



Stichting Mathematisch Centrum

J A A R V E R S L A G

'95

Kruislaan 413, 1098 SJ Amsterdam
Postbus 94079, 1090 GB Amsterdam

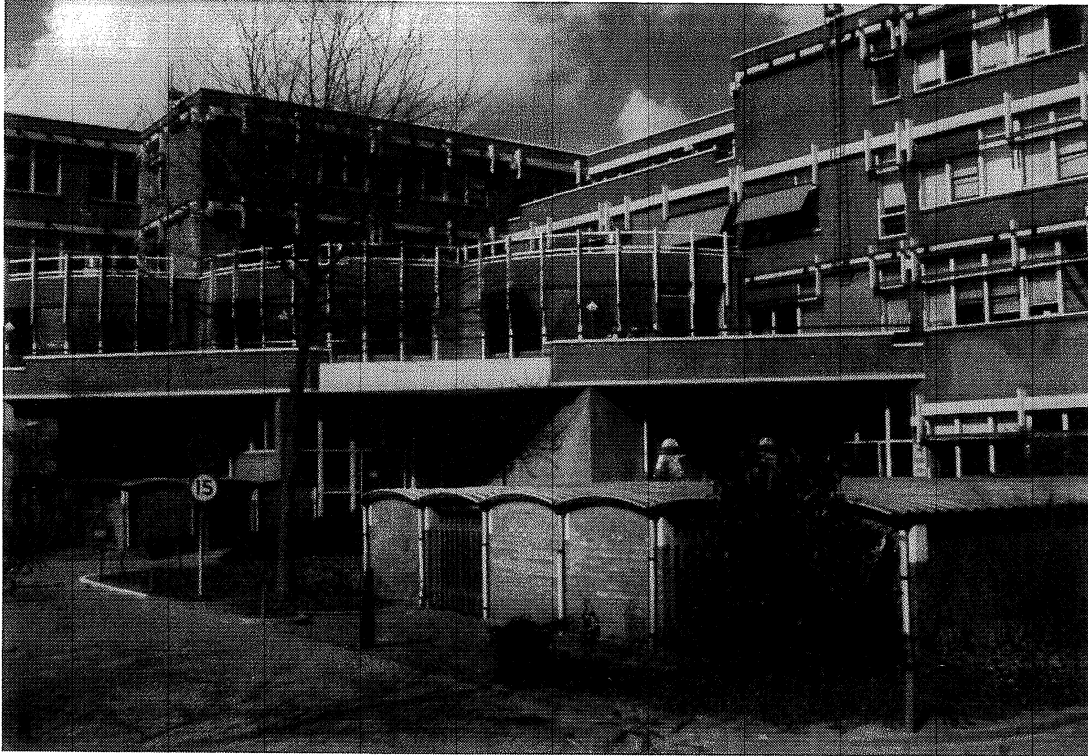


Foto: Sjoerd Mullender

De Stichting Mathematisch Centrum (SMC) is een non-profit organisatie met als doel het bevorderen van de systematische beoefening en toepassingen van de wiskunde en informatica.

De SMC wordt gefinancierd door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

Directie

Algemeen directeur

Dr. ir. G. van Oortmerssen

Redactie

Bureau SMC

Vormgeving en productie

Facilitaire Dienst SMC

Uitgave

juni 1996

Copyright ©1996 Stichting Mathematisch Centrum

Postbus 94079, 1090 GB Amsterdam

Kruislaan 413, 1098 SJ Amsterdam

Telefoon +31 20 592 9333

Telefax +31 20 592 4199

URL: <http://www.cwi.nl>

ISSN 0926-4841

INHOUD

Voorwoord	5
Stichting Mathematisch Centrum algemeen	6
<i>Algemene beschouwing</i>	6
Algemene ontwikkelingen	6
Onderzoek – programma's en projecten	7
CWI	8
ERCIM	10
Inkomsten	11
SARA	12
<i>Bibliotheek en Informatiedienst</i>	13
Landelijke Activiteiten Wiskunde	15
<i>Algemeen</i>	15
<i>Enige projectbeschrijvingen</i>	17
Invariante discretiserings- en oplosmethoden voor de behoudswetten voor incompressibele stromingen	17
Machinevolgordeproblemen en samenwerking	22
Berekenen en visualiseren van invariante variëteiten in dynamische systemen	26
Het ontbinden van grote getallen in priemfactoren	29
Onafhankelijkheid in de quantum-kanstheorie	33
Niet-commutatieve meetkunde	37
Het Witten-vermoeden	40
Percolatie	43
Numerieke bifurcatie-analyse	47

Dit deel van het Jaarverslag 1995 Stichting Mathematisch Centrum beschrijft de algemene activiteiten van de Stichting Mathematisch Centrum en de Landelijke Activiteiten Wiskunde.
Het kan besteld worden bij SMC, mevrouw D.C.M. Amende-Konijn, tel. 020-592 4128;
email: tamende@cw.nl

De overige delen van het Jaarverslag 1995 zijn:

- Annual Report 1995 Centrum voor Wiskunde en Informatica (Engelstalig)
- Financieel Jaarverslag 1995 Stichting Mathematisch Centrum
- Sociaal Jaarverslag 1995 Stichting Mathematisch Centrum
- Overview Research Activities 1995 Centrum voor Wiskunde en Informatica (Engelstalig)

<i>Overzicht van lopende projecten</i>	50
<i>Publicaties</i>	57
<i>Academische promoties</i>	64
Bijlagen	65
Bijlage 1: Doelstelling en organisatie	65
Bijlage 2: Beleidsorganen van de Stichting Mathematisch Centrum	67
Bijlage 3: Financiën, personeel en promoties	68

VOORWOORD

Dit is het laatste door de SMC uit te brengen jaarverslag waarin zowel het CWI als de LAW aan bod komen. In de loop van 1996 zal de LAW namelijk in een aparte stichting ondergebracht worden.

Deze verzelfstandiging is één van de gevolgen van de evaluatie van de relatie tussen SMC en SION door het organisatieadviesbureau Andersson, Elffers & Felix, zulks op verzoek van NWO. Een tweede belangrijk gevolg van deze evaluatie is een herstructurering van het CWI, zowel op bestuurlijk niveau als op afdelingsniveau. Deze herstructurering zal veel inspanning vergen van alle betrokkenen, maar ik ben ervan overtuigd, dat het CWI hierin uitstekend zal slagen.

Aan de SMC-gemeenschap ontvielen in 1995 twee medewerkers: kantinemedewerker R. Resin en wetenschappelijk onderzoeker J.G.L. Booten. Daarnaast overleden mevrouw E.P. Reckman-van Kampen, voormalig hoofd van de Personeelsdienst, mevrouw M. Homburg-Knieper, voormalig hoofd van de Ponskamer en mevrouw J. van der Vegt, voormalig wetenschappelijk medewerkster.

Van de vele projecten die de SMC in 1995 – vaak in samenwerking met andere instellingen – uitvoerde valt het volgende te melden:

- Het CAFE-project, een ESPRIT-project voor veilig en anoniem elektronisch betalen, werd in 1995 afgerond en zal zeer zeker een succesvolle follow-up hebben, gezien de wereldwijde belangstelling voor dit onderwerp.
- Het belangrijke aandeel van het CWI bij de landelijke HPCN-projecten. Het CWI doet mee in 4 van de 6 door EZ gehonoreerde projecten.
- De participatie van het CWI in zes nieuwe Europese projecten van het Vierde Kaderprogramma.

Andere voor de SMC belangrijke gebeurtenissen waren onder meer:

- Academische promoties op het gebied van de wiskunde en informatica: 10 medewerkers in de Landelijke Activiteiten Wiskunde en 8 CWI-medewerkers.
- De uitreiking van de *Akademiepenning* door de KNAW aan de in 1995 afgetreden wetenschappelijk directeur van de SMC, prof. dr. P.C. Baayen, wegens zijn bijzondere verdiensten voor de bloei der wetenschappen in Nederland.
- In 1995 werd het wiskundeonderzoek van het CWI geëvalueerd door een internationale visitatiecommissie. Het oordeel van deze commissie luidde dat het wiskundeonderzoek in het algemeen goed, in sommige gevallen zelfs uitzonderlijk goed was.
- De honorering van de projecten *Getaltheorie* en *Mathematische Modelling van Open Dynamische Systemen*.
- De voordracht door de SMC van het *PIONIER*-voorstel *Semiparametric Models, Empirical Processes, Statistical Processes*.
- De voorbereidingen van de viering van het 50-jarig bestaan van de SMC, met name de publicatie van een Jubileumboek en de organisatie van enige symposia.

Details van de hierboven geschetste gebeurtenissen zijn te vinden in de onderdelen Algemene Beschouwing en Landelijke Activiteiten Wiskunde.

Het Curatorium dankt al degenen, binnen en buiten de Stichting, die hun bijdrage aan de SMC in 1995 geleverd hebben.

G.Y. Nieuwland
Voorzitter Curatorium

STICHTING MATHEMATISCH CENTRUM ALGEMEEN

Algemene beschouwing

Algemene ontwikkelingen

Samenwerkingsrelatie tussen SION en SMC

In maart 1995 verstrekte NWO aan het organisatieadviesbureau Andersson, Elffers & Felix (&AEF) de opdracht om de samenwerkingsrelatie tussen de SMC en SION te evalueren. In het kader van deze evaluatie voerde &AEF diverse gesprekken met vertegenwoordigers van NWO, SION en SMC. In november heeft &AEF zijn advies aan NWO uitgebracht, waarna in overleg tussen de betrokken partijen de volgende besluiten zijn genomen:

- Splitsing van de SMC in twee nieuwe stichtingen: een Stichting Wiskunde Onderzoek Nederland (SWON) voor de coördinatie van de Landelijke Activiteiten Wiskunde en een stichting voor het beheer van het CWI.
- Het CWI dient in de toekomst een groter deel van de financiering in de vorm van projecten in competitie met de universiteiten te werven bij SWON en SION.
- Het CWI krijgt een uit vijf personen bestaand Bestuur, waarin SION en SWON zijn vertegenwoordigd.
- De organisatie van de wetenschappelijke afdelingen zal veranderen: van discipline-georiënteerd naar thema-gericht. Deze herstructurering komt overeen met de adviezen van de Visitatiecommissie Wiskunde in september 1995 en dient mede om de synergie wiskunde-informatica verder te stimuleren.

In 1996 zal SWON worden opgericht met de Wetenschappelijke Raad als eerste bestuur en zal de herstructurering van het CWI worden uitgevoerd.

Curatorium

De Stichting Mathematisch Centrum (SMC) wordt bestuurd door een Curatorium. Zie Bijlage 2 voor de samenstelling. Het Curatorium laat zich inzake het wetenschappelijk beleid adviseren door de We-

tenschappelijke Raad (WR) van de SMC en door de Stichting Informatica Onderzoek Nederland (SION).

In 1995 waren onder meer de volgende punten onderwerp van overleg en besluitvorming.

- De samenwerkingsrelatie SION-SMC. Zie vorige sectie.
- Meerjarenplan CWI 1997 – 2001.

In het verslagjaar werd het Meerjarenplan 1995 – 1999 van de SMC geactualiseerd tot het Meerjarenplan CWI 1997 – 2001. In dit Meerjarenplan wordt geanticipeerd op de komende herstructurering van het onderzoek van het CWI. Als belangrijke leidraad voor dit Meerjarenplan diende een aantal documenten: de beleidsnota's *Kennis Verrijkt* van NWO, en *Kennis in Beweging* van de Ministeries van OC&W en EZ, het evaluatierapport van de internationale visitatiecommissie Wiskunde (zie pagina 8), het rapport over de samenwerkingsrelatie SMC-SION van Andersson, Elffers & Felix (zie vorige sectie) en de AWT-publicatie *Advies inzake de Para-Universitaire Instituten*.

EURANDOM.

In 1995 nam het Curatorium het besluit om de initiatieven tot oprichting van een Europees instituut voor niet-deterministisch onderzoek (*EURANDOM*) in Nederland te steunen.

- Het 50-jarig Jubileum van de SMC.
- De status van CAN en RIACA.
- De initiatieven van het CWI om in samenwerking met andere technologische instituten te komen tot de oprichting van een *Technologisch Top Instituut* (TTI). Deze initiatieven kwamen voort uit het voorstellen van de Ministeries van EZ en OC&W om in de komende jaren een vijftal TTI's te realiseren en daarvoor een bedrag van Mf. 55 beschikbaar te stellen.

Wetenschappelijke Raad (WR)

De Wetenschappelijke Raad (WR) van de SMC adviseert het Curatorium van de SMC, met name op

het gebied van de wiskunde. Voor de samenstelling van de WR wordt verwezen naar Bijlage 2. De WR kwam in het verslagjaar vijfmaal bijeen en wel op 18 januari, 18 april, 6 juni, 30 augustus en 14 november. De belangrijkste agendapunten waren:

- De begroting en planning van de wetenschappelijke activiteiten voor 1995.
- De Bibliotheek & Informatiedienst SMC/CWI.
- De beoordeling en selectie van onderzoeksvoorstellen in de *Beleidsruimte SMC*.
- De selectie, beoordeling en prioritering van de voorstellen voor *Grote Projecten*.
- De beoordeling en selectie van onderzoeksvoorstellen in het kader van het aandachtsprogramma *High Performance Computing and Networking*.
- De selectie van een kandidaat voor het NWO-programma *PIONIER*.
- De selectie en beoordeling van een *Centraal Jaar-thema*.
- De honorering van de aanvragen voor wetenschappelijke bijeenkomsten.
- De continuëeringsaanvragen 1996. Er werden 9 continuëeringsaanvragen voor honorering voorgedragen in de *Beleidsruimte SMC*. Alle aanvragen werden van een positief advies voorzien. Alle aandachtsprogramma's en Grote projecten werden eveneens gecontinueerd.
- De continuëring van het Samenwerkingsverband FOM/SMC Mathematische Fysica.
- De advisering over wetenschappelijke aangelegenheden ten behoeve van het GB-E.
- De status van CAN en RIACA.
- De relatie SION-SMC.
- Het Meerjarenplan NWO 1997-2001.
- De discussienota *Beoordeling van onderzoeksvoorstellen*.
- De ontwikkelingen rondom *EURANDOM*.
- De concept-begroting LAW 1996.
- Het 50-jarig jubileum SMC in 1996.

Stichting voor de Technische Wetenschappen (STW)
In het verslagjaar werd de samenwerking tussen de STW en de SMC voortgezet. De functie van Programme Officer, voor zover het wiskundeonderzoek betreft, beruiste bij het Bureau SMC.

In 1995 werd het project *Mathematische modellering van het transport van verontreinigd grondwater* (LUW) beëindigd. De volgende projecten werden gehonoreerd:

- *Wavelets* (CWI).
- *High Performance Computing voor niet-lineaire*

problemen binnen numerieke modellering van constructies (KUN).

De eerder gehonoreerde projecten zijn:

- *Constrained interpolation and approximation using splines in one and two variables* (UT).
- *Parameteridentificatie en modelanalyse voor niet-lineaire dynamische systemen* (CWI).
- *Parallel codes for circuit analysis and control engineering* (CWI en UvA).
- *ACELA - Architecture of a Computer Environment for Lie Algebras* (CWI en TUE).

Ondernemingsraad

In 1995 werden zes overlegvergaderingen OR-directie gehouden. Daarnaast had ook zeer geregeld informeel overleg tussen OR en directie plaats.

Onder meer de volgende zaken werden met de OR besproken:

- Financiële zaken, zoals begrotingen, jaarverslagen en rapportages, besteding geoormerkte subsidies.
- De uitvoeringsregelingen voortkomend uit en verband houdend met de *Collectieve Arbeidsvoorwaarden Regeling*.
- Het arbeidsmarktbeleid met name over leeftijdsbewust personeelsbeleid, regelingen m.b.t. JWG'ers (Jeugd Werk Garantiewet), WEP'ers (Werkervaringsplaats) en herintreedsters.
- De toekomstige organisatie en exploitatie van de WCW-kantine.
- De positie van de wetenschappelijk programmeurs.
- Arbo-zaken.

Onderzoek – programma's en projecten

Het onderzoeksprogramma van de SMC wordt uitgevoerd enerzijds in het kader van de *Landelijke Activiteiten Wiskunde* (LAW) en anderzijds op het CWI, het Centrum voor Wiskunde en Informatica.

Het onderzoek vindt voor een belangrijk deel plaats in samenwerking met andere instellingen en het bedrijfsleven, onder meer door middel van *Grote Projecten*, *Aandachtsprogramma's* bij de LAW of participatie in grootschalige, internationale programma's bij het CWI, zoals bijvoorbeeld het Vierde Kaderprogramma van de Europese Unie (onder meer *ESPRIT*, *Human Capital & Mobility (HCM)*, *Transport & Mobility of Researchers (TMR)*).

Het volgende biedt een overzicht van de thans lopende programma's en projecten van de LAW. Met ingang van 1996 zal het LAW-gedeelte van dit onderzoek onder de verantwoordelijkheid van de SWON worden uitgevoerd.

Aandachtsprogramma's LAW

In het verslagjaar werd een aanvraagronde gehouden in het kader van het aandachtsprogramma High Performance Computing and Networking. Er werden 9 aanvragen ingediend. Er werden 3 plaatsen gehonoreerd. Met de invulling van het aandachtsprogramma *High Performance Computing and Networking* is het maximum van zes programma's bereikt. Hieronder volgt een overzicht van de lopende aandachtsprogramma's:

- *Wiskundige aspecten van niet-lineaire dynamische systemen.*
- *Algoritmen in de algebra.*
- *Algebraïsche krommen en Riemann-oppervlakken.*
- *High Performance Computing and Networking.*
- *Computerintensieve methoden in de stochastiek (gefinancierd uit de Beleidsruimte GB-E).*
- *Mathematische Fysica (samenwerkingsverband met FOM).*

CWI-projecten	Aantal	Met externe partners
Extern gefinancierd	72	48
SION	20	11
STW	4	3
NCF	3	0
NFI	4	3
EU-projecten	13	13
HCM-netwerken	10	10
NWO	3	3
Overig	15	5
Door SMC gefinancierd	55	
Totaal CWI-projecten	127	48
LAW-projecten	57	Deelprojecten
Grote Projecten	3	3
Aandachtsprogramma's	6	21
Individuele projecten	33	33

Tabel 1. Overzicht van door CWI en LAW uitgevoerde projecten

Grote Projecten LAW

Onderzoeksgroepen en Onderzoekscholen werden in het verslagjaar uitgenodigd een beknopte aanvraag in te dienen in het kader van de Grote Projecten. Er werden 8 aanvragen ingediend. Daarvan werden de volgende twee aanvragen gehonoreerd:

- *Getaltheorie.*
- *Mathematische modellering van open dynamische systemen.*

Beleidsruimte SMC

In het voorjaar van 1995 werd een aanvraagronde in het kader van de *Beleidsruimte SMC* gehouden. Er werden 26 aanvragen ingediend, waarvan er 6 werden gehonoreerd (6 oio's). *Centraal jaarthema LAW* Voor het academisch jaar 1995/1996 werd het centraal jaarthema *Probabilistic algorithms and algorithmic probability* vastgesteld.

High Performance Computing and Networking

Een belangrijk onderzoeksgebied voor de SMC, tevens een voorbeeld van inbedding in een groter kader, is het onderzoek op het gebied van grootschalig rekenen onder diverse namen als *High Performance Computing and Networking (HPCN)* en *Massaal Parallel Rekenen (MPR)*. Binnen diverse verbanden verricht de SMC op dit gebied onderzoek:

- Het NWO-prioriteitsprogramma *Massaal Parallel Rekenen*.
- Het nationale HPCN-programma met als thema's *Complex Reactieve Systemen* en *Computational Fluid Dynamics*. Het CWI participeert in 4 van de 6 door het Ministerie van EZ gehonoreerde projecten. Dit zijn de projecten *Environment Modelling – ICES*, *HPCN in Financial Services*, *Visualization, Computational Fluid Dynamics – NICE*.
- Het prioriteitsgebied HPCN van het Vierde Kaderprogramma van de Europese Unie.
- Het LAW-aandachtsprogramma *HPCN* van de SMC.
- Als onderzoeksthema binnen het CWI.

CWI

Voor de verslaglegging van het wetenschappelijk onderzoek van het CWI wordt verwezen naar de delen 2 en 5 van het Jaarverslag: het *Annual Report* en het rapport *CWI Overview Research Activities*.

Evaluatie wiskundeonderzoek CWI

In september 1995 werd het wiskundeonderzoek op het CWI geëvalueerd door een internationale visitatiecommissie onder voorzitterschap van prof. dr. ir. J.C. Willems (RUG). In haar eindrapport oordeelde de visitatiecommissie dat het wiskundeonderzoek over het geheel van goede tot zeer goede kwaliteit was. Daarnaast gaf de commissie de volgende aanbevelingen:

- Positionering van *Wiskundig Modelleren* als centraal thema in het onderzoek. Dit is vooral van belang voor onderzoek op het gebied van Financiële wiskunde, Signaal- en beeldverwerking, Mileumodellering en Grootschalig modelleren in

- (bio)chemie en andere fysische wetenschappen.
- Meer aandacht voor contractonderzoek en kennisoverdracht, met inzet van alle senior medewerkers en bereidheid minder geavanceerd werk uit te voeren.
 - Flexibele inzet bij de wetenschappelijke staf om interdisciplinair onderzoek op diverse terreinen van de wiskunde en informatica – en in de fysische wetenschappen – uit te voeren.
 - Selectie van het CWI door de overheid als topinstituut op het gebied van de informatietechnologie.
 - Vestiging van het nieuw op te richten instituut EURANDOM in de onmiddellijke omgeving van het CWI.
 - *Gelijktijdige* evaluatie van het wiskunde- en informaticaonderzoek door toekomstige visitatiecommissies.
 - Herstructurering van het wiskunde- en informaticaonderzoek op basis van onderzoeksthema's.

Extern gefinancierd onderzoek CWI

- Van toenemend belang voor het CWI is het verwerven van inkomsten voor onderzoek buiten het basis-subsidie. Vaak ook verlangt de financierende instelling dat meer dan één instituut (b.v. een industriële partner) deelneemt aan het project. Enige voorbeelden van externe subsidies zijn:
- Stichting voor de Technische Wetenschappen (STW). In 1995 liepen er binnen het CWI 4 door de STW gefinancierde projecten, waarvan het *Wavelet*-project in 1995 van start ging.
 - SION-projecten. In 1995 liepen er binnen het CWI circa 20 door SION (mede) gefinancierde projecten. Twee daarvan werden in de loop van het verslagjaar afgerond, 1 project werd door SION aan het CWI toegekend.
 - Het nationaal HPCN-programma van het Ministerie van Economische Zaken.
 - Overige subsidies, zoals *Nationale Faciliteit Informatica*, *Nationale Computer Faciliteiten*.

Europese programma's en netwerken

Het CWI heeft sinds de invoering van de Europese Kaderprogramma's omstreeks 1984 steeds met succes meegedongen (*ESPRIT*, *RACE*, *BRITE*, *SCIENCE*, *COMETT*, *HCM*). In 1995 participeerde het CWI in circa 13 EU-projecten, waaronder *PYTHAGORAS* (databases), *CAFE* (veilig en anoniem elektronisch betalen; zie ook het kader op pagina 10), *MADE* (Multimedia) en *NeuroCOLT* (*Neural Networks in Computational Learning Theory*). Voorts participeerde het CWI in circa 10 HCM-netwerken, waaronder twee ERCIM-netwerken. Zie

het *Annual Report 1995* voor een uitvoeriger overzicht.

Voor het CWI is participatie in het Vierde Kaderprogramma van de Europese Unie van groot belang met het oog op voortzetting van deelneming in Europese projecten en netwerken.

Voor het CWI zijn belangrijke onderzoekgebieden in dit programma: *Multimedia*, *Long Term Research* en *High Performance Computing and Networking*. In het verslagjaar zijn 6 projecten door de Europese Commissie gehonoreerd: *DACCORD*, *STEM*, *MERCURY*, *SEMPER*, *CHAMELEON*, *KESO*.

Conferenties, workshops, cursussen

Een belangrijk deel van de kennisoverdracht vindt plaats door middel van conferenties, workshops, cursussen, etc.. In 1995 organiseerde het CWI de volgende evenementen:

- *Runge-Kutta 100*, een symposium ter gelegenheid van de 100^{ste} verjaardag van de *Runge-Kutta*-methode.
- *Korteweg-De Vries '95*, een symposium ter gelegenheid van de 100^{ste} verjaardag van de *Korteweg-De Vries Vergelijking*.
- De jaarlijkse conferenties van enige werkgemeenschappen van de Landelijke Activiteiten Wiskunde.
- De *Presentatiedag CWI in Bedrijf*.
- De traditionele vakantie cursus voor leraren met als onderwerp dit jaar *Kegelsneden en kwadratische vormen*.
- *Eurographics '95*. Zie pagina 11.

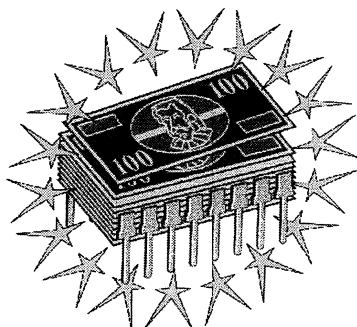
	1993	1994	1995
Artikelen in tijdschriften en proceedings	224	255	301
CWI-rapporten	125	135	155
Boeken	4	4	6
Overige publicaties	99	104	97
Proefschriften	8	15	8
Totaal	460	513	567

Tabel 2. *Publicaties CWI*

Boeken

Naast de vele publicaties in tijdschriften, congresverslagen, en dergelijke (zie Tabel 2), verschenen er ook diverse boeken, geschreven door of met medewerking van CWI-onderzoekers. Hier noemen wij de volgende:

CAFE



(a) Het CAFE-logo

(b) Projectleider R. Hirschfeld tijdens de CAFE-conferentie van januari 1996 in Brussel.

Het CAFE-project

In 1995 werd het ESPRIT-project CAFE (Conditional Access for Europe) met succes afgesloten. Dit project, waarvan het CWI de coördinator was, had als doel een elektronische portefeuille en een veilige architectuur, die als basis kan dienen voor een uitlopende scala van elektronische betalingsapparaten, zodat de consument veilig en anoniem kan betalen.

Deze wijze van elektronisch bankieren heeft inmiddels wereldwijde belangstelling getrokken, getuige onder meer een artikel van het Amerikaanse blad NEWSWEEK, waarin CAFE-partner DigiCash uitvoerig aan de orde komt.

In januari 1996 werd door het CWI in samenwerking met het CAFE-team in Brussel een CAFE-conferentie georganiseerd met als thema *Electronic Consumer Payment Systems: the Next Generation*.

- O. DIEKMANN, S.A. VAN GILS, S.M. VERDUYN LUNEL, H-O. WALTHER, *Functional-, Complex- and Nonlinear Analysis*.
- YU.A. KUZNETSOV. *Elements of Applied Bifurcation Theory*.
- P. CHRÉTIENNE, E.G. COFFMAN, JR., J.K. LENSTRA, Z. LIU (eds.), *Scheduling Theory and Its Applications*.

Academische promoties

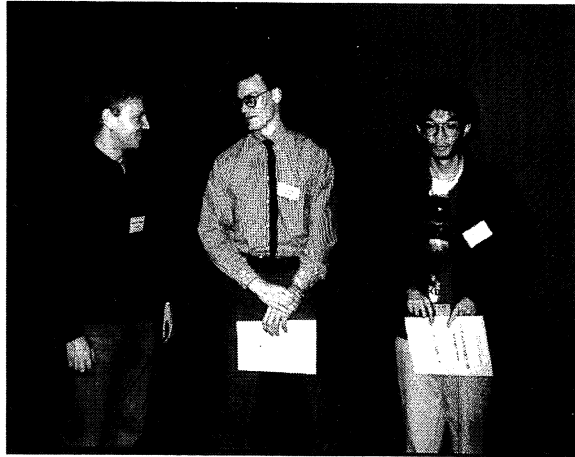
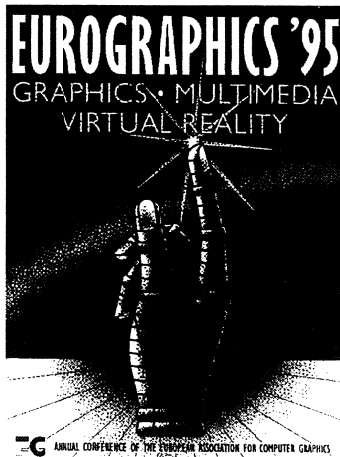
Behalve het publiceren van onderzoeksresultaten is één van de belangrijkste vormen van kennisoverdracht het opleiden van wetenschappelijk kader dat vervolgens een plaats vindt elders in de maatschappij. Veel CWI-medewerkers vervullen een deeltijd-hoogleraarschap, terwijl veel belangrijke posities aan universiteiten worden bezet door voormalige CWI-medewerkers. Een essentieel onderdeel van deze kadervorming vormen de academische

promoties van jonge medewerkers. Wat dit laatste betreft was 1995 een goed jaar, met acht promoties van CWI-medewerkers en tien promoties van LAW-medewerkers.

ERCIM

Het in 1988 mede door het CWI opgerichte *European Research Consortium for Informatics and Mathematics* (ERCIM) bestond in 1995 uit dertien leden. In 1996 wordt de toetreding van Tsjechië verwacht.

Met een totaal van bijna zeventuizend onderzoekers speelt ERCIM een vooraanstaande rol bij het sturen en realiseren van het Europese onderzoeksbeleid in de informatietechnologie en toegepaste wiskunde. Op de directors meeting in november te Budapest was G. Metakides van de Europese Commissie te gast. Op deze meeting liet hij weten dat de Europese Commissie *de facto* ERCIM als gesprekspartner inzake informatietechnologie erkende.



(a) Het EUG'95-logo

(b) Juryvoorzitter H.P. Seidel (links) reikt de Günther Enderle Award uit voor de beste voordrachten.

Eurographics '95

De *European Association for Computer Graphics* (Eurographics) is een in 1980 mede door het CWI opgerichte internationale vereniging ter bevordering van computergrafiek. Inmiddels omvat het werkteerrein van Eurographics de beeldinformatica in de ruimste zin des woords.

In september 1995 werd de jaarlijkse conferentie van Eurographics door het CWI georganiseerd in

Maastricht.

Onderdelen van die conferentie waren:

- Geavanceerde cursussen.
- Workshops.
- Parallele voordrachten.
- Paneldiscussies.
- Uitreiking van de *Günther Enderle Award* voor de beste voordracht.

Belangrijke activiteiten van ERCIM waren onder meer:

- Participatie in twee netwerken voor *Digitale Bibliotheken*: DELOS en SAMOS. DELOS wordt door de EU gesubsidieerd.
- Diverse activiteiten op het gebied van *World Wide Web*: onder meer het lidmaatschap van de *World Wide Web Consortium (W³C)*, waarvan ERCIM-lid INRIA de Europese activiteiten coördineert en oprichting van de *ERCIM World Wide Web Working Group (W⁴G)*.
- Workshops met als onderwerpen *Object-Oriented Databases, Systems & Control, Commercial World Wide Web Applications, Design & Electronic Publishing, Mobile Code in WWW, Database Issue & Infrastructure in Cooperative Information Systems, User Interfaces for All*.
- Het ERCIM Fellowship Programme. Met behulp van het EU-programma Human Capital and Mobility (HCM) zijn voor de ronde 1996 – 1997 thans 26 beurzen beschikbaar. Toekenning van deze beurzen

zal worden toegespitst op onderzoek op het gebied van Digitale Bibliotheken.

- Twee HCM-programma's van de ERCIM-werkgroepen Computer Graphics en Databases.
- De uitreiking van de *Cor Baayen Award* (een prijs voor jonge veelbelovende ERCIM-medewerkers) aan C. Samuelsson (SICS, Zweden).
- De publicatie van *ERCIM News* met als speciale researchthema's *Electronic Publishing Computer Supported Cooperative Work, Computational Mathematics* en *Software Quality*.

Inkomsten

In 1995 heeft de SMC een subsidie van 16.9 Mf ontvangen voor het CWI. Daarnaast is voor de LAW een subsidie ontvangen van 3.4 Mf.

Behalve een subsidie van NWO genereert het CWI inkomsten uit projecten die door andere organisaties zoals SION en STW worden gefinancierd. Ook worden inkomsten behaald door deelname door het CWI aan internationale projecten die in opdracht van

de EU en in samenwerking met buitenlandse instituten en bedrijfsleven worden uitgevoerd. Bovendien worden in toenemende mate inkomsten behaald uit contractresearch.

Voor 1995 bedroegen de inkomsten van het CWI in totaal 26.5 Mf, waarvan

Basissubsidie NWO	16.9 Mf
Internationale samenwerking	1.7 Mf
Contractresearch en andere inkomsten	2.6 Mf
Investeringsubsidie NWO	2.6 Mf

De inkomsten uit contractresearch en (inter)nationale samenwerking zijn vooral het effect van de inspanningen om duurzame samenwerkingsvormen met het bedrijfsleven tot stand te brengen. Die mogelijkheden ontstaan op het moment dat concrete onderzoekresultaten, dan wel op stapel staande projecten, toepasbare betekenis hebben voor het bedrijfsleven.

Belangrijke opdrachtgevers zijn in 1995 onder meer geweest: Kluwer, Elsevier, Railned, MeesPierson, KPN Research, Nederlandse Spoorwegen, SKF, Nederland Haarlem BV.

