Kennisnetwerken

Vrijdag 5 oktober 2001

CWI, Kruislaan 413, 1098 SJ Amsterdam

Over dit thema organiseert het
Centrum voor Wiskunde en Informatica
zijn jaarlijkse manifestatie

CWI IN BEDRIJF
'01

Kennisnetwerken

In de kenniseconomie is een intensieve samenwerking tussen kennisinstellingen en bedrijven van levensbelang. Resultaten van onderzoek moeten snel doorstromen naar de markt, en onderzoekers moeten geïnspireerd worden door contacten met de praktijk. Zoals de AWT Verkenningscommissie *Kennis voor de Netwerkeconomie* stelde: "het moet gaan zinderen tussen de kennisinstellingen en de bedrijven". En dat is precies het doel van de jaarlijkse manifestatie **CWI in Bedrijf**, met dit jaar als centraal thema **Kennisnetwerken**.

Onderzoek en kennisoverdracht vindt steeds meer plaats in samenwerkingsverbanden en dit leidt in toenemende mate tot netwerkorganisaties. Het CWI participeert in diverse netwerken: het Wetenschap & Technologie Centrum Watergraafsmeer, de Kenniskring Amsterdam, het Telematica Instituut, en internationaal bijvoorbeeld in het Europese onderzoeksconsortium ERCIM en het World Wide Web Consortium, W3C.

Door participatie in kennisnetwerken kunnen bedrijven de grote groeikansen voor de komende jaren beter benutten: ambient intelligence, embedded systemen, mobiel internet, software renovatie, e-commerce, intelligent agents, multimediale technologiëen... De macro-economische invloed hiervan kan nauwelijks overschat worden: voor de ICT-sector voorspelt het NPB een marktgrootte van circa 40 miljard euro in 2002.

De volgende sprekers zullen het thema belichten:

Dr. ir. G. van Oortmerssen is Algemeen Directeur van het Centrum voor Wiskunde en Informatica (CWI) in Amsterdam. Hij zal spreken over de ontwikkelingen van het onderzoek van het CWI en de rol die kennisnetwerken daarbij spelen.

Drs. R. Bemer (Ministerie van Economische Zaken) is Directeur-Generaal voor Innovatie bij het Ministerie van Economische Zaken. De heer Bemer zal spreken over het nationaal innovatiesysteem.

Mw. E. Colinet (DG XII, EU) is Directeur van de Centers and Networks of Excellence bij Directoraat-generaal XII van de EU. Mevrouw Colinet zal spreken over de plannen voor kennisnetwerken in het nieuwe kaderprogramma van de EU.

Dhr. A. Reuver (IBM) is Directeur externe betrekkingen van IBM Nederland. Hij zal spreken over ervaringen en ontwikkelingen vanuit het bedrijfsleven rondom samenwerking met kennisinstellingen.

Drs. A.H.J. Risseeuw (ex-Getronics) was voorzitter van de ICT Verkenningscommissie van de AWT (Adviesraad voor Wetenschap en Technologie). Hij zal spreken over het advies van de Verkenningscommissie.

In de ochtend zal een tiental voordrachten worden gegeven over CWI-onderzoek in parallelle sessies. Deze voordrachten hebben een sterk demonstrerend karakter: steeds zal worden aangegeven hoe fundamenteel onderzoek uiteindelijk leidt tot praktische toepassingen.

Bovendien is een aantal demonstraties gepland, waar u een indruk kunt krijgen van wat er op het CWI gebeurt, en waar u contact kunt leggen met CWI-onderzoekers.

Programma: *in de ochtend parallelle sessies*

9.00 Ontvangst

ochtend

Zaal Z011

10.00 Dr.ir. Arjen de Vries, *Zoeken naar een speld in de multimediale hooiberg*
10.30 Steven Pemberton, *XHTML: HTML in XML*
11.00 Prof.dr. Michel Mandjes, *Quality of Service in Future Networks*
11.30 Pauze
12.00 Dr. Jacco van Ossenbruggen, *Multimedia en het Semantic Web*
12.30 Dr. David van Bragt, *Hoe elektronische advertenties en verkoop de honger naar informatie kunnen stillen*

Zaal Z009

10.00 Dr. Jaco van de Pol, *Gedistribueerde architectuur onder vuur*
10.30 Dr.ir. Ben Schouten (MxVision), *Oog op ICT: Visuele intelligentie en de markt*
11.00 Drs.ir. Joost Visser, *Large-scale Software Transformation*
11.30 Pauze
12.00 Drs. Joke Blom, *De Silicon Cell*
12.30 Dr. Ute Ebert, *Elektrische ontladingen - patroonformatie tussen esthetiek en toepassingen*

middag

13.00 Lunch
14.00 **Dr.ir. G. van Oortmerssen**, *De Kennisnetwerken van het CWI*
14.30 **Drs. R. Bemer**, *Het Nationaal Innovatiesysteem*
15.00 **Mw. E. Colinet**, *Networking mechanisms foreseen in the Framework Programme 2002–2006, with special emphasis on the Networks of excellence*
15.30 Pauze
16.00 **Dhr. A. Reuver**, *Samenwerking met kennisinstellingen: Ervaringen en ontwikkelingen vanuit het bedrijfsleven*
16.30 **Drs. A.H.J. Risseeuw**, *Het advies van de ICT-verkenningscommissie AWT*
17.00 Borrel

Gedurende de pauzes kunt u onder andere de volgende stands bezoeken

Quality of Service in Future Networks
Elektronische advertenties en intelligent agents
W3C Kantoor Nederland
XHTML: HTML in XML
Dynamisch generen van presentaties
Approaching the Limit with Computer Algebra
Geometrische methoden voor klimaat en weersimulaties
Content-Based Image Retrieval

CWI spin-off bedrijven:

Software Improvement Group - software renovatie
MxVision - visuele datamining op UMTS
Eidetica - knowledge management systems
Epictoid - facial animation
Oratrix - multimedia authoring & player systems

Wat is het CWI?

Het Centrum voor Wiskunde en Informatica (CWI) is een onafhankelijke non-profit organisatie die tot doel heeft het wiskunde- en informatica-onderzoek te bevorderen.

Het CWI heeft een tweeledige missie:

- Het uitvoeren van grensverleggend onderzoek op het gebied van wiskunde en informatica
- De overdracht van nieuwe kennis in deze gebieden naar de maatschappij in het algemeen en naar bedrijfsleven en industrie in het bijzonder.

Het CWI-onderzoek vindt plaats aan het front van de wetenschap; het levert fundamentele bijdragen aan de voortgang van de wiskunde en de informatica. Tegelijkertijd heeft het CWI een scherp oog voor praktische toepassingen van dit fundamentele onderzoek. De onderzoeksthema's worden strategisch gekozen, en bij de selectie van nieuwe projecten wordt scherp gelet op de maatschappelijke bruikbaarheid van de kennis.

Het CWI neemt deel in het Telematica Instituut en het Wetenschap & Technologie Centrum Watergraafsmeer (WTCW), en stond aan de wieg van het European Research Consortium for Informatics and Mathematics (ERCIM). Het CWI participeert in bijna honderd nationale en internationale onderzoeksprojecten en werkt samen met de bestaande onderzoeksscholen op het gebied van wiskunde en informatica. Ook het beheer van het Nederlandse Kantoor van het World Wide Web Consortium (W3C) wordt gedaan door het CWI. Contractonderzoek voor bedrijven neemt een grote plaats in.

Als onderdeel van zijn beleid ten aanzien van technologieoverdracht voert het CWI een actief spin-off beleid, dat de laatste jaren zorgt voor een gestage stroom van nieuwe ondernemingen.

Deelname aan CWI in Bedrijf is kosteloos. Voor nadere informatie kunt u contact opnemen met Wilmy van Ojik, tel. 020–592 4009, fax 020–592 4199, e-mail `Wilmy.van.Ojik@cwi.nl`. U kunt natuurlijk ook onze website bezoeken (`www.cwi.nl/CiB`) waar eveneens alle informatie over deze dag is terug te vinden.

CWI

Centrum voor Wiskunde en Informatica

Centre for Mathematics and Computer Science

Frontier research for practical applications

CWI is the national research institute for mathematics and computer science, located in Amsterdam, The Netherlands, at the Amsterdam Science & Technology Centre (WTCW). Since its foundation in 1946 the institute has aquired a prominent position in the research world.
CWI is a non-profit organisation, operating on a budget of 14 million EUR (70% basic funding from NWO, 30% from national programmes, EU programmes, and commissions). Its 210 employees include 160 researchers, 20 of them holding also positions as university professors.

The mission of CWI is twofold:
- to perform frontier research in mathematics and computer science;
- to transfer new knowledge in these fields to society in general, and trade & industry in particular.

www.cwi.nl

CWI Research - some application areas

CWI carries out both fundamental explorative research and research with concrete applications in mind. Quantum computing is a fine example of the first. Some major application areas are detailed below.

Traffic

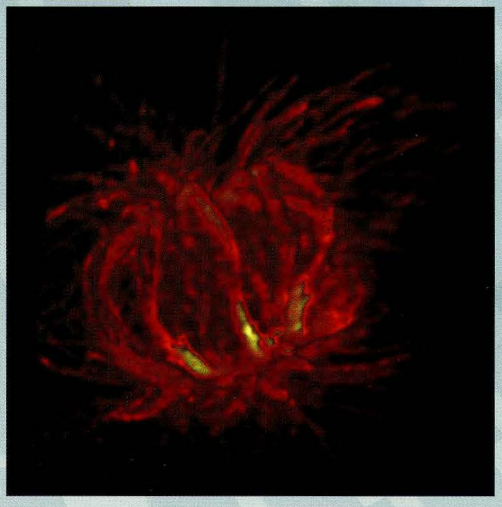
Traffic increases everywhere in density and in complexity. A scientific approach is needed to deal with the resulting problems. CWI developed a new tool for designing **railroad timetables** for Dutch Rail, which operates one of the world's most complex railroad systems. The resulting expertise and software is now being utilized on a European scale. Traffic in **telecommunication networks** is studied by developing and applying queueing theory for integrated services of voice, video, and data, each with different traffic characteristics and customer requirements. For **motorway networks** around urban centres there is a need for network control aiming at optimising travel costs for the users. CWI developed control measures for the Amsterdam ringroad and shares its expertise in an EU project.

Photo: Rijkswaterstaat, Meetkundige Dienst Afdeling Grafische Technieken, Delft: **Motorway network control**

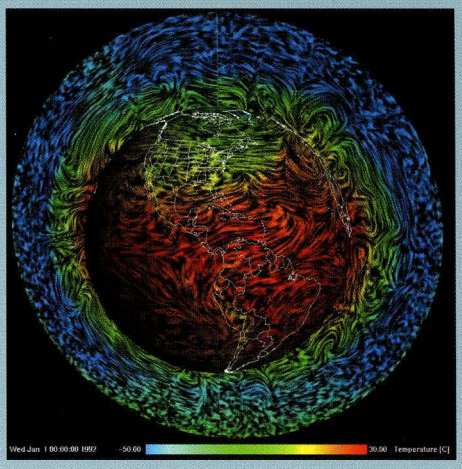
Visual information

In understanding complex processes, visualisation is a most useful tool. CWI researchers have developed **interactive visualisation** tools and applied them to turbulent phenomena and the modeling of biological processes in cells. CWI developed software based on **graph visualisation** in order to get more insight into concurrent, distributed computation processes. Sending and searching **images across the Web** requires new ways of compression, transmission, indexing and retrieval. CWI focuses on 'multi-resolution' methods, including fractal, wavelet and morphological methods. Furthermore we use feature detectors to simplify and speed up queries in large, distributed **multimedia databases**, such as the Web.

RSA-155 =109417386415
= 1026395928297411057



Source CWI: **Cell division during mitosis**



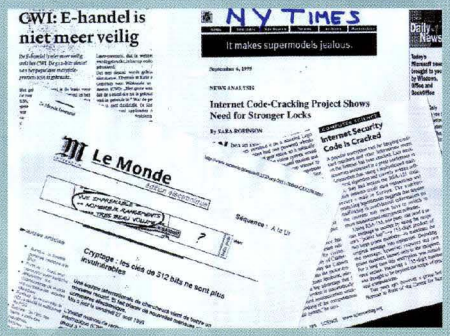
Source CWI: **Global atmospheric models**

Natural systems

Pollution of air, water, and soil is still a major concern in our society. To learn more about long-term effects, CWI developed new methods to solve the very complex underlying equations. Applications include studies of smog formation, the spread of waste by rivers into the North Sea, and salt water intrusion into fresh water reservoirs. CWI's experience with computation of air flows around aircraft wings is now directed to computation of the optimal shape of **ship hulls,** by simulating a complete ship in free surface waves. This may lead to considerable energy savings. Furthermore CWI studies the mathematical equations underlying several **biological systems** and their numerical solution, often aided by visualisation tools. Examples include the development of neuronal connections in the nervous system and the growth of phytoplankton.

The Web

CWI has been involved from the very beginning in the development of the Internet and the World Wide Web. The institute was the **first non-military Internet site in Europe** and acted for several years as the gateway between the USA and Europe. It created the **domain registration** system for The Netherlands, which is extensively used abroad as well. CWI actively participates in several activities of the **World Wide Web Consortium**. Apart from image processing and retrieval, CWI research focuses on the following Web applications: **Python** - an interpreted, interactive, object-oriented language (comparable to Java), the specification language **SMIL** for multimedia authoring; **style sheets** for special purposes such as serving handicapped people; and **XHTML** - a bridge between HTML and the far more flexible and extensible XML. SMIL and XHTML were developed in W3C Working Groups to which CWI made crucial contributions. Coding techniques to protect Internet traffic rely on the difficulty to retrieve large prime numbers from their product. CWI explores the fastest **factoring methods** to determine the coding's safety limit. The factoring of RSA-155 was world news.



Source CWI: **Internet security**

0527421809707322040357612003732945449205990913842131476349984288934784717997257891267332497625752899781833797076537244027146743531593354333897
2054196573991675900716567808038066803341933521790711307779 * 106603488380168454820927220360012878679207958575989291522270608237193062808643

Software engineering

A typical industrial or governmental organisation maintains millions of lines of old programming code. **Renovation of this 'legacy' software** is economically very important, and in most cases also the only way out. With its extensive knowledge of mathematically rigorous construction methods, CWI develops practical renovation tools and languages. Another point of worry is the risk of calamities due to **errors in software systems**, such as the exploding Ariane rocket in the mid-nineties. This can be prevented by the **verification of software** built into physical devices (**embedded software**). CWI checked the control software of a railroad yard and of video devices. Quite another field of interest is the study of emerging markets like **E-commerce**, with many interacting agents and largely unknown behaviour. CWI develops evolutionary methods based on natural principles like 'survival of the fittest' to explore such systems.

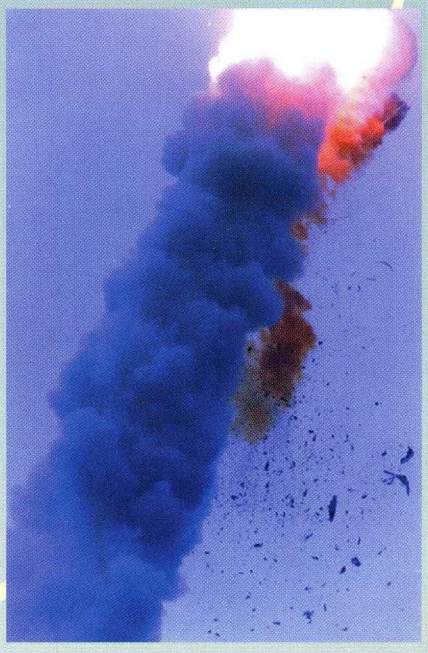
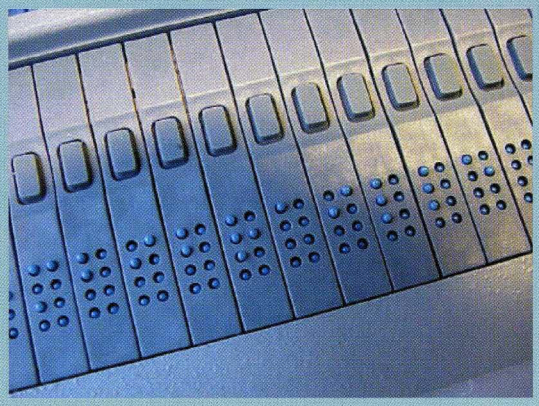


Photo: ESA: **Software should be error-free**

Frontier research, knowledge transfer

CWI performs fundamental research on themes which are derived from societal needs and are continuously renewed. This ranges from explorative areas like quantum computing to concrete questions like optimal railroad timetables. There is close cooperation with **academia, industry,** and **knowledge and financial institutions.** CWI participates in the **Telematics Institute** and the **WTCW** (Amsterdam Science & Technology Centre). Results are made available through publications, lectures, staff mobility, contract research, and the creation of **spin-off companies** based on results of CWI research. An active policy which started in the 1990s, has led to ten such companies in fields including datamining, software improvement, and several aspects of the Web (security, design, multimedia, animation). CWI also organizes an annual networking event for the Trade & Industry sector.

W3C



Internet accessibility for impaired people

Photos: Stichting Bartiméus

International cooperation

A substantial part of the research is performed in international collaborative frameworks. CWI participates in **fourteen EU projects** in ICT and related areas. It also plays an active role in the World Wide Web Consortium (W3C), defining Web standards in several Working Groups. The **W3C Office in The Netherlands** is managed by CWI, and the institute hosted the Ninth International World Wide Web conference in Amsterdam. CWI is a founding member of the European Research Consortium for Informatics and Mathematics (ERCIM) and keeps a prominent position in it. The objective of **ERCIM** is to promote research in information technology and related mathematics in Europe, and to intensify contacts between research organisations and industry. At present leading research institutions from thirteen European countries have joined ERCIM, representing over 7000 researchers.

CWI
P.O. Box 94079,
1090 GB Amsterdam,
The Netherlands
+31 20 592 9333
+31 20 592 4199 (fax)
www.cwi.nl

Annette Kik
+31 20 592 4248
E-mail: kik@cwi.nl

Henk Nieland
+31 20 592 4092
E-mail: henkn@cwi.nl

September 2001

Centrum voor Wiskunde en Informatica

CWI

CLUSTER Information Systems

THEME Networks and Logic - Optimization and Programming

PROGRAMMEREN MET CONSTRAINTS

Verscheidene berekeningsproblemen kunnen heel natuurlijk worden omschreven door middel van eisen ('constraints') waaraan een oplossing moet voldoen. In dergelijke situaties is het genereren van die eisen even belangrijk als het oplossen zelf. 'Constraint programming' is een alternatieve benadering van programmeren waarbij deze manier van rekenen wordt gebruikt. Het programmeerproces bestaat dan uit het genereren van constraints en de oplossing daarvan door middel van algemene of domein-specifieke methodes. Bij het CWI bestuderen we zowel de grondbeginselen als de toepassingen van constraint programming.

In de jaren tachtig ontstond het idee van constraint programming uit het ontwerpen van verschillende zogenoemde constraint logic programmeertalen. Deze talen berusten op het begrip 'logische variabele', hetgeen betekent dat uitdrukkingen met niet geïnitialiseerde variabelen kunnen worden toegewezen aan andere variabelen. Een dergelijk gebruik van variabelen (als onbekende) is gebruikelijk in de wiskunde.

