CWI Visiting Committee on Computer Science

16 - 19 September 1991

Description of the research groups

July 1991

CWI Visiting Committee on Computer Science

16 - 19 September 1991

Description of the research groups

July 1991

Overview of the Research Groups

AP: Department of Software Technology
Head: J.W. de Bakker

Research groups:

AP1	Semantics	J.W. de Bakker
AP2	Concurrency and Real Time Systems	J.C.M. Baeten
AP3	Extensible Programming Environments	P. Klint
AP4	Algebraic and Syntactic Methods	J.W. Klop
AP5	Logic and Language	K.R. Apt

AA: Department of Algorithmics and Architecture
Head: L.G.L.T. Meertens

Research groups:

AA1	Algorithms and Complexity	P.M.B. Vitányi
AA2	Cryptology	D. Chaum
AA3	Computersystems and Ergonomics	S. Pemberton
AA4	Databases	M.L. Kersten
AA5	Constructive Algorithmics	L.G.L.T. Meertens

IS: Department of Interactive Systems
Head: P.J.W. ten Hagen

Research groups:

IS1	Computer Graphics	A.A.M. Kuijk
IS2	Interaction	I. Herman
IS3	Intelligent CAD Systems	F. Arbab

CST: Department of Computer Systems and Telematics
Head: D.C.A. Bulterman

Research group:

CS1	Multimedia Kernel Systems	D.C.A. Bulterman

DEPARTMENT OF SOFTWARE TECHNOLOGY

The Department of Software Technology (AP, from the dutch Afdeling Programmatuur) was founded at the CWI in 1985. Since its inception it has pursued research in the areas of applied logic and semantics, and of formal methods in programming. Recently, natural language processing and the parallels between natural and programming languages were added as research themes. The work of AP is organized in the following five research groups:

AP1 Semantics
AP2 Concurrency and Real Time Systems
AP3 Extensible Programming Environments
AP4 Algebraic and Syntactic Methods
AP5 Logic and Language.

Below, detailed information is provided by the research groups on their past activities and future plans. In this introduction, we firstly add some information concerning the collaborative structure between the groups. Part of this refers to formal cooperation in externally funded projects, partly it describes informal interaction around themes of mutal interest.

Formal cooperation

- Groups AP1, 4 and 5 each participate (with 1 fte) in ESPRIT Basic Research Action Integration;
- Groups AP2 and 4 both participate in ESPRIT BRA CONCUR.

Informal

- AP4 is an offspring of group AP2; both groups share an ongoing interest in process algebra;
- AP3 and AP2 work together on *algebraic specification* and on *module algebra;*
- AP3 profits from AP4's expertise on *term rewriting systems*;
- AP4 is involved in cooperation with:
  - AP1 on *projection spaces* and on *process algebra*;
  - AP2 on *Hoare logic* and *process algebra*;
  - AP5 on *dynamic interpretation* and *Hoare deduction* (in the context of natural languages);
- AP1 and AP5 work together on the *semantics of logic programming.*

We conclude with two strategic considerations concerning the department's policy:

a. (future new projects) Our first priority is to split AP5 into two independent groups, one concerned with Logic and the other with (natural) Language. The second priority is to initiate a new project which, following the example set by AP3 -at present the only group

which also develops software systems- aims at the implementation of ideas conceived in a theoretical context.

b. (external funding) As will become abundantly clear from the information to follow, AP is critically dependent on externally funded contracts (altogether, this concerns at present about 20 positions). Budgetary cuts in IT funding both by the Dutch government and by the CEC are rather likely, and this may severely affect the department's future: only 8 of our staff are at present in tenured CWI positions, and cuts in external funding might easily result in a 50% reduction of the department's size in a few years.

J.W. de Bakker
June 1991

RESEARCH GROUP AP1
SEMANTICS

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

prof.dr. J.W. de Bakker	department head and group leader	0.8 fte	
dr. J.J.M.M. Rutten	researcher	1.0 fte	

Nonpermanent:

dr. J.N. Kok	researcher from Utrecht Univ.	0.2 fte	since 01.07.89
dr. J.M. Jacquet	researcher	1.0 fte	since 01.10.89
drs. D. Turi	junior researcher	1.0 fte	since 01.05.91
drs. J. Warmerdam	junior researcher	1.0 fte	since 01.11.89

External funding:

1. ESPRIT BRA INTEGRATION, from 01.07.89 until 31.12.91

prof.dr. J.W. de Bakker	project leader	0.1 fte
dr. J.J.M.M. Rutten	project secretary	0.2 fte
dr. J.N. Kok	researcher	0.2 fte
dr. J.M. Jacquet	researcher	0.7 fte

2. NFI project REX, from summer 1988-summer 1992

drs. J. Warmerdam	junior researcher	1.0 fte
dr. M. Kwiatkowska	guest researcher	3 months

3. SION project Nonwellfounded sets in semantics

dr. J.J.M.M. Rutten	project leader	p.m.
drs. D. Turi	junior researcher	1.0 fte

Former staff members 1987-1991:

dr. M. Kwiatkowska	guest researcher	1.0 fte	18.04.91-18.07.91

2. Introduction

Continuing earlier work on the semantics and proof techniques of sequential programs, research group AP1 has devoted most of its efforts in the eighties towards the study of the semantics of concurrent languages. In order to delimit its activities from those of AP2, the group has renamed itself in 1990 as Semantics. At present its area of investigation is defined as 'Research into the semantic aspects of parallel computation according to various

programming styles (imperative, logic, object-oriented, declarative); also foundational and comparative issues related to semantic modelling'.
Since 1984, the group has profited substantially from its participation in a number of collaborative projects

A. International
ESPRIT 415: Parallel architectures and languages (1984-1989). This project has involved us in a large-scale European effort to design novel parallel architectures driven by languages models of the functional, logic and object-oriented style. Especially fruitful has been our cooperation with Philips Research Eindhoven concerning the semantics and proof techniques for Philips' parallel object-oriented language POOL. Altogether, ESPRIT 415 has sponsored or supported research and organizational events resulting in 3 to 4 Ph.D. theses, 5 books and numerous further publications.
ESPRIT Basic Research Action (EBRA) Integration (1989-1991). The task of AP1 in this project is, besides its role as action manager, to investigate the semantics of parallel LP and OO. Several results have been obtained concerning (the semantics of) each of these two programming styles. Integrative work has been done especially in Eliëns' thesis and in the cooperation between AP1 and Uninova, Lisbon (L. Monteiro) on synchronous communication in concurrent LP, specified both globally and locally.

B. National
This refers to two projects: the National Project on Concurrency (LPC, 1984-1988) and the (NFI) project REX-Research and Education in Concurrent Systems (1988). These projects, jointly with RUL and TUE, have been a major factor in Dutch research in syntactic, semantic and proof-theoretic aspects of concurrency.
Both Ph.D. research and several educational events have been sponsored (national seminars, schools-workshops), as well as international cooperation with the French C3 and British FACS programmes.

Besides the above mentioned projects, cooperation has been going on for several years in the Amsterdam Concurrency Group, an informal seminar with members (Ph.D. students or Ph.D.'s) from Free University Amsterdam, University Utrecht, Erasmus University, TU Eindhoven, and AP1.

3. Research 1987-1991
Main subthemes of AP1's research during the indicated period have been:
a. Foundations for semantics and comparative issues: the development of the metric semantics machinery, with contrasting themes such as uniform/nonuniform languages, linear time/branching time models, and operational/denotational semantics; moreover, non-wellfounded sets (which may be used as domains where metric spaces do not work), general properties of transition systems.
b. Semantics for parallel object-oriented languages (process creation, rendez-vous, dynamically evolving process structures), in particular POOL.
c. Proof theory for POOL.

d. Semantics for nondeterministic dataflow.
e. Semantics of a large variety of concurrent logic languages, including Horn Clause Logic, PARLOG, Concurrent PROLOG, GHC, versions of contextual LP and constraint LP.
f. Integration of LP and OO.
g. Full abstractness issues.
h. (Interleaving vs.) true concurrency.
i. Exploration of the relationship between (the category of) metric spaces, other topological spaces, cpo's and nonwellfounded sets.
j. (At a limited scale) relations between AP1's methodology and questions in process algebra (e.g. the determination of representatives of weak bisimulation equivalence classes).
k. Several edited collections of results obtained by AP1, ESPRIT 415, LPC, REX, or conferences/workshops around their themes.

4. Plans for the future

We are preparing an extension proposal for EBRA Integration - with added emphasis on the LP/OO integration, and de-emphasizing the role of FP.
Prospective new partners are ECRC (Munich), University Genova (and enlarged involvement from ENS, Paris).

We have applied for an extension of the funding for REX in 1992, 1993, to allow us to continue its educational activities (workshops, visiting scholars, etc.). Also, we hope that the proposal submitted to the SCIENCE programme to support a twinning project in the field of the mathematical foundations for concurrency semantics will be successful.

As to the research themes, we shall (continue to) work on:
a. Mathematical foundations for semantics: metric vs. cpo domains, projection spaces, nonwellfounded sets, non-metric tolopogies, Stone dualities.
b. Fully abstract models for OO, CCS-generalizations such as the pi calculus.
c. Semantics for concurrent constraint and contextual LP.
d. OO/LP integration through the study of more elaborate forms of communication, e.g. requesting the presene of events, and more powerful mechanisms like those merging inheritance and concurrency.
e. (Systems of) domain equations and generalized bisimulation.
f. Relations between ACG's semantic methodology, and the refinement calculus and predicate transformed semantics.

5. Cooperation 1987-1991

A. Contract research

1. ESPRIT project 415:
Parallel Architectures and Languages, CWI (AP1) as subcontractor of Philips Research Eindhoven, other partners AEG (D), GEC (UK), Bull (F), Nixdorf (D), CSELT (I), Stollmann (D).In project 415 (1984-1989) the role of AP1 was:
- member project coordination committee;

- chair WG on Semantics and Proof techniques;
- design semantics and proof techniques for the language POOL.

2. ESPRIT BRA:
   Integration: integrating the foundations of functional logic and object-oriented programming. Current partners CWI (action coordinator), ENS (Paris), Imperial College (UK), Philips Research Eindhoven (NL), Univ.Pisa (I), UNINOVA (P).
   Expected changes in consortium in extension phase:
   - Univ. Genova, ECRC (Munich);
   - Philips Reserach Eindhoven.
3. SION (Netherlands Research Foundation for Computer Science):
   - 1984/1988: National Concurrency Project (jointly with W.P. de Roever (TUE), G. Rozenberg (RUL));
   - 1991/1995: Project on nonwellfounded sets in semantics.
4. NFI (Netherlands national facility for informatics):
   1988- : project REX: Research and Education in Concurrent Systems (jointly with W.P. de Roever (TUE/Kiel Univ.), G. Rozenberg (RUL)).
5. (Application submitted to EC SCIENCE program) twinning project on Mathematical Structures in Concurrency Semantics, CWI coördinator, partners Univ. Pisa (Montanari), CNRS-Rennes (Darondeau), Univ. Udine (Honsell), Univ. Mannheim (Majster), Univ. Paderborn (Priese).

B. Contacts and/or cooperation with industry
None.

C. Contacts and/or cooperation with scientific institutes
McGill Univ. (Canada), McMaster Univ. (Canada), NTT (Tokyo), Novosibirsk (Acad. of Science), Univ. Edinburgh-LFCS (UK), Univ. Oldenburg (D), Univ. Swansea (UK), Abo Akademi (Finland), LITP (F), Univ. Utrecht, Groningen, Leiden, EU Rotterdam, Vrije Universiteit Amsterdam, TU Eindhoven.

6. Further activities 1987-1991

Prof.dr. J.W. de Bakker
- Member Koninklijke Nederlandse Akademie van Wetenschappen (Royal Netherlands Academy of Arts and Sciences).
  Member Academia Europaea, April 1990.

Thesis supervisor of:
- J.N. Kok, May 1989, Semantic models for parallel computation in dataflow, logic- and object-oriented programming;
- P.H.M. America, May 1989, A parallel object-oriented language: design and semantic foundations (jointly with J.J.M.M. Rutten);

- J.J.M.M. Rutten, May 1989, A parallel object-oriented language: design and semantic foundations (jointly with P.H.M. America);
- E.P. de Vink, May 1990, Designing stream based semantics for uniform concurrency and logic programming;
- F.S. de Boer, April 1991, Reasoning about dynamically evolving process structures, a proof theory for the parallel object-oriented language POOL;
- A. Eliëns, February 1991 (as second promotor), DLP-A language for Distributed Logic Programming.

External examiner of:
- R. Gerth, Utrecht University, May 1989;
- R.L.C. Koymans, Eindhoven Technological Univ., May 1989;
- W.P. Weijland, University of Amsterdam, June 1989;
- R.J. van Glabbeek, Free Univ. of Amsterdam, May 1990;
- A. Middeldorp, Free Univ. of Amsterdam, November 1990;
- J.F. Groote, University of Amsterdam, November 1991.

Program committees:
- International Colloquium on Automata, Languages and Programming, Warwick 1990;
- Mathematical Foundations of Computer Science Cracow, 1989;
- IFIP TC2 Working Conference on Formal Description of Programming Concepts, Sea of Galilee, 1990;
- CAAP/TAPSOFT, Pisa 1987;
- PARLE, Parallel Architectures and Languages Europe, Eindhoven 1987 (co-chairman), Eindhoven 1989;
- CONCUR 91, Amsterdam, 1991.

Organizing committees:
- C3/LPC French/Dutch Colloquium on Concurrency, Amsterdam 1989.

Editor of:
- Journal of Computer and System Sciences (associate editor), 1973-;
- Theoretical Computer Science, 1975-;
- Fundamenta Informaticae, 1983-;
- CWI Publications (managing editor);
- Cambridge University Press Tracts in Theoretical Computer Science;
- Parallel Computing, Special Issue on the PARLE Conference;
- Wiley Series on Parallel Computing (consulting editor).

Invited lectures:
- Abo Akademi Lecture series on Parallelism, Turku 1989;
- IFIP Congress '89, San Francisco, 1989;
- TOPSOFT '91, Brighton, 1991;
- PARLE '91, Eindhoven 1991;
- Stefan Banach Centre, Warsaw 1991.

Concurrency:
- Project leader (with W.P. de Roever, G. Rozenberg) Dutch National Concurrency Project, 1984-1989;
- Project leader (with W.P. de Roever, G. Rozenberg) NFI National Project on Research and Education in Concurrent Systems (REX), 1988-;
- (co-)director of REX Workshop 'Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency', May, June 1988;
- (co-)director of REX Workshop 'Refinements of Distributed Systems: Models, Formalisms, Correctness', May, June 1989;
- (co-)director of REX School/Workshop 'Foundations of Object-Oriented Languages', May, June 1990;
- (co-)director of REX Workshop 'Real-Time', June 1991.

ESPRIT:
- Member project coordination committee ESPRIT project 415: Parallel Architectures and Languages for AIP, 1984-1989 (ESPRIT project 415 was the largest project in the area Advanced Information Processing, budgeted at 250 man years for 1984-1989);
- Chairman Working Group on Semantics and Proof Techniques, ESPRIT project 415, 1984-1989;
- Project leader, ESPRIT Basic Research Action on Integration of Functional, Logic and Object Oriented Programming;
- Reviewer, ESPRIT Basic Research Actions Cedisys and Demon.

Miscellaneous:
- Council member European Association for Theoretical Computer Science, 1982-1988;
- Cofounder and chairman Dutch Research Community for Theoretical Computer Science,1979-1987;
- Member Dutch Academy Committee for Mathematics, 1977-1990;
- Cofounder and member of the board, Dutch Research Foundation for Computer Science,1980-1988;
- Chairman, scientific advisory board, Dutch Research Foundation for Computer Science, 1988-;
- IFIP Working Group 2.2 on Formal Description of Programming Concepts, member 1967;
- Member advisory board, Foundations of Computation Laboratory, Queensland, Australia, 1988 -;
- Curator, (special) chair for Theoretical Computer Science - Logic for Distributed Systems and Artificial Intelligence, Free University Amsterdam, 1988 -.

Dr. J.M. Jacquet
Organizer of the ICLP'91 preconference workshop on Constructing Logic programs.

Dr. J.J.M.M. Rutten
Member and the secretary of the BR Action Integration. He is also the editor of a EC SCIENCE proposal entitled MASK: Mathematical Structures in Semantics of Concurrency.

7. Experimental systems and programs 1987-1991
None.

8. Selected publications 1987-1991

1. Ph.D.thesis by P. America and J.J.M.M. Rutten:
   A parallel object-oriented language: design and semanticfoundations, Free University, Amsterdam, 1989. (Promotor: J.W. de Bakker, referee G. Plotkin.) This thesis consists of the following papers:
- P. America, Issues in the design of a parallel object-oriented language, Formal Aspects of Computing 1(4), 1989, pp. 366-411;
  P. America and J.J.M.M. Rutten, Solving reflexive domain equations in a category of complete metric spaces, Journal of Computer and System Sciences 39(3), 1989, pp. 343-375;
- P. America, J.W. de Bakker, J.N. Kok and J.J.M.M. Rutten, Denotational semantics of a Parallel Object-Oriented Language, Information and Computation 83(2), 1989, pp. 152-205;
- P. America and J.W. de Bakker, Designing equivalent semantic models for process creation, Theoretical Computer Science 60(2), 1988, pp. 109-176;
- J.N. Kok and J.J.M.M. Rutten, Contractions in Comparing Concurrency Semantics, Theoretical Computer Science 76, 1990, pp. 179-222;
- J.J.M.M. Rutten, Semantic equivalence for a parallel object oriented language, SIAM J. Comput. 19 (2), 1990, pp. 341-383;
- J.J.M.M. Rutten and J.I. Zucker, A semantic approach to fairness, to appear in Fundamenta Informaticae.

2. J.W. de Bakker, Comparative semantics for flow of control in logic programming without logic, Information and Computation 93, 1991. (Appeared earlier as CWI technical report CS-R8840, 1988).
3. J.W. de Bakker, W.P. de Roever and G. Rozenberg (eds.), Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency, Proceedings of REX School/Workshop, Noordwijkerhout, The Netherlands, 1988, Lecture Notes in Computer Science 354, 1989.

RESEARCH GROUP AP2
CONCURRENCY & REAL TIME SYSTEMS
State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

dr. J.C.M. Baeten	group leader	0.8 fte	since 01.02.89

Nonpermanent:

J.O. Blanco	junior researcher	1.0 fte	since 01.05.91
drs. W.J. Fokkink	junior researcher	1.0 fte	since 01.03.91
drs. J.F. Groote	researcher	1.0 fte	since 16.02.88
drs. A.S. Klusener	researcher	1.0 fte	since 01.03.90
drs. H. Korver	researcher	1.0 fte	since 01.01.91
drs. A. Ponse	researcher	1.0 fte	since 16.03.88
prof.dr. J.A. Bergstra	researcher	0.2 fte	
prof.dr. J.A. Bergstra	advisor	-	since 01.05.88

External funding:

1. ESPRIT BRA CONCUR, from 01.09.89 until 31.08.91

dr.J.C.M. Baeten	project leader	0.2 fte
drs.W.J. Fokkink	junior researcher	0.55 fte
drs.J.F. Groote	researcher	0.3 fte
prof.dr J.W. Klop	researcher (from AP4)	0.1 fte
drs. A.S. Klusener	researcher	0.1 fte

2. RACE project SPECS, from 01 01.88 until 31.12.92

dr. J.C.M. Baeten	project leader	0.2 fte
drs. J.F. Groote	researcher	0.6 fte
drs. H. Korver	researcher	1.0 fte
drs. A. Ponse	researcher	0.9 fte
prof.dr. J.A. Bergstra	researcher	0.2 fte

3. ESPRIT TIP ATMOSPHERE, from 01.03.89 until 31.05.92

dr. J.C.M. Baeten	project leader	0.2 fte
drs. A.S. Klusener	researcher	0.9 fte

4. NFI project TRANSFER, from 01.01.91 until 31.12.94

dr. J.C.M. Baeten	project leader	-
drs. J.O. Blanco	junior researcher	1.0 fte

2. Introduction

The research group Concurrency & Real Time Systems was called Formal Specification Methods until 1990. It does research in both these areas, and looks to apply the results of this research in an industrial context, in the development of large, integrated, distributed software systems.

The group started in 1982, and has from the start played an important role in European programs: in 1983 and 1984 in the ESPRIT pilot project FAST, from 1984 to 1989 in the ESPRIT I project METEOR, in 1987 and 1988 in the RACE pilot project VIP, from 1988 in the RACE project SPECS, from 1989 in the ESPRIT II technology integration project ATMOSPHERE and the ESPRIT Basic Research Action CONCUR. These cooperative projects have provided us with the means to have a reasonably sized team, to have close contacts with European IT industry and other academic institutions, and to get feedback from them on our work. A drawback from spending all effort on these short-term projects, that demand deliverables every six months, is that no effort can be spent on important fundamental research, that has a longer maturing time. Thus, project AP 2.5 is important, but has no staff because of lack of internal funding (see below).

At the present time, we see that both in ESPRIT III and in RACE II programs the emphasis has moved away from research to the actual applications and system, environment building efforts. This is making it increasingly difficult to maintain the high level of external funding. Therefore, it is to be expected that either the level of internal funding (now almost non-existent in this group) has to be increased considerably, or the size of the group will shrink dramatically over the next few years.

Division in projects:

- AP 2.1. CONCUR (Baeten 0.2, Fokkink, Groote 0.3, Klusener 0.1, Klop 0.1);
- AP 2.2. SPECS (Baeten 0.2, Groote 0.6, Korver, Ponse, Bergstra 0.2);
- AP 2.3. ATMOSPHERE (Baeten 0.2, Klusener 0.9);
- AP 2.4. TRANSFER (Baeten p.m., Blanco);
- AP 2.5. Longer Term Fundamental Research (no staff).

3. Research 1987 - 1991

Our work on algebraic concurrency theory (process algebra), coming into full power in the context of the ESPRIT project METEOR, has put us among the most important groups worldwide, together with the CCS-group in Edinburgh with e.g. and the CSP-group in Oxford. A sign of this is the coordination of the current ESPRIT BRA CONCUR, the proposed ESPRIT BRA ACE and the proposed Concurrency Network. This work has culminated in two books that appeared at Cambridge University Press. At the moment, extensions with real time aspects and probabilities receive most attention.

Our work on specification languages started with cooperation with AP3 on the algebraic specification language ASF and modularisation concepts in general (module algebra). In METEOR and currently in ATMOSPHERE, we work on the Philips wide spectrum language COLD. In VIP, we worked on the specification language VVSL. In SPECS, we designed the specification language CRL (Common Representation Language), that incorporates process algebra, and can be used to translate high level specifications in SDL or LOTOS into, and in

turn derived representations, tools and in the end product quality code can be derived from CRL. Version 3.0 is due at the end of SPECS (end 1992).
We are also involved with the development of the process specification language PSF at the University of Amsterdam.
Apart from these two main lines of research, we also have some research on term rewriting systems (in cooperation with AP4), as applications are found in proving results about process algebra, and t.r.s. are also very important in the implementation (or prototyping) of specification languages.