SARA

De Stichting Academisch Rekencentrum Amsterdam (SARA) is in 1970 door de Universiteit van Amsterdam (UvA), de Vrije Universiteit (VU) en de Stichting Mathematisch Centrum (SMC) opgericht ten behoeve van het rekenwerk van deze stichters. Namens de SMC had de algemeen directeur zitting in het bestuur van SARA.

In 1995 bedroeg de bijdrage van de SMC aan SARA ruim 1.3 Mf, waarvan bijna 0.9 Mf in de vorm van een exploitatiebijdrage.

Per 1 januari 1996 participeert de SMC niet meer in SARA en is zij niet meer vertegenwoordigd in het bestuur van SARA. De dienstverlening door SARA aan NWO-instituten wordt in de toekomst geregeld via een contract tussen de NWO-stichting NCF (Nationale Computer Faciliteiten) en SARA. Via dit contract kan het CWI gebruik blijven maken van de SARA-faciliteiten.

Bibliotheek en Informatiedienst

In het verslagjaar kwam de Bibliotheekcommissie achtmaal bijeen. Aan de orde kwamen onder meer het aanschafbudget voor boeken, de automatisering, het bibliotheekplan voor 1996, samenwerking met andere bibliotheken en de bezuiniging op de uitgaven voor tijdschriften. De wetenschappelijke afdelingen gaven advies inzake de aanschaf van boeken en van abonnementen op tijdschriften. Daarnaast verleenden zij medewerking bij het classificeren van de nieuwe boeken.

De bezuinigingen op de uitgaven voor de tijdschriften, die aan het eind van 1992 waren begonnen zijn in het verslagjaar voortgezet. Ook in 1995 zijn ten behoeve van 1996 abonnementen (57) opgezegd om de aanschaf van nieuwe titels mogelijk te maken en binnen het budget te blijven. Een volledige lijst is gepubliceerd in de Mededelingen van het Wiskundig Genootschap van september 1995.

Van de mogelijkheid om via het netwerk de catalogus te kunnen raadplegen door zowel medewerkers van het CWI als door derden, werd in het verslagjaar druk gebruikgemaakt. De raadpleegmogelijkheid via netwerken door derden accentueert de feitelijke landelijke functie van de bibliotheek.

In het verslagjaar werden de WWW-pagina's van de bibliotheek (als onderdeel van de WWW-opzet van het CWI) voortdurend verbeterd en uitgebreid. Via dit medium is onder meer de bibliotheekcatalogus raadpleegbaar voor gebruikers. Voorts is er allerhande informatie over de bibliotheek beschikbaar en worden er diensten via WWW aangeboden. Het aantal elektronische tijdschriften dat kan worden geraadpleegd is groeiende, evenals de elektronische inhoudsopgaven van een aantal tijdschriften.

Met Elsevier wordt samengewerkt om gegevens over tijdschriftartikelen, die worden aangeleverd in SGML (zogenaamde CAPCAS informatie), via WWW beschikbaar te stellen binnen het CWI.

In toenemende mate worden wetenschappelijke rapporten uitsluitend via ftp aangeboden in plaats van in de traditionele gedrukte vorm. Dit houdt in dat ten behoeve van de beschikbaarstelling in de collectie, voor de bibliotheek de wijze van verwerving van deze rapporten verandert en arbeidsintensiever wordt.

De bibliotheek neemt deel aan het Amsterdams bi-

bliotheeknetwerk AdamNet. In dit kader werden de vergaderingen bijgewoond. Een van de belangrijkste doelstellingen van AdamNet betreft de realisering van het wederzijds online raadplegen van de bibliotheekcatalogi. Ook wil men de samenwerking in de regio bevorderen.

Op initiatief van de bibliotheek is in het verslagjaar een overleg gestart tussen de wiskunde- en informaticabibliotheken in Nederland. Een belangrijke doelstelling is de bevordering van een betere samenwerking en een betere afstemming van de collecties. Het overleg, dat tweemaal per jaar gehouden wordt, voorziet in een behoefte. Vrijwel alle wiskunde- en informaticabibliotheken waren vertegenwoordigd in de vergaderingen.

In het verslagjaar zijn de besprekingen met de VVS over plaatsing van haar (lopende) tijdschriftencollectie in de bibliotheek, afgerond. Met ingang van 1 januari 1996 zullen namens de VVS, tijdschriften worden verkregen in ruil voor het tijdschrift *Statistica Neerlandica*.

Het EC-project RIDDLE (Rapid Information Display and Dissemination in a Library Environment), waaraan de bibliotheek deelnam, werd afgerond.

De bibliotheek is in het verslagjaar begonnen om actief deel te nemen aan het Digital Library Initiative van ERCIM. Een belangrijk onderdeel hiervan is een project, dat het bouwen van een gezamenlijke ERCIM 'digital library' beoogt.

Teneinde het bestand van de bibliotheek toe te kunnen voegen aan de TechRom CD-ROM, waartoe een uitnodiging werd ontvangen, zijn werkzaamheden uitgevoerd. De 3de editie van de TechRom zal dan naast de bibliotheekbestanden van respectievelijk de TU Delft, de TU Eindhoven en het Waterloopkundig Laboratorium, ook het bibliotheekbestand van de SMC bevatten. Deze 3de editie zal in 1996 uitkomen.

Ten behoeve van de informatieverzorging werden door de informatiemedewerker 76 (1994: 77) opdrachten voor het literatuurzoeken in externe databases uitgevoerd. Twee bibliografische bestanden op CD-ROM zijn door bibliotheekgebruikers zelf raadpleegbaar. Het betreft:

- CompactMath (elektronische versie van het

Zentralblatt für Mathematik) vanaf 1985;
- CompArch (elektronische versie van de Computing Reviews) en ACM Guide to Computing Literature vanaf 1982.

Na strenge selectie en evaluatie, werden 55 (1994: 36) nieuwe abonnementen aan de collectie toegevoegd. Een aantal titels hiervan behoort tot de lopende tijdschriftencollectie van het Wiskundig Genootschap, die op het CWI is ondergebracht. Van

de tijdschriftabonnementen werden er 22 door koop, 17 door ruil (incl. WG ruil) en 16 gratis verkregen. Met ingang van 1995 werden 17 koopabonnementen opgezegd.

De omvang van de bibliotheekcollectie bedraagt ongeveer 43000 boeken (toename: 1107), circa 1300 abonnementen op tijdschriften (totale tijdschriftencollectie van circa 37000 banden) en circa 123000 wetenschappelijke rapporten (toename: 8024).

LANDELIJKE ACTIVITEITEN WISKUNDE

Algemeen

Inleiding

De Landelijke Activiteiten Wiskunde (LAW) zijn sinds 1981 in de vorm van een aantal werkgemeenschappen en samenwerkingsverbanden onder de hoede van de SMC geplaatst. De Wetenschappelijke Raad (WR) adviseerde het Curatorium van de SMC ten aanzien van het door NWO gefinancierd onderzoek in de wiskunde en speelde tevens een belangrijke rol bij de ontwikkeling van nieuwe initiatieven zoals aandachtsgebieden, grote projecten en centrale jaarthema's.

In het najaar van 1995 vond op verzoek van het GB-E een onderzoek plaats naar de relatie tussen SMC/CWI en SION. Het onderzoek werd uitgevoerd door het organisatie-adviesbureau Andersson, Elfers & Felix en resulteerde in een advies het tweede geldstroom onderzoek in wiskunde en informatica in drie afzonderlijke stichtingen onder te brengen: SION voor informatica-projecten, SMC als beheerder van het CWI en een nieuwe stichting wiskunde onderzoek in Nederland (SWON), waarin de huidige landelijke activiteiten wiskunde zouden worden ondergebracht. De WR zal naar verwachting aantreden als eerste bestuur van SWON.

Activiteiten in 1995

Een deel van de activiteiten waarbij de LAW betrokken was, staat beschreven in de *Algemene Beschouwing*. Dit betreft onder meer het volgende:

- Beleidsruimte SMC.
- Aandachtsprogramma *Massaal Parallel Rekenen*.
- Grote Projecten.
- De persoonsgerichte steunvorm *PIONIER*.

Aandachtsprogramma's

De omvang van een aandachtsprogramma zal gemiddeld 4 à 5 oio- en post-doc-plaatsen bedragen en de duur gemiddeld 4 à 5 jaar. Daarbij zullen eveneens buitenlandse experts en bezoekers worden betrokken. Mogelijke uitgangspunten voor het aanwijzen van aandachtsgebieden zijn:

- Terreinen binnen de wiskunde, die in Nederland nu of in de nabije toekomst als belangrijk worden gezien (als fundamenteel onderzoek, vanwege toepassinggerichtheid of om maatschappelijke redenen).

- Gebieden binnen de wiskunde waar veelbelovend (jong) talent aanwezig is.

Eind 1995 waren er vijf aandachtsprogramma's in uitvoering:

- *Wiskundige aspecten van niet-lineaire dynamische systemen*.
- *Algoritmen in de algebra*.
- *Rekenintensieve methoden in de stochastiek*.
- *Algebraïsche krommen en Riemann-oppervlakken*.
- *Mathematische Fysica*.

In 1996 (1 januari) zal het aandachtsprogramma *HPCN/MPR* van start gaan met de volgende projecten:

- *Automatic meshdomain partitioning for adaptively refined meshes*.
- *Design and analysis of domain decomposition based preconditioning techniques for large sparse systems of equations and linear eigenproblems*.
- *Parallel local search for realistic variants of the job scheduling problem*.

In 1996 wordt het aandachtsprogramma, dan onder de naam *Computer Assisted Mathematics*, aangevuld.

Grote Projecten

Met een Groot Project beoogt de SMC tijdelijke impulsen te geven aan terreinen binnen de wiskunde die nu of in de nabije toekomst als belangrijk worden gezien. Een Groot Project dient bij te dragen aan de versterking van de samenwerking van onderzoekers op nationaal niveau. Het initiatief voor een Groot Project wordt genomen door een onderzoekschool, dan wel een aantal onderzoekers (als regel verbonden aan meer dan één universiteit). In het verslagjaar werden de volgende Grote Projecten gehonoreerd:

- *Getaltheorie*.
- *Mathematische modellering van open dynamische systemen*.

Beleidsruimte SMC

In het voorjaar van 1995 werd na een pauze van twee jaar weer een aanvraagronde in het kader van de Beleidsruimte SMC (individuele oio- en post-

doc voorstellen) gehouden. Er werden 26 aanvragen voor 27 plaatsen ingediend (23 oio's en 4 postdocs). De volgende projecten werden gehonoreerd (6 oio-plaatsen):

- *Integer polyhedra and binary spaces.*
- *Analyse van tijdreeksen met een zware staart.*
- *Statistische eigenschappen van bewegingen in het vlak.*
- *Krommen over eindige lichamen met veel punten en codes.*
- *Ruimtelijke patronen die worden beschreven door hogere orde reactie-diffusievergelijkingen.*
- *Sferische distributies.*

Centrale jaarthema's

Bij een centraal jaarthema denkt de SMC zowel aan onderwerpen waarop in Nederland nog geen onderzoek is gestart en waarbij het van belang is dat Nederland daarin gaat participeren, als aan onderwerpen waarop Nederlandse onderzoekers reeds werkzaam zijn en waar, door een wat intensiever en langduriger contact van Nederlandse en uit te nodigen buitenlandse experts, een sprong voorwaarts in het onderzoek mogelijk is. Door middel van allerlei op elkaar afgestemde activiteiten (symposia, seminars, werkgroepen) krijgen deze onderwerpen landelijk extra aandacht.

Voor het academisch jaar 1995/1996 werd het jaarthema *Probabilistic algorithms and algorithmic probability* vastgesteld.

Samenwerkingsverband FOM/SMC Mathematische Fysica

De SMC zal het in 1992 gestarte samenwerkingsverband continueren en 50% van het jaarlijks budget voor haar rekening nemen. Doordat het samenwerkingsverband over een budget van *kf*400 per jaar kan beschikken, is het mogelijk dat gemiddeld twee à drie nieuwe projecten per jaar gehonoreerd kunnen

worden.

In het verslagjaar werden zes projecten ingediend. De volgende twee projecten werden gehonoreerd:

- *Duality symmetries in string theory and supersymmetric field theories.*
- *Nonequilibrium statistical mechanics and dynamical systems.*

Het project *Relaxation and oscillation dynamics in diode lasers* werd alsnog gehonoreerd (NWO-prioriteitsprogramma niet-lineaire systemen).

Netwerken

Op het gebied van de wiskunde bestaan sinds 1 september 1991 vijf aio-netwerken die een tweede fase onderzoeksopleiding verzorgen.

Het betreft hier het Landelijk Netwerk Mathematische Besliskunde, het netwerk Systeem- en Regeltorie, het netwerk Taal, Logica en Informatie, het netwerk Stochastiek en het netwerk Numerieke Wiskunde.

Deze netwerkactiviteiten zijn in het verslagjaar steeds meer door de onderzoekscholen van de wiskunde overgenomen.

Overige activiteiten

De werkgemeenschappen organiseren en coördineren vele onderzoeksactiviteiten, zoals de jaarlijkse meerdaagse conferenties, landelijke colloquia en summer schools. Voorbeelden zijn de Conferentie Numerieke Wiskunde, de Bijeenkomst van Stochastici, de Conference on the Mathematics of Operations Research, Benelux Meeting on Systems and Control, Lie Groups Seminar, Intercity Seminarium Meetkunde, Logic Intercity Seminar, Symposium Mathematische Fysica en het Colloquium History of Computing.

Enige projectbeschrijvingen

Invariante discretiserings- en oplosmethoden voor de behoudswetten voor incompressibele stromingen

Werkgemeenschap	:	Numerieke Wiskunde
Project	:	Invariante discretiserings- en oplosmethoden voor de behoudswetten voor incompressibele stromingen
Projectleider(s)	:	Prof. dr. ir. P. Wesseling
Projectmedewerker(s)	:	Ir. M. Zijlema
Instelling	:	Technische Universiteit Delft

De rol van de numerieke stromingsleer

Door de ontwikkelingen op het gebied van computertechnologie is de betekenis van de numerieke wiskunde voor de technische wetenschappen sterk toegenomen. Op vele niveaus bewijst de numerieke wiskunde haar nut; van evalueren van elementaire functies tot het simuleren van de stroming rond vliegtuigen.

Binnen het vakgebied van de numerieke wiskunde beleeft het deelgebied 'numerieke stromingsleer' de afgelopen decennia een enorme bloei. Dit betreft het ontwikkelen en het gebruik van numerieke methoden voor het oplossen van de behoudswetten voor stromingen. Deze behoudswetten (geformuleerd in de 19de eeuw door Navier [6] en Stokes [9]) geven een wiskundige beschrijving van het empirische gegeven dat massa, impuls en energie in een stroming behouden grootheden zijn.

Praktische stromingsproblemen, zoals deze voorkomen in bijvoorbeeld de vliegtuigindustrie (stroming rond een vleugel-romp combinatie), waterloopkunde en milieubeheer (stroming door een rivierdelta of verspreiding van stoffen in de atmosfeer), de turbine-industrie (stroming rond compressorbladen) of de procesindustrie (reagerende stromingen) worden vaak gekenmerkt door ingewikkelde structuren, samenhangend met onregelmatige geometrieën en turbulentie.

Om stromingen in gecompliceerde geometrieën te kunnen simuleren, zijn in de jaren zestig en zeventig programmapakketten ontwikkeld gebaseerd op eindige-elementen techniek. Hoewel de eindige-elementen methode zeer geschikt is voor de behandeling van gekromde geometrieën, heeft de toepassing van deze methode geleid tot ingewikkelde algoritmen, wat samenhangt met ongestructureerdheid van

rekenroosters. Vooral het gebruik van speciale computerarchitecturen (vector en parallel processing) wordt hierdoor belemmerd. Niettemin waren de eindige-elementen-pakketten onontbeerlijk voor het oplossen van technische problemen gezien de toeneemende belangstelling voor de stromingsleer vanuit de industrie.

Ontwikkelingen in de laatste 15 jaar

Algemeen wordt erkend dat rekenintensieve toepassingen van de stromingsleer sterk kunnen bijdragen aan technologische ontwikkelingen. Men gaat er van uit dat de grote rekenkracht, die hiervoor in de toekomst verlangd wordt, slechts realiseerbaar zal zijn met massaal parallelle computers. Sinds de jaren tachtig werden nieuwe numerieke methoden ontwikkeld voor het berekenen van incompressibele stromingen op basis van gestructureerde kromlijnige rekenroosters. Hierbij worden de incompressibele Navier-Stokes vergelijkingen gediscretiseerd met een eindige-volume aanpak. Dergelijke algoritmen lenen zich goed voor efficiënt rekenen op parallelle computers. Een belangrijke consequentie is dat de Navier-Stokes vergelijkingen in kromlijnige coördinaten moeten worden geformuleerd. Dit kan op verschillende manieren worden gedaan. Hoewel de verschillende formuleringen dezelfde wiskundige basis hebben, beïnvloeden onderlinge verschillen de numerieke algoritmen op essentiële punten, zoals nauwkeurigheid, stabiliteit, efficiëntie en eenvoud. Er moeten afwegingen worden gemaakt tussen Cartesische en rooster-georiënteerde snelheidscomponenten. In tegenstelling tot rooster-georiënteerde snelheidsvariabelen leidt de keuze voor Cartesische variabelen tot eenvoudig ogende formuleringen en discretisaties. Dit is een aantrekkelijke optie die met name de

ontwikkelingen van pakketten op commerciële basis heeft beïnvloed.

Behalve in de keuze van onbekenden speelt de keuze van de ligging van de onbekende variabelen in het rekenrooster een belangrijke rol. Sinds het werk van Harlow en Welch in 1965 [2] wordt bij numerieke methoden voor incompressibele stromingen op rechthoekige roosters bijna altijd gebruik gemaakt van zogenaamde *staggered grids*, waarbij verschillende variabelen aan verschillende punten in het rooster worden toegekend. Het gebruik van staggered grids met Cartesische snelheidscomponenten als basisvariabelen kent problemen. De resulterende discretisaties zijn in een aantal gevallen, met name bij sterk gekromde geometrieën, instabiel. Een belangrijke doorbraak werd bereikt door Rhie en Chow in 1983 [7]. Zij ontwikkelden een methode op basis van *colocated grids* (de stromingsvariabelen worden op dezelfde plaats in het rooster gekozen) zonder dat het bekende 'even/oneven ontkoppeling' probleem, waarin de druk een oscillerend gedrag vertoont, optreedt. Colocated discretisaties laten zich relatief makkelijk opstellen in algemene coördinaten, nodig voor ingewikkelde geometrieën. Zodoende zijn er hedentendage vele pakketten gebaseerd op de methode van Rhie en Chow. Echter, er is een belangrijk bezwaar. Het onderdrukken van drukoscillaties geschiedt door het toevoegen van kunstmatige termen die de nauwkeurigheid nadelig beïnvloeden.

Een recente ontwikkeling is het gebruik van staggered grids in combinatie met de zogenaamde contravariante massa-fluxes als basisvariabelen voor de eindige-volume discretisatie van de incompressibele Navier-Stokes vergelijkingen in algemene coördinaten. Deze wiskundig elegante aanpak staat bekend als de coördinaat-invariante formulering en kan beschouwd worden als generalisatie van de voorgaande besproken methode van [2]. Belangrijke bijdragen werden geleverd in [8, 1, 3, 5, 13, 12]. De resultaten, zowel in twee als in drie ruimtelijke dimensies wijzen uit dat deze ontwikkeling in methode en werkwijze geslaagd is.

In Nederland staat de stromingsleer sterk in de belangstelling, zowel bij universiteiten en overheidslaboratoria, als in de industrie. Het universitaire onderzoek is gebundeld in het J.M. Burgerscentrum, Onderzoeksschool voor de Stromingsleer. In onze groep (TUD) wordt hoofdzakelijk aandacht besteed aan het berekenen van stromingen in ingewikkelde gebieden, gebruik makend van coördinaat-invariante formuleringen en discretisaties van de incompressibele Navier-Stokes vergelijkingen. Dit onderzoek is uitgemond in het ontwerpen van een informatie-

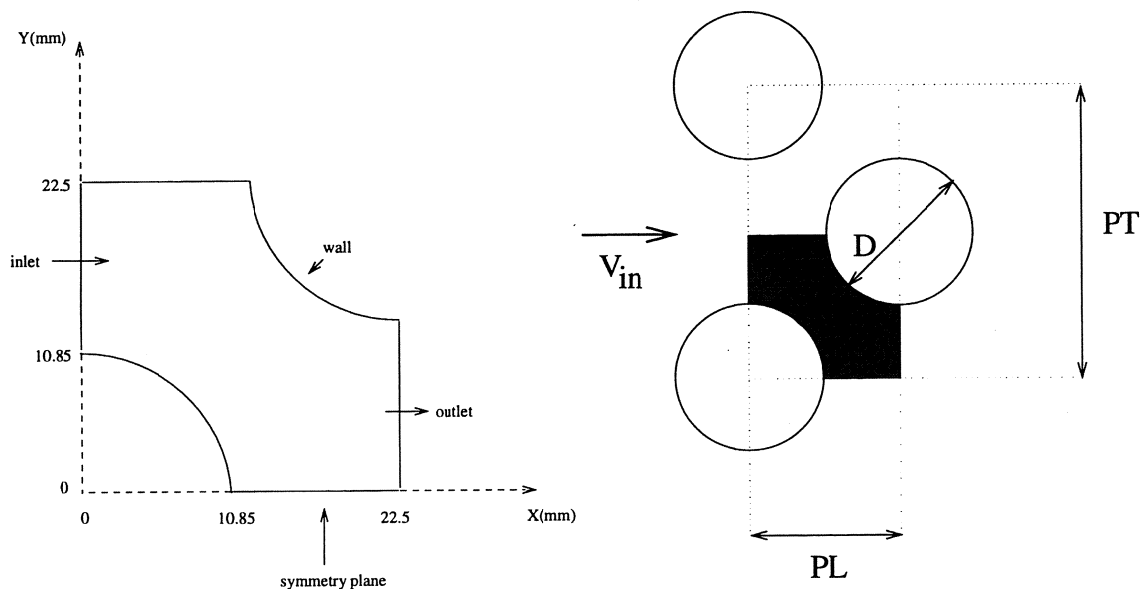
systeem voor het oplossen van de Navier-Stokes vergelijkingen (ISNaS) voor uiteenlopende toepassingen. Het bleek noodzakelijk te zijn nieuwe technieken te ontwikkelen en/of over te nemen. Zo is er veel aandacht besteed aan de numerieke aspecten van turbulentiemodellen, het toepassen van domeindecompositie voor het oplossen van stromingsproblemen in ingewikkelde geometrieën en het inbouwen van compressibiliteitseffecten. Er zijn nauwkeurige discretisaties ontwikkeld zodanig dat zij exact zijn voor constante vector- en scalarvelden op willekeurige kromlijnige roosters. Er wordt aandacht geschonken aan het ontwikkelen en implementeren van numerieke algoritmen, die efficiënt zijn op massaal parallelle computers.

Doelstelling en inhoud van het SMC-project

Het doel van het SMC-project is het ontwikkelen en evalueren van numerieke methoden voor de incompressibele Navier-Stokes vergelijkingen in algemene coördinaten met turbulentiemodellering.

In de wereld om ons heen zijn stromingen bijna altijd turbulent. Dat wil zeggen dat de Navier-Stokes vergelijkingen zich gedragen als een chaotisch dynamisch systeem. Het blijkt dat de computercapaciteit vereist voor het oplossen van die Navier-Stokes vergelijkingen voorlopig nog alle perken te buiten gaat. Er moet daarom gewerkt worden met vereenvoudigde aannamen, zogenaamde turbulentiemodellen. Het ontwikkelen van geschikte turbulentiemodellen is al geruime tijd onderwerp van intensief onderzoek en is door de veelheid van voorgestelde modellen een zeer omvangrijk terrein. Een veelvuldig gebruikt principe is het zogenaamde *eddy viscosity* concept. Hierin wordt verondersteld dat turbulent transport van een fysische grootte het produkt is van een turbulente diffusiecoëfficiënt en de gradiënt van de betreffende grootte loodrecht op het vlak waardoor het transport plaats vindt. Voor de beschrijving van de turbulente diffusiecoëfficiënt zijn diverse modellen ontwikkeld. Een van die modellen is het sinds 1974 bekende $k-\varepsilon$ model [4]. In een berekening van een turbulente stroming moet men daartoe twee extra differentiaalvergelijkingen oplossen. Dit leidt tot een flinke toename van de rekeninspanning. Niettemin is dit model vrij goed geschikt voor de meeste technische toepassingen van de stromingsleer.

Als eerste is gewerkt aan de implementatie van het $k-\varepsilon$ model in twee dimensies binnen het ISNaS pakket. De implementatie van dit model in programma-pakketten is jammer genoeg nog geen *proven technology* omdat enkele eigenschappen van dit model een hinderlijke sta-in-de-weg zijn.

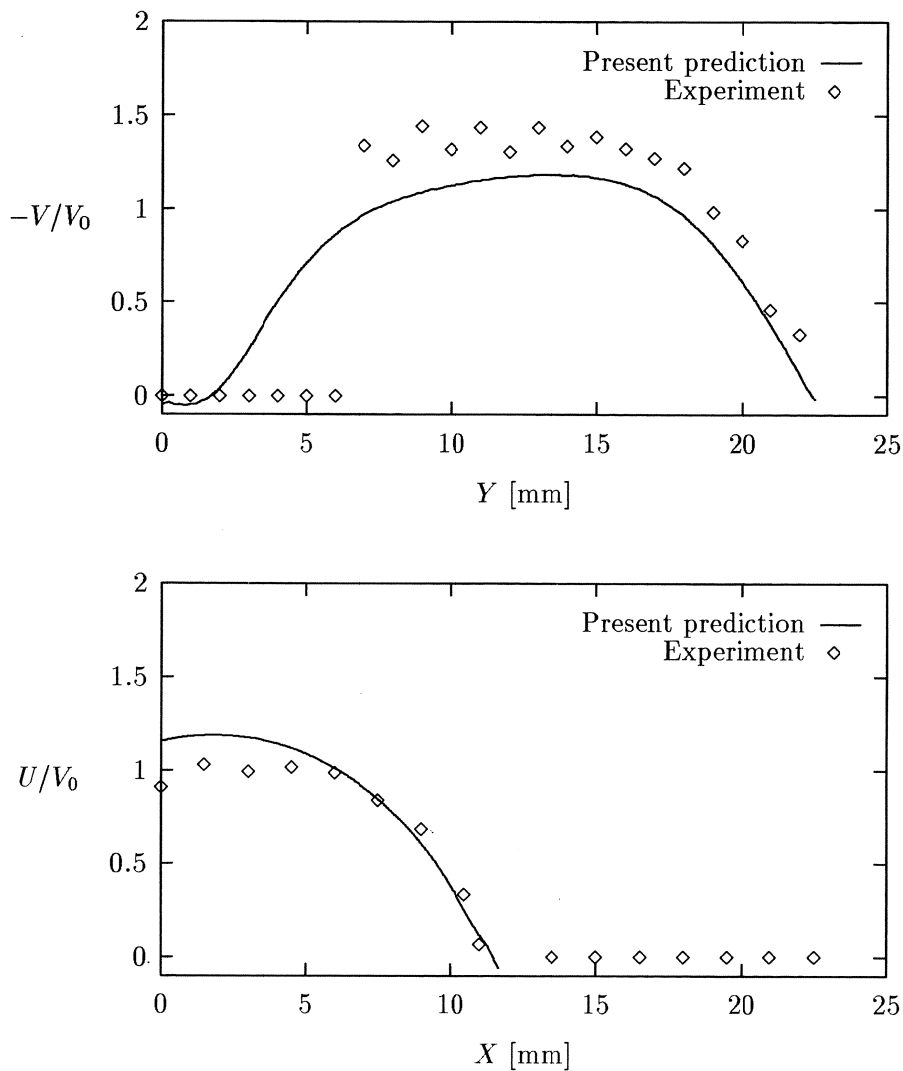


Figuur 1. Geometrie van een deel van een pijpenbundel bestaande uit pijpen met een bepaalde diameter (rechts). In de berekening is de veronderstelling gemaakt dat de stroming periodiek is. Voor de simulatie kan men daarom volstaan met de geometrie zoals links is weergegeven.

Hierbij moet gedacht worden aan het kiezen van compatibele randvoorwaarden op instroomranden en het ten onrechte optreden van negatieve waarden voor k en/of ε . Verder wordt de convergentie naar een stationaire oplossing veelal nadelig beïnvloed wanneer het k - ε model wordt gebruikt. Eerst hebben wij gekeken naar condities voor positiviteit van turbulente grootheden. Gebleken is dat negatieve waarden voor k en/of ε kunnen worden vermeden door het gebruik van zogenaamde opwind discretisaties. In eerste instantie hebben wij gewerkt aan zogenaamde eerste orde opwind schema's. In een later stadium is er uitgebreid onderzoek gedaan naar geavanceerde hogere orde opwind schema's. Hierbij is toepassing van zogenaamde *limiters* van belang om positiviteit te waarborgen. Daarnaast is er aandacht besteed aan de implementatie van enkele andere turbulentiemodellen, te weten het zogeheten RNG geformuleerde k - ε model en Wilcox's k - ω model. Hiermee wordt beoogd om een grotere klasse van stromingsproblemen nauwkeuriger op te lossen.

Er werd deelgenomen aan de *ERCRAFT-IAHR Workshop on Refined Flow Modelling* in 1993. ERCRAFT staat voor European Research Community on Flow, Turbulence And Combustion, en IAHR staat voor International Association for Hydraulic Research. Hierbij werd een stroming loodrecht op

een pijpenbundel, bestaande uit pijpen met een bepaalde diameter, doorgerekend [14] (zie figuur 1). Dergelijke configuraties komen in de praktijk veel voor als verhittings- of afkoelings-element in een vloeistof- of gasstroom (warmtewisselaar). De voorspelling van de stroming in deze geometrie is op dit moment alleen mogelijk met k - ε modellering; een directe simulatie is vanwege de vereiste computercapaciteit volstrekt onmogelijk. In dit probleem willen we de snelheidsverdeling over de bundel berekenen. Kennis van deze verdeling is van belang voor het bepalen van onder andere de warmtestroom. In figuur 2 wordt een vergelijking gemaakt met experimentele resultaten. De uitkomst is typerend voor de mate van overeenstemming van de betere rekenresultaten, waaronder de onze, die in de Workshop werden gepresenteerd. De kwalitatieve overeenstemming is zodanig dat de berekeningen nut hebben voor het ontwerp van dergelijke warmtewisselaars. De discrepanties dienen te worden toegeschreven aan het gebruikte turbulentiemodel. ISNaS is zo opgezet, dat nieuwe modellen die op de markt komen gemakkelijk kunnen worden geïncorporeerd. Voor hydraulische toepassingen die wij hebben behandeld, zoals turbulente stroming over een richel in een rivierbodembodem [13], zijn de resultaten buitengewoon bevredigend.



Figuur 2. Voorspelde en experimentele resultaten voor de snelheidsverdeling voor de stroming loodrecht op een pijpenbundel. Boven: verticale snelheidsverloop in $X = 11$ mm en onder: horizontale snelheidsverloop langs symmetrielij $(Y = 22.5$ mm).

Recent onderzoek

In 1995 richtte het onderzoek in het kader van dit project zich voornamelijk op het nauwkeurig discretiseren van differentiaalvergelijkingen voor het modelleren van turbulentie. Twee aspecten zijn hierbij aan de orde geweest. Ten eerste is er speciaal aandacht besteed aan de numerieke behandeling van de convectie- en diffusietermen. De eerste groep bevat eerste afgeleiden, terwijl in de tweede groep van termen tweede afgeleiden moeten worden benaderd. Een goede numerieke weergave van convectie is een belangrijk probleem omdat er nogal wat

tegenstrijdige eisen gesteld kunnen worden, zoals nauwkeurigheid, monotoniciteit, efficiëntie en algebraïsche eenvoud. Er is gewerkt aan de zogenoemde *flux-limiting* techniek om de turbulente grootheden als k en ε nauwkeurig en oscillatie-vrij te kunnen berekenen. In de literatuur bestaat een grote variatie aan flux-limiting schema's. Voorts is een nieuw schema ontworpen dat kan wedijveren met bestaande opwind technieken [15]. Aan de hand van een aantal karakteristieke testproblemen zijn een aantal van dergelijke schema's aan de tand gevoeld. Hierbij werd

gelet op de numerieke nauwkeurigheid, de rekenin-
spanning en de mogelijkheid om negatieve oplossin-
gen te vermijden [12].

Het tweede aspect van het onderzoek betreft het
nauwkeurig discretiseren zodanig dat de discretisatie
exact is voor constante oplossingen op willekeurige
kromlijnige roosters. Dit lijkt eenvoudiger dan het is
op de door ons gebruikte staggered grids; vandaar de
populariteit van colocated grids. Er zijn voorbeelden
met rechthoekige niet-uniforme dan wel onregelma-
tige rekenroosters doorgerekend. De resultaten zien
er veelbelovend uit ([11, 10, 15]).

Uit de voorlopige resultaten kan geconcludeerd
worden dat coördinaat-invariante formuleringen en
staggered discretisaties van de Navier-Stokes verge-
lijkingen met turbulentiemodellering voldoende tot
ontwikkeling zijn gebracht voor het nauwkeurig op-
lossen van turbulente stromingen in gecompliceerde
geometrieën. In het kader van dit project, dat in 1996
zijn afronding zal vinden, ligt de interesse nu vooral
op het implementeren van numerieke algoritmen
voor het oplossen van turbulente stromingen in drie
ruimtelijke dimensies, waarbij de nadruk zal worden
gelegd op parallel rekenen met domeindecompositie.