In de jaren negentig werden er op verschillende terreinen nieuwe toepassingen gevonden voor constraint programming. Zo zijn constraints gebruikt bij interactieve grafische systemen om meetkundige samenhang uit te drukken in de analyse van scenes, en in de elektrotechniek voor het testen en toetsen van circuitontwerpen, de berekening van de modellen (layouts) en het opsporen van fouten. Recente toepassingen betreffen het genereren van coherente muziekprogramma's op de radio en het herstel van ontwerpen in software engineering. In de besliskunde en de numerieke analyse bleek dat programmeren met constraints soms efficiëntere oplossingen bood voor complexe problemen dan de gebruikelijke methoden konden leveren. Voorbeelden zijn het maken van roosters onderworpen aan complexe, niet-lineaire beperkingen, of het oplossen van algebraïsche vergelijkingen met een gegarandeerde precisie (zie de grafiek op de achterkant).

Constraint programming omvat uiteenlopende vakgebieden zoals lineaire algebra, lineaire en geheeltallige programmering en globale optimalisering. In deze gebieden ontwikkelde technieken zijn meestal beschikbaar in de vorm van domein-specifieke methodes, vaak 'constraint solvers' genoemd. Daarbinnen zijn de gespecialiseerde algoritmen, zoals die voor lineaire programmering, direct beschikbaar.

Roosters voor sportcompetities kunnen met behulp van constraint programming zeer efficiënt worden geprogrammeerd (foto ANP).

De algemene methodes daarentegen zijn gericht op de generieke technieken voor het beperken van de zoekruimte en op specifieke zoekmethodes. Het beperken van de zoekruimte heet 'constraint propagation', en wordt tot stand gebracht met behulp van algoritmen die proberen de combinatorische explosie te beperken. Welk type constraint propagation wordt gebruikt hangt af van de initiële keuze van constraints en domeinen, en van de toepassingen. Verscheidene methoden en technieken uit de toegepaste wiskunde en de informatica zijn eigenlijk voorbeelden van constraint propagation.

Op het CWI is een algemeen raamwerk ontwikkeld om de constraint propagation algoritmen op een uniforme manier te beschrijven. Hiermee kunnen wij deze algoritmen ontwikkelen, aanpassen, vergelijken, correctheid bewijzen en combineren. Bovendien blijken deze algoritmen hierdoor eenvoudig te parallelliseren.

Constraint programming biedt een andere kijk op programmeren. Het stoelt op een twee-lagen architectuur waarin constraints kunnen worden gehanteerd door middel van een ingebouwd constraint propagation mechanisme en 'hard-wired' constraint solvers. Ook zijn er voorzieningen voor het genereren en manipuleren van constraints en verschillende ingebouwde hulpmiddelen bij het zoeken. Een en ander leidt tot een radicaal andere programmeerstijl.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telephone +31(0)20 592 9333 Telefax +31(0)20 592 4199 http://www.cwi.nl

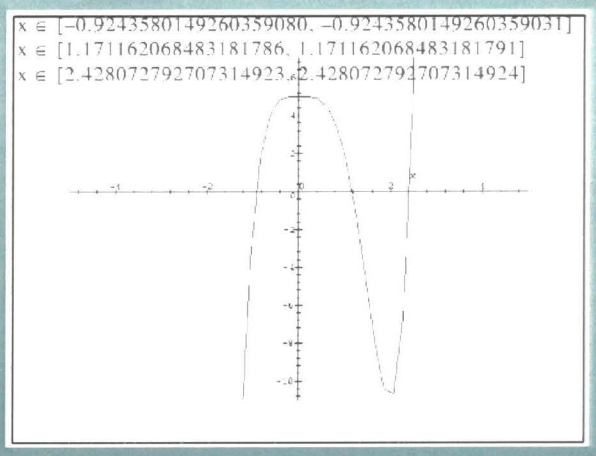
Neem bijvoorbeeld de volgende puzzel die een unieke oplossing heeft. Gevraagd wordt iedere letter te vervangen door een cijfer zodanig dat de som

```
  SEND
+MORE
 MONEY
```

uitkomt. Een oplossing in de constraint logic programmeertaal ECL^{i}PS^e spreekt bijna vanzelf en lijkt opvallend veel op de formele specificatie van het probleem:

```
send(List):-
    List = [S,E,N,D,M,O,R,Y],
    List :: 0..9,
    alldifferent(List),
    1000*S + 100*E + 10*N + D +
    1000*M + 100*O + 10*R + E
 #= 10000*M + 1000*O + 100*N + 10*E + Y,
    M ## 0,
    S ## 0,
    labeling(List).
```

Een van de uitdagingen op het gebied van constraint programming is hoe we het gebruik van constraints kunnen opnemen in de gebruikelijke programmeertalen als Pascal, C, of Java, waarin de variabelen fundamenteel anders worden gebruikt dan in bovenstaand programma. Daartoe is op het CWI een imperatieve programmeertaal Alma-0 ontworpen en geïmplementeerd, ontstaan uit een niet-triviale subset van de Modula-2 taal door toevoeging van slechts enkele 'inbouwsels' die het zoeken mogelijk maken. In Alma-0 zijn beide soorten gebruik van variabelen toegestaan: als onbekende of als variabele grootheid. Sommige Alma-0 programma's zijn vrijwel identiek aan de specificaties.
Lopend onderzoek betreft de toevoeging van logische variabelen en constraints aan Alma-0.



Met behulp van constraint programming kan men algebraïsche vergelijkingen oplossen met gegarandeerde precisie. De grafiek toont de functie

$$2 * x^5 - 5 * x^4 + 5$$

en haar nulpunten.

Voor nadere informatie over dit CWI onderzoek:
www.cwi.nl/pna1

Prof.dr. K.R. Apt
Telefoon: 020-592 4135
E-mail: K.R.Apt@cwi.nl

september 2001

DOMEIN-SPECIFIEKE TALEN

Domein-specifieke talen (domain-specific languages of DSLs) bestrijken, in afwijking van hogere programmeertalen, een beperkt toepassingsgebied. Door de notaties en concepten van een toepassingsgebied in een DSL ter beschikking van de programmeur te stellen wordt het mogelijk applicatieprogramma's korter en directer uit te drukken dan in een programmeertaal voor algemeen gebruik. De DSL compiler beschikt over de vereiste kennis van het toepassingsgebied en kan de DSL bijvoorbeeld vertalen naar executeerbare code en bibliotheekroutines, database transacties, of HTML formulieren aanroepen. Het CWI ontwikkelt tools en methoden ter ondersteuning van het effectieve gebruik van DSLs binnen bestaande software engineering projecten.

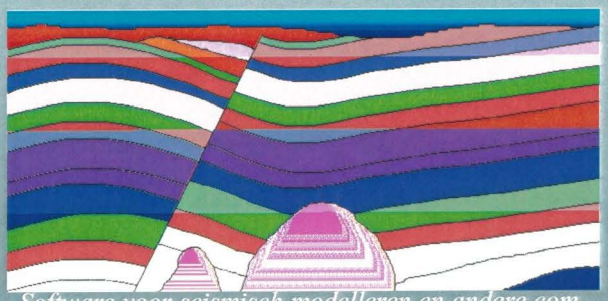
Voorbeelden

Een bekend voorbeeld van een DSL is HTML, dat de laatste jaren faam heeft verworven als opmaaktaal voor hypertext op het web. Een andere veel gebruikte DSL is Backus-Naur Form (BNF) om grammatica's van bijvoorbeeld programmeertalen en DSLs te beschrijven. Door hun aard zijn DSLs echter veelal onbekend buiten een kleine kring van domeinspecialisten. De hardware beschrijvingstaal VHDL bijvoorbeeld is een belangrijk hulpmiddel voor chipontwerpers, maar daarbuiten grotendeels onbekend.

CWI is betrokken geweest bij het ontwerp van Risla, een DSL voor financial engineering ontwikkeld door CAP Gemini en MeesPierson. Op basis van een beschrijving van de karakteristieken van een renteproduct, zoals een lening, *swap* of *future*, genereert de Risla compiler datastructuren in VSAM formaat, data invoerschermen in CICS formaat en COBOL routines om modificaties in het product te loggen of managementinformatie te produceren.

Voordelen

Het gebruik van een DSL heeft veel software engineering voordelen. Aangezien de taal aansluit bij de notaties en concepten die in het toepassingsgebied in zwang zijn, heeft hij een grote uitdrukkingskracht binnen dat gebied. Bovendien hoeft de DSL compiler geen willekeurige programma's aan te kunnen, maar



Software voor seismisch modelleren en andere computational modelling toepassingen profiteert van Sophus, een domeinspecifieke programmeerstijl die wordt ontwikkeld bij CWI en de Universiteit van Bergen, Noorwegen.

kan hij domein-specifieke optimalisaties toepassen tijdens codegeneratie. Deze factoren leiden tot een productiviteitsverbetering en een kortere introductietijd voor nieuwe applicatiesoftware. Dankzij de toepassing van Risla kon MeesPierson de productietijd van nieuwe financiële producten verlagen van 3 maanden naar 3 weken.

Ontwikkeling van DSLs

Ontwikkeling van nieuwe domein-specifieke talen is niet gemakkelijk. Het vereist zowel kennis van het applicatiegebied als expertise op het gebied van taalontwerp. De drempel is dus hoog, waardoor veel gebruikers vasthouden aan hun applicatiebibliotheek, ook als deze wat betreft notaties en functionaliteit te kort schiet.

CWI kan hier de unieke 'ASF+SDF Meta-Environment' inzetten. Deze vermindert de vereiste taalontwerpexpertise en verlaagt daarmee de drempel voor ontwerp en implementatie van DSLs. De invoer voor de Meta-Environment bestaat uit beschrijvingen van diverse aspecten van de te ontwikkelen DSL, zoals de grammatica en de vertaling van DSL constructies naar aanroepen van een COBOL applicatiebibliotheek. Uit deze beschrijvingen genereert de Meta-Environment een implementatie en andere programmeerhulpmiddelen voor de DSL in kwestie.

Bovendien heeft CWI een ruime ervaring op het gebied van domein engineering. Dit is het in kaart brengen en ordenen van eerder opgedane ervaring met het bouwen van systemen in een bepaald toepassingsgebied. Het resultaat is een domeinmodel dat de overeenkomsten en verschillen tussen sofwaresystemen

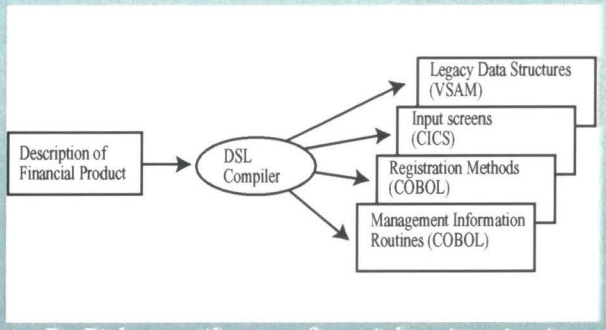
binnen het gegeven gebied beschrijft. Op basis van dit model kan de domeiningenieur een DSL voor dat toepassingsgebied ontwerpen.

Language Design Assistants

Language Design Assistants die significant meer kennis van DSL ontwerp bezitten dan de huidige taalontwerpsystemen zouden de drempel voor DSL ontwerp nog verder kunnen verlagen. Dit is een perspectief op de langere termijn waaraan CWI werkt. De gebruiker die een Language Design Assistant gebruikt selecteert voor zijn doel geschikte taalfragmenten uit een bibliotheek, past ze aan en stelt ze samen tot steeds grotere taalfragmenten.

Samenwerking

CWI voert een vierjarig onderzoeksproject uit op het gebied van DSLs dat wordt gesubsidieerd door het Telematica Instituut. In het kader hiervan onderzoekt CWI methoden, tools en case studies die het Telematica Instituut kunnen helpen om te profiteren van op domein-specifieke talen gebaseerde softwareconstructie. CWI heeft op het gebied van DSLs samengewerkt met verscheidene industriele partners waaronder Lucent, CAP Gemini en MeesPierson.



De Risla compiler voor financial engineering is ontwikkeld door het CWI, in samenwerking met CAP Gemini en MeesPierson.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/sen1/

dr. A. van Deursen en dr. J. Heering
Telefoon 020-5924075 / 020-5924130
E-mail: Arie.van.Deursen@cwi.nl,
Jan.Heering@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

CONTENT-BASED IMAGE RETRIEVAL EN PROCESSING

Beelden zijn een zeer belangrijke bron van informatie voor ons. Aangezien beeld- en video-databanken spectaculair in omvang blijven groeien, wordt het noodzakelijk om bij het terugzoeken en verwerken van visueel materiaal rekening te houden met de beeldinhoud. Onderzoekers aan het CWI werken aan systemen die deze beeldinhoud autonoom kunnen analyseren en gebruiken bij verdere verwerking.

Een groot percentage van de bestanden die momenteel in multimedia-databanken wordt opgeslagen bestaat uit beeld- of video-materiaal; de omvang van dit soort databanken groeit spectaculair. Maar terwijl het steeds makkelijker en goedkoper wordt om beelden te verzamelen, wordt het daarentegen steeds moeilijker om deze collecties van visueel materiaal efficiënt te doorzoeken. Aangezien het dikwijls onmogelijk is om een plaatje met enkele sleutelwoorden te omschrijven, zou men bij het indexeren en terugzoeken van beelden het liefst direct gebruik maken van de beeldinhoud. Met andere woorden, in plaats van de computer te vragen het plaatje *AK-C-4355.jpg* te tonen, wil men eerder de zoekrobot de opdracht geven een figuur te zoeken waarop bijvoorbeeld de *3-dimensionale structuur van een DNA-molecuul* te zien is. Er zijn tal van andere mogelijke toepassingen. Denk maar aan een binnenhuis-architect die op zoek is naar kunstwerken om het nieuw ingerichte kantoor van zijn cliënt mee op te vrolijken. Hij zou dan het systeem kunnen vragen om kleurrijke abstracte schilderijen te vinden. In een medische toepassing kan men zich voorstellen dat een patholoog alle dossiers wil nakijken van patiënten wier biopsie dezelfde rare stervormige cellen vertoonden die hij in de microscopische sectie van zijn huidige patiënt terugvindt.

Elk van de bovenstaande scenario's illustreert de noodzaak van 'inhoudsbewuste visie systemen' die de gebruiker kunnen helpen om grote beeldbestanden te doorzoeken door alle duidelijk irrelevante plaatjes op voorhand uit te sluiten. Op die manier krijgt het zoeksysteem als het ware een paar automatische ogen waarmee het snel grote beelddatabanken kan scannen en een eerste pre-selectie kan maken. Doordat de menselijke gebruiker zich hierdoor niet langer een weg hoeft te banen door een grote hoeveelheid van irrelevante 'hits' wordt het zoekproces veel efficiënter. Het is echter duidelijk dat zo'n systeem alleen maar nuttig kan zijn als het sterk adaptief is. Immers, wat als 'interessant', of 'relevant' wordt beschouwd zal sterk

Interactieve definitie van beeldgelijkenis. Links: de interface laat 5 plaatjes zien, gegroepeerd volgens zijn huidige model van beeldgelijkenis. Rechts: de gebruiker kan de plaatjes hergroeperen op het scherm tot een betere sortering door een drag-en-drop operatie. Als bijvoorbeeld het plaatje linksboven de gebruiker meer doet denken aan bergen, dan sleept hij het naar rechts. De volgende iteratie selecteert kenmerken om deze nieuwe gelijkenis zo getrouw mogelijk te reproduceren.

verschillen van toepassing tot toepassing. Het is daardoor onmogelijk om met vaste relevantie-maten te werken.

Om dit probleem te omzeilen werken CWI-onderzoekers van het PNA4-subthema Content-Based Image Retrieval (als coördinator van het EU-project FOUNDIT) aan de ontwikkeling van een zoekrobot die niet over voorgeschreven relevantie-maten beschikt maar deze 'al doende leert' op basis van voorbeelden en tegenvoorbeelden die worden aangereikt door de gebruiker. Het systeem kijkt toe hoe de gebruiker een klein aantal beelden classificeert als gelijkend en/of relevant en bepaalt vervolgens welke visuele beeldkarakteristieken het best correleren met de geobserveerde classificatie. Hiermee wordt een mathematisch model geconstrueerd dat voorspelt welke beelden in de databank het meeste kans hebben om relevant te zijn en deze worden dan aan de gebruiker aangeboden voor een volgende feedback-cyclus. Deze mathematisch modellen zijn gebaseerd op recent ontwikkelde niet-lineaire technieken voor dimensiereductie en probabilistische classificatiemodellen.

Het grote voordeel van deze aanpak is dat de gecompliceerde wiskunde voor de gebruiker verborgen blijft waardoor de interactie met de zoekrobot op een heel natuurlijke en transparante manier geschiedt. Beelden die de gebruiker als gelijkend beoordeelt, worden op het scherm eenvoudigweg naar elkaar toe gesleept, en of plaatjes al dan niet als relevant moeten worden beschouwd wordt aangegeven door erop te klikken. Dit soort van transparante interactie is erg belangrijk in toepassingen zoals e-commerce waar men er niet van uit kan gaan dat de klant vertrouwd is met de technische begrippen waarop zulke visie- en zoeksystemen zijn gebaseerd.

Visuele datamining is ook de focus van *MxVision*, een nieuw CWI spin-off bedrijf. MxVision ontwikkelt en produceert visueel intelligente software. Als gevolg van het onstaan van nieuwe media zoals Internet, mobiele telefonie (UMTS), interactieve televisie en digitale camera,s vinden nieuwe wetenschappelijke ontwikkelingen nieuwe toepassingen.

MxVision voorziet in software oplossingen die visuele inhoud kunnen beheersen. Voorbeelden hiervan zijn:

- Digitaal copyright: merkbescherming door het automatisch opsporen en lokaliseren van logo's en andere objecten met copyright
- Sport en entertainment: automatische selectie en detectie van (belangrijke) momenten in sportwedstrijden voor UMTS telefoons
- Reclame: visuele inhoud aangepast aan de persoonlijke, culturele of commerciële voorkeuren van de doelgroep (digitale reclameborden)
- Embedded software voor videocamera's.

Samenwerking: Universiteiten van Leuven en Gent (België), Sophis, Universiteit van Amsterdam.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/pna4/, www.mxvision.nl

Dr. E.J. Pauwels, Dr.ir. B.A.M. Schouten
Telefoon: 020 - 592 4225, 592 4288
E-mail: Eric.Pauwels@cwi.nl,
B.A.M.Schouten@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

PATROONVORMING IN ONTLADINGEN

Bliksem is de indrukwekkendste vorm van elektrische ontlading in de natuur. Zo'n ontlading bestaat uit een elektrische stroom door materiaal dat normaal niet geleidend is. De geleiding komt tot stand door blootstelling aan sterke elektrische velden. Er ontstaat geïoniseerd materiaal -- een plasma. In het algemeen zullen de plasmagebieden niet homogeen zijn, maar complexe ruimtelijke structuren 'patronen' gaan vormen. Een groep op het CWI bestudeert fundamentele en toegepaste aspecten van zulke patronen, speciaal 'streamer' en barrière-ontladingen. De resultaten zijn te gebruiken voor het zuiveren van rookgassen, voor zeer snelle hoogspanning halfgeleider-schakelaars, of voor platte computerschermen.