4. Plans for the future

It is likely (but not certain) that Baeten will leave CWI in the near future. CWI management is of the opinion that the research should be continued. It seems possible to find a capable new groupleader. Before this person can start Baeten will manage the group on a part-time basis.
In research, we will further develop our real time process algebra and real space process languages, we will concentrate on the small language. CRL, in order to better understand the interpaly between processes and data.
Concerning external funding, we are very much involved in deliberations concerning BRA I. In the proposed project ACE (Action on Concurrency in Europe) 4 current BRA's (CONCUR, CEDISYS, DEMON, SPEC) will go together. Baeten is proposed coordinator. CWI would coordinate a related so-called 'network of excellence' in Concurrency.
Negotiations concerning RACE I are continuing. Nothing more can be said as of yet. concerning ESPRIT II (main stream) promise no good for CWI. We are monitoring events w.r.t. ESS I.
Concerning educational activiteis, in August 1991, CONCUR'91, is organized by CWI, the second international conference on concurrency theory. The first, CONCUR'90 was co-organised by CWI.

5. Cooperation 1987 - 1991

A. Contract research

1. METEOR:
   Philips Research (B, NL); CGE, Laboratoire de Marcoussis (F); LRI, Université Paris-Sud(F); ATP (B); CWI (NL); COPS (IRL); TXT (I); Politecnico di Milano (I); Universität Passau (D).
2. SPECS:
   GSI-TECSI (F); CNET (F); STET-CSELT (I); PTT-RNL (NL); IBM France (F); NIHE (IRL); TFL (DK); INESC (P); GPT (UK); EB (N); Bell (B); ELIN Alcatel (A); Laboratoire de Marcoussis (F); SESA (F).
3. ATMOSPHERE:
   Bull (F, I); GIE Emeraude (F); SFGL (F); GMV (E); INTECS Sistemi (I); DATAMAT (I); Cap Gemini (F); GEI (D); Sema (B); Universität Dortmund (D); Siemens-Nixdorf (D); Universität Paderborn (D); University of Strathclyde (UK); Philips (NL, B); SERC (NL); NOKIA (SF); TeleSoft (S); CTC (GR); Generics (IRL); GMD (D); 2i (D).

4. CONCUR:
   CWI (NL); University of Amsterdam (NL); University of Edinburgh (UK); Oxford University (UK); University of Sussex (UK); INRIA (F); SICS (S).
5. TRANSFER:
   CWI (NL); University of Amsterdam (NL); Leiden University (NL).
6. PVT: (a SION project)
   University of Amsterdam (NL); CWI (NL).

B. Contacts and/or cooperation with industry
Philips Research (NL), PTT-Research Neher Lab (NL), Shell Research (NL), Ipsys (UK), MARI (UK), Intracom (GR).

C. Contacts and/or cooperation with scientific institutes
SUNY at Stony Brook (USA), Aalborg University (DK), University Hildesheim (D), University Pisa (I), TU München (D), University Liège (B), MIT (USA), Stanford (USA).

6. Further activities 1987-1991

Dr. J.C.M. Baeten
Thesis supervisor of:
- A. Middeldorp (Free Univ., 1986);
- L. Kossen (Univ. of A'dam, 1987);
- R. Groenveld (Univ. of A'dam, 1987);
- W. Brouwer (Univ. of A'dam, 1990);
- H.P. Korver (Univ. of A'dam, 1990);
- W.P. Weijland (Univ. of A'dam, June 1989);
- J.F. Groote (Univ. of A'dam, Nov 1990).

Member of the reading committee:
- J.L.M. Vrancken (April 1991, Univ. of A'dam);
- H.R. Walters (June 1991, Univ. of A'dam).

Member of the promotion committee:
- F.W. Vaandrager (February 1990, Univ. of A'dam);
- J.C. Mulder (December 1990, Univ. of A'dam).

Editor of:
- Informatie (dutch magazine) since 1988.

Chairman of:
- The organisation committee of conference CONCUR'90, Amsterdam;
- The program committee of conference CONCUR'91, Amsterdam.

7. Experimental systems & programs 1987-1991
None.

8. Selected publications 1987-1991
1. J.C.M. Baeten & W.P. Weijland, Process algebra, Cambridge Tracts in Theoretical Computer Science 18, Cambridge University Press 1990.
2. J.C.M. Baeten (ed.), Applications of process algebra, Cambridge Tracts in Theoretical Computer Science 17, Cambridge University Press 1990.
3. J.C.M. Baeten & J.W. Klop (eds.), Proceedings of CONCUR'90, Amsterdam, Springer LNCS 458, 1990.

RESEARCH GROUP AP3
EXTENSIBLE PROGRAMMING ENVIRONMENTS

State of the group June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
prof.dr. P. Klint	group leader	0.6 fte	
J. Heering	researcher	1.0 fte	
Nonpermanent:			
drs. A. van Deursen	junior researcher	1.0 fte	since 01.08.90
drs. E.A. van der Meulen	researcher	1.0 fte	since 01.04.88
drs. J. Rekers	researcher	1.0 fte	
dr. H.R. Walters	researcher	0.8 fte	since 01.02.91
drs. J. Kamperman	researcher	1.0 fte	since 01.04.91
drs. F. Tip	researcher	1.0 fte	since 01.04.91
N.N.	researcher	1.0 fte	
External funding:			
1. ESPRIT project GIPE II			
prof.dr. P. Klint	group leader	0.4 fte	
J. Heering	researcher	0.6 fte	
drs. E.A. van der Meulen	researcher	0.5 fte	since 01.04.88
drs. J. Rekers	researcher	0.5 fte	
N.N.	researcher	1.0 fte	
2. ESPRIT project COMPARE			
prof.dr. P. Klint	group leader	0.2 fte	
dr. H.R. Walters	researcher	0.8 fte	since 01.02.91
drs. J. Kamperman	researcher	1.0 fte	since 01.04.91
drs. F. Tip	researcher	1.0 fte	since 01.04.91
3. NWO project Incremental Program Generators			
drs. A. van Deursen	junior researcher	1.0 fte	since 01.08.90
drs. E.A. van der Meulen	researcher	0.5 fte	since 01.04.88
drs. J. Rekers	researcher	0.5 fte	
Former staff members 1987-1991:			
dr. P.R.H. Hendriks	researcher	1.0 fte	until 01.01.91
drs. J.W.C. Koorn	on detachment	1.0 fte	01.09.88-01 09.89
drs. N.W.P. van Diepen	junior researcher	1.0 fte	until 31.03.88
drs. M.H. van Dijk	on detachment	1.0 fte	15.11.87-01.11.89
ir. M. Logger	on detachment	1.0 fte	until 31.12.87

2. Introduction

Purpose

The global goal of this research group is the automatic generation of programming environments from formal language definitions as well as the construction of an interactive meta-environment for developing such definitions. To this end, research is carried out in the following areas: algebraic specification of programming languages, incremental (interactive) development of modular language definitions, implementation of algebraic specifications, and lazy/incremental program generators.

Year of starting

The group was started in 1982.

Description of development

Programming environments are an aid for the software engineer and consist of collections of tools for constructing and processing programs. Earlier investigations in this project led us to the insight that the various *modes* in a programming environment (such as, e.g., subsystems for editing and debugging, each with its own command language) can be integrated into a single linguistic framework. This leads to systems with a higher consistency and lower complexity than conventional ones. However, in many applications it is desirable that the user can extend such a system with its own application languages. Even an integrated system gives little help under such circumstances: the implementation of a new application language and its supporting tools have to be constructed from scratch.

In this research group we investigate how the components of a programming environment can be generalized in such a way that the effort needed for adding a new language to it can be reduced drastically. For this purpose, the environment is based on *language definitions*, from which a syntax-directed editor, pretty printer, incremental typechecker and evaluator for the defined language can be derived automatically. The user who adds a language definition thus obtains automatically an environment for that particular language. It is important that new language definitions can re-use parts of already existing definitions. This avoids duplications and improves the uniformity of the system. Not surprisingly, modular language definitions play a prominent role in our research.

How should new languages be defined in such a system and how can these definitions be made operational? Various formalisms already exist for the definition of the syntactic aspects of languages (i.e. regular grammars for lexical syntax, context-free grammars for concrete syntax, and signatures for abstract syntax). These have been integrated in SDF (Syntax Definition Formalism), a formalism which has been developed in the context of this project. For the definition of semantics we have opted for the algebraic specification method. The reason being that such specifications are easily amenable to modularization and that many results from the area of term rewriting systems can be used for compiling them to an executable form. The specification language ASF (Algebraic Specification Formalism) has been developed for this purpose. These two formalisms have been combined into the single formalism ASF+SDF that allows the specification of all syntactic and semantic aspects of (programming) languages.

As we currently envisage, a language definition will primarily consist of the following parts:

1. A definition of concrete and abstract syntax of the language. A syntax-directed editor can be generated on the basis of this definition.
2. An algebraic definition of the *static semantics* of the language, from which an incremental typechecker will be derived.
3. An algebraic definition of the *dynamic semantics* of the language, from which an incremental evaluator and debugger will be derived.
4. Algebraic definitions of other operations on programs such as, for instance, dataflow analysis, compilation to another (lower-level) language, program transformations.
   It is unavoidable that some applications will require customizations of the standard user-interfaces that are generated in order to apply certain functions in the language definition to the whole program being edited (or to parts of it).

Typical examples are:

- providing a context-sensitive help function when filling in identifiers in programs;
- application of a program transformation to the program fragment currently in the focus of the editor;
- simulation of a concurrent process by rewriting a term describing that process, where potential choices in the development of the process are resolved by an interactive dialog with the user.

A specification language for describing such customizations is currently being designed.

The incremental development of language definitions and the generation of incremental tools from these definitions (parsers, typecheckers, interpreters, debuggers, etc.) form a promising area of research to which this project has already made several contributions. Currently, we have a prototype system running that supports the simultaneous interactive development of language definitions in ASF+SDF as well as experimentation with the environments generated for these languages.

Division in projects

The group is divided into three projects, each with a particular emphasis in the broad area of generating interactive environments from formal language definitions.

1. Generation of Interactive Programming Environments II (GIPE II). This ESPRIT project is a continuation of the GIPE I project and will last until 1-1-94.
2. Compiler Construction for Parallel Machines (COMPARE). This ESPRIT project has recently started (1-1-91) and will last three years with a possible extension of another year.
3. Incremental Program Generators (Special Programme NWO). This project started 1-5-90 and will last four years.

3. Research 1987-1991

a. Algebraic Specification Formalism (ASF): a formalism based on first-order signatures and conditional equations, and supporting modularity constructs like import, export, hiding, renaming and parameterization.

b. Module Algebra: a theoretical framework for the description and analysis of the semantics of modularity constructs.

c. Syntax Definition Formalism (SDF): a formalism for the definition of lexical, concrete and abstract syntax.
d. Lazy/incremental/modular program generation techniques: general techniques for incrementally adapting (as opposed to regenerating) the output of a program generator when its input is modified. Has been applied to scanner and parser generation.
e. ASF+SDF: a fully integrated algebraic specification formalism for the definition of both syntax and semantics of programming (and other) languages.
f. ASF+SDF meta-environment: a fully interactive development environment for ASF+SDF specifications. The language specific environment generated from the ASF+SDF specification can be used and tested in the same environment.

4. Plans for the future

The area we are working in is so rich that we see many interesting problems to be addressed in the future:
a. Generic treatment of error messages generated during typechecking.
b. Automatic calculation of the origin of program fragments (for the benefit of the animation of program execution, debugging, generation of error messages, etc.)
c. Generic treatment of input/output statements in interpreted programs.
d. Continuation of the work on the optimization of the code generation process for algebraic specifications.
e. Continuation of the research on deriving incremental implementations from given, non-incremental, language definitions.
f. Typechecking of *incomplete* programs.
g. Automatic generation of language-specific debuggers.
h. Application of the language definition formalism in various case studies, with the goal of studying particular languages features (e.g. concurrency, type systems based on inheritance) and application domains (e.g., proof editing, program transformations, simulation of parallel processes, compilation to parallel architectures).
i. Automatic generation of various tools (e.g., dataflow analysis, version management).
j. Application of partial evaluation techniques for the automatic generation of compilers.

5. Cooperation 1987-1991

A. Contract Research

1. ESPRIT project 1985-1990: Contract 348 (GIPE I: Generation of Interactive Programming Environments): 2 fte/year.
2. ESPRIT project 1989-1993: Contract 2177 (GIPE II: Generation of Interactive Programming Environments): 2 fte/year.
3. ESPRIT project 1991-1994: Contract 5399 (COMPARE: Compiler Construction for Parallel Architectures): 3 fte/year.
4. NWO Special Programme in Informatics (SPI): 1990-1994.
5. Incremental Program Generators: 2 fte/year.

B. Contacts and/or cooperation with industry

ACE, Amsterdam (M. de Lange, M. Schoorel, W. Wakker), BSO, Utrecht (J. Symes Harlequin, London: V. Goetcherian, C. Meldrun), IBM Research, Zürich (J.Gustafsson), Philips CAD Centre (Polak), SEMA, Paris (D. Clément), STERIA, France (C. Koutsoumallis), BULL, Sophia Antipolis, GIPSI, Paris (B. Mélese, X. Franc, G. Popovitch), PLANET, Athens (P. Moukas), PTT Telematics Laboratory, Groningen: (A. Terpstra, J. Wester), PTT Dr. Neher Laboratory, Leidsendam (W. Bouma, H. Luden).

C. Contacts and/or cooperation with scientific institutes

INRIA Sophia Antipolis (G. Kahn), INRIA, Rocquencourt (B. Lang, M. Jourdan), GMD, Karlsruhe (S. Jähnichen, H. Emmelmann), Programming Research Group, University of Amsterdam (J.A. Bergstra, J.W.C. Koorn), Software Engineering Research Centre, Utrecht (P.R.H. Hendriks), Universität des Saarlandes (R. Wilhelm), Universität Darmstadt (G. Snelting), University of Linköping (P. Fritzson), University of Nijmegen (M. van de Brandt), University of Utrecht (H. Vogt), University of Twente (A. Nijholt, K. Sikkel), University of Waterloo (N. Horspool), University of Wisconsin (T. Reps).

6. Further activities 1987-1991

Staff members act regularly as referees/program committee members for national and international conferences, journals, and organizations, of which we mention:
- European Symposium on Programming, 1988, Nancy, France;
- IFIP Conference 1989;
- Computing Science in the Netherlands, (annual);
- Transactions on Programming Languages and Systems;
- IEEE Transactions on Software Engineering;
- Theoretical Computer Science;
- NSF (National Science Foundation);
- NWO (Dutch National Research Organization);
- ESPRIT.

The whole group actively participates in giving courses:
- PAO course on software engineering;
- AvI course on algebraic specification;
- AvI course on syntax analysis;
- AvI course on syntax-directed editing;
- AvI course on static type analysis.

Prof.dr. P. Klint

- Part-time appointment as professor in Computer Science at the Programming Research Group, University of Amsterdam;
- One of the initiators and member of the board of the Software Engineering Research Centre (SERC), Utrecht;
- Director (with J.A. Bergstra) of the Software Technology School of the Academie voor Informatica (AvI);

- Member of various committees in the Dutch research organization for computer science (SION: WAR, WPA);
- Organiser (with T. Reps and G. Snelting) of an International Workshop on Programming Environments, to be held in Schloss Dagstuhl, Germany, March 9-13, 1992.

Promotor for the following Ph.D Thesis:
- V.J. de Jong, Conductor: a multilingual programming environment for statistical software, Ph.D. Thesis, University of Groningen, 1988 (first promotor: prof.dr. P. Klint, second promotor prof.dr. T.J. Wansbeek);
- J.L.M. Vrancken, Studies in Process Algebra, Algebraic Specification and Parallelism. Ph.D. Thesis, Programming Research Group, University of Amsterdam 1991 (first promotor prof.dr. J.A. Bergstra, second promotor: prof.dr. P. Klint).

7. Experimental Systems and Programs 1987-1991

1. ASF implementation:
   Batch-oriented software tool to support the writing of ASF specifications. It performs syntax analysis, typechecking and compilation of specifications to Prolog.
2. SDF implementation:
   Batch-oriented software tool to support the writing of SDF specifications.
3. Incremental Scanner Generator (ISG):
   A scanner generator that takes a regular grammar as input and generates a lexical scanner in LeLisp. The scanners are generated in a lazy fashion, i.e., only those parts are generated that are actually needed for scanning input. In addition, the original grammar can be modified by adding or deleting a regular expression. As a result, the generated scanner is updated (as opposed to being regenerated).
4. Modular Scanner Generator (MSG):
   A scanner generator extending ISG by allowing module selections: each regular expression is labelled with a module name and the generated scanner can be restricted to subsets of rules (by giving a list of enabled module names). This forms the basis for implementing modular regular grammars. Experimentally, this system has been extended for the matching of trees using finite automata.
5. Incremental Parser Generator (IPG):
   A parser generator that takes an SDF definition as input and generates a parser in LeLisp. These parsers are capable of parsing arbitrary context-free grammars. The parsers are generated in a lazy fashion, i.e., only those parts are generated that are actually needed for parsing input. In addition, the original SDF definition can be modified by adding or deleting rules. As a result, the generated parser is updated (as opposed to being regenerated).
6. Modular Parser Generator (MPG):
   A parser generator extending IPG by allowing module selections in a similar fashion as MSG.
7. Generic Syntax-directed Editor (GSE):
   A generic syntax-directed editor parameterized with the syntax of the language in which texts (programs) have to be edited. Provides a user-interface based on X-windows.

8. Equation Manager (EQM):
   Interactive system for the management, compilation and use of conditional equations. Uses various compilation techniques, to obtain fast rewriting systems.
9. Pretty Printer Generator (PPG):
   A tool to derive a prettyprinter from an SDF definition. Generates input for the Figue pretty printing system from INRIA.
10. ASF+SDF meta-environment:
    An interactive development system for writing ASF+SDF specifications. This system contains the stand-alone tools MSG, MPG, PPG, GSE and EQM listed above. In addition it contains new components for Module Management (interactive maintenance of complete specifications and their modular structure) and for handling of the top level user-interface of the system.

8. Selected publications 1987-1991

1. J. Heering, P. Klint & J. Rekers, Incremental Generation of Parsers, IEEE Transactions on Software Engineering 16 (12), pp. 1344-1351, 1990.
2. J.A. Bergstra, J. Heering & P. Klint (eds) Algebraic Specification, The ACM Press Frontier Series, Addison-Wesley 1989.
3. P. Klint (1990), A meta-environment for generating programming environments, CWI Report CS-R9064.

RESEARCH GROUP AP4
ALGEBRAIC AND SYNTACTIC METHODS
State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
prof.dr. J.W. Klop	group leader	0.7 fte	
Nonpermanent:			
dr. A. Middeldorp	researcher	1.0 fte	since 01.09.89
dr. F.J. de Vries	researcher	1.0 fte	since 01.01.89
External funding:			
1. ESPRIT BRA INTEGRATION			
prof.dr. J.W. Klop	group leader	0.1 fte	
dr. A. Middeldorp	researcher	0.7 fte	
2. ESPRIT BRA SEMAGRAPH			
prof.dr. J.W. Klop	group leader	0.3 fte	
dr. F.J. de Vries	researcher	0.7 fte	
3. ESPRIT BRA CONCUR			
prof.dr. J.W. Klop	group leader	0.1 fte	
Former staff members 1987-1991:			
dr. Y. Toyama	guest researcher		01.09.90-01.09.91

2. Introduction

Purpose
Foundational research centering around term rewriting systems, with an emphasis on algebraic and syntactic methods; foundational research in process algebra.

Year of starting
The group was started January 1, 1989.

Description of development

The research group has started January 1, 1989, initially with a staff consisting of prof. dr J.W. Klop (group leader), 0.7 part time; drs. R.J. van Glabbeek (junior researcher, Ph.D. student); dr F.-J. de Vries (post-doc). In September 1989 the group was extended with drs. A. Middeldorp, Ph.-D.student ('aio') in his last year at the Free University and on assignment to CWI for 0.8 part time. Van Glabbeek left the group December 1, 1989, after completion of his Ph.-D. Thesis. Last year Dr. M. Bezem joined the group (June 1, 1990), sponsored (0.8) by the SION project 'Typed Lambda Calculi', but he left the group at March 1, 1991. From September 1990 the group includes for one year Dr. Y. Toyama (NTT Basic Research Labs, Tokyo) as a guest researcher, supported mainly by NTT and partly by NWO. Most of the work in AP4 was and is performed in the framework of ESPRIT contracts. Van Glabbeek worked full-time under auspices of ESPRIT project METEOR; next to local management work for this project he completed his Ph.D. Thesis (May 1990) containing a comparative study of various process semantics. Van Glabbeek's contract with CWI ended December 1, 1989; also the project METEOR had finished by that time (October 1989). Klop and De Vries took part in METEOR with a small part-time factor during the first half year of 1989. Medio 1989 some new ESPRIT projects have started, in the framework of the Basic Research Actions, in which AP4 participates in cooperation with some other research groups of AP. July 1989 was the start of BRA projects SEMAGRAPH (Klop 0.3; De Vries 0.7) and INTEGRATION (Klop 0.1; Middeldorp 0.7). September 1989 was the start of BRA project CONCUR (Klop 0.1). In INTEGRATION AP4 is cooperating with AP1 (De Bakker et al.) and AP5 (Apt et al.); in CONCUR there is cooperation with AP2 (Baeten et al.).

Division in projects

Summarizing, the projects that AP4 is involved in are listed below:

1. AP4.1 INTEGRATION:
   (Integrating the Foundations of Functional, Logic and Object-Oriented Programming)
   Start date: 89.07.01. End date: 91.12.31.
   Financed externally by ESPRIT BRA.
   Project members:

prof.dr.J.W. Klop	project leader	0.1 fte
dr. A. Middeldorp	senior researcher	0.8 fte

2. AP4.2 SEMAGRAPH:
   (Semantics and Pragmatics of Generalised Graph Rewriting)
   Start date: 89.07.01. End date: 91.12.31.
   Financed externally by ESPRIT BRA.
   Project members:

prof.dr. J.W. Klop	project leader	0.3 fte
dr. F.J. de Vries	senior researcher	0.7 fte
dr. Y. Toyama	senior researcher	consultant

3. AP4.3. CONCUR:
   (Theories of Concurrency: Unification and Extension)
   Start date: 89.09.01. End date: 91.08.31.
   Financed externally by ESPRIT BRA.