Literatuur

1. L. DAVIDSON, P. HEDBERG (1989). Mathematical derivation of a finite volume formulation for laminar flow in complex geometries. *Int. J. for Num. Methods in Fluids* **9**, 531–540.
2. F.H. HARLOW, J.E. WELCH (1965). Numerical calculation of time-dependent viscous incompressible flow of fluid with free surface. *Phys. Fluids* **8**, 2182–2189.
3. T. IKOHAGI, B.R. SHIN (1991). Finite difference schemes for steady incompressible Navier-Stokes equations in general curvilinear coordinates. *Comput. Fluids* **19**, 479–488.
4. B.E. LAUNDER, D.B. SPALDING (1974). The numerical computation of turbulent flows. *Comput. Meth. Appl. Mech. Engng.* **3**, 269–289.
5. A.E. MYNETT, P. WESSELING, A. SEGAL, C.G.M. KASSELS (1991). The ISNaS incompressible Navier-Stokes solver: invariant discretization. *Appl. Sci. Res.* **48**, 175–191.
6. C.L.M.H. NAVIER (1823). Mémoire sur les lois du mouvement des fluides. *Mém. Acad. R. Sci. Paris* **6**, 389–416.
7. C.M. RHIE, W.L. CHOW (1983). Numerical study of the turbulent flow past an airfoil with trailing edge separation. *AIAA J.* **21**, 1525–1532.
8. M. ROSENFELD, D. KWAK, M. VINOKUR (1988). A solution method for the unsteady and incompressible Navier-Stokes equations in generalized coordinate systems. *AIAA Paper 88-0718*.
9. G.G. STOKES (1845). On the theories of the internal friction of fluids in motion, and of the equilibrium and motion of elastic solids. *Trans. Camb. Phil. Soc.* **8**, 287–305.
10. P. VAN BEEK, R.R.P. VAN NOOYEN, P. WESSELING (1995). Accurate discretization of gradients on non-uniform curvilinear staggered grids. *J. Comput. Phys.* **117**, 364–367.
11. P. WESSELING, P. VAN BEEK, R.R.P. VAN NOOYEN (1994). Aspects of non-smoothness in flow computations. In *Computational Methods in Water Resources X* (edited by A. PETERS, G. WITTUM, B. HERRLING, U. MEISSNER, C.A. BREBBIA, W.G. GRAY, G.F. PINDER), Kluwer, Dordrecht, 1263–1271.
12. M. ZIJLEMA (1996). *Computational modeling of turbulent flow in general domains*, Delft University of Technology, Ph.D. thesis.
13. M. ZIJLEMA, A. SEGAL, P. WESSELING (1995). Invariant discretization of the $k-\epsilon$ model in general co-ordinates for prediction of turbulent flow in complicated geometries. *Comput. Fluids* **24**, 209–225.
14. M. ZIJLEMA, A. SEGAL, P. WESSELING (1995). Finite volume computation of incompressible turbulent flows in general co-ordinates on staggered grids. *Int. J. Numer. Meth. Fluids* **20**, 621–640.
15. M. ZIJLEMA, P. WESSELING (1995). On accurate discretization of turbulence transport equations in general coordinates. In *Proc. Ninth Int. Conf. on Numer. Meth. Laminar and Turbulent Flow* (edited by C. TAYLOR, P. DURBETAKI), Pineridge Press, Swansea, 34–45.

Machinevolgordeproblemen en samenwerking

Werkgemeenschap	: Mathematische Besliskunde en Systeemtheorie
Project	: Machinevolgordeproblemen en samenwerking
Projectleiders	: Prof. dr. S.H. Tijs, dr. P.E.M. Borm
Projectmedewerker(s)	: Dr. H.J.M. Hamers
Instelling	: Katholieke Universiteit Brabant

Probleembeschrijving

In machinevolgordeproblemen moeten verschillende taken worden uitgevoerd op een aantal machines. Eigenschappen van de machines (bijvoorbeeld parallel of identiek), restricties op de taken (bijvoorbeeld starttijden of precedentierestricties) en het gekozen kostencriterium bepalen een specifiek machinevolgordeprobleem. Het gestelde doel is het vinden van een toelaatbaar toewijzingsschema van de taken over de machines zodat het gegeven kostencriterium geoptimaliseerd wordt.

Machinevolgordeproblemen zijn zowel voor de theorie als voor de praktijk aantrekkelijk. Vandaag de dag is men vanuit theoretisch oogpunt vooral geïnteresseerd in de rekenkundige complexiteit van machinevolgordeproblemen. Hierbij wordt ernaar gestreefd een algoritme te ontwikkelen dat voor elk probleem in 'korte' tijd een optimale toewijzing genereert. Helaas zijn veel klassen van machinevolgordeproblemen NP-hard. Dit betekent dat het hoogst onwaarschijnlijk is een optimale oplossing te vinden via een tijdsefficiënt algoritme. Voor dit type problemen worden dan heuristische ontwikkeld om 'snel' een benadering te krijgen van een optimaal toewijzingsschema in een gegeven probleem.

Een groot aantal praktische beslissingssituaties kunnen beschreven worden door machinevolgordeproblemen. Men kan hierbij denken aan de productie van auto's, het toewijzen van patiënten aan operatiekamers of het onderhoud aan vliegtuigen. De aanwezige theoretische kennis kan vaak behulpzaam zijn om deze praktische problemen aan te pakken. Omgekeerd geven praktische problemen ook aanleiding tot het ontwikkelen van nieuwe oplossingsmethoden en wordt op deze manier de theorie verrijkt.

Laten we nu eens machinevolgordeproblemen bekijken met één extra aspect: iedere taak die uitgevoerd dient te worden, behoort toe aan een economische agent. Denk hierbij bijvoorbeeld aan verschillende agenten die ieder afzonderlijk van elkaar een

bepaald produkt willen laten maken. In deze situatie bestaat een taak uit een opdracht van een agent. In dergelijke gevallen zal de produktievolgorde bepaald worden door bijvoorbeeld het 'first in first out principe'. Als hierbij een wachtrij is ontstaan, kan het betreffende bedrijf dat over de machine(s) beschikt, niet zomaar de volgorde wijzigen. Met andere woorden, de beslissing om een taak een andere plaats te geven in de wachtrij kan slechts genomen worden na toestemming van de agenten. In deze nieuwe situatie, waarin verscheidene beslissers een rol spelen, zal de ontstane wachtrij niet noodzakelijk optimaal zijn voor de groep als geheel. In feite kunnen we de gegenereerde wachtrij beschouwen als een begintoewijzing op de machines. Wellicht kunnen groepen van agenten kosten besparen door samen te werken en de taken van de betreffende agenten een nieuwe plaats toe te wijzen, natuurlijk onder bepaalde restricties met betrekking tot de overige agenten. Indien een samenwerkingsverband van een groep agenten kosten bespaart, is de vraag hoe deze kostenbesparing op een eerlijke manier verdeeld kan worden over de betrokken agenten.

De coöperatieve speltheorie draagt in belangrijke mate bij aan de oplossing van kostenbesparende toewijzingsproblemen. In de coöperatieve speltheorie wordt aangenomen dat de kosten(besparingen) van elke groep van spelers, een coalitie, gerepresenteerd kan worden door een functie c die aan elke coalitie S een getal $c(S)$ toevoegt. Interessante oplossingen zijn kosten(besparende) toewijzingen die in de core van het spel liggen. De core bestaat uit die toewijzingen waarvoor geen coalitie bestaat die zich kan verbeteren door zich af te splitsen. Omdat de core kan bestaan uit een groot aantal toewijzingen is het interessant om een speciale toewijzing te vinden door extra eisen op te leggen of bekende en meer algemene speltheoretische oplossingsconcepten voor deze speciale situatie te gebruiken.

Het coöperatieve spel dat een machinevolgorde-

probleem beschrijft waarbij de taken aan agenten toebehoren, is een machinevolgordespel (of sequencing spel) waarin de spelers de agenten zijn en de functie c voor elke coalitie de maximale kostenbesparing weergeeft die een coalitie door samenwerking kan behalen. Een machinevolgordespel is een typisch voorbeeld van een combinatorisch spel: een spel dat voortkomt uit een combinatorisch optimaliseringsprobleem.

Geschiedenis van combinatorische spelen

De afgelopen twintig jaar is veel onderzoek verricht naar de interactie tussen combinatorische optimaliseringsproblemen en coöperatieve speltheorie. Dit onderzoek resulteerde in een groot aantal combinatorische spelen, zoals minimum opspannende boomspelen, bezorgingsspelen, lineaire productiespelen, handelsreizigersspelen, stroomspelen en sequencing spelen. Voor een beter begrip zullen we de twee eerstgenoemde typen spelen nader beschouwen.

Bekijk de situatie waarin een aantal landen verbonden wil worden met een bepaalde oliebron (zie figuur 1). Deze verbindingen mogen rechtstreeks zijn, maar kunnen ook via andere landen lopen. Het is wenselijk dat het netwerk dat alle landen met de oliebron gaat verbinden zo goedkoop mogelijk is. De kosten van elke pijpleiding tussen twee landen en de kosten van de pijpleidingen tussen elk land en de oliebron zijn bekend. Bovenstaand probleem kunnen we beschrijven met behulp van een graaf. De kanten van de graaf representeren de pijpleidingen, één punt van de graaf is de oliebron en de andere punten zijn de landen. Op elke kant van de graaf worden de kosten gezet van de aanleg van deze pijpleiding.

Het probleem is nu gereduceerd tot het vinden van een zo goedkoop mogelijke deelgraaf die de oliebron met alle landen verbindt. Dit probleem staat bekend als het minimum opspannende boom probleem. De oplossing blijkt een boom te zijn die relatief eenvoudig gevonden kan worden met de algoritmes van Kruskal of Prim.

Door nu de landen te beschouwen als spelers en de kosten van elke coalitie te definiëren als de goedkoopste boom die deze coalitie verbindt met de bron, ontstaat een minimum opspannend boom spel. Dit spel geeft de mogelijkheid te analyseren wat ieder land moet bijdragen in de kosten voor de aanleg van het globale netwerk, bijvoorbeeld door het bepalen van een core-allocatie.

Beschouw nu de situatie dat een postbode de post moet bezorgen in een plaats waar slechts één post-

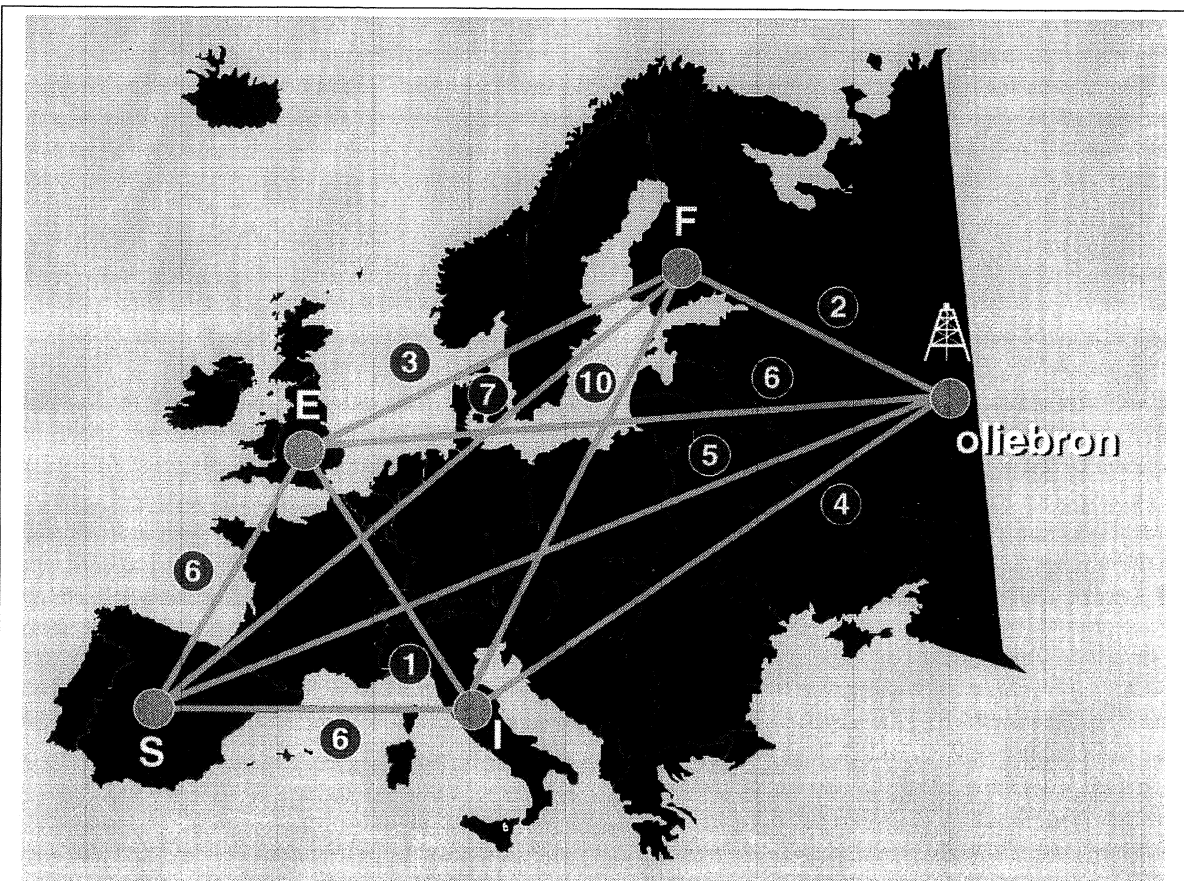
kantoor is. Hij wil een route lopen waarin hij begint vanuit het postkantoor, vervolgens in alle straten de post bezorgt en tenslotte weer terugkeert in het postkantoor. De postbode wil een zo goedkoop mogelijke route lopen die bovenstaande eigenschap heeft. Ook dit probleem is te beschrijven met behulp van een graaf waar de kanten de straten representeren. Aan de kanten wijzen we de (bezorgings)kosten toe van de corresponderende straat en één punt vertegenwoordigt het postkantoor. Het probleem is nu het vinden van een zo goedkoop mogelijke tour in de graaf die iedere kant minstens één keer bezoekt. Edmonds en Johnson losten dit probleem, dat bekend staat als het Chinese postbode probleem, op met een tijdsefficiënt algoritme.

Door nu elke straat (kant) als een speler te beschouwen en de kosten van elke coalitie te definiëren als de goedkoopste tour die elke kant van deze coalitie minstens één keer bezoekt, ontstaat een bezorgingsspel. Voor deze spelen is een toewijzingsregel ontwikkeld die voldoet aan een aantal fraaie eigenschappen. Bovendien kan de klasse van grafen waarvoor er core-toewijzingen bestaan volledig gekarakteriseerd worden.

Het project

De doelstelling van het project 'Machinevolgordeproblemen en samenwerking' was het ontwerpen van kostentoewijzingsmechanismen voor verschillende klassen van machinevolgordeproblemen en het karakteriseren van deze problemen met behulp van specifieke eigenschappen. Het accent lag hierbij op de eerlijkheid, stabiliteit en berekenbaarheid van de mechanismen. De wijze van benadering werd ontleend aan de coöperatieve speltheorie.

Als startpunt werden de machinevolgordeproblemen genomen die bestudeerd waren door Curiel, Pederzoli en Tijs. De verdeelregel die zij ontwikkelden is gegeneraliseerd. Dit leidde tot een verzameling van verdeelregels die door een aantal mooie eigenschappen gekarakteriseerd konden worden. Bovendien liggen alle verdeelregels van dit type in de core en kunnen ze relatief snel uitgerekend worden door gebruik te maken van het algoritme dat een optimale toewijzing genereert voor deze klasse van machinevolgordeproblemen. Behalve nieuwe verdeelregels werden ook klassieke speltheoretische oplossingsconcepten bestudeerd. Dit leverde expliciete uitdrukkingen op voor zowel de Shapley-waarde als de τ -waarde.



Figuur 1. De aanlegkosten van pijpleidingen tussen Finland (F), Engeland (E), Spanje (S), Italië (I) en de oliebron zijn omcirkeld. Zo zijn bijvoorbeeld de aanlegkosten van de pijpleiding tussen Italië en Finland gelijk aan 10. De volgende tabel geeft nu de waarde van elke coalitie in het bijbehorende minimum opspannende boomspel.

S	{F}	{E}	{S}	{I}	{F,E}	{F,S}	{F,I}	{E,S}	{E,I}
c(S)	2	5	5	4	5	7	6	10	5

S	{S,I}	{F,E,S}	{F,E,I}	{F,S,I}	{E,S,I}	{F,E,S,I}
c(S)	9	10	6	11	10	11

Bijvoorbeeld de waarde van coalitie {E} wordt verkregen door E zo goedkoop mogelijk te verbinden met de bron. In deze situatie is de goedkoopste verbinding via Finland. Dus de kosten van {E} zijn $3 + 2 = 5$. Een core-toewijzing is bijvoorbeeld $(F, E, S, I) = (2, 3, 1, 5)$.

Verder is er een grotere klasse van machinevolgordeproblemen geanalyseerd waarin de aanname dat elke taak op dezelfde tijd zou kunnen beginnen, is versoepeld. Voor een generalisatie van de zogenaamde convexiteitseigenschap van 'gewone' sequencing spelen, bleek het nodig het algoritme dat een optimale toewijzing van de taken geeft, verder te ontleden, in die zin dat relaties tussen optimale volgorden

van verschillende coalities gelegd moesten worden. Zo moesten specifieke eigenschappen van algoritmen worden bestudeerd die voor het eigenlijke optimaliseringsprobleem niet direct relevant zijn, maar voor een speltheoretische analyse noodzakelijk.

Recent onderzoek

In 1995 richtte het onderzoek zich op andere gene-

realisaties van de in de vorige paragraaf beschreven machinevolgordeproblemen.

Ten eerste werden machinevolgordeproblemen geanalyseerd waarin twee typen van agenten zijn betrokken: actieve en inactieve agenten. Voor deze spelen werden elegante uitdrukkingen voor de Shapley-waarde en de τ -waarde gevonden. Vervolgens zijn machinevolgordeproblemen bekeken waarin onzekerheid bestaat over de begintoewijzing. Voor deze machinevolgordeproblemen is een verdeelregel geïntroduceerd die op twee verschillende manieren is gekarakteriseerd. Tot slot beschouwden we machinevolgordeproblemen met een aantal parallelle, identieke machines. Hier werd een procedure beschreven die tot een optimale toewijzing leidt en

tegelijkertijd een allocatie genereert.

Het project, dat in 1995 is afgerond, heeft voor een aantal machinevolgordeproblemen nieuwe verdeelmechanismen voortgebracht. Daarnaast zijn eigenschappen gevonden voor speciale klassen van sequencing spelen. De verwantschap van machinevolgordeproblemen met andere combinatorische optimaliseringsproblemen gaf bovendien aanleiding tot de analyse van een nieuwe klasse van combinatorische spelen, de bezorgingsspelen.

Literatuur

HERBERT HAMERS (1995). *Sequencing and Delivery Situations: a Game Theoretic Approach*, CentER Dissertation no. 7, Tilburg University.

Berekenen en visualiseren van invariante variëteiten in dynamische systemen

Werkgemeenschap	: Analyse
Project	: Berekenen en visualiseren van invariante variëteiten in dynamische systemen
Projectleider(s)	: Prof. dr. H.W. Broer, dr. G. Vegter
Projectmedewerker(s)	: Mw. drs. H.M. Osinga
Instelling	: Rijksuniversiteit Groningen

Meetkundige studie van dynamische systemen

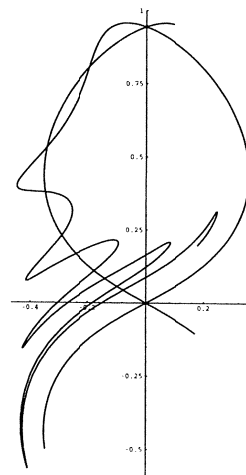
Stelsels gewone, autonome differentiaalvergelijkingen worden veel gebruikt bij de beschrijving van dynamische systemen. Te denken valt aan de bewegingsvergelijkingen van een fysisch, biologisch of economisch systeem. Voor een ruimere definitie van dynamische systemen wordt verwezen naar [1].

Het oplossen van zulke differentiaalvergelijkingen is in het algemeen geen eenvoudige zaak. In de periode van Newton tot Poincaré pakte men dit probleem vooral aan vanuit het oogpunt van individuele evoluties en eventuele benaderingen hiervan.

Poincaré liet zien dat die methode essentiële belemmeringen kent, daar deze bepaalde dynamische verschijnselen (o.a. chaos) niet zichtbaar maakt. Hij stelde een meetkundige aanpak voor, die vooral dan goed werkt als het aantal vrijheidsgraden niet al te groot is. Het voorstel komt erop neer dat in de toestands- of faseruimte het geheel van alle mogelijke integraalkrommen (oplossingen) moet worden bestudeerd: het zogenaamde faseportret. Belangrijk is de organisatie van dit faseportret rondom stationaire en periodieke oplossingen, vooral wat betreft het asymptotisch gedrag van de integraalkrommen in de oneindig verre toekomst. Heden ten dage wordt vaak de computer ingezet voor simulatie van de tijds-evolutie.

Eén van de vele begrippen die zo ontstonden is het 'basin van attractie' van een aantrekkend stationair punt. Dit basin wordt gevormd door alle begintoestanden waarvan de tijdsevolutie eindigt in het stationaire punt. Belangrijk hierbij zijn de 'separatrices', de grenzen tussen verschillende basins van attractie. Poincaré zelf was reeds verbaasd door de meetkundige complexiteit van dergelijke separatrices. In een bepaald geval, waarin de separatrix zichtbaar gemaakt wordt als kromme in het vlak,

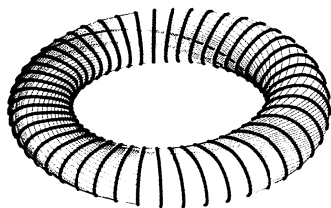
spreekt hij van 'een soort traliewerk, een door elkaar gevlochten weefsel, een stelsel van mazen dat oneindig dicht in elkaar gegroeid is'. Deze complexiteit was uiteindelijk pas enigszins in kaart te brengen met behulp van de computer en leidde onder meer tot het begrip 'fractal'. Deze meetkunde blijkt gerelateerd aan bepaalde vormen van chaos (homokliene chaos, om precies te zijn), zie figuur 1. Deze separatrices zijn algemeen invariant onder de tijdsevolutie van het systeem: met een bepaalde toestand liggen ook alle toekomstige (en verleden) toestanden erin. Ook geldt in belangrijke gevallen dat de separatrix, althans lokaal, een gladde deelvariëteit van de toestandsruimte is. De meest gebruikelijke conditie voor deze gladheid is gerelateerd aan de term 'hyperboliciteit'.



Figuur 1. Homokliene wirwar in een Poincaré-afbeelding.

Een bepaald type separatrix wordt voortgebracht door stationaire of periodieke evoluties die de eigenschap van hyperboliciteit bezitten. Men spreekt wel van de stabiele en onstabiele variëteit van de betreffende evolutie. Een ander type 'separatrix'

heeft een globaler karakter en de gebruikelijk conditie heet hier ‘normale hyperboliciteit’. Te denken valt aan een torus-attractor in een drie-dimensionale toestandsruimte (zie figuur 2). In het algemeen kan een (normaal) hyperbolische invariante variëteit zowel aantrekkende als afstotende richtingen hebben. Dergelijke objecten zijn niet gemakkelijk door numerieke simulatie op te sporen.



Figuur 2. Een torus-attractor. De torus is invariant onder de tijdsevolutie van het systeem. Alle punten in de buurt van de torus bewegen met het verstrijken van de tijd naar de torus toe.

In al deze gevallen geeft de hyperboliciteitsconditie de unieke existentie van de betreffende invariante variëteit. Het bewijs maakt gebruik van een contractie-argument en de dekpuntsstelling van Banach in een oneindig-dimensionale ruimte.

Recente ontwikkelingen

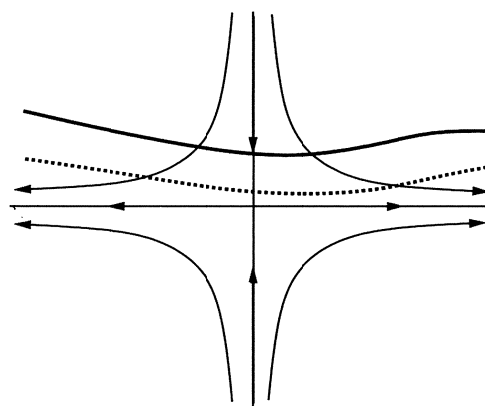
De ontwikkeling van krachtige computers heeft de numerieke en computer-grafische bestudering van dynamische systemen mogelijk gemaakt. Gedurende het laatste decennium zijn met dit doel vele interactieve software-pakketten ontwikkeld, zoals DsTool, LocBif en Auto. Deze pakketten zijn goed in staat evenwichtspunten en periodieke oplossingen van redelijk algemene dynamische systemen te berekenen en te visualiseren. In sommige gevallen is het mogelijk een-dimensionale invariante variëteiten te berekenen, maar daarmee is meteen de grens van het softwarematig mogelijke bereikt. De berekening van hoger-dimensionale invariante variëteiten is met de in de meeste pakketten gebruikte methoden (numerieke integratie van het systeem) niet mogelijk.

In enkele recente ontwikkelingen in de literatuur worden met diverse nieuwe methoden de grenzen van het kunnen verlegd. Zo is het inmiddels mogelijk torus-attractoren en hoger-dimensionale invariante variëteiten te berekenen, maar elk van de uit de literatuur bekende methoden heeft zijn beperkingen. Soms moet de invariante variëteit van een bepaald type zijn (bijvoorbeeld een cirkel of torus), of moet het dynamisch gedrag op of in de buurt van de invariante variëteit aan bepaalde eisen voldoen

(bijvoorbeeld een quasi-periodiek of normaal aantrekkend karakter hebben). Ook is voor veel van deze methoden niet, of slechts onder zeer beperkende voorwaarden, aangetoond dat het numerieke proces convergeert. Deze moeizame ontwikkelingen illustreren de noodzaak een algemeen numeriek algoritme te ontwerpen, dat aantoonbaar convergeert. In het kader van het onderhavige SMC-project is een dergelijke methode inmiddels met succes ontwikkeld.

Het SMC-project

De in Groningen ontwikkelde algoritmen zijn gebaseerd op meetkundige ideeën die al te vinden zijn in de bewijzen van de eerste stellingen over de existentie van invariante variëteiten van hyperbolische dekpunten. Deze dateren uit het begin van deze eeuw en zijn van de hand van Hadamard (1901) en Peron (1929). De zeer algemene theorie van normaal-hyperbolische variëteiten, die in de zeventiger jaren door Hirsch, Pugh en Shub is ontwikkeld, is gebaseerd op vergelijkbare meetkundige ideeën.



Figuur 3. De grafiek-transformatie beeldt de bijna-horizontale kromme h af op de bijna-horizontale kromme h' . De instabiele variëteit van het zadelpunt in de oorsprong is het dekpunt van deze operator.

Het centrale meetkundige concept is de grafiek-transformatie, een contractie-operator die de te berekenen invariante variëteit als dekpunt heeft. Om te illustreren hoe deze operator werkt, bekijken we een sterk vereenvoudigd lineair systeem op het vlak met een hyperbolisch zadelpunt in de oorsprong (zie figuur 3). Gemakshalve nemen we aan dat zowel de horizontale als de verticale as invariant zijn onder de evolutie van het systeem, waarbij de evolutie langs de horizontale as afstotend en langs de verticale as aantrekkend is. Anders gezegd, buiten het zadelpunt bewegen alle punten op de horizontale as met het

verstrijken van de tijd van het zadelpunt af, terwijl punten op de verticale as juist naar het zadelpunt toe bewegen.

Alle andere banen in de buurt van de oorsprong hebben een hyperboolachtige vorm, waaraan dit type singulariteit zijn naam (zadelpunt) dankt. De grafiektransformatie werkt op de ruimte van 'bijna-horizontale' krommen, waartoe ook de horizontale as behoort. Door zo'n bijna-horizontale kromme gedurende één tijdseenheid met het systeem te laten evolueren ontstaat een nieuwe bijna-horizontale kromme. Deze laatste is per definitie het beeld onder de grafiektransformatie van de oorspronkelijke kromme. Deze bijna-horizontale krommen kunnen worden opgevat als grafieken van functies, vandaar de naam van deze operator.

De horizontale as wordt door de grafiektransformatie op zichzelf afgebeeld (is een dekpunt), aangezien hij invariant is onder de tijdsevolutie van het systeem. Door een aantal technische restricties op te leggen aan de ruimte van bijna-horizontale krommen (we beperken ze tot een klein vierkantje gecentreerd rond de oorsprong en introduceren een functie die de afstand meet tussen elk paar krommen) kunnen we bewijzen dat de grafiektransformatie een contractie (een 'afstands-verkleinende operator') is. Bovendien kunnen we de contractiefactor van de grafiektransformatie zeer nauwkeurig uitdrukken in enkele dynamische parameters van het systeem (in het voorbeeld de eigenwaarden van het zadelpunt).

Zoals al genoemd is in de inleiding, hebben contracties, en dus ook de grafiektransformatie, een uniek dekpunt, dat zeer eenvoudig middels een numeriek iteratieproces is uit te rekenen. De convergentiesnelheid van het proces wordt bepaald door de contractiefactor van de operator, en dus, zoals al eerder opgemerkt, door enkele dynamische parameters van het systeem. De grafiektransformatie is analoog te introduceren voor zadelpunten van niet-lineaire systemen, waarbij ook de dimensie van de onderliggende ruimte willekeurig kan zijn.

Uiteraard moet nog een groot aantal implementatieproblemen worden opgelost voordat bovenstaand meetkundig idee is vertaald in een efficiënt algoritme. Zo moeten we bijvoorbeeld voor de ruimte van bijna-horizontale krommen, die oneindig-dimensionaal is, een geschikte eindig-dimensionale

benadering construeren. Dergelijke problemen zijn in de eerste fase van het project opgelost voor de berekening van invariante variëteiten van zadelpunten.

Recent onderzoek

In 1995 is het onderzoek voornamelijk gericht op het berekenen van normaal-hyperbolische invariante variëteiten en de daarbij horende (in)stabile variëteiten. Er is een algemeen algoritme ontwikkeld voor discrete systemen, gebaseerd op een generalisatie van de al eerder beschreven grafiektransformatie. Daarbij is het simpele, nul-dimensionale zadelpunt uit het voorbeeld van figuur 3 vervangen door een normaal-hyperbolische variëteit van willekeurige dimensie. De dynamica van het systeem in richtingen die niet raken aan deze variëteit lijkt enigszins op de dynamica van het lineaire systeem uit dit voorbeeld.

Het recentst ontwikkelde algoritme is in staat dergelijke invariante variëteiten van het meest algemene type uit te rekenen. De hierboven geschatte beperkingen van veel van de bestaande methoden zijn daarmee overwonnen. Dit volgt niet alleen uit de wiskundige onderbouwing van de methode, maar ook uit een aantal case-studies, waarbij telkens andere dynamische kenmerken een rol spelen (zie []).

Deze methode is inmiddels goed ontvangen in de literatuur. Niettemin is verdere ontwikkeling nodig alvorens aanspraak gemaakt kan worden op het predicaat 'production software'. Daarbij zal, meer dan in het kader van het huidige project mogelijk was, aandacht besteed worden aan de ontwikkeling van op het probleem toegesneden datastructuren voor de representatie van invariante variëteiten en zal ook nauwkeuriger worden gekeken naar de effecten van discretisatie op de nauwkeurigheid van de berekeningen. Tenslotte heeft het ontwikkelen van methoden voor het visualiseren van de berekende variëteiten hoge prioriteit.

Litaratuur

1. H.W. BROER, J. VAN DE CRAATS en F. VERHULST, (1995). *Het Einde van de Voorspelbaarheid? Chaostheorie, Ideeën en Toepassingen*, Aramith Uitgevers/Epsilon Uitgaven.
2. H.M. OSINGA (1996). *Computing Invariant Manifolds. Variations on the Graph Transform*, proefschrift Rijksuniversiteit Groningen.

Het ontbinden van grote getallen in priemfactoren

Werkgemeenschap	: Algebra en Meetkunde
Project	: Numerieke getaltheorie: Het ontbinden van grote gehele getallen in priemfactoren
Projectleider(s)	: Prof. dr. R. Tijdeman, dr. ir. H.J.J. te Riele
Projectmedewerker(s)	: Mw. drs. R.H. Elkenbracht-Huizing
Instelling	: CWI Amsterdam, Rijksuniversiteit Leiden

Inleiding

De fundamentele stelling van de rekenkunde zegt dat ieder natuurlijk getal kan worden geschreven als een produkt van eindig veel priemgetallen en dat deze schrijfwijze uniek is, afgezien van de volgorde van de priemfactoren. Zo is $1995 = 3 \times 5 \times 7 \times 19$ en hieruit ziet men bijvoorbeeld gemakkelijk dat het aantal delers van 1995 gelijk is aan $2 \times 2 \times 2 \times 2 = 16$. Iedere deler van 1995 is namelijk te schrijven als het product van de elementen uit een deelverzameling van $\{3, 5, 7, 19\}$ en deze laatste verzameling heeft precies 16 deelverzamelingen. Dit brengt ons op het probleem om, gegeven een natuurlijk getal, zijn priemdelers te vinden: het factorisatieprobleem.