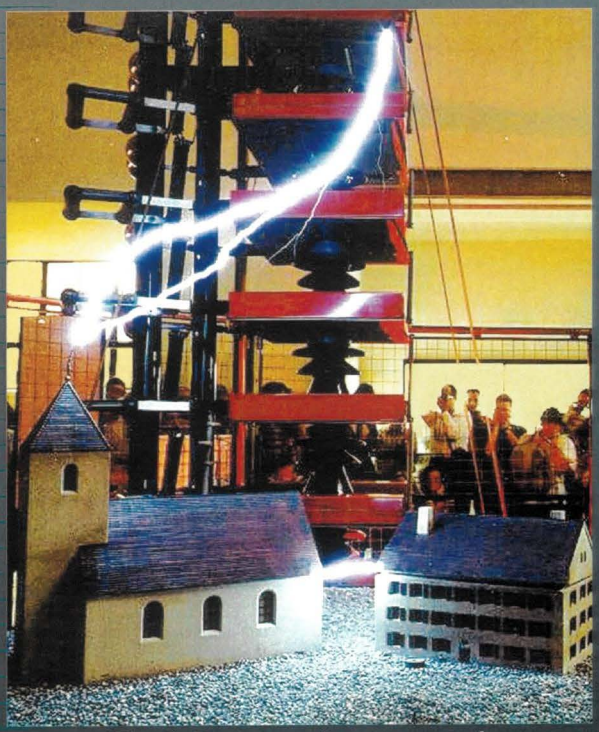


Fig. 1: Demonstratie van een vonk. [Deutsches Museum München]

Verschijnselen en toepassingen

Vonken komen voor op allerlei lengteschalen. Figuur 1 toont een kunstmatige vonk over een afstand van ongeveer een meter -- een karakteristiek en gevaarlijk verschijnsel in de hoogspanningstechniek. Vonken van enkele millimeters lengte in de bougies van automotoren worden gebruikt voor ontsteking van het lucht-brandstof mengsel. Vonken of hun voorlopers ('streamers') worden ook gebruikt voor de chemische verwerking van gassen, zoals het zuiveren van verbrandingsgassen (zie figuur 2). Ze komen ook voor in vloeistoffen en vaste stoffen met een aanvankelijk verwaarloosbaar elektrisch geleidingsvermogen. Streamer ontladingen in water kunnen worden gebruikt bij de waterzuivering. Zij kunnen echter ook transformators in het elektriciteitsnet onklaar maken door een ontlading via de transformatorolie. Streamer-achtige ontladingen in gedoteerde gelaagde halfgeleiders kunnen worden gebruikt voor zeer snelle schakeling in hoogspanning-circuits, met toepassingen in radartechnologie, en mogelijk ook bij twee nieuwe types hoogvermogen gepulste lasers. Ontladingen op micro-schaal in chips zijn schadelijker naarmate de geïntegreerde circuits op de chip kleiner worden. Een ontlading kan ook stationair zijn. Het bekendste voorbeeld is de TL-buis. Een ontlading is een niet-lineair proces waarbij gemakkelijk patronen optreden. Daarom is het homogene en stationaire schijnsel van een TL-buis in het geheel niet vanzelfsprekend, maar te danken aan het vernuft van de ingenieur. Dit blijft bijvoorbeeld bij Philips een voortdurende uitdaging bij de ontwikkeling van nieuwe energiebesparende en speciale lichtbronnen. Figuur 3 laat typische instabiliteiten zien. Veel aandacht gaat nu uit naar de ontwikkeling van 'plasma display panels': platte, heldere computer- of televisieschermen die in essentie werken als een rooster van snelle, microscopisch kleine TL-buizen in de kleuren rood, groen en blauw.

Wat gebeurt er in een ontlading?

Bij alle ontladingen neemt het elektrisch geleidingsvermogen van een stof enorm toe in een sterk elektrisch veld, terwijl de stof zelf in rust blijft. Een bij benadering lokale ionisatie-reactie zorgt voor een snelle toename van de vrije ladingdragers zolang het lokale elektrische veld sterk genoeg is. Een geleider kan echter zijn ruimtelading herverdelen en daarmee het uitwendige elektrische veld veranderen. Afhankelijk van de ruimtelijke verdeling van de geïoniseerde gebieden wordt de ionisatie-reactie dan versterkt op sommige plaatsen en verzwakt op andere. Deze niet-lineaire dynamische koppeling tussen ionisatiegraad en elektrisch veld is verantwoordelijk voor de in ontladingsexperimenten waargenomen patronen in ruimte en tijd. Sommige toepassingen zoals bij rookgaszuivering of bougies werken op patroonvorming. Bij andere toepassingen zoals lichtbronnen of zeer snelle halfgeleider-schakelingen vormt het begin van patroonvorming juist de grens van de toepasbaarheid.

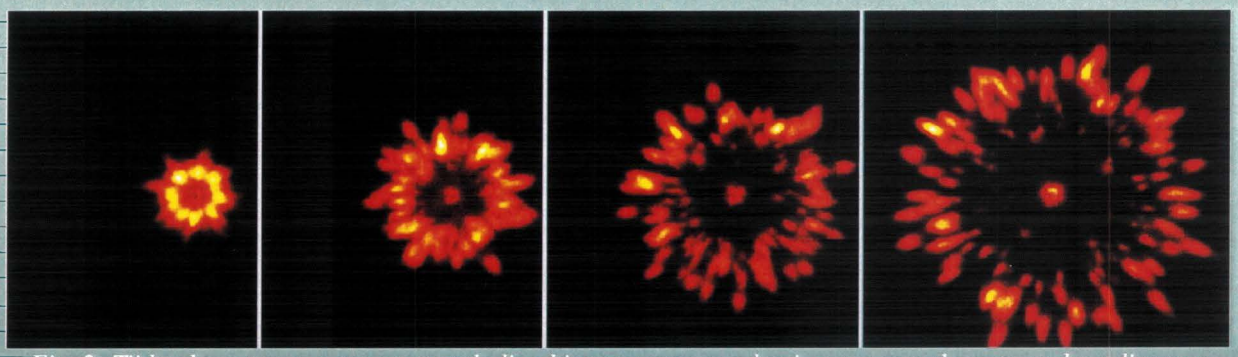


Fig. 2: Tijdverloop van een streamer ontlading binnen nanoseconden in een verwerker van verbrandingsgassen aan de TU Eindhoven [P.P.M. Blom en E.J.M. van Heesch]. De foto is genomen op de as van de draad der elektrode; de maximale straal van de ontlading is ongeveer 10 cm.

Fundamentele vergelijkingen en uitdagingen

De partiële differentiaalvergelijkingen die ontladingsverschijnselen beschrijven in verschillende stoffen zijn verrassend universeel. Deze zijn vergelijkingen voor tenminste twee types geladen deeltjes (typisch elektronen en positief geladen ionen). Hun ladingsverdeling beïnvloedt het uitwendige elektrische veld volgens de wet van Coulomb. Het elektrisch veld bepaalt de 'drift' snelheden van de deeltjes volgens de wet van Ohm, evenals de mate van produktie van meer geladen deeltjes. Het minimale ontladingsmodel is van een eenvoud en algemeenheid vergelijkbaar met bijvoorbeeld de Navier-Stokes vergelijkingen in de hydrodynamica. Toch is ondanks het enorme economische belang van ontladingstechnologie zeer weinig bekend over basisoplossingen van de fundamentele vergelijkingen. Recente ontwikkelingen in de theorie van niet-lineaire partiële differentiaalvergelijkingen geven echter hoop op vooruitgang op dit terrein.

Projecten en financiering

Op het CWI worden met analytische en numerieke hulpmiddelen de basiswetten onderzocht voor de voortplanting van de geïoniseerde streamer-kanalen, zoals te zien in figuur 2. Streamers zijn ook aan de vonk in figuur 1 voorafgegaan en hebben deze bepaald. Een fundamenteel nieuw inzicht is de sterke wiskundige analogie met patronen gevormd in visceuze vingers of in kristalgroei uit onderkoelde smelt. Ander onderzoek betreft zeer snelle hoogspanning halfgeleider-schakelingen voor radar- en lasertoepassingen die op een streamer-achtige manier werken. Dit gebeurt in samenwerking met het Ioffe-Instituut in St. Petersburg, internationaal leider in de productie van zulke schakelingen. Een derde project richt zich op de basis-instabiliteiten in barrière-ontladingen (zie figuur 3). Deze ontladingen bestaan uit een sandwichstructuur van elektrode, weerstand-laag, gloei-ontlading en elektrode, aangedreven door gelijk- of wisselspanning. De patroonvorming is hier nog maar ten dele begrepen, en wij werken aan kwantitatieve voorspellingen betreffende aanvang en structuur. Gebruik wordt gemaakt van wiskundige analogieën met bijvoorbeeld temperatuur-gedreven convectie in vloeistoffen of met chemische systemen.

Het onderzoek wordt gesteund door NWO, direct en via haar stichting FOM, en door de Europese Unie. De CWI-groep maakt deel uit van de onderzoekschool Centrum voor Plasmafysica en Stralingstechnologie, en onderhoudt regelmatige contacten met Philips.

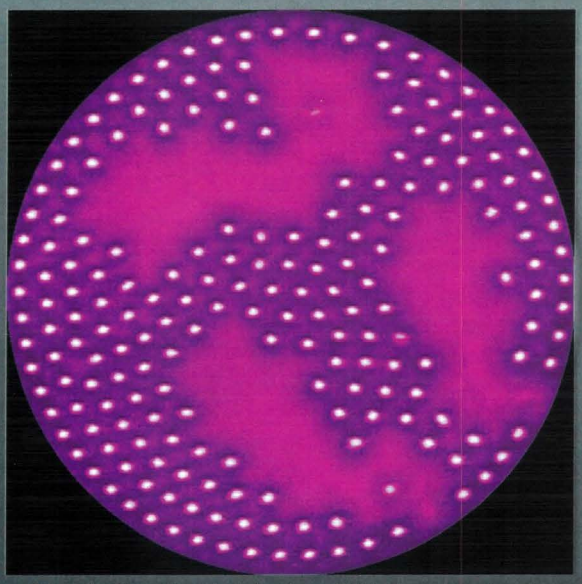


Fig. 3: Karakteristieke instabiliteiten in wisselspanning barrière gloei-ontladingen tussen coplanaire elektroden [I. Brauer en H.-G. Purwins, Univ. Münster]. Hier bestaan gebieden met homogene gloei en gebieden met spontane gloei-filamentatie naast elkaar.

Voor nadere informatie over dit CWI onderzoek:
www.cwi.nl/~ebert

Dr. Dipl.-Phys. U. Ebert
Telefoon: 020 592 4206
E-mail: Ute.Ebert@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

MIA: ZOEKEN IN MULTIMEDIA DATABASES

De wereld om ons heen creëert enorme hoeveelheden multimedia: complexe 'documenten', die bestaan uit stukjes tekst, (bewegend) beeld, en geluid. Het grote probleem met multimedia is het efficiënt vinden en terughalen van de informatie waarnaar je op zoek bent. De tekstuele informatie op het groeiende World Wide Web is al steeds lastiger te doorzoeken, maar dat is helemaal het met de enorme hoeveelheden multimedia die om ons heen ontstaan, en die een groot deel van onze toekomstige digitale bronnen gaan vormen. Het MIA project (Multimedia Informatie & Analyse) op het CWI richt zich daarom op het toegankelijk maken van multimediale collecties. Dit onderzoek dient als basis voor een nieuwe generatie zoekmachines op het World Wide Web en ter ondersteuning van digitale archivering in grote bedrijven.

mensen thuis ook steeds meer eigen gedigitaliseerde data: het maken van eigen compact discs met muziek is ongekend populair en digitale foto- en film-camera's worden steeds gewoner. De technologie die ontwikkeld wordt in het MIA project richt zich daarom ook op het terugvinden van 'dat liedje met dat leuke melodietje', of 'die foto van het zeilen, met de skyline van Boston; toen met dat mooie weer, was het nou 1997 of 1998?'. Dit project zal een stimulans zijn voor informatieleveranciers, en ieder ander die informatie toegankelijk wil maken.

Het doel van MIA is een nieuwe stimulans te geven aan de ontwikkeling van software voor de ontsluiting van multimedia, door het samenbrengen van onderzoekers uit traditioneel gescheiden domeinen: beeldanalyse, visualisatie, databases en informatie-ontsluiting. Na een voortvarende start van de ontwikkeling van multimedia zoeksystemen aan het begin van de

Zoeken op tekst: 'bos en boom'

• Voor gebruikers interactie:

• Na gebruikers interactie (1+4)

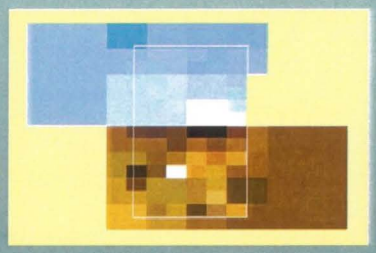
Initiële zoekresultaten uit een fotocollectie kunnen verbeterd worden met feedback van de gebruiker.

Digitale multimedia-documenten zijn eenvoudig centraal op te slaan en te distribueren via breedbandig internet. Zo kun je ze steeds weer afspelen zonder fysiek in de buurt te zijn, en in de nabije toekomst zelfs overal waar je ontvangst hebt op een mobiele telefoon. Bovendien kun je gedigitaliseerde data eenvoudig uitwisselen met anderen, en stukjes bestaand materiaal hergebruiken in nieuwe documenten. Daarom hebben

jaren '90 (met verschillende aanpakken in de diverse onderzoeksgebieden), lijkt het de laatste tijd alsof de ontwikkelingen 'vastzitten'. De hypothese achter MIA is dat meer bereikt wordt als de verschillende aanpakken geïntegreerd kunnen worden.

Het onderzoek in MIA vindt plaats op het WTCW terrein (het Wetenschap & Technologie Centrum Watergraafsmeer), waar zich ook de basis bevindt van

de transatlantische internet- verbinding; onderzoek dat hard nodig is om de grensverleggende mogelijkheden van internet-2 straks optimaal te kunnen benutten. MIA wordt gefinancierd door de Nederlandse overheid, het CWI, de Universiteit van Amsterdam, TNO-TPD, en diverse partners in de Nederlandse industrie.



Met behulp van patroonherkenning kunnen plaatjes gevonden worden die lijken op een voorbeeld. Het CWI onderzoekt de schaalbaarheid van deze technieken, opdat uiteindelijk miljoenen beelden op het Web doorzocht kunnen worden.

MIA bestaat uit twee hoofdonderwerpen: multimedia databases (CWI) en analyse en modellering van multimedia inhoud (UvA). Het database-team richt zich op twee thema's: schaalvergroting en het formuleren van goede zoekopdrachten. Voor het onderzoek naar schaalvergroting is het eerste doel het verwerken van zoekvragen in een collectie van meer dan 1 miljoen plaatjes. Een standaard methode op basis van kleurverdeling selecteert bijvoorbeeld typisch alles (de hele collectie) of niets (hooguit het gebruikte voorbeeld). Bovendien blijkt uit een eenvoudige optelsom dat de benodigde tijd per iteratie van het zoekproces al bij een paar duizend beelden oploopt tot onacceptabele wachttijden.

Het grootste probleem met het zoeken in beelden is echter dat de gevonden resultaten van een zoekvraag vaak zelfs voor de ontwikkelaars van de software moeilijk te begrijpen zijn. Voor een eindgebruiker is het al helemaal onbegrijpelijk waarom een voorbeeldplaatje van een zonsondergang op zee resulteert in (mooie) beelden van Afrikaanse savannes. Zulke onnauwkeurige antwoorden zijn een ongewenst neveneffect van onzekerheid bij de vraagformulering, en het grote gat tussen het hoge niveau van onze perceptie en de (noodzakelijkerwijs) veel eenvoudiger methodes voor automatische beeldanalyse.

We zoeken de oplossing voor dit probleem in twee verschillende aanpakken met behulp van beter samengestelde zoekvragen. De eerste aanpak richt zich op het assisteren van de gebruiker bij het automatisch formuleren van zoekvragen (*query formulation*); wij denken dat hier veel verbetering te halen is door meer informatie over de gebruiker te verzamelen in een zorgvuldig ontworpen interactie tussen mens en computer. De andere aanpak probeert gebruikers meer inzicht te geven in het zoekproces dat plaatsvindt in het systeem zelf, zodat zij zelf kunnen ingrijpen in het proces en dit kunnen bijsturen (*query articulation*). De grootste uitdaging voor ons onderzoek ligt in het vinden van de juiste balans tussen deze twee aanpakken.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/WTCW/MIA

dr.ir. Arjen P. de Vries
Telefoon 020 - 592 4306
E-mail: Arjen.de.Vries@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

TOEPASSINGEN UIT DE LEVENSWETENSCHAPPEN

De 20e eeuw was een periode met belangrijke technologische en wetenschappelijke doorbraken. Wetenschappers uit alle gebieden verwachten dat deze ontwikkelingen doorgaan, en gezien de huidige snelle vooruitgang in bio- en informatietechnologie met name in de levens- en computerwetenschappen. Nieuwe subdisciplines zijn gecreëerd op het raakvlak van biologie, natuurkunde, scheikunde, informatica en wiskunde, zoals computationele biologie en bioinformatica. Het CWI is actief in een aantal projecten met toepassingen in de levenswetenschappen.

In de afgelopen tien jaar is het onderzoek in de levenswetenschappen kwantitatiever geworden en steunt meer en meer op computers. De ontwikkeling en analyse van de partiële-differentiaalvergelijking modellen uit de mathematische biologie is niet alleen van belang voor een beter begrip van biologische processen en de verificatie van hypothesen over de onderliggende biologie, maar ook bijvoorbeeld voor de ontwikkeling van nieuwe medicijnen. Dit onderzoek vereist een nauwe samenwerking met zowel theoretische als experimentele biologen.

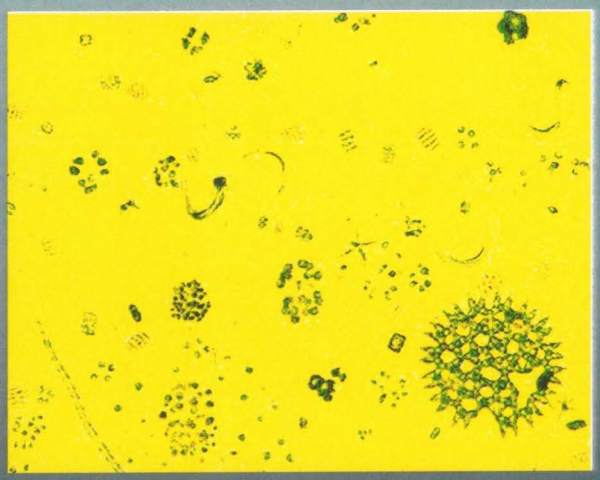
Lopende activiteiten zijn:

Het berekenen van de levende cel

Het Silicon Cell (SiC) Consortium verenigt drie belangrijke Amsterdamse academische instellingen: de Universiteit van Amsterdam (Swammerdam Instituut voor Levenswetenschappen en het Instituut voor Informatica), de Vrije Universiteit (Instituut voor Moleculaire Biologie) en het CWI. Lange-termijn doel is de berekening van 'het leven op cellulair niveau', uitgaande van alle informatie die beschikbaar zal komen in de komende jaren. Het realiseren van deze ambitie zal meer dan tien jaar vergen. In het kader van de Silicon Cell werkt het CWI aan een aantal projecten. Twee hiervan zijn:

- Ruimtelijke effecten in chemische paden. Ruimtelijke variaties in de concentraties van biochemische verbindingen werden tot nu toe verwaarloosd, maar deze kunnen in bijzondere situaties belangrijk worden. Het CWI onderzoekt dit probleem met numerieke (experimentele) en analytische methoden. Dit heeft inmiddels geleid tot een nieuw type 'optieltheorema voor regelcoëfficienten'.

- Continuum modellering van biologische membranen. Deze modellering heeft onlangs geleid tot een mesoscopische beschrijving van membraangedrag, in termen van partiele differentiaalvergelijkingen met een rekenintensieve niet-lokale component. Ook deze vergelijkingen worden zowel numeriek als analytisch bestudeerd.