Project members:

prof.dr. J.W. Klop	project leader	0.1 fte

3. Research 1989 - 1991

A. Background

The objective of AP4 is to perform foundational research in the field of (primarily but not exclusively) term rewriting systems. This extends to theoretical applications in the field of process algebra (in cooperation with AP2, Concurrency & Real Time Systems), as well as in logic programming (in cooperation with AP5, Logic and Language). The primary theme of AP4, term rewriting systems (TRSs), and the secondary themes, process algebra and logic programming, are not unrelated. Investigations in all subjects strictly adhere to the algebraic-axiomatic methodology. Just as TRSs are nothing else than equational axiom systems with oriented equations, the core of process algebra consists of a family of (mainly) equational axiom systems, which have been explicitly designed to be amenable for a term rewriting analysis. This ensures both the possibility for rigorous proofs of consistency of axiomatizations and the possibility - in principle - of a further development towards executability (and thus, in the long run, towards mechanical tools assisting in manipulating process expressions and system specifications).

We now discuss in more detail the scientific relevance of the theme of term rewriting systems.

a. TRSs are a theoretical tool to analyze abstract data type specifications or algebraic specifications (consistency properties, computability theory, decidability of word problems, theorem proving).
b. TRSs provide the foundation for functional programming. Historically, the paradigm TRSs Combinatory Logic and Lambda Calculus served to formalize the concept of computable or recursive number theoretic function; especially the Lambda Calculus has been viewed as a rudimentary functional programming language. Several functional programming languages have been based on Lambda Calculus or Combinatory Logic, starting with LISP and recently Miranda. Theory about TRSs, concerning for instance evaluation strategies, has proved to be of direct relevance in a proper understanding of existing functional language features as well as in the design of new functional languages; especially the relation between term rewriting and 'term graph rewriting' is of importance here (this is the substance of BRA project SEMAGRAPH, see below).
c. Recently, there is a surge of interest in combining the functional programming style and the logic programming style. Various proposals are being developed at many research sites for integrating the concepts of term rewriting and 'resolution', the main derivation method in logic programming. An important link between term rewriting and logic programming is given by conditional TRSs. A conditional TRS can be viewed as a logic program defining an equality relation, which can serve as the underlying equality of some other logic program. (This is the substance of part of the BRA project INTEGRATION, see below).

B. Research results

We now present a short report of the work done by AP4 in each of the three BRA projects.

INTEGRATION:
Participation by AP4 follows two main lines. Together with K.R. Apt (AP5) and C. Palamidessi (guest researcher in AP5) the present project group, in particular Klop and Middeldorp, endeavours to compose an extensive survey and systematization of numerous known results in the area of 'Equational Logic Programming'. ELP is a framework that aims at an integration of (the foundations of) functional programming and logic programming; with respect to the component of functional programming it turns out that conditional term rewriting systems play a key role. This last fact leads to the second and more specific main line of investigation, with A. Middeldorp as primary researcher: the study of modular properties of term rewriting systems, in particular conditional ones. A key result here is Middeldorp's generalization of Toyama's classical theorem stating that confluence is a modular property for (unconditional) term rewrite systems, to the larger class of conditional term rewrite systems (CS-R8944). Other related results by Middeldorp have been reported in CS-R8959 and CS-R9003. Middeldorp's research is collected in his Ph.D. Thesis (Nov. 1990).

SEMAGRAPH:
The task of AP4 is to study to what extent the existing body of theory about term rewrite systems can be generalized or adapted to term graph rewriting. Term graph rewriting is a technique involving sharing of subterms that is of major importance for implementations of functional program languages for reasons of efficiency and feasibility of computations. Also, term graph rewriting introduces infinite terms, as unwindings of cyclic term graphs. A start was made with a study of infinitary term rewriting (where rewrite sequences may have as length an arbitrary ordinal) and infinitary normal forms. Infinitary normal forms arise naturally as the output of programs in a functional programming language. In this study AP4 cooperates with the University of East-Anglia (Norwich), where the initiator and project manager of SEMAGRAPH, prof. M.R. Sleep, is located. A surprising discovery of this research was that confluence for orthogonal term rewrite systems does not generalize to the transfinite setting, although the normal form property does generalize. Subsequently it was found that the failure of infinitary confluence for orthogonal rewriting is only marginal, and can be located to a small class of 'bad'terms.

CONCUR:
The only participant of AP4 in this project is J.W. Klop (0.1 part time), who acted as Program Committee Chairman for the international conference CONCUR 90, at the end of year 1 (August 1990), with theme: 'Theories of Concurrency: Unification and Extension'. Together with Baeten (AP2, general project manager of CONCUR) conference proceedings have been edited.

Other work (not in ESPRIT BRA framework):
Dr. F.J. de Vries has performed together with Prof. J. van Eijck (AP5, Logic and Language) a study aiming at the application of process algebra techniques in order to formulate a semantical theory for natural languages. More about this work can be found in the analogous document of AP5. This work is another example of a fruitful interaction between the various research groups in our department AP.

4. Plans for the future

General prospects

Recent years show a strong and growing interest in term rewriting, both with respect to foundational or more theoretical aspects as well as aspects of application. This observation is substantiated by the emergence of workshops and conferences devoted exclusively to term rewriting, such as the RTA (Rewriting Techniques and Applications) conferences and the CTRS (Conditional and Typed Rewrite Systems) workshops. As a side remark we mention that this is also visible with respect to the educational side of computer science: most of the introductory books on functional programming that have appeared the last two or three years contain substantial theory sections treating lambda calculus and combinatory logic, or even categorical combinatory logic (CCL). It is to be expected that in a few years the same can be said for theory about general term rewriting. At present, the work done in this group has at present good fund raising capabilities-most of the work is sponsored by external contracts (75 - 80%). Of course no guarantee can be given or should be expected that this state of affairs will continue over a long period.

Specific plans

INTEGRATION:
Working plan remainder of 1991. Future research in this framework will be the continuation of the ELP survey as well as continuations of Middeldorp's work. Working plan after 1991. Depending on funding of an extension of INTEGRATION.

SEMAGRAPH:
Working plan remainder of 1991. As to future work by AP4 in SEMAGRAPH, the intention is to follow up the research of 1990, laying the foundations of infinitary rewriting, by a similar foundational study of term graph rewriting, which in part rests upon the results obtained for infinitary rewriting. A typical topic that will be considered is establishing the modularity of some basic concepts of rewriting, confluence and termination, for term graph rewriting with cycles, generalizing some results by german researchers. Here AP4 is profiting from the presence, as guest researcher, of Dr. Toyama, who originated the study of modular properties in term rewriting. Working plan after 1991. Depending on funding of an extension of SEMAGRAPH.

CONCUR:
After completion of the first round of ESPRIT BRA CONCUR (end 1991), it is envisaged that AP4 will no longer participate in possible continuations of this project, due to developments in the research group AP2 (among which the probable departure of the group leader of AP2, J.C.M. Baeten), as well as due to the small size of the present group and the relatively many projects that we are involved in, or will be. New initiatives are presented now.

Parallelism and Lambda Calculi (BRA II proposal):
AP4 is participating in a new BRA II proposal in cooperation with french researchers (Curien, Lévy, Boudol, et al.) and english researchers (Milner, Abramsky, et al.) concerning 'concurrent lambda calculi', in an attempt to formulate systems that extend lambda calculus on the one hand and on the other hand are able to embed process algebras. In case of success, CWI participation will be 1 fte.

Other work:
AP4 is participating with a number of european researchers in a proposal for a Working Group Equational Theories and Applications (ETA). Although not as profitable as a BRA project, granting this proposal will yield some means for travel and international contacts.
AP4 has submitted in May 1991 a project proposal with WTI-SION (the working group Theoretical Computer Science of the Stichting Informatica Onderzoek Nederland), for one OIO (junior researcher) during 4 years, concerning the investigation of syntactic aspects of extensions of lambda calculi and related calculi.

5. Cooperation 1989-1991

A. Contract research
ESPRIT BRA partners
1. INTEGRATION:
   CWI, CAIMENS (France), Imperial College (UK), UNINOVA (Portugal), Univ. of Pisa, Philips Research Labs.
2. SEMAGRAPH:
   Univ. of East Anglia, CWI, ICL (Manchester), Imperial College, Catholic Univ. of Nijmegen, LIENS (Paris).
3. CONCUR:
   CWI, Univ. of Amsterdam, Univ. of Edinburgh, Oxford Univ. Univ. of Sussex, INRIA, SICS (Swedish Institute for Computer Science).

B. Contacts and/or cooperation with industry
NTT Basic Research Laboratories Tokyo (dr. Y. Toyama Hitachi), Advanced Research Laboratory (dr. A. Takano).

C. Contacts and/or cooperation with scientific institutes
Univ. of Amsterdam (prof. dr. J.A. Bergstra), Univ. Leiden (prof. dr. G. Rozenberg), Catholic Univ. Nijmegen (prof. dr. H.P. Barendregt, dr. R. Plasmeyer), Free University of Amsterdam (drs. V. van Oostrom, dr. R.C. de Vrijer, prof. dr. J.-J. Ch. Meyer), Univ. of Utrecht (prof. dr. D. van Dalen, dr. A. Visser), University of Illinois, Urbana (prof. dr. N. Dershowitz), Concordia University, Montreal (prof. M. Okada), INRIA Rocquencourt, prof. P.-L. Curien (dr. Th. Hardin, prof. J..J. Lévy), University of East Anglia, Norwich (prof. M.R. Sleep, dr. J.R. Kennaway), University of Edinburgh (prof. R. Milner, dr. F. Moller, dr. J. Power), Univ. of Cambridge (dr. T. Nipkow), University of Oldenburg (prof.dr. E.-R. Olderog), Univ. di Pisa (dr. C. Palamidessi), Stanford University (dr. R. van Glabbeek), MIT Boston (dr. F.W.

Vaandrager, prof. A. Meyer, prof. Arvind), DAIMI Aarhus (prof. G. Winskel), University of Tblisi (dr. Z. Khasidashvili), Power Institute Moscow (dr. Y. Korablin), Univ. di Milano (dr. N. Sabadini), Univ. Hildesheim (prof. dr. E. Best), ETL Tsukuba (dr. K. Futatsugi), Hebrew Univ.(Givat Ram, dr. S. Kaplan), Tata Institute, Bombay (prof. R.K. Shyamasundar, dr. P.S. Subramanyan).

6. Further activities 1989-1991

Prof.dr. J.W. Klop

- Part-time (0.3) professor in Applied Logic at the Free University of Amsterdam. Although this is strictly speaking not an activity in AP4, there is an obvious symbiosis;
- Finishing a chapter 'Term Rewriting Systems' in the Handbook of Logic in Computer Science (eds. Abramsky, Maibaum and Gabbay, Oxford Univ. Press), Vol.2, to appear 1991. The chapter contains a 140 page introductory survey of term rewriting, and will be, in cooperation with Dr R. de Vrijer (Free University Amsterdam) extended to a monograph scheduled to appear with Cambridge University Press;
- Participated as lecturer in some AvI- and PAO-courses (AvI = Academy for Informatics, PAO = Post-Academic Education). J.W. Klop taught a course on TRSs in the 2nd summer school Language, Logic and Information (August 1990) which was organized in the ERASMUS framework of cooperating European universities;
- From January 1, 1989, secretary of the WTI-committee (Werkgemeenschap Theoretische Informatica), including an editorship of the WTI Newsletter;
- Program Chairman of the conference CONCUR 90 (August 1990, Amsterdam), including (together with J.C.M. Baeten) editor of the conference proceedings;
- Co-conference chair for the international conference LICS 91 (Logic in Computer Science), to be held in July 1991 in Amsterdam. This also involves a membership of the Organizing Committee of LICS;
- Member of the Steering Committee of ETA, the Working Group in spe 'Equational Theories and Applications' mentioned above;
- Member of the Program Committees of ICALP 92, CAAP-TAPSOFT 92, ALP 92;
- Ph.D. thesis supervision: R. Wieringa (May 1990; referent), R. van Glabbeek (May 1990, promotor together with J.A. Bergstra), A. Middeldorp (Nov. 1990; promotor), V. van Oostrom (in preparation).

Dr. A. Middeldorp

Participated as lecturer in some AvI- and PAO-courses (AvI = Academy for Informatics, PAO = Post-Academic Education). J.W. Klop taught a course on TRSs in the 2nd summer school Language, Logic and Information (August 1990) which was organized in the ERASMUS framework of cooperating European universities.

Dr. F.J. de Vries

Organised PSSL 46 (the 46th meeting of the Peripatetic Seminar on Sheaves and Logic) in March 1991 at the CWI.

Other activities in 1989 and 1990 such as giving invited courses, membership of promotion committees, conference lectures will not be mentioned here (see Annual Reports CWI).

7. Experimental Systems and Programs 1989-1991
None.

8. Selected publications 1989-1991
1. A. Middeldorp (1990). Modular Properties of Term Rewriting Systems. Ph.D. Thesis, Vrije Universiteit, Amsterdam 1990.
2. J.W. Klop (1990), Term rewriting systems, CWI Report CS-9073. To appear in slightly shorter form as chapter in the Handbook of Logic in Computer Science (eds. Abramsky, Maibaum & Gabbay), Vol.2, Oxford Univ. Press, 1991.
3. J.R. Kennaway, J.W. Klop, M.R. Sleep and F.J. de Vries (1990). Transfinite reductions in orthogonal term rewriting systems (Full paper), CWI Report CS-R9041.

RESEARCH GROUP AP5
LOGIC AND LANGUAGE

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

Prof. dr. K.R. Apt	group leader	1.0 fte	since 01.03.87
Prof. dr. M. Moortgat	researcher	0.2 fte	since 01.12.90

Nonpermanent:

drs. E. Marchiori	guest researcher	1.0 fte	07.02.91-07.08.91
drs. W. Meyer Viol	junior researcher	1.0 fte	since 01.01.91
J. Villadsen	guest researcher	1.0 fte	01.03.91-30.09.91

External Funding:

1. ESPRIT II Basic Research Action 3020 Integration:
   - Prof.dr. K.R. Apt — project leader
   - drs. R. Bol — junior researcher
   - dr. C. Palamidessi — guest researcher
2. Non-monotonic Reasoning and Semantics of Natural Languages (Project sponsored by OTS Utrecht):
   - Prof.dr. J. van Eijck — researcher
   - drs. W. Meyer Viol — junior researcher
3. Structural and Semantic Parallels in Natural Languages and Programming Languages (NFI Project NF 102/62-356):
   - Prof.dr. M. Moortgat — researcher

Former staff members 1987-1991:

Prof. dr. J. van Eijck	researcher,	1.0 fte	01.11.89-01.12.90
drs. R. Bol	junior researcher	1.0 fte	01.10.87-01.10.91
dr. C. Palamidessi	guest researcher	0.2 fte	01.08.90-31.12.91
Dr. H. Walinska	guest researcher	1.0 fte	01.04.89-01.04.90
D. Turi	junior researcher	1.0 fte	01.05.89-01.11.89
Dr. M. Bezem	researcher (mostly)	0.8 fte	01.06.88-01.06.90

2. Introduction

Purpose

The group's research comprises logic programming, deductive and knowledge-based database systems, program verification, non-monotonic reasoning, natural language processing and the parallels between natural and programming languages.

Year of starting
The group was started in 1987.

Global prospects
The research carried out in this group lies in the areas of computer science marked by international and interdisciplinary character. This can be witnessed by several joint publications with researchers from other countries. The existing possibilities for external financing have been so far successfully utilized.

Division in projects
The research of the group naturally divides into two projects. The first one concerns logic programming, deductive and knowledge based database systems and is led by Prof. dr. K.R. Apt. The second one concerns natural language processing and the parallelsbetween natural and programming languages and is led by Prof. dr. J. van Eijck. Both projects involve research on program verification and non-monotonic reasoning.

3. Research 1987-1991

a. Logic programming

The main thrust of our research since 1989 was the study of termination of logic and Prolog programs. First, we investigated which natural conditions imposed on on logic programs and goals ensure termination. To this end in total four classes of logic programs were investigated by Apt, Bezem, and Pedreschi (University of Pisa):
- those which terminate for all ground goals for all selection rules;
- those which terminate for all ground goals for the Prolog selection rule and two corresponding classes of programs allowing negative literals in the bodies.

For each class of programs a simple and complete method of proving termination was provided and illustrated by some natural examples. It was argued these classes of programs comprise most natural logic and pure Prolog programs. Also it was investigated how infinite derivations can be stopped by modifying the underlying interpreter of logic programs. Apt, Bol and Klop (AP4) made in 1988 and 1989 a systematic study of a number of natural loop checking mechanisms was made concentrating on the subject of their soundness (no solution is lost), completeness (all infinite derivations are pruned), relative strength and related properties. Once the basic definitions of loop checking were firmly set, Bol studied in 1990 and 1991 generalizations, alternative applications and implementation issues of loop checking mechanisms.

- Bezem, Bagai and Van Emden (University of Victoria, Canada) studied downward closure ordinals of logic programs;
  Apt wrote a systematic introduction to logic programming which recently appeared in the Handbook of Theoretical Computer Science;
- Turi proposed in 1990 a new type of semantics for general logic programs based on the use of non-ground atoms.

b. Deductive databases
Two forms of computing which are used in deductive databases (DDB in short) - top down and bottom up computing were studied in detail. Animplementation of top down computing formed one of the motivations for the above reported work on loop checking. Also Apt systematically derived best known algorithms for the bottom computing.

c. Non-monotonic reasoning
Apt and Blair (University of Syracuse) studied the arithmetical complexity of the perfect model of stratified logic programs and various known formalisms for non-monotonic reasoning. Apt and Bezem applied their study of the terminating general logic programs to formalize temporal reasoning, a special form of non-monotonic reasoning exemplified by the so-called Yale Shooting Problem, by means of logic programming.

d. Program verification
Apt, Francez and Katz (Technion, Haifa) provided a systematic study of the notion of fairness for various models of distributed computing. Apt and Olderog (University of Oldenburg) finished their book on program verification. It treats in a uniform framework both sequential and concurrent programs. A large portion of the material is entirely new, in particular the use of program transformations for program verification. In the book they systematically discuss deterministic and nondeterministic programs, parallel programs with shared variables, and distributed programs with message passing, concentrating in each case on operational semantics, syntax-directed assertional proof systems and their soundness proofs, program transformations and their correctness proofs, and a correctness proof of a substantial example. In particular, solutions to the classical problems of consumer/producer, mutual exclusion and distributed termination are discussed and proved correct.

e. Natural language processing
In April 1989, work on natural language understanding has started. The focus of attention of work of a guest researcher H. Walinska was the study of verb formation of so-called "zero-headed" English verbs and an extensive comparison of English and Slavic verbal prefixation. In 1989 and 1990 the focus of the work of van Eijck has been on the semantics of quantification in natural language. Several overview papers on quantifiers and determiners were completed; research on quantifiers in partial models and on dynamic aspects of quantification was started. In particular Van Eijck and de Vries (AP4) proposed a Hoare style proof system allowing us to reason about sentences involving dynamic interaction of quantification and description. The focus of the work of Moortgat has been the development of categorial grammar formalisms, with prototype implementations in Prolog. Relations between categorial systems and substructural logics (linear logic, relevance logic) were studied. Polymorphic type inference mechanisms were devised to handle underspecified typing in categorial grammars.

4. Plans for the future
The project led by K.R. Apt plans to study the verication of Prolog programs using the declarative means and to study the computational aspects of the non-monotonic reasoning.

The project led by J. van Eijck plans to study the non-monotonic aspects of the use of generic expressions in natural language and pursue research on structural and semantic parallels in natural language and programming language analysis.
Also, further work on the relation between categorial grammar formalisms and substructural logics is envisaged.

5. Cooperation 1987-1991

A. Contract Research - see 1

B. Contacts and/or cooperation with industry

Since 1987 regular scientific contacts are maintained with the group of Dr. J.L. Lassez at the IBM Research Center, Yorktown Heights, USA. In 1988 Dr. J. Jaffar from this Center visited our group for 3 weeks.

C. Contacts and cooperation with scientific institutes

Prof. K.R. Apt was associated during the period 1987-1991 with the University of Texas at Austin, USA, where he was the William B. Blakemore II Professor of Computer Sciences. In the first semester of 1991 he was a Visiting Professor at the University of Leuven, Belgium.

Prof. J. van Eijck is associated for 0.2 time as Professor of Linguistics with the Institute OTS of the University of Utrecht.

Prof. M. Moortgat is associated for 0.8 time as Professor of Linguistics with the Institute OTS of the University of Utrecht.

The scientific contacts of the group, apart of those resulting from the participation in the already mentioned projects include: University of Syracuse, Syracuse, USA (Prof. H. Blair), IBM Research Center, Yorktown Heights, USA (group of Dr. J.L. Lassez), University of Victoria, Canada (Prof. M. van Emden), University of Oldenburg, West Germany (Prof. E.-R. Olderog), University of Bristol, Great Britain (Profs. J. Lloyd and J. Shepherdson), Applied Logic Section, Free University of Amsterdam (Prof. J.J.C.C. Meyer), Logic and Computation Section (ITLI), University of Amsterdam (Prof. J. van Benthem, Prof. P. van Emde Boas, Dr. T.M.V. Janssen), Philosophical Logic Group at the State University of Utrecht (Dr. M. Bezem, Dr. A. Visser), SRI International Cambridge Computer Science Research Centre, Cambridge, UK (Dr. S. Pulman, Dr. H. Alshawi).

6. Further activities 1987-1991

Prof.dr. K.R. Apt
Member of Editorial boards:
- Science of Computer Programming, since 1981;
- RAIRO, Theoretical Informatics, since 1982;
- Information and Computation, since 1987;

- Journal of Logic and Computation, since 1989;
- Wiley/Teubner Series in Computer Science, since 1989;
- Fundamenta Informaticae, since 1990.

Member of International Initiatives and Boards:
- IFIP Working Group 2.2 (Formal Description of Programming Concepts), since 1981;
- Scientific Board of INRIA (Institut National de Recherche en Informatique et en Automatique), France, since 1989;
- Scientific Commission for Computer Science of the Belgian National Fund for Scientific Research, since 1990;
- European Network in Computational Logic (initiated by the ESPRIT Basic Research Action "Compulog"), since 1991;
- Executive Committee of the Association for Logic Programming, since 1991.