Dit probleem heeft wiskundigen—zowel amateurs als professionals—altijd zeer geboeid. In de waarschijnlijk oudste factorisatiemethode neemt men een lijst van priemgetallen $2, 3, 5, \dots$ (die men eenvoudig kan maken met behulp van de zgn. zeef van Eratosthenes), en gaat men na welke priemgetallen dat getal delen. Men begint dan natuurlijk met het kleinste priemgetal 2, deelt een gevonden priemdelers uit, en gaat verder met het verkregen quotiënt. Men moet na het uitdelen van een gevonden priemfactor deze ook nog een keer uitproberen op het gevonden quotiënt, omdat priemfactoren tot een hogere macht in een getal kunnen voorkomen. Uiteindelijk blijft er een getal over dat misschien nog in de gebruikte lijst van priemgetallen staat (als die tenminste lang genoeg is), of dat men als priem kan erkennen omdat dat getal geen priemdelers heeft die kleiner dan of gelijk zijn aan de wortel uit dat getal. Het is ook nog mogelijk dat de gebruikte lijst niet lang genoeg is: deze moet dan uitgebreid worden, of men moet op zoek naar een betere methode ...

In de loop der eeuwen zijn er steeds efficiëntere factorisatiemethoden ontdekt, maar voor grotere getallen leek ‘factoriseren’ altijd een niet erg nuttige bezigheid. De ontdekking van het zgn. RSA-cryptosysteem (in 1976) heeft daarin verandering

gebracht omdat dat systeem gebaseerd is op de praktische ervaring dat factoriseren van grote getallen die zelf het produkt zijn van twee verschillende grote priemgetallen, verschrikkelijk veel tijd kost, zelfs met behulp van de allersnelste computers. Het onderzoek van factorisatiemethoden en met name van hun rekencomplexiteit is door de ontdekking van RSA sterk gestimuleerd omdat het voor de gebruikers van dit beveiligingssysteem van groot belang is te weten hoeveel tijd het *minimaal* kost om een groot getal te factoriseren. Tot op heden is echter nog geen afdoend antwoord op deze vraag gevonden. Daarnaast is door de ontdekking van RSA het zoeken van nieuwe, efficiëntere factorisatiemethoden in een stroomversnelling geraakt. Eén van de belangrijkste recent ontdekte methoden is de zgn. Number Field Sieve, onderwerp van uitgebreid onderzoek in dit project!

Factorisatiemethoden

Als we een factor van een getal hebben gevonden moeten we ook kunnen beslissen of die factor priem of samengesteld is. Factoriseren en primaliteitstesten zijn dus nauw met elkaar verbonden, maar in zijn algemeenheid is het *vinden van factoren* veel moeilijker dan *bewijzen dat een getal priem is*. Als we getallen die een speciale vorm hebben (zoals Fermat-getallen $2^{2^k} + 1$ en Mersenne-getallen $2^k - 1$) buiten beschouwing laten, is het grootste tot op heden gefactoriseerde getal 129 cijfers lang en heeft het grootste getal waarvan men tot nu toe primaliteit heeft kunnen bewijzen ongeveer 1500 cijfers. We zullen ons hier beperken tot het factorisatieprobleem en een korte opsomming geven van de belangrijkste bekende methoden. Gedetailleerde overzichten zijn te vinden in [2] en [5].

Zoals in de inleiding al is aangegeven is de oudste bekende factorisatiemethode de zgn. ‘trial’-methode. Een voordeel van deze methode is dat daarmee ook het priem zijn van een getal kan worden

bewezen, namelijk als het geen priemdelers heeft kleiner dan of gelijk aan de wortel uit dat getal. Fermat was de eerste die een ander idee had door op te merken dat een oneven samengesteld getal $N = rs$ kan worden geschreven als het verschil van twee kwadraten $N = a^2 - b^2$, met $a = (r + s)/2$ en $b = (r - s)/2$. De kunst is nu om een getal a te vinden zodanig dat $a^2 - N$ een kwadraat is. Een algemener idee is om getallen a en b te vinden zo dat $a^2 - b^2$ een *veelvoud* is van N , zeg kN . Er geldt dan:

$$kN = krs = (a - b)(a + b) \quad (0.1)$$

en als bijvoorbeeld r een deler is van $a - b$, en s een deler is van $a + b$, dan kunnen we r eenvoudig vinden door de grootste gemeenschappelijke deler van N en $a - b$ te bepalen (met de bekende algoritme van Euclides). Het vinden van a en b is het kernprobleem en met name het *uitsluiten* van mogelijke waarden van a en b met behulp van zeeftechnieken die gebaseerd zijn op arithmetische eigenschappen van N , is intensief bestudeerd. Het simpelste idee—dat ten grondslag ligt aan de geavanceerdste factorisatiemethoden—is uit te gaan van het kwadratische polynoom $p(x) = (x - s)^2 - N$ met $s = \lfloor N^{1/2} \rfloor$ en waarden van x in de buurt van s proberen te vinden waarvoor $p(x)$ een geheel getal is dat slechts kleine priemfactoren bevat, ofwel *glad* is. Omdat $p(x)$ een kwadratisch polynoom is, geldt dat als we voor een bepaald priemgetal q een x_0 kennen waarvoor $q|p(x_0)$, dan geldt ook: $q|p(x_0 + tp)$ voor ieder geheel getal t . Op deze manier is het mogelijk op een snelle manier gladde polynoomwaarden $p(x)$ te *zeven*. Onder bepaalde voorwaarden kan men vervolgens een aantal van deze polynoomwaarden combineren tot de gewenste vorm (0.1). Deze algoritme staat bekend onder de naam ‘kwadratische zeef’.

Moderne factorisatie-algoritmen kan men in twee klassen indelen: de eerste klasse spoort kleine priemfactoren sneller op dan grote (zoals trial division, Pollard Rho, $p \pm 1$ en de Elliptic Curve methode) en de tweede klasse van methoden vindt een factor in een tijd die onafhankelijk is van zijn grootte, maar kost meer naarmate toegepast op grotere getallen (zoals de kettingbreukmethode, de kwadratische zeef, en de Number Field Sieve). De twee klassen vullen elkaar in de praktijk goed aan: eerst probeert men één of meer methoden uit de eerste klasse en als dan voldoende lang naar kleine priemfactoren is gezocht (en de resulterende cofactor niet priem is) past men een methode uit de tweede klasse toe.

De beste methode uit de eerste klasse is H.W. Lenstra’s Elliptic Curve methode (ECM) waarin een

elliptische kromme wordt gezocht (gedefinieerd over de getallen modulo N) waarvan de groep-orde een veelvoud van een glad getal is dat dicht in de buurt ligt van een priemdelers van N . De grootste tot op heden met ECM gevonden priemfactor is een getal van 47 cijfers. De beste methode uit de tweede klasse was tot voor kort de kwadratische zeefmethode. Het grootste hiermee gefactoriseerde getal is een getal van 129 cijfers [2]. Zeer binnenkort zal dit record verbeterd worden: dan zal een getal van 130 cijfers worden ontbonden met behulp van de Number Field Sieve, ten koste van een hoeveelheid rekentijd die ongeveer 10% bedraagt van de rekentijd die nodig was om met de kwadratische zeefmethode het getal van 129 cijfers te factoriseren (zie onder *Recent onderzoek*).

Op een klassieke Von Neumann computer neemt men aan dat factorisatie een hoeveelheid tijd kost die een *niet-polynomiale* functie is van de lengte van de input (hoewel dit nog steeds niet bewezen is). Zeer recentelijk heeft Peter Shor van AT&T Bell Labs algoritmen voorgesteld voor het vinden van discrete logaritmen en het factoriseren van gehele getallen op een zgn. quantum computer, die een aantal stappen vereisen dat *polynomiaal* is in het aantal cijfers van de modulus van de discrete logaritme, respectievelijk van het te factoriseren getal [4]. De quantum computer is een nog niet bestaande, op quantummechanica gebaseerde computer, maar als men er in zou slagen zo’n machine te bouwen zou dat, althans theoretisch, het einde betekenen van RSA!

Inhoud van het SMC-project

Bij aanvang van het SMC-project bestonden er wereldwijd slechts enkele implementaties van de zgn. *speciale* Number Field Sieve: deze methode werkt uitsluitend voor getallen van de vorm $N = a^b \pm c$, waarbij a en c klein zijn (zoals Mersenne-getallen $2^k - 1$). De implementatie van de zgn. *algemene* Number Field Sieve—die toepasbaar is voor *willekeurige* getallen—stuitte vooral in de laatste twee fasen van de methode op problemen. Het eerste probleem was het vinden van vectoren uit de kern van een gigantische matrix over \mathbb{F}_2 , het lichaam met twee elementen 0 en 1. Het tweede probleem was het ontbreken van een adequate methode om een wortel uit een ‘algebraïsch’ getal te trekken (zie tekstbox *Beknpte beschrijving van de Number Field Sieve*).

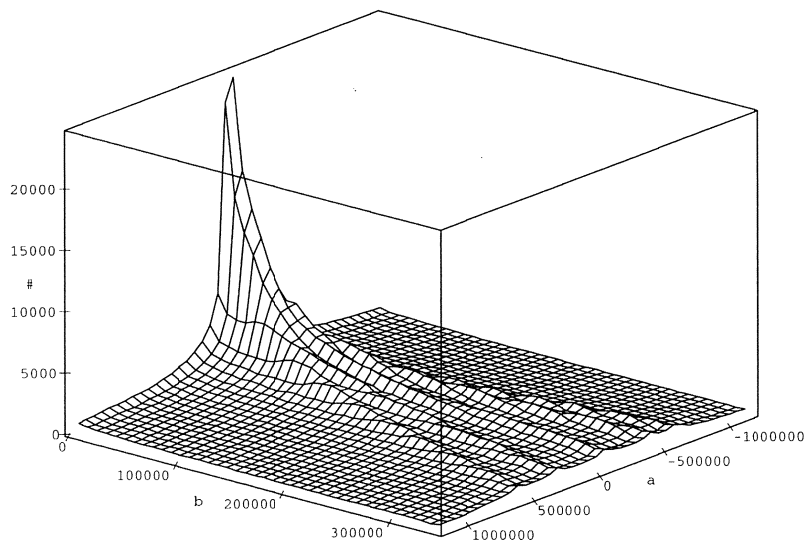
Nadat in het eerste jaar van het project de Number Field Sieve methode bestudeerd is en ervaring is opgedaan met de speciale NFS-implementatie van Bob Silverman, kwam in het tweede jaar Peter Montgomery naar Nederland. Een Stimulans-beurs en steun

Beknopte beschrijving van de Number Field Sieve

In de eerste fase van de Number Field Sieve worden twee irreducibele polynomen

$f_i(x) = c_{i,d_i}x^{d_i} + c_{i,d_i-1}x^{d_i-1} + \dots + c_{i,0} \in \mathbb{Z}[x]$ ($i = 1, 2$) gekozen die een gemeenschappelijke wortel m modulo n hebben. Zij α_i een wortel van $f_i(x)$ in \mathbb{C} en zij $F_i(x, y) = y^{d_i} f_i(x/y) \in \mathbb{Z}[x, y]$ de homogene vorm van $f_i(x)$ ($i = 1, 2$). In de tweede fase—het *zeven*—worden paren $(a, b) \in \mathbb{Z}^2$ geselecteerd zodanig dat zowel $F_1(a, b)$ als $F_2(a, b)$ glad zijn, ofwel uitsluitend kleine priemfactoren bevatten. Zulke paren heten *relaties*.

De polynomen moeten zo gekozen worden dat we zoveel mogelijk relaties op een vast gebied $|a| \leq C_1, 0 < b \leq C_2$ zullen vinden. Figuur 1 laat zien dat als zo'n polynoom veel reële wortels heeft dit een positieve uitwerking op het aantal relaties kan hebben. In de derde fase maken we een selectie uit de gevonden relaties. Een relatie (a, b) waarvoor een priem p het getal $F_1(a, b)$ deelt, maar deze p deelt geen enkele andere $F_1(a, b)$ is nutteloos en wordt tijdens deze *filter* fase weggegooid. In de vierde fase wordt een matrix gebouwd waarbij de kolommen corresponderen met relaties en de rijen met priemmen die de $F_i(a, b)$ delen. Met de block Lanczos methode worden vectoren uit de kern van deze ijle matrix over \mathbb{F}_2 gevonden. Zij \mathbb{Q}_n de ring van rationale getallen met noemer relatief priem met n . Een vector uit de kern correspondeert met een deelverzameling \mathcal{S} van de relaties zodanig dat zowel $\prod_{\mathcal{S}}(a - b\alpha_1)$ als $\prod_{\mathcal{S}}(a - b\alpha_2)$ kwadraten zijn—zeg β^2 en γ^2 —in, respectievelijk, $\mathbb{Q}_n[\alpha_1]$ en $\mathbb{Q}_n[\alpha_2]$. Toepassing van twee natuurlijke ringhomomorphismen $\phi_i : \mathbb{Q}_n[\alpha_i] \rightarrow \mathbb{Z}/n\mathbb{Z}$ bepaald door $\phi_i(\alpha_i) = m \pmod{n}$ ($i = 1, 2$) op β^2 en γ^2 levert $\phi_1(\beta^2) \equiv \phi_2(\gamma^2) \pmod{n}$. Oftewel $(\phi_1(\beta))^2 \equiv (\phi_2(\gamma))^2 \pmod{n}$. Wanneer $\phi_1(\beta)$ en $\phi_2(\gamma)$ relatief priem zijn met n , zal de grootste gemene deler van n en $\phi_1(\beta) - \phi_2(\gamma)$ een niet-triviale factor van n opleveren in tenminste de helft van het aantal gevallen. De laatste fase van de Number Field Sieve—het worteltrekken—is verborgen in het feit dat de vector uit de kern correspondeert met een uitdrukking voor β^2 en γ^2 , maar ϕ_i op β en γ toegepast moeten worden.



Figuur 1. Aantal gevonden relaties per 60000 a -waarden en 8625 b -waarden voor de ontbinding van een getal van 119 cijfers dat een deler is van $3^{319} - 1$. Eén van de polynomen is $f_1(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ met 5 reële wortels. De vijf ruggen geven een verhoogde opbrengst aan voor paren (a, b) met a/b dichtbij een wortel.

van het CWI maakten het mogelijk dat hij van oktober 1993 tot augustus 1994 aan het CWI en de Rijksuniversiteit Leiden verbleef. Montgomery, die voorheen onderzoek had verricht naar de Elliptic Curve methode, ging zich nu toeleggen op de Number Field Sieve, in het bijzonder op de laatste twee fasen van de methode. Hij bracht een mede door hem op Oregon State University ontwikkelde implementatie van de eerste fasen van de Number Field Sieve mee.

Tijdens zijn verblijf werd eerst de bottleneck opgeheven aan het eind van de algemene NFS-implementatie waar de wortel uit een algebraïsch getal getrokken moet worden. Tot dusverre bestond er alleen een relatief langzame algoritme die uitsluitend werkte voor polynomen van oneven graad. Montgomery's nieuwe algoritme heeft deze beperking niet en is bovendien sneller. Samen met Elkenbracht-Huizing implementeerde hij deze algoritme. Daarna implementeerde hij een zeer snelle versie van de block Lanczos-algoritme om vectoren uit de kern van een gigantische matrix over \mathbb{F}_2 te vinden. Hoewel dit dient ter gebruik in de NFS-implementatie, kan dit Lanczos-algoritme in principe toegepast worden op iedere ijle matrix over \mathbb{F}_2 . Hiermee werd de weg geopend voor het factoriseren van een speciaal getal van 162 cijfers—nog steeds een wereldrecord voor de speciale Number Field Sieve—en het ontbinden van een algemeen getal van 105 cijfers, destijds ook een wereldrecord voor de algemene NFS. Daarna werden in het SMC-project vele 'most and more wanted' en andere getallen uit de 'Cunningham table' ontbonden. Een jaar geleden werd door een internationale groep rond Arjen Lenstra een algemeen getal van 119 cijfers ontbonden. Met behulp van de CWI-implementatie werd de laatste stap gezet. Elkenbracht-Huizing schreef een artikel over de hele Number Field Sieve implementatie. Hierin worden ideeën achter de implementatie en parameterkeuzen uitgelegd en programmeersuggesties gedaan [1].

Recent onderzoek

Vanaf augustus 1995 zijn Elkenbracht-Huizing en Montgomery in een internationaal samenwerkingsverband onder leiding van Arjen Lenstra betrokken bij de factorisatie van een getal van 130 cijfers met behulp van de algemene Number Field Sieve. In deze wereldrecordpoging zullen Elkenbracht-Huizing en Montgomery de laatste twee fasen verzorgen. De ontbinding wordt in april 1996 verwacht.

Meer structureel van aard is de implementatie door Elkenbracht-Huizing van een meer-polynoom-versie van de Number Field Sieve. Theoretisch levert het gebruik van $k > 2$ polynomen een versnellingsfactor op van $2(k-1)/k$ ten opzichte van het gebruik van twee polynomen. In eerste experimenten lijkt deze versnelling in de praktijk te kunnen worden gerealiseerd.

Literatuur

1. R.-M. HUIZING (1996). Experiments with the Number Field Sieve. *Experimental Mathematics*, to appear (also appeared as CWI Report NM-R9511, July 1995).
2. P.L. MONTGOMERY (1994). A Survey of Modern Integer Factorization Algorithms. *CWI Quarterly* 7 (4), 337–366.
3. H.J.J. TE RIELE, J. VAN DE LUNE (1994). Computational Number Theory at CWI in 1970–1994. *CWI Quarterly* 7 (4), 285–335.
4. PETER W. SHOR (1994). Algorithms for Quantum Computing: Discrete Logarithms and Factoring. S. GOLDWASSER (ed.). *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, California, 124–134.
5. H.C. WILLIAMS, J.O. SHALLIT (1994). Factoring Integers Before Computers. W. GAUTSCHI (ed.), *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics*, Proceedings of Symposia in Applied Mathematics, Vol. 48, AMS, 481–531.

Onafhankelijkheid in de quantum-kanstheorie

Samenwerkingsverband	: FOM/SMC Mathematische Fysica
Project	: Onafhankelijkheid in de quantum-kanstheorie
Projectleider(s)	: Dr. J.D.M. Maassen
Projectmedewerker(s)	: Drs. J.H.M. van Leeuwen
Instelling	: Katholieke Universiteit Nijmegen

Wat is quantum-kanstheorie?

Niet-commutatieve kanstheorie of 'quantum-kanstheorie' ontstaat door een verruiming van de axioma's van de klassieke kanstheorie die tegemoetkomt aan de merkwaardige gedragingen van de materie op atomaire en sub-atomaire schaal. Als apart vakgebied is de quantum-kanstheorie ontstaan aan het einde van de jaren zestig, maar de grondideeën stammen uit de twintiger jaren, toen de quantummechanica werd geformuleerd.

Zowel de klassieke kanstheorie als de niet-commutatieve generalisatie houden zich bezig met het berekenen van de kansen op de verschillende mogelijke uitslagen van een toevalsexperiment. Er is echter een belangrijk verschil tussen de manieren waarop de klassieke kanstheorie en de quantum-kanstheorie hun uitslagen beschrijven.

In de klassieke theorie gaat men uit van een kansruimte Ω , de lijst van alle mogelijke combinaties van uitslagen van het experiment, en kent men aan elke combinatie een kans toe. In de quantum-kanstheorie wordt rekening gehouden met de mogelijkheid dat niet alle combinaties van uitslagen kunnen worden afgelezen. Zo'n kanstheorie hoeft dus niet aan alle combinaties een kans toe te kennen: de axioma's kunnen worden afgezwakt. Zo verkrijgt men een ruimere wiskundige structuur, waar zowel de quantummechanica als de klassieke kansrekening in kan worden ondergebracht. Bouwstenen zijn Hilbert-ruimten en algebra's van lineaire operatoren daarop.

Een sleutelbegrip in de klassieke kansrekening is (*statistische*) *onafhankelijkheid*. Lange reeksen van onafhankelijke herhalingen van een experiment leiden tot de bekende *normale* of *Gauss-verdeling*. Het begrip onafhankelijkheid leidt tevens tot de constructie van *Brownse beweging* of *witte ruis*, basis voor de theorie van stochastische differentiaalvergelijkingen en stochastische integratie.

Probleemstelling

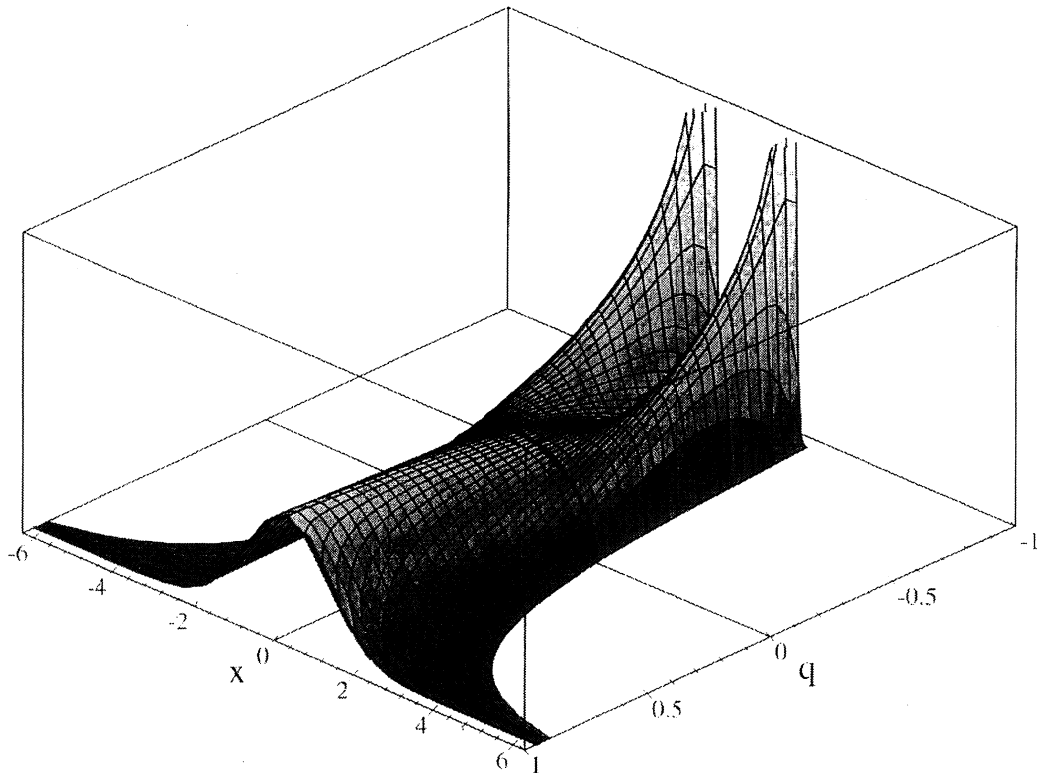
Het project 'onafhankelijkheid in de quantum-

kanstheorie' richt zich op de fundamentele vraag welke vormen van onafhankelijkheid zich in dit wiskundig raamwerk kunnen voordoen en welke varianten op de Gauss-verdeling en op witte ruis deze opleveren. Pas daarna komt de vraag of en waar deze varianten in de natuur optreden.

De ontwikkeling van de quantum-kanstheorie

Na de wiskundige formulering van de kansrekening door Kolmogorov en die van de quantummechanica door von Neumann in de jaren dertig, zijn beide gebieden lange tijd gescheiden gebleven. Hierin is verandering gekomen toen de school van Wightman in de quantumveldentheorie en de groep rond Araki in de statistische mechanica op de noodzaak stuitten een quantummechanische beschrijving te geven van fysische systemen met een oneindig aantal vrijheidsgraden. Zij stapten over van de vertrouwde Hilbert-ruimte van de fysici naar de meer abstracte C^* -algebra's en von Neumann algebra's; tot dan toe het domein van wiskundigen. Zulke algebra's kunnen op verschillende Hilbert-ruimten leven. De keuze van de Hilbert-ruimte wordt gedicteerd door de toestand van het te modelleren fysische systeem. Nu sprong de formele gelijkheid met de kansruimte van Kolmogorov in het oog: de begrensde meetbare functies hierop vormen immers ook een von Neumann-algebra, zij het een commutatieve. De kansmaat definieert een toestand op deze algebra. Toen de brug eenmaal was geslagen, lag de weg open voor het verder uitbouwen van de verbinding: Accardi, Frigerio en Lewis formuleerden in 1981 het raamwerk van de theorie van quantum-stochastische processen. Kümmerer vulde dit in tot een veelomvattende theorie van niet-commutatieve Markovketens, met toepassingen in de quantumoptica. Stochastische differentiaalvergelijkingen vonden hun plaats in het werk van Hudson en Parthasarathy.

Al de zo verkregen Markov-ketens worden 'aangedreven' door *witte ruis*, in zijn niet-commutatieve versie *quantumruis* geheten, en zijn op te vatten als



Figuur 1. De ' q -Gauss-verdeling' als functie van $q \in [-1, 1]$. Bij $q = 1$ behoort de bekende normale verdeling, bij $q = 0$ de halve cirkel van Wigner en bij $q = -1$ een soort quantum-muntworp met uitslagen 1 en -1 . Bij elke waarde van q is de verdeling stabiel onder optelling van q -onafhankelijke stochasten.

een stationaire stroom van steeds weer nieuwe, onafhankelijke informatie. Bekende soorten van quantumruis zijn Bose-ruis, zoals wit licht, en Fermi-ruis, dat een vrij Fermi-veld beschrijft. Zo kunnen bijvoorbeeld de overgangen tussen de energieniveaus van een atoom of molecuul worden opgevat als een Markov-keten, aangedreven door de Bose-ruis van het elektromagnetische veld.

De volgende stap die in dit verband een grote rol heeft gespeeld werd gezet door de wiskundige Voiculescu, die een extreem niet-commutatieve vorm van statistische onafhankelijkheid formuleerde in puur operator-theoretische termen: *vrije onafhankelijkheid*. Deze verhoudt zich tot gewone onafhankelijkheid als het vrije product tot het tensorproduct en brengt een geheel nieuwe schaduw-kansrekening met zich mee: een andere normale verdeling (met de vorm van een halve cirkel, eerder ontdekt door Wigner), een nieuw ('vrij') convolutieproduct, een nieuw

Poisson-proces en een nieuwe niet-commutatieve Brownse beweging. Toepassingen van deze vrije kansrekening zijn te vinden in de theorie van stochastische matrices en in de kernfysica.

In 1991 vonden Bozejko en Speicher een hele familie van soorten van quantum-ruis, geparametriseerd met een parameter $q \in [-1, 1]$, waarbij $q = 1$ staat voor klassieke witte ruis, $q = -1$ voor Fermi-ruis en $q = 0$ voor Voiculescu's vrije ruis (zie figuur 1). In samenwerking met Kümmerer construeerden zij Markov-ketens bij al deze waarden van q .

Uitwerking van de probleemstelling

Structuur van de klassieke theorie

In de klassieke theorie vormen de mogelijke gebeurtenissen een σ -algebra Σ van deelverzamelingen van de kansruimte Ω . Een functie $P : \Sigma \rightarrow [0, 1]$ voegt

aan deze gebeurtenissen kansen toe op een additieve manier en genormeerd op $P(\Omega) = 1$. Een kans is een getal variërend van 0 (onmogelijk) tot 1 (zeker) dat uitdrukt hoe waarschijnlijk men het acht dat de betreffende gebeurtenis zal optreden wanneer het experiment wordt uitgevoerd. Gebeurtenissen A en B heten onafhankelijk als kennis over het al of niet optreden van A niets leert over de kans op B : $P(A \cap B)/P(B) = P(A)$.

Voorbeeld: Een worp met twee dobbelstenen. Ω is de verzameling van paren (x, y) , waarbij x en y gehele waarden van 1 tot 6 aannemen. Aan elk paar $\omega = (x, y) \in \Omega$ wordt de kans $1/36$ toegekend.

Structuur van de quantum-kanstheorie

Een quantum-kansruimte bestaat uit een von Neumann-algebra \mathcal{A} met daarop een positieve lineaire functionaal φ . De gebeurtenissen worden voorgesteld door de orthogonale projecties in \mathcal{A} . De kans op de gebeurtenis P is $\varphi(P)$. In het dobbelstenenvoorbeeld is \mathcal{A} de commutatieve algebra van alle complexe functies op $\Omega = \{1, 2, 3, 4, 5, 6\}^2$. Gebeurtenissen worden beschreven door functies P die voldoen aan $P^2 = \bar{P} = P$; dit zijn de functies die enkel de waarden 0 en 1 aannemen: indicatorfuncties van deelverzamelingen van Ω . In de quantum-kanstheorie houdt men rekening met de mogelijkheid dat het aflezen van het aantal ogen van de ene dobbelsteen dat van de andere in de weg staat. In dat geval is het niet meer zinvol om over de kans op het paar uitslagen (x, y) te spreken: de kansruimte Ω vervalt. De uitslagen van de twee dobbelstenen heten dan *incompatibel*. Dit wordt geïllustreerd in het volgende voorbeeld.

Voorbeeld: Zij \mathcal{A} de algebra van alle complexe 6×6 -matrices. Zij φ het genormeerde spoor op \mathcal{A} : $\varphi(A) := \frac{1}{6} \sum_{j=1}^6 A(j, j)$. Zij $P_x, (x = 1, \dots, 6)$ de matrix die een 1 heeft op de positie (x, x) , en overall elders een 0. De P_x zijn onderling orthogonale en commuterende projecties, die elk 'kans' $\frac{1}{6}$ hebben: $\varphi(P_x) = \frac{1}{6}$. Laten nu de matrices $Q_y, (y = 1, \dots, 6)$ gegeven zijn door

$$Q_y(j, k) := \frac{1}{6} \exp(i\pi y(k - j)/3).$$

Ook dit zijn zes onderling orthogonale, commuterende projecties met $\varphi(Q_y) = \frac{1}{6}$. We interpreteren nu P_x als de gebeurtenis: de eerste dobbelsteen vertoont x ogen, en Q_y als: de tweede dobbelsteen vertoont y ogen. De gebeurtenissen P_x en Q_y zijn

onafhankelijk, want de kans op Q_y , gegeven het optreden van P_x is nog steeds $\frac{1}{6}$:

$$\frac{\varphi(P_x Q_y P_x)}{\varphi(P_x)} = \frac{1}{6}.$$

De gebeurtenissen zijn echter niet compatibel: $P_x Q_y \neq Q_y P_x$, en deze produkten zijn geen projecties. Er is dan ook geen projectie behorende bij 'de eerste dobbelsteen vertoont x ogen en de tweede vertoont y ogen'.

Het bovenstaande voorbeeld maakt duidelijk dat er, zonder de eis van commutativiteit, nieuwe vormen van onafhankelijkheid denkbaar zijn. Er blijkt zelfs een verwarrend rijk nieuw terrein open te gaan, waarin we ons tot taak gesteld hebben enige oriëntatie-punten aan te brengen. We leggen ons eerst een beperking op: we zoeken alleen vormen van onafhankelijkheid waar continue ruis van te maken is.

Het FOM/SMC-project

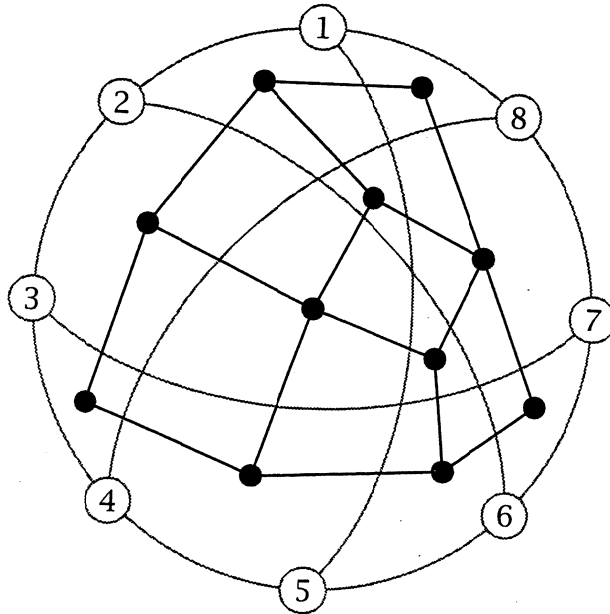
q-ruis

Uitgangspunt van de theorie van *q*-ruis is de commutatorrelatie

$$a_i a_j^* - q a_j^* a_i = \begin{cases} 0, & \text{als } i \neq j, \\ 1, & \text{als } i = j. \end{cases}$$

De stochastische variabelen zijn $X_i := a_i + a_i^*$. Deze vormen de prototypen van *q*-onafhankelijke variabelen.

In het onderzoek zijn we begonnen met een geschikte analytische beschrijving te geven van de kansverdeling van deze variabelen (zie figuur 1). Voor $q \in [0, 1]$ is deze op te vatten als de '*q*-Gaussverdeling'. Vervolgens hebben wij ons de vraag gesteld wat een '*q*-convolutieproduct' zou moeten zijn. Hierbij stuiten we echter op een probleem: de kansverdelingen van $f(X_1)$ en $g(X_2)$ leggen die van hun som $f(X_1) + g(X_2)$ niet vast. Dit negatieve resultaat, gestaafd door een concreet tegenvoorbeeld, kwam als een verrassing voor de meeste onderzoekers op dit gebied. Blijkbaar impliceert de *q*-onafhankelijkheid van X_1 en X_2 niet die van $f(X_1)$ en $g(X_2)$. Dit verzwakt het concept van *q*-onafhankelijkheid aanzienlijk. Desondanks is er een goede kandidaat voor het *q*-convolutieproduct gevonden door Nica, waarvan echter nog moet worden nagegaan of het de positiviteit van kansmaten behoudt. Hierop concentreert zich nu het onderzoek.



