopf mode interactions in Taylor-Couette flow of an upper convected Maxwell liquid* | 17/04/96 |
| JD Goddard | *Material instabilities in fluid particle suspensions* | 17/04/96 |
| M Renardy | *Asymptotic evolution and break-up of Newtonian and viscoelastic jets* | 17/04/96 |
| JD Sherwood | *Squeeze-film rheometry of rigid-plastic material* | 18/04/96 |
| D Pissarenko | *Statistical models of velocity-dependent friction* | 18/04/96 |
| Y Shikhmurzaev | *Pardoxes in mathematical modelling of viscous flows and the problem of universal boundary conditions* | 18/04/96 |
| A Nadim | *The role of surfactants and surface rheology in determining the rheological properties of dilute emulsions* | 18/04/96 |
| RG Larson | *Film models for the elasticity of foams and emulsions* | 18/04/96 |
| E Shaqfeh | *Modelling the rheology of tethered layers by Brownian dynamics* | 18/04/96 |
| GM Homsy | *Viscoelastic free-boundary problems* | 18/04/96 |
| A Beris | *Surface effects on the rheology and conformation of polymer solutions* | 18/04/96 |
| FTP Baaijens | *Evaluation of constitutive models in complex flows* | 19/04/96 |
| R Keunings | *Micro-macro simulations of polymeric solutions* | 19/04/96 |
| OG Harlen | *Calculations of transient viscoelastic flows using Langrangian methods* | 19/04/96 |
| P Szabo | *Viscoelastic flow through axisymmetric and planar orifices* | 19/04/96 |
| RI Tanner | *Lessons from turbulent computations - the use of finite-volume models in viscoelastic flows* | 19/04/96 |
| AL Yarin | *Impact of drops on solid surfaces - capillary and shock waves* | 23/04/96 |
| S Milner | *Theories for self-dilute additives in polymer melts - theory of branched polymer additives in polymer melt rheology* | 25/04/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| G Fuller | *The fluid dynamics and structure of Langmuir monolayers* | 29/04/96 |
| D Long | *Simultaneous action of electric fields and nonelectric forces on a polyelectrolyte: motion and deformation* | 30/04/96 |
| V Entov | *Flow of foams through porous media* | 02/05/96 |
| TCB McLeish | *Introduction to rheology/chain structures in polymers workshop* | 14/05/96 |
| WW Graessley | *Molecular aspects of polymer rheology* | 14/05/96 |
| HM Laun | *Analytical rheology of polymer melts in industry - a dream?* | 14/05/96 |
| EL Heino | *The use of rheology in polymer development* | 14/05/96 |
| M Wagner | *Long chain branching, polydispersity and drawability* | 14/05/96 |
| E Lucchelli | *Investigation of induced branching through rheometry* | 14/05/96 |
| D Dobraszczyk | *Strain hardening of doughs in biaxial extension* | 14/05/96 |
| S Cobianco | *Low temperature rheology of synthetic lubricants* | 14/05/96 |
| P Ehricke | *The irreversibility assumption for models of polmer melts* | 14/05/96 |
| R Koopmans | *Rheology of tailormade polyolefin resins* | 14/05/96 |
| R Wimberger-Friedl | *Chain stiffness of copolycarbonates* | 14/05/96 |
| PG de Gennes | *Dynamics of muscle fibres* | 14/05/96 |
| M Van Gurp | *Rheology of hyperbranched polyesters* | 15/05/96 |
| TCB McLeish | *Molecular rheology of specific branched structures* | 15/05/96 |
| R Larson | *Reconciling shear and extensional reheology of branched polymers* | 15/05/96 |
| D Mead | *Analytical scaling of the double reptation mixing rule* | 15/05/96 |
| T Borg | *Rheology calculations and linear polymer viscoelasticity* | 15/05/96 |
| M Kroger | *Microscopic models of nonequilibrium polymer fluids* | 15/05/96 |
| PG de Gennes | *Josephson droplets* | 16/05/96 |
| N Clarke | *An approach to early-stage effects of viscoelasticity in spinodal decomposition of polymer blends* | 21/05/96 |
| M Renardy | *Imposing 'No' boundary conditions at outflow - why it works* | 23/05/96 |
| D Gollmann | *Attacking attacks* | 24/05/96 |
| D Wheeler | *A better protocol* | 24/05/96 |
| Y Renardy | *Snakes and corkscrew waves in core-annular flows* | 28/05/96 |
| GH McKinley | *Sedimentation of spheres in conc. polymer solutions: transient oscillations, negative wakes and elastic recoil* | 30/05/96 |
| A Kraynik | *The microrheology of foams and emulsions* | 03/06/96 |
| P Solis | *Torsional modes of polymers* | 04/06/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| D Lu | *Dielectric response of bilayer vesicles* | 04/06/96 |
| B Andersson | *Structure-rheology relations in branched polymers* | 12/06/96 |
| L Hilliou | *Mechanical properties of side chain liquid crystal polymers and elastomers* | 13/06/96 |
| DF James | *Viscoelasticity of associated polymers* | 19/06/96 |
| A Rozhkov | *Experiments with microjets of polymer solutions* | 20/06/96 |