Program Committee memberships:
- Fundamentals of Computation Theory (FCT '87), Kazan, USSR, June 1987;
- Principles of Database Systems (PODS '88), Austin, U.S.A., March 1988;
- Principles of Distributed Computing (PODC '88), Toronto, Canada, August 1988;
- International Conference on Logic Programming, Lisbon, June 1989;
- Logic in Computer Science (LICS '90), Philadelphia, U.S.A., June 1990;
- Principles of Distributed Computing (PODC '90), Quebec, Canada, August 1990;
- Journées Europèennes sur la Logique en Intelligence Artificielle (JELIA '90), Amsterdam, The Netherlands, September 1990;
- North American Conference on Logic Programming, Austin, U.S.A., October 1990;
- Logic in Computer Science (LICS '91), Amsterdam, The Netherlands, July 1991;
- 18th International Conference on Automata, Languages and Programming (ICALP '91), Madrid, Spain, July 1991;
- Mathematical Foundations of Computer Science (MFCS '91), Poland, September 1991;
- International Workshop on Logic Programming and Non-Monotonic Reasoning, Washington, U.S.A., July 1991.

Invited speaker:
- Symposium on Artificial Intelligence, University of Amsterdam, The Netherlands, April 1987;
- Interdisciplinary Conference on Axiomatic Systems, Columbus, Ohio, U.S.A., December 1988;
- Italian Association in Logic Programming, Bologna, Italy, June 1989;
- Presentation of a tutorial, Very Large Data Bases, Amsterdam, The Netherlands, August 1989;
- Conference on Theories of Partial Information, Austin, U.S.A., January 1990;
- Conference on Logic and Computer Science, Luminy, France, June 1990;
- Workshop on Non-Monotonic Reasoning and Logic Programming, Austin, U.S.A., November 1990;

- Symposium on Computational Logic, 7th ESPRIT Conference, Brussels, Belgium, November 1990.

Lecturer during International Schools:
- UNESCO and IFIP Course "Formal Description of Programming Concepts", Rio de Janeiro, Brazil, April 1989;
- Summer School of the Italian Association in Logic Programming, Alghero, Italy, September 1990;
- Logic Programming School (LOP '91), Rupechtov, Czechoslovakia, January 1991.

Other professional activities:
- Speaker in the Distinguished Lecturer Series, University of Maryland, U.S.A., November 1987;
- Organizer of the Symbolic Computing Day, CWI, Amsterdam, The Netherlands, April 1988;
- Speaker in the Distinguished Lecturer Series, University of California, San Diego, U.S.A., December 1988;
- Advisor of the Handbook of Logic in Artificial Intelligence and Logic Programming Project, since 1989;
- Member of the Advisory Committee, International Conference on Knowledge Based Computer Systems, Bombay, India, December 1989;
- Guest editor, special issue of Fundamenta Informaticae on Logic Programming, 1990;
- Co-organizer of 2nd BENELOG - 2nd Benelux Meeting on Logic Programming and PROLOG, Amsterdam, The Netherlands, September 1990;
- Member of the Advisory Committee, International Conference on Knowledge Based Computer Systems, Bombay, India, December 1990.

Prof.dr. D.J.N. van Eijck
Program Committee membership:
- Journées Europeènnes sur la Logique en Intelligence Artificielle (JELIA '90), Amsterdam, The Netherlands, September 1990.

Editorship:
- Proceedings of the Conference Journées Europeènnes sur la Logique en Intelligence Artificielle (JELIA '90), Lecture Notes in Computer Science, Springer-Verlag, vol. 478, 1991.

Invited speaker:
- CompEuro 1989, Hamburg;
- 3rd Symposium on Logic and Language, Revfulop (Hungary), August 1990.

Lecturer during International Schools:
- Second European Summer School in Language, Logic and Information, Louvain 1990;
- Third European Summer School in Language, Logic and Information, Saarbruecken 1991.

Colloquium organization:
- Organizer of the Amsterdam 'Parallels' Colloquium.

Dr. M. Bezem
Program Committee memberships:
- Journeés Europeènnes sur la Logique en Intelligence Artificielle (JELIA '90), Amsterdam, The Netherlands, September 1990.

Colloquium organization:
- Coorganizer of the "Algemeen" CWI Colloquium.

M. Moortgat
Lecturer during International Schools:
- Second European Summer School in Language, Logic and Information, Louvain 1990;
- Third European Summer School in Language, Logic and Information, Saarbruecken 1991.

Invited speaker:
- A series of lectures at the Indiana University, Bloomington, Dec. 1990;
- Categorial logics: a computational perspective, Keynote address, Computing Science in the Netherlands 1990;
- Types, terms and strings: a sign-based perspective on categorial deduction, ASL/LSA Conference on Logic and Linguistics. Santa Cruz, July 1991.

Colloquium organization:
- Organizer of the Colloquium "Categorial Grammar", OTS, University of Utrecht.

7. Experimental systems and programs 1987-1991
None.

8. Selected publications 1987-1991
1. K.R. Apt, Logic programming, Handbook of Theoretical Computer Science, Vol. B, (J. van Leeuwen, ed.), Elseviers, pp. 493-574 (1990).
2. R.N. Bol, K.R. Apt and J.W. Klop, An analysis of loop checking mechanisms for logic programs, Theoretical Computer Science, in press.
3. J. van Eijck, F-J. de Vries, Dynamic interpretation and Hoare deduction, Tech. Report CS-R9115, presented at the Conference "Semantics and Linguistic Theory", Cornell University, April 1991, submitted for publication.

RESEARCH GROUP AA1
ALGORITHMS AND COMPLEXITY

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

Prof.dr.ir. P.M.B. Vitányi	group leader	0.8 fte	
Dr. E. Kranakis	project leader	1.0 fte	

Nonpermanent:

Drs. J.T. Tromp	junior researcher	1.0 fte	since 01.06.89

External Funding:

Realized recently:

- 1989 100 kfl SPIN-project, projected for 1990, 1991, 1992: 100 kfl, 1993: 25 Kfl;
- CNRS France, and NWO stipends for short-term visitors and long-term vistors (e.g. prof. P. Clote);
- Netherlands-France bilateral exchange grants;
- NSERC International Scientific Exchange Award ISE0046203;
- NUFFIC Israel-Netherlands exchange award.

Applied for:

- SION/NWO for two oio's (junior researchers) in Distributed Computing and Computational Learning Theory, respectively;
- NFI (National Facility Computer Science) proposal together with University of Utrecht (Prof. J. van Leeuwen) for a larger project in Distributed and Parallel Computing involving 6 oio's and postdocs and one full time foreign expert possibly split over several persons, and overhead: run time 4 years;
- Initiator/Coordinator and main Contractor of an ESPRIT BRA II Consortium in Computational Learning Theory involving over 10 sites in Europe, including: Amsterdam (P. van Emde Boas, P. Vitányi), Saarbruecken (W. Paul, R. Solomonoff), Rome (M. Protassi), Barcelona (J. Balcazar), Dortmund (I. Wegener, J. Simon), London (N. Biggs, J. Shawe-Taylor), Graz (W. Maass), Helsinki (E. Ukkonen, M. Pekkonen), Harvard (L. Valiant), Waterloo (M. Li), and so on, involving at CWI and University of Amsterdam 3-4 oio/postdocs and overhead.

Former staff members 1987-1991:

Prof.dr. P. Clote	guest researcher	1.0 fte	01.01.91-15.05.91
L. Kirousis	guest researcher		
G. Kissin	guest researcher		
D. Krizanc	guest researcher		
A.K. Lenstra	junior researcher		

2. Introduction

Purpose

Information is processed using algorithms. We can distinguish three phases: design and analysis of algorithms, implementation of algorithms, semantics and correctness of implementations. The purpose of this group is the analysis and design of algorithms, currently aimed at distributed computing, descriptional complexity and learning theory, and study of their complexity aspects.

Year of starting

The group was started in 1981.

Description of development

In the early eighties the stress was at machine complexity and computational number theory. Some of the results obtained were as follows. In machine complexity (Vitányi) two well-known open problems of at least 20 years standing were solved: real-time simulation of many independent counters on-line by a one tape Turing machine (STOC82, SICOMP85, JACM88 with J. Seiferas); and a square lower bound on the on-line simulation time of k-tape Turing machines by one-tape Turing machines, and many such results, using Kolmogorov complexity (e.g., INF&COMP88 with M. Li; SICOMP with L. Longpre and M. Li). In computational number theory (A.K. Lenstra) it was shown that factorization of polynomials over the radicals into irreducible factors can be performed in deterministic polynomial time: the Lenstra-Lenstra-Lovasz paper (ANN. MATH.82). A.K. Lenstra left for Univ. of Chicago.
In the middle eighties attention of the group (E. Kranakis, L. Kirousis, P. Vitányi) shifted to distributed and parallel computing. Some highlights: novel leader election algorithms and a real-time model of asynchronous distributed computation (STOC84); realistic parallel models and lower bounds for VLSI computation (FOCS85); first solution to multi-user concurrent wait-free atomic variable (FOCS86 with B. Awerbuch); general framework problem for distributed nameserver, mutual exclusion, routing in the form of the paradigm 'distributed match-making' (PODC85 with S. Mullender).
At the end of the eighties, we explored various aspects of concurrent wait-free objects, including one of the first solutions to the wait-free concurrent multiwriter variable construction (WDAG87) and formal proof systems for such objects (FST&TCI88 with B. Awerbuch).
Previous bounded solutions to the multiwriter problem being erroneous (FOCS86 Vitányi-Awerbuch, FOCS87 Peterson-Burns), R. Schaffer patched the solution and we introduced a simple new solution for both the multireader and the multiwriter problem (ICALP89 with M. Li). With J. Tromp we found many improved solutions for wait-free variable constructions, a new finite-state proof method, and novel randomized algorithms for test-and-set (also with Y. Afek and E. Gafni).
Although, numerous techniques had been introduced for the study of lower bounds on the complexity of boolean functions (Sipser, Hastad, Yao, Razborov, etc) no general method was known for the study of upper bounds. Novel group theoretical methods in the theory of computation led to upper bounds on the complexity of boolean functions (every language

with polynomial cycle index is almost symmetric) (STRUCTURES88, E. Kranakis with P. Clote). Recent results of Babai et al (every language with polynomial cycle index is computable in logarithmic time with a polynomial number of processors) justify the importance of using group theoretic techniques in the study of upper bounds. E. Kranakis and P.Clote are now collaborating on a book giving a comprehensive treatment of boolean functions, parallel computation and proof systems, which emphasizes parallel algorithmic techniques.
Using techniques of geometric number theory Art gallery theorems, pertaining to visibility between point obstacles and point cameras, were studied (COMP. GEOM. CONF. 90 E. Kranakis with M. Pocchiola). The results obtained throw new light into non-algorithmic investigations of Abbott on the minimal number of guards necessary in order to see all the vertices of a grid.
New efficient algorithms (for the first time, of polynomial bit complexity) were given for computing non-constant boolean functions on general anonymous networks (ICALP90 E. Kranakis with D. Krizanc and J. van der Berg). Together with D. Krizanc new algorithms were also given for anonymous hypercubes and Cayley networks, thus on the one hand significantly improving previous results in the area and on the other, making possible the study of architectures having optimal complexity characteristics for such computability problems.
The energy consumption model of VLSI which was earlier introduced by G. Kissin was improved and published (JACM91). Realistic models (Vitányi) for physical parallel computation (as opposed to PRAMs) were investigated by analysing the average interconnect length in Euclidean embeddings of arbitrary graphs, expressed in terms of diameter and symmetry (SICOMP88).
Following several successful applications of Kolmogorov complexity in the theory of computation, in 1987 P. Vitányi started a comprehensive survey of Kolmogorov complexity and its applications in the theory of computation and inductive reasoning (STRUCTURES88, USPEKHI MAT. NAUK89 (in Russian), Ch. 4 in: Handbook Theoretical Computer Science 90 with M. Li). This was followed by several papers exploring and pioneering applications of Kolmogorov complexity in several areas including inductive inference (STRUCTURES89, JCSS with M. Li), formal language theory (ICALP89, JACM with M. Li), computational learning theory (FOCS89, COLT89, AAAI90, SICOMP91, with M. Li), combinatorial theory (STRUCTURES91 with M. Li). These results are acknowledged world-wide as wittnessed by translations appearing in Russia's foremost mathematical journal Uspekhi Mat. Nauk. Since 1988, P. Vitányi in collaboration with M. Li of the University of Waterloo are engaged in a project of producing a comprehensive monograph and textbook 'Introduction to Kolmogorov Complexity and Its Application', a first in this area, to be published by Addison-Wesley. Contact has been established with the Academica Sinica for speedy translation and publication of the book in Chinese.

Global prospects

In the near future the group will concentrate on algorithmic aspects of distributed computation, computational learning theory including bayesian reasoning and on-line learning, and the fulfillment of the Kolmogorov complexity project. To further this aim we

have started a policy of attracting considerable outside funding, nationally (NWO, SION, NFI) as well as internationally (ESPRIT, NSERC). This should lead to relatively large personel expansion and increase of funds and attraction of new foreign visitors in the near future. Our activities have been recognized in editorships (Distributed Computing, PPL, Math. Systems Theory), progr. committees (WDAG, STRUCTURES), IFIP working groups (Descriptional Complexity, Machine Learning).

Division in Projects
Projects are:
a. Distributed computing algorithms;
b. Computational machine learning;
c. Descriptional complexity.

3. Research 1987-1991

a. Distributed Computing
A general theorem expressing the total interconnect (wire) length of physical embeddings of computation networks in d-dimensional Euclidean space (d =1,2,3) which is technology independent, and the proof that this lower bound is optimal within a factor 10 for n-cube, cube-connected cycles, mesh, and so on (SICOMP88 Vitányi).
A first direct solution of constructing multi-user wait-free atomic variables from single reader single writer atomic variables. A special case is the construction of multireader variables which is optimal and simpler than existing constructions. Another special case is the construction of multiwriter variables from multireader variables, of which the complexity improves orders of magnitudes over all other known (none of them earlier) solutions. This one is much more simple than other solutions as well (ICALP89 Li-Vitányi, JACM under revision Li-Tromp-Vitányi).
General lower bounds, which are often optimal, on the message complexity of the 'Distributed Match-Making Problem' as a theoretical paradigm for nameserver, mutual exclusion, distributed routing (Algorithmica88, Mullender-Vitányi, Math. Syst. Th., Kranakis-Vitányi).

b. Computational machine learning
Valiant's seminal model of distribution-free pac (probably approximately correct) learning has started the field of computational learning theory. Yet it turns out that classes of concepts which should intuitively be learnable in this sense are NP-complete to learn. Hence certain investigations have focussed on learning under specific distributions, like the uniform distribution, to increase the number of learnable concept classes. Yet this approach is too restrictive for a viable theory. In practice we do not meet such a specific distribution. There arises the problem of finding a class of distributions which is large enough to be significant, and small enough to enhance learnability. Li-Vitányi have identified the class of 'simple' distributions, which include all computable and enumerable distributions (hence anything with rational parameters which has ever been used or has a name). We show completeness results both for discrete sample spaces and continuous sample spaces. A discrete concept class is polynomial pac learnable under all simple distributions iff it is polynomial pac learnable

under one specific distribution: the universal distribution $m(x) = 2^{-K(x)}$, where K(x) is the length of the shortest effective binary description of x (its Kolmogorov complexity)-provided we draw examples according to m(x) in the learning phase. A continuous concept class is pac learnable under all simple measures if it is learnable under the universal measure M(x)-the continuous analogue of m(x). Several classes are shown to be learnable under the new model which were not known to be learnable under the old (Valiant's) model, or which were known to be NP-complete (in the discrete case) to learn or unlearnable (in the continous case) in the old model. We also introduce the idea that learning syntactically described classes of concepts (like all finite automata) is not reasonable. In practice, we only want to learn 'simple' concepts, like finite automata which recognize parity rather than a long random string. We formulate this idea precisely and prove several results. We also bring the model in the feasible (polynomial time computable universal distribution) domain. See FOCS89, COLT89, AAAI90, SICOMP91.

c. Kolmogorov complexity

Li-Vitányi solved a well-known 20 year old problem in time complexity of Turing machine computations (1-work tape versus k work tape computation time from Hopcroft & Ullman 69) and related problems involving pushdown stores and queues (INFO&COMP88, STRUCTURES86, SICOMP with L. Longpré). Li-Vitányi have given the authoritative survey on Kolmogorov complexity and its applications (STRUCTURES88; USPEKHI MAT. NAUK89; Complexity Theory Retrospective, Springer; Chapter 4 in Handbook of Theoretical Computer Science, Part A, 1990). We gave a new approach to formal language theory using Kolmogorov complexity, replacing the classic 'pumping lemma's' by stronger Kolmogorov complexity characterizations and lemmas, which are far more intuitive and easy to use, both replacing existing theorems and providing new results (ICALP89, JACM). We have analysed the relation between Solomonoff's inductive inference and induction principles in recursion theory (Gold's paradigm) and statistics (Fisher's Maximum Likelihood, Rissanen's Minimum Description Length, Jaynes' Maximum Entropy), and connected it with distribution-free learning (STRUCTURES89, JCSS). We have found a new Kolmogorov complexity method in combinatorial theory and applied it to prove results earlier proven by the probabilistic method (in Erdoes and Spencer's book), and by information theoretic (second moment) methods by Pippenger (STRUCTURES91). Work is in full progress on the comprehensive textbook M. Li and P.M.B. Vitányi, 'Introduction to Kolmogorov Complexity and Its Applications', Addison-Wesley, to appear.

4. Plans for the future

We plan to pursue our work in distributed and parallel computing in the framework of the comprehensive NFI proposal with the group at Utrecht University involving 6 extra oio's/postdocs stationed at CWI, University of Amsterdam, and Utrecht University. This will also involve full-time visits from excellent foreign experts. Moreover we applied for one more oio from NWO/SION in distributed computing. Overall the research will involve a balanced mix of global computation in networks, algorithms for distributed control of network operation, and low-level wait-free concurrent object implementation.We propose to investigate such matters both in networks were communiacation is costly and computation

(almost) for free, and in new fast networks (glass-fiber optics technology) where communication is essentially free but the computation in the nodes is costly. We will also proceed along the lines of real-time (Archimedean time) computational models as pioneered by us. This work will also involve tight cooperation with the University of Waterloo, Carleton University, Technion, as well as possible future cooperation with groups at MIT-for instance in the context of a sabbatical. Long term visits of foreign experts are part of this, as well as organisation of WDAG93 (Workshop on Distributed Algorithms = European PODC) in Amsterdam. We propose to coordinate the seminars at CWI and University of Utrecht on the common NFI platform.

In computational learning theory we have taken the initiative and coordinate the new ESPRIT BRA II Consortium 'Machine Learning' which coordinates (we think) all significant centers in machine learning in Europe today, embracing the scale from recursion theoretic learning via pac learning to mathematically sound neural learning.We have listed some of the participants of the 10 odd. European sites above, and have secured cooperation from extra European experts like L. Valiant at Harvard, R. Solomonoff at Oxbridge Research, and M. Li at University of Waterloo. From the Esprit proposal we expect to be able to attract 3-4 oio's/postdocs divided between CWI and University of Amsterdam. The aim of the research will be to further enhance the computational learning theory, combining Bayesian approaches with on-line approach, until the model becomes intuitively satisfying, and develop interactively new learning algorithms and implement them to test them in practice. To give an example: our earlier research with M. Li (STRUCTURES89) led to an application by Q. Gao and M. Li to machine learning of handwritten characters using the Minimum Description Length principle (IJCAI89), and implemented and running on pc. We have also requested an extra oio in this project from NWO/SION.
Cooperation in the Netherlands will be with the University of Amsterdam, the group at Twente University. Outside the Netherlands with 10 plus groups in context of the ESPRIT project. In the context of this project we plan to attract the COLT conference to Europe, evolve a yearly European COLT-like conference from the general ESPRIT meetings of the project, and perhaps form a European Computational Machine Learning Society. We are furthermore member of the IFIP working group on Descriptive Complexity, and have been chartered to form a new IFIP working group on Machine Learning under our chairmanship. It is planned to organize several conferences and meetings and seminars on this subject at CWI in the near future.
Research in Kolmogorov complexity (Li-Vitányi) is expected to culminate in physically oriented applications in the theory of Chaos, solution to paradoxes in thermodynamics, and new proofs of thermodynamical theorems (like the Sackur-Tetrode Equation for the entropy of a typical microscopic state of a system). It is of major importance to us, and we flatter ourselves also to parts of the computer science community and other scientific communities at large, that our comprehensive treatment of Kolmogorov complexity and its applications gets finished in the forseeable future. Our preliminary pioneering efforts have already considerably stimulated applications of Kolmogorov complexity in the theory of computation, for instance in the structures in complexity theory community. A comprehensive treatment is dearly needed, since the knowledge concerning this topics is scattered far and wide, between

different disciplines east and west. Currently, it would seem, only the intended authors have an overview. This work involves tight cooperation with Ming Li at the University of Waterloo, and long term stays of P. Vitányi at Univ. of Waterloo, and possibly (part sabbatical) at Boston University (L.A. Levin and P. Gacs).

5. Cooperation 1987-1991

A. Contract research

Running NFI proposal; NWO/SION proposals, ESPRIT BRA II proposal (see above).

B. Contacts and/or cooperation with industry

In context with computational learning theory we have contact with 'Syllogic BV', Houten, Netherlands, were a preliminary Ph.D. Thesis is being prepared on language learning using our work on simple learning of simple concepts (application of Kolmogorov complexity in learning theory).

C. Contacts and/or cooperation with scientific institutes

CWI (K. Apt, L. Schrijver), Univ. of Amsterdam (P. van Emde Boas, L. Torenvliet), Univ. Utrecht (L. van Leeuwen, G. Tel), Univ. Twente (U. Feige, W. Kern, S. Mullender), Univ. Waterloo (M. Li), Stanford T. Cover, G. Plotkin, A. Goldberg), Columbia University (Z. Galil), Univ. Maryland, Washington D.C. (C. Smith), Univ. Wisconsin, Madison (E. Bach), Weizmann Institute of Science, Rehovot, Israel (Y. Moses), IBM Almaden Research Center (J. Halpern, R. Fagin, J. Rissanen, UCSD (W. Savitch), UCSC (M. Warmuth, D. Haussler, Ph. Kolaitis), AT&T (E. Pednault, S. Tewksbury), Boston University (L.A. Levin, P. Gacs), Moscow University (V. Uspenskii, A.K. Shen), Harvard (L. Valiant), U. Illinois, Chicago/ Univ. Graz (W. Maass, G. Turan), Saarbruecken Univ. (W. Paul, R. Solomonoff), (Technion: S. Even, Y. Afek, A. Israeli, S. Zaks, S. Moran, A. Itai), UCLA (E. Gafni), Carleton Univ (N. Santoro), MIT (B. Awerbuch, N. Lynch), North-Eastern University (L. Longpré), University of Buffalo (A. Selman), Cornell University (J. Hartmanis, F. Schneider), Ecole Normale Superieure, Paris (J. Stern, M. Pochiola), INRIA, Paris (Ph. Flajolet), DEC SRC, Palo Alto (L. Lamport), Rochester University (J. Seiferas, D. Krizanc), University of Texas, Austin (M. Gouda), Comp. Techn. Institute, Patras, Greece (P. Spirakis, L. Kirousis), Georgia Tech (J. Burns), Barcelona Polytechnic (J. Balcazar), University of London, London School of Economics (N. Biggs, M. Anthony), Rome University (M. Protassi), University of London Royal Holloway and Bedford New College (J. Shawe-Taylor).