Figuur 2. Het verband tussen paartpartities van de getallen $1, 2, 3, \dots, 8$ (grijs), lussen in het veeldimensionale raamwerk (rand van de zwarte figuur) en door die lussen omspannen oppervlakken van plaquettes (de zwarte vierhoekjes). Er is een één-één-correspondentie tussen paartpartities en lussen, en ook tussen partitie-diagrammen en zekere oppervlakken in het raamwerk. De verwachtingswaarde van $e^{i\Phi}$, waarbij Φ de magnetische flux door het oppervlak voorstelt, is een term in het 8ste moment van de q -Gauss-verdeling. De term die bij dit plaatje hoort is q^5 omdat het oppervlak vijf vierhoekjes telt. $q = 1$ komt overeen met $\Phi = 0$: alle paartpartities van $1, 2, 3, \dots, 8$ leveren dezelfde bijdrage 1 aan het 8ste moment.

Spinglazen en Josephson-contacten

q -onafhankelijke, q -Gauss-verdeelde stochasten komen voor in een bepaald natuurkundig model. Het gaat hierbij om veel-dimensionale raamwerken van zogenaamde Josephson-contacten, blootgesteld aan een constant magneetveld, waarvan de richting willekeurig gekozen is. Het model is in 1994 gepubliceerd door Parisi in een onvolledig uitgewerkte vorm, maar bleek stand te houden onder wiskundige pre-

cisering. In het bewijs van het geclaimde q -gedrag wordt gebruik gemaakt van een correspondentie tussen alle manieren waarop de getallen $1, 2, \dots, n$ in paren kunnen worden verdeeld, en bepaalde, uit plaquettes opgebouwde oppervlakken in het veeldimensionale raamwerk (zie figuur 2). Er is een relatie tussen de magnetische flux door dit oppervlak en het n de moment van de q -Gauss-verdeling.

Niet-commutatieve meetkunde

Aandachtsprogramma	: Algoritmen in de algebra (AIDA)
Project	: Lie-algebra's
Projectleider(s)	: Prof. dr. R. Martini (UT), prof. dr. M. Hazewinkel
Projectmedewerker(s)	: Dr. ir. N.W. van den Hijligenberg
Instelling	: CWI

Niet-commutatieve meetkunde

Een differentieerbare variëteit is een verzameling punten M voorzien van een additionele geometrische structuur. De meetkundige structuur biedt de mogelijkheid krommen in M te definiëren; dit zijn differentieerbare afbeeldingen van een interval in \mathbb{R} naar M . Men kan zo'n kromme $\{m(t)\}_{t \in \mathbb{R}}$ opvatten als de baan van een deeltje in de ruimte M waarbij $m(t)$ de positie van het betreffende deeltje op tijdstip t voorstelt. In een willekeurig punt $m(t)$ geeft de afgeleide $\frac{d}{dt}m(t)$ de snelheidsvector van het deeltje op het tijdstip t weer.

De meetkundige structuur van een differentieerbare variëteit wordt volledig gekarakteriseerd door de bijbehorende functie-algebra; dit is de commutatieve algebra van complex-waardige differentieerbare functies op de variëteit waarbij optelling en vermenigvuldiging puntsgewijs zijn gedefinieerd. De meetkundige concepten, zoals bijvoorbeeld vectorvelden, differentiaalvormen, uitwendige en covariante afgeleiden, kunnen worden geformuleerd in de terminologie van deze functie-algebra. Het fundamentele idee van de niet-commutatieve meetkunde is de commutatieve functie-algebra te vervangen door een niet-commutatieve algebra en vervolgens deze formeel te beschouwen als de functie-algebra van een niet-commutatieve variëteit. Daar functie-algebra's intrinsiek commutatief zijn, betreft het hier een virtuele niet bestaande variëteit. Niettemin, vrijwel alle operaties op commutatieve functie-algebra's die bepaalde meetkundige concepten weergeven, kunnen worden gegeneraliseerd naar gelijksoortige operaties op niet-commutatieve algebra's en in die zin ontstaat datgene wat men gebruikelijk aanduidt met niet-commutatieve meetkunde.

Een mogelijke motivatie voor de bestudering van dit soort objecten kan worden gegeven aan de hand van de overgang van de klassieke mechanica naar de quantummechanica. In de klassieke mechanica wordt een dynamisch systeem beschreven door mid-

del van een Poisson-variëteit. Dit is een variëteit \mathcal{P} , ook wel de faseruimte genoemd, waarvan de functie-algebra $\mathcal{F}(\mathcal{P})$, de ruimte der observabelen, is voorzien van een speciale operatie $\{, \}$, de Poisson-haak. De evolutie van het betreffende systeem wordt bepaald door de volgende differentiaalvergelijking:

$$\frac{d}{dt}f(x(t)) = \{\mathcal{H}, f\}(x(t))$$

$$x(t) \in \mathcal{P}; f, \mathcal{H} \in \mathcal{F}(\mathcal{P}).$$

De functie \mathcal{H} is de Hamiltoniaan, deze functie herbergt specifieke dynamische eigenschappen van het onderhavige systeem. In de quantummechanica wordt de faseruimte \mathcal{P} vervangen door een complexe Hilbert-ruimte H , de functie-algebra $\mathcal{F}(\mathcal{P})$ wordt vervangen door een algebra van operatoren op deze Hilbert-ruimte. De evolutie van het quantumsysteem wordt gegeven door een soortgelijke differentiaalvergelijking waarin de rol van de Poisson-haak is overgenomen door de gebruikelijke commutator van operatoren en de rol van Hamiltoniaan wordt gespeeld door een specifieke operator H op V .

Het feit dat bij deze overgang de commutatieve functie-algebra wordt vervangen door een niet-commutatieve algebra van operatoren, inspireerde J.E. Moyal te zoeken naar een alternatieve beschrijving van de quantummechanica. Hij trachtte de puntsgewijze vermenigvuldiging van $\mathcal{F}(\mathcal{P})$ te vervangen door een niet-commutatief produkt $*_{\hbar}$, dat afhangt van een parameter \hbar , zodanig dat voor \hbar gelijk aan nul de gewone produktstructuur terug wordt gevonden net zoals de quantummechanica overgaat in de klassieke mechanica wanneer de konstante van Planck gelijk aan nul wordt gekozen, waarbij het niet-commutatieve karakter van het produkt $*_{\hbar}$ in eerste orde wordt beschreven door de Poisson-haak. Door vervolgens de resulterende niet-commutatieve algebra $\mathcal{F}_{\hbar}(\mathcal{P})$, dit is de ruimte $\mathcal{F}(\mathcal{P})$ voorzien van het nieuwe produkt $*_{\hbar}$, op te vatten als functie-algebra van een quantumruimte \mathcal{P}_{\hbar} , betreedt men de wereld van de niet-commutatieve meetkunde.

Quantumgroepen

Een variëteit voorzien van een additionele groepstructuur waarbij de groepperaties, zoals de vermenigvuldiging en het inverteren, differentieerbaar zijn, heet een Lie-groep. Lie-groepen en hun differentiaalmeetkunde spelen een prominente rol in de formulering van fysische theorieën, zoals bijvoorbeeld de klassieke mechanica, vloeistofmechanica, elasticiteitsleer en de conforme veldentheorie. De groepstructuur van een Lie-groep \mathcal{G} kan eveneens worden geherformuleerd in termen van afbeeldingen op de bijbehorende functie-algebra $\mathcal{F}(\mathcal{G})$. De vermenigvuldiging $\mu : \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}$ wordt getransformeerd in een covermenigvuldiging $\Delta : \mathcal{F}(\mathcal{G}) \mapsto \mathcal{F}(\mathcal{G}) \otimes \mathcal{F}(\mathcal{G})$ gegeven door $\Delta(f)(g, g') = f(gg')$, het één-element e van \mathcal{G} geeft een co-énelement $\epsilon : \mathcal{F}(\mathcal{G}) \mapsto \mathbb{C}$ volgens $\epsilon(f) = f(e)$, tenslotte geeft het inverteren aanleiding tot de zogeheten antipode $S : \mathcal{F}(\mathcal{G}) \mapsto \mathcal{F}(\mathcal{G})$ gedefinieerd door $S(f)(g) = f(g^{-1})$. Uiteraard zullen de afbeeldingen Δ , ϵ en S aan specifieke axioma's voldoen die zeer nauw verbonden zijn met de eigenschappen van de oorspronkelijke groep operaties. Deze extra structuur op $\mathcal{F}(\mathcal{G})$ maakt het tot een commutatieve Hopf-algebra. Het belang van deze herformulering is gelegen in het feit dat de Hopf-algebra $\mathcal{F}(\mathcal{G})$ de structuur van de Lie-groep \mathcal{G} volledig en uniek bepaalt.

Niet-commutatieve deformaties van de Hopf-algebra $\mathcal{F}(\mathcal{G})$ zijn speciale voorbeelden van quantumgroepen. Quantumgroepen verschenen voor het eerst in de fysische literatuur in 1979 in werk van L.D. Faddeev en zijn medewerkers aangaande de 'inverse scattering methode'. In de afgelopen tien jaar is er een enorme hoeveelheid aan publikaties verschenen over het fenomeen quantumgroep. Dit komt niet alleen door de fysische importantie maar eveneens door de gecompliceerde en fascinerende achterliggende wiskundige structuur. In 1985 waren het Yu.I. Manin en S.L. Woronowicz die, onafhankelijk van elkaar, quantumgroepen presenteerden als Hopf-algebra deformaties van de hiervoor beschreven functie-algebra's. Door algebraïsche operaties uit te voeren op deze gedeformeerde Hopf-algebra's, die de bekende operaties op de klassieke functie-algebra behorende bij specifieke meetkundige objecten generaliseren, kan men niet-commutatieve meetkunde bedrijven op quantumgroepen. Dit abstracte concept is geformuleerd door S.L. Woronowicz en later in meer concrete gevallen uitgewerkt door J. Wess and B. Zumino.

Nauw verbonden met het begrip Lie-groep is het begrip Lie-algebra. De Lie-algebra behorende bij

een Lie-groep wordt gedefinieerd als de lineaire ruimte van vectorvelden op deze Lie-groep die invariant zijn onder de rechts (of links) actie van de groep op zichzelf, voorzien van de commutator van vectorvelden opgevat als differentiaal operatoren. Men kan deze vectorvelden voorstellen als infinitesimale generatoren van groeppacties. De Lie-algebra is een behulpzaam stuk gereedschap in de Lie-groepen theorie, daar vele constructies, zoals bijvoorbeeld de berekening van invarianten, op elegante wijze kunnen worden gesimplificeerd met behulp van Lie-algebra berekeningen. Men kan dit vergelijken met linearisatie.

Elke Lie-algebra heeft een universeel omhullende algebra. Deze bezit een natuurlijke Hopf-algebra structuur, die dual is aan de Hopf-algebra afkomstig van de functies op de corresponderende Lie-groep. Op grond van deze dualiteit voldoet de universeel omhullende aan een eigenschap die het duale analoog is van commutativiteit, dit wordt dan ook cocommutativiteit genoemd. V.G. Drinfel'd en M. Jimbo hebben ontdekt dat bepaalde quantumgroepen beschreven kunnen worden als niet-cocommutatieve Hopf-algebra deformaties van universeel omhullende van Lie-algebra's. Deze quantumgroepen worden dan ook wel aangeduid met de term gequantiseerde universeel omhullende algebra's.

Het onderzoek bij het CWI

Het onderzoek bij het CWI op het gebied van de niet-commutatieve meetkunde is gericht geweest op de constructie van differentiaalcalculi op quantumgroepen en wel met name in hun verschijningsvorm als gequantiseerde universeel omhullende algebra's. Op een klassieke Lie-groep is er sprake van een unieke differentiaalcalculus. Deze uniciteit gaat verloren indien men niet-commutativiteit introduceert. Zelfs indien men voor de calculus de bicovariantie-eigenschap oplegt, dit is het analoog van het commuteren van de rechts en links actie van de groep op zichzelf, dan nog zal deze in het algemeen niet uniek zijn. Aan de hand van algemene ideeën van A. Connes is een effectieve methode ontwikkeld om differentiaal Hopf-algebra's, dit zijn abstracte generalisaties van De Rham-complexen, op gequantiseerde omhullende algebra's te construeren. Deze differentiaal Hopf-algebra's worden voortgebracht door Lie-algebra elementen en de bijbehorende differentiaal 1-vormen. De relaties, die het commutatiedrag tussen functies en vormen beschrijven, geven in de klassieke limiet aanleiding tot een kleuren Lie superalgebraïsche voortzetting van de Lie algebra:

$$[x^i, x^j] = C_k^{ij} x^k \quad [x^i, dx^j] = A_k^{ij} dx^k$$

$$[dx^i, dx^j] = 0$$

Deze klassieke limiet van de calculus dient in bepaald opzicht compatibel te zijn met de Lie-bialgebra structuur behorende bij de klassieke limiet van de quantisatie. De compatibiliteit is een fundamenteel aspect van de ontwikkelde methode. Bovendien geeft het de mogelijkheid de benodigde berekeningen op Lie-algebraïsch niveau uit te voeren, hetgeen zeer efficiënt kan worden gedaan met behulp van ontwikkelde implementaties in het computer algebra pakket REDUCE. De resulterende differentiaal Hopf-algebra's hebben een basis bestaande uit specifiek geordende monomen analoog aan de bekende

Poincaré-Birkhoff-Witt basis voor universeel omhullende algebra's.

In de klassieke theorie kan men exponentiële coördinaten gebruiken teneinde de dualiteitsrelatie tussen de Lie-groep en Lie-algebra expliciet weer te geven. In 1993 hebben C. Fronsdal and A. Galindo een generalisatie hiervan gepresenteerd voor matrix quantumgroepen en hun duale gequantiseerde universeel omhullende algebra's. Aan de hand hiervan is de ontwikkelde methode toegepast om differentiaalcalculi te construeren op matrix quantumgroepen. Deze calculi zijn intrinsiek bicovariant. Verder onderzoek op dit gebied is momenteel in ontwikkeling.

Het Witten-vermoeden

Aandachtsprogramma	:	Algebraïsche krommen en Riemann-oppervlakken
Project	:	Algebraïsche krommen en mathematische fysica
Projectleider(s)	:	Prof. dr. R.H. Dijkgraaf
Projectmedewerker(s)	:	J.N.H.J. Cremers M.Sc.
Instelling	:	Universiteit van Amsterdam

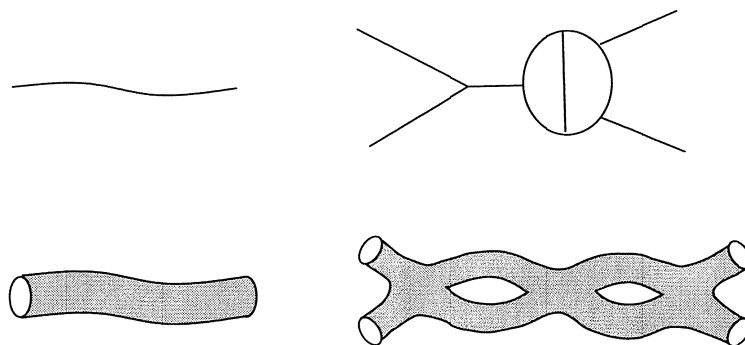
Snaren en Riemann-oppervlakken

Snaartheorie is een ambitieuze en controversiële poging een fundamentele theorie te formuleren van alle materie en krachten in de natuur. De belangrijkste hindernis die iedere serieuze kandidaat van zo'n 'theorie van alles' moet nemen is de zwaartekracht in overeenstemming te brengen met de wetten van de quantummechanica, iets waar snaren inderdaad wonderwel in slagen. De basisgedachte van snaartheorie is eenvoudig: elementaire deeltjes worden niet langer puntvormig verondersteld, maar zijn één-dimensionaal. Dit geeft een natuurlijke unificatie van alle deeltjes – er is maar één snaar en de verschillende oscillaties geven aanleiding tot een (oneindig) spectrum aan puntdeeltjes, waaronder in het bijzonder de deeltjes die op dit moment in de grote versnellers waarneembaar zijn. Dit simpele uitgangspunt doet echter geen recht aan de rijkdom en diepte van de theorie. Juist omdat we waarschijnlijk het correcte geometrische standpunt nog niet gevonden hebben, weten de snaren ons keer op keer te verrassen. Een van deze verrassingen wordt gevormd door de onverwacht sterke wiskundige uitspraken die men vanuit de snaartheorie kan doen in de (algebraïsche) meetkunde, in het bijzonder in de theorie van Riemann-oppervlakken en algebraïsche krommen.

De relatie met oppervlakken ligt voor de hand.

Een puntdeeltje dat zich voortbeweegt in de vier-dimensionale ruimte-tijd beschrijft een lijn. Als de deeltjes ook nog met elkaar in wisselwerking staan wordt deze 'wereldlijn' een graaf. De vertices beschrijven het uiteenvallen en recombineren van de deeltjes. Dit zijn de beroemde Feynman-diagrammen. In deze diagrammen kunnen trouwens ook gesloten lussen voorkomen. Dankzij Heisenberg's onzekerheidsrelaties kunnen namelijk spontaan paren deeltjes ontstaan die allerlei processen aangaan en uiteindelijk door annihilatie weer verdwijnen. Het aantal grafen dat dit soort processen beschrijft groeit exponentieel in het aantal lussen, hetgeen de analyse snel ondoorzichtig maakt.

Voor een snaar wordt het Feynman-diagram vervangen door een oppervlak. Een van de elegante eigenschappen van de snaartheorie is nu dat de interactie-vertex niet langer singulier is, maar eenvoudig wordt verkregen door de topologie van het oppervlak te veranderen (zie figuur 1). Dit heeft als consequentie dat snaren zich veel beter gedragen bij hoge energie en, in tegenstelling tot puntdeeltjes, wel de quantumeffecten van gravitatie kunnen doorstaan. De introductie van oppervlakken geeft ook een drastische reductie van de combinatoriek van de diagrammen. Voor een snaar met een vast aantal, zeg g lussen, is er maar één diagram – een oppervlak van genus g .



Figuur 1. De interacties van puntdeeltjes geven aanleiding tot Feynman-diagrammen; voor snaren worden dit Riemann-oppervlakken.

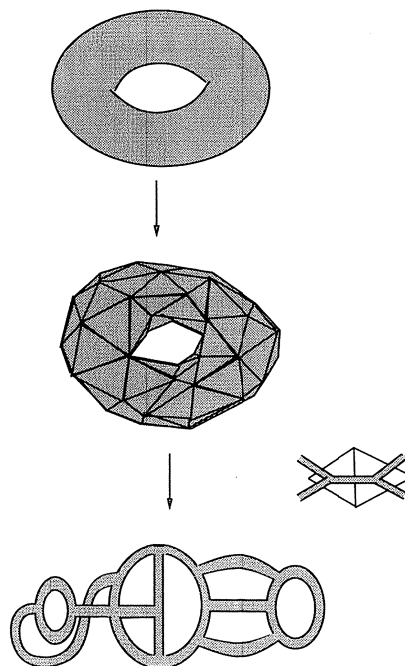
Wel moet er voor een gegeven topologie nog een gewicht berekend worden, de zogeheten amplitude, die de waarschijnlijkheid van het beschreven proces bepaalt. Het is in deze stap dat de relatie met de algebraïsche meetkunde tot stand komt. Het gewicht kan namelijk worden uitgedrukt door een integraal over de moduli-ruimte \mathcal{M}_g van inequivalente complexe structuren op het oppervlak. Deze moduli-ruimte, die terug gaat tot Riemann, kan ook gezien worden als de parametrisatie van alle (complexe) algebraïsche krommen en is één van de rijkste en gecompliceerdste objecten in de algebraïsche meetkunde. Zoals onder andere door David Mumford in de jaren 70 werd ingezien, wordt een interessant deel van de geometrie van \mathcal{M}_g gevangen in de intersectiegetallen van de zogeheten tautologische klassen. De traditionele berekeningswijze van deze getallen groeit echter met het geslacht g snel in complexiteit. Mumford zelf heeft de berekening voor $g = 2$ gedaan; het voorlopig hoogtepunt was de berekening door Carel Faber in zijn proefschrift (Amsterdam, 1988) voor $g = 3$.

Het Witten-vermoeden

In het najaar van 1989 werd echter een spectaculaire doorbraak gemaakt uit een onverwachte hoek. Voor het eerst slaagden snaartheoretici erin (in een bepaalde limiet) exacte amplitudes te berekenen. Dit deden ze niet door de gecompliceerde integralen over \mathcal{M}_g daadwerkelijk uit te voeren, maar door hun fysische neus te volgen en een discretisatie in te voeren. Het Riemann-oppervlak werd benaderd door steeds fijnere triangulaties. Door naar duale grafen te kijken kunnen deze triangulaties worden geherformuleerd in termen van random matrix-integralen (zie figuur 2). De basis voor deze correspondentie is gelegd door de bekende Nederlandse theoretisch fysisch Gerard 't Hooft. Deze bedacht in 1974 in zijn studie van ijkvelden dat een matrix-integraal een asymptotische ontwikkeling heeft in zogeheten 'lintgrafen', waar de één-dimensionale lijnstukken worden vervangen door twee-dimensionale stroken of linten. Zo'n lintgraaf kan in het algemeen niet getekend worden in een vlak, maar wel op een oppervlak van een bepaald geslacht g . Met behulp van deze matrix-integralen werd een elegante uitdrukking gevonden voor de snaaramplitudes. Ze gaven een oplossing van de bekende Korteweg-de Vries hiërarchie van integreerbare differentiaalvergelijkingen. Deze vergelijking, die in 1995 zijn honderdste geboortedag heeft gevierd, vond zijn oorsprong in de

beschrijving van soliton golf-oplossingen in ondiep water, maar is berucht voor zijn reputatie de meest uiteenlopende verschijnselen te beschrijven, zoals bijvoorbeeld het rondzwemmen van amoeben! Nu kunnen we hier dus ook de snaren aan toevoegen.

Kort na de oplossing van dit matrix-model verbaasde de snaartheoreticus Edward Witten van het *Institute for Advanced Study* te Princeton zowel de fysische als wiskundige wereld met zijn uitspraak dat deze snaaramplitudes precies overeenkwamen met de intersectiegetallen op de moduli-ruimte \mathcal{M}_g .



Figuur 2. Door middel van triangulaties kan de integraal over de moduli-ruimte \mathcal{M}_g van Riemann-oppervlakken benaderd worden door een som over de (duale) lintgrafen.

Deze intersectiegetallen voldoen dus ook aan de Korteweg-de Vries hiërarchie! Dit vermoeden kwam voor alle betrokkenen als een donderslag bij heldere hemel en is eigenlijk nog steeds niet echt goed begrepen. Wel werd snel duidelijk dat het zeer waarschijnlijk waar was. Eén van de belangrijke ingrediënten in de fysische intuïtie is dat deze integreerbare structuur pas duidelijk wordt als alle oppervlakken van alle geslachten te samen worden beschouwd. Het uiteindelijke bewijs van het Witten-vermoeden werd een jaar later gevonden door de jonge briljante Russische wiskundige Maxim Kontsevich. Zijn aanpak is geheel anders dan die van de fysici, hoewel ook op fysische intuïtie gebaseerd.

Op naar hogere dimensies

Wat zijn nu concrete probleemstellingen rond het Witten-vermoeden waar in het SMC-project aandacht aan wordt besteed? Allereerst is het belangrijk dat Wittens vermoeden betrekking heeft op een compactificatie van \mathcal{M}_g . De oorspronkelijke moduli-ruimte is niet compact, omdat oppervlakken kunnen degenereren. Door speciale singuliere oppervlakken toe te voegen, verkrijgen we de zogeheten Deligne-Mumford compactificatie. Een van de open vragen is in hoeverre de oplossing van Witten ook uitspraken doet over de intersectie-ring van \mathcal{M}_g zelf. Er is hier een precies vermoeden van Faber, dat zegt dat er wederom een eenvoudige uitdrukking bestaat. Met behulp van de correspondenties met de matrixmodellen wordt dit vermoeden verder onderzocht.

Een tweede, meer algemene vraagstelling die in het SMC-project bestudeerd wordt, is de uitbreiding van het Witten-vermoeden naar Riemann-oppervlakken tezamen met een afbeelding in een andere variëteit X . Vanuit de snaartheorie is dit een natuurlijke stap; deze situatie beschrijft immers een snaar die zich voortbeweegt in de 'ruimte-tijd' X . Het Witten-vermoeden betreft dan het gedegeneerde geval $X = \text{punt}$. Ook in het meer algemene geval is er een moduli-ruimte van zogeheten stabiele afbeeldingen te definiëren met bijbehorende tautologische klassen en er kunnen weer intersectiegetallen berekend worden. Men spreekt in dit geval van de Gromov-Witten invarianten.

Kunnen de snaren ons hier weer helpen? Het is waarschijnlijk te veel gevraagd om voor een willekeurige ruimte een exacte oplossing met de elegantie van de Korteweg-de Vries vergelijking te vinden, hoewel we hebben kunnen aantonen dat er altijd een integreerbare structuur aanwezig is. Toch zijn er weer verrassende uitspraken te doen vanuit een fysisch perspectief. Hiertoe moeten we terug naar de

oorsprong van de snaartheorie als een 'theorie van alles'.

Er zijn twee aspecten van snaartheorie die deeltjesfysici in verlegenheid brengen. Allereerst kunnen snaren alleen consistent worden gedefinieerd in een ruimte-tijd van dimensie tien in plaats van vier. Daartoe moet verondersteld worden dat deze tien-dimensionale variëteit lokaal van de vorm $\mathbb{R}^4 \times X$ is, met X (de compactificatie-ruimte) een compacte zes-dimensionale variëteit. De vraag is natuurlijk welke ruimte X daarvoor in aanmerking komt. Er zijn allerlei fysische argumenten dat X een zogeheten Calabi-Yau ruimte moet zijn (compact, Kähler, met triviale canonieke bundel). Helaas zijn daar op dit moment zo'n 10.000 families van bekend. Een tweede problematisch aspect is dat er in principe vijf verschillende types snaartheorieën bestaan, o.a. onderscheiden doordat we de oppervlakken open of gesloten, oriënteerbaar of niet-oriënteerbaar kiezen.

Deze verscheidenheid in types en compactificaties kunnen elkaar echter in zekere zin 'opheffen'. De afgelopen jaren zijn er namelijk aanwijzingen dat er sterke equivalenties zijn. Zo'n equivalentie heeft de algemene vorm: 'type A op variëteit $X \cong$ type B op variëteit Y '. Daarmee is het mogelijk vermoedens uit te spreken over de Gromov-Witten invarianten op X in termen van de geometrie van Y en vice versa. Dit verschijnsel staat bekend als 'spiegelsymmetrie' of meer algemeen 'snaardualiteit'. In het kader van het SMC-project wordt deze benadering verder bestudeerd. In het simpelste geval, van tori, hebben we laten zien dat dit inderdaad tot een volledige oplossing leidt.

Samengevat kunnen we stellen dat de inbreng van snaartheorie binnen de theorie van Riemann-oppervlakken tot vele verrassende inzichten heeft geleid. Zeker gezien het hoge tempo van de ontwikkelingen in de fysica zijn de verwachtingen voor de toekomst hooggespannen.

Percolatie

Aandachtsprogramma	: Rekenintensieve methoden in de stochastiek
Project	: Stochastische modellen in natuur en techniek
Projectleider(s)	: Dr. J. van den Berg, prof. dr. M.S. Keane
Projectmedewerker(s)	: Drs. A. Ermakov
Instelling	: CWI

Inleiding

Wiskundige percolatiemodellen werden aan het eind van de jaren vijftig ingevoerd door Hammersley en Welsh. Zij wilden inzicht krijgen in de globale verbindingsstructuur van poreuze media. (De directe motivatie voor hun onderzoek hield verband met gasmaskers voor gebruik in steenkolenmijnen.) Spoedig bleken hun modellen van belang voor de beschrijving van een veel grotere klasse ‘coöperatieve’ verschijnselen, zoals epidemieën, bosbranden, spontane magnetisatie, polymerisatie en de betrouwbaarheid van grote, gestructureerde (communicatie) netwerken.

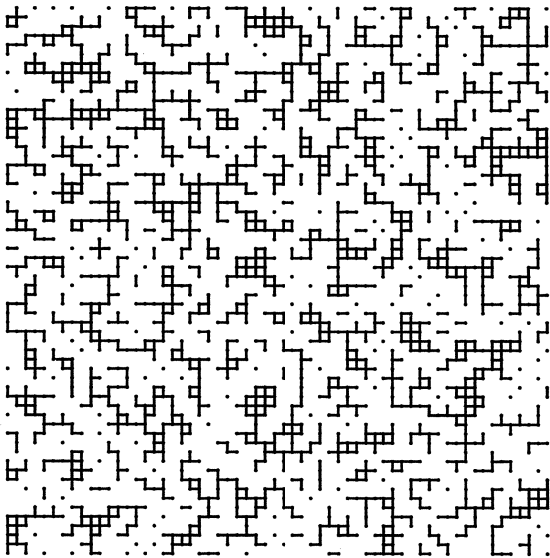
De eenvoudigste mathematische modellen zijn als volgt. Beschouw een regelmatig rooster, bijvoorbeeld het 2-dimensionale kwadratisch rooster of het 3-dimensionale kubisch rooster. Stel nu dat elk roosterpunt, onafhankelijk van de andere, met zekere kans p open en kans $1 - p$ gesloten is. We zeggen dat twee punten v en w tot hetzelfde open cluster behoren, als er een roosterpad van v naar w bestaat waarop elk punt open is. Hammersley en Welsh toonden aan dat dit model kritisch gedrag vertoont: er bestaat een kritieke waarde p_c (waarvan de waarde afhankelijk is van het rooster) ongelijk aan 0 of 1, zó dat voor alle $p < p_c$ met kans 1 alleen eindige clusters voorkomen, en voor alle $p > p_c$ met kans 1 een oneindig open cluster bestaat. De kans dat een gegeven punt behoort tot een oneindig open cluster wordt meestal aangegeven als $\theta(p)$. Dus voor $p < p_c$ is $\theta(p) = 0$, maar voor $p > p_c$ is $\theta(p) > 0$.

In de context van poreuze media stellen de open punten lokale gaten in het materiaal voor. Als we veronderstellen dat gaten die bij buurpunten behoren met elkaar in verbinding staan, dan betekent het bovenstaande dat als $p < p_c$ het materiaal niet, maar als $p > p_c$ wel poreus is. In de context van epidemieën corresponderen de open punten met leden van

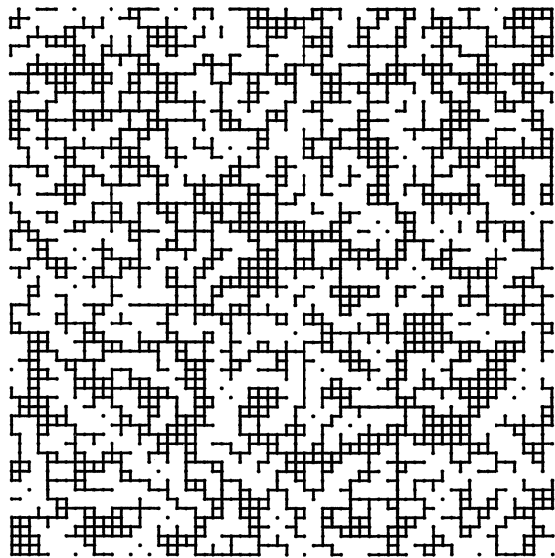
een populatie die vatbaar zijn voor een bepaalde besmettelijke ziekte. Als we aannemen dat elk ziek individu al zijn vatbare buuren infecteert, en er aanvankelijk slechts 1 ziek individu is, dan zal er voor $p < p_c$ geen epidemie optreden (want de infectie beperkt zich tot de bij het aanvankelijk zieke punt behorende open cluster), terwijl er voor $p > p_c$ met kans $\theta(p) > 0$ wel een epidemie optreedt. In het geval van magnetisatie stellen de open punten elementaire magneetjes voor. Stel nu dat elk elementair magneetje zich op twee manieren kan richten en dat binnen een cluster alle magneetjes dezelfde richting hebben terwijl verschillende clusters zich niets van elkaar aantrekken. Dan zullen voor $p < p_c$ de clusters elkaar min of meer neutraliseren, maar voor $p > p_c$ is er sprake van collectief gedrag op grote schaal en hebben we ‘spontane magnetisatie’. Op analoge wijze kan een beschrijving gegeven worden voor polymerisatie, bosbranden en betrouwbaarheid van zeer grote netwerken.

Het bovenbeschreven wiskundige model wordt ‘puntpercolatie’ genoemd. Als niet de punten maar de kanten (de verbindingslijnen tussen buurpunten) open of gesloten zijn, spreken we van lijnpercolatie. Bij lijnpercolatie kunnen we soortgelijke interpretaties in termen van epidemieën etc. geven als voor puntpercolatie. Zo zal een ziek individu nu alle buuren besmetten met wie het een open kant gemeen heeft.

Deze modellen geven natuurlijk een zeer vereenvoudigde en geïdealiseerde weergave van de werkelijkheid. Toch zijn ook (of zelfs juist) deze eenvoudige modellen om allerlei redenen van belang: ze blijken een goed kwalitatief inzicht te geven; bovendien lijken allerlei grootheden (zoals de zogenaamde kritieke exponent β , die het gedrag van $\theta(p)$ voor p groter dan, maar zeer dicht bij p_c beschrijft) ongeveer te zijn voor allerlei details van het model,



$p = 0.52$



$p = 0.66$

Figuur 1. Puntpercolatie op het kwadratisch rooster. Typische realisaties op een 60×60 vierkant voor $p = 0.52$ (subkritisch) en $p = 0.66$ (superkritisch). De open punten en de kanten tussen open buurpunten zijn weergegeven. Merk op dat in de eerste afbeelding de eindige clusters 'lokaal' zijn; er is geen open pad tussen tegenoverliggende zijden van het vierkant. In het tweede geval zijn er diverse verbindingen tussen de tegenoverliggende zijden.

hetgeen overigens nog lang niet goed begrepen wordt; bij het bestuderen van de eenvoudigste modellen zijn technieken ontwikkeld die, met enige aanpassing, ook voor realistischer modellen bruikbaar zijn; ten slotte kunnen de eenvoudige modellen dienen om, van allerlei grootheden, onder- of bovengrenzen te vinden voor meer gecompliceerde modellen.