*Total number of seminars within this table: 183*

## G.4 Computer Security, Cryptology and Coding Theory

| Name | Seminar Title | Date Presented |
|---|---|---|
| R Pellikaan | *Algebraic geometry codes without algebraic geometry* | 09/01/96 |
| H Stichtenoth | *Some interesting curves* | 09/01/96 |
| T Hoeholdt | *Decoding algebraic geometry codes* | 09/01/96 |
| H Niederreiter | *Cyclotomic function fields, codes and low discrepancy sequences* | 11/01/96 |
| C Xing | *Drinfeld modules and algebraic curves with many rational points* | 11/01/96 |
| J Wolper | *Codes from Schubert varieties* | 11/01/96 |
| A Campillo | *Weierstrass semigroups from singular models* | 11/01/96 |
| T Hoeholdt | *Decoding algebraic geometry codes* | 16/01/96 |
| T Helleseth | *Exponential sums over Galois rings and applications to sequences and codes over* $z_4$ | 16/01/96 |
| V Job | *Codes from Fourier and Wavelet Transforms* | 16/01/96 |
| D MacKay | *Good error-correcting codes based on very sparse matrices* | 16/01/96 |
| B McEliece | *Turbo codes - an introduction* | 23/01/96 |
| J Golic | *Decoding beyond the minimum distance - fast correlation attacks* | 23/01/96 |
| M de Boer | *Codes spanned by quadratic and Hermitian forms* | 23/01/96 |
| K-H Zimmermann | *On Hecke modules of type A as linear codes* | 23/01/96 |
| O Moreno | *Exponential sums and applications: an overview of a new book* | 26/01/96 |
| S Maric | *1- and 2-dimensional correlation properties of various families of algebraically designed sequences* | 30/01/96 |
| T Johansson | *Relations between error correcting codes authentication codes, and universal hashing* | 30/01/96 |
| J Golic | *Asymptotic secret sharing* | 06/02/96 |
| T Jokobsen | *Correlation attacks on block ciphers* | 13/02/96 |
| M Matsui | *On duality between differential and linear cryptanalysis* | 13/02/96 |
| B Preneel | *New attacks and constructions for MACs* | 13/02/96 |
| L Knudsen | *Cryptanalysis of RC5* | 20/02/96 |
| J Golic | *On correlation attacks on stop/go cascades (joint with R. Menicocci)* | 20/02/96 |
| X Lai | *Attacks on the HKM/HFX cryptosystem* | 21/02/96 |
| L Knudsen | *Truncated differentials of SAFER* | 21/02/96 |
| S Murphy | *The PHT of SAFER* | 21/02/96 |
| S Vaudenay | *On the weak keys of Blowfish* | 21/02/96 |
| M Blaze | *High-bandwidth encryption with low-bandwidth smartcards* | 21/02/96 |
| B Jenkins | *ISAAC* | 21/02/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| W Geiselmann | *A note on the hash function of Tillich and Zémor* | 22/02/96 |
| H Dobbertin | *Cryptanalysis of MD4* | 22/02/96 |
| H Dobbertin | *RIPEMD-160: A strengthened version of RIPEMD* | 22/02/96 |
| K Nyberg | *Fast accumulated hashing* | 22/02/96 |
| R Anderson | *Tiger: a new hash function* | 22/02/96 |
| V Rijmen | *The cipher SHARK* | 22/02/96 |
| R Anderson | *Two practical and provably secure block ciphers: BEAR and LION* | 22/02/96 |
| B Schneier | *Unbalanced Feistel networks and block cipher design* | 22/02/96 |
| A Clark | *A comparison of fast correlation attacks* | 23/02/96 |
| W Penzhorn | *Correlation attacks on stream ciphers: Computing low-weight parity checks based on error-correcting codes* | 23/02/96 |
| J Golic | *On the security of nonlinear filter generators* | 23/02/96 |
| S Lucks | *Faster Luby-Rackoff ciphers* | 23/02/96 |
| M Matsui | *New structure of block ciphers with provable security against differential and linear cryptanalysis* | 23/02/96 |
| W Diffie | *The committee to get RC4* | 26/02/96 |
| J Massey | *Generalised DFT and linear complexity* | 27/02/96 |
| G Simmons | *Qualified set identification in an RSA-like setting* | 27/02/96 |
| I Damgaard | *Linear zero-knowledge - A note on efficient zero-knowledge proofs and arguments* | 28/02/96 |
| M Yung | *The dark side of 'black-box' cryptography* | 01/03/96 |
| B Schneier | *Related key cryptanalysis: applications and results* | 05/03/96 |
| A Klapper | *Existence results for families of secure feedback registers* | 05/03/96 |
| M Dichtl | *Some remarks on key dependent S-boxes* | 08/03/96 |
| B Kaliski | *A chosen message attack on Demytko's cryptosystem* | 12/03/96 |
| C Schnorr | *Security and efficiency of $2^t$ root identification and signatures* | 12/03/96 |
| C Pomerance | *Multiplication independance for random integers* | 19/03/96 |
| P Landrock | *Squares and factors* | 19/03/96 |
| F Morain | *State of the art of point-counting on elliptic curves over finite fields* | 22/03/96 |
| J Stern | *Security proofs for signature schemes* | 26/03/96 |
| U Maurer | *Diffie-Hellman oracles and the discrete log problem* | 26/03/96 |
| B Kaliski | *Timing attacks* | 29/03/96 |
| W Mao | *A pragmatic off-line electronic cash technique for the internet* | 02/04/96 |
| T Matsumoto | *Human-computer cryptography* | 09/04/96 |
| C Schnorr | *Lattice-reduction and factorisation - a survey* | 09/04/96 |
| R Needham | *Keynote address* | 10/04/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| W Mao | *A proposed revision to two internet payment protocols* | 10/04/96 |
| P Landrock | *A new realisation of negotiable instruments* | 10/04/96 |
| B Crispo | *Untrusted third parties* | 10/04/96 |
| E Fujisaki | *Practical escrow cash systems* | 10/04/96 |
| R Anderson | *A practical electronic cash system* | 10/04/96 |
| T Pedersen | *Electronic payments of small amounts* | 10/04/96 |
| A Shamir | *Keynote address* | 10/04/96 |
| M Joyce | *Protocol failures for RSA-like functions using Lucas sequences and elliptic curves* | 11/04/96 |
| R Cramer | *Efficient and provable security amplifications* | 11/04/96 |
| A Yasinsac | *Evaluating cryptographic protocols* | 11/04/96 |
| B Morris | *Keynote address* | 11/04/96 |
| M Burmester | *Efficient and secure conference key distribution* | 11/04/96 |
| P Joong Lee | *Directed signatures and application to threshold cryptosystems* | 11/04/96 |
| P Rogaway | *Provably secure session key distribution* | 11/04/96 |
| A Yasinsac | *Evaluating cryptographic protocols* | 11/04/96 |