6. Further activities 1987-1991

Dr. E. Kranakis

- Editor 'CWI Quarterly', CWI.

Prof.dr.ir. P. Vitányi

- Editor 'Distributed Computing', Springer;
- Editor 'Parallel Processing Letters', World Scientific;

- Editor 'Mathematical Systems Theory', Springer;
- Editor 'Frontiers in Computing Systems Research', Plenum Press;
- Editor 'Journal of New Generation Computer Systems', Akademie Verlag;
- Scientific Board 'Encyclopaedia of Mathematics', Reidel;
- Programme committee, Compar92 - VAPP V, Lyon, France;
- Programme Subcommittee Chair, Theory of Computation stream, IEEE CompEuro92;
- Programme committee STACS91, Paris, France, 1991;
- Steering committee WDAG= International Workshop on Distributed Algorithms;
- Programme committee WDAG91, Delphi, Greece, 1991;
- Programme committee 6th IEEE Structures in Complexity Th. Conf., Chicago, 1991;
- Programme committee WDAG90, Otranto, Italy, 1990;
- Publicity Committee Dutch Mathematical Society;
- Programme committee WDAG89, Nice, France, 1989;
- Programme committee 4th IEEE Structures in Complexity Th. Conf., Eugene, OR, 1989
- Programme Committee Princeton U./AT&T Bell Workshop on Formal Models For General Purpose Distributed Computation, 1987
- Dutch delegate CREST Subcommittee on Training in Informatics 1981-1988;
- IFIP Special Working Group on Descriptional Complexity (member);
- IFIP Special Working Group on Machine Learning (chair);
- Closing Panel Member IAAA90 Spring Symposium Series, Theory and Application of Minimum-Length Encoding, Stanford Univ., 1990;
- Coordinator and Initiator ESPRIT BRA II Consortium on ' Machine Learning';
- Invited Speaker 6th IEEE Structures in Complexity Theory Conference, Chicago, 1991;
- Invited Speaker 4th IEEE Structures in Complexity Theory Conference, Washington D.C., 1989;
- Invited speaker Princeton U./AT&T Bell Workshop on Formal Models For General Purpose Distributed Computation, 1987;
- Visiting Professor, Computer Science Department, University of Waterloo, June-July 1991, November 1990, April 1990, November 1989;
- NSERC International Scientific Exchange Award, 1990;
- NUFFIC Visiting Scientist, Dept. Electrical Engineering, Technion, Haifa, May 1989;
- Visiting Lecturer, Comp. Sci. Dept., York University, June-July 1988, June 1989.

7. Experimental systems & programs 1987-1991

None.

8. Selected publications 1987-1991

Distributed computing

1. M. Li, J. Tromp and P.M.B. Vitányi, How to share concurrent wait-free variables (revised), ITLI Prep. Series, Computation and Complexity Theory, Tech. Rept. CT-91-02, University of Amsterdam, 1991.

Comments:
previous version published in ICALP89. This is a revised version under consideration for J. Assoc. Comp. Mach.

Descriptive complexity:

2. M. Li and P.M.B. Vitányi, Kolmogorov Complexity and its Applications, Chapter IV in: Handbook of Theoretical Computer Science, J. van Leeuwen, Ed., Elsevier, 1990, pp. 189-254.

Comments:
partly published in Russian: M. Li and P.M.B. Vitányi, Kolmogorovskaya slozhnost': dvadsat' let spustia, Uspekhi Mat. Nauk, 43:6 (1988), pp. 129-166. (= Russian Mathematical Surveys).
Book in preparation:
M. Li and P.M.B. Vitányi, Introduction to Kolmogorov Complexity and its Applications, Addison-Wesley, to appear.

Parallel complexity:

3. P. Clote and E. Kranakis, Boolean Functions, Invariance Groups and Parallel Complexity, SIAM Journal on Computing, 20:3(1991).

Comments:
previous version in STRUCTURES '89,

Book in preparation:

4. P. Clote and E. Kranakis Boolean Functions, Parallel Computation and Proof Systems, to appear in 1992, (ca 400 pp).

Machine learning:

5. M. Li and P.M.B. Vitányi, Learning simple concepts under simple distributions, SIAM J. Comput., 20:5 (1991).

Comments:
previous version in FOCS '89.
A. Blum, T. Jiang, M. Li, J. Tromp, M. Yanakakis, Linear approximation of shortest superstrings, Proc. 23rd ACM Symp. Theory of Computing, New Orleans, 1991, pp. 328-336.

RESEARCH GROUP AA2
CRYPTOLOGY

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
Dr. D. Chaum	group leader	0.6 fte	since 01.10.88
Non-permanent:			
ir. J.N.E. Bos	junior researcher	1.0 fte	since 01.10.87
ir. E.J.L.J. van Heijst	junior researcher	1.0 fte	since 01.06.88
ir. M.W. van der Ham	junior researcher (RIPE)	1.0 fte	since 16.03.90

External funding:
a. NFI, single site, 1985–1990, NLG 1,990,300.
b. DGXIII RACE, RIPE, prime contractor,1988-92, NLG 1,161,270.
c. Ministerie van verkeer en waterstaat, consulting, NLG 140,000.
d. PBTS, joint with DigiCash, 1991–92, NLG 100,000.
d. Miscellaneous smaller contracts (see 5.a below).

2. Introduction

Aims

The research in this project concerns all aspects of cryptology that are related to information security. This involves in particular the construction, and analysis (from the point of view of cryptanalysis, information theory, and complexity theory) of cryptographic protocols and their underlying cryptographic algorithms, and the mathematical proofs of their theoretical limits, security, and performance.
In particular, there has been substantial emphasis on: theoretical results establishing the limits of what can and cannot be accomplished by cryptographic and other security protocols in general; analysis of basic secrecy coding schemes; practical techniques for the protection of privacy of individuals in transmission of messages, payment systems, and the treatment of personal data by organizations; and introduction of primitives offering new possibilities in application.

Year of starting

Although there had been some interest in cryptography at CWI since the beginning of 1980, the Crypto Group really became an active participant in research during 1985.

Description of development

During the past 5 years the Crypto Group has gone from a visiting expert and a post-doc, to include: two o.i.o.'s; extended visits from 8 major researchers; prime-contractor role in a

major European community project; hosting international conferences on the subject; organizing courses; and a significantly expanded monthly working group series. By now it must be said that our group is at least among the top few non-secret research centers for modern cryptography in Europe, and that we have established ourselves as initiators and still active participants in several areas within the field.

Prospects
A number of new results, that potentially open new areas of investigation, are in the process of being written up and elaborated on. A few European Community projects are in the process of being proposed. Growing cooperation with industrial partners is planned.

Division in projects
The research has been carried out in four major areas within cryptography: (a) theoretical results, (b) conventional cryptography, (c) untraceable transactions, and (d) new kinds of cryptographic primitives. The work for RIPE may be thought of as an additional project, a part of which falls within (b) above.

3. Research 1987-1991
The field of open research in modern (i.e. not paper and pencil or electro-mechanical machine based) cryptography emerged in about 1976. The first conferences occurred in 1981, both in Europe and in the U.S., each attended by some 75 or so participants. The following year the International Association for Cryptologic Research was founded during the launch of what remains an unbroken series of international conferences, "Crypto" in Santa Barbara California each August and "Eurocrypt" held somewhere in Europe each Spring Attendance at the conferences has grown surprisingly steadily to about 250 or 300, with over 100 papers submitted, and about 30 presented. These remain the only regular international conferences devoted to the theme, although the association has sponsored one in Australia and another in Japan. The association has also launched a journal a few years back, which like the conference proceedings is published by Springer-Verlag.

The research of the Crypto Group during the last five years can best be described separately for each of the four main research project themes.

Theoretical results
A line of development can be traced through a series of significant results by the Crypto Group in this area, although there were also some scattered other results (see list of publications section I: 1, 2, 7, 8, 11, 25, 28 & section II: 2, 4, 5) in this area. This line began with publication 19, which was first presented at a conference at which a 'dual' result was first presented by a team of researchers from M.I.T. The results show that Alice can give exponentially high certainty to Bob that she knows a satisfying assignment of some predicate, without helping Bob learn the assignment. The model we used allows Alice to protect her secret from Bob even if he has infinite computing power (and thus he may find all instances but still will not know which one Alice had) called “unconditional privacy”, whereas their model was that Bob had polynomially bounded resources, called "computational privacy".

These results were elaborated and made accessible to the generally interested reader in the invited section II.14 also listed as 8.1.

The next step in this line, reference 16, extended the results to multiple parties, each having their own secrets, and each wishing to participate in an agreed computation that takes the secrets as input, and where the output of the computation will become known to all parties. Again there was a related independent result by the same team. Their model was the same as in their original paper, ours included theirs as a special case, but also allowed for one distinguished participant to have unconditional privacy. Next 17 appeared at the same conference as an almost identical independent result by a partly overlapping Israeli team. This showed that if two-thirds of the participants are honest, then all you need is secure channels between every pair of participants to do a multiparty computation. (17 was invited to JCSS, and is also shown as 8.2.) Subsequently, using the distinguished participant of 16, together with an extension of 17 improving it to the optimal one-half honest participants, we have been able to achieve in 24 the strongest result in a natural model to date, which in essence says constructively that privacy can be protected unconditionally if a majority do not conspire, and even if they do they will have to break the underlying cryptosystem in order to learn secrets of the others.

Conventional cryptography

The area of conventional cryptography is typified by the well known and somewhat controversial DES (U.S. Data Encryption Standard). The cipher is composed of sixteen iterations, each of the same basic structure. In a paper presented in 1986, we showed how to break a cipher made up of seven of these iterations, while the most that had previously been achieved was the more or less trivial four. In 13 we propose a generalization of our attack which includes several other attacks and observations in the literature. Last year at Crypto Biham and Shamir, in a seventy page quite technical paper, were able to break eight iterations. A Japanese alternative to DES, which was submitted to ISO and received some significant attention, was completely broken by us in 6.

Untraceable transactions

A comprehensive approach to secure consumer transactions allowing individuals maximum privacy was proposed and surveyed in 21, several translations of which were invited and others of which have appeared in the last five years. These results were in three parts: untraceable communication (see invited paper 23); untraceable payments (see 3, 4, 9 10, 12, 18, 19, 27); and a way for people to maintain the database about themselves while allowing them to prove that queries to it are answered correctly, called credential mechanisms (see 22 and section.II.3). Although we have played a major role in launching this area of investigation, there are a number of sites around the world which have published related theoretical as well as practical results.

New kinds of cryptographic primitives

Apart from the cryptographic primitives needed for untraceable transactions, we have created some additional novel ones that have also received some attention. One of the main ideas that

perhaps catalyzed the field of modern cryptography was Whitfield Diffie's notion of "digital signature". We have proposed an alternative to this, which has arguable advantages in many applications. A digital signature is self-authenticating, in the sense that anyone can verify it using only the public key identifying the signer and the message claimed to have been signed. With our "undeniable" signatures, cooperation of the signer is needed each time the signature is verified; if the signer refuses to allow, say, a judge to verify the signature, the signer can be asked to use the protocol that lets him show that the alleged signature is not his, without revealing anything more. Since this notion first appeared in 26, we have improved it in 29, extended it in 5, and currently have submitted a survey on the topic, which has attracted a number of other researchers to the extent that it occupied its own session at the last Eurocrypt conference.
Another new cryptographic primitive just introduced in 30 called "group signatures," lets any member of a group form a signature (either self-authenticating or undeniable) that can only be traced to the particular member by some action such as cooperation of a majority of other group members.

4. Plans for the future

Three new areas are expected to be the focus of investigation in the near term: (a) Multiparty computations in communication models with novel channel configurations, including channels that are assumed not to exist, to be readable by one subset of parties but writeable by another subset of parties, and unreliable channels; (b) three-party protocols, where the middle party moderates the communication between the other two, with application to secure and privacy protecting transactions including maintenance and transfer of credentials; (c) transferability between parties and convertibility between currencies of electronic money.

Additionally, the RIPE project work will of course continue. Furthermore, the PBTS projects with DigiCash have gotten off to a slow start, but are expect to pick up. Other EC project proposals are in preparation, including another where Crypto Group has been asked to serve as the coordinating (prime) contractor.

5. Cooperation 1987-1991

A. Contract Research

Ministerie van Verkeer en Waterstaat; Bank Giro Centrale; Rabobank; Norwegian Telecom, (and several smaller ones).

B. Contacts and/or cooperation with industry

Btronic (NL); Cryptomathic (DK); DigiCash (NL); GEC Card technology (UK); Gemplus Card International (F); Logica (UK,NL); Philips Crypto (NL); PTT Research (NL); Siemens (D); Sligos (F).

C. Contacts and/or cooperation with scientific institutes

National:
Bert den Boer: Philips Crypto; Jan Hendrik Evertse: RU Leiden, Wiskunde & Informatica; Cees Jansen: Philips Crypto; Hans van Tilborg: TU Eindhoven, Wiskunde & Informatica; Gert Roelofsen: PTT Research, Neher Laboratories; Peter de Rooij: PTT Research, Neher Laboratories.

Participants of the workinggroup cryptology come from the following organizations:
Cryptech Nederland; HEAO Den Haag; H.O.N.; Enschede HIO; KU Brabant, Subfac. Econometrie; KU Nijmegen, Fac. W&N, sectie Informatica; Ministerie van Defensie; KL; Ministerie van Defensie; KLU; Ministerie van Defensie; KM; Nat. Lucht- en Ruimtevaart laboratorium; NLUUG (Netherlands Unix Users Group); Open Universiteit, Heerlen; Philips Crypto BV; PTT-Dr. Neher Lab.; PTT-Telecommunicatie; RU Groningen, Interfac. Act en Econometrie; RU Leiden, afd. Wiskunde & Informatica; Smid, Harderwijk; TNO-FEL; TNO-MT; TU Delft; TU Eindhoven, Onderafd. Wiskunde & Informatica; TU Twente, Afd. EL; U.v. Amsterdam, Fac. Wiskunde & Informatica; VU Amsterdam, Fac. Wiskunde & Informatica.

International:
Gilles Brassard (U. Montreal, Canada); Ernest Brickell (Sandia Labs, U.S.A.); Claude Crépeau (E.N.S., France); Ivan Damgård (Arhus U., Denmark); Yvo Desmedt (U. Wisconsin, U.S.A.); Markus Dichtl (Siemens, Germany); Whitfield Diffie (B.N.R., U.S.A.); Ronald Ferreira (C.T.I., France); Walter Fumy (Siemens, Germany); Siegfried Herda (G.M.D., Germany); Hideki Imai (NTT, Japan); Peter Landrock (Århus U., Denmark); Tsutomu Matsumoto (Yokohama U., Japan); James Michael (U. London, England); Stig;Frode Mjølsnes (U. Trondhiem, Norway); Andrew Odlylzco (Bell Labs, U.S.A.); Andreas Pfitzmann (U. Karlsruhe, Germany); Jean-Jacques Quisquater (Philips Research, Belgium); Jennifer Seberry (National U., Australia); Gustavus Simmons (Sandia, U.S.A.); Joos Vandewalle (KU Leuven, Belgium).

6. Further activities 1987-1991

Dr. D. Chaum
- General Chairman: Eurocrypt 87.
- General Chairman: IFIP TC-11.6.
- Co-General & Program Chairman: Smart Card 2000, 1987.
- Program Chairman: Smart Card 2000, 1989.
- Course Director: Crypto Concepts, 1989.
- Member Editorial Board: Journal of Cryptology (founding and current).
- Founder & Member Board of Directors: International Association for Cryptologic Research.
- Final Project Supervisor: S. Rooijakkers, H. Beuze, P. Sliepenbeek, B. Neven, H. van Antwerpen, and T. Veugen.
- Invited Lectures: more than 20 during 1987–91.

7. Experimental systems & programs 1987-1991

1. Macintosh application showing inner-workings of offline electronic cash (see list of publications section I.9), with a full "finder" like user interface.
2. Contributed to the RIPE toolbox, which is an extensive but confidential collection of cryptanalitic tools.

8. Selected publications 1987-1991

1. Minimum Disclosure Proofs of Knowledge, G. Brassard, D. Chaum & C. Crèpeau, Journal of Computer an Systems Sciences, vol. 37 no. 2, 1988, pp. 156–189.
2. Multiparty Unconditionally Secure Protocols, D. Chaum, C. Crépeau & I. Damgård, Proceedings of the Twentieth ACM Symposium on the Theory of Computing, ACM, 1988, pp. 11–19.
3. The Dining Cryptographers Problem: Unconditional Sender Untraceability, D. Chaum, Journal of Cryptology, vol. 1 no. 1, pp. 65–75, 1988.

RESEARCH GROUP AA3
COMPUTER SYSTEMS AND ERGONOMICS

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
S. Pemberton	group leader	1.0 fte	
	(funded by SERC, Utrecht	0.2 fte)	
Prof. L.G.L.T. Meertens	researcher	0.3 fte	
	(also 0.3 fte AA5)		
Drs. F. van Dijk	programmer	1.0 fte	
Drs. T.J.G. Krijnen	programmer	1.0 fte	until 15.08.91
Non-permanent:			
L.G. Barfield M.Sc	researcher	0.8 fte	since 01.04.89
	(funded by SERC, Utrecht	0.2 fte)	
Ir. E.D.G. Boeve	junior researcher (NFI)	1.0 fte	since 16.03.90

2. Introduction

As computers become more and more widespread, so the spread of users of computers in society becomes greater, and the numbers of applications grow. Accompanying this proliferation is a perception that something is problematic with how computers are used. Computer literate people are likely to opine that applications are usable if you use them for a few weeks and get used to their difficulties, but computer initiates are likely to blame themselves, and assume that they aren't 'computer people', and they will often give up trying to use computers. The people in the middle ground struggle on, wondering if there is an easier way.

A large part of the problem is historical, that all aspects of computer systems tend to be designed by technical people with very deep knowledge of computers and how they work, and little specific knowledge of what has come to be known as "human factors". As a result, computer interfaces tend to reflect low-level aspects of computers, or details of the implementation of the application.

As a result, computer users at all levels are left with systems and applications that singly and in combination are arcane, non-interoperable, inconsistent, and inflexible.

The Ergonomics of Computer Systems group does research on the user interface of computer systems. We use the term "user interface" in the widest sense, including research into programming languages, automating the portability of computer systems, and integrating applications into a single model of computer use. The research focusses on software-technological models, tools, methods, architectures and systems that reflect and support the "soft" results in this area, such as general user-interface design principles based on insights

and experiments from cognitive psychology, and that can be used for the construction of software that incorporates these results.

The development of the research area in the group

The initial research of the group, when it was formed in 1985, was into the programming language ABC. This was originally intended to be a language for beginner and non-experienced computer users, but with the development of later versions, it turned out to be a useful tool for beginners and experts alike: the principle observation being that 'simple to define' and 'easy to use' are not synonymous, and that users are better served by a few, very high-level, tools, which they may also use for low-level ends if they wish, than a set of low-level tools which can be used to build high-level tools.

Part of the development of the language involved implementations, and this has led to the research into portability. This includes design and implementation of 'virtual' models of aspects of computer systems, such as terminals and windowing systems and building of toolkits, as well as investigating self-configuring systems.

ABC is not just a programming language, but a complete programming environment, and the research into the environment involved investigating models of computer use and interaction that would allow users to do as much as possible while learning a minimum of new concepts. This line of the research led to the Views project, which is an investigation into an open-architecture user interface system, where new applications can be easily added, on the fly without recompilation, with guaranteed consistency of user interface and interoperability between applications.

Global prospects

Ergonomics is a new field in computer science. In a recent survey (on Usenet), it was clear that computer companies are only just starting to recognise the problem, by forming human factors groups for designing computer systems. This year, the world's first degree course in the subject will start (in the Netherlands). While there are groups across the world studying topics like User Interface Management Systems, and toolkits, in other words studying ways to simplify the implementation of user interfaces, the unique aspect of AA3 is that we are researching taking the user interface out of the program's domain, and supplying it as a central system service.

3. Research 1987-1991

The most important result of the ABC sub-project was the release of 4 implementations of the language (described below), and a book published by Prentice Hall. ABC is a language that is extremely easy to learn - someone who knows Pascal or C can learn it in an hour or two: we have observed a teenager, armed with only a quick-reference card and no other knowledge of the language, sit down at a terminal and start to program. Despite this ease of learning, the language is very powerful, and typical ABC programs are a quarter or a fifth the length of equivalent Pascal or C programs. ABC is used by number theorists, cryptographers, teachers, and hobbyists alike. While there are areas for further work, such as graphics and system programming, all recent work in the system has been on maintainance and promulgation, and attention focussed on Views, in itself a generalisation of the precepts discovered in the ABC

research. The initial research into Views was to find a user model of computer interaction that would encompass all possible applications. This was done via a number of experimental systems, such as editors and mail-readers (described below). This led to our TAXATA model of interaction: all information is presented to the user as documents which are in principle editable, all actions are accomplished by editing documents, and what is presented on the screen is precisely the state of things (Things are exactly as they appear - a stronger version of WYSIWYG, what you see is what you get). More details of this approach can be found in the included article on Views.
This model led to the development of an implementation model for the system, and a test implementation of Views. Based on the success of this pilot, SERC, the Software Engineering Research Centre in Utrecht, joined with us, and widened the research into multi-user authoring using Views, widening the system from single-user to multi-user. In this context we have developed (but not yet tested in practice) a simple model for safeguarding consistency on concurrent access of an object by different users, as well as a model for a user-accessible representation of the current state of progress in a cooperative design process. Current research is in the graphics model of the system, the extension of the model to low-level interaction tools, the application specification language, the persistent object world model (in cooperation with AA4), the maintenance of consistency of the system through use of a network of invariants between objects, and user-transparent object locking during sharing.

4. Plans for the future

The research of the research group AA3 will be terminated, with the exception of the research of the Ph.D. student E.D.G. Boeve. The way in which his research will be coordinated is still under discussion. However, the work on Views will be continued in 1992, resulting in a prototype implementation of the Views kernel. There are many directions of research for which the Views approach can form a basis, and groups both inside and outside the CWI have shown interest in collaborating. It is obvious that for a system that is designed for the easy addition of new applications, the best way to take the research forward is to confront the theory with practice by testing it on a diversity of application types.
The most obvious future direction is multi-media. The current Views object model has no direct provision for time-dependent objects, such as sound or animation. There is an obvious extension that can be made, and it seems likely that this expanded model can deal with both synchronous and asynchronous events equally. An important research question here, essential in view of the user model of Views, is to find good principles for easy-to-use editing of multi-media documents; this is unlikely to be a straightforward extension of the proven principles for static objects. There are obvious contact points with the current CWI multi-media project. Further, SERC are currently initiating a multi-media project, and are seriously considering basing on Views.
Other proposed projects that would draw upon the Views research are for interactive mathematical 'books', with advanced typesetting, hypertext, and interactive experiments (in cooperation with the AM department), a networked image analyser for cardiologists, and scientific data visualisation of marine data.