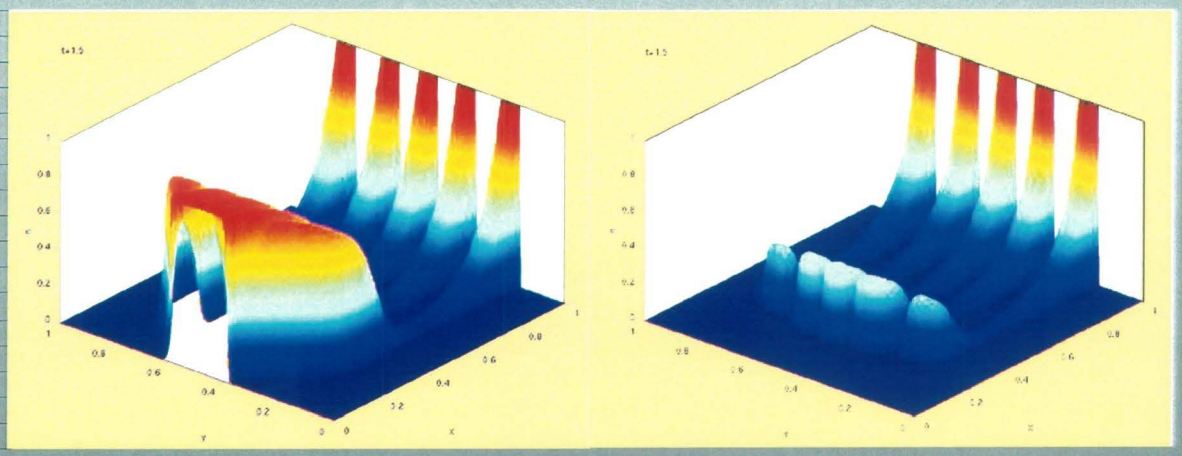
Fytoplankton.
Bron: Dr Petra Visser, IBED-Microbiologie UvA.

De Dynamica van Fytoplankton Populaties

Oceanen zorgen voor een reductie van ongeveer 15% van de CO_2 in de atmosfeer. Het mechanisme hierachter is de absorptie van CO_2 door een specifiek type alg dat naar de bodem van de oceanen zinkt. Exportproductie - het transport door de thermocliene laag (grenslaag tussen warm en koud water) - en de competitie tussen verschillende soorten fytoplankton is van groot belang. In waterige omgevingen is de belangrijkste factor voor overleving van een specifieke soort de lichtgradiënt, die op zijn beurt beïnvloed wordt door de absorptie door de soort zelf. Een een-dimensionaal model is al geïmplementeerd. Het bevat verticaal transport en regeling van drijfvermogen, zinken, verstoringen in het mengregime, etc. Het plan is om het bestaande model naar twee of zelfs drie dimensies uit te breiden en om horizontale advectie toe te voegen. Voor zulke complexe modellen zijn efficiënte numerieke oplossingstechnieken noodzakelijk.

Dynamisch Model voor Biofilms op Natte Oppervlakken

Biofilms zijn dunne lagen van slijm en bacteriën die voorkomen op elk nat oppervlak. Het slijm wordt afgescheiden door de bacteriën, en dient als een extern skelet dat de bacteriën van waterstromen afschermt. De bacteriën leven van organisch materiaal dat gevangen wordt in het slijm. Bij de zuivering van drinkwater worden biofilms als schadelijk beschouwd en er worden maatregelen genomen om ze te voorkomen. Het doel van het huidige project is



Simulatie van door een tumor veroorzaakte angiogenese. De simulatie gaat uit van een ronde tumor op het punt (x=0, y=0.5) en een bloedvat langs x=1, waaruit aan het begin van de simulatie nieuwe capillaire uitstulpingen groeien. De plaatjes laten zien hoe de concentratie van endotheelcellen zich ontwikkelt zonder therapie (links) en met therapie (rechts). Zonder therapie bereiken de endotheelcellen de tumor. Met therapie ontstaat er geen bloedtoevoer naar de tumor. Als de simulatietijd verlengd wordt, dan degenereert zelfs de bestaande bloedtoevoer. Bron: Alf Gerisch, Institut für Numerische Mathematik, Martin-Luther-Universität, Halle, Duitsland.

om een dynamisch model te ontwikkelen dat een beter begrip mogelijk maakt van de uitwisseling van opgeloste stoffen en deeltjes tussen biofilms en drinkwater en zo te komen tot een numerieke simulator die gebruikt kan worden door biologen voor validatie van experimentele data.

Computational Neuroscience Project

Computational neuroscience onderzoek is erop gericht om wiskundige en rekenmodellen te gebruiken om de functie en de structuur van de hersenen te begrijpen. Het huidige project komt voort uit computerstudies van de ontwikkeling van neuronale verbindingen in het zenuwstelsel. Het doel is bij te dragen aan onderzoek naar de biochemische mechanismen die de groeirichting en het bundelingsproces van axonen sturen. Een beter begrip van deze mechanismen is relevant voor het ontwikkelen van strategieën om hernieuwde groei te stimuleren na zenuwbeschadiging. De diffusieprocessen, de chemische interacties en de posities van de axonen worden gemodelleerd met systemen van parabolische vergelijkingen, gekoppeld met gradiëntvergelijkingen voor de posities van de axonen.

Axon ontwikkeling.
Bron: Dr Arjen van Ooyen, NIH.

De bijdrage van het CWI is het bestuderen van deze modellen en hun numerieke oplossing en het implementeren van efficiënte numerieke algoritmes in een gebruikersvriendelijke software tool.

Numerieke Simulatie van Taxis-Diffusie-Reactie Modellen

Tumor invasie en door een tumor veroorzaakte angiogenese (het ontstaan en uitgroeien van nieuwe bloedvaten) worden gemodelleerd door een 'taxis-diffusie-reactie systeem'. Vragen bij het eerste type model zijn bijvoorbeeld hoe ver tumoren kunnen binnendringen in het omliggende weefsel en onder welke omstandigheden de initiële celmassa in stukken opbreekt. Angiogenese kan worden veroorzaakt door een tumor die een verbinding probeert te leggen met de bloedsomloop - en dus voedselvoorziening.

Deze modellen worden bijvoorbeeld toegepast op patiënt-specifieke data in de geneeskunde. Numerieke oplossingen moeten binnen redelijk korte rekentijd verkregen worden om uitgebreide parameterstudies mogelijk te maken. Omdat de modelparameters en de initiële data vaak alleen ruwe benaderingen zijn, is men tevreden met relatief onnauwkeurige oplossingen, maar het is wel belangrijk om zekere kwalitatieve eigenschappen van de oplossing correct te simuleren.

Voor nadere informatie over dit CWI onderzoek:
www.cwi.nl/projects/lifesciences

Jan Verwer, tel. 020 - 592 4095
E-mail: Jan.Verwer@cwi.nl
Mark Peletier, tel. 020 - 592 4226
E-mail: Mark.Peletier@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

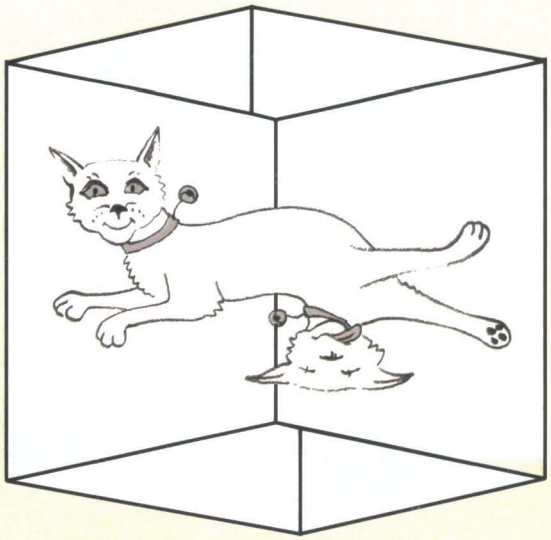
Centrum voor Wiskunde en Informatica

QUANTUM COMPUTING

Kent u de uitdrukking: een kat heeft negen levens? Een Quantum-Kat heeft het zelfs nog beter: hij kan tegelijkertijd dood en levend zijn. Deze tovertruc is de kern van quantum computing, een nieuwe manier van rekenen gebaseerd op bepaalde karakteristieken van de quantum mechanica. Het ontstond in de jaren tachtig als een theoretisch alternatief voor het traditioneel rekenen, dat binnen afzienbare tijd zal worden geconfronteerd met zijn fysieke beperkingen. De mogelijkheden zijn zeer veelbelovend, maar het vakgebied staat nog in de kinderschoenen en het verwezenlijken van een bruikbare quantum computer is nog een enorme uitdaging. In 1995 startte Prof. Paul Vitányi op het CWI de eerste quantum computing onderzoeksgroep in Nederland (en één van de eerste in Europa) in samenwerking met de Universiteit van Amsterdam. Deze groep heeft belangrijke inzichten toegevoegd aan het vakgebied. De Europese Unie onderkent het belang van dit onderzoek en heeft de groep aanzienlijke ondersteuning gegeven.

De ervaringen van de laatste 50 jaar laten zien dat het rekenvermogen iedere 18 maanden verdubbelt (de wet van Moore). Dit is vooral te danken aan de voortschrijdende miniaturisatie van rekenelementen, die mogelijk werd gemaakt door het tegelijk verminderen van warmteverspilling tijdens het rekenproces, zodat dit binnen aanvaarde grenzen blijft. Miniaturisatie zal echter snel de grootte van individuele atomen bereiken. Daar wordt het geconfronteerd met een fundamentele ondergrens van energieverspilling, tenzij de rekenmethodes grondig veranderen. Op atomair niveau gaan de regels van de mechanica, die ons dagelijks leven bepalen, niet langer op en moeten vervangen worden door de regels van de quantum mechanica. Deze complicatie geeft ons echter ook een extra voordeel: quantum mechanica maakt een nieuwe manier van rekenen mogelijk, waarmee berekeningen kunnen worden uitgevoerd die voor traditionele computers onmogelijk zijn, zelfs wanneer deze kunnen worden geminiaturiseerd tot hetzelfde niveau. Een voorbeeld is het kraken van grote getallen dat van cruciaal belang is bij, bijvoorbeeld, internet beveiliging.

De quantum mechanica ontwikkelde zich in de jaren twintig om verschijnselen te beschrijven op atomair niveau, dingen die men niet kon verklaren met de gewone klassieke mechanica. Ondanks het grote succes is het altijd een moeilijk onderwerp gebleven, omdat verschillende kenmerken de normale intuïtie tegenspreken. Een cruciaal begrip is 'superpositie': objecten zoals elektronen lijken zich enerzijds te gedragen als kleine gelokaliseerde deeltjes, anderzijds als een golf. Een elektron, afgevuurd op een scherm waarvoor twee nauwe doorgangen zijn geplaatst,



Erwin Schrödinger, *die een Nobelprijs won voor de uitvinding van de golf (quantum) mechanica, ontwierp in de jaren dertig een gedachtenexperiment om een schijnbaar absurd gevolg van de nieuwe mechanica te demonstreren. Een kat zit in een gesloten doos samen met één radio-actief atoom. Dit atoom zal vervallen met een zekere waarschijnlijkheid, volgens de wetten van de quantummechanica. Direct na verval breekt het uitgezonden kerndeeltje een dun glazen buisje gevuld met cyanide en de kat sterft onmiddellijk. Omdat wij buiten de doos zijn weten we niet of het radio-actieve deeltje vervallen is en dus weten we niet of de kat dood is of levend. In quantummechanisch opzicht is het beest in een superpositie van beide toestanden met een zekere waarschijnlijkheid. Als we in de doos kijken zien we maar één van deze twee toestanden: de kat is dood of levend. Een waarneming van de superpositie van deze toestanden laat deze met een zekere waarschijnlijkheid vervallen naar één van de twee mogelijkheden.*

gedraagt zich echter noch als een deeltje, noch als een golf. Volgens de quantum mechanica is het 'in superpositie': het gaat door de eerste én door de tweede opening.

Quantummechanica beschrijft materie als een superpositie van alle mogelijke toestanden, alle met een bepaalde amplitude – een complex getal waarvan het kwadraat van de absolute waarde wordt geïnterpreteerd als een waarschijnlijkheid. Deze amplitudes hebben dus extra eigenschappen die anders zijn dan de gewone waarschijnlijkheid – een kenmerk dat duidelijk wordt bij 'interferentie'. Juist aan dit kenmerk, samen met het superpositie principe, ontleent quantum computing zijn kracht. De evolutie van een systeem wordt beschreven door een 'unitaire' operatie op de superpositie die de waarschijnlijkheids-interpretatie van de amplitudes behoudt.

Bij de traditionele rekenmethodes is de kleinste eenheid een 'bit' die alleen de waarden 1 of 0 kan aannemen. Quantum computing is gebaseerd op 'qubits', bestaande uit een superpositie van de twee klassieke toestanden 0 en 1, ieder met een eigen amplitude. Verschillende fysieke realisaties van qubits zijn voorgesteld, waaronder een atoom in de grondtoestand (0) of aangeslagen toestand (1), de spin van een atoomkern (naar boven of naar beneden), de horizontale of verticale polarisatie van een foton, een stroom in een supergeleidende ring (links- of rechtsdraaiend) en een ingewikkelder constructie gebaseerd op siliconen. Een berekening begint met een aantal qubits in een duidelijk bepaalde toestand (0 of 1) waarop een aantal unitaire operaties wordt uitgevoerd (het algoritme). Door interferentie worden bepaalde superposities versterkt, terwijl andere elkaar opheffen. Na een aantal stappen wordt de eindtoestand bekeken (het resultaat). Tijdens de tussenliggende evolutie worden alle mogelijke rekenpaden tegelijkertijd gevolgd (quantum parallellisme), maar zij blijven verborgen in een doos. In bepaalde gevallen kan deze manier van rekenen leiden tot een enorme versnelling in vergelijking met de traditionele methodes, maar tegelijkertijd stelt het ons ook voor grote problemen. 'Niet storen tijdens berekening', luidt de slogan: de kleinste storing uit de omgeving kan de kwetsbare superpositie vernietigen en maakt de berekening waardeloos.

Een belangrijk begrip in de quantum mechanica en in quantum computing is 'verstrengeling' (entanglement): twee (of meer) qubits kunnen dusdanig worden geprepareerd dat ze, hoewel ze gescheiden zijn in ruimte – één zou er op Mars kunnen zijn en de andere hier op aarde – correlaties hebben die niet verklaard kunnen worden door de klassieke waarschijnlijkheidstheorie, bijvoorbeeld twee atoomkernen die onbekende maar tegenovergestelde spin hebben. Zo gauw één qubit is gemeten is de inhoud van de andere ook bekend, hoever ze ook van elkaar zijn verwijderd. Deze eigenschap kan worden gebruikt voor foutencorrectie tijdens de berekening, voor een efficiëntere overbrenging van informatie en voor bepaalde vormen van gespreide berekeningen. (Het is interessant om te weten dat de term 'verstrengeling' in de jaren dertig als paradox werd ingevoerd door Einstein, Podolsky en Rosen. Zij wilden de onvolkomenheid van de quantum-mechanica aantonen omdat dit het principe dat informatie niet sneller kan gaan dan de lichtsnelheid lijkt te ontkrachten.)

Het vakgebied quantum computing begon in de jaren tachtig en kreeg een impuls toen P.W. Shor in 1994 liet zien hoe je een efficiënt algoritme kon maken voor het kraken van grote getallen door middel van een slim gebruik van superpositie, interferentie, Fourier analyse en wat getaltheorie. De meeste cryptosystemen met een publieke sleutel, die op grote schaal worden gebruikt op het internet en in de financiële wereld, zijn gebaseerd op de moeilijkheid om grote getallen te kraken met behulp van de traditionele rekenmethodes. Quantum computing zou deze codes kunnen kraken, maar biedt als tegenprestatie andere, veiliger manieren om informatie te coderen. Een ander quantum algoritme, dat van L.K. Grover (1996) om in een database te zoeken, is kwadratisch sneller dan alle klassieke algoritmen.

CWI heeft begrippen uit de quantum computing toegepast op de complexiteit van communicatie, dat probeert antwoord te geven op de vraag hoeveel bits er moeten worden doorgegeven tussen twee partijen die samen een functie willen berekenen, waarbij een ieder slechts een gedeelte van de informatie tot zijn beschikking heeft. In bepaalde gevallen kan de hoeveelheid communicatie aanzienlijk worden verminderd. Een aantal belangrijke en algemene beperkingen van quantum computing zijn gevonden, maar ook nieuwe versnellingen. De enorme kwetsbaarheid van quantum superpositie heeft geleid tot quantum versies van foutencorrigerende codes. Om dit in praktijk te kunnen brengen is er meer kennis nodig van quantum informatietheorie. Het CWI onderzoekt dit vakgebied in combinatie met begrippen als quantum Kolmogorov complexiteit. Tot slot heeft CWI's onderzoek naar 'quantum verstrengeling' ook bijgedragen aan de quantumtheorie als zodanig.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/ins4

Prof.dr. H.M. Buhrman en Prof.dr.Ir. P.M.M. Vitányi
Telefoon: 020 - 592 4076 en 4124
E-mail: Harry.Buhrman@cwi.nl, Paul.Vitanyi@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

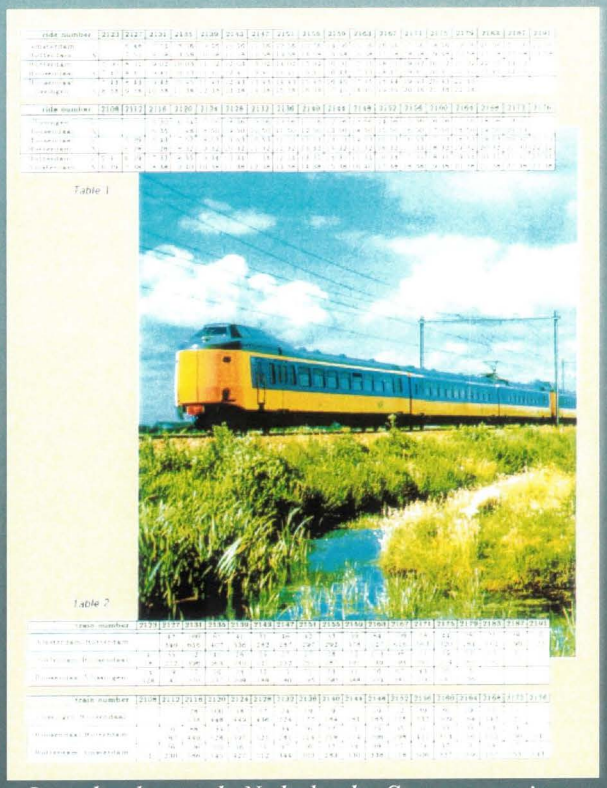
VOLGORDEPROBLEMEN KOMEN OVERAL VOOR

In de praktijk doen zich vaak problemen voor die betrekking hebben op het bepalen van de beste volgorde van een aantal taken, of het maken van de beste keuze van productiemiddelen. Voorbeelden zijn het vaststellen van vestigingsplaatsen van een bedrijf, het opstellen van productieschema's, roosters en dienstregelingen, het maken van snij- of knippatronen en het vaststellen van routes voor bestelwagens.

De oplossing van dit type vraagstukken bestaat steeds uit het maken van een keuze uit een groot aantal mogelijkheden. In theorie ligt de oplossing in het stuk voor stuk langsgaan van alle mogelijkheden, maar in de praktijk is dat aantal mogelijkheden zo groot dat zelfs met zeer snelle computers deze rechttoe-rechtaan methode veel te veel tijd vergt. Slimmere zoekstrategieën zijn dus vereist. De groep Combinatorische Optimalisering van het CWI heeft de laatste jaren veel onderzoek verricht naar dergelijke vraagstukken, hetgeen heeft geleid tot de ontwikkeling van aanzienlijk snellere computerprogramma's die ook voor zeer grote praktijkproblemen een oplossing kunnen bieden.