| L Chen | *A key escrow system in mutually mistrusting domains* | 12/04/96 |
| J Kelsey | *Automatic event-stream notarization using digital signatures* | 12/04/96 |
| W Harbison | *Why isn't trust transitive* | 12/04/96 |
| S Chuang | *Security in ATM networks* | 12/04/96 |
| T Okamoto | *The relationship between statistical zero knowledge proofs* | 16/04/96 |
| M Naor | *Digital signets - self-enforcing protection of digital content* | 16/04/96 |
| J McLean | *Secure composition: An application area for formal methods* | 23/04/96 |
| B Pfitzmann | *Cryptographic semantics of formal specifications* | 23/04/96 |
| A Gordon | *Introduction to pi calculus* | 23/04/96 |
| M Abadi | *Pi calculus and cryptography* | 23/04/96 |
| K Wagner | *The authentication logics project at Cambridge* | 23/04/96 |
| R Yahalom | *Formal analysis of electronic payment protocols: some challenges and opportunities* | 23/04/96 |
| V Kessler | *On authentication logics* | 23/04/96 |
| R Kemmerer | *Animated formal specifications for cryptographic protocol analysis* | 23/04/96 |
| M Staples | *Implementing the Clark-Wilson security policy model in SML* | 23/04/96 |
| P Curzon | *Hardware verification and ATM switches* | 23/04/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| P Wayner | *Strong theoretical steganography: grammars, text and intractability* | 26/04/96 |
| M Blaze | *Decentralised trust management* | 26/04/96 |
| R Anderson | *A security policy model for clinical information systems* | 30/04/96 |
| R Morris | *Protocol failures* | 30/04/96 |
| R Safavi-Naini | *Authentication systems with shared generation of authenticators* | 30/04/96 |
| P Ryan | *Advances in the CSP/FDR approach to analysing security protocols* | 01/05/96 |
| P Nikander | *Building authorisation on the top of IPSEC* | 07/05/96 |
| J Gordon | *How to steal a car* | 07/05/96 |
| C Meadows | *A language for the specification of cryptographic protocols* | 21/05/96 |
| KY Lam | *What the banks want* | 28/05/96 |
| R Pinch | *On-line multiple secret sharing* | 28/05/96 |
| D Kahn | *The history of steganography* | 30/05/96 |
| E Franz | *Computer based steganography* | 30/05/96 |
| T Handel | *Hiding data in the OSI network model* | 30/05/96 |
| R Anderson | *Redefining the limits of steganography* | 30/05/96 |
| B Pfitzmann | *Trials of traced traitors* | 30/05/96 |
| Y Desmedt | *Establishing Big Brother using cover channels and other techniques* | 30/05/96 |
| C Meadows | *Covert channels - a context based view* | 30/05/96 |
| M Anderson | *Covert channel analysis for stubs* | 30/05/96 |
| D Aucsmith | *Tamper resistant software* | 30/05/96 |
| M Blaze | *Key escrow without escrow agents* | 30/05/96 |
| T Berson | *HMOS* | 30/05/96 |
| I Jackson | *Anonymous addresses and confidentiality of location* | 31/05/96 |
| H Federrath | *Mixes in mobile communication systems: location management with privacy* | 31/05/96 |
| D Goldschlag | *Hiding routing information* | 31/05/96 |
| R Anderson | *The Newton channel* | 31/05/96 |
| M Burmester | *A progress report on subliminal-free channels* | 31/05/96 |
| S Low | *Collusion in cryptographic protocols* | 31/05/96 |
| I Cox | *Secure spread spectrum watermarking for multimedia* | 31/05/96 |
| J Smith | *Modulation and information hiding in images* | 31/05/96 |
| J Brassil | *Watermarking document images with bounding box expansion* | 31/05/96 |
| G Simmons | *Keynote address* | 31/05/96 |
| K Sakurai | *Blind decoding for on-line shopping with privacy protection* | 01/06/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| T Aura | *Practical invisibility in digital communication* | 01/06/96 |
| P Davern | *Fractal based image steganography* | 01/06/96 |
| D Gruhl | *Echo hiding* | 01/06/96 |
| Y Desmedt | *Reliable private digital libraries* | 04/06/96 |
| L Gong | *Enclaves: enabling secure collaboration in the Internet* | 04/06/96 |
| D Gollmann | *Blaming Alice and Bob* | 04/06/96 |
| Y Deswarte | *Quantitative assessment of operational security* | 07/06/96 |
| R Anderson | *The eternity service* | 07/06/96 |
| M Reiter | *The omega key management service* | 07/06/96 |
| Y Deswarte | *Fault-tolerance and security* | 11/06/96 |
| J Daugman | *Biometric identification by a test of statistical independence* | 11/06/96 |
| P Landrock | *On prime generation for public keys* | 14/06/96 |
| P D'haeseleer | *An immunological approach to change detection* | 14/06/96 |
| C Landwehr | *Wireless identification system case study in computer security engineering* | 18/06/96 |
| J Bezuidenhoudt | *Trust of third parties in distributed pre-payment systems* | 18/06/96 |
| S Jajodia | *Flexible mechanisms to support multiple access control policies* | 18/06/96 |
| M Kuhn | *Security analysis of the DS5002 micro controller* | 20/06/96 |
| S Forrest | *Building a computer immune system* | 20/06/96 |
| S Chuang | *Security management of ATM networks* | 20/06/96 |
| S Jenkins | *Comments on the information strategy of the NHS* | 21/06/96 |
| O Ulrich | *Chip cards in German healthcare* | 21/06/96 |
| R Cushman | *Exceptionalism redux: is health care information practice really different?* | 21/06/96 |
| B Blobel | *Clinical record systems in oncology. Experiences and developments on cancer registers in Eastern Germany* | 21/06/96 |
| M Hawking | *Organisation of general practice: implications for IM&T in the NHS* | 21/06/96 |
| R Roberts | *Practical protection of confidentiality* | 21/06/96 |
| A Hassey | *Clinical systems security - implementing the BMA policy & guidelines* | 21/06/96 |
| P Landrock | *Using commercial off-the-shelf technology to secure GP provider links* | 21/06/96 |
| P Bruening | *Medical information privacy law in the United States* | 21/06/96 |
| B Woodward | *Information management is no longer records management but a risk management issue* | 21/06/96 |
| A Blyth | *Responsibility modelling: a new approach to the realignment and re-engineering of health care organisations* | 22/06/96 |