Ontwikkelingen

Na de eerste publikaties rond 1960 was de vooruitgang in het vakgebied tot het eind van de jaren zeventig beperkt. Vervolgens vonden er, door Russo, door Seymour en Welsh, en met name door Kesten een aantal doorbraken plaats, die tot enorme activiteit leidden. Inmiddels zijn de belangrijkste vragen voor het subkritische gebied ($p < p_c$) en het superkritische gebied ($p > p_c$) opgelost. Zo is bewezen dat voor $p < p_c$ de kans dat de bij een gegeven punt behorende open cluster groter is dan n , exponentieel begrensd is als functie van n . Daarom gaat de kans op een open pad tussen twee tegenoverliggende zijden van een doos (vierkant of (hyper-)kubus) naar 0 als de afmeting van de doos naar oneindig gaat.

In het superkritische geval is er juist een grote rijkdom aan verbindingen tussen tegenoverliggende zijden van een grote doos (zie figuur 1). Deze rijkdom blijkt voldoende te zijn om op macroscopische schaal transport (elektrische geleiding, diffusie) plaats te doen vinden. De functie $\theta(p)$ is, voor $p > p_c$ oneindig vaak differentieerbaar. Over het gedrag in of zeer dicht bij het kritieke punt bestaan veel vermoedens maar wordt nog weinig echt begrepen, behalve (enigszins merkwaardig) in hoge dimensies. Een van de belangrijke vermoedens is dat, voor p dicht bij p_c , $\theta(p)$ zich ruwweg gedraagt als $(p - p_c)^\beta$, waar β een rationaal getal tussen 0 en 1 is. Bovendien denkt men dat β in essentie alleen van de dimensie afhangt (dus, bijvoorbeeld, voor het kwadratisch rooster en het driehoeksrooster precies gelijk is). Tot nu toe zijn alleen ondergrenzen van deze vorm aangetoond met exponenten die vrij ver van de veronderstelde juiste waarde van β liggen. Voor het 3-dimensionale geval is zelfs nog niet bewezen dat $\theta(p_c) = 0$. Een bewijs hiervan zou opnieuw een belangrijke doorbraak betekenen, maar er zijn nog geen aanwijzingen dat dit op korte termijn zal gebeuren.

Een onderwerp dat tijdens de gehele geschie-

denis van de percolatietheorie aandacht heeft gekregen is het berekenen of afschatten van p_c voor verschillende roosters. Voor lijnpercolatie op het kwadratisch rooster is p_c precies $1/2$. (Het bewijs hiervan, door Kesten in 1980, was één van de eerder genoemde doorbraken.) Ook de kritieke waarschijnlijkheden voor puntpercolatie op het driehoeksrooster, lijnpercolatie op het driehoeksrooster en lijnpercolatie op het zeshoekig rooster, zijn exact bekend, namelijk respectievelijk $1/2$, $2 \sin(\pi/18)$ en $1 - 2 \sin(\pi/18)$. Echter, de kritieke waarde voor puntpercolatie op het kwadratisch rooster (dat we voortaan met S , van *square lattice*, aanduiden) is niet exact bekend, en niemand gelooft nog dat het een ‘mooi’ getal is. Monte Carlo simulatie suggereert dat deze kritieke waarde, die we voortaan $p_c(S)$ noemen, ongeveer 0.593 is. Ons onderzoek heeft zich onder andere beziggehouden met het vinden van ondergrenzen voor $p_c(S)$. De beste ondergrens in 1960 was $p_c(S) \geq 1/2$. Pas rond 1980 werd bewezen dat $1/2$ ook een *strikte* ondergrens is. Daarna werden diverse verbeteringen gevonden met als beste resultaat de ondergrens 0.541 van Menshikov en Pelikh (1989). Door een verbetering van hun methode verkregen wij de ondergrens 0.556 zoals we hieronder zullen beschrijven.

Resultaten van het project

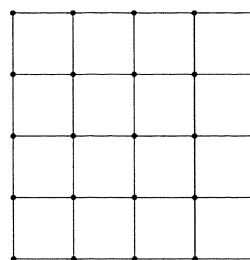
Ondergrens voor kritieke waarschijnlijkheid

Laat, zoals boven afgesproken, S het kwadratisch rooster zijn en $p_c(S)$ de kritieke waarde voor puntpercolatie op dat rooster. Laat nu S^* het rooster zijn dat door S wordt verkregen door de diagonaal verbindingen toe te voegen (zodat op S^* elk punt acht burens heeft). Onder S^* -percolatie zullen we verstaan de aanwezigheid van een oneindig *gesloten* cluster voor S^* . Al sinds begin jaren zestig is bekend dat als er S^* -percolatie is, dan zijn er (met kans 1) willekeurig grote circuits (in S^*) van gesloten punten rond de oorsprong. Dus dan kan er geen oneindig open cluster op S zijn. Met andere woorden, als $1 - p > p_c(S^*)$, dan $p \leq p_c(S)$, ofwel:

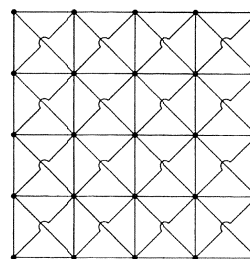
Lemma:

$$p_c(S) + p_c(S^*) \geq 1.$$

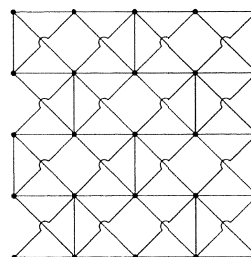
Sinds begin jaren tachtig is bekend dat er zelfs sprake is van een *gelijkheid*, maar dat speelt geen rol bij deze methode.



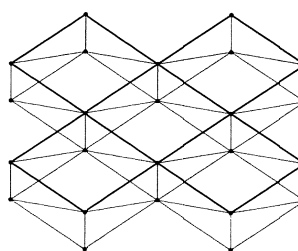
a.



b.



c.



d.

Figuur 2. a. – Het rooster S
b. – Het rooster S^*
c. en d. – Twee ruimtelijke representaties van het rooster L

Een belangrijk element in de methode van Menshikov en Pelikh is dat als men een deel van de kanten van S^* weglaat, men een graaf L verkrijgt die ruimtelijk gerepresenteerd kan worden als twee lagen van S met dwarsverbindingen tussen die lagen (zie figuur 2). Hierdoor kan men, op natuurlijke wijze, percolatie op L vergelijken met percolatie op S . Men kan namelijk de open cluster van een punt van L stap voor stap ‘opbouwen’ door steeds één of meer verticale paren van punten (die grenzen aan de cluster voor zover die op dat moment is gegenereerd) te ‘inspecteren’ en door een toevalsmechanisme te beslissen of ze aan de cluster moeten worden toegevoegd. Als men nu goede ondergrenzen heeft voor de conditionele kansen (gegeven het groeiproces tot dat moment) dat bepaalde paren inderdaad worden toegevoegd, dan leidt dit, na toepassing van het bovenstaande lemma, tot een ondergrens van $p_c(S)$. Het is dus belangrijk dit groeiproces zo verstandig mogelijk te organiseren en de conditionele kansen slim af te schatten. Op deze punten hebben wij een significante verbetering van de methode aangebracht, hetgeen leidde tot een beduidend betere ondergrens van $p_c(S)$. Het resultaat zal gepubliceerd worden in het tijdschrift *Random Structures and Algorithms*.

Percolatie en cellulaire automaten

Meer recent hebben we percolatie-ideeën toegepast op de volgende cellulaire automaat. Stel op tijdstip 0 heeft elk punt van het kwadratisch rooster een niet-negatieve waarde, zijn *gewicht*. We nemen aan dat deze begin-gewichten onafhankelijk en uniform verdeeld tussen 0 en 1 zijn. De tijd is discreet en op elk tijdstip inspecteert elk punt de gewichten in zijn omgeving (zichzelf en zijn vier burens) en stuurt vervolgens zijn gewicht naar degene met het grootste gewicht. Dit gebeurt door alle punten simultaan. Vervolgens is het nieuwe gewicht van een punt gelijk aan de som van de inkomende gewichten.

Dit model werd rond 1990 ingevoerd door Coffman, Courtois, Gilbert en Piret. Zonder bewijs sug-

gereren zij dat (met kans 1) elk punt slechts eindig vaak van waarde verandert. Dit probleem werd in het verleden aan de orde gesteld door Van den Berg en Meester, die met symmetrie en ergodiciteitsargumenten een aantal stabiliteitseigenschappen voor dit model bewezen. Het bovenstaande probleem bleef echter open.

Dit probleem hebben wij nu benaderd met percolatie-achtige argumenten. Het is duidelijk dat als een punt eenmaal waarde 0 heeft, dan blijft het 0. Verder, als er rond een eindig gebied een circuit van punten met waarde 0 is, dan zal dit gebied zich geïsoleerd van de rest ontwikkelen en is het eenvoudig in te zien dat de waarden in zo’n gebied inderdaad slechts eindig vaak veranderen. Het is dus voldoende aan te tonen dat er op tijdstip 1 alleen *eindige* clusters van punten met gewicht ongelijk 0 bestaan (met andere woorden: dat op tijdstip 1 de bezette punten niet percoleren). Met behulp van tamelijk bekende ideeën uit de percolatietheorie hebben we dit teruggebracht tot het volgende probleem: stel dat voor zekere waarde van n geldt dat de kans dat er in een $n \times 3n$ rechthoek een pad van bezette punten bestaat tussen de lange zijden van de rechthoek, kleiner is dan $1/36$. Dan is het antwoord op het oorspronkelijke probleem positief. (Bovendien volgt dan dat als we niet het proces op het volledige rooster beschouwen, maar op een $m \times m$ torus, de verwachte tijd waarna geen enkel punt meer van waarde verandert, hoogstens van orde $\log m$ is.) Dit nieuwe probleem is, bij gegeven n , een *eindig* probleem, in de zin dat het in principe opgelost kan worden door een eindig aantal gevallen te bekijken. Dit aantal is reeds voor betrekkelijk kleine n echter zo groot dat dit zelfs voor de snelste computers niet in een aanvaardbare tijd gedaan kan worden. Daarom hebben we onze toevlucht genomen tot een Monte Carlo studie van dit eindige probleem, die overtuigend aangaf dat bovenstaande kans reeds voor $n = 8$ kleiner is dan $1/36$. Een korte publikatie hierover is in voorbereiding.

Numerieke bifurcatie-analyse

Aandachtsprogramma	:	Wiskundige aspecten van niet-lineaire systemen
Project	:	Ontwikkeling van programmatuur van numerieke bifurcatie-analyse
Projectleider(s)	:	Dr. J. Sanders
Projectmedewerker(s)	:	Dr. Y. Kuznetsov, dr. V. Levitin
Instelling	:	CWI

Wat is numerieke bifurcatie-analyse?

In dynamische systemen (en hieronder rekenen we voorlopig afbeeldingen en gewone differentiaalvergelijkingen, maar men kan ook aan partiële differentiaalvergelijkingen denken), is men geïnteresseerd in bijzondere oplossingen die als het ware het geraamte vormen van het systeem. Denk aan evenwichtspunten, periodieke oplossingen, maar ook homo- en heterokliene zadelpuntverbindingen en invariante tori. Bifurcatie-analyse houdt zich bezig met het onderzoek naar het ontstaan van dergelijke bijzondere oplossingen. Een gedeelte van dit werk kan puur analytisch gedaan worden in veel problemen. Het bepalen van evenwichtspunten geeft gewone vergelijkingen die in modelsituaties veelal expliciet oplosbaar zijn. Bij het bepalen van periodieke oplossingen in de buurt van evenwichtspunten kan men gebruik maken van normaalvormberekeningen om expliciete benaderingen te vinden van deze oplossingen. Maar wanneer men wil gaan rekenen in de omgeving van een periodieke oplossing die niet meer in de buurt van een evenwichtspunt ligt, dan wordt het al moeilijk om analytisch resultaten te vinden. De enige mogelijkheid die dan nog rest is numerieke analyse. In de loop der jaren zijn binnen het kader van de numerieke wiskunde vele algoritmen ontwikkeld om differentiaalvergelijkingen efficiënt op te lossen, en om grote lineaire algebra problemen, die een rol spelen bij het ontstaan van bijzondere oplossingen, te analyseren. Het project *Ontwikkeling van programmatuur voor numerieke bifurcatie-analyse* beoogt een werkplaats te creëren waarbinnen deze gereedschappen in een grafische omgeving gebruikt kunnen worden. De gebruiker van deze werkplaats kan iemand zijn die alleen interesse heeft voor een specifiek dynamisch systeem, maar ook iemand wiens interesse juist ligt in het ontwikkelen van nog meer en verfijnder gereedschap. De eerste gebruiker hoeft alleen zijn systeem in te voeren en dient daarna meteen aan de slag te kunnen door zijn keuze uit menu's te ma-

ken. De tweede gebruiker zal dieper het systeem in moeten duiken en zich bezig moeten houden met de vraag hoe zijn algoritmen inpasbaar zijn in het gegeven kader.

Ontwikkelingen in de laatste 10 jaar

De gedachte om een dergelijke werkplaats te maken is niet nieuw en in feite gaat het dan ook om een opzet die tracht het beste over te nemen van de voorgangers, waarvan AUTO en *Locbif* de bekendste zijn. Van het pakket AUTO van Eusebius Doedel bestaan verschillende versies met diverse grafische mogelijkheden. Het pakket beschikt over uitstekende numerieke faciliteiten en is met name zeer goed in het vinden en continueren van periodieke oplossingen. Nadelen zijn het gebrek aan interactieve mogelijkheden en de merk-gebondenheid. *Locbif*, gemaakt door een Russisch team waar V. Levitin en Yu. Kuznetsov deel van uitmaakten, onderscheidt zich door het grote aantal bifurcaties dat is ingebouwd, maar beperkt zich voornamelijk tot evenwichtspunten en ook het aantal dimensies is begrensd. *Locbif* draait alleen op PC's.

Inhoud van het SMC-project

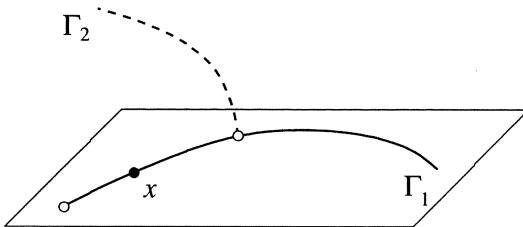
De doelstelling van het project is een interactieve grafische werkomgeving te maken voor bifurcatie-analyse en continueringsmethoden die niet beperkt is tot een enkel platform. Als secundaire doelstelling is aangehouden dat het systeem zo veel mogelijk uitbreidbaar moet zijn door anderen. Meer in het bijzonder zijn er de volgende eisen.

- Wiskundige vereisten.
 - Simulatie (generatie van banen).
 - Continuering van evenwichtspunten, periodieke en homokliene banen.
 - Detectie van bifurcaties, normaalvormberekening en over kunnen gaan op andere takken.

- Programmatuur vereisten.
 - Gebruikersvriendelijk.
 - Uitbreidbaar, zowel met nieuwe dynamische systemen als met numerieke algoritmen.
 - Portabiliteit naar Unix en Windows.
 - Archivering van resultaten.
 - Help systeem.

Het programma draagt als naam CONTENT. CONTENT kent de volgende basisbegrippen.

- Vergelijkingen. Dit zijn de formules (of programma's) waarmee het systeem omschreven wordt.
- Krommen (zie figuur 1). Dit zijn berekende stukken van het bifurcatiediagram. Er zijn verschillende typen krommen, die allen bepaalde routines hebben om ze op te starten en te continueren, test functies om nieuwe bifurcaties te vinden en technische gegevens om er mee te kunnen werken.



Figuur 1. Krommen

Gedurende een werksessie worden systemen geïnitieerd of gewijzigd. Het aanmaken en compileren van de programma's wordt geheel automatisch gedaan.

Er is een archief manager waarin de resultaten van één of meer sessies bewaard kunnen worden.

De interactie met de gebruiker vindt plaats via windows en menu's. Op deze wijze kan de gebruiker berekeningen starten en onderbreken. Via verschillende windows kan de gebruiker alle instellingen

wijzigen, zowel wat betreft de visualisatie als de numerieke aspecten. Uiteraard kan men de berekende krommen op diverse wijzen plotten.

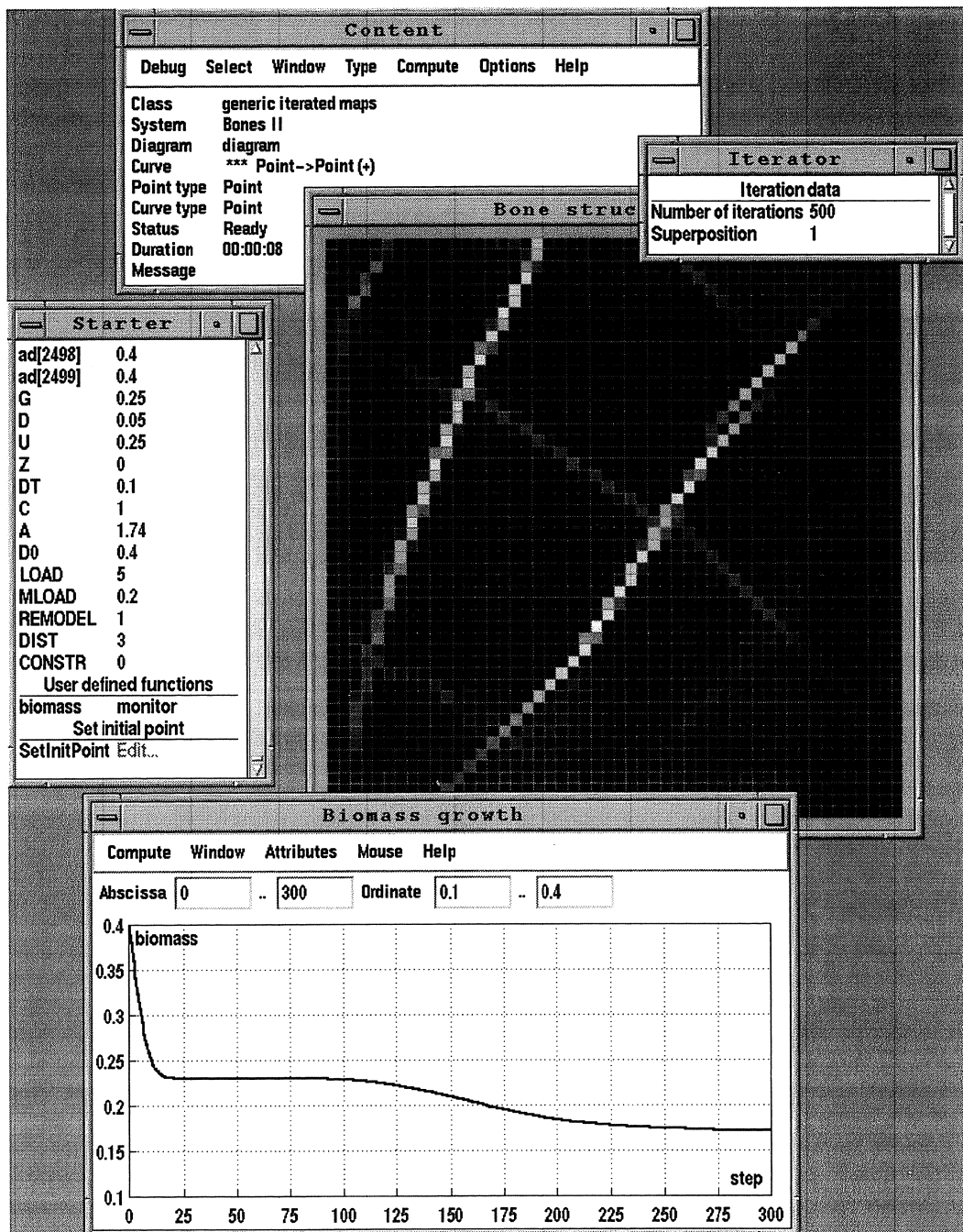
Het systeem is zo opgezet dat er zo weinig mogelijk begrenzingen zijn ingebouwd. Dat wil natuurlijk niet zeggen dat alles ook meteen kan, met sommige problemen zal men moeten wachten op krachtiger hardware. Maar experimenten met honderden variabelen zijn succesvol verlopen. Er is echter nog geen voorziening getroffen de resultaten van dergelijke grote systemen te visualiseren.

Het Dynamisch Systeem Laboratorium

Het Dynamisch Systeem Laboratorium (DSL) is opgericht met als doel behulpzaam te zijn bij de verspreiding van kennis over dynamische systemen en met name over de software die de onderzoeker vandaag de dag ter beschikking staat. Behalve de ontwikkeling van een eigen pakket CONTENT beschikt het DSL ook over andere programma's. Deze collectie wordt aangevuld indien hieraan behoefte blijkt te bestaan bij gebruikers.

Voorbeeld: een model voor botgroei

Als illustratie van zowel de rol van het DSL als de mogelijkheden van CONTENT noemen we de samenwerking met Dr. H. Weinans, Institute of Orthopaedics, Section Biomechanics, Katholieke Universiteit Nijmegen. Het betreft hier een project waarin de onderzoekers reeds hun eigen simulatie software (voor een model van botgroei) geschreven hadden en programma's om hun resultaten te plotten. Wat ontbrak was een continueringskader om systematisch de bifurcaties te kunnen analyseren. Door een niet al te grote aanpassing aan de eigen software was het mogelijk alles aan CONTENT te koppelen (zie figuur 2). Naar aanleiding hiervan is vervolgens besloten de implementatie van afbeeldingen in CONTENT versneld uit te voeren.



Figur 2. CONTENT output

Overzicht van lopende projecten

Werkgemeenschap Numerieke Wiskunde

Reken- en communicatiecomplexiteit voor preconditioneringsmethoden (prof. dr. A.O.H. Axelsson, KU Nijmegen)

Voor elliptische problemen zijn recentelijk nieuwe preconditioneringsmethoden ontwikkeld van optimale rekencomplexiteit. Maar, zelfs als de hoeveelheid rekenwerk per roosterpunt in essentie vast ligt, onafhankelijk van de fijnheid van het rooster, kan de echte hoeveelheid rekenwerk groot zijn en andere, niet-optimale methoden kunnen efficiënter zijn voor de probleemafmetingen die men in de praktijk tegenkomt. Het doel is het vinden van de echte rekencomplexiteit van verschillende iteratieve oplossingsmethoden door bepaling van nauwkeurige eigenwaardebenaderingen voor de gepreconditioneerde geconjugeerde gradiëntenmethoden gebruikmakend van verschillende types van preconditioneringen en meerdere (gegeneraliseerde) geconjugeerde gradiëntenmethoden. Dit zal ook gedaan worden voor bepaalde niet-symmetrische en indefiniëte matrixproblemen. Het doel is ook dezelfde soort problemen te behandelen wat betreft reken- en communicatiecomplexiteit voor enkele typische parallelle computerarchitecturen.

Invariante discretiserings- en oplossingsmethoden voor de behoudswetten voor incompressibele stromingen (prof. dr. ir. P. Wesseling, TU Delft)

Het doel van het project is het ontwikkelen en vergelijken van methoden voor de invariante discretisatie van de behoudswetten voor incompressibele stromingen in algemene coördinaten, en van corresponderende numerieke oplossingsmethoden. Ontwikkeling en evaluatie van numerieke methoden voor de incompressibele Navier-Stokes vergelijkingen in algemene coördinaten met turbulentie-modellering. Toepassing op een realistisch geval.

Globale tijd-ruimte discretisatiemethoden (prof. dr. A.O.H. Axelsson, KU Nijmegen)

Het gebruik van globale tijd-ruimte eindige elementmethoden voor parabolische en gekoppelde parabolische/hyperbolische differentiaalvergelijkingen hebben veel voordelen boven gewone tijdstapmethoden. Ze kunnen onder andere stabiele methoden opleveren ook voor problemen, waar de gewone

methode instabiel is en vaak maken ze gebruik van een aantal roosterpunten dat een orde van grootte kleiner is.

De methode is toepasbaar op voorwaarts-achterwaartse warmtevergelijkingen, op bepaalde optimale controle (besturings)problemen die onder andere ontstaan bij numerieke weersvoorspelling, en voor beginrandwaardeproblemen met niet-lokale randvoorwaarden.

De niet-symmetrische stelsels die ontstaan kunnen opgelost worden met bepaalde iteratieve methoden, gebaseerd op gegeneraliseerde geconjugeerde gradiëntenmethode en algebraïsche multiroostermethoden als preconditioneringen.

Doel van het onderzoek is stabiliteit en discretisatiefoutschattingen te analyseren en te laten zien dat de methoden optimale (of bijna optimale) complexiteit hebben.

Werkgemeenschap Stochastiek

Statistiek van extreme waarden (\mathbb{R}^d) (prof. dr. L.F.M. de Haan, Erasmus Universiteit Rotterdam)
Onderzoek van statistische problemen samenhangend met uiteinden van een meer-dimensionale kansverdeling.

Statistiek voor grote parameterruimten. Deelproject: functionele en structurele modellen (prof. dr. C.A.J. Klaassen, Universiteit van Amsterdam)

In statistische modellen met grote parameterruimten spelen mengmodellen een belangrijke rol. Daarbij zijn de storingsparameters in de verdelingen van de waarnemingen realisaties van onafhankelijke en identiek verdeelde (iid) stochasten onder een mengverdeling. Dit structurele model (met iid waarnemingen) heeft andere eigenschappen dan het functionele model waarin de (onbekende) storingsparameters deterministisch zijn en de waarnemingen onafhankelijk maar niet identiek verdeeld. In het voorgestelde project zal een vergelijking van deze modellen worden gemaakt en zullen efficiënte grenzen en schatters worden geconstrueerd voor het functionele model.

Analyse van tijdreeksen met een zware staart (dr. T. Mikosch, RU Groningen)

Tijdreeksen vertonen vaak vreemde uitschieters en wilde schommelingen. Soms worden die veroor-

zaakt door meetfouten, maar vaak is er sprake van iets intrinsieks dat niet tot uitdrukking wordt gebracht door de klassieke theorie (o.a. op normaliteit gebaseerd). Door Davies en Resnick is baanbrekend werk verricht om die klassieke theorie te vervangen door iets beters. Het is de bedoeling dat het onderzoek zich richt op modelconstructie en parameterschatting als oneindige varianties optreden in ARMA-processen. Asymptotische theorie zal hierbij een belangrijke rol spelen.

Werkgemeenschap Mathematische Besliskunde en Systeemtheorie

Het machtreeksalgoritme voor de analyse van wachtrijproblemen (dr. J.P.C. Blanc, KU Brabant)
Theoretische rechtvaardiging van het machtreeksalgoritme, verbetering van dit algoritme en uitbreiding van de toepasbaarheid ervan. Numerieke analyse van diverse wachtrijmodellen met behulp van dit algoritme.

*Inwendige-punt-methoden voor lineair, geheeltal-
lig lineair en niet-lineair programmeren* (dr. ir. C. Roos, TU Delft)

Voortzetting van het onderzoek aan recent ontwikkelde inwendige-punt-methoden voor lineair programmeren en uitbreidingen naar niet-lineaire optimalisering. Met name de mogelijkheid om deze methoden toe te passen op geheeltallige optimaliseringsproblemen zal worden onderzocht. Implementaties van de methoden zullen worden getest op hun praktische effectiviteit.

Machinevolgordeproblemen en samenwerking (prof. dr. S.H. Tijs, KU Brabant en dr. J.A.M. Potters, KU Nijmegen)

Het project beoogt kostentoewijzingsmechanismen te ontwerpen voor machinevolgordeproblemen. Deze mechanismen dienen onder alle omstandigheden een eerlijke verdeling van kosten te bewerkstelligen die zo mogelijk eenvoudig te berekenen is. Het is de opzet de eigenschappen van dergelijke regels te bestuderen en axiomatisch te karakteriseren. De wijze van benadering zal ontleend zijn aan de coöperatieve speltheorie, een theorie die al vaker met succes is toegepast bij kostentoewijzingsproblemen.

Anticiperende en adaptieve planning met neurale netwerken (prof. dr. J. Wessels en prof. dr. E.H.L. Aarts, TU Eindhoven)

Nagaan in hoeverre neurale netwerken bruikbaar zijn voor het ontwikkelen van planningen in situa-

ties waarin het herkennen van patronen in de externe vraag van belang is, terwijl bovendien de patronen in de tijd variëren. Hierbij wordt in de eerste plaats gedacht aan productieplanningsproblemen. Tevens is het de bedoeling om ontwerpmethoden voor neurale netwerken met bovengenoemd doel te ontwikkelen.

Werkgemeenschap Discrete Wiskunde

Algebraïsch-meetkundige codes (dr. G.R. Pellikaan, TU Eindhoven)

Het onderzoek richt zich op:

- Het decoderen van algebraïsch-meetkundige codes.
- Het bepalen van grenzen van de minimum-afstand en dimensie van algebraïsch-meetkundige codes.
- Het vinden van MDS-codes op krommen.
- Berekeningen in de Jacobiaan van de kromme spelen een centrale rol in alle drie de onderdelen.

Codes in klassieke afstandsreguliere grafen en polynomiale ruimten

(prof. dr. A.E. Brouwer, TU Eindhoven)

Onderzoek van codes en designs in associatieschema's en aanverwante structuren, speciaal in het eindige geval.

Ternaire codes en hun designs (prof. dr. J.H. van Lint, TU Eindhoven)

Onderzoek naar de minimum-afstand van ternaire codes, in het bijzonder optimale codes en de constructie van nieuwe t -designs.

Werkgemeenschap Analyse

De analyse van partiële differentiaalvergelijkingen uit de theorie der supergeleiding (dr. B.H. Gilting en prof. dr. ir. P.J. Zandbergen, Universiteit Twente)

Supergeleiding wordt gemodelleerd door een aantal (stelsels van) partiële differentiaalvergelijkingen. Tot nu toe is er echter weinig theorie voor deze vergelijkingen ontwikkeld. Dit onderzoek bestudeert existentie en eenduidigheid voor geschikte randvoorwaardeproblemen en het karakteriseren van vrije randen in de oplossingen en verwante kwalitatieve eigenschappen van de oplossingen.

Berekenen en visualiseren van invariante variëteiten in dynamische systemen (dr. G. Vegter, prof. dr.

H.W. Broer en prof. dr. F. Takens, RU Groningen)

Doel is te komen tot een toolkit voor systematische berekening en visualisering van invariante variëteiten in lage dimensie (≤ 4). Te denken valt aan (on)-

stabile variëteiten van evenwichten en periodieke banen, aan invariante tori en ook aan optredende hetero- en homocliene verschijnselen. De numerieke algoritmen zijn geënt op (contractie-)methoden uit existentie-bewijzen. De toolkit dient een gebruikersvriendelijk hulpmiddel te zijn bij onderzoek op het gebied van dynamische systemen, zowel in experimenten als bij het leveren van bewijzen.

Plotselinge verandering in systemen met adiabatische variabelen (prof. dr. ir. J. Grasman, LU Wageningen, prof. dr. ir. W. Eckhaus en prof. dr. F. Verhulst, Universiteit Utrecht)
Door een langzame verandering van parameters kan een niet-lineair systeem plotseling van de ene limietoplossing naar de andere springen. Als de verandering een functie van de toestandsvariabelen is, dan is het moment van plotselinge verandering moeilijk te voorspellen. Toepassingen worden gevonden in de mechanica, klimatologie en de biologie. Het doel van dit onderzoek is een kwantitatieve wiskundige theorie voor deze klasse van problemen te ontwikkelen.

Validiteit van modulatievergelijkingen van het Ginzburg-Landau type (prof. dr. ir. W. Eckhaus, prof. dr. A. van Harten en dr. A. Doelman, Universiteit Utrecht)
Onderzoek van de validiteit van de Ginzburg-Landau vergelijking en de stabiliteit van de Ginzburg-Landau variëteit in een algemene opzet, die de klassieke hydrodynamische problemen (Rayleigh-Bénard convectorie, Poiseuille-stroming, etc.) omvat.

Complexe analyse en approximatie. Deelproject A: Potentiaaltheorie en kwadratuurformules (prof. dr. J. Korevaar, Universiteit van Amsterdam)
Aanvrager heeft gevonden dat er voor gebieden zoals de sfeer, een nauw verband is tussen goede n -punt kwadratuurformules met gelijke coëfficiënten en configuraties van n gelijke (punt)ladingen met klein corresponderend elektrostatisch veld. Doel van het onderzoek is om precieze resultaten te verkrijgen over beide onderwerpen en om verwante vragen uit de potentiaaltheorie te bestuderen.

Niet-lineaire convectorie en diffusie van verontreinigingen in poreuze media (prof. dr. ir. C.J. van Duijn, TU Delft en prof. dr. ir. L.A. Peletier, RU Leiden)
In dit project wordt voorgesteld een aantal wiskundige aspecten uit de modellering van het transport van reactieve stoffen door een poreus materiaal (bijvoorbeeld verontreinigingen in grondwater) te bestuderen. Een centrale rol speelt hierbij een niet-

lineaire convectorie-diffusie-vergelijking (voor het transport), gekoppeld met een gewone differentiaalvergelijking (voor de chemische reacties). Deze studie zal zich richten op de kwalitatieve analyse van de oplossingen van dit stelsel, zoals existentie, eenduidigheid, regulariteit, vrije randen, asymptotisch gedrag in de tijd, etc.