5. Cooperation 1987-1991

Within Europe, AA3 has worked on the Euromath project, a project to link mathematicians continent-wide with a network and communication tools. We were responsible for the functional specification and a pilot implementation.
ABC is being furthered with cooperation with several other institutes (see below).
Views is carried out in cooperation with SERC, as mentioned above, and with four Dutch Universities (Free University, Delft, Tilburg, and Twente) in an NFI project "Systematic User Interface Design", a broad-based cross-fertilisation project covering expertise from computer science, psychology and physiology.
The planned multi-media project with SERC will be carried out in cooperation with another academic institute, and two commercial companies.
The planned Cardiologist network is in collaboration with CADANS, a medical research centre based in Utrecht.
The planned "interactive mathematical book" is in collaboration with Arjeh Cohen of the CWI AM department.

6. Further activities 1987-1991

AA3 organised this year a successful course on system portability which will be repeated this year, and again next year to coincide with the EurOpen conference which will be in Amsterdam.

7. Experimental systems and programs 1987 - 1991

AA3 is a practical and experimental group: it does its research on the basis of working systems and prototypes. Research into ergonomy, user interfaces and programming languages demands such an approach, since it is exactly the dynamic between user and system that is being studied.
The ABC system is one of the largest systems we have produced, and the one most used outside of the CWI. It consists of 56,000 lines of code (1.25 Mbytes), in 4 versions of the system: for the Apple Macintosh, the IBM PC and compatibles, for the Atari ST, and for Unix systems. In collaboration with 5 external institutes (the Minnesota Supercomputer Center, Minneapolis, the T.U. Muenchen, the Idaho National Engineering Lab, Indiana University and the University of Nijmegen) 5 new versions are being prepared: for Cray computers, for OS/2, for DEC VMS, for the Commodore Amiga, and for the Acorn Archimedes. The ABC system includes online documentation, and system documentation, as well as the ABC Programmer's Handbook, published by Prentice-Hall. The ABC Newsletter (in a print-run of 1000) keeps users in touch with developments.
ABC is used for teaching at schools and universities. Since the system is freely available on servers worldwide, there is no way to discover the extent to which it is being used, since usually the only contact we have is if something goes wrong, which seldom occurs. For instance, we only recently learned, in one case via, that both Leeds University and Osnabrueck University use ABC for teaching programming, and that it is being used in at least one school in Denmark for teaching purposes. Exeter and Manchester Universities have both announced the intention of using ABC for teaching, and New York University is

considering it. At a recent open day, the Vrije Universiteit used ABC to demonstrate programming, and to let people try programming themselves, and the guests were invited to take a copy home with them.
It is only the appearance of The ABC User's Handbook that makes ABC usage viable; this year ABC has been used in two books: three chapters are dedicated to ABC in "The Art of Lisp Programming" (R. Jones, C. Maynard, and I. Stewart, Springer Verlag), and it is the programming language used in a book on number-theoretical cryptology by K. Nissen and P. Landrock. There has recently been an article on ABC in the USA Journal "Unix Today".
A novel aspect of the ABC system is that it configures itself automatically to the machine it is being compiled on, by first running a program that determines run-time properties of the machine and compiler. An offshoot of this is a program produced by the group, called enquire.c, a generalised version of the above mentioned program, which reports on the properties of the machine and C compiler, and optionally produces 2 of the header files required by the new ANSI C standard.
Enquire.c is 2800 lines of code (75 Kbytes); it has gone through 7 released versions. It has been adopted for use by the GNU project at MIT for their portable C compiler, one of the most widely used C compilers available, used at thousands of sites worldwide.
Enquire is a unique program, and is used by several major manufacturers (such as Cray and Prime) for testing their C compilers. It is referenced in several sources on portability (for instance "Notes on Writing Portable C Programs" by Andre Dolenc).
In the initial research into generalising the ideas of ABC to user interfaces in general, leading to the Views project, the ideas in the ABC structure editor have been embodied in a text editor, known as 'Linda' or 'be'. The editor is widely used within the CWI by support staff. This is 17,000 lines of code (0.3 Mbyte). Three versions have been made (reflecting the machines used at the CWI): for the IBM PC, for Unix, and for the Macintosh. Documentation includes a user manual.
An offshoot of the work on editors has resulted in a package called 'vtrm', a virtual terminal interface. Part of the problem with producing portable interactive programs is that there is no standard portable way of handling computer screens. Vtrm, in several versions, allows the C programmer to easily port screen handling programs to different platforms.
More difficult yet, is porting programs that use windowing systems to different platforms. A system produced by AA3 is STDWIN, a windowing package that runs on top of several different window managers, which allows a program to be compiled without change on different machines with different windowing systems. It has gone through three versions, for five platforms: for X windows, for the Apple Macintosh, for the Atari ST, for the Whitechapel MG1 series of computers, and a generic alphanumeric version for non-graphic screens and terminals. This is 68,000 lines of code (1.3 Mbytes). It is widely used within the CWI for prototypes and systems that need windowing facilities. Outside the CWI, it is used for instance in the Little Smalltalk system (Budd, "A Little Smalltalk", Addison Wesley).
Our involvement in Euromath included contractual requirements to produce software, specifications and documentation for the planned Euromath system. This resulted in the Epis system produced by AA3, 54,000 lines of code running on two platforms, Unix and VMS, in both a windowing and a terminal-oriented version. Epis is an integrated text editor, file browser and handler, mail reader and sender, and news reader and sender. The documentation

written includes a User Manual, system documentation, and an installation guide. Epis was distributed to several participating members of the Euromath project.
Also produced for Euromath was the Functional Specification of the complete envisaged Euromath system. This was a 248 page document describing the philosophy and system interfaces of the full Euromath system.
Finally, as part of the Views research, a pilot Views implementation has been produced. This is 17,000 lines of code (0.5 Mbytes). Documentation includes internal system documentation, and specifications of the graphics interface.

8. Selected publications 1987-1991

1. Leo Geurts, Lambert Meertens, Steven Pemberton (1990). The ABC Programmer Handbook, ISBN 0-13-000027-2, Prentice Hall, UK, 176 p.
2. Steven Pemberton (1990). Open User-Interfaces: The Views System. Proceedings of the Conference 'Interacting with Computers: Preparing for the Nineties', Noordwijkerhout, The Netherlands.
3. Lon Barfield, Eddy Boeve, Steven Pemberton. Program: Views.

RESEARCH GROUP AA4
DATABASES

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
Dr. M.L. Kersten	group leader	0.8 fte	
Non-permanent:			
Dr. A.P.J.M. Siebes	project leader (NFI)	1.0 fte	until 01.09.91
drs. C.A. van den Berg	researcher (SION)	1.0 fte	since 16.03.87
I.J.P. Elshoff M.Sc.	researcher (NFI)	1.0 fte	since 16.05.90
ir. A. Plomp	junior researcher (SION)	1.0 fte	since 16.10.90
drs. C.J.E. Thieme	junior researcher (NFI)	1.0 fte	since 01.08.90
drs. M.H. van der Voort	junior researcher	1.0 fte	since 01.06.88
NN	senior researcher (NFI)	1.0 fte	

2. Introduction

The Database research group was established in 1985 to study topics in the area of distributed information systems. The research being carried out is focussed on the theory of datamodels and architectures for database management systems. In particular, those issues stemming from requirements posed by information systems which are distributed over time and location, where the organization of the data and the applications changes frequently, and where the content of the database is only guaranteed to be locally consistent. Such information systems can be found in office environments, (financial) trading environments, in design environments, and scientific environments where the kinds of data being collected cannot be frozen for long periods and the way in which the data is being used to produce information changes frequently.

Since its inception, the group is organized around projects, which study the problems from complementary perspectives, and where a balance is maintained between theoretical and experimental computer science research.

During the first five years, we have been involved in the design of an object-oriented datamodel based on Category Theory and the design and implementation of a Distributed Main-Memory Database Machine.

In the coming five years, our research efforts will be further focussed on the object-oriented approach, such as the formalisation of an object-oriented database design, the development and the evaluation of efficient algorithms for object-oriented databases in a distributed environment, and the storage management of replicated objects in a distributed system.

3. Research 1987-1991

Research in this period centered around several projects: PRISMA, Floc, Tropics, ISDF, and ECOS. They are discussed briefly below.

The PRISMA project (1986-1990) was a large-scale research effort (30 persons) in the design and implementation of a highly parallel machine for data and knowledge processing. It was organized as a nationwide Dutch research activity with combined forces from four universities, a governmental research institute, and Philips Research Laboratories.
During these years considerable effort was spent by our members in the PRISMA team on the design and prototyping of the database system, which resulted in ca. 45K lines of documented POOL code, developed together with our partners at Twente University. By the end of 1988 a stable interpreter for the programming language POOL became available, which was used to finalize the prototype PRISMA/DB in the spring of 1989. This first implementation round was finished with a two-day workshop to evaluate the code produced and to assess future enhancements.
Awaiting the delivery of the POOL compiler for the multi-processor machine, we spent our time on research issues related to the PRISMA database system, such as an evaluation of the programming language POOL for its expressiveness of relational database concepts at the level of the One-fragment manager, database recovery, and the semantics of nested queries in SQL. In 1990, we had to rework major portions to make the system run on the 100-node multiprocessor.
The Ph.D project Floc ran from 1985 till 1989. It aimed at the formalisation of object oriented datamodels, in particular the structural parts of these models. Moreover, a design theory for this formalism was developed.
As category theory is the mathematical theory of structures, it was chosen as vehicle for the development of the formalism called Floc. During the course of this project, category theory proved to be more than adequate to formalise both the static and the dynamic structure, including constraints, of object oriented datamodels. Moreover, it allowed for the inclusion of negative and disjunctive information as well as the development of a, deductive, query language for Floc.
The main theme for the design theory was on structural equivalence, for which category theory proved to be, again, indispensable. Briefly, this allows a database designer to switch between alternative, but equivalent, models of the same Universe of Discourse. For example, it was shown that traditional constraints such as functional, multivalued and join-dependencies can also be modelled by a suitable type construction and a (simple) dynamic constraint.
The Esprit-II project TROPICS ran from 1989 till June 1990. One of the major themes in this project was to enhance the PRISMA database system to become a viable platform for carthographic and office systems. Therefore, our group has developed an extended version of SQL and implemented a prototype for feasibility studies. After termination of this project, we refocussed our effort on active databases.
The Integrated Systems Design Framework (ISDF) project (1990-1993) is a research collaboration between several Dutch universities. The overall goal of this project is the development of an integrated framework for the description of information systems and the analysis of information systems descriptions within this framework. The importance of such a framework lies in the outlook it offers for the development of truly integrated information systems design methodologies, which apply hitherto largely unused mathematical theories for the analysis of their design. In particular, it provides a sound theoretical basis for such

methodologies to formulate requirements and logical designs, and it forms a reference point for the accompanying software development tools.
The task of our group is, in close collaboration with Twente University, to develop a formalism which is suitable for both:

- the expression of the design concepts within the framework, such as specialisation and generalisation;
- the analysis of a design with regard to structure, dynamics and constraints, for problems such as structure equivalences, lifeness/deadlock and consistency, as well as the interaction between these three areas.

The activities undertaken are an extension of our earlier research in Floc. In the past year, structure equivalence has, again, be a major theme. In particular, a sound and complete axiom system for structural equivalence for a large collection of type-systems has been developed. Moreover, a Datalog-variant for deduction over databases with complex objects and subtyping has been defined. The semantics of this language have been defined using category theory. Finally, the design-theory for object oriented databases is now focussed on the normalisation of class-hierarchies.
The ECOS project (1990-1993) aims at the design of the nucleus of a new generation DBMS, which provides the user a model and query language to describe and manipulate graph-like objects. The task of such an object server is to efficiently implement the model on a (distributed) computing system, shielding the complexity of maintaining the fragmented representation through clustering, indexing, and query-evaluation strategies.
The research actions within our group focus on the software architecture of an extensible complex object server (ECOS) with an emphasis on active database support and dynamic distributed query processing. An active database systems is characterised by a set of event-condition-action pairs, which describe actions to be taken upon encountering an event in a particular database state. In a dynamic query processing scheme one considers query processing in a distribute setting as a scheduling and load balancing problem. The expectation is to achieve better system utilization (and response time) compared to traditional approaches (such as PRISMA).

4. Plans for the future

The research activities for the coming years are settled and aimed at getting the Ph.D. theses out. Future directions are likely to explore the problems associated with interoperability and evaluation of database technology in other parts of science.
Our current projects are mostly financed externally by SION and NFI. For the future we aim for acquiring Esprit-III and STW funds. Currently (June 1991) we are discussing several ESPRIT-III projects with colleagues in France, the Netherlands, UK, Germany, and Italy in the following areas: Development of a complex object server (B-type), Performance analysis and evaluation of DBMS architectures (B-type), and Formal models for object-oriented databases (BRA).

5. Cooperation 1987-1991

1. About 80% of the manpower in this period was financed through SPIN, SION, NFI, Esprit-II
2. Cooperation with Dutch industry is mainly focussed through the Software Engineering Research Center. Foreign contacts through Esprit-II reviewer role.
3. The projects described above were conducted in close cooperation with the database research group of Twente University (prof. P.M.G. Apers), operating systems group UvA (prof. B. Hertzberger), Philips Research Laboratories (dr. L. Nijman), and that of the Free University (prof. Van de Riet).

6. Further activities 1987-1991

Dr. M.L. Kersten

- Associate professor Free University, Amsterdam;
- EDBT International Conferences, referee;
- EDBT'90, Venice, Italy, programme committee member;
- ESPRIT-II, EP 2025, European Declarative System, reviewer;
- HIO- "Oost-Nederland", reviewer;
- International Conference on Very Large Databases (VLDB), referee;
- International Conference on Very Large Databases (VLDB '89), Amsterdam, 22-25 August, 1989. 520 participants, organizing chairperson;
- Journal on Data and Knowledge Engineering, referee;
- National Scientific Board (WAR) of SION, member;
- National Scientific Board of Information Systems Research (WIS), member;
- SIGMOD Conference, referee.

Dr. A.P.J.M. Siebes

Workshop Object-Oriented Databases, Aug 20-21 1989, Amsterdam, 60 participants, organizer;
Workshops ISDF project, 1990 & 1991, The Netherlands, organizer.

7. Experimental systems and programs 1987-1991

None.

8. Selected Publications 1987-1991

1. M.L. Kersten, P.M.G. Apers, M.A.W. Houtsma, E.J.A. van Kuyk, R.L.W. van de Weg (1987). A Distributed, Main-Memory Database Machine; research issues and preliminary architecture, Proc. 5th Int. Workshop on Database Machines, Karuizawa, Japan, pp. 496-512.
2. A.P.J.M. Siebes (1990).On Complex Objects. Ph.D. Thesis, University of Twente.

RESEARCH GROUP AA5
CONSTRUCTIVE ALGORITHMICS

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
prof. L.G.L.T. Meertens	group leader (also 0.3 fte AA3)	0.3 fte	
Non permanent:			
drs. M.M. Fokkinga	researcher (on secondment from UT)	1.0 fte	01.07.87-01.07.91
dr. J.C.S.P. van der Woude	researcher (NFI) (on secondment from TUE)	0.8 fte	since 01.10.90
drs. J.T. Jeuring	junior researcher (NFI)	1.0 fte	since 01.01.88
Former staff member 1987-1991:			
Dr. C.C. Morgan	guest researcher (NFI)	1.0 fte	15.03.90-01.10.90

2. Introduction

Two prominent concerns in program design and implementation are correctness and efficiency. Efficient algorithms are usually complex, and therefore hard to get correct. Evidently correct algorithms, on the other hand, are often not of an acceptable efficiency. 'Transformational Programming' is an approach to the design of correct *and* efficient algorithms. The basic idea is as follows. Start with a high-level specification, paying only attention to its correctness. Next, derive an efficient implementation from it by a sequence of meaning-preserving 'transformations'. In this last phase, the concern for efficiency guides the selection of the steps to be tried. With regard to correctness, the only concern is not to make clerical errors. In principle, it should be possible to check the steps mechanically.

In spite of a large international effort, and substantial achievements on small examples, the research in this area has largely not fulfilled the early promises. The general trend has been to aim for more mechanisation of the derivation process, but this has not resulted in substantial improvements. Considering the bare essence of the transformational approach, it is clear that it is a form of formula manipulation, something that is at the heart of the daily practice of mathematics. Yet, the usual transformational derivation is in spirit very unlike a mathematical one all the things that make mathematics manageable in practice are absent. In much of the work in program construction the basis is a formalisation of some programming language which justifies the transformations. The formalisation yields a fixed and not problem-oriented theory in which a derivation has to proceed.

No working mathematician could obtain results if forced to work in a theory like ZFC, or pure predicate calculus the level is too low. But it is also not the case that a new theory is developed specifically for each next problem. A working mathematician uses a collection of established theories that were often developed, extended and refined over a long period of

use. Our diagnosis is that there is nothing wrong with the transformational idea perse but that the problem lies in the quite unmathematical spirit with which it is usually approached.
In a nutshell, then, the research of the group focusses on increasing the applicability of the transformational approach by *explicitly recognising its mathematical nature*. This requires reconsideration and remodelling of the fundaments, using algebraic and category-theoretic tools. The research is concerned with the development of concepts, notations, formalisms and methods, on a high level of abstraction, for deriving algorithms from a specification. The issues investigated include the unification of specification formalisms and formalisms for denoting algorithms into formalisms that are *amenable to calculation*, and the development of *specialised theories* for certain data types or classes of problems, in all cases with the aim to uncover principles of a broad applicability to a diversity of problems. The aspiration of the constructive-algorithmics approach is to cover, eventually, large parts of the 'tricks of the trade' of the practice of computing, and to provide a body of concepts, notations and theories with which the methods and results in such areas can be described and taught in a systematic way.
This rather ambitious goal can of course only be reached if research in this area is pursued on a larger scale than it is today, which by itself is a reason to attach importance to cooperation. In any case, actual progress requires tackling, one by one, specific problems which by themselves are of a modest scale.
The present research group started in 1988, with the appointment of Jeuring as junior researcher, although Meertens has done research in this area since 1978 with a time involvement that was very limited (except during a visit to NYU in 1982/1983).

3. Research 1987 - 1991

Most of the results that have been obtained to date are characterised by taking an algebraic view on certain important data types and considering homomorphisms on the algebraic structures obtained. From a theoretical perspective this is nothing new; the novelty of the approach lies in the development of notation that makes it possible to express this in a way that is suitable for calculation. This approach, which was developed in collaboration with Richard Bird (Programming Research Group, University of Oxford), has proven surprisingly fruitful. Many important 'program transformations' turn then out to be special cases of general and simple algebraic identities. By using initiality of the algebra, and therefore the unique property of homomorphisms (usually in the form of so-called 'promotion properties'), induction proofs can be replaced by calculation using equational reasoning. An important impulse to the research was given by the work of Grant Malcolm (then at Groningen), who showed how to formulate various results 'generically', that is, independent of a specific data type, by using a categorical approach.
This productive approach has by no means been exhausted, and extensions in several directions have been explored: to infinite structures, which correspond to a final rather than an initial algebra, to categories of continuous algebras, and to categories (or 'almost' categories) in which the morphisms are relations rather than functions. In all these cases it is possible to use a calculational style of program derivation. An important recent result is the discovery by Fokkinga of a very elegant category-theoretical formulation of the notion of 'law' imposed on a data-type, which abstracts from the algebraic signature by using instead its encapsulation as

an endofunctor. The work on relations was initiated by Roland Backhouse (first at Groningen, now at Eindhoven). In the context of VLSI design, methods that are closely related in spirit and contents have been developed and used by Mary Sheeran (Glasgow) and Geraint Jones and Wayne Luk (Oxford) for the synthesis of essentially systolic algorithms.
Part of the research approach is an emphasis on theory development that is example-driven, by focussing each time on a specific problem or class of problems (and methods). Jeuring has given calculational derivations of (in some cases well-known) algorithms for a diversity of classes of problems on sequences, and of new algorithms for such problems on other data types, such as binary labelled trees and multi-dimensional arrays. The general method is the systematic derivation, by calculation, of conditions under which the efficient computation of an optimal 'disposition' (for sequences, e.g a segment, subsequence, partition or permutation) is possible, which are then applied to specific problems, like sorting, pattern matching, or the 0-1 knapsack problem. Recently, the synthesis of programs involving asynchronously communicating processes has begun to appear to yield to a relational approach, but much remains to be done there (work in cooperation with Morgan, Oxford).
Next to the development of theory, some attention has been paid to design requirements for tools providing mechanical assistance in creating and manipulating program derivations. This is done in the context of the STOP project (see below).

4. Plans for the future

Presently, the research is performed in close cooperation with researchers at other sites, and we intend to continue this for the topics we hope to investigate in the future.
An urgent issue is the clarification of the relationship between relations as categorically introduced by De Moor, and the Eindhoven axiomatisation of the relational calculus. More in general, we want to investigate the possibilities for calculationally smooth transitions between various function- or relation-based formalisms, if possible extended with predicate-transformer-based formalisms, by considering the relationships between the corresponding categories. A point of particular interest is to establish a formal link for the transition from the category CPO, with powerful calculation properties but having partial (potentially diverging) functions as morphisms, to categories with only total functions. There is a wealth of problems that can be tackled by 'stepping over' at an appropriate point in the derivation, but presently we have to use ad-hoc methods and some handwaving to do this.
Now that we have a categorically tractable notion of algebraic laws, it can be investigated more generically what the role of the laws is in various results.
A further point of interest, related to both of the previous issues, is the further development of De Moor's generic theory for dynamic programming into more specialised, and calculationally more readily accessible, subtheories. As it appears now, this holds the potential of a nice integration with, as well as a better formulation and explanation of, the techniques of filter promotion and branch-and-bound, and various 'greedy' methods. The 'Theorems for Free!' result of Wadler (independently found by De Bruin of Groningen) can sometimes yield a dramatic simplification of the calculations. Although it appears to have a categorical flavour, tied as it is to the notions of functor and natural transformation, its applicability is based on proof-theoretical properties of the second-order polymorphic lambda-calculus with polymorphic typing in the sense of Girard and Reynolds, and the result

does not hold in all categories with which we want to work. It appears, however, that the 'free theorems' sometimes do work in other categories. We should like to understand better what exactly makes them work when.
An area into which some recent excursions have been made is that of deriving incremental algorithms. The preliminary results strongly suggest that this topic is rich enough to serve as the focus for Ph.D. research. The Views project in the department is an immediate source of inspiration for practical problems in this area. The research concerning the use of relational techniques for constructing distributed programs composed of asynchronous processes will be continued, in cooperation with Morgan at Oxford and Joost Kok at Utrecht, and possibly Manfred Broy in Munich.
Finally, we mention that Meertens is planning to collaborate with Bird in writing a book summarising their joint research.
While there is no lack of interesting and promising topics to explore, the future shape of the group is unclear. The externally funded STOP project runs until the end of 1992, but in 1991 already two of the current group members will complete their Ph.D. research and leave CWI (one to serve Her Majesty, the other, being on secondment, returning to Twente University). In 1992 a third group member, on secondment from Eindhoven, will leave CWI.
Unless it is possible to maintain at least some research positions, it will not be possible to continue the group as such at CWI after 1992.
Currently there is no allocation for CWI-financed positions in the group next to that of the group leader. Since this year the possibility exists for CWI to submit grant proposals to SION (the Dutch equivalent of SERC), and this has been used to apply for a junior researcher. It is, further, the intention to formalise the existing Dutch cooperation in the form of a so-called 'aandachtsgebied' (literally 'area of attention') within SION. A proposal has been formulated, together with Eindhoven, Twente and Utrecht, but is currently being held awaiting a procedure for establishing these 'areas of attention'.