Een bekend voorbeeld is het zogenaamde handelsreizigersprobleem. Hierbij moet een (handels)reiziger een zo kort mogelijke route vinden langs een aantal te bezoeken steden. Dit vraagstuk komt in de praktijk in allerlei gedaanten voor: bijvoorbeeld het routeren van vrachtauto's, het boren van gaatjes in een printplaat van een computer en het sturen van de handelingen van een robot.

Tot voor kort kon de computer dergelijke opgaven met meer dan 40 'steden' niet aan. Met de in de afgelopen jaren ontwikkelde programmatuur kunnen echter inmiddels problemen van meer dan 3000 'steden' worden opgelost. Bovendien heeft het onderzoek verschillende nieuwe wiskundige technieken opgeleverd, die toepasbaar blijken bij vele verwante problemen.



In opdracht van de Nederlandse Spoorwegen is op het CWI een optimaal plan ontwikkeld voor de inzet van rijdend materieel op het traject Amsterdam-Vlissingen (foto NS).

De onderzoekers van de groep Combinatorische Optimalisering maken gebruik van een aantal van deze technieken, zoals 'constraint programming', lineaire en geheeltallige programmering, optimaliserende algoritmen voor onderdelen van problemen en benaderingsalgoritmen of 'heuristieken' voor grote problemen.

Deze methoden lenen zich goed voor praktische vraagstukken zoals, meetkundige methoden afkomstig uit de lineaire programmering met toepassingen bij VLSI-ontwerp, patroonherkenning en robotica.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Praktijk

In de praktijk bestaat veel behoefte aan flexibele oplossingsmethoden die geschikt zijn voor verschillende planningssituaties. De aanpak van het CWI bestaat uit de toepassing van recente algoritmische vondsten op deelproblemen, waardoor de gebruiker het oplossingsproces interactief kan blijven sturen met de computer als hulpmiddel.

Ter illustratie een aantal projecten die zijn uitgevoerd voor bedrijven en organisaties:

- Voor de **Nederlandse Spoorwegen** heeft het CWI een praktisch systeem (CADANS) ontwikkeld dat dienstregelingen ontwerpt en knelpunten signaleert in infrastructuur en reizigerswensen. Zo kan worden aangegeven waar viaducten of extra sporen zouden moeten worden bijgebouwd om gewenste frequenties of aansluitingen te realiseren. Het systeem wordt onder meer gebruikt bij het ontwerpen van het 'spoorboekje van de 21^{e} eeuw'.

Daarnaast is, eveneens voor de NS, onderzoek gedaan naar de meest effectieve inzet van treinstellen bij een gegeven dienstregeling en een aantal andere randvoorwaarden. Het CWI heeft hiervoor een praktische oplossing gevonden met behulp van zogenaamde polyhedrale combinatoriek.

- Voor de **Universiteit Maastricht** en de **Vrije Universiteit** in Amsterdam werd een systeem ontwikkeld dat een efficiënt rooster bepaalt voor de stages van de studenten geneeskunde.

- Voor **Van Gend & Loos** is een beslissingsondersteunend systeem ontwikkeld voor de routering van hangend confectievervoer (CAR= Computer Aided Routing). Het vervult alle functies, van kladblok en geheugensteuntje tot en met het genereren van volledige planningen.

- Voor **ECT/Nedlloyd** is een interactief planningssysteem gemaakt voor het wereldwijd of regionaal beheer van containers, waarbij computers ter ondersteuning van planningsdeskundigen zijn ingeschakeld.

- In samenwerking met het **TNO-Vezelinstituut** is een interactief planningssysteem ontwikkeld (KLIPP) voor de productieplanning in de naaizaal van een confectie-industrie.

De onderzoekers van het CWI hebben uitgebreide ervaring opgedaan met het toepassen van hun verworven theoretische kennis op praktische problemen. De oplossingen zijn gebruiksvriendelijk: voor de buitenwereld is de wiskundige basis niet direct herkenbaar.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/pna1

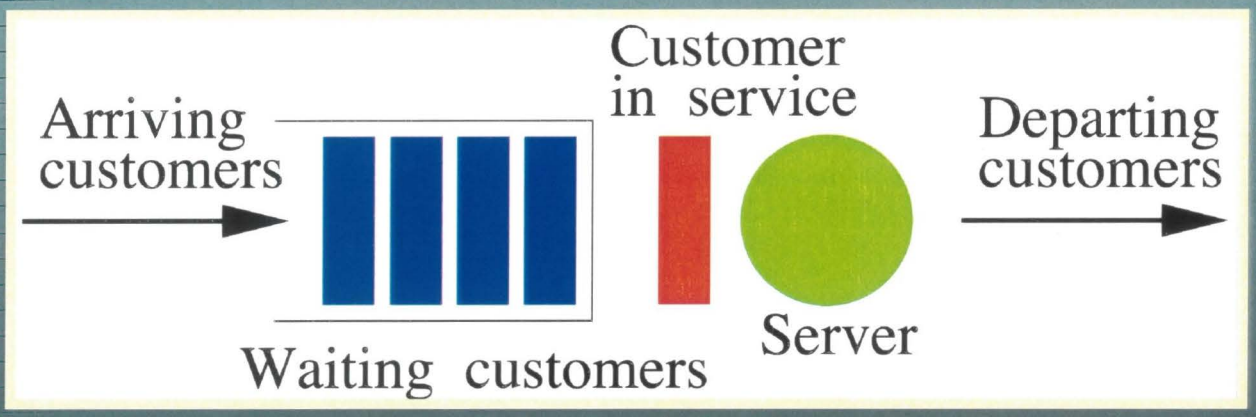
Prof.dr. ir. A.M.H. Gerards
Telefoon 020-592 4045
(secretariaat 020-592 4189)
E-mail: Bert.Gerards@cwi.nl

september 2001

Centrum voor Wiskunde en Informatica

TOEGEPASTE KANSREKENING VOORKOMT ERGERNIS BIJ WACHTEN

Wachten is een zo algemeen verschijnsel dat de ergernis waarmee het gepaard gaat eveneens deel is gaan uitmaken van het dagelijks bestaan. Wachten in de file, op het postkantoor, het 'aantal wachtenden vóór u' bij de telefoon, of achter de computer bij het downloaden van Internet-documenten lijkt bovendien steeds maar toe te nemen, terwijl in onze informatiemaatschappij tegelijkertijd steeds meer geavanceerde en snellere systemen in gebruik komen.



Het klassieke wachtrij model.

Het wachtrijprobleem verheugt zich al bijna een eeuw in de belangstelling van wiskundigen. Sterker nog, de kanstheoretische aanpak van deze problemen heeft zich ontwikkeld tot een essentieel hulpmiddel bij het ontwerpen en dimensioneren van communicatiesystemen (die al of niet via computers werken) en bij allerlei fabricageprocessen. Kort gezegd: daar waar een beperkte capaciteit voor 'dienstverlening' beschikbaar is voor elkaar beconcurrerende klanten. Het kernprobleem bij wachtrijen is: hoe wijs je de beperkte capaciteit zo goed mogelijk toe aan zo veel mogelijk gebruikers?

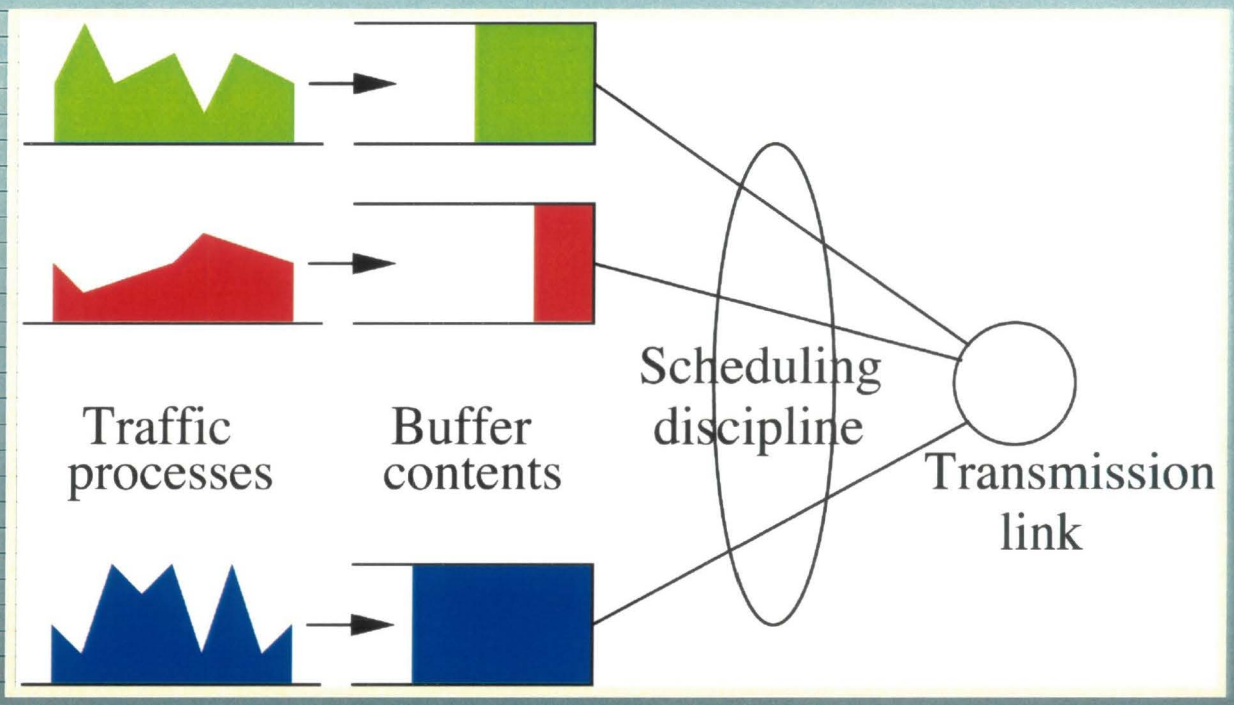
Om een dergelijk systeem voor dienstverlening optimaal te laten presteren wordt een wiskundig model gemaakt van de manier waarop de wachtenden moeten worden bediend. Omdat het aankomstproces van de klanten en hun bedieningsvraag stochastische aspecten bevatten, zijn ook de belangrijkste grootheden (het aantal wachtende klanten en de wachttijden) stochastisch: wachtrijtheorie is een onderdeel van de toegepaste kansrekening.

Het CWI doet al jaren fundamenteel onderzoek naar modellen en methoden uit de wachtrijtheorie. Het onderzoek spitst zich toe op wachtrijmodellen voor prestatie-analyse van computers en communicatiesystemen.

Het zwaartepunt van het onderzoek ligt momenteel bij de prestatie-analyse van geïntegreerde communicatienetwerken. Belangrijke prestatie-analyse problemen waar speciaal aandacht aan is besteed betreffen onder andere het effect van zogenaamde zwaarstaartige verkeersprocessen en de interactie tussen *real-time* verkeer en *best-effort* verkeer. Real-time verkeer is verkeer dat extreem gevoelig is voor vertraging in het versturen van informatie, zoals telefoongesprekken en video-conferenties. Best-effort verkeer daarentegen kan enige vertraging tolereren, zolang de gemiddelde capaciteit over langere tijdsperiodes voldoende is. (Het verzenden van data bestanden is een typisch voorbeeld.)

Wegens de extreme vertragingsgevoeligheid, is het gebruikelijk het real-time verkeer prioriteit te geven bij de verzending van informatie-pakketjes.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl



Het multiplexen van stromen informatie-pakketjes.

Het best-effort verkeer wordt zodoende de capaciteit toegewezen die is overgelaten door het real-time verkeer. Deze resterende capaciteit kan sterk fluctueren als gevolg van de grillige patronen in het real-time verkeer. De beschikbare capaciteit wordt vervolgens verdeeld onder de best-effort connecties volgens bepaalde vaste verhoudingen ('processor-sharing'). Dit motiveerde gedetailleerd onderzoek naar `processor-sharing' modellen met een variërende bedieningscapaciteit.

Een tweede belangrijk onderzoeksonderwerp betreft het effect van zogenaamde zwaarstaartige verkeersprocessen. Metingen hebben aangetoond dat stromen van informatie-pakketjes duidelijke tekenen vertonen van 'afhankelijkheid over lange afstand' en 'zelf gelijkenis'. Deze verschijnselen worden gewoonlijk toegeschreven aan de zwaarstaartige karakteristieken van de onderliggende verkeersprocessen (connectie duren, file groottes). Dit wijkt cruciaal af van traditionele verkeersmodellen, waar correlaties snel afzwakken in de tijd, en verkeersfluctaties snel uitmiddelen over langere tijdsperiodes.

Wachtrijmodellen met zwaarstaartige aankomstprocessen bieden een nuttige methode om het effect van 'afhankelijkheid over lange afstand' en 'zelf gelijkenis' te evalueren. Zo is bijvoorbeeld gevonden dat als het aankomstproces zwaarstaartig is, de buffer inhoud en de vertraging dat ook zijn. Recentelijk heeft het onderzoek zich geconcentreerd op de vraag hoe 'rooster' algoritmes gebruikt kunnen worden om de negatieve effecten van zwaarstaartige verkeersprocessen te neutraliseren. Er is aangetoond dat als databestanden niet in volgorde van aankomst worden verstuurd, maar met behulp van 'processor-sharing', de vertraging al aanzienlijk minder erg is.

Tenslotte verricht het CWI rechtstreeks toegepast onderzoek voor bedrijven en andere organisaties. Daarbij wordt er meestal van uitgegaan dat bij het bedrijf medewerkers beschikbaar zijn die kennis hebben van de wachtrij-problematiek en van de wiskundige technieken die daarbij worden toegepast.

Voor nadere informatie over dit CWI-onderzoek:
`www.cwi.nl/pna2`

Prof.dr.ir. S.C. Borst en Prof.dr. M. Mandjes
Telefoon 020-592 4205/4195
E-mail: Sem.Borst@cwi.nl, Michel.Mandjes@cwi.nl

september 2001

Centrum voor Wiskunde en Informatica

CWI

REGELEN, VOORSPELLEN EN MODELLEREN

Hoe kan een automobilist een route kiezen door een autosnelwegnetwerk die, gezien de actuele verkeerstoestand, een kortere reistijd heeft dan alternatieve routes? Bij files en ongelukken in een netwerk beschikt de weggebruiker niet over de voor deze keuze benodigde informatie. Daarom geeft Rijkswaterstaat via panelen met lichtborden boven de weg informatie of routeadviezen. Het achterliggende systeem bestaat uit meetapparatuur, een communicatienetwerk, computers en de panelen. De kern van het regelsysteem is een routeringsalgoritme. Op het CWI werkt men aan deze en andere problemen op het gebied van systeem- en regeltheorie, waarin naast de ontwikkeling van regeltheorie ook wordt gewerkt aan de constructie van wiskundige modellen in de vorm van regelsystemen.

De huidige technische apparatuur heeft intelligente regelalgoritmen nodig om te kunnen voldoen aan de hoge prestatie-eisen. Het met de hand regelen of gebruik maken van een standaard industriële regelaar voldoen al gauw niet meer. Voor het ontwerpen van intelligente regelaars is kennis van regeltechniek en systeemtheorie onontbeerlijk. Dergelijke regelaars zijn bijvoorbeeld nodig voor het opstellen van procedures voor de vluchtgeleiding van vliegtuigen en voor het detecteren van niet-functionerende onderdelen in grootschalige technische systemen zoals klimaatinstallaties voor gebouwen. Ook zijn zij nodig voor het bepalen van realistische modellen op basis van meetgegevens voor het transport van dioxine in mens of dier (deze modellen worden gebruikt bij het onderzoek op het gebied van volksgezondheid en milieu).

Dynamische Route Informatie Paneel (DRIP) in de omgeving van Rotterdam.
Foto: Rijkswaterstaat, Meetkundige Dienst, afdeling Grafische Technieken, Delft.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Hiernaast doen zich bijvoorbeeld ook regelproblemen voor bij de regeling van treinverkeer, het tot stand brengen van telefoongesprekken en het overbrengen van berichten in communicatienetwerken.

Op het CWI is vooral kennis opgebouwd van stochastische systemen (wiskundige modellen voor verschijnselen met onzekerheid), van systemen met discrete gebeurtenissen (modellen voor het in volgorde zetten van logische operaties, zoals in regelcomputers), en van lineaire systemen waarbij het uitgangssignaal evenredig verandert met het ingangssignaal.

Voor de oplossing van een signaalverwerkings- of regelprobleem wordt eerst een wiskundig model gemaakt, gebaseerd op fysische principes of economische wetten. Het model bevat ingangen die zijn te beïnvloeden teneinde te voldoen aan de beoogde regeldoelen. Het heeft ook uitgangen: bepaalde variabele grootheden die kunnen worden gemeten en die veranderen afhankelijk van het ingangssignaal. Bovendien beschrijft het model de ontwikkeling van de toestand. Het ideaal is dat een model zo goed mogelijk aansluit bij de metingen en tegelijkertijd zo eenvoudig mogelijk van opzet is. Afhankelijk van het probleem worden regeldoelen geformuleerd, zoals een korte responstijd, stabiliteit, minimale regelenergie en robuustheid. Omdat het meestal onmogelijk is om aan al deze doelen tegelijk te voldoen, moet er een compromis worden gevonden, bijvoorbeeld met behulp van optimale regeltheorie. Voor de oplossing van regelproblemen wordt een regelwet ('regelaar') opgesteld die is gebaseerd op het terugkoppelingsprincipe: uitgaande van het verschil tussen het actuele en het gewenste uitgangssignaal wordt het ingangssignaal zodanig aangepast dat dit verschil kleiner wordt. Tenslotte wordt de regelaar getest in de praktijk.

Rijkswaterstaat: In Europees verband heeft het CWI samengewerkt met Rijkswaterstaat aan het routeringsprobleem voor autosnelwegen. De totale reistijd van weggebruikers kan worden verminderd door hen informatie te tonen over de verkeerstoestand of hen route-adviezen te geven. Het onderzoek richt zich op het regelprobleem van de inzet van routeringsmaatregelen.

In samenwerking met de Adviesdienst Verkeer en Vervoer is ook onderzoek gedaan naar het effect van variabele snelheidslimieten op de verkeersstroom. Het bleek dat bij hoge verkeersdichtheden de doorstroming werd bevorderd door informatie te geven via het verkeerssignalerings-systeem. Het regelprobleem bestond uit de bepaling van de verkeersdichtheid bij welke de adviessnelheid op de matrixborden moet worden getoond. Voor dit probleem heeft het CWI een model opgesteld en een regelaar ontworpen. Een door Rijkswaterstaat nader uitgewerkt regelalgoritme werd in 1992 uitgetest op de A2 tussen Utrecht en Amsterdam.

In samenwerking met de Technische Universiteit Delft (TRAIL) wordt onderzoek verricht naar regelingen van wegverkeer netwerken.

Biologie: In samenwerking met de Faculteit Biologie van de Vrije Universiteit wordt onderzoek verricht naar het biochemische functioneren van de cel. Doel van het onderzoek is een beschrijving van dit functioneren in termen van een dynamisch systeem mogelijk met hiërarchische niveaus en met gereduceerde-orde systemen. Een tweede doel is de analyse van hoe een dergelijk systeem geregeld wordt door enzymen en hoe het extern te beïnvloeden is. Het onderzoek wordt gemotiveerd door vragen vanuit de biotechnologie en de geneeskunde.