Speciale functies en de methode van quantum-inverse verstrooiing (prof. dr. T.H. Koornwinder, Universiteit van Amsterdam)
De methode van scheiding van variabelen zal worden beschouwd voor quantum-integreerbare stelsels van fysisch belang. Deze methode is een generalisatie van de standaardmethode van coördinaatscheiding. Zij is nauw verbonden met de representaties van kwadratische R -matrixalgebra's (quantumgroepen). Voor de algebraïsche beschrijving van de corresponderende speciale functies, die de gezamenlijke eigenfuncties zijn van het volledige stel bewegingsconstanten voor het betreffende integreerbare stelsel, zal een algemene aanpak worden ontwikkeld. Nieuwe klassen van q -speciale functies, op deze manier verkregen, zullen worden bestudeerd.

Ruimtelijke patronen die worden beschreven door hogere orde reactie-diffusievergelijkingen (prof. dr. ir. L.A. Peletier, RU Leiden)
Centraal in het onderzoek staan de ruimtelijke structuren van bistabiele systemen zoals de hogere orde diffusieverschijnselen. De aandacht zal zich vooral richten op parabolische partiële differentiaalvergelijkingen. Eigenschappen die onderzocht zullen worden zijn onder andere: het bestaan en de vorm van periodieke oplossingen, chaotische oplossingen en de stabiliteit of instabiliteit van stationaire oplossingen.

Werkgemeenschap Algebra en Meetkunde

Cykels op algebraïsche variëteiten (prof. dr. F. Oort, Universiteit Utrecht en prof. dr. J.H.M. Steenbrink, KU Nijmegen)
Deformaties van een variëteit met behoud van een cykel. Deformaties van families.

Numerieke getaltheorie: het ontbinden van grote gehele getallen in priemfactoren (prof. dr. R. Tijdeman, RU Leiden en dr. ir. H.J.J. te Riele, CWI Amsterdam)
Onderzoek van de *Number Field Sieve*-factorisatiemethode voor een zo groot mogelijke klasse van gehele getallen (mogelijk zelfs voor willekeurige gehele getallen). Ontwikkeling van een machine-onafhankelijke implementatie van deze methode en

aanpassing en optimalisatie hiervan voor parallelle supercomputers (zoals de Cray Y-MP4 en de NEC SX-3). Onderzoek en, zo mogelijk, verhoging van de praktische bruikbaarheid van de NFS-methode. Vergelijking met de tot nu toe beste bekende algemene factorisatiemethode (MPQS) en experimentele bepaling van het interval waar NFS het wint van MPQS.

Deelvariëteiten van de moduli-ruimte van krommen (prof. dr. G.B.M. van der Geer en dr. C. Faber, Universiteit van Amsterdam)

- Onderzoek van complete deelvariëteiten van M_g ;
- constructie van complete deelvariëteiten van M_g .
- Enumeratieve meetkunde van M_g : bepaling van klassen van meetkundig gedefinieerde deelvariëteiten in de Chow-ring; interpretatie van de vermoedens van Witten.

WINST: Wiskunde- en Informatica: Samenwerkings-Thema's (prof. dr. H. Barendregt, KU Nijmegen, prof. dr. A.M. Cohen, TU Eindhoven, prof. dr. M. Hazewinkel en prof. dr. J.W. Klop, CWI Amsterdam)

WINST is een samenwerkingsproject tussen de Stichting Mathematisch Centrum (SMC) en de Stichting Informatica Onderzoek Nederland (SION). Het doel van het project is het realiseren van een vruchtbare interactie tussen de drie gebieden *theorem proving*, *term rewriting* en *symbolic computation*.

Werkgemeenschap Logica en Grondslagen van de Wiskunde

Interpreteerbaarheid en begrensde rekenkunde (prof. dr. J.F.A.K. van Benthem, Universiteit van Amsterdam)

Onderzoek van het begrip interpreteerbaarheid in rekenkundige en verzamelingstheoretische systemen, met speciale aandacht voor systemen van begrensde rekenkunde. Tevens onderzoek van de metamathematische en complexiteitstheoretische aspecten van die begrensde systemen van rekenkunde.

Exacte modellen voor fragmenten van intuïtionistische logica (prof. dr. G.R. Renardel de Lavalette, RU Groningen en dr. D.H.J. de Jongh, Universiteit van Amsterdam)

Doel van het project is het verrichten van onderzoek naar de structuur van fragmenten (c.q. hun Lindenbaum-algebra) van de intuïtionistische propositielogica (IpL). De bestudering van de zogeheten exacte modellen zal hierbij centraal staan. Het onderzoek zal ondersteund worden door automatische stellingentesters en -bewijzers voor IpL. Er zal spe-

ciale aandacht worden besteed aan toepassingen van de resultaten van het onderzoek in de theorie van IpL, typentheorie en in de ontwikkeling van nieuwe algoritmen voor stellingbewijzers.

Samenwerkingsverband FOM/SMC Mathematische Fysica

Mathematische fundering van de thermodynamica (prof. dr. M. Winnink, dr. A.C.D. van Enter, RU Groningen)

Voorgesteld wordt enkele aspecten te onderzoeken van het inverse probleem uit de statistische mechanica. In het bijzonder wordt gezocht naar voorwaarden waaronder het inverse probleem oplosbaar of onoplosbaar is.

Ergodiciteit voor grote systemen (prof. dr. H.W. Broer, dr. A.C.D. van Enter, prof. dr. F. Takens en prof. dr. M. Winnink, RU Groningen)

Centraal in het onderzoek staat het verschijnsel van ergodisch gedrag van grote systemen. In het bijzonder wordt het mogelijke bestaan van invariante tori in niet-lineaire systemen, zoals de random-vector modellen van het Heisenberg-type, onderzocht. Recente ontwikkelingen verbinden namelijk aspecten uit de theorie van de thermodynamische systemen met die uit de theorie der niet-lineaire dynamische systemen.

Onafhankelijkheid in de quantum-kanstheorie (dr. J.D.M. Maassen, KU Nijmegen)

Inventarisatie van de mogelijke realisaties van het begrip 'statistische onafhankelijkheid' in de quantum-kanstheorie. Nu bekende mogelijkheden: de tensorprodukt-structuur (omvat het klasieke, commutatieve geval), de anticommutatieve tensorprodukt-structuur en het gereduceerde vrije produkt (ontdekt in 1983), elk met haar eigen optelwet, centrale-limietstelling en 'witte ruis', en bovendien elk met een eigen fysische interpretatie. Het gebied lijkt rijk aan structuur, voor het grootste deel nog onontgonnen.

Topologische veldentheorie, stringtheorie en de meetkunde van moduli-ruimten (prof. dr. R.H. Dijkgraaf, Universiteit van Amsterdam)

Het onderzoek richt zich op de relatie tussen quantumveldentheorie en stringtheorie met behulp van algebraïsch meetkundige en algebraïsch topologische methoden.

Toepassingen van oneindig-dimensionale Lie-algebra's in de mathematische fysica (dr. G.F. Helminck, Universiteit Twente)

Onderzoek naar de rol die representaties van oneindig-dimensionale Lie-algebra's en vlagvariëteiten spelen in de quantumveldentheorie en de theorie van de integreerbare systemen. In het bijzonder worden onderzocht de interactie tussen de constructie van vertexoperatoren, rangorden van solitonvergelijkingen, partitiefuncties en W -algebra's.

Mathematische structuren van de Bethe-Ansatz en Yang-Baxter vergelijkingen (prof. dr. B. Nienhuis, Universiteit van Amsterdam)

Het project heeft tot doel een aantal wiskundige structuren van oplosbare modellen uit de statistische fysica op te helderen. In het bijzonder wil men de relatie tussen de Boltzmann-gewichten van het roostermodel en de S -matrix van de corresponderende veldentheorie begrijpen en het feit dat beide objecten voldoen aan de Yang-Baxter vergelijking. Een ander probleem dat aandacht zal krijgen is de relatie tussen de Yang-Baxter voorwaarde en de Bethe-Ansatz.

Fusieringen en quantumdimensies (dr. J.W. van Holten en dr. J. Fuchs, NIKHEF-H Amsterdam)

Fusieringen en quantumdimensies komen bijvoorbeeld voor in bepaalde groeptheoretische problemen, bij de representatietheorie van W -algebra's, quantumgroepen en cohomologieproblemen die alle toepassingen hebben in de quantumveldentheorie, bijvoorbeeld bij de bepaling van het spectrum van fysische toestanden. Het doel van het project is het geven van een nieuw inzicht in de structuur van fusieringen en hun beschrijving in termen van moderne algebra en algebraïsche meetkunde. Verwacht wordt dat dit inzicht kan worden gebruikt voor de afleiding van een gedetailleerde classificatie van quantumdimensies.

Bogoliubov transformaties voor ijtheorieën (prof. dr. P.J. van Baal, RU Leiden)

Met behulp van geschikte Bogoliubov transformaties hopen de onderzoekers de geschikte grondtoestanden te construeren in de supersymmetrische Yang-Mills theorie en de algemene Yang-Mills theorieën met fermionen.

Renormalisatie van verspreidingen (prof. dr. W. Th.F. den Hollander, KU Nijmegen)

Het doel van het project is het verdiepen en verbreden van recent onderzoek betreffende een renormalisatie-analyse voor verspreidingen. Dit on-

derzoek heeft een aantal vragen opgeleverd die tot nu toe onbeantwoord zijn gebleven. Renormalisatie-technieken worden toegepast in de statistische fysica op systemen die in evenwicht verkeren. Er zijn echter weinig succesvolle pogingen om renormalisatie-analyse toe te passen op systemen die niet in evenwicht verkeren. Het onderzoek zal zich ook richten op een speciale klasse van veeldeeltjessystemen met een eenvoudige dynamica, zodat concepten en technieken uit de waarschijnlijkheidsrekening, functionaalanalyse en statistische fysica kunnen worden gecombineerd om een beter inzicht te krijgen.

Relaxatie-oscillatie dynamica in diode lasers (prof. dr. D. Lenstra, VU Amsterdam)

Centraal staat de theoretische analyse van de dynamica van een diode laser met behulp van analytische en numerieke technieken. Onderzoek van periodieke attractoren, hun bifurcaties, classificaties en hun gevoeligheid voor stochastische ruis.

Aandachtsprogramma Wiskundige Aspecten van Niet-lineaire Dynamische Systemen

Dynamica van de opgedikte Arnold familie (prof. dr. H.W. Broer en prof. dr. F. Takens, RU Groningen)

De dynamica van de opgedikte Arnold familie speelt een belangrijke rol bij het onderzoek van resonantieverschijnselen en homocliene bifurcaties. Het voorgestelde onderzoek heeft veel aanknopingspunten met lopend onderzoek op het gebied van niet-lineaire systemen zoals de dissipatieve KAM-theorie, de theorie van 1-D afbeeldingen en de reeds genoemde homocliene bifurcaties.

Chaos en quasi-periodiciteit in verdraaide Hopf-bifurcaties nabij cirkelsymmetrie (prof. dr. H.W. Broer en prof. dr. F. Takens, RU Groningen)

De verdraaide Hopf-bifurcatie is een zekere ontwikkeling van quasi-periodieke naar chaotische dynamica. Dit verschijnsel manifesteert zich in systemen met cirkelsymmetrie. In systemen zonder cirkelsymmetrie gebeurt iets dergelijks. Eenvoudige numerieke experimenten laten zien dat er in dit geval sprake is van een rijke dynamica. Het onderzoek heeft tot doel een verklaring voor dit verschijnsel te vinden.

Passage door resonantie in adiabatisch variërende Hamilton-systemen (prof. dr. F. Verhulst, Universiteit Utrecht)

Het onderzoek heeft tot doel de analyse van systemen met twee vrijheidsgraden, die zich van een conserva-

tief asymmetrisch naar een conservatief symmetrisch systeem ontwikkelen. Hierbij wordt met name aandacht besteed aan de invloed van tijdsafhankelijke processen op de integreerbaarheid van normaalvormen en het verband met adiabatische varianten.

Dynamica van de gekoppelde Josephson junction (dr. S.A. van Gils, Universiteit Twente)

De dynamica van globaal gekoppelde functies wordt onderzocht, zowel numeriek als analytisch, in het bijzonder in de buurt van een twist bifurcatiepunt, speciale aandacht wordt besteed aan symmetrie-aspecten.

Numerieke bifurcatie-analyse (dr. J. Sanders, RIACA Amsterdam)

Het doel is te komen tot een numeriek bifurcatie-analyse programma met een grafische interface onder X-windows en de gebruikersinterface te implementeren.

Laag-dimensionale dynamica: hyperbolische systemen (prof. dr. S.J. van Strien, Universiteit van Amsterdam)

In veel opzichten modelleren een-dimensionale systemen hoger-dimensionale systemen. Het onderzoek van Benedicks en Carleson over het bestaan van vreemde aantrekkers met positieve Liapunov-exponenten in de Henon-afbeelding is daar een mooi voorbeeld van. Het doel van het onderzoek is het voortbouwen op het werk van Benedicks en Carleson; met name het vinden van een bewijs voor de resultaten voor de een-dimensionale systemen.

Aandachtsprogramma Algoritmen in de Algebra

Algebraïsche aspecten van differentiaalvergelijkingen (prof. dr. M. van der Put, RU Groningen)

Het onderzoek richt zich op het construeren van algoritmen voor het berekenen van differentiaal Galois-groepen voor een zo groot mogelijk aantal klassen van differentiaalvergelijkingen en voor de bepaling van algebraïsche oplossingen waarvan verwacht wordt dat ze bestaan op grond van vermoedens. Verder zal aandacht worden besteed aan de voltooiing van de moderne algoritmische theorie van normaalvormen.

Lie-algebra's (prof. dr. M. Hazewinkel en prof. dr. A.M. Cohen, CWI Amsterdam)

Het onderzoek richt zich onder andere op:
- het toepassen van bestaande basisalgoritmen

voor de systematische structuurbepaling van Lie-algebra's en hun cohomologie;

- het gebruik van goede bases voor semisimpele Lie-algebra's, hun constructies en hun betekenis voor de decomposities van tensorprodukten;
- het ontwikkelen van algoritmen voor het rekenen met bases van Lusztig en Kashiwara;
- Gröbner-bases in relatie met Hopf-algebra's;
- de expliciete berekeningen voor Lie-algebra's met methoden die op Buchberger-bases berusten.
- een onderzoek naar berekenbaarheid van verscheidene in de literatuur aangegeven bases voor reductieve Lie-algebra's en het ontwikkelen van verdere voor de representaties relevante algoritmen.

Representaties van algebraïsche groepen (prof. dr. A.M. Cohen, TU Eindhoven)

Het onderzoek richt zich op de representaties van halfnkelvoudige algebraïsche groepen en bijbehorende bases met de nadruk op algoritmische methoden.

Overdekkingen van de projectieve lijn (dr. F. Beukers, Universiteit Utrecht)

De relatie tussen de theorie van overdekkingen en Galois-theorie heeft geleid tot onderzoek, vooral op het gebied van Grothendieck's 'dessins d'enfants' een bijnaam voor grafen die bepaalde boloverdekkingen karakteriseren. De theorie van de overdekkingen kent veel aspecten waarbij de computer met vrucht kan worden ingezet voor een beter begrip voor die theorie.

Aandachtsprogramma Rekenintensieve Methoden in de Stochastiek

Niet-parametrische schatting (prof. dr. R.D. Gill en dr. B. Levit, Universiteit Utrecht)

Centraal staat het onderzoek in de niet-parametrische schatting, met name het onderzoek naar asymptotisch optimale, niet-parametrische regressie schattingsprocedures met het doel de optimale snelheden van convergentie binnen bepaalde parametrische gebieden (ellipsoiden in geschikte Hilbert-ruimten) precies te bepalen.

Stochastische meetkunde (prof. dr. M.S. Keane, CWI Amsterdam)

Centraal staat het onderzoek naar een beter begrip van de klassieke limietstellingen in de waarschijnlijkheidsrekening. De stochastische meetkunde wordt in het onderzoek toegepast voor de stochastische modellering van longen.

Stochastische modellen in natuur en techniek (dr. J. van den Berg, CWI Amsterdam)

Onderzoek op het gebied van ruimtelijke stochastische processen met nadruk op percolatieverschijnselen.

Extremen: kanstheorie en statistiek (prof. dr. L.F.M. de Haan, Erasmus Universiteit Rotterdam)
Het onderzoek beoogt toepassingen van de kanstheorie in de statistiek. Met name betreft het hier de kanstheorie van extreme waarden in het oneindig-dimensionale geval waarbij wordt uitgegaan van stochastische processen.

Continue percolatiemodellen (dr. R.W.J. Meester, Universiteit Utrecht)

Het doel van het project is het onderzoek naar het asymptotische gedrag van kritieke dichtheden in hoge dimensies, continuïteit van kritieke dichtheden, compressie en decompressieverschijnselen.

Ruimtelijke stochastische processen (dr. R.W.J. Meester, Universiteit Utrecht en prof. dr. M.S. Keane, CWI, Amsterdam)

Het onderzoek zal zich richten op ruimtelijke stochastische processen, in het bijzonder fractale percolatieprocessen. In eerste instantie is de doelstelling het aantonen van een fase-overgang en het onderzoek van de structuur van het oneindige cluster.

Efficiënte schatters in het Error in Variables Model (prof. dr. C.A.J. Klaassen, Universiteit van Amsterdam)

Het errors in variables model is een lineair regressiemodel waar zowel de onafhankelijke als de respons variabele met fout worden waargenomen. In 1987 hebben Bickel en Ritov efficiënte schatters voor de regressieparameters afgeleid in het bijzondere geval dat de fouten normaal verdeeld zijn. Het voornaamste aandachtspunt in het onderzoek is de structuur

van het schattingsprobleem als men de aanname van normaliteit laat vallen. Kennis van deze structuur zal uiteindelijk leiden tot efficiënte schatters.

Aandachtsgebied Algebraïsche krommen en Riemann-oppervlakken

Algebraïsche krommen en mathematische fysica (prof. dr. R.H. Dijkgraaf, Universiteit van Amsterdam)

In de quantumveldentheorie spelen algebraïsche krommen een fundamentele rol. Een kromme is hier een natuurlijke generalisatie van het concept 'punt-deeltje'. Het onderzoek richt zich vooral op de toepassing van algebraïsche krommen in de stringtheorie en de twee-dimensionale quantumveldentheorie.

Chow-ringen van moduli-ruimten (prof. dr. E.J.N. Looijenga, Universiteit Utrecht)

Studie van de meetkunde en topologie van de moduli-ruimten van Riemann-oppervlakken en hun natuurlijke compactificaties.

Groot Project Lie-Theorie en Speciale Functies

Yang-Baxter-vergelijkingen en toepassingen op knoop- en schakelvarianten (dr. W.L.J. van der Kallen, Universiteit Utrecht)

Het onderzoek zal zich concentreren op multiparameteroplossingen van Yang-Baxter-vergelijkingen. Als uitgangspunt dient de analyse gegeven in het artikel Multiparameter quantum groups and multiparameter R-matrices.

Quantumgroepen en q-speciale functies (prof. dr. T.H. Koornwinder, Universiteit van Amsterdam)
Het onderzoek concentreert zich op twee hoofdstromen: a) Quantum analogieën van niet-compacte reële halfenkelvoudige symmetrische ruimten en b) limietovergangen van speciale functies.

Publicaties

Werkgemeenschap Numerieke Wiskunde

A.O.H. AXELSSON, M.G. NEYTCHEVA, B. POLMAN (1995). An application of the bordering method to solve nearly singular systems. *Vestnik Moskovskogo Universiteta, Seria V'chisl. Math. Cybern.*

M.G. NEYTCHEVA (1995). Experience in implementing the Algebraic Multilevel Iteration Method on a SIMD-type computer. *Appl. Num. Math.* 19, 71–90.

A.O.H. AXELSSON, M.G. NEYTCHEVA (1995). Scalable parallel algorithms in CFD computations. M. HAFEZ, K. OSHIMA (eds.). *Computational Fluid Dynamics Review*, 837–857.

A.O.H. AXELSSON, M.G. NEYTCHEVA (1995). Scalable algorithms for the solution of Navier's equations of elasticity. *J. Comp. Appl. Math.* 63, 149–178.

M.G. NEYTCHEVA, P. VASSILEVSKI (1995). *Preconditioning of Indefinite and Almost Singular Finite Element Elliptic Equations*, Report 9532, Katholieke Universiteit Nijmegen.

M.G. NEYTCHEVA (1995). *Arithmetic and Communication Complexity of Preconditioning Methods*, proefschrift, Katholieke Universiteit Nijmegen.

M. ZIJLEMA, A. SEGAL, P. WESSELING (1995). Invariant discretization of the k - ε model in general coordinates for prediction of turbulent flow in complicated geometries. *Computers and Fluids* 24, 209–225.

M. ZIJLEMA, A. SEGAL, P. WESSELING (1995). Finite volume computation of incompressible turbulent flows in general coordinates on staggered grids. *Int. J. Numer. Meth. Fluids* 20, 621–640.

M. ZIJLEMA (1995). *On the Sensitivity of the Results to the Numerical Approximation of Turbulence Convective Transport in a k - ε Turbulence Model*, Report 95-06, Technische Universiteit Delft.

M. ZIJLEMA, P. WESSELING (1995). *On Accurate Discretization of Turbulence Transport Equations in General Coordinates*, Report 95-25, Technische Universiteit Delft.

P. WESSELING, M. ZIJLEMA, A. SEGAL, C.G.M. KASSELS (1995). *Computation of Turbulent Flow in General Domains*, Report 95-85, Technische Universiteit Delft.

M. ZIJLEMA, P. WESSELING (1995). *Higher Order Flux-limiting Methods for Steady-state Multi-dimensional, Convection-dominated Flow*, Report

95-131, Technische Universiteit Delft.

M. ZIJLEMA (1995). Description of numerical methodology for 2D hill flows. W. RODI, J.-C. BONNIN (eds.). *Proc. Fourth ERCOFTAC-IAHR Workshop on Refined Flow Modelling*, 91–94.

M. ZIJLEMA, P. WESSELING (1995). On accurate discretization of turbulence transport equations in general coordinates. C. TAYLOR, P. DURBETAKI (eds.). *Proc. Ninth. Int. Conf. on Numer. Meth. Laminar and Turbulent Flow*, 34–45.

A.O.H. AXELSSON, H. LU (1995). On eigenvalue estimates for block incomplete factorization methods. *SIAM J. Matrix Anal. Appl.* 16, 1074–1085.

H. LU (1995). A uniform-consistency barrier on finite-difference schemes of positive type for convection-diffusion equations. *SIAM J. Sci. Comput.* 16, 169–172.

H. LU (1995). Fast algorithms for confluent Vandermonde linear systems and generalized Trummer's problems. *SIAM J. Matrix Anal. Appl.* 16, 655–674.

H. LU (1995). *Forward-backward Heat Equations and Analysis of Iterative Methods*, proefschrift, Katholieke Universiteit Nijmegen.

Werkgemeenschap Stochastiek

E.R. VAN DEN HEUVEL (1995). *A Convolution Theorem for Locally Asymptotically Quadratic Likelihood Ratios*, Report 95-07, Universiteit van Amsterdam.

J.H.J. EINMAHL, L.F.M. DE HAAN, A.K. SINHA (1995). *Estimating the Spectral Measure of an Extreme Value Distribution*, Report 9533/A, Erasmus Universiteit Rotterdam.

L.F.M. DE HAAN, A.K. SINHA (1995). *Asymptotic Normality for the Exponential Measure*, Discussion Paper Erasmus Universiteit Rotterdam.

A.K. SINHA (1995). *Estimation of Exceedance Probability in Multi-dimensional Case*, Discussion Paper Erasmus Universiteit Rotterdam.

Werkgemeenschap Mathematische Besliskunde en Systeemtheorie

H. HAMERS (1995). *On the Concavity of Delivery Games*, CentER Discussion Paper 9529, Katholieke Universiteit Brabant.

H. HAMERS (1995). On games corresponding to

sequencing situations with ready times. *Mathematical Programming* 69, 471–483.

H. HAMERS, M. SLIKKER (1995). *The PEGS Rule for Probabilistic Sequencing Situations*, Research Memorandum FEW 703, Katholieke Universiteit Brabant.

J. SUIJS, H. HAMERS, S. TIJS (1995). *On Consistency of Reward Allocation Rules in Sequencing Situations*, CentER Discussion Paper 9518, Katholieke Universiteit Brabant.

H. HAMERS (1995). *Sequencing and Delivery Situations: a Game Theoretic Approach*, proefschrift, Katholieke Universiteit Brabant.

J.A. LOEVE (1995). *Markov Decision Chains with Partial Information*, proefschrift, Rijksuniversiteit Leiden.

W.B. VAN DEN HOUT, J.P.C. BLANC (1995). The power-series algorithm for Markovian queueing networks. W.J. STEWART (ed.). *Computations with Markov Chains*, Kluwer, 321–338.

W.B. VAN DEN HOUT, J.P.C. BLANC (1995). Development and justification of the power-series algorithm for BMAP-systems. *Commun. Statist.-Stochastic Models* 11, 471–496.

E.H.L. AARTS, H.P. STEHOUWER, J. WESSELS, P.J. ZWIETERING (1995). Neural networks for combinatorial optimization. J. DOLEŽAL, J. FIDLER (eds.). Optimization-based Computer-aided Modelling and Design, *Proc. of the third IFIP WG-7.6 Working Conference*, 25–40.

H.P. STEHOUWER, E.H.L. AARTS, J. WESSELS (1995). Multi-layered perceptrons for on-line lot sizing. *Proc. INRIA/IEEE Symposium on Emerging Technologies and Factory Automation* 3, 279–287.

O. GÜLER, C. ROOS, T. TERLAKY, J.P. VIAL (1995). A survey of the implications of the behavior of the central path for the duality theory of linear programming. *Management Science* 41, 1922–1934.

D. DEN HERTOEG, F. JARRE, C. ROOS, T. TERLAKY (1995). A sufficient condition for self-concordance with application to some classes of structured convex programming problems. *Mathematical Programming* 69, 75–88.

B. JANSEN, C. ROOS, T. TERLAKY (1995). Inwendige Punt Methoden voor lineaire en niet-lineaire optimalisering. *Jaarverslag Stichting Mathematisch Centrum* 1994, 23–27.

D. DEN HERTOEG, C. ROOS, J. KALISKI, T. TERLAKY (1995). A logarithmic barrier cutting plane method for convex programming. *Annals of Operations Research* 58, 69–98.

B. JANSEN, C. ROOS, T. TERLAKY (1995). Interior Point Methods, A decade after Karmarkar - A survey

with application to the smallest eigenvalue problem. *Statistica Neerlandica* 50, 146–170.

B. JANSEN, C. ROOS, T. TERLAKY (1995). Interior Point Methods for Linear and nonlinear programming. *Thomas Stieltjes Institute, Biennial Report 1993-1994*, 35–41.

B. JANSEN, C. ROOS, T. TERLAKY (1995). *A Short Survey on Ten Years of Interior Point Methods*, Report 95-45, Technische Universiteit Delft.

B. HE (1995). *Inexact Implicit Methods for Monotone General Variational Inequalities*, Report 95-60, Technische Universiteit Delft.

B. HE (1995). *Some Predict-Correct Projection Methods for Monotone Variational Inequalities*, Report 95-68, Technische Universiteit Delft.

B. JANSEN, C. ROOS, T. TERLAKY (1995). *A New Algorithm for the Computation of the Smallest Eigenvalue of a Symmetric Matrix and its Eigenspace*, Report 95-70, Technische Universiteit Delft.

B. JANSEN, C. ROOS, T. TERLAKY, A. YOSHISE (1995). *Polynomiality of Primal-Dual Affine Scaling Algorithms for Nonlinear Complementarity Problems*, Report 95-83, Technische Universiteit Delft.

J.P. WARNERS, T. TERLAKY, C. ROOS, B. JANSEN (1995). *Potential Reduction Algorithms for Structured Combinatorial Optimization Problems*, Report 95-88, Technische Universiteit Delft.

J.P. WARNERS, T. TERLAKY, C. ROOS, B. JANSEN (1995). *A Potential Reduction Approach to the Frequency Assignment Problem*, Report 95-98, Technische Universiteit Delft.

E. DE KLERK, C. ROOS, T. TERLAKY (1995). *Semi-Definite Problems in Truss Topology Optimization*, Report 95-128, Technische Universiteit Delft.

E. DE KLERK, C. ROOS, T. TERLAKY (1995). *A Nonconvex Weighted Potential Function for Polynomial Target Following Methods*, Report 95-127, Technische Universiteit Delft.

R. BOSCH, R.V. TORENBEEK (1995). *A Family of Algorithms for Approximating the Smallest Eigenvalue of a Real Matrix with No Complex Eigenvalues*, Report 95-125, Technische Universiteit Delft.

K. AARDAL, A. HIPOLITO, C.P.M. VAN HOESEL, B. JANSEN, C. ROOS, T. TERLAKY (1995). *Implementation and Testing of Polyhedral Techniques and Interior Point Methods*, EUCLID CALMA Report 2.2.1.

K. AARDAL, A. HIPOLITO, C.P.M. VAN HOESEL, B. JANSEN, C. ROOS, T. TERLAKY (1995). *A Branch-and-Cut Algorithm for the Frequency Assignment Problem*, EUCLID CALMA Report Technical Annex T-2.2.1.

H. VAN BENTHEM, A. HIPOLITO, B. JANSEN, C.

ROOS, T. TERLAKY, J.P. WARNERS (1995). *Potential Reduction Methods*, EUCLID CALMA Report 2.3.2.

H. VAN BENTHEM, A. HIPOLITO, B. JANSEN, C. ROOS, T. TERLAKY, J.P. WARNERS (1995). *Potential Reduction Methods*, EUCLID CALMA Report Technical Annex T-2.3.2.

H. VAN BENTHEM, A. HIPOLITO, B. JANSEN, C. ROOS, T. TERLAKY, J.P. WARNERS (1995). *GRAPH: A Test Case Generator. Generating Radio Link Frequency Assignment Problems Heuristically*, EUCLID CALMA Report.

J.P. WARNERS, T. TERLAKY, C. ROOS, B. JANSEN, A. HIPOLITO, H. VAN BENTHEM (1995). *GRAPH: A Test Problem Generator for the Radio Link Frequency Assignment Problems*, EUCLID CALMA Report Supplement 2.3.2a.

Werkgemeenschap Analyse

A. HOMBURG, H.M. OSINGA, G. VEGTER (1995). On the computation of invariant manifolds of fixed points. *Z. für Angewandte Math. und Physik* 46, 171–187.

H.W. BROER, H.M. OSINGA, G. VEGTER (1995). On the computation of normally hyperbolic invariant manifolds. H.W. BROER, S.A. VAN GILS, I. HOVEIJN, F. TAKENS (eds.). *Nonlinear Dynamical Systems and Chaos, Progress in Nonlinear Partial Differential Equations and their Applications* 19, 423–447.

H.W. BROER, H.M. OSINGA, G. VEGTER (1995). *Algorithms for Computing Normally Hyperbolic Invariant Manifolds*, Report W-9518, Rijksuniversiteit Groningen.

M.A. PELETIER, H. ZANG (1995). Self-similar solutions of a fast diffusion equation that do not conserve mass. *Differential and Integral Equations* 8, 2045–2064.

M. GUEDDA, D. HILHORST, M.A. PELETIER (1995). *Nonlinear Diffusion in an Inhomogeneous Aquifer*, Report 95-44, Technische Universiteit Delft.

G.J.M. MARÉE (1995). *Sudden Change in Second Order Nonlinear Systems: Slow Passage through Bifurcation*, proefschrift, Landbouwniversiteit Wageningen.

G.J.M. MARÉE (1995). *Slow Periodic Crossing of a Pitchfork Bifurcation in an Oscillating System*, Report 94-04, Landbouwniversiteit Wageningen.

P.A.A.J. BOLLERMAN, A. VAN HARTEN, G. SCHNEIDER (1995). On the justification of the Ginzburg-Landau approximation. A. DOELMAN, A. VAN HARTEN (eds.). *Nonlinear Dynamics and Pattern Formation in the Natural Environment*, Pitman Research Notes in Mathematics Series.

P.A.A.J. BOLLERMAN (1995). Validity of the

Ginzburg-Landau approximation in two-dimensional Poiseuille flow. A. MIELKE, K. KIRCHGASSNER (eds.). *Structure and Dynamics of Nonlinear Waves in Fluids, Advanced Series in Nonlinear Dynamics* 7.

E.G. KALNINS, V.B. KUZNETSOV, W. MILLER JR. (1995). Separation of variables and XXZ Gaudin magnet. *Rend. Sem. Mat. Univ. Politec. Torino* 53, 109–120.

V.B. KUZNETSOV, M.F. JØRGENSEN, P.L. CHRISTIANSEN (1995). New boundary conditions for integrable lattices. *J. Phys. A* 28, 4639–4654.

V.B. KUZNETSOV, E.K. SKLYANIN (1995). Separation of variables in the A2 type Jack polynomials. *RIMS Kokyuroku* 919, 27.

A.B.J. KUIJLAARS (1995). Chebyshev-type quadrature and partial sums of the exponential series. *Math. Comp.* 64, 251–263.