*continued on next page*

*continued from previous page*

| Name | Seminar Title | Date Presented |
|---|---|---|
| M Rigby | *Keeping confidence in confidentiality* | 22/06/96 |
| R Draper | *Electronic patient records: usability vs security, with special reference to mental health records* | 22/06/96 |
| U Kohl | *User-oriented control of personal information security in communication systems* | 22/06/96 |
| G Bleumer | *Privacy oriented clearing for the German health care system* | 22/06/96 |
| Y Okada | *Series of personal health data on optical memory cards* | 22/06/96 |
| F Fisher | *The perspective of medical ethics* | 22/06/96 |
| D Banisar | *Legal requirements for computer security: an American perspective* | 22/06/96 |
| A Breitenstein | *US health information privacy legislation: theory and practice* | 22/06/96 |
| R Neame | *Healthcare informatics security in New Zealand* | 22/06/96 |
| R Anderson | *An update on the BMA security policy* | 22/06/96 |

*Total number of seminars within this table: 167*

## G.5 Institute Seminars

| Name | Seminar Title | Date Presented |
|---|---|---|
| D Scott | *Twenty-five years of domain theory* | 09/10/95 |
| Y Lafont | *Interaction, the fine structure of computation* | 16/10/95 |
| P Constantin | *Scaling exponents in turbulence* | 23/10/95 |
| J Lighthill | *Hurricane dynamics* | 30/10/95 |
| H Araki | *Application of modular theory in operator algebras to physics* | 06/11/95 |
| B Smith | *The Smith Institute: A collaboration between academia and industry* | 13/11/95 |
| P Fife | *The peculiar dynamics of the Cahn-Hilliard Equation ics* | 20/11/95 |
| M King | *Messages from the markets: inferring expectations from the proces of c ash and derivative instruments: applications to economic policy* | 27/11/95 |
| S Donaldson | *Symplectic geometry and four-dimensional geometry* | 22/01/96 |
| A Pearson | *Challenges in the dynamics of complex fluids* | 29/01/96 |
| G Simmons | *Share and share alike; the mathematics of distributed capability* | 05/02/96 |
| P Swinnerton-Dyer | *Rational solutions of diophantine equations* | 12/02/96 |
| J Eells | *Harmonic and geodesic spaces - for non-specialists* | 26/02/96 |
| F Kirwan | *Does geometric quantisation commute with symplectic reduction?* | 04/03/96 |
| S Howison | *The rewards of risk: opportunities for mathematics in finance* | 11/03/96 |
| J Coates | *Cyclotomic fields and Fermat's last theorem* | 06/05/96 |
| A Wiles | *MORDELL LECTURE: Elliptic curves and Fermat's last theorem* | 15/05/96 |
| A Wiles | *Elliptic curves and modular forms* | 20/05/96 |
| R Brady | *Murphy's Law, the fitness of evolving species and the limits of software reliability* | 27/05/96 |
| J Goddard | *Material instabilities in complex fluids: what our constitutive equations may be trying to say* | 03/06/96 |
| MF Atiyah | *Duality in geomtery and physics* | 10/06/96 |

*Total number of seminars within this table: 21*

# H Seminars given Outside the Institute

## H.1 Semantics of Computation

| Name<br>Title | Location |
|---|---|
| M Abadi<br>*Authentication in distributed systems* | Computer Lab, University of Cambridge |
| L Cardelli<br>*Mobile computing* | Dept of Computer Science, University of Glasgow |
| RL Constable<br>*Type theory as a foundation for computer science* | Dept of Mathematics, University of Leeds |
| P Dybjer<br>*An introduction to reduction-free normalisation* | Dept of Computer Science, University of Kent at Canterbury |
| P Dybjer<br>*An introduction to reduction-free normalisation* | Dept of Computer Science, University of Edinburgh |
| C Gunter<br>*Representing dependencies between software configuration items* | PRG, Oxford |
| R Harper<br>*ML2000: The next generation* | INRIA, France |
| R Harper<br>*Typical closure conversion* | INRIA, France |
| JME Hyland<br>*Dana Scott in Oxford* | Dept of Computer Science, University of Edinburgh |
| CB Jay<br>*Covarient types* | Dept of Computer Science, University of Nottingham |
| P Johnstone<br>*Cartesian functions between toposes* | Dept of Computer Science, University of Edinburgh |
| CB Jones<br>*Partial functions and logic* | Dept of Computer Science, Cornell University |
| A Jung<br>*Stone duality for continuous domains* | Dept of Computing, Imperial College |
| A Jung<br>*Stone duality and domain logics* | Dept of Computing and Cognitive Science, University of Sussex |
| P Lincoln<br>*Byzantine agreement under hybrid fault model* | Computer Lab, University of Cambridge |
| P Lincoln<br>*Embedded system design* | Technology Center, Honeywell Inc, Minnesota |
| P Lincoln<br>*Authenticated agreement* | DCCA Conference, University of Illinos |
| BC Pierce<br>*Comparing objects and ADTs* | Dept of Computer Science, University of Indiana |
| BC Pierce<br>*Comparing objects and ADTs* | Dept of Computer Science, Carnegie-Mellon University |
| BC Pierce<br>*Linearity and the pi-calculus* | Dept of Computer Science, University of Edinburgh |