Rijksinstituut voor Volksgezondheid en Milieuhygiëne (RIVM): Er is een toenemend besef dat het milieu om ons heen er slecht aan toe is. Op veel plaatsen zijn het water, de bodem en de lucht vervuild. Wat is het gevolg daarvan bij de mens? Welke stoffen zijn giftig en bij welke hoeveelheden richten ze echt schade aan? Beslissingen over de normen van de hoeveelheid gifstoffen in voedsel of lucht worden gebaseerd op wiskundige modellen van het gedrag van die gifstoffen in het lichaam. Hiervoor moet uit metingen een eenvoudig en realistisch model bepaald worden. Op het CWI is onderzoek verricht naar de bepaling van compartimentele systemen als modellen voor de verwerking van stoffen in het menselijk lichaam.

PTT Telecom/Philips: Is er bij telefooncentrales veel vraag naar verbinding, dan ontstaan lange wachttijden. De effectieve capaciteit daalt door de grote vraag, waardoor de centrale in feite voor niets werkt en vrijwel geen gesprekken meer afhandelt. Het is daarom beter om alleen zoveel aanvragen binnen te laten als op korte termijn zijn af te werken. Op het CWI is fundamenteel onderzoek verricht naar toelatingsregelingen voor communicatiesystemen. Voor specifieke problemen ontwerpt en analyseert het CWI gepaste regelalgoritmen.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/pna2

Prof.dr.ir. J.H. van Schuppen
Telefoon 020 - 592 4085
E-mail: J.H.van.Schuppen@cwi.nl

september 2001

WAVELETS VOOR EFFICIENTE OPSLAG VAN BEELD EN GELUID

Wavelets zijn golfpatroontjes van beperkte omvang, met behulp waarvan vooral abrupte overgangen in een signaal of scherpe contrasten in een beeld kunnen worden bestudeerd, en verschijnselen met structuur op verschillende schalen. De wavelet-methode is in de jaren tachtig ontwikkeld en is inmiddels voorzien van een solide wiskundige basis. De wavelet-methode is uitgegroeid tot een machtig hulpmiddel bij toepassingen op het gebied van datacompressie, ruisonderdrukking en beeld- en geluidverwerking. Op het CWI loopt een aantal projecten, waarin wavelet-technieken worden gebruikt voor beeldverwerking en beeldanalyse.

Het krachtigste wiskundige hulpmiddel bij de analyse en verwerking van signalen en beelden is de Fourier-methode, bedacht in de jaren twintig van de 19^{e} eeuw door de Franse wis- en natuurkundige Joseph Fourier. Hierbij wordt een signaal (wiskundig: een functie) gezien als opgebouwd uit bouwstenen in de vorm van sinus-vormige golven van verschillende frequenties. Het grote succes van de Fourier-methode komt doordat in de praktijk vaak een beperkt aantal bouwstenen voldoende blijkt om een aantal belangrijke karakteristieken van een signaal te ontdekken.

Dit is bijvoorbeeld het geval bij het beschrijven van de invloed van oceaangolven in de Noordzee. De 'Fourier-coëfficiënt' voor een bepaalde frequentie geeft aan hoe sterk die frequentie gemiddeld in het totale signaal is vertegenwoordigd. Omdat een sinus-functie tot in het oneindige blijft doorgolven geven de Fourier-coëfficiënten geen directe informatie over het lokale gedrag van een signaal; zij geven alleen een soort gemiddelde informatie over het hele signaal. Sla bijvoorbeeld op een piano een C aan en een seconde daarna de naasthogere G. Doe het vervolgens net andersom: eerst de G en dan de C. Aan de Fourier-coëfficiënten is het verschil nauwelijks te zien. De Fourier-methode is dan ook niet erg effectief in het ontdekken van snelle veranderingen in signalen, zoals het begin van een gesproken woord of een scherpe rand in een beeld. Verder vertonen vele signalen, bijvoorbeeld bij spraak en video, structuur op diverse schalen. De Fourier-methode "mist" het grootste deel van deze multi-schaal structuur.

Jean Morlet, een Franse geofysicus in dienst van de oliemaatschappij Elf Aquitaine, ondervond begin jaren tachtig bij zijn analyse van seismische signalen dermate hinder van bovenstaande beperkingen van de Fourier-methode dat hij op zoek ging naar iets beters. Voortbouwend op eerder werk van onder anderen de fysicus en Nobelprijswinnaar Dennis Gabor kwam hij met het idee van wavelets. Een

Decompositie van een beeld, waarbij gebruik wordt gemaakt van een morfologische wavelet transformatie.

wavelet is een golfpakketje, een golf-achtige functie die met een bepaalde frequentie rond het nulpunt schommelt in een klein gebied en daarbuiten gelijk is aan nul of zeer snel uitdempt. Een wavelet is dus gelokaliseerd zowel in frequentie als in positie. Van een "moeder-wavelet" kan een hele familie andere wavelets afgeleid worden door de moeder, als een harmonica, uit te rekken of samen te drukken en te verschuiven. In deze familie is op elke gewenste positie elke schaal vertegenwoordigd. Een wavelet-familie is te vergelijken met de verzameling van sinus- en cosinus-functies van alle frequenties in de Fourier-analyse.

Met wavelets wordt een signaal in kaart gebracht door elke wavelet van de familie als een mal langs het signaal te schuiven en op elk tijdstip te meten hoe goed die mal past. De resulterende wavelet-coëfficiënten zien er in een grafiek uit als een berglandschap boven het tijd-frequentie vlak. Een abrupte overgang in het signaal is direct zichtbaar als een piek bij de hoge frequenties op het tijdstip van overgang. Wavelet-analyse werkt als een microscoop: door de beschikbaarheid van wavelets van willekeurig kleine schaal kun je 'inzoomen' op elk gewenst detail van het signaal. Een belangrijk verschil met Fourier-analyse is dat de wavelet-coëfficienten van een één-dimensionaal signaal een twee-dimensionale verzameling vormen (afhankelijk van tijd en frequentie). Juist deze extra vrijheidsgraad (flexibiliteit) verklaart het succes van wavelets bij de analyse van abrupte overgangen en multi-schaal structuren.

Wavelets opereren op dezelfde "markt" als de Fourier-methode en zijn dus in principe zeer breed toepasbaar. Omdat de mens beeld en geluid voornamelijk door contrasten waarneemt, zijn wavelets bij uitstek geschikt om beelden en akoestische signalen efficiënt op te slaan en over te zenden door data-compressie. Zo heeft de Amerikaanse FBI in de jaren negentig zijn bestand van 200 miljoen vingerafdrukken (meer dan duizend terabyte) door waveletcompressie weten terug te brengen tot een paar procent van de oorspronkelijke omvang, met behoud van de herkenbaarheid der afdrukken. Wavelets worden ook met succes gebruikt voor het verwijderen van ruis in oude geluidsopnamen en het opknappen van beelden afkomstig van MRI- en CT-scans. Omdat een wavelet-familie bestaat uit zelfgelijkende functies is de methode ook zeer geschikt voor het ontdekken van fractale structuren in waarnemingen. Recent is de wavelet-methode toegepast bij onder meer de opsporing van kort-durende onregelmatigheden in een signaal (bijvoorbeeld een ECG), het goed functioneren van een lopende band, spraaksynthese en is onlangs gebruikt als de basis voor de nieuwe standaard JPEG2000 voor beeld-compressie.

In Nederland zijn wavelets en hun toepassingen onder meer bestudeerd bij het KNMI (structuur van het wolkendek, seismiek) de TU Delft (bodemstructuren, in verband met oliewinning), de Rijksuniversiteit Groningen (beeldverwerking in de geneeskunde) en het CWI (morfologische beeldanalyse).

Het onderzoek op het CWI spitst zich momenteel toe op de ontwikkeling van wavelet-methoden die zich kunnen aanpassen aan het te onderzoeken beeld of signaal, en op 'niet-lineaire' wavelets, in het bijzonder wavelets die gebaseerd zijn op morfologische filters. Mathematische morfologie is een deelgebied in de beeldverwerking gebaseerd op meetkundige concepten als grootte, vorm, en oriëntatie. Een groot aantal morfologische technieken, zoals skelet-algoritmen en granulometrieën, hebben veel gemeen met wavelets. Een belangrijk verschil is echter dat morfologische technieken altijd niet-lineair zijn. Daarentegen is de "klassieke" wavelet-transformatie lineair. Op het CWI wordt momenteel onderzoek gedaan naar wavelets die gebaseerd zijn op morfologische in plaats van lineaire filters. Daarbij gaat de aandacht ook uit naar allerlei toepassingen, met name op het gebied van beeldcompressie, beeldfusie, het zoeken in multimediadatabases en video-codering.

De FBI heeft zijn 200 miljoen vingerafdrukken met behulp van wavelets compact opgeslagen.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/pna4

Dr. ir. Henk J.A.M. Heijmans
Telefoon 020 - 592 4057
E-mail: Henk.Heijmans@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

SYSTEEMRENOVATIE

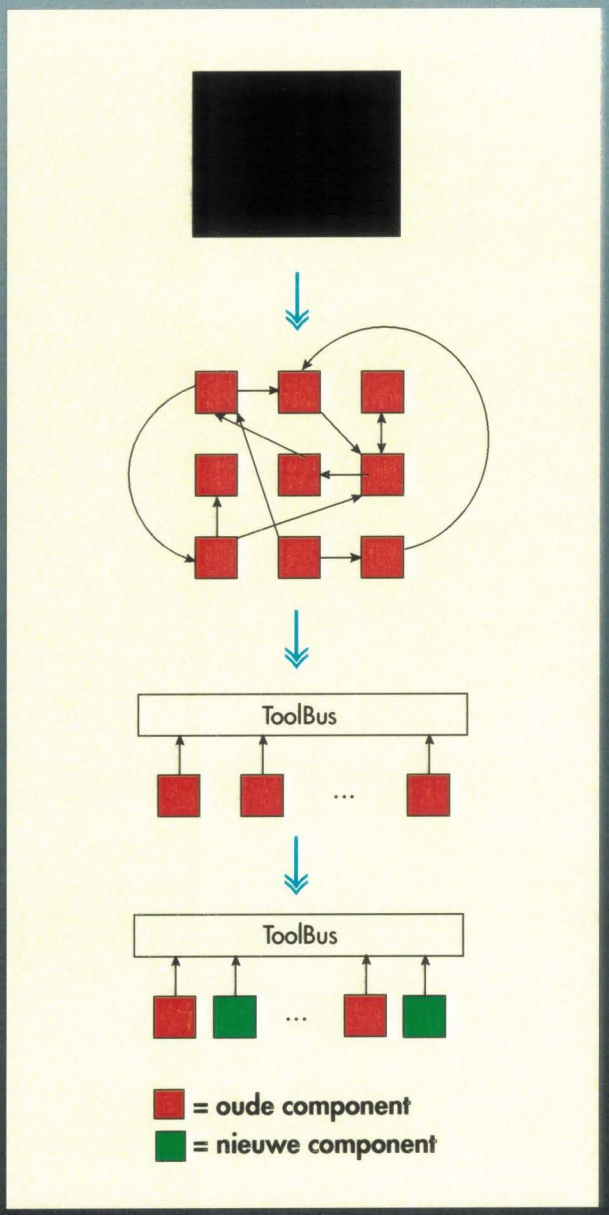
Oude software, geschreven in een oude taal, wel gebruik makend van goto's en niet van object-oriëntatie, en vaak enorm in omvang, is moeilijk aanpasbaar. Toch zijn aanpassingen altijd nodig: gebruikers willen toegang via Internet, hardwareplatforms verdwijnen, de (belasting)wetgeving verandert, er worden nieuwe producten geïntroduceerd, enzovoorts. Om dit soort wijzigingen door te voeren, is allereerst een goed begrip van de bestaande programmatuur noodzakelijk. In samenwerking met een aantal bedrijven die omvangrijke computersystemen in beheer hebben, ontwikkelt het CWI kennis die helpt grootschalige wijzigingen sneller, goedkoper, en beter beheersbaar uit te voeren.

Een *systeemrenovatie* heeft ten doel een oud (legacy) systeem zodanig te herstructureren dat het eenvoudig aanpasbaar wordt. Over het algemeen is dit niet gemakkelijk, omdat documentatie — indien aanwezig — verouderd is, de modulaire opzet verre van optimaal is, en er veel onoverzichtelijke afhankelijkheden tussen de softwarecomponenten bestaan. Het CWI doet onderzoek naar technieken die helpen een systeemrenovatie (gedeeltelijk) geautomatiseerd uit te voeren. Het onderzoek is gebaseerd op twee pijlers: taaltechnologie, en coördinatietechnologie.

Taaltechnologie

De enige betrouwbare informatie over wat een systeem nu werkelijk doet zit in de source code. Stap nummer één in een renovatie is dan ook het analyseren van de sources van een oud systeem. Nodig daarvoor zijn tools die in staat zijn softwarecomponenten te identificeren, samenhangende componenten te clusteren, de gevolgen van wijzigingen te voorspellen, en veranderingen systematisch door te voeren.

Voor systeemrenovaties, waarin vaak diverse talen en zeer speciale taaldialecten een rol spelen (COBOL, C, FORTRAN, JCL, ...) is het van groot belang taalspecifieke tools eenvoudig af te leiden. Op het CWI is de afgelopen jaren, in samenwerking met de Universiteit van Amsterdam, de 'ASF+SDF Meta-Environment' ontwikkeld, een generieke omgeving voor het produceren van taal-specifieke tools. De Meta-Omgeving genereert zulke tools automatisch uit een grammatica van de betreffende taal (bijv. COBOL) en een formele specificatie van de regels voor bijvoorbeeld typering, dataflow of programmatransformaties.



Stappen in het renovatieproces:
(1) Systeemanalyse met behulp van taaltechnologie:
(2) Globale herstructurering;
(3) Incrementele renovatie per component.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Coördinatietechnologie

Essentieel in het eenvoudiger aanpasbaar maken van software is een flexibile architectuur, waarin goed geïsoleerde componenten op een duidelijk gedefinieerde manier met elkaar communiceren. Op het CWI en de Universiteit van Amsterdam is om die reden de 'ToolBus' ontwikkeld, een component-based architectuur die de interactie tussen (gedistribueerde) softwarecomponenten (tools) coördineert. Een van de belangrijke eigenschappen van deze ToolBus is dat de communicatie tussen de diverse tools formeel is beschreven met behulp van procesalgebra. Programma's geschreven in allerlei talen kunnen aan de ToolBus worden gehangen: per taal is hiervoor slechts een eenvoudige 'adapter' nodig voor de uitwisseling van events en data tussen het programma en de ToolBus.

Stappen in het renovatieproces

De tekening op de voorzijde illustreert de samenhang tussen taal-en coördinatietechnologie. Beginnend met een zwarte doos, de legacy waar niets over bekend is, worden met behulp van taaltechnologie de losse softwarecomponenten en hun interfaces geïdentificeerd. Dit levert een beeld op van de architectuur van het legacy systeem. Daarna worden de interfaces expliciet beschreven, geformaliseerd, en gestructureerd met behulp van een ToolBus script. Is de communicatie eenmaal op die manier gestructureerd, dan kunnen de losse componenten ieder apart worden aangepast.

Program Understanding

Een belangrijk aandachtspunt is de analyse van legacy systemen ten behoeve van 'program understanding'. Met behulp van de ontwikkelde COBOL analyse-tools kan allerlei informatie over een legacy systeem verzameld worden, bijvoorbeeld welke programma's, schermen, databases, enz., waar worden gebruikt, en hoe al deze onderdelen met elkaar samenhangen. Deze informatie wordt vervolgens beschikbaar gesteld via hypertext (HTML) of via klikbare grafen. Daarnaast is het mogelijk (door middel van filtering en clustering) deze informatie te gebruiken om op semi-automatische wijze een object-georiënteerd herontwerp van het legacy-systeem te verkrijgen.

Programmatransformaties

Het tweede aandachtspunt is het uitvoeren van fabrieksmatige code-transformaties op grote COBOL systemen. Hiertoe is een COBOL grammatica ontwikkeld, waarmee de gewenste transformaties op hoog niveau kunnen worden gespecificeerd. Door het gebruik van deze technologie is het mogelijk een aantal onderhoudsactiviteiten sneller en beter door te voeren, en kunnen dialectmigraties worden geautomatiseerd.

Software Improvement Group

Het onderzoek op het gebied van systeemrenovatie heeft geleid tot een CWI spin off, de Software Improvement Group B.V. (SIG). Deze spin off ondersteunt bedrijven bij het omgaan met hun legacy systemen. De Software Improvement Group maakt daartoe gebruik van de onderzoeksresultaten van het CWI op het gebied van systeemrenovatie. SIG levert producten op het gebied van programmatransformaties en geautomatiseerde herdocumentatie van legacy systemen. Daarnaast biedt SIG strategische consultancy op het terrein van software-verbetering.

Verdere samenwerking

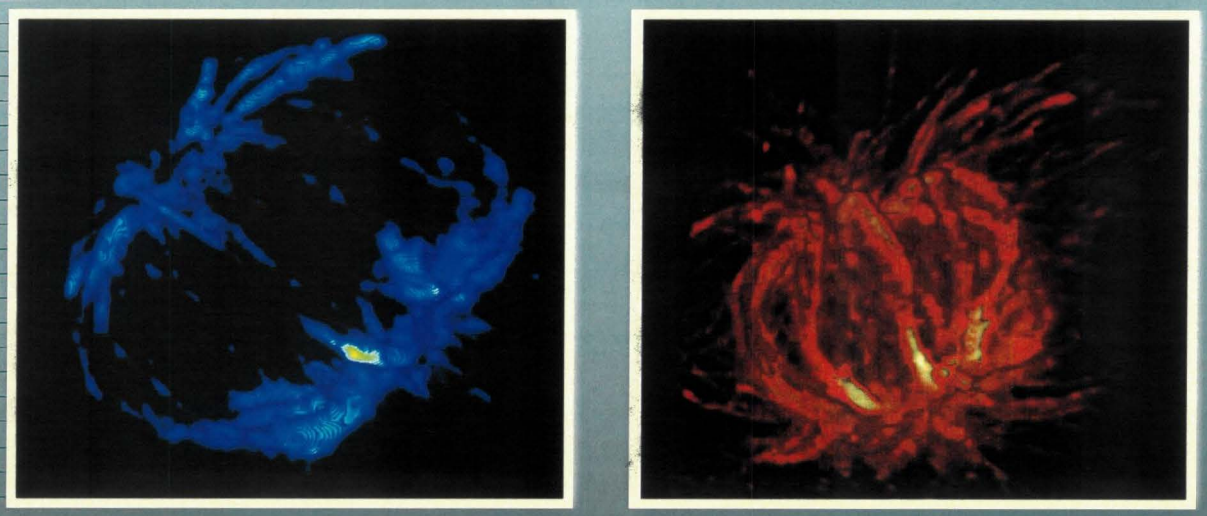
Bij het onderzoek naar systeemrenovatie werkt het CWI samen met diverse bedrijven, zoals ABN AMRO, Roccade, CAP Gemini en Lucent. Systeemrenovatie is een onderwerp van groot praktisch belang, dat tegelijkertijd een breed scala aan fundamentele vragen oproept. Het CWI levert diensten op het gebied van de kennisontwikkeling ten behoeve van systeemrenovatie, en werkt daarbij zo veel mogelijk samen met partijen die actief zijn in de renovatiepraktijk.