5. Cooperation 1987-1991

On a national scale, the group forms part of the STOP project (Specification and Transformation Of Programs), a joint effort with the Catholic University Nijmegen and Utrecht University, sponsored by the NFI (Nationale Faciliteit Informatica). An important aim of the STOP project is to increase the level of expertise in this area in the Netherlands, among other means by holding regular meetings, seminars, workshops and summer schools, and inviting foreign experts.
As already indicated before, there also exists a close cooperation with the PRG at Oxford and with Eindhoven.
An ESPRIT BRA proposal involving, among others, the universities of Eindhoven, Glasgow, Oxford and Utrecht, is in preparation. Although CWI is formally not a partner in the proposal for technical 'grantological' reasons, if awarded it would make travel funds available to members of the group for participating in the activities.
For the quick distribution of results between researchers in this area a forum was created in the form of an (unrefereed) journal, *The Squiggolist*, edited by Jeuring. Its first volume saw four issues with altogether 19 articles by 13 different authors.

Weekly research meetings are held at Utrecht, which are also attended by researchers from the Universities of Eindhoven, Groningen, Nijmegen, Twente and Utrecht.

6. Further activities 1987-1991

Prof. L.G.L.T. Meertens
- Commmissie Nationale Faciliteit Informatica (NFI), member
- International Summerschool on Constructive Algorithmics, Hollum, Ameland, 12-21 September, 1989, 50 participants, co-director
- STOP Workshop on Program Transformation & Specification: Paradigms, Tactics & Strategies, Noordwijkerhout, 18-21 April, 1989, 44 participants. co-organiser.

7. Experimental systems and programs 1987-1991
None.

8. Selected publications 1987-1991
1. M.M. Fokkinga and E. Meijer.Program calculation properties of continuous algebras.Technical Report CS-R9104, CWI, Amsterdam, January 1991.
2. J.T. Jeuring (1990). Algorithms from theorems. In M. Broy and C.B. Jones, editors, Programming Concepts and Methods, North-Holland, pp. 247-266.
3. Lambert Meertens (1990). Paramorphisms.Revised version of Technical Report CS-R9005, CWI, Amsterdam. To appear in: Formal Aspects of Computing.

RESEARCH GROUP IS1
COMPUTER GRAPHICS
State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

Drs. A.A.M. Kuijk	group leader	1.0 fte	
Dr. M. Bakker	programmer (from STO)	0.2 fte	
F.J. Burger	programmer (from STO)	1.0 fte	
Drs. W. Eshuis	researcher	1.0 fte	

Non permanent:

Dr. E.H. Blake	researcher	1.0 fte	since 01.04.88
Drs. V.C.J. Disselkoen	junior researcher	1.0 fte	since 02.01.90
M.A. Guravage	programmer	1.0 fte	since 08.01.89
R. van Liere	programmer	1.0 fte	

2. Introduction

The group IS1 is involved in aspects of basic graphics systems. Research is centered around configurability for efficient use of hardware resources and support for interactive use.
To achieve this part of the research is focussed on hardware architectures and related graphics algorithms. This includes design and implementation on VLSI for those parts of the architecture for which the functional requirements and/or capacity cannot be met by of-the-shelf hardware.
Another important theme of the research is to develop a methodology in which the specification of highly interactive programs and systems can be achieved in an effective and efficient way. Initially, this research focussed on the specification of interactive programs. Later this research was focussed on the specification of interactive systems and the role of the graphics pipeline in these systems.

Division in projects

- Design and development of an interaction based architecture;
- Design and development of the dialogue cell system;
- Formal specification of input models;
- Specification techniques for configurable graphics pipelines.

3. Research 1987-1991

The research between 1987 and 1991 involved the design of an interaction based graphics workstation. This work was initiated by a study on interaction aspects which formed the basis of the design of a non-conventional architecture. The feasibility of this design was shown by actual implementation on VLSI of some of the critical modules in the architecture. With these modules a complete prototype will be assembled by the end of 1991. The feasibility study

included development of new shading algorithms, optimized for the specific hardware configuration. These algorithms turned out to be generally applicable and are competitive to existing efficient algorithms. To support the design effort, a graphics hardware simulator has been implemented. The modularity of this simulator makes it suitable to implement a layered set of simulators, needed for design validation on different abstraction levels.
Besides this, the research between 1987 and 1990 involved the development and completion of the dialogue cell system. The dialogue cell system has been used in house as a tool for the development of user interfaces. More recently, it has been used by an external software house.
From 1990 onwards, this research has been directed towards the specification of highly configurable graphics subsystems. To gain insight in this type of systems, research has been done in spatial subdivisioning techniques for a class of radiosity algorithms.
In 1991, work is being done on identifying research areas for the CWI research theme on Scientific Visualization. This new research theme is scheduled to start in 1992.

4. Plans for the future

a. Continuation of research in configurable graphics subsystems based on the previously obtained results. In particular, the interaction facilities of the new architecture will be used for further exploration of the area of animated interaction.
b. Continuation of research on graphics algorithms. This will be focussed on generic texture functions, transformation invariant functions and concurrent object space HSR algorithms.
c. Research on the relation between image analysis and image synthesis.
d. Start of the research theme on Scientific Visualization. Initial research will focus on development of a methodology for the steering of applications in a highly interactive computing environment.
e. Start of a project on multimedia. This project is going to be a large scale effort which spans a number of departments at the institute. In order to bring it off, the CWI has to attract funds from industry as well as its more traditional government and European Community sources.
f. Joint proposal of an STW project (on graphical simulators) currently being evaluated.

5. Cooperation 1987-1991

A. Contract research
STW.

B. Contacts and/or cooperation with industry
TNO-IBBC, Océ, Philips CAD center, NLR, PTL (Groningen) and DTN.

C. Contacts and/or cooperation with scientific institutes
Univ. of Twente (Dept. of Manufacturing), Univ. of Twente (Dept. of Electrical Engineering), Rutherford Appleton Laboratories, GMD (Dr. P. Wisskirchen) and University of Geneva (Prof. Thierry Pun).

6. Further activities 1987-1991

Drs. A.A.M. Kuijk
Reviewer Computer Graphics Forum.

- Eurographics '87 Conference, chair poster-session;
- Second Eurographics Workshop on Graphics Hardware, 24-25 August, 1987, Amsterdam 27 participants;
- Third Eurographics Workshop on Graphics Hardware, 11-12 September 1988, Sophia-Antipolis, France.

Programme committee:
- Second Eurographics Workshop on Graphics Hardware, 24-25 August, 1987, 27 participants;
- Third Eurographics Workshop on Graphics Hardware, 11-12 September 1988, Sophia-Antipolis, France.
- Fourth Eurographics Workshop on Graphics Hardware, 3-4 September 1989, Hamburg, Germany;
- Fifth Eurographics Workshop on Graphics Hardware, 2-3 September 1990, Lausanne, Switzerland;
- Sixth Eurographics Workshop on Graphics Hardware, 1-2 September 1991, Vienna, Austria.

Editor:
Springer-Verlag EurographicSeminars Series:
- Advances in Computer Graphics Hardware II;
- Advances in Computer Graphics Hardware III.

Drs. W. Eshuis
- Member conference board EUROGRAPHICS, the European Association for Computer Graphics;
- Eurographics'87 Conference, 24-28 August 1987, Amsterdam, 400 participants, secretary.

R. van Liere
- ACM Computer Surveys, reviewer;
- Computer Graphics Forum, reviewer;
- Eurographics '87 Conference, tutorial on User Interface Management Systems;
- ISO/IEC/JTC1/SC24/WG1 and SC24/WG2, NNI representative;
- ISO/IEC/JTC1/SC24/WG1 Workshop The New API, CWI, 15-17 February, 1989, 15 participants, organiser;
- ISO/IEC/JTC1/SC24/WG1 Workshop An Improved Graphics Input Model, CWI, 15-17 February 1989, 5 participants, organiser;
- PAO Course on Computer Graphics, Amsterdam, February. '90.

Dr. M. Bakker
- ISO/IEC/JIC1/SC24, SC24/WG2, and SC24/WG4, NNI representative;
- Stichting Computer Grafiek, chairperson.

Dr. E.H. Blake
- Second Eurographics Workshop on Object-Oriented Graphics, 4-7 June, 1991, De Koog, the Netherlands, 31 participants, co-chairperson;
- SigGraph '91 Conference, Course on "Constraint and Object Paradigms for Graphics"
- Springer-Verlag EurographicSeminars Series, editor Advances in Object-Oriented Graphics I;
- Eurographics '89 Conference, 4-8 September 1989, Hamburg, Germany, Tutorial on Object Oriented Graphics;
- Eurographics '90 Conference, 3-7 September 1989 Hamburg, Germany, Invited state-of-the-art report on Object Oriented Graphics;
- Eurographics working group on the relationship between image analysis and image synthesis, joint co-ordinator;
- First Eurographics Workshop on Object-Oriented Graphics, 5-8 June, 1990, Königswinter, BRD, 34 participants, co-chairperson;
- Computer Graphics Forum, reviewer.

7. Experimental systems and programs 1987-1991

1. DICE - An experimental system for developing interactive systems according to the dialogue cell methodology.
2. RADIOSITY - An experimental system for researching the behaviour of various spatial subdivisioning schemes. This system will provide insight in how a set of graphical resources should be configured in order to effectively solve the radiosity equations.
3. Interactive shading algorithm testbed - Object-oriented extensible system for testing shading algorithms on Sun Workstations. Developed second half of 1988. The main algorithm tested was the angular interpolation method Phong shading. Images produced were also used to illustrate various papers on the subject.
4. XInPosse - A structural simulator to both validate hardware design and to visualize software that should run on that hardware. In a layered set of graphics hardware simulators, this one bridges the gap between hardware fidelity on the one hand and sufficient performance to visualize graphics algorithms on the other. In order for this simulator to be extensible and reusable, object oriented methods were adopted. It is the intention to use the modularity provided by the object-oriented design to produce a toolkit for building graphics hardware simulators.
5. An interactive testbed for object space hidden surface removal algorithms. With this testbed a variety of 3D models can be constructed. The reduced 3D model a HSR algorithm produces can be manipulated for visual inspection. The user interface part of the tested runs on a SiliconGraphics workstation. The HSR algorithms can run on remote platforms, including multiprocessor configurations for concurrent implementations.

8. Selected publications 1987-1991

1. A.A.M. Kuijk & E.H. Blake. Faster Phong Shading via Angular Interpolation, Computer Graphics Forum, 8, 4, pp. 315-324.
2. F. Kuijk, R. van Liere. Display architecture for VSLI-based graphics workstations. CWI-Quarterly.
3. R. van Liere. Divide and Conquer Radiosity. Preprints of the Second Eurographics Workshop on Rendering, Barcelona, Spain, 13-15 May 1991. To appear as Proceedings (ed. F.W.J. Jansen), Springer-Verlag.

RESEARCH GROUP IS2
INTERACTION

State of the project, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
Dr. I. Herman	group leader	1.0 fte	
Drs. P.J.W. ten Hagen	researcher	0.5 fte	
Drs. C.L. Blom	researcher	1.0 fte	
Drs. M.M. de Ruiter	researcher	1.0 fte	
B. Rouwhorst	programmer (from STO)	1.0 fte	
Non permanent:			
Drs. D. Soede	junior researcher	1.0 fte	
Drs. J. van der Vegt	junior researcher	0.8 fte	since 01.05.88
M. Haindl	researcher (ERCIM fellow)	1.0 fte	01.04.91-01.10.91
E. Rutten	researcher (ERCIM fellow)	1.0 fte	16.09.91-15.03.92

2. Introduction

The group, in its present format, has been formed in July 1990 only. Also, the majority of the members of IS2 works today on the "Manifold" project which is a joint project of IS2 and IS3. There is therefore a clear overlap of the activities of these two groups.

Parallelism

It has already been recognised that one of the clues to interaction is parallelism. Indeed, interactive systems usually consist of a whole set of independent actors, processes (in the abstract sense; in this case a human may also be considered as a process), and one of the major questions arising when planning and realising an interactive environment is the proper and effective organisation of cooperating processes. Previous activities of the IS department have also shown that this question plays a major role in interaction (e.g. DICE project, Dataflow project). It is for this reason, IS2 plays a major role in the Manifold project (together with IS3) both on the specification and on the implementation level. Furthermore, after having investigated some general specification rules and approaches for User Interface Management Systems (UIMS), the Manifold system should clearly be used for the development of some kind of an experimental interactive system to test the ideas and the methods involved. This cooperation with IS3 has a particular interest in the sense that it aims at exploring the underlying principles which govern AI based systems and interactive systems alike. (For the details of the Manifold Project, see the separate description).

Independently of the Manifold Project, but also in relation with parallelism in interaction, separate research is being done on the possible use of neural networks for the purposes of very intelligent interactive systems.

General Purpose Interactive Graphics Standards

The second project, in which IS2 is involved aims at the development of a standard software base for the coming generation of advanced graphics capabilities. The project is very ambitious, and it is clearly not realisable within one research group of CWI; instead, this project (referred to as NEW API project) will hopefully become one of the flagship projects of ERCIM in the near future. IS, and especially IS2 plans to play a leading role within the project itself. It has to be made clear that the project is in this very moment in its planning stage. The main characteristics of the project are as follows.

Some of the major technical concerns in the specification and the development of a new generation graphics standard is extensibility and to provide a real platform for wide-scale integration. Indeed, it has been recognised that one of the main deficiencies of the older graphics systems specified by ISO is the fact that they provide a fixed set of functions only, in the form of a closed function specification; a set of functions which tends to be extremely large and therefore very hard to comprehend and use. Also, new application areas have turned towards graphics in the past years and very often the ISO standards could not offer those specific functionalities these new application areas needed. For example, GKS and others failed to serve as a common platform for the integration of different albeit related fields, like image analysis, multimedia, image processing, and image synthesis. These specifications also had and still have difficulties in being used properly on modern window-based workstations.

It has also been recognised that, to achieve these goals, a radically new approach is needed, based on the newest results and models in computer science. Methods based on an object-oriented approach, explicit use of concurrency and parallelism are all at the basis of a new graphics system, which should also give the possibility to include the most up-to-date results of the research concerning full realism.

The expertise already present and to be gained by the activities of IS(2) will strongly influence the activities on the development of general graphics systems in general, especially in the specification of a new international graphics standard, which should be done in cooperation with IS1 and, basically, within the framework of an ERCIM cooperation. Based on the previous activities of IS members in the international standardisation bodies on graphics standards (activities which date back, in some cases, to 10 years) IS can play a major role in the specification and also the pilot implementation of such modern graphics standards.

3. Research 1987-1991

As stated before, the group is only one year old. In the past year, the group has actively taken part in the specification and the implementation work of the Manifold system, aspects of its visual programming. As a first larger example (and related also to the NEW API acitivities), the GKS Input Model has been fully described with the help of the Manifold computing model; this has proven the feasibility of this model to be used for future generation interactive graphics standard (the paper resulting from that work has been offered for publication lately).

4. Plans for the Future

We will continue our activities in the field of parallelism versus interactivity in the future. This activity will have two differents facets:

1. How does parallelism influence the development of interactive systems, how can parallelims be used to conceive and develop new graphics systems, etc.?
2. How to visualize, debug, visually program parallel systems?

Clearly, the efforts on the Manifold project will still go on for a while. The first, experimental version of the system is expected by the end of the present year. We intend to use this system to develop new models; by making these tests, it is almost sure that an upgraded version of this model and language will have to be developed, still jointly with IS3. A possible commercial outcome for the system is also possible. Parallel to these activities, a visual interface and programming/debugging tool is and will be under development as a case study for the questions arising in section 2 above.

The NEW API project (if it gets financed) will lead to another significant effort both on the conceptual and development level. It is to be expected (just as it was the case with older Standards) that while working on its specification and pilot implementation, a number of algorithmic problems will arise which might lead to new directions of development in computer graphics; details of such directions are not clear yet.

5. Cooperation 1987-1991

A. Contract research

None.

B. Contacts and/or cooperation with industry

The dataflow project (see below) has been done (in the years 1988-89) in cooperation with Dataflow Technology b.v., Den Haag.

C. Contacts and/or cooperation with scientific institutes

The NEW API project from the start has been a cooperative project with INRIA, RAL and GMD; CNR Pisa has joined recently. The idea is to have this project accepted as a project of the European Steering Committee for Computer Graphics (this is under way at the time of writing this report).

6. Further activities 1987-1991

Computer Graphics Forum:
Drs. P.J.W. ten Hagen, member editorial board;
Drs. M.M. de Ruiter, chief-editor.

EUROGRAPHICS, the European Association for Computer Graphics:
Drs. P.J.W. ten Hagen, vice-chairperson (1987/88), member executive committee, chairperson working groups and workshops board (1988/89);
Dr. I. Herman, member executive committee, chairperson working groups and workshops board (from 1989);
Drs. M.M. de Ruiter, member executive committee.
EUROGRAPHICS '87 Conference, 24-28 August 1987, Amsterdam,

400 participants:
Drs. M.M. de Ruiter, chairperson tutorials;
Drs. P.J.W. ten Hagen, chairperson.

EUROGRAPHICS '88 & '89 Conference:
Drs. P.J.W. ten Hagen, member programme committee:
Dr. I. Herman, member programme committee.

EUROGRAPHICS '90 Conference:
Drs. P.J.W. ten Hagen, member programme committee;
Dr. I. Herman, co-chair tutorials.

EUROGRAPHICS '91 Conference:
Drs. P.J.W. ten Hagen, member programme committee;
Dr. I. Herman, member programme committee.

Eurographics Workshop on Mathematics and Computer Graphics, October 1991, Genova: Dr. I. Herman, co-chairperson.

European Steering Committee for Computer Graphics:
Drs. P.J.W. ten Hagen, committee member.

Multimedia, the state of the art, round table discussion, 11-12 April, 1990, CWI. 26 participants.

NGI (Nederlands Genootschap voor Informatica):
Drs. P.J.W. ten Hagen, board member.

PAO Course on Computer Graphics, Amsterdam, February'90:
Drs. C.L. Blom, Drs. P.J.W. ten Hagen.

Third Eurographics Workshop on Graphics Hardware, 11-12 September 1988 Sophia-Antipolis, France:
Drs. P.J.W. ten Hagen, member programme committee.

Wetenschappelijke commissie NLR-NIVR:
Drs. P.J.W. ten Hagen, member subcommittee computer science and applied mathematics.

7. Experimental Systems & Programs 1987-1991

- One of the major developments within IS was the so-called Dataflow Project, lead primarily by members of IS who are now in IS2 (At the time of this development IS2 did not exist in its present form, and the project was under the heading IS1). This was a joint project with Dataflow Technology b.v. (The Hague) and the aim was the development of a high-speed

graphics terminal based on a NEC dataflow processor and a custom-designed graphics controller board. The hardware development was concentrated on Dataflow Technology, whereas the software planning and development was done within CWI. As such, the following software modules (partly in Dataflow Assembly, Partly in Microcode and partly in C) were done at CWI (or contracted out by CWI):

- 3D rendering microcode for graphics output.
- Complete transformation pipeline and graphics hardware control in dataflow.
- UNIX drivers for the graphics controllers and the dataflow board.
- High-level drivers to interface the graphics system from GKS-3D, and other high-level graphics systems.
- Restricted C to Dataflow compiler.

Only part of the software could be tested through simulation. The project was ended by the external financers (of Dataflow Technology b.v.) before the actual hardware could be delivered to use.

- In the past year the Manifold compiler development was done within IS2; as such, the following developments are still under way (again, together with IS3):
  - Manifold intermediate language specification.
  - Compiler from Manifold programs to the intermediate language.
  - Specification of the runtime model (based at this moment on Concurrent C++, but possibly environment independent) of the Manifold computing model.
  - Implementation of the runtime model in Concurrent C++.

- An Interactive, structured picture editor was developed (and is still under development) by J. van der Vegt; it has originally been developed under Hypernews on SUN SparcStations, and is now being ported to X11.

8. Selected Publications 1987-1991

1. P.J.W. ten Hagen, I. Herman and J.R.G. de Vries (1990), A Dataflow Graphics Workstation, Computers Graphics, Vol. 14. (Also CWI Report CS-R8910).
2. F. Arbab and I. Herman (1991). MANIFOLD: A Language for Specification of Inter-process communication, Proceedings of the EurOpen Autumn Conference, Budapest, September 1991. (Also CWI Report CS-R9065).
3. D. Soede, F. Arbab, I. Herman and P.J.W. ten Hagen (1991). The GKS Input Model in MANIFOLD, Computer Graphics Forum, Vol. 10.

RESEARCH GROUP IS3
INTELLIGENT CAD SYSTEMS

State of the project, June 1991

1. Staff (situation July 1st, 1991)

Permanent:			
Drs. P.J.W. ten Hagen	researcher	0.5 fte	
Non permanent:			
Dr. F. Arbab	group leader (NFI)	1.0 fte	since 01.01.90
Drs. H.E. v. Klarenbosch	junior researcher (NFI)	1.0 fte	since 01.06.91
Ing. D.B.M. Otten	junior reseacher	1.0 fte	since 01.01.88
Ir. J.L.H. Rogier	researcher (from TNO)	1.0 fte	since 01.12.86
Ir. P. Spilling	junior reseacher (NFI)	1.0 fte	since 01.01.88
Drs. P.J. Veerkamp	researcher (NFI)	1.0 fte	
Drs. R.C. Veltkamp	junior researcher (NFI)	1.0 fte	since 16.02.90
NN	junior researcher (NFI)	1.0 fte	

2. Introduction

The goal in this group is to study the issues involved in building CAD systems that:

- contain more complete knowledge about the activity of design, as well as domain-dependent design knowledge;
- are better integrated to provide a consistent set of functionalities which can be combined to cover a broad range of the activities involved in a production cycle,
- have high-quality, high-functionality, intelligent user interfaces.