*continued on next page*

*continued from previous page*

| Name<br>Title | Location |
|---|---|
| BC Pierce<br>*Experience with PICT* | Dept of Computer Science, University of Edinburgh |
| A Pitts<br>*Operationally based logical relations for idealised algol* | Dept of Computing, Imperial College |
| JC Reynolds<br>*From algol to polymorphic linear lambda calculus* | Dept of Computer Science, University of Glasgow |
| JC Reynolds<br>*Dana Scott at Carnegie Mellon University* | Dept of Computer Science, University of Edinburgh |
| JG Riecke<br>*A generalization of exceptions and control in ML-like languages* | Computing Lab, University of Oxford |
| JG Riecke<br>*Kripke logical relations and PCF* | Dept of Computer Science, Queen Mary and Westfield College |
| D Sangiorgi<br>*Proof techniques for bisimulation* | Dept of Computer Science, University of Warwick |
| V Sassone<br>*AW algebra of nets* | Computer Lab, University of Cambridge |
| A Scedrov<br>*Linear logic proof games and optimization* | Dept of Mathematics, University of Rome |
| A Scedrov<br>*Optimization problems in propositional linear logic* | Dept of Computing Science, Imperial College |
| A Scedrov<br>*Stochastic interaction and linear logic* | 10th Intl Congress: Logic, Methodology..., Florence |
| A Scedrov<br>*Optimization problems in propositional linear logic* | Dept of Mathematics, University of Oslo |
| DS Scott<br>*Experience teaching mathematics with a computer* | Computing Lab, University of Oxford |
| DS Scott<br>*25 years of domain theory* | Computing Lab, University of Oxford |
| PJ Scott<br>*Linear Läuchli semantics and full completeness* | Dept of Computing Science, Imperial College |
| PJ Scott<br>*What is linear logic?* | Dept of Maths & Computer Science, University of St Andrews |
| PJ Scott<br>*Läuchle Semantics* | Dept of Computer Science, University of Edinburgh |

*Total number of talks within this table: 39*

## H.2 From Finite to Infinite Dimensional Dynamical Systems

| Name | Location |
|---|---|
| Title | |
| PW Bates | Dept of Mathematics, University of Rome II |
| *Travelling waves for nonlocal and higher order Allen Cahn equations* | |
| PW Bates | Conference on generalized Stefan problems, Pavia |
| *Theoretical and numerical results for a Hele-Shaw type model of phase transitions* | |
| PW Bates | Dept of Mathematics, University of Sussex |
| *Travelling waves for nonlocal and higher order parabotic PDGs* | |
| PW Bates | Dept of Mathematics, University of Southampton |
| *Dynamics of interfaces for higher order phase field systems* | |
| PW Bates | Dept of Mathematics, University of Strathclyde |
| *Travelling waves for nonlocal and higher order phase field eqts* | |
| P Collet | Dept of Mathematics, University of Exeter |
| *Statistics or entrance and exit times for dynamical systems* | |
| P Constantin | ICMS, University of Edinburgh |
| *Statistical Navier Stokes* | |
| P Constantin | Dept of Mathematics, University of Sussex |
| *The temporal and inviscid limit* | |
| C Doering | Dept of Physics, University of Marburg, Germany |
| *Convection, stability, and turbulence* | |
| C Doering | Dept of Physics, University of Bayreuth |
| *Convection, stability and turbulence* | |
| C Doering | Dept of Physics, University of Lancaster |
| *Energy stability and turbulent energy dissipation* | |
| C Doering | Centre for Nonlinear Dynamics, University College London |
| *Convection, stability and turbulence* | |
| C Doering | Dept of Physics, Humboldt University |
| *Stochastic ratchets* | |
| C Doering | ICTP, Trieste |
| *Stochastic ratchets* | |
| P Fife | Dept of Mathematics, University of Bath |
| *Allan-Kahn theory with nonlocal interactions* | |
| P Fife | Dept of Mathematics, University of Sussex |
| *Hypercooled vililitication and phase field theories* | |
| J Hale | Dept of Mechanics, University College London |
| *Synchronization* | |
| J Hale | Dept of Mathematics, University of Sussex |
| *Synchronization* | |
| DD Holm | Basic Research Inst in the Mathematical Sciences, Hewlett-Packard |
| *Fibre optics communication using solitons* | |
| DD Holm | Dept of Mathematics, University of Bristol |
| *Wave mean flow interaction* | |
| DD Holm | UK Meteorological Office |
| *Wave mean flow interaction* | |

*continued on next page*

*continued from previous page*

| Name | Location |
|---|---|
| Title | |
| R Kerr | DAMTP, University of Cambridge |
| *Magnetic reconnection* | |
| R Kerr | Dept of Mathematics, University of St Andrews |
| *Magnetic reconnection* | |
| Y Nishiura | Mathematics Institute, University of Utrecht |
| *Nonlocal effects and sealing law in phase separation dynamics* | |
| P Polacik | Dept of Mathematics, Heriot-Watt University |
| *Space time asymptotics of solutions of a class of reaction diffasion equations* | |
| EA Spiegel | Dept of Applied Maths, University of Leeds |
| *(Bio) Convective Patterns* | |
| EA Spiegel | NBI, Copenhagen |
| *(Bio) Convective Patterns* | |
| EA Spiegel | Dept of Applied Maths, University of Bristol |
| *Bifurcation of Species* | |
| EA Spiegel | Dept of Applied Maths, Imperial College |
| *Bifurcation of Species* | |
| EA Spiegel | Institute of Astronomy, University of Cambridge |
| *Evidence for a cosmic cascade* | |
| EA Spiegel | Dept of Astronomy, University of Leicester |
| *Evidence for a cosmic cascade* | |
| EA Spiegel | DAMTP, University of Cambridge |
| *Problems of photofluid dynamics* | |
| EA Spiegel | Dept of Physics, University of Turin |
| *Bifurcations of chaos* | |
| EA Spiegel | Dept of Applied Maths, University of Exeter |
| *(Bio) Convective Patterns* | |
| EA Spiegel | DAMTP, University of Cambridge |
| *(Bio) Convective Patterns* | |
| Y Takei | Dept of Mathematics, University of Manchester |
| *WKB analysis of Painlevé transcendents* | |
| E Titi | Dept of Mathematics, University of Ferrara |
| *Approximate inertial manifolds and their computational efficiency* | |
| E Titi | Dept of Mathematics, University of Pisa |
| *Degrees of freedom in turbulent flows* | |
| E Titi | Dept of Civil Engineering, University College London |
| *On the effectiveness and efficiency of the nonlinear Galerkin method* | |
| E Titi | Navier-Stokes Workshop, Université de Montreal |
| *Computational efficiency of nonlinear Galerkin* | |
| Y Yi | Dept of Mathematics, Limburgs University Centre |
| *On almost automorphic dynamics* | |
| Y Yi | Dept of Mathematics, University of Amsterdam |
| *On non-autonomous differential equations* | |

| Name | Location |
|---|---|
| Title | |
| Y Yi | Applied Mathematics Institute, Comenius University |
| *Topological dynamics and differential equations* | |
| Y Yi | Dept of Mathematics, University of Rome II |
| *Dynamical system method in semilinear elliptic equations* | |
| Y Yi | Dept of Information and Systems, University of Florence |
| *On almost periodic differential equations* | |
| Y Yi | Dept of Control and Dynamical Systems, California Institute of Technology |
| *Differential equations with almost periodic coefficents* | |
| Y Yi | CIAM meeting on singular perturbation |
| *A variational problem related to liquid crystals* | |

*Total number of talks within this table: 49*

## H.3 Dynamics of Complex Fluids

| Name | Location |
|---|---|
| Title | |
| RS Anderssen | Schlumberger Cambridge Research |
| *The analysis and interpretation of indirect measurements - solving practical inverse problems* | |
| J Brady | Polymer and Colloids Group, Cavendish Lab, Cambridge |
| *Colloids under stress* | |
| M Cates | Centre for self-organising molecular systems, University of Leeds |
| *The depletion force in colloids* | |
| Masao Doi | Dept of Chemical Engineering, University of Naples |
| *Rheology of liquids with domain structure* | |
| V Entov | OCIAM and Computer Mathematics, University of Oxford |
| *Free boundary problems in flows through porous media: Extremal domains and non-parcian flows* | |
| V Entov | Dept of Applied Maths, Imperial College |
| *Instability and breakup of jets and filaments of polymeric fluids* | |
| V Entov | Dept of Engineering Mathematics, University of Newcastle |
| *One-dimensional dynamics of jet flows of polymeric fluids* | |
| V Entov | Dept of Theoretical Mechanics, University of Nottingham |
| *Free boundary flows in porous media* | |
| V Entov | Dept of Applied Mathematics and Statistics, University of Edinburgh |
| *Free boundary problems in seepage theory* | |
| H Hu | Schlumberger Cambridge Research |
| *Particle motion in a viscoelastic fluid* | |
| D James | Dept of Mathematics, University of Minnesota |
| *Entanglements in long chains at high strain* | |
| R Keunings | DAMTP, University of Cambridge |
| *Stochastic simulation of the flow of polymeric solutions* | |
| R Larson | Dept of Physics, University of Edinburgh |
| *Hydrodynamics of DNA* | |
| R Larson | Dept of Physics, University of Bristol |
| *Hydrodynamics of a single DNA molecule* | |
| R Larson | Dept of Physics, University of Leeds |
| *Hydrodynamics of a single DNA molecule* | |
| GH McKinley | Dept of Physics, University of Essen |
| *Elastic instabilites in extensional flows of polymer solutions* | |
| GH McKinley | DAMTP, University of Cambridge |
| *Spiral instabilites in torsional flows of elastic fluids* | |
| GH McKinley | Dept of Applied Maths, University of Leeds |
| *Extensional rheology and elastic instability of dilute polymer solutions* | |
| GH McKinley | Dept of Chemical Engineering, University of Cambridge |
| *Spiral instabilites in viscoelastic flows* | |
| GH McKinley | DAMTP, University of Cambridge |
| *Spiral instabilities in non Karman flows of viscoelastic fluids* | |
| GH McKinley | Dept of Physics, University of Essen |
| *Extensional rheology and elastic instability of dilute polymer solutions* | |

| Name<br>Title | Location |
|---|---|
| GH McKinley<br>*Extensional rheology of polymer solutions* | Dept of Chemical Engineering, Danish Technical University, Copenhagen |
| GH McKinley<br>*Extensional flows of polymer solutions* | Dept of Applied Mathematics, University of Leeds |
| GH McKinley<br>*Constitutive modeling of polymer solutions* | TA Instruments, Newcastle, Delaware |
| GH McKinley<br>*Spiral instabilities in torsional dlows of elastic fluids* | Engineering Dept, University of Cambridge |
| S Milner<br>*Rules of thumb for extension-thickening with branched polymers* | Exxon Chemical Company, Machelen, Belgium |
| S Milner<br>*How copolymers really help in missing immiscible homopolymers* | Cavendish Lab, University of Cambridge |
| S Milner<br>*Stabilisation of polymeric emulsions* | Dept of Physics, University of Edinburgh |
| WCK Poon<br>*The tenuous existence of liquids* | Dept of Chemistry/Physics, University of Bath |
| S Ramaswamy<br>*Long-ranged forces between hard spheres in a nematic* | Dept of Physics, University of Edinburgh |
| S Ramaswamy<br>*Sedimentary colloidal crystals* | Dept of Physics, University of Edinburgh |
| M Renardy<br>*Mathematical issues in viscoelastic flows* | DAMTP, University of Cambridge |
| M Renardy<br>*Mathematical issues in viscoelastic flows* | Dept of Mathematics, University of Bristol |
| M Renardy<br>*Surfactant spreading on thin films* | Dept of Physics, Brussels Free University |
| M Renardy<br>*Mathematical issues in viscoelastic flows* | Dept of Mathematics, University of Manchester |
| M Renardy<br>*Instability of differentiability of semi-groups* | Dept of Mathematics, ETH Zurich |
| M Renardy<br>*Hopf bifurcation with small frequency on the hexagonal lattice* | Institute for Theoretical Physics, University of Bayreuth |
| Y Renardy<br>*Mode interactions in two-layer convection and a viscoelastic Taylor-Couette flow* | Dept of Mathematical Sciences, University of the West of England |
| Y Renardy<br>*Topics in double-layer convection* | Institute for Theoretical Physics, University of Bayreuth |
| Y Renardy<br>*Topics in double-layer convection* | Centre for Nonlinear Phenomena and Complex Systems, Brussels Free University |
| Y Renardy<br>*Topics in double-layer convection* | Dept of Mathematics, University of Manchester |
| Y Renardy<br>*Topics in double-layer convection* | Dept of Mathematics, University of Birmingham |

| Name | Location |
|---|---|
| Title | |
| Y Renardy | DAMTP, University of Cambridge |
| *Mode interactions in two-layer convection and a viscoelastic Taylor-Couette flow* | |
| S Shiyanowskii | Dept of Chemistry, University of Southampton |
| *Spontaneous and induced decacemization of nematics* | |
| FJ Solis | Dept of Physical Chemistry, Center for Studies of Nuclear Energy, Saclay |
| *Bulk response of polymer brushes* | |
| R Tanner | Polymer Processing Society Conference, Sorrento |
| *3-D viscoelastic flows* | |
| LR White | Particle Research Institute, Nancy |
| *Filtration throughput optimization of flocculated suspensions* | |
| LR White | Cavendish Lab, University of Cambridge |
| *Compressional rheology of flocculated suspensions* | |
| T Witten | Cavendish Lab, University of Cambridge |
| *Crumpling* | |
| AL Yarin | DAMTP, University of Cambridge |
| *Impact of drops on solid surfaces - capillary and short waves* | |

*Total number of talks within this table: 51*

## H.4 Computer Security, Cryptology and Coding Theory

| Name<br>Title | Location |
|---|---|
| M Abadi<br>*A theory of objects* | Dept of Computer Science, University of Edinburgh |
| B Christianson<br>*Networks and distributed systems* | Dept of Computer Science, University of Hertfordshire |
| H Dobbertin<br>*Cryptanalysis of MD4* | Dept of Computer Sciences, Royal Holloway and Bedford New College |
| J Golic<br>*Decoding linear codes beyond half the minimum distance* | Signal Processing Group, University of Cambridge |
| J Golic<br>*Decoding linear codes beyond half the minimum distance* | Signal Processing Group, University of Cambridge |
| L Gong<br>*Enabling secure collaboration in the Internet* | Dept of Mathematics, Ecole Normale Superieure, Paris |
| T Helleseth<br>*Sequences from codes over Z4* | Royal Holloway and Bedford New College |
| V Korjik<br>*Error detecting codes* | Communication Research Centre, University of Lancaster |
| KY Lam<br>*Security infrastructure for electronic commerce* | Computer Lab, University of Cambridge |
| KY Lam<br>*Generation elliptic curves for DL-based cryptosystems* | DPMMS, University of Cambridge |
| KY Lam<br>*Practical aspects of public key cryptography* | Dept of Computer Science, Royal Holloway and Bedford New College |
| D Mackay<br>*Good error correcting codes based on very sparse matrices* | Dept of Engineering, University of Cambridge |
| JF McKee<br>*Subtleties in the distribution of the numbers of points on elliptic curves over finite prime fields* | Dept of Mathematics, University of Edinburgh |
| J McLean<br>*Software engineering for computer security* | Computer Lab, University of Cambridge |
| C Meadows<br>*Why we shouldn't think in terms of 'Attacks'* | Computer Security Foundations Workshop, Diemquinna |
| C Meadows<br>*Language generations and verification in the NRL protocol analyzer* | Computer Security Foundation Workshop, Diemquinna |
| F Morain<br>*Algorithms for computing isogenies* | University of Edinburgh |
| R Morris<br>*Ways of losing information* | Dept of Computer Science, Royal Holloway and Bedford New College |
| R Morris<br>*Ways of losing information* | Dept of Computer Science, University of Hertfordshire |
| R Morris<br>*Factorization* | Computer Lab, University of Cambridge |
| B Pfitzmann<br>*Asymmetric fingerprinting* | Eurocrypt 96, Zaragoza |
| R Pinch<br>*Attacking elliptic curve cryptosystems* | ICMS, University of Edinburgh |

*continued on next page*

*continued from previous page*

| Name | Location |
|---|---|
| Title | |
| B Preneel | Dept of Mathematics, Royal Holloway and Bedford New College |
| *New results on message authentication codes* | |
| R Safavi-Naini | Dept of Mathematics, Royal Holloway and Bedford New College |
| *Authentication systems with shared generation of authenticators* | |
| G Simmons | Dept of Mathematics, Royal Holloway and Bedford New College |
| *Secret sharing and identification* | |
| G Simmons | Dept of Mathematics, Royal Holloway and Bedford New College |
| *A keyed permutation generator* | |

*Total number of talks within this table: 29*

# I Call for Proposals

The Isaac Newton Institute for Mathematical Sciences is a national research institute in Cambridge. It aims to bring mathematical scientists from UK universities and leading experts from overseas together for concentrated research on specialised topics in all branches of the mathematical sciences from pure mathematics, applied mathematics, and statistics, to engineering, computer science, theoretical physics and mathematical biology.

At any time there are two visitor programmes in progress, each with about twenty scientists in residence. During these programmes, there will be periods of more expanded activity including instructional courses and workshops. The first fourteen programmes: Low-dimensional Topology and Quantum Field Theory; Dynamo Theory; L-functions and Arithmetic; Epidemic Models; Computer Vision; Random Spatial Processes; Geometry and Gravity; Cellular Automata, Aggregation and Growth; Symplectic Geometry; Topological Defects; Exponential Asymptotics; Financial Mathematics; Semantics of Computation; From Finite to Infinite Dimensional Dynamical Systems; Dynamics of Complex Fluids; Computer Security, Cryptology and Coding Theory have now been completed, and the programmes which are running now or have already been chosen for future years are:

*Mathematics of Atmosphere and Ocean Dynamics (Jul – Dec 1996)*
*Mathematical Modelling of Plankton Population Dynamics (29 Jul – 6 Sep 1996)*
*Four-dimensional Geometry and Quantum Field Theory (4 Nov – 13 Dec 1996)*

*Representation Theory of Algebraic Groups and Related Finite Groups (Jan – Jun 1997)*
*Non-perturbative Aspects of Quantum Field Theory (Jan – Jun 1997)*

*Disordered Systems and Quantum Chaos (Jul – Dec 1997)*
*Neural Networks and Machine Learning (Jul – Dec 1997)*

*Arithmetic Geometry (Jan – Jun 1998)*
*Dynamics of Astrophysical Discs (Jan – Jun 1998)*

*Biomolecular Function and Evolution in the Context of the Genome Project (Jul – Dec 1998)*
*Nonlinear and Nonstationary Signal Processing (Jul to Dec 1998)*

*Turbulence (Jan – Jul 1999)*
*Mathematics and Applications of Fractals (Jan – April 1999)*
*Complexity, Entropy and the Physics of Information (May – Aug 1999)*

*Singularity Theory (Jul – Dec 2000)*

The Institute is now actively seeking new proposals for programmes for 1999 onwards, particularly from areas which have been under-represented so far. The Institute has decided to change the programme structure in 1999 to have two six-month programmes (Jan-June and Jul-Dec) and three four-month programmes (Jan-Apr, May-Aug and Sep-Dec). By having some shorter programmes the Institute will be able to accommodate important, but less well-developed areas and also to improve the coverage of all areas of the mathematical sciences. Proposals should be addressed to The Director, Professor Keith Moffatt, Isaac Newton Institute for Mathematical Sciences, 20 Clarkson Road, Cambridge CB3 0EH, UK; proposers should state whether they would prefer a four-month or six-month programme and their order of preference for the time periods above. The Institute is pleased to receive proposals at any time. Proposals for consideration at the next meeting of the Scientific Steering Committee should be received by 31st January 1997; proposals for consideration at the second meeting in 1997 should be received by 31st July 1997.

Further information is also available from the Director (email i.newton@newton.cam.ac.uk; Tel 01223 335999) who will answer any enquiries.

### Submission of Proposals

The Isaac Newton Institute for Mathematical Sciences welcomes proposals for research programmes of either four-month or six-month duration. The Scientific Steering Committee meets twice a year to consider proposals and make recommendations on which programmes to adopt.

There are about twenty scientists associated with each programme in residence at any time, with more for special workshops and meetings. The scientific planning and organisation are the responsibility of a team of three or four organisers (aided in some cases by a group of scientific advisers). Each programme is provided with a budget for salary support, subsistence allowances and travel expenses but, because space and financial support are limited, all formal invitations must be issued, and all commitments entered into, only by the Director.

Proposals should in the first instance be two to four sides of A4 in length and should be formulated under the following headings:

1. Name of the author(s) of the proposal;
2. Scientific case for the proposal, preferably set out under the following headings:
   a. scientific background/history of proposed topic
   b. recent progress
   c. possible future directions and developments
   d. why the topic is particularly suited to the Newton Institute at this time
3. Possible organisers
4. About 30 to 60 possible participants, listed in the categories "essential", "desirable" and "reserve"
5. An outline of how the programme would be organised

It is expected that each of the organisers will be present for the major part of the programme. Appropriate financial arrangements will be made. Participants should be selected not necessarily for their seniority but for their active involvement in current research. Proposals should list the affiliations of possible organisers and participants.

Proposals will be welcomed at any time. They should be submitted to:

The Director,
Isaac Newton Institute for Mathematical Sciences,
20 Clarkson Road,
Cambridge, CB3 0EH,
UK.

The Director, Professor Keith Moffatt, will be glad to answer any queries about the submission of proposals (tel. 01223 335999; fax 01223 330508; e-mail i.newton@newton.cam.ac.uk).

The Scientific Steering Committee meets in October and April each year to consider proposals for programmes to run about two years later. Proposals for consideration at these meetings should reach the Director preferably at least two months before the meeting but late proposals will be given preliminary consideration.

In making their recommendations, the Scientific Steering Committee will be concerned to see that the programmes taken together reflect the broad scope within the mathematical sciences

which the Institute is intended to cover. Proposals for programmes which will facilitate cross-fertilisation between different disciplines within the mathematical sciences are particularly welcome. Successful proposals are usually the subject of discussion between the authors and the Committee conducted through the agency of the Director and aimed at the development of the proposal. They may be considered at at least two meetings of the Committee before selection is recommended.

# J Brief History of the Institute

The Isaac Newton Institute for Mathematical Sciences was opened in July 1992, after four years of careful preparation. For a number of years and a variety of reasons, a need had been felt for a UK national institute in theoretical physics and mathematics. The realisation of this idea became possible with the availability of "pump-priming" financial support from Cambridge Colleges, notably St John's College and Trinity College (through the Isaac Newton Trust). St John's offered to provide a purpose-built building on land it owned in West Cambridge, promising to subvent the rent by £150,000 *pa* for five years and Trinity offered £200,000*pa* towards running costs for the first five years.

Further support and endorsement came from the London Mathematical Society (LMS) at its retreat in May 1989 at the Isle of Thorns.

This was followed by negotiations with the Science and Engineering Research Council (SERC), since replaced by the Engineering and Physical Sciences Research Council (EPSRC), which invited proposals from universities wishing to develop a mathematics institute and, after consideration of proposals from Cambridge, Edinburgh (Edinburgh and Heriot-Watt Universities), London, Oxford and Warwick, recommended the funding of the Cambridge proposal and offered a 'rolling grant' of about £366,000*pa* for the first four years. This grant is reviewed every two years.

Sir Michael Atiyah was appointed Master of Trinity College in early 1990 and at the same time consented to become the first Director of the Institute. Professor Peter Goddard acted as Deputy Director until in 1994 he was elected Master of St John's.

Further funding was forthcoming from NM Rothschild and Sons and other generous contributions to setting-up costs came from Apple UK; Cambridge University Press; Princeton University Press; Springer-Verlag and other publishers; Christ's, Gonville and Caius, Emmanuel and Jesus Colleges; the Nuffield Foundation; Sun Microsystems and the University of Cambridge.

The Institute was formally established as part of the University of Cambridge on 2 November 1990, with a Management Committee and Scientific Steering Committee (see 3.1 and 4.3 below).

The Scientific Steering Committee met for the first time in 1990 and recommended the Director to select *Low Dimensional Topology and Quantum Field Theory* and *Dynamo Theory* as the first programmes to start in July 1992.

By the time the Institute opened on 3rd July 1992, the eight programmes for the first two years were at active stages of preparation, with invitations issued for nearly all of the first year and much of the second.

The official opening of the building had to wait until 30th October 1992 when the Chancellor of the University, HRH the Duke of Edinburgh, came to the Institute and met many of the visiting members.