Voor nadere informatie over dit CWI-onderzoek:
`http://www.cwi.nl/sen1`

dr. Arie van Deursen en prof. dr. Paul Klint
Telefoon 020-5924075 / 020-5924126
E-mail: Arie.van.Deursen@cwi.nl,
Paul.Klint@cwi.nl

september 2001

VISUALISATIE VAN GEGEVENS GEEFT EXTRA DIMENSIE AAN ONDERZOEK



Visualisatie van celdeling (mitosis). Het gekleurde deel zijn de chromosomen die uit elkaar getrokken worden.

Computers spelen een steeds belangrijker rol in het wetenschappelijk onderzoek. Hun succes brengt echter ook problemen met zich mee: de gegevens worden geproduceerd in zulke hoeveelheden en zo snel dat het moeilijk wordt nog door de bomen het bos te zien. Visualisatie is hierbij een beproefd hulpmiddel, dat thans sterk in ontwikkeling is. Op het CWI wordt in het bijzonder aandacht besteed aan 'computational steering'.

Het is bijna ondoenlijk om uit een grote hoeveelheid gegevens snel samenhangen of trends te destilleren. Als die gegevens echter in de een of andere vorm grafisch worden weergegeven, dan ziet een mens de opmerkelijke trekken vaak in één oogopslag. 'Eén beeld zegt meer dan duizend woorden', aldus het wat afgezaagde, maar daarom niet minder ware oude Chinese gezegde. Een serie metingen grafisch weergeven is al op school een standaard bezigheid. Iets ingewikkelder is het gebruik van een 'heuvellandschap' om bijvoorbeeld het temperatuurverloop in een vlakke ijzerplaat in kaart te brengen. Men zou daarvoor ook kleur kunnen gebruiken (bijvoorbeeld de heetste delen rood en de koudste blauw). Veel praktijkgevallen betreffen natuurlijk ruimtelijke verschijnselen, zoals luchtstromingen rond vliegtuigvleugels. Hierbij kan men bijvoorbeeld het snelheidsveld van de stroming visualiseren door in elk punt de snelheidsvector te tekenen en de luchtdruk weergeven in kleur.

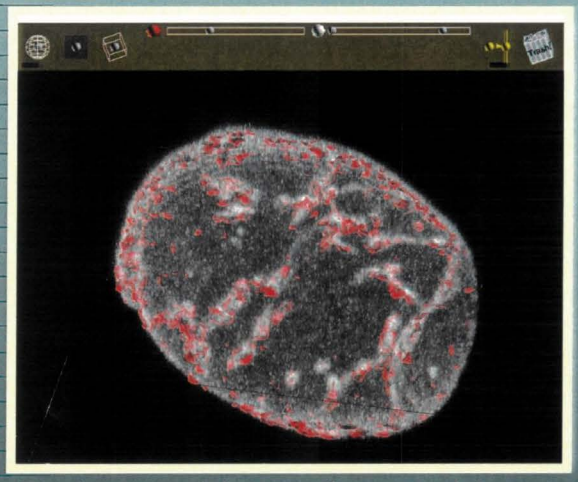
Doorsnede van turbulente stroming rond een blok. Kleur geeft de druk aan.

Door de snel toegenomen rekenkracht en grafische mogelijkheden van computers zijn tegenwoordig realistische simulaties, gebaseerd op wiskundige modellen en gebruik makend van vorm, kleur en beweging, mogelijk die tot voor kort ondenkbaar waren. In combinatie met het visueel vermogen van de mens levert dat een machtig hulpmiddel bij het wetenschappelijk onderzoek, waarbij het vooral gaat om het opsporen en volgen van structuren die anders verborgen zouden blijven.

Op het CWI wordt binnen het thema Visualitatie onderzoek gedaan naar 'computational steering'. Bij de meeste bestaande technieken en pakketten is het uitgangspunt dat de te visualiseren gegevens vastliggen. Na de simulatie vindt visualisatie en analyse plaats, op grond waarvan eventueel de simulatie wordt herhaald met aangepaste invoergegevens. In plaats van dit vrij

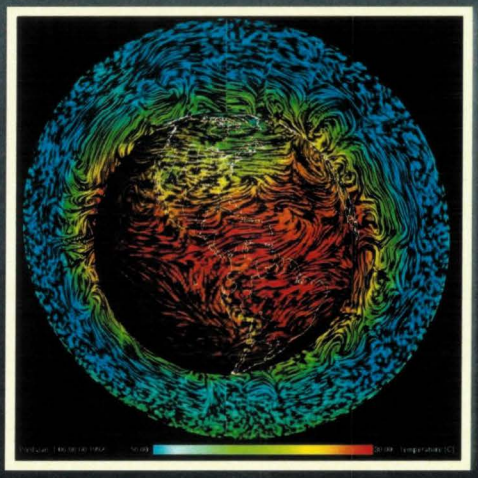
omslachtige proces is het beter om invoer, simulatie en visualisatie van de uitvoer te integreren in één systeem, waardoor de onderzoeker het effect van wijzigingen in de invoer op de uitvoer snel kan zien. Men onderscheidt hier twee snelheden: voor 'interactie' is een responstijd van 3-10 seconden gewenst, voor 'animatie' 0.1-0.2 seconden. De behoefte aan computational steering technieken zal naar verwachting snel toenemen, omdat de gesimuleerde modellen steeds ingewikkelder worden.

De kern van zo'n geïntegreerd systeem vormt het begrip

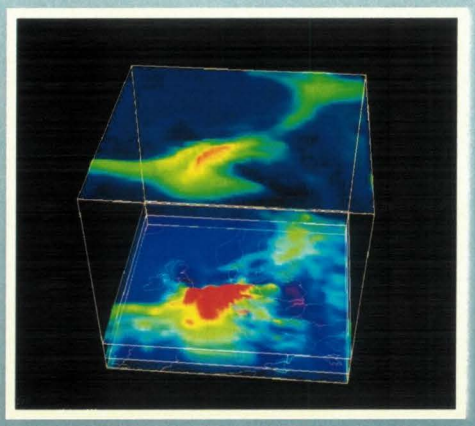


Visualisatie van de buitenrand van een cel (lamine).

'navigatie'. De onderzoeker varieert zijn invoer als functie van de tijd en volgt een bepaald plan om een doel te bereiken, bijvoorbeeld het vinden van een lokaal maximum van een functie. Het visualisatiesysteem moet dan een efficiënt hulpmiddel zijn om de weg naar het doel te vinden. Ook is het van belang dat de invoer als functie van de tijd vastligt ('loggen') om eventueel te kunnen terugzoeken, en dat er verband wordt gelegd tussen invoervariabelen en eventuele grenzen in de uitvoer ('heuristiek'). Een andere gewen-



Visualisatie van de temperaturen op de aarde en daarboven; Kleur geeft de temperatuur weer en de zwarte lijnen de luchtstromen.



Gesimuleerde ozon-verdeling boven Europa in vier lagen.

ste functie van computational steering is die van waakhond: de onderzoeker hoeft lang niet altijd de voortgang van het simulatieproces op de voet te volgen. Hij moet in staat worden gesteld bijzondere omstandigheden te definiëren, zoals instabiliteit of convergentie. Alleen als deze optreden krijgt hij een melding en kan dan desgewenst een inspectie uitvoeren en de invoer wijzigen.

Voorbeeld: In het kader van de Landelijke High-Performance Computing and Networking (HPCN) activiteiten is op het CWI in enkele proefprojecten gekeken naar het visueel specificeren en volgen van invoergegevens. Dit resulteerde in de ontwikkeling van een Computational Steering Environment (CSE) die de onderzoeker in staat stelt om de simulatie zelf, zonder hulp van visualisatie-experts, te sturen. Zo kan men in CSE direct manipuleren met grafische gegevens die tijdens de simulatie veranderen. Op het CWI vindt intensief onderzoek plaats op het gebied van het numeriek oplossen van grootschalige transportproblemen, beschreven door stelsels partiële differentiaalvergelijkingen van het advectie-diffusie-reactie type. Deze vergelijkingen spelen een belangrijke rol in bijvoorbeeld het wiskundig modelleren van milieuproblemen, zoals verontreinigingen van lucht, oppervlaktewater en grondwater. Bij het oplossen is de CSE gebruikt om de simulatie te sturen. De onderzoeker kan bijvoorbeeld emissie-velden manipuleren, terwijl de simulatie gewoon doordraait.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/ins3

Dr.ir. R. van Liere
Telefoon 020-592 4118
E-mail: Robert.van.Liere@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

CWI

CLUSTER Software Engineering

THEMA Specification and Analysis of Embedded Systems

FOUTLOZE SOFTWARE IN APPARATUUR

Steeds meer apparatuur bevat ingebouwde software die van vitaal belang is voor het goed functioneren van die apparatuur. Voorbeelden van deze 'embedded' software vindt men onder meer in de luchtvaartelektronica, de regeling van industriële processen, robotica, telecommunicatie en in diverse consumentenprodukten. Vanzelfsprekend worden hoge kwaliteitseisen gesteld aan deze embedded software. Het CWI doet onderzoek op dit gebied via twee wegen: bestudering van specificatietechnieken om tot een eenduidige beschrijving van embedded systemen te komen, en van analysetechnieken om aan te tonen dat de implementatie van die systemen de verwachte functionaliteit ook daadwerkelijk bezit ('dat het doet wat het moet doen'). Beoordeling van de uitvoerbaarheid van die technieken gebeurt door experimenten met fundamentele gedistribueerde algoritmen en door concrete industriële toepassing.

In veel gevallen moet de software in de toepassing functioneren in real-time en in een gedistribueerde omgeving. Dergelijke systemen nemen echter zo snel toe in omvang en complexiteit dat hoge eisen moeten worden gesteld aan de correctheid van de embedded software. Dit maakt het toepassen van formele methoden zeer gewenst.

De weg naar correcte software begint bij een specificatie van het probleem. Hieruit volgen criteria voor het te ontwerpen programma. Het programma heet 'correct' als aan die criteria is voldaan. De criteria worden geformuleerd in een specificatietaal, die bij voorkeur een hoog abstractieniveau heeft en die bijvoorbeeld niet executeerbaar hoeft te zijn. In algebraïsche specificaties leveren axioma's regels voor de vereenvoudiging van uitdrukkingen en leggen de semantiek vast van de algebraïsche constructies. Dergelijke formele methoden worden steeds meer gebruikt bij de specificatie van complexe systemen. Zij hebben als voordeel dat alle aannamen al in een vroeg stadium van het ontwerp expliciet zijn gemaakt. Daardoor voorkomt men fouten, waarvan de opsporing en verbetering in een latere fase van de productontwikkeling buitengewoon kostbaar zou zijn.

Neervallende brokstukken na zelfdestructie van de Ariane-501 raket, 4 juli 1996. De Ar-501 is ontploft door een softwarefout: de snelheid paste niet in de daartoe gereserveerde geheugenruimte. Nieuwe technieken zijn nodig om dergelijke ongelukken te voorkomen. Foto: ESA.

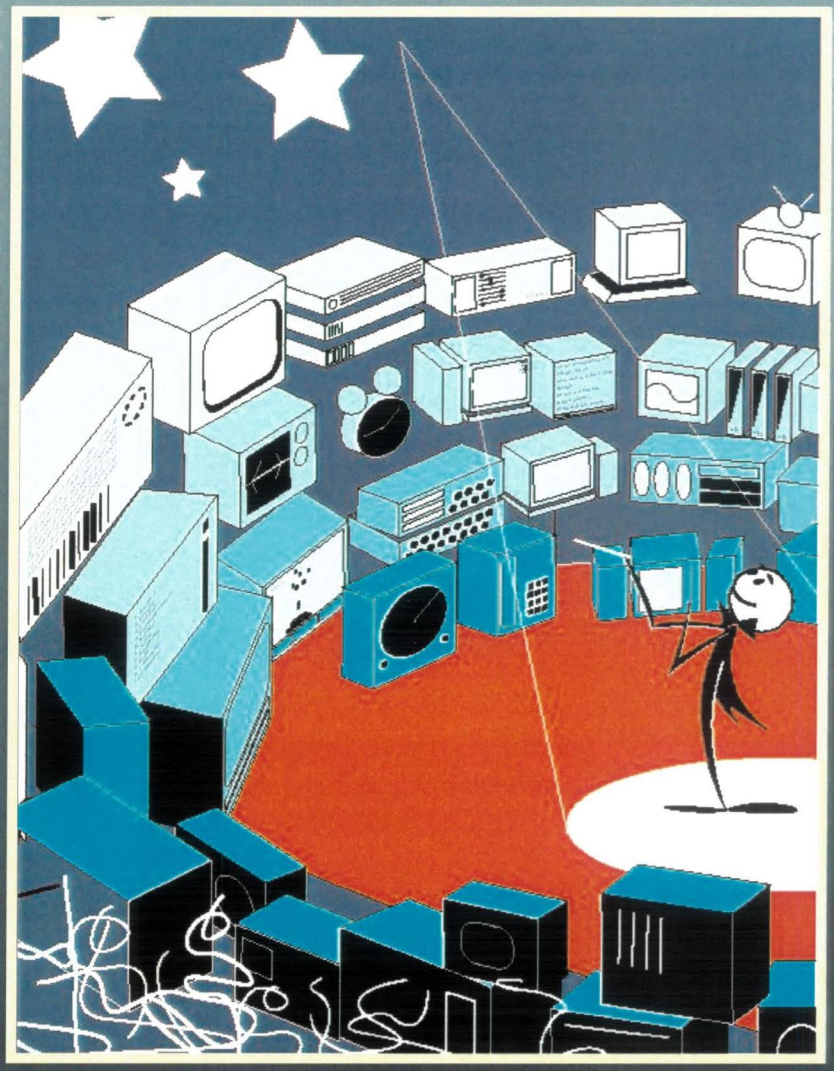
De opkomst van gedistribueerde computersystemen en parallelle rekenmethoden schiep een behoefte aan nieuwe specificatietechnieken, bijvoorbeeld om synchronisatieproblemen te kunnen beschrijven. Een veelbelovende aanpak is het gebruik van procesalgebra, waarmee concurrente processen formeel kunnen worden beschreven. Het CWI heeft belangrijke bijdragen geleverd aan de ontwikkeling van procesalgebra en van de daarop gebaseerde specificatietaal µCRL (micro Common Representation Language). Het theoretisch onderzoek op het CWI is thans tevens gericht op een real-time uitbreiding van µCRL.

De expressiviteit van de taal wordt bestudeerd in praktische toepassingen. De effectiviteit van het gebruik van formele methoden werd goed aangetoond bij de keuring van (kritieke onderdelen van) de soft-

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

ware in een aantal toepassingen binnen Philips, waaronder de komende generatie geïntegreerde schakelingen. Verder neemt het CWI deel in een project bij Philips, waarin het juiste functioneren van de in ontwikkeling zijnde DVB (Digital Video Broadcast) source decoder wordt bestudeerd. Het CWI zorgt voor de ontwikkeling en uitvoering van conformance tests gebaseerd op logische modellen en uitgebreide finite-state modellen, af te leiden uit de relevante standaarden en systeemdocumentatie.

Een tweede onderzoekstak op het CWI betreft bewijstheorie, met name het zoeken en het controleren van bewijzen. Het eerste doel is verhoging van de effectiviteit van gangbare symbolische technieken voor het verifiëren van aan een proces gestelde eisen. Daartoe wordt getracht op fundamenteel niveau inzicht te krijgen in het zoeken van bewijzen in eenvoudige logische systemen (in casu propositielogica). Voorts zijn methoden ontwikkeld voor het controleren van bewijzen, teneinde de correctheid van geprogrammeerde systemen 'buiten alle redelijke twijfel' vast te stellen.



SEN2 orkestreert verificatie van embedded systemen. Illustratie: I.A. van Langevelde. CWI (2001)

Een recente toepassing betreft de tool 'Heerhugo', gebaseerd op propositielogica. Heerhugowaard is het grootste station in Nederland dat werkt met één VPI (Vital Process Interlocking) systeem - een soort programmeerbare regelaar. Het systeem moet voldoen aan diverse veiligheidseisen, in de trant van: 'als een sein op groen staat, mag het volgende sein niet rood zijn'. Al deze eisen kunnen worden geformuleerd als statements in propositielogica. De controle of aan alle eisen is voldaan is een 'NP-compleet' probleem (ruw gezegd neemt de rekentijd exponentieel toe met de omvang van de beveiliging). In de praktijk moet men dan zijn toevlucht nemen tot een slimme benadering van het probleem met een aanvaardbare rekentijd. Voor dit speciale geval slaagde het CWI erin een werkbare 'prover' Heerhugo te ontwikkelen. Hiermee werd aangetoond dat de veiligheidssystemen van de Nederlandse Spoorwegen, in tegenstelling tot vele andere gevallen, van zeer hoge kwaliteit zijn. Heerhugo is ook met succes gebruikt bij consistentiecontroles op een grote databank, ontstaan uit samenvoeging van twee afzonderlijke databanken voor autoonderdelen van NedCar en Volvo.

In de toekomst zal het onderzoek zich met name richten op een steeds grotere inzetbaarheid van specificatie- en analysemethoden, teneinde de kwaliteit van computergestuurde systemen verder te verbeteren.

Voor nadere informatie over dit CWI-onderzoek:

Prof.dr. W.J. Fokkink
Telefoon 020 - 592 4104
E-mail: Wan.Fokkink@cwi.nl

september 2001

Centrum voor Wiskunde en Informatica

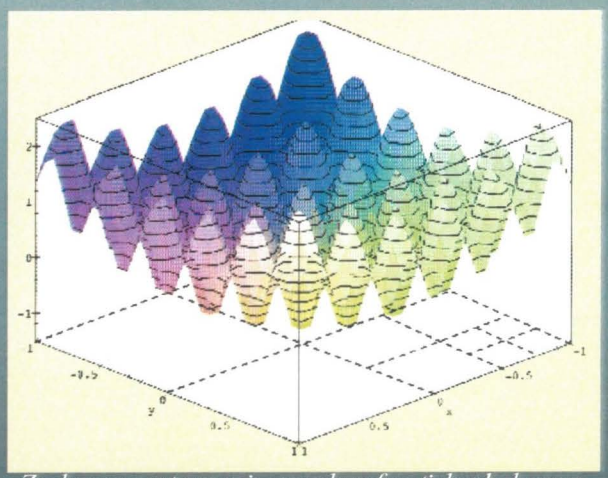
COÖRDINATIETALEN

Mensen gaan vaak samenwerken om een gemeenschappelijk doel te bereiken. Meestal treedt daarbij één van hen naar voren als leider, die dan de activiteiten van de groep als geheel coördineert. Dit ziet men ook steeds meer gebeuren in de computerwereld. Met behulp van een nieuwe klasse van parallelle programmeertalen, coördinatietalen, kan men de samenwerking tussen de diverse onderdelen van een geautomatiseerd systeem specificeren, analyseren en regelen. Een belangrijk toepassingsgebied is het parallelliseren van rekenintensieve sequentiële programma's. Op het CWI begon het onderzoek naar coördinatie in 1990. Dit resulteerde in een nieuw coördinatiemodel (IWIM) en een daarop gebaseerde coördinatietaal MANIFOLD. Er zijn inmiddels diverse licentiehouders in Europa en de VS.

Computers doen tegenwoordig veel meer dan alleen rekenen. Zij treden ook op als helper, bemiddelaar en coördinator. Het abstracte model voor de 'reken'-computer is de Turing Machine. Voor de 'regel'-computer, die naast zijn rekentaak ook die andere taken moet kunnen vervullen, introduceerde P. Wegner in 1995 het meer omvattende concept van een 'Interaction Machine', die communiceert met zijn omgeving via nieuwe soorten invoer en uitvoer. Zulke Interaction Machines blijken het gedrag van veel systemen in de praktijk te kunnen modelleren.

Onder coördinatie wordt verstaan de sturing van de wisselwerking tussen 'concurrente' programma's. Coördinatie richt zich op gemeenschappelijke eigenschappen van ogenschijnlijk sterk verschillende programma's, en wel op die eigenschappen die te maken hebben met interactie. De details van het rekenwerk van Interaction Machines doen dan niet ter zake.

Coördinatie is noodzakelijk bij ontwerp, ontwikkeling, debugging, onderhoud en hergebruik van concurrente systemen. Bij het ontwerp staat het modelleren van de samenwerking tussen de systeemcomponenten centraal. Coördinatietalen vormen de taalkundige



Zoeken van extremen in complexe functielandschappen door middel van domeindecompositie. De zoekopdrachten in de verschillende gebieden worden gecoördineerd.

tegenhanger van de tegenwoordig populaire 'middleware' die wordt gebruikt bij het ontwikkelen van concurrente toepassingen.

De coördinatietaal MANIFOLD, ontwikkeld op het CWI gedurende de jaren negentig, beschrijft de controle over de diverse processen binnen een concurrent systeem, in plaats van de (grootschalige) gegevensverwerking zelf. Daarom is de taal geschikt voor toepassing op bijvoorbeeld workflows in organisaties of op processen, waar de inhoud, het formaat en/of de aard van de informatie een aantal sterk verschillende fasen doorloopt. MANIFOLD is gebaseerd op het abstracte communicatiemodel IWIM (Idealized Worker Idealized Manager), waarin de 'managers' (coördinatiemodulen) door een strikte scheiding van de 'workers' (berekeningsmodulen) ook bruikbaar zijn in andere toepassingen. Zo deed op het CWI hetzelfde coördinatiemoduul dienst in een parallelle/gespreide sorteeralgoritme en in een toepassing van domeincompositie in de numerieke wiskunde.

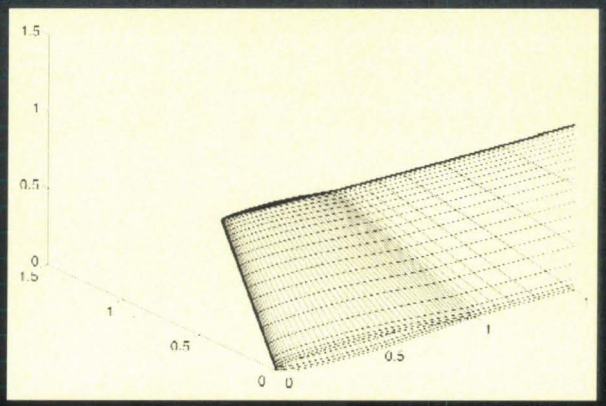
MANIFOLD werkt niet met 'berekenings'-begrippen als integer, float, string, loop, etc., maar kent alleen 'processes', 'ports', 'events', en 'streams'. De enige controlestructuur is een door events gedreven mechanisme van toestandsovergangen. MANIFOLD's coördinatiemodulen construeren en onderhouden een

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

dynamische dataflow graaf, waarin elke vertex een proces voorstelt. De modulen veranderen dan alleen de topologie van de graaf door de verbindingen tussen processen anders te leggen. De berekeningsmodulen hebben geen invloed op de graaftopologie.

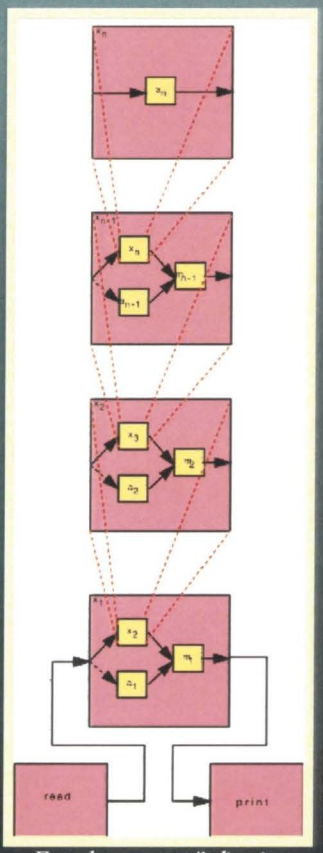
Het MANIFOLD systeem bestaat uit een compiler, een run-time systeembibliotheek, diverse utilities en bibliotheken van ingebouwde en voorgedefinieerde processen van algemene aard. Momenteel draait het op IBM RS6000 AIX, IBM SP1/2, Solaris, Linux, Cray en SGI IRIX systemen. Een MANIFOLD toepassing bestaat uit een (in principe zeer groot) aantal processen die verlopen binnen een netwerk van heterogene computersystemen, waaronder mogelijk enkele parallelle systemen. Binnen eenzelfde toepassing hoeven de processen niet in dezelfde programmeertaal te zijn geschreven. Ook hoeven zij niets te weten over MANIFOLD zelf of over hun samenwerking met andere processen via MANIFOLD.

Op het CWI is MANIFOLD met succes toegepast bij de implementatie van parallelle en gespreide versies van een zogenaamd half-vergrofde multirooster Euler algoritme. Het gaat hier om een realistische grootschalige toepassing uit de Computational Fluid Dynamics. Met behulp van zuivere coördinatieprotocollen in MANIFOLD kon de bestaande sequentiële Fortran programmatuur worden getransformeerd voor gebruik op parallelle en gespreide platforms. De resultaten waren zeer gunstig: geen aanpassingen van het berekeningsdeel van de Fortran 77 code, eenvoudige, kleine en herbruikbare MANIFOLD coördinatiemodulen, en lineaire versnelling van de totale executietijd met betrekking tot het aantal processoren (bijvoorbeeld van bijna negen uur tot ruim twee uur). Andere toepassingen van MANIFOLD betreffen de modellering van samenwerkende informatie-systemen, de coördinatie van zwak-gekoppelde genetische algoritmen op parallelle en gespreide platforms, de coördinatie van meervoudige solvers in een concurrent constraint programming systeem, en een gespreide checker van theorema's in de propositielogica.



Coördinatie van de berekeningen rond de ONERA-M6 vliegtuigvleugel.

Veel onderwerpen die met coördinatie te maken hebben, zijn gerelateerd aan basisproblemen uit Component Based Software Engineering en mobile computing. Zo levert het IWIM-model een krachtig raamwerk voor de samenvoeging van software componenten, waarin via 'kanalen' anonieme communicatie mogelijk is tussen systeemcomponenten. Het IWIM model kan gemakkelijk het begrip mobiliteit ondersteunen, zowel de mobiliteit van componenten zelf als de dynamische herconfiguratie van een systeem van componenten. Het CWI onderzoek op dit gebied omvat het ontwikkelen van Pεω, een paradigma voor samenvoeging gebaseerd op het begrip 'mobiele kanalen', evenals deelname aan het EU-project Omega: Component Based Software voor Real-time Systems (Vijfde Kaderprogramma).



Een algemene coördinatiemodule voor parallel sorteren en domeindecompositie.

Voor nadere informatie over dit CWI-onderzoek:
`http://www.cwi.nl/~farhad/`

Dr. F. Arbab
Telefoon 020 - 592 4056
E-mail: Farhad.Arbab@cwi.nl

september 1999

EVOLUTIE EN NEURONEN IN E-BUSINESS EN MANAGEMENT

Evolutionaire methoden en neurale netwerken zijn belangrijke nieuwe gebieden in de informatica. Deze computermethoden zijn geïnspireerd op essentiële principes uit de natuur, zoals 'survival of the fittest', evolutie, leerprocessen, interactie en parallellisme.

Op het CWI wordt hieraan onderzoek en ontwikkeling verricht, met name op management- en ICT-gerelateerde toepassingsgebieden, zoals e-commerce, on-line process management, remote-sensing classificatie en economie.

Evolutionaire algoritmen (ook wel: genetische algoritmen) zijn rekenmethoden die hun kracht in het bijzonder ontlenen aan autonome mechanismen uit de biologische evolutie, zoals selectie, 'survival of the fittest' (competitie) en recombinatie. Met natuurlijke selectie worden bijvoorbeeld oplossingen voor een (optimaliserings-) probleem ontwikkeld. Hierdoor is er geen expliciete kennis nodig over hoe een goede oplossing moet worden gecreëerd: het evolutionair algoritme bouwt zelf de kennis over goede oplossingen impliciet op. Een evolutionair algoritme kan dus zelfstandig kennis absorberen. Daarom zijn evolutionaire algoritmen vaak zeer geschikt om economische en management-gerelateerde problemen op te lossen en nieuwe ICT-technologieën te genereren.

Neurale netwerken zijn berekeningsstructuren, die geïnspireerd zijn door biologische modellen van de hersenen. Hierbij wordt een adaptieve structuur van elementaire rekeneenheden ('neuronen') gebruikt, die op bepaalde wijze aan elkaar verbonden zijn. Zodoende ontstaat er een flexibel adaptief netwerk dat in staat is (autonoom) te leren en extraheren uit een verzameling gegevens. Daarom zijn neurale netwerken vaak heel geschikt voor toepassing binnen beslissingsprocessen, zoals voor het autonoom classificeren en structureren van relevante gegevens uit beperkte data.

Elektronisch zakendoen (e-commerce) zal een ander beeld geven in handel en logistiek. In de toekomst zullen bijvoorbeeld magazijnen leger worden, doordat er meer maatproductie kan zijn en minder massaproductie. Foto: Frog Navigation Systems BV, Utrecht.

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Op het CWI wordt bij de groep 'Evolutionary Systems and Applied Algorithmics' onderzoek en ontwikkeling verricht aan evolutionaire algoritmen, neurale netwerken en on-line algoritmen. De toepassingsgebieden zijn daarbij gerelateerd aan economische en management-situaties, zoals die voorkomen in bedrijven (bijvoorbeeld e-commerce, optimalisatie, classificatie) of in de technologie (bijvoorbeeld 'embedded process management'). Hieronder geven we enige voorbeelden van recente en huidige projecten bij de onderzoeksgroep.

Agent-Technologie in E-Commerce: hierin worden lerende agenten ontwikkeld voor verschillende e-commerce toepassingen, zoals onderhandelen, dynamische prijsvorming, of profiling. Anderzijds worden nieuwe e-business concepten en toepassingen ontwikkeld, zoals het ontwerpen van nieuwe marktmechanismen of marktplaatsen. Doel is zowel het verkrijgen van fundamentele kennis als het ontwikkelen van toepassingen (prototypes). Dit project wordt in samenwerking gedaan met TNO, ING en KPN.

E-Commerce Exploratie: hier wordt een exploratiesysteem ontwikkeld om elektronische markten te kunnen modelleren en onderzoeken. Het systeem is gebaseerd op evolutioniare methoden. Doel is inzicht te verkrijgen in de effecten van de nieuwe mechanismen in e-commerce. Dit project wordt gedaan in samenwerking met de faculteit Technologie Management van de Technische Universiteit Eindhoven en met NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek).

Neural Vision: een tool voor visualisatie en clustering van hoog-dimensionale data door middel van data-projectie. De tool gebruikt hiervoor verschillende soorten neurale netwerken. Als zodanig is het een belangrijk onderdeel voor exploratieve data-analyse binnen een besluitvormingsproces. Het project is uitgevoerd in samenwerking met de Universiteit van Nijenrode en met Rijkswaterstaat.

Customers Choice: hier wordt door middel van clustering met behulp van neurale netwerken bepaald welke klantkenmerken belangrijk zijn voor het koopgedrag. Hierbij wordt de informatie uit verkoopbonnen gebruikt, dus een gigantische hoeveelheid van zeer beperkte, maar eenvoudig te verkrijgen informatie. Het project is uitgevoerd in samenwerking met een groothandel en de Universiteit Leiden. Op dit gebied vindt ook samenwerking plaats met de CWI groep.

Unsupervised Classification: hierin wordt uit remote-sensing data informatie over rampgebieden gehaald. Dit gebeurt door middel van clustering en classificatie van data. De classificatie is 'unsupervised', dat wil zeggen dat er geen informatie van experts of van grondmetingen hoeft te worden verkregen (tijdrovend en duur). Het project is in samenwerking met het Centre for Computer Science in Organization and Management (CCSOM - Universiteit van Amsterdam) en het CRREL (Cold Regions Research and Engineering Laboratory, USA).

On-line Process Management in Information Technology: het betreft hier beslissingsproblemen die voorkomen in moderne informatie-technologie, bijvoorbeeld in computernetwerken of multimediasystemen. Hierbij moet het management on-line zijn, dat wil zeggen dat continu (real-time) de beslissingen binnen een actief systeem moeten worden genomen. Het project is in samenwerking met NWO en het Philips Natuurkundig Laboratorium.

Data met betrekking tot de kwaliteit van het wegdek kunnen efficiënt worden geïnspecteerd met Neural Vision.
Foto: Rijkswaterstaat, Meetkundige Dienst, afdeling Grafische Technieken, Delft

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/sen4/

Prof.dr.ir. J.A. La Poutré
Telefoon 020 - 592 4082
E-mail: Han.La.Poutre@cwi.nl

september 2001

STROMINGEN BEGRIJPEN MET BEHULP VAN COMPUTER

Wie melk door de koffie roert beseft meestal niet dat wetenschappelijk nog steeds niet goed is begrepen hoe de twee vloeistoffen zich mengen. Naast dit huis-tuin-en-keuken voorbeeld heeft men in een groot aantal industriële toepassingen te maken met stromingsverschijnselen, bijvoorbeeld waterstromingen rond scheepsrompen en luchtstromingen rond vliegtuigvleugels. De laatste decennia is het inzicht in de aard van deze verschijnselen vooral dankzij de computer aanzienlijk toegenomen. Er blijven echter nog veel vragen onopgelost, ook op fundamenteel niveau. De studie van stromingen van vloeistoffen en gassen met behulp van de computer (CFD — Computational Fluid Dynamics) vormt dan ook al sinds jaren een belangrijk onderzoeksthema op het CWI.

Tegenwoordig wordt het belang van de stromingsleer voor het technologisch onderzoek overal erkend. Vroeger was het echter voornamelijk een academische aangelegenheid, met resultaten die sterk afweken van de waarnemingen. De praktijk ontwikkelde zich dan ook eerst vrijwel onafhankelijk van de theorie. Theoretische en technologische doorbraken hebben de kloof echter gedicht en er is nu sprake van een vruchtbare wisselwerking tussen theorie en praktijk.

Geschiedenis

In 1759 publiceerde Leonhard Euler zijn bewegingsvergelijkingen voor vloeistoffen, uitgaande van de tweede wet van Newton (massa X versnelling = de som van externe krachten). Eulers idee om kennis over vloeistofstromingen uit te drukken in de vorm van partiële differentiaalvergelijkingen was een revolutionaire vernieuwing. Voor praktische toepassing waren de vergelijkingen echter nog ongeschikt, omdat geen rekening werd gehouden met wrijvingskrachten. Pas bijna een eeuw later, in 1845, stelde George Stokes de algemene vergelijkingen op, die voor het geval van een niet-samendrukbare vloeistof al in 1822 waren gevonden door Claude Navier, en thans bekend staan onder de naam Navier-Stokes vergelijkingen. Nu leek het begrijpen en beheersen van een grote klasse vloeistofstromingen onder handbereik, want het probleem was teruggebracht tot het wiskundig oplossen van een paar fundamentele differentiaalvergelijkingen.

Hoewel Navier-Stokes theoretisch grote vooruitgang bracht, bleek de analytisch-wiskundige oplossing

Een uitdaging bij het hydrodynamisch ontwerpen van schepen is om die vorm van de scheepsromp te vinden die het best voldoet aan de vooraf gestelde gebruikerseisen, economische eisen, veiligheidseisen, enzovoorts. Linker foto: Oude scheepsromp. De lange golven die het schip maakt zijn hoog, deze bevatten dus veel energie (geleverd door het schip). Rechter foto: Verbeterde scheepsromp. De hoogte van de lange golven is sterk gereduceerd, deze verbetering is gerealiseerd met behulp van CFD. (foto's: MARIN)

van de complete vergelijkingen te hoog gegrepen. Het gevolg was een fragmentatie in een groot aantal van Navier-Stokes afgeleide, vereenvoudigde vergelijkingen voor speciale gevallen die wèl analytisch, dat wil zeggen met potlood en papier, waren aan te pakken. Al deze verschillende modellen beschreven echter wel de stroming van dezelfde soort vloeistof, een theoretisch hoogst ongewenste situatie.

De komst van de computer veranderde echter veel. Reeds in 1946 schetste John von Neumann een toekomstbeeld waarin 'automatische rekenmachines' de analytische oplossing van vereenvoudigde stromingsvergelijkingen zouden vervangen door een 'numerieke' oplossing van de complete, niet-lineaire stromingsvergelijkingen voor willekeurige geometrieën. (Volgens Von Neumann zou deze numerieke aanpak zelfs de experimentele vloeistofdynamica overbodig maken.) Daarmee stond hij aan de wieg van wat thans Computational Fluid Dynamics (CFD) heet. Von Neumann's voorspelling is in zoverre niet uitgekomen dat naast CFD het analytisch-theoretisch en het experimenteel onderzoek beide zijn blijven bestaan. Wel ontstond er een nieuwe tak van onderzoek: cruciale eigenschappen van CFD-methoden zoals consistentie, stabiliteit en convergentie moesten wiskundig worden bestudeerd. Nog steeds is veel fundamenteel onderzoek nodig om CFD nauwkeuriger, efficiënter en robuuster te maken. Het CWI draagt hieraan al vele jaren actief bij en past de daarmee opgebouwde expertise toe op stromingsproblemen die zich voordoen in de industrie.

Onderzoek op het CWI

Op het CWI rekent men aan stromingen ten behoeve van industriële toepassingen. Het kan daarbij gaan om gassen, vloeistoffen of combinaties van deze (tweefasen-stromingen). Het onderzoek richt zich op geavanceerde discretisatiemethoden voor systemen van niet-lineaire behoudswetten, multirooster- en ijlrooster-methoden, lokale rooster-aanpassing en gespreide (parallelle) berekeningen. De nadruk ligt momenteel op algoritmen voor waterstromingen met oppervlaktegolven. Het meeste onderzoek betreft toepassingen voor Nederlandse instellingen en industrieën, waarvan hier enkele voorbeelden volgen.

MARIN — Maritiem Research Instituut Nederland, Wageningen

MARIN's visceuze CFD-technologie betreft vooral stationaire Navier-Stokes methoden en het bijbehorende rekendomein de omgeving van achterstevens en een vlak wateroppervlak. Het CWI en MARIN onderzoeken samen uitbreiding naar niet-stationaire, volledige Navier-Stokes vergelijkingen, met toepassing op complete schepen (boeg en achtersteven) en met vrije oppervlaktegolven. De nieuw te ontwikkelen CFD-methoden zullen worden gebruikt voor de bestudering van stromingstopologieën om scheepsrompen (loslating en aanligging, wervelvorming, etc.), onder uiteenlopende vaarcondities (kruisen, trimmen, inzinken).

AKZO/Nobel Central Research, Arnhem

Het CWI heeft een Navier-Stokes methode ontwikkeld voor de berekening van de samendrukbare luchtstroming in een blazer, gebruikt bij het trekken van garens in een smelt-spinproces. Dit proces wordt toegepast voor het maken van niet-geweven stof, die de basis vormt voor vele andere produkten zoals tapijten, dakbedekking en verband. In het proces wordt een polymeer gesmolten en uitgeperst tot een grote hoeveelheid zeer dunne garens, die vervolgens met hoge snelheid door de blazer worden getrokken. Doel van het onderzoek was de ontwikkeling van een stromingsberekeningsmethode voor het ontwerp van de garenblazer, teneinde de relatief hoge bedrijfskosten daarvan te verminderen.

MacNeal-Schwendler, Europees