The IIICAD project started in 1987 with 75% funding from NFI plus 5% funding from TNO. The initial 3-year period of support ended in 1990, at which time further support was extended for a second 3-year period, ending in 1993.

The initial goal of this project was to attempt to develop the necessary schemes to produce CAD systems that are more complete, integrated, and have a high quality user interface. The use of AI techniques was particularly emphasized. To implement such a system, the project started to develop a language based on the object-oriented and logic programming paradigms. This language (IDDL, Integrated Data Description Language) has special dedicated features to encode existing and newly acquired knowledge about the design object, about the design process and about their relations. The encoding and treatment of design knowledge is studied in the context of geometric modelling, object-oriented databases, user interfaces and geometric reasoning.

The Design process can be defined as transforming a set of specifications into a set of object definitions, which together embody the desired functionality. This process can be structured according to the so-called design stages (e.g, analysis, synthesis, evaluation), by decomposition into subprocesses for parts of the partitioned design. Moreover, there may be forms of backtracking, iteration, detailing, etc. Every CAD system has its own model of the

design process, at least implicitly, embedded inside. To support highly interactive, intelligent CAD systems, a more explicit embedding of a flexible model of the design process is necessary. Furthermore, the CAD system itself must be conscious of this embedding.
Three Ph.D students who had joined the IIICAD project early on, and another one who joined the project in 1990, are all expected to finish their work and defend their theses within the next 4-9 months. One Ph.D student left CWI after two years in June 1991.
In 1990, two new research areas were also started in IS3: incremental satisfaction of geometric constraints, and dynamic interactions among sets of autonomous concurrent processes. The work on the latter topic is in the context of the Manifold project which is carried out jointly with the people in IS2.

3. Research 1987-1991

Our research activity in this group can be roughly divided into three areas.

1. Design knowledge representation

This effort is primarily focused on a design theory suitable for intelligent CAD, its implication on design knowledge representation, and the use of AI techniques for its implementation. The language ADDL (formerly called IDDL) was designed for this purpose. It is based on object-oriented and logic programming paradigms. The ADDL system has a two-level architecture with meta-level and object-level scenarios. Each level has its own interpreter for its scenarios, which are sets of if-then rules. Architectural design has been the test-bed of the ideas and tools developed in this effort.
Control architectures for coordination of dynamic and interactive tasks, which frequently arise in design, is another focus of research. Closely related issues involving incomplete information and belief revision are also being studied.

2. Design object representation

The primary focus of this effort is on design object modeling and its representation. An important aspect of a design object in most design applications is its geometric shape. The field of geometric modeling has by now matured to the point that efficient representation and manipulation of the nominal geometries of solids and surfaces are commercial reality. In the context of intelligent CAD, this ability is far from sufficient. Using incomplete geometric information, reasoning with the high-level semantics of geometric entities and relationships, and dealing with geometric constraints are vital necessities.
Our experiments with some of the issues in design object representation produced a language (Oar) that combines the power of logic programming for expressing declarative facts about objects and their interrelationships, with the concept of message passing as the mechanism for triggering the imperative knowledge associated with objects. Oar is being used elsewhere to implement a system for incremental satisfaction of geometric constraints in the context of a small two-dimensional drafting application. Further development and extension of this work will continue under this effort. Efficient storage, manipulation, and retrieval of large amounts of information define a different focus of activity in this effort. There are significant differences between the requirements of Intelligent CAD systems and the premises of conventional database systems. Consequently, contemporary databases do not provide

adequate solutions for the problems of information management in Intelligent CAD. Nevertheless, many of the traditional concerns in the field of databases are still valid and relevant in this domain, e.g., management of large volumes of persistent data, security, concurrent multiple access, updates and coherence, locking, etc. Furthermore, some of the major requirements of Intelligent CAD systems point in the same direction as some of the current trends in database research. These include object-oriented-ness, dynamism, evolution, heterogeneity, deductive databases, distributed databases, versions, etc.

3. Communication and interaction

The focus of this effort is on communication and interaction between processes. This is a fundamental area of research with applications in a wide range of seemingly different problems. Among them, programming of massively parallel systems, coordination of multiple agents in distributed problem solving, and flexible user interface management systems. Our ideas in this area have culminated in a new language for coordination of the interaction between independent processes, called Manifold.

Manifold is a language for defining dynamic interaction among a set of processes. A manifold definition coordinates the communication between a number of independent processes to perform a higher level task. Manifolds are themselves processes and can cooperate with other processes to perform still higher level functions. The novelty of Manifold is that unlike many other multi-process languages and systems, the primary focus of attention in Manifold is the interaction among the processes, not the processes themselves.

A special, but important, case is when one of the processes involved in a system is a person. The proper interface to such a process is quite different than that for other processes: it involves some degree of graphics (ranging from simple character shapes, to two-dimensional graphics, to three-dimensional visualizations), special timing constraints, various presentation filters, and multi-media formats. In addition to our work on Manifold, advanced AI techniques and context-dependent anticipation of user actions are among the issues being studied in the area of intelligent user interfaces.

The paradigm of event-driven cooperation among independent agents that is supported by Manifold seems to provide an appropriate high-level control in complex open systems. Specifically, it seems to be applicable to intelligent CAD system architecture. Much of a designer's activities involves manipulating a representation of a design object by adding new information, changing, and inspecting. Except for the simplest examples, this manipulation is quite complex because it involves multiple aspects of the design objects and implies different interpretations of its representation. The most natural architecture to accommodate such an activity is that of multiple cooperating expert agents. In an intelligent CAD system, the context in which such agents cooperate may change in time. Even the exact purpose of the activity of an agent may be initially unspecified: it may, for instance, discover its exact purpose in time by inspecting the status and the contents of the design object representation.

4. Plans for the future

Until the end of 1992 the workplan fairly accurately follows the approved NFI project proposal. After 1992 attempts will be made to produce several practical results which will have great value also as evaluations. At the same time these can be the basis for further

external funding. Also the problem definitions for a successor project may take shape. A tentative list of results and research activities includes:

a. Constraint satisfaction, especially in the area of geometry and in the context of interactive, incremental resolution.
   F. Arbab and R. Veltkamp have already done some work in this area, and the Vrije Universiteit group is also now actively involved in general constraint satisfaction. This work is likely to continue more intensely after R. Veltkamp completes his Ph.D work in the next few months. There is a prospect for a medium-to-long-term visiting researcher whose work is also related to this area, who may arrive in late 1991.
b. Continuation of work on ADDL to include a design scenario facility and an extension for concurrent design support.
   P. Veerkamp is expected to continue his work on ADDL after he finishes his Ph.D work in Fall 1991.
c. A useful and proven implementation of the Manifold system F. Arbab, P. Spilling, and perhaps another researcher will continue their work on the Manifold system and its application in coordination of the cooperation of autonomous expert agents in design environments.
   After completion of our present implementation effort, several prospects for external funding can be pursued for the continuation of the Manifold project itself, as well as some of its applications.
d. The idea of a summer school on intelligent CAD systems has attracted interest from many people in the reseach community. Plans are being made to attract additional sponsorship to hold such an event within the next year or so. IS3 is spear heading this effort.
e. IS3 has been actively following the development of the international initiative proposal made by the Japanese for Intelligent Manufacturing Systems. Related activities and proposals in EC are also being followed.

5. Cooperation 1987-1991

A. Contract research

1. NFI project NF 51/62-514: 1986 - 1992 Intelligent CAD Systems.
2. IMS/EC:
   As soon as the green light for negotiations will be given by Brussels a proposal for a pilot study jointly with University of Tokyo and CMU will be produced. This is expected to happen at the end of 1991. At the same time a Dutch National consortium is preparing a similar proposal for extending CAD/CAM systems with advanced facilities to support mechanotronics and simulation facilities. IS participated in this effort joinly with TNO-ITP.

B. Contacts and/or cooperation with industry

TNO-ITI (ir. H. Overmeer), TNO-IBBC (ir. P. Kuyper), Philips CFT (dr. M. Brouwer), NLR (ir. M. Schuurmans).

C. Contact and/or cooperation with scientific institutes
Part of the research activity within the IIICAD project was carried out by a research group at the University of Amsterdam. This research group moved to the Vrije Universiteit in Amsterdam in February 1990. Their effort has been complementary to the work at CWI.

The IS3 group has established very good relations with several other research groups (Tokyo University, Carnegie-Mellon University and University of Glasgow). They are currently forming a consortium to participate in the worldwide IMS programme, sponsored by EC.
University of Tokyo (prof.dr. H. Yoshikawa, prof.dr. T. Tomiyama), Bilkent University, Ankara (prof.dr. V. Akman), University of Strathclyde, Glasgow (prof.dr. K. MacCallum), Université de Compiègne (dr. J.-P. Barthes), University of Edinburgh (prof. A. Bijl), Carnegie Mellon University (dr. S. Finger),Technical University, Berlin (prof.dr. F. Krause), Computer and Automation Institute, Budapest (dr. Zs. Ruttkay), Free University Amsterdam (prof.dr. J. Treur), Delft University of Technology (prof.dr. F. Tolman).

6. Further activities 1987-1991
First Eurographics Workshop on Intelligent CAD Systems, 21-24 April 1987, Noordwijkerhout, The Netherlands.
Drs. P.J.W. ten Hagen, co-chairperson;
Dr. T. Tomiyama, co-chairperson.

Second Eurographics Workshop on Intelligent CAD Systems, 19-24 april 1988, Veldhoven, The Netherlands, 38 participants:
Dr. V. Akman, co-chairperson;
Dr. P. Bernus, member programme committee;
Drs. P.J.W. ten Hagen, co-chairperson;
Drs. P.J. Veerkamp, member programme committee.

Third Eurographics Workshop on Intelligent CAD Systems
Practical Experience and Evaluation 3-7 April, 1989,
De Koog, The Netherlands, 35 participants:
Drs. P.J.W. ten Hagen, co-chairperson;
Drs. P.J. Veerkamp, co-chairperson.

Fourth Eurographics Workshop on Intelligent CAD Systems,
Mortefontaine, France, 24-27 April 1990:
Dr. F. Arbab, programme committee member;
Drs. P.J.W. ten Hagen, programme committee member;
Drs. P.J. Veerkamp, programme committee member.

IFIP WG 5.2 Working Conference on Intelligent CAD,
Columbus, Ohio, USA, 30 September - 3 October 1991:
Dr. F. Arbab, programme committee member;
Drs. P.J.W. ten Hagen, programme committee member.

Intelligent CAD Systems III, Practical Experience and Evaluation, EurographicSeminars Series, Springer-Verlag, 1991:
Drs. P.J.W. ten Hagen, co-editor;
Drs. P.J. Veerkamp, co-editor.

Intelligent CAD, III, Elsevier Science Publishers, 1991:
Dr. F. Arbab, co-editor.

7. Experimental Systems and Programs 1987-1991

1. Implementation of the ADDL system in Smalltalk.
2. 2D and 3D hierarchical approximation scheme 'Flintstones'.
3. 2D constraint satisfaction with the quantum approach.
4. Extension of the existing ADDL system to include the following features:
   - World enclosure mechanism which allows a scenario to look only at a partition of the fact-base.
   - Adding meta-predicates to the language. These predicates make a statement about the state of the design process rather than the design object.
   - Multi-world mechanism which allows for multiple scenarios being active at the same time.
5. Integrating a geometric modeler into the current version of the IIICAD system.
6. Implementation of the Manifold system.

8. Selected Publications 1987-1991

1. V. Akman, P.J.W. ten Hagen, P.J. Veerkamp (eds.), Intelligent CAD Systems II, Implementational Issues, Proceedings of the Second Eurographics Workshop on Intelligent CAD Systems, EurographicSeminars Series, Springer-Verlag.
2. J.L.H. Rogier, D.B.M. Otten, Retrospective creation of Virtual Alternative Hierarchies, in Advances in Object-Oriented Graphics, edited by E. H. Blake and P. Wisskirchen, EurographicSeminars Series, Springer-Verlag, Berlin, pp. 117-129.
3. H. Takeda, P.J. Veerkamp, T. Tomiyama, and H. Yoshikawa, Modeling Design Processes, AI Magazine, 11 (4), pp. 37-48.

RESEARCH GROUP CS1
MULTIMEDIA KERNEL SYSTEMS

State of the group, June 1991

1. Staff (situation July 1st, 1991)

Permanent:

dr. D.C.A. Bulterman	department head group leader	1.0 fte
drs. G. van Rossum	scientific programmer	1.0 fte
drs. J. Jansen	programmer	1.0 fte
D.T. Winter	programmer (on loan from NW)	0.5 fte

Nonpermanent:

prof.dr. S.J. Mullender	advisor (from UT-Twente)	0.1 fte
R. van Liere	programmer (on loan from IS)	0.5 fte

External Funding:
At present, funding proposals have been submitted to various organizations; informal agreements have been made with Hewlett-Packard Labs (Palo Alto, USA) to fund one Ph.D. candidate for work in distributed operating support for multimedia systems. Other proposals are still under consideration (see below).

2. Introduction

Multimedia research is a new direction for work at CWI; the project CS1 began in 1991. To support this work, an inter-disciplinary research theme has been defined to study those aspects of the multimedia problem which can fruitfully be addressed at CWI. In addition, the project groups of the department CST have begun to do preliminary investigations on various systems-related aspects of the multimedia problem. In this section, we will provide information on the work of the CST groups. Note that dr. Bulterman is the project leader for both the CST work and the inter-disciplinary research theme.

2.1. Project motivations

The goal of the CS1 group is to research systems support for multimedia applications at the operatingsystems level. Areas of interest include the development of robust multimedia systems that offer acceptable levels of performance and fault tolerance as well as data and location transparency for higher-level interfaces. Research themes include basic support for the synchronization and storage/access of multiple streams of component information (such as sound data, picture data and text data), development of interface structures to provide low-

level assistance in manipulation and synchronization of data, and the development of replicated information manipulation services for both data storage and data processing.
During the past year, the purpose of the CS1 project has been two-fold: first, this project has investigated the structure of a working prototype operating system kernel upon which short- and middle-term CWI multimedia research could be built; second, it has investigated operating systems interface functions for supporting various high- and low-level aspects of CWI's inter-disciplinary multimedia project.The general aspects of CWI's multimedia research goals are outlined in the Multimedia Interdisciplinary Research Theme section of CWI's long-range research plan; these plans will not be repeated here. Instead, we will comment on what we have done recently and what we hope to accomplish in the coming years.

Overview of work-to-date
Initial work on CS1 has focused on the evaluation of existing operating systems and the development of a general framework upon which to build future research systems. At the same time, we have invested one-half year in surveying detailed research projects at other institutions in order to better focus on thecore research aspects of multimedia work. We see that these two activities are intimately related: work on multimedia systems must include a practical building component, in which systems are built and evaluated; it must also include a more general modelling approach that abstracts problems from any particular implementation. Although we feel that we are still in the problem-definition stage of our work, we have tried to address both the theory and practice of multimedia systems in our initial efforts. All of the problems that we will investigate will concentrate on distributed multimedia systems: systems in which data synchronization and network scheduling play a central role. Local aspects of multimedia systems (such as database definition/access and user interface design) will be done in coordination with other research groups at CWI and elsewhere (Please see sections 3 and 4 for more details).

2.2. Research 1991
At present, we have investigated two key areas of systems-level multimedia support: the adaptation of existing distributed operating systems for multimedia work (project CS1.1) and the investigation of the systems-interface aspects of multimedia user interfaces (CS1.2). The current status of both of these projects will be briefly outlined below.

CS1.1: Operating systems evaluation
The goal of this work is to select an operating systems base for future experimentation. At present, we have had a group porting the Amoeba operating system to our multimedia platform (a Silicon Graphics 4D25G); this work is expected to be completed by September, 1991. Use of Amoeba has several advantages for our work: first, it is a system that is still evolving in functionality, meaning that (in coordination with researchers at the Vrije Universiteit in Amsterdam) we can propose extensions that are not limited by broad compatibility concerns. It is also an operating system with excellent communication performance characteristics (a key ingredient for multimedia applications).While these reasons have provided the motivation for the use of Amoeba, the final choice of this system

will depend on its perceived robustness and the degree to which constructive partnerships can be made with other groups using this system (most notably at the Vrije Universiteit). Other operating systems that are being investigated for consideration are CMU's Mach-3 kernel and the OSF/1 kernel. If we decide to use Amoeba, then we will also work together with the group of Mullender at UT-Twente (who is planning to base his research on the Mach-3 kernel) in order to insure the inter-operability of our results. Our present work has resulted in one conference paper, to be presented at the EurOpen Fall technical conference in Budapest.

CS1.2: Systems aspects of user interface support

The first-year goals of this project are to develop a deeper understanding of the problems associated with providing operating systems support for higher-level interface functions. As an initial project, we developed a document structure that could be used to encode representation-independent (and target-system independent) encoding of multimedia documents. The emphasis of this structure was to partition the general processing pipeline in such a way documents could be defined for a heterogeneous environment while retaining basic document synchronization and presentation information. As a follow-up to this work, we will investigate specific representations for particular applications and target platforms. This research will be done in coordination with a number of other projects at CWI, notably AA3 (Computer Systems and Ergonomics), AA4 (Databases), B4 (Image Analysis) and IS2 (Interaction). The initial focus of this work will be to investigate document manipulation primitives for creating, recalling and transferring multimedia data among heterogeneous hosts, with later work in the year aimed at developing a proof-of-concept demonstration system for the initial stages of our multimedia work. Our present work has resulted in one conference paper, presented in June 1991 at the USENIX Multimedia Research and Systems conference in Nashville, TN (USA). The basic aspects of the operating systems work on CS1 have their roots in the Amoeba project. The reader is referred to the Long-Range Scientific Programme of SMC/CWI and the annual research report for the years through 1990 to obtain a detailed description of this project. The reader is also directed to the relevant Amoeba publications listed under the AA* heading of this total report.

4. Plans for the future

The long-term goals of this research are to investigate broad operating systems level support for generic multimedia research. This investigation will complement other CWI multimedia activity and will also work in conjunction with the project CS2: Silicon Operating Systems.The emphasis of the CS1 project will be to study those aspects of (distributed) systems to provide mid-level support to the development of robust multimedia workstations in the following areas: "Operating Systems for Multimedia Workstations extensions": to Amoeba (or possibly Mach) will be designed and implemented to provide support for heterogeneous, distributed data access that provide a proof-of-concept model for more abstract (and more general) solutions to these problems. Key issues are the development of protocols for data synchronization, process scheduling and network bandwith allocation.
"Multimedia User Interface Support": new models of user interaction with the operating system to be able to access multiple streams of information concurrently. This will require the

study of new I/O access models at the system call level and new methods of inter- and intraprocess communication and scheduling.
Multimedia Database Interface Support": as a companion to the work on general user/data access, we see a need formore detailed study of the problem of support for multimedia databases in a networked environment. Research topics here include the investigation of operating systems support for data location transparency, data access synchronization and data redundancy.While many of the aspects of this work may be common with the work done for the user interface support project (above), the differences between file server and database server functionality will probably require investigation of quite separate protocol and support concerns.
In each of the areas above, we expect that our work will be cooperative in nature with other projects being undertaken at CWI and elsewhere.

In addition to the projects listed above, a separate group will be formed (project CS2) to study alternative architectures for supporting multimedia work. This project, which is named."Silicon Operating Systems", will look at the feasibility of modelling operating systems for possible implementation as (virtual or real) co-processors, much in the same way that arithmetic co-processors provide extended support for functions that do not fit on to conventional CPU systems.This project is concerned with investigating fundamental system structures for supporting high speed communications and process control support in a manner that makes them suited for direct implementation as VLSI components. Research themes include minimum functionality determination of network protocols and I/O support, algorithms for efficient buffer management that allow for synchronized access of information across I/O interfaces, and process allocation and control support for a reduced micro-kernel operating system (Note: the use of the term silicon in the title of the project should not be used to emphasize implementation architecture research; our particular goals for this project will initially be limited to studying functional differentiation at the OS level). Funding for this project is expected to be obtained in part by a joint research agreement with Hewlett-Packard Labs in Palo Alto, CA (USA).

5. Cooperation

As already indicated, CS1 is a new project that has no prior history as a single unit at CWI.As such, most of the existing cooperative efforts have been with other research groups at CWI. There have been several cooperation agreements investigated to date, however. These are:.UT- Twente: plans exist for the joint development of operating systems facilities with the group of Mullender at UT-Twente; information and protocols will be shared, and implementation of subsystems will be exchanged. Complimentary sets of hardware platforms are being developed and personnel exchanges are being investigated.
Vrije Universiteit Amsterdam: an intention exists to coordinate the future development with the group of Tanenbaum at the VU/Amsterdam. Our desire is to establish the VU as the sole distributor of Amoeba and to provide updates to this system which may possibly be integrated into future releases.

"Hewlett-Packard Labs": an intention exists to establish multi-year research support and cooperation efforts between HP and CWI. A final research support proposal is currently being considered by the multimedia operating systems group at HP.
In addition to these contacts, several joint work proposals have been submitted to various Dutch corporations and Ministries for supporting aspects of our Multimedia research. As of this writing, no firm contracts have been signed.
As a new project, a great deal of energy is being spent on establishing research contacts with other groups working on similar projects. As a result, we also expect that a number of European project proposals will be submitted for consideration in 1991 and early 1992.

6. Further activities 1991

In addition to the projects above, members of the multimedia group have considerable prior expertise with operating systems, computer communication protocols, network management and system modelling software. In addition, the principal investigator has published work on high-speed architecture design for real-time distributed computing, communication protocol evaluation, VLSI architectures for signal processing applications, and graphical modelling systems for distributed and parallel applications (This work was completed prior to 1988).

7. Experimental systems and programs

An incremental approach to prototype development is presently used by the CS1 project groups. As a result, a number of demonstration systems have been developed as proof-of-concept systems. The expectation is that this will continue.

8. Selected Publications

1. Bulterman, D.C.A., Multi-Media Research at CWI: Goals and Objectives, CST Report, 1990.
2. Bulterman, D.C.A., van Rossum, G., and. van Liere, R., A Structure for Transportable, Dynamic Multimedia Documents, USENIX Summer Technical Conference on Multimedia, June 1991.
3. Bulterman, D.C.A., Winter, D.T., and. van Rossum, G. Multimedia Synchronization and UNIX - of - If Multimedia is the Problem, Is UNIX the Solution? Preprint of Proceedings, EurOpen Fall Technical Conference, Budapest, September 1991.