A.B.J. KUIJLAARS (1995). Chebyshev-type quadrature for Jacobi weight functions. *J. Comput. Appl. Math.* 57, 171–180.

A.B.J. KUIJLAARS (1995). Chebyshev-type quadrature and zeros of Faber polynomials. *J. Comput. Appl. Math.* 62, 155–179.

A.B.J. KUIJLAARS (1995). Chebyshev quadrature for measures with strong singularity. *J. Comput. Appl. Math.* 62.

A.B.J. KUIJLAARS (1995). Chebyshev-type quadrature for analytic weights on the circle and the interval. *Indag. Math. N.S.* 6, 419–432.

A.B.J. KUIJLAARS, E.B. SAFF (1995). Asymptotic distribution of the zeros of Faber polynomials. *Math. Proc. Cambridge Philos. Soc.* 118, 437–447.

A.B.J. KUIJLAARS (1995). *A Note on Weighted Polynomial Approximation with Varying Weights*, Report 95-20, Universiteit van Amsterdam.

A.B.J. KUIJLAARS (1995). *Weighted Approximation with Varying Weights: the Case of a Power-type Singularity*, Report 95-21, Universiteit van Amsterdam.

A.B.J. KUIJLAARS, E.B. SAFF (1995). *Asymptotics for Minimal Discrete Energy on the Sphere*, Report 95-22, Universiteit van Amsterdam.

J. KOREVAAR (1995). A monotonicity property of ultraspherical Christoffel numbers. *Ann. Numer. Math.* 5, 277–287.

M.A. MONTERIE (1995). *Studies in Potential Theory*, proefschrift, Universiteit van Amsterdam.

Werkgemeenschap Algebra en Meetkunde

R.M. HUIZING (1995). *Experiments with the Number Field Sieve*, CWI Report NM-R9511.

P. ALUFFI, C.F. FABER (1995). A remark on the Chern class of a tensor product. *Manuscripta*

Math. 88, 85–86.

G.B.M. VAN DER GEER, M. VAN DER VLUGT (1995). On the existence of supersingular curves of a given genus. *Z. für die Reine und Angewandte Mathematik* 458, 53–61.

C. ZAAL (1995). Explicit complete curves in the moduli space of curves of genus three. *Geometriae Dedicata* 56, 185–196.

G.B.M. VAN DER GEER, M. VAN DER VLUGT (1995). *How to Construct Curves over Finite Fields with many Points*, Report 95-24, Universiteit van Amsterdam.

R.H. DIJKGRAAF, C.F. FABER, G.B.M. VAN DER GEER (eds.) (1995). *The Moduli Space of Curves*, Birkhäuser.

B.J.J. MOONEN, YU.G. ZARHIN (1995). Hodge classes and Tate classes on simple abelian fourfolds. *Duke Math. Journal* 77, 553–581.

B.J.J. MOONEN (1995). *Special Points and Linearity Properties of Shimura varieties*, proefschrift, Universiteit Utrecht.

G. BARTHE (1995). Extensions of pure type systems. M. DEZANI-CIANCAGLINI, G. PLOTKIN (eds.). *Proc. TLCA '95, LNCS 902*, Springer-Verlag, 16–31.

G. BARTHE (1995). A simple abstract semantics for equational theories. H. REICHEL (ed.). *Proc. FCT '95, LNCS 965*, Springer-Verlag, 126–135.

Werkgemeenschap Logica en Grondslagen van de Wiskunde

A. HENDRIKS (1995). Exact models and computations in propositional logic. S. FISCHER, M. TRAUTWEIN (eds.). *Proc. Accolade '95*, 59–73.

M.B. KALSBEK (1995). *Meta-logics for Logic Programming*, proefschrift, Universiteit van Amsterdam.

M.B. KALSBEK (1995). Correctness of the Vanilla meta-interpreter and ambivalent syntax. K.R. APT, F. TURINI (eds.). *Meta-logics and Logic Programming*, 1–26.

M.B. KALSBEK, Y. JIANG (1995). A vademecum of ambivalent logic. K.R. APT, F. TURINI (eds.). *Meta-logics and Logic Programming*, 27–56.

J.P.C.M. VAN DRAANEN (1995). *Models for Simply Typed Lambda-calculi with Fixed Point Combinators and Enumerators*, proefschrift, Katholieke Universiteit Nijmegen.

Samenwerkingsverband FOM/SMC Mathematische Fysica

R.H. DIJKGRAAF ET AL. (eds.) (1995). *String Theory, Gauge Theory and Quantum Gravity*, Triest

Spring School and Workshop, *Nucl. Phys. B, Proc. Suppl.* 41.

O. DE MIRLEAU (1995). *Non-Gaussian Generalizations of Wick's Theorems Related to the Schwinger-Dyson Equation*, hep-th/9507039.

M. BAAKE, U. GRIMM, C.P. PISANI (1995). Partition function zeros for non-periodic systems. *J. Stat. Phys.* 78, 285–297.

U. GRIMM, S.O. WARNAAR (1995). New RSOS models based on the dilute BWM algebra. *Nucl. Phys. B* 435, 482–504.

U. GRIMM, S.O. WARNAAR (1995). Yang-Baxter algebras based on the two-colour BWM algebra. *J. Phys. A* 28, 7197–7207.

U. GRIMM, M. BAAKE, H. SIMON (1995). Ising spins on the labyrinth. C. JANOT, R. MOSSERI (eds.). *Proc. 5th International Conference on Quasicrystals*, World Scientific, Singapore, 80–83.

H. SIMON, M. BAAKE, U. GRIMM (1995). Lee-Yang zeros for substitutional systems. C. JANOT, R. MOSSERI (eds.). *Proc. 5th International Conference on Quasicrystals*, World Scientific, Singapore, 100–103.

Y.K. ZHOU, P.A. PEARCE, U. GRIMM (1995). Fusion of dilute AL lattice models. *Physica A* 222, 261–306.

M. BAAKE, V. ELSER, U. GRIMM (1995). *On the Entropy of Square-free Words*, Preprint ITFA-95-21.

U. GRIMM (1995). *Dilute Algebras and Solvable Lattice Models*, Preprint ITFA-95-25.

U. GRIMM, B. NIENHUIS (1995). *Scaling Properties of the Ising Model in a Field*, Preprint ITFA-95-26.

K. PEETERS, C. SCHWEIGERT, J.W. VAN HOLTEN (1995). Extended geometry of black holes. *Class. Quantum Grav.* 12, 173.

J. FUCHS, A.N. SCHELLEKENS, C. SCHWEIGERT (1995). Galois modular invariants of WZW models. *Nucl. Phys. B* 437, 667.

J. FUCHS, A.N. SCHELLEKENS, C. SCHWEIGERT (1995). *Quasi-Galois Symmetries of the Modular S-Matrix*, preprint hep-th/9412009.

M. KREUZER, C. SCHWEIGERT (1995). On the extended Poincaré Polynomial. *Phys. Lett. B* 352, 276.

J. FUCHS, A.N. SCHELLEKENS, C. SCHWEIGERT (1995). *From Dynkin Diagram Symmetries to Fixed Point Structures*, preprint hep-th/9506135.

J. FUCHS, A.N. SCHELLEKENS, C. SCHWEIGERT (1995). *The Resolution of Field Identification Fixed Points in Diagonal Coset Theories*, preprint hep-th/9509105.

C. SCHWEIGERT (1995). *Galois and Simple Current Symmetries in Conformal Field Theory*, proef-

schrift, Universiteit van Amsterdam.

J. LÓRINCZI (1995). *On Limits of the Gibbsian Formalism in Thermodynamics*, proefschrift, Rijksuniversiteit Groningen.

J.H.M. VAN LEEUWEN, J.D.M. MAASSEN (1995). A q deformation of the Gauss distribution. *J. Math. Phys.* 36, 4743–4756.

J.W. VAN DE LEUR (1995). The Adler-Shiota-van Moerbeke formula for the BKP hierarchy. *J. Math. Phys.* 36, 4940–4951.

Aandachtsprogramma Wiskundige Aspecten van Niet-lineaire Dynamische Systemen

I. HOVEIJN, M. RUIJGROK (1995). On the stability of parametrically driven coupled oscillators in sum resonance. *ZAMP* 46, 384–392.

I. HOVEIJN (1995). *Normal Forms and Versal Deformations of Reversible and Hamiltonian Linear Systems*, Report W-9515, Rijksuniversiteit Groningen.

R.H. CUSHMAN, I. HOVEIJN (1995). Visualizing special motions of the Euler top. R.P. ARGWAL (ed.). *Dynamical Systems and Applications*, World Scientific Series in Applicable Analysis 4, 153–167.

R. ROUSSARIE, F.O.O. WAGENER (1995). A study of the Bogdanov-Takens bifurcation. *Resenhas IME-USP* 2, 1–25.

Y. KUZNETSOV (1995). *Elements of Applied Bifurcation Theory*, Springer-Verlag.

V. LEVITIN (1995). *Computations of Functions and their Derivatives in CONTENT*, CWI Report AM-R9512.

G. LEVIN, S.J. VAN STRIEN (1995). *Locally Connected Julia Sets of Real Polynomials*, Report 95-5, Stony Brook.

C.H. HOMMES, S.J. VAN STRIEN, R.G. DE VILDER (1995). Chaotic dynamics in a two-dimensional overlapping generations model. A numerical investigation. J. GRASMAN, G. VAN STRATEN (eds.). *Predictability and Nonlinear Modeling in Natural Sciences and Economics*, Kluwer, 211–229.

R.G. DE VILDER (1995). *Endogenous Business Cycles*, proefschrift, Universiteit van Amsterdam.

S.J. VAN STRIEN (1995). *Polynomial Maps with a Julia Set of Positive Lebesgue Measure*, Report, Universiteit van Amsterdam.

S.J. VAN STRIEN (1995). *Transitive Rational Maps which are not Ergodic*, Report, Universiteit van Amsterdam.

O.S. KOZLOVSKY (1995). *Dynamo Theory*, Report, Universiteit van Amsterdam.

R.J.A.G. HUVENEERS (1995). *The Quantum 2D-harmonic Oscillator in 1:1 Resonance with Time-*

dependent Perturbation, Preprint 875, Universiteit Utrecht.

R.J.A.G. HUVENEERS, F. VERHULST (1995). *A Metaphor for Adiabatic Evolution to Symmetry*, Preprint 919, Universiteit Utrecht.

Aandachtsprogramma Algoritmen in de Algebra

M. VAN DER PUT (1995). Reductions of differential equations modulo p . *Indagationes*.

M. VAN DER PUT (1995). Differential equations in characteristic p . *Compositio Mathematica* 97, 227–251.

P.A. HENDRIKS, M. VAN DER PUT (1995). Galois actions on solutions of differential equations. *Journal of Symbolic Computation*.

N.W. VAN DEN HILLIGENBERG, Y. KOTCHETKOV, G. POST (1995). Deformation of vector fields and Hamiltonian vector fields on the plane. *Math. of Comp.* 64, 1215–1226.

N.W. VAN DEN HILLIGENBERG, G. POST (1995). Computation by computer of Lie superalgebra homology and cohomology. *Acta Appl. Math.* 41, 123–134.

N.W. VAN DEN HILLIGENBERG, R. MARTINI (1995). *Differential Hopf Algebra Structures on the Universal Enveloping Algebra of a Lie Algebra*, CWI Report AM-R9515.

N.W. VAN DEN HILLIGENBERG, R. MARTINI (1995). *From Exponential Coordinates to Bivariant Differential Calculi on Matrix Quantum Groups*, CWI Report AM-R9518.

N.W. VAN DEN HILLIGENBERG, R. MARTINI (1995). *A Natural Differential Calculus on Lie Bialgebras with Dual of Triangular Type*, CWI Report AM-R9519.

Aandachtsprogramma Algebraïsche krommen en Riemann-oppervlakken

R.H. DIJKGRAAF (1995). Mirror symmetry and elliptic curves. R.H. DIJKGRAAF, C.F. FABER, G.B.M. VAN DER GEER (eds.). *The Moduli Space of Curves*, Birkhäuser, 149–163.

E.J.N. LOOIJENGA (1995). On the tautological ring of M_g . *Invent. Math.* 121, 411–419.

E.J.N. LOOIJENGA (1995). Cellular decompositions of compactified moduli spaces of pointed curves. R.H. DIJKGRAAF, C.F. FABER, G.B.M. VAN DER GEER (eds.). *The Moduli Space of Curves*, Birkhäuser, 369–400.

M. PIKAART (1995). An orbifold partition of M_g^n . R.H. DIJKGRAAF, C.F. FABER, G.B.M. VAN DER GEER (eds.). *The Moduli Space of Curves*,

Birkhäuser, 467–482.

M. PIKAART, A.J. DE JONG (1995). Moduli of curves with non-abelian level structure. R.H. DIJK-GRAAF, C.F. FABER, G.B.M. VAN DER GEER (eds.). *The Moduli Space of Curves*, Birkhäuser, 483–509.

F. OORT, YU. ZARHIN (1995). Endomorphism algebras of complex tori. *Math. Ann.* 303, 11–29.

F. OORT (1995). Complete subvarieties of moduli spaces. W. BARTH ET AL. (eds.). *Abelian Varieties*, De Gruyter, 225–235.

F. OORT (1995). Moduli spaces of abelian varieties in positive characteristic. W. MESSING, V. CRISTANTE (eds.). *Barsotti Symposium in Algebraic Geometry, Perspectives in Math.*, Acad. Press, 253–276.

A.J. DE JONG, F. OORT (1995). *On Extending Families of Curves*, Preprint 930, Universiteit Utrecht.

Aandachtsprogramma Rekenintensieve Methoden in de Stochastiek

S. CHENG, L. PENG, Y. QI (1995). *Almost Sure Convergence in Extreme Value Theory*, Report 9504/A, Erasmus Universiteit Rotterdam.

Y. QI, R.J.G. WILMS (1995). *The Limit Behavior of Maxima Modulo One and the Number of Maxima*, Report 9519/A, Erasmus Universiteit Rotterdam.

S. CHENG, L. PENG, Y. QI (1995). *Ergodic Behavior of Extreme Values*, Report 9524/A, Erasmus Universiteit Rotterdam.

I.S. MOLCHANOV (1995). Statistics of the Boolean model: from the estimation of means to the estimation of distributions. *Adv. Appl. Prob.* 27, 63–86.

I.S. MOLCHANOV (1995). Abstract landmarks and their applications. K.V. MARDIA, C.A. GILL (eds.). *Proc. in Current Issues in Statistical Shape Analysis*, Leeds University Press, 82–87.

I.S. MOLCHANOV (1995). On the convergence of random processes generated by approximations of convex compact sets. *Theory of Probability and its Applications* 40.

I.S. MOLCHANOV, E. OMEY, E. KOZAROVITZKY (1995). An elementary renewal theorem for random compact convex sets. *Advances in Applied Probability* 27, 931–942.

I.S. MOLCHANOV (1995). Set-valued estimators for mean bodies related to Boolean models. *Statistics*.

I.S. MOLCHANOV, D. STOYAN (1995). Statistics of compact sets and random polygons. *Stochastic Models*.

I.S. MOLCHANOV, D. STOYAN (1995). *Statistical Models of Random Polyhedra*, CWI Report BS-R9510.

D. STOYAN, I.S. MOLCHANOV (1995). *Set-valued Means of Random Particles*, CWI Report BS-R9511.

I.S. MOLCHANOV (1995). *A Limit Theorem for Solutions of Inequalities*, CWI Report BS-R9515.

L. HEINRICH, I.S. MOLCHANOV (1995). *Central Limit Theorem for a Class of Random Measures Associated with Germ-grain Models*, CWI Report BS-R9518.

Y.K. GOLUBEV, B.Y. LEVIT (1995). *Distribution Function Estimation: Adaptive Smoothing*, Report 897, Universiteit Utrecht.

Y.K. GOLUBEV, B.Y. LEVIT, A.B. TSYBAKOV (1995). *Asymptotically Efficient Estimation of Analytic Functions in Gaussian Noise*, Report 894, Universiteit Utrecht.

R.D. GILL, B.Y. LEVIT (1995). Applications of the van Trees inequality: a Bayesian Cramer-Rao bound. *Bernoulli* 1, 59–80.

Groot Project Lie-theorie en Speciale Functies

M. HAZEWINKEL (1995). Multiparameter quantum groups and multiparameter R-matrices. *Acta Appl. Math.* 41, 57–98.

P.G.A. FLORIS (1995). Gel'fand pair criteria for compact matrix quantum groups. *Indag. Math. N.S.* 6, 83–98.

H.T. KOELINK (1995). Addition formula for big q -Legendre polynomials from the quantum $SU(2)$ group. *Canad. J. Math.* 47, 436–448.

H.T. KOELINK (1995). Identities for q -ultraspherical polynomials and Jacobi functions. *Proc. Amer. Math. Soc.* 123, 2479–2487.

H.T. KOELINK (1995). The quantum group of plane motions and basic Bessel functions. *Indag. Math. N.S.* 6, 197–211.

H.T. KOELINK, R.F. SWARTTOUW (1995). A q -analogue of Graf's addition formula for the Hahn-Exton q -Bessel function. *J. Approx. Theory* 81, 260–273.

H.T. KOELINK, W. VAN ASSCHE (1995). Orthogonal polynomials and Laurent polynomials related to the Hahn-Exton q -Bessel Function. *Constr. Approx.* 11, 477–512.

T.H. KOORNWINDER (1995). Discrete hypergroups associated with compact quantum Gel'fand pairs. W.C. CONNETT, M.-O. GEBUHRER, A.L. SCHWARTZ (eds.). *Applications of Hypergroups and Related Measure Algebras, Contemp. Math.* 183, Amer. Math. Soc., 213–235.

YU. BESPALOV, B. DRABANT (1995). *Hopf (Bi) Modules and Crossed Modules in Braided Monoidal Categories*, Report 95-18, Universiteit

van Amsterdam.

P.G.A. FLORIS, H.T. KOELINK (1995). *A Commuting q -analogue of the Addition Formula for Disk Polynomials*, Report W95-07, Rijksuniversiteit Leiden.

H.T. KOELINK (1995). *Addition Formulas for q -special Functions*, Report 95-17, Universiteit van Amsterdam.

T.H. KOORNWINDER (1995). *Special Functions and q -commuting Variables*, Report No. 1, Institut Mittag-Leffler.

J.V. STOKMAN (1995). *Multivariable Big and Little q -Jacobi Polynomials*, Report 95-16, Universiteit van Amsterdam.

J.V. STOKMAN, T.H. KOORNWINDER (1995). *Limit Transitions for BC Type Multivariable Orthogonal Polynomials*, Report 95-19, Universiteit van Amsterdam.

P.G.A. FLORIS (1995). *On Quantum Groups, Hypergroups and q -special Functions*, proefschrift, Rijksuniversiteit Leiden.

Academische promoties

In het verslagjaar promoveerden wetenschappelijke onderzoekers die in het kader van de Landelijke Activiteiten Wiskunde hun onderzoek hadden verricht.

- J.A. Loeve; op 22 maart aan de Rijksuniversiteit Leiden op het proefschrift *Markov Decision Chains with Partial Information*.
Promotor: Prof. dr. A. Hordijk.
- J.-P. van Draanen; op 2 mei aan de Katholieke Universiteit Nijmegen op het proefschrift *Models for Simply Typed Lambda-calculi with Fixed Point Combinators and Enumerators*.
Promotor: Prof. dr. H.P. Barendregt.
- Chr. Schweigert; op 15 juni aan de Universiteit van Amsterdam op het proefschrift *Galois and Simple Current Symmetries in Conformal Field Theory*.
Promotor: Prof. dr. R.H. Dijkgraaf.
- B.J.J. Moonen; op 5 september aan de Universiteit Utrecht op het proefschrift *Special Points and Linear Properties of Shimura Varieties*.
Promotor: Prof. dr. F. Oort.
- G.J.M. Marée; op 19 september aan de Landbouwuniversiteit Wageningen op het proefschrift *Sudden Change in Second Order Nonlinear Systems – Slow Passage through Bifurcation*.

Promotores: Prof. dr. ir. J. Grasman en prof. dr. F. Verhulst (UU).

- M.B. Kalsbeek; op 22 september aan de Universiteit van Amsterdam op het proefschrift *Metalogics for Logic Programming*.
Promotores: Prof. dr. J.F.A.K van Benthem en prof. dr. K.R. Apt.
- M.G. Neytcheva; op 27 september aan de Katholieke Universiteit Nijmegen op het proefschrift *Arithmetic and Communication Complexity of Preconditioning Methods*.
Promotor: Prof. dr. A.O.H. Axelsson.
- H.J.M. Hamers; op 29 september aan de Katholieke Universiteit Brabant op het proefschrift *Sequencing and Delivery Situations: a Game Theoretic Approach*.
Promotor: Prof. dr. S.H. Tijs.
- H. Lu; op 10 oktober aan de Katholieke Universiteit Nijmegen op het proefschrift *Forward-Backward Heat Equations and Analysis of Iterative Methods*.
Promotor: Prof. dr. A.O.H. Axelsson.
- J. Lőrinczi; op 6 november aan de Rijksuniversiteit Groningen op het proefschrift *On Limits of the Gibbsian Formalism in Thermodynamics*.
Promotor: Prof. dr. M. Winnink.

BIJLAGE 1

DOELSTELLING EN ORGANISATIE

Doelstelling

De Stichting Mathematisch Centrum (SMC) werd op 11 februari 1946 opgericht door prof. dr. J.G. van der Corput, prof. dr. D. van Dantzig, prof. dr. J.F. Koksma, prof. dr. H.A. Kramers, prof. dr. M.G.J. Minnaert en prof. dr. ir. J.A. Schouten.

De SMC heeft als doelstelling de systematische beoefening van de zuivere en toegepaste wiskunde en de informatica in Nederland te bevorderen.

Doel.

Artikel 2.

- 2.1. De stichting heeft ten doel de systematische beoefening van de zuivere en toegepaste wiskunde en de informatica in Nederland te bevorderen, teneinde daardoor enerzijds de bijdragen van deze gebieden van wetenschap tot de verhoging van het welvaarts- en beschavingspeil in Nederland, anderzijds de bijdrage van Nederland tot de internationale cultuur te vergroten.

Middelen ter bereiking van het doel

Artikel 3.

3. De Stichting tracht haar doel te bereiken door:
- het bevorderen van de onderlinge samenwerking der Nederlandse wiskundigen en informatici;
 - het bevorderen van de samenwerking der Nederlandse wiskundigen en informatici met beoefenaars van andere gebieden van wetenschap, techniek en maatschappelijk leven, waarin de wiskunde en informatica worden toegepast (bij afkorting genaamd aangrenzende gebieden);

menwerking met onderzoekers van 'aangrenzende' wetenschapsgebieden en met collega's uit het buitenland.

- Onderzoekers uit binnen- en buitenland de gelegenheid te geven het instituut van de Stichting te bezoeken.
- Het uitgeven of ondersteunen van wetenschappelijke publicaties.
- Onderzoek in de wiskunde en informatica te laten uitvoeren.
- Het organiseren van cursussen en voordrachten.
- Leiding te geven aan het werk van jonge onderzoekers, bezoeken van (jonge) Nederlandse onderzoekers aan andere onderzoekscentra mogelijk te maken, en talentvolle onderzoekers de mogelijkheid te bieden zich aan onderzoek te wijden.

Belangrijke middelen tot verwezenlijking van de doelstelling zijn:

- Het beheren van een instituut: het CWI (Centrum voor Wiskunde en Informatica), inclusief een bibliotheek en een geavanceerde computerinfrastructuur.
- De coördinatie van de Landelijke Activiteiten Wiskunde (LAW) en de instelling van zogenaamde *Grote Projecten*.
- Deelname in andere samenwerkingsverbanden, zoals bijvoorbeeld European Research Consortium for Informatics and Mathematics (ERCIM) en Research Institute for Applications in Computer Algebra (RIACA).

Organisatie

De Stichting Mathematisch Centrum wordt bestuurd door een Curatorium. Leden van het Curatorium worden op voordracht van onder meer de Stichting Informatica Onderzoek Nederland en de Koninklijke Nederlandse Academie van Wetenschappen

Tabel 1. Uit de statuten van de SMC

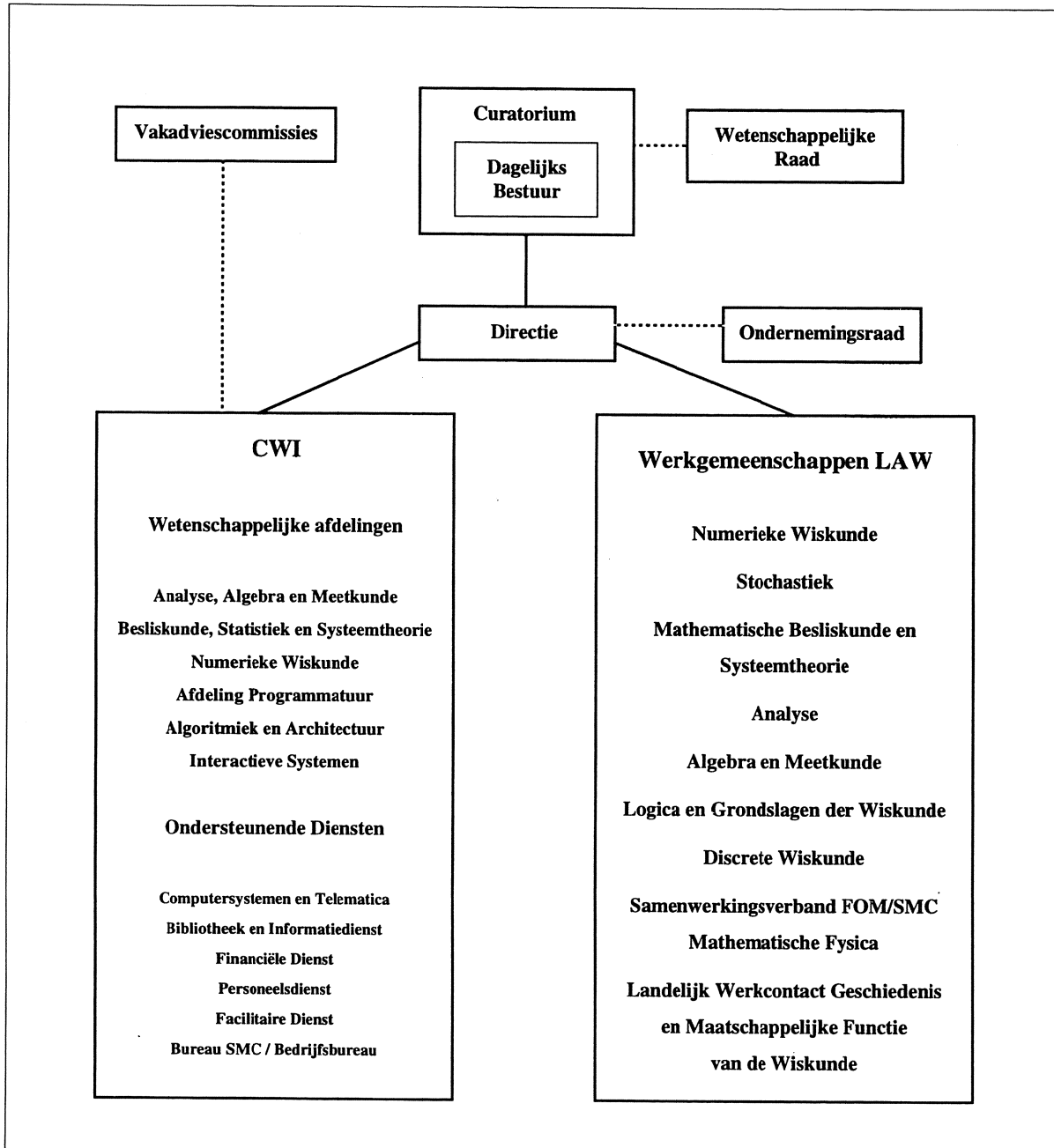
De Stichting tracht haar doel te bereiken door

- Het bevorderen van de samenwerking tussen Nederlandse wiskundigen en informatici, alsook sa-

benoemd. De dagelijkse leiding van de werkzaamheden van de Stichting en haar instituut berust bij de Directie. Een Wetenschappelijke Raad dient het Curatorium en de Directie van advies aangaande het algemene wetenschappelijk beleid.

Onder de Stichting ressorteren het Centrum voor Wiskunde en Informatica (CWI) en zeven werkge-

meenschappen, één samenwerkingsverband, alsmede één landelijk werkcontact. Het CWI telt zes wetenschappelijke afdelingen en zeven ondersteunende diensten. De directie van het CWI wordt bijgestaan door de Wetenschappelijke Beleidsgroep, bestaande uit de chefs van de wetenschappelijke afdelingen.



Tabel 2. Organisatieschema Stichting Mathematisch Centrum per 31 december 1995

BIJLAGE 2

BELEIDSORGANEN VAN DE

STICHTING MATHEMATISCH CENTRUM

Curatorium

Prof. dr. ir. G.Y. Nieuwland voorzitter
Prof. dr. Th.M.A. Bemelmans vice-voorzitter
Ir. C.M.N. Belderbos
Ir. A. Boesveld (tot 1 juni)
Prof. drs. B.K. Brussaard (tot 1 juni)
Ir. L.A.A.M. Coolen (vanaf 1 juli)
Prof. C.H.A. Koster
Prof. dr. J.H. van Lint
Dr. A.H.G. Rinnooy Kan
Prof. dr. A. van der Sluis (tot 1 juni)
Prof. dr. J.H.M. Steenbrink
J.A. Symes
Prof. dr. W.R. van Zwet

Wetenschappelijke Raad

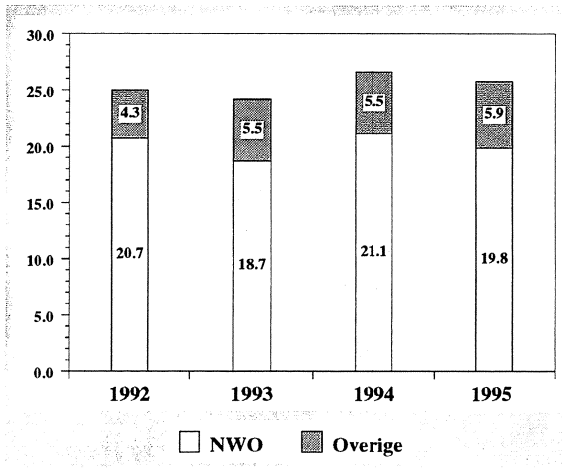
Prof. dr. ir. J.H.A. de Smit voorzitter
Prof. dr. G. van Dijk vice-voorzitter
Prof. dr. E.J.N. Looijenga
Prof. dr. A. Schrijver
Prof. dr. ir. P. Wesseling

Directie

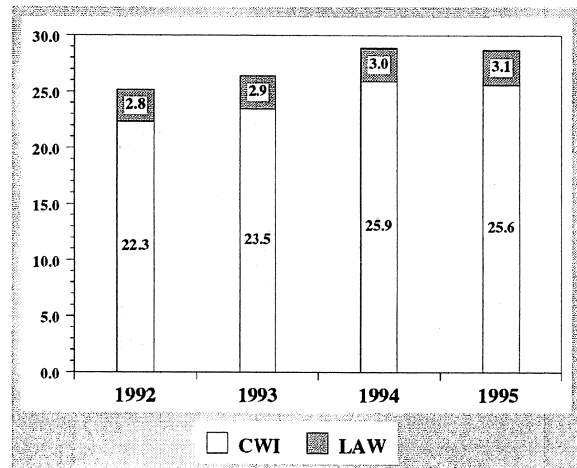
Dr. ir. G. van Oortmerssen algemeen directeur

BIJLAGE 3

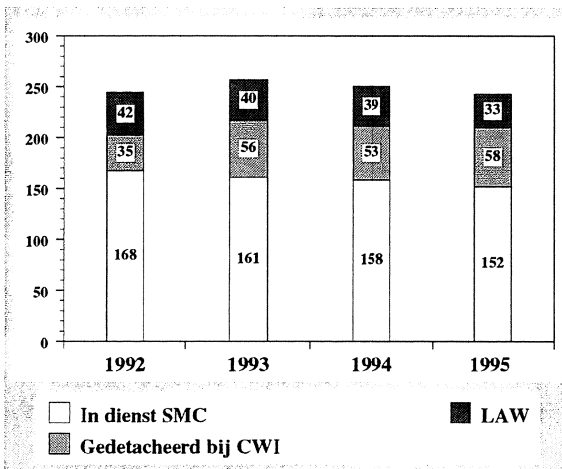
FINANCIËN, PERSONEEL EN PROMOTIES



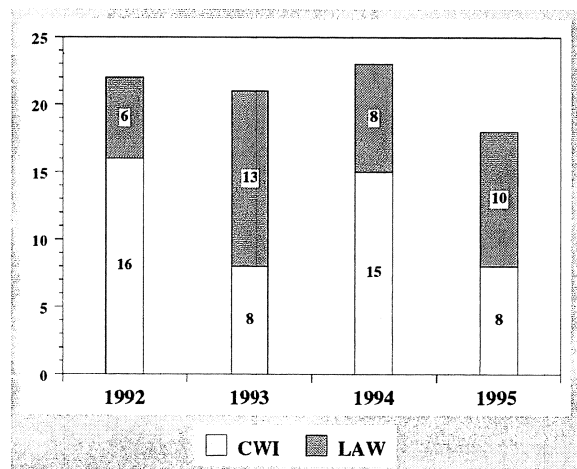
Tabel 1. Inkomsten in Mf (exclusief LAW)



Tabel 2. Uitgaven in Mf



Tabel 3. Personeel einde jaar in fte



Tabel 4. Academische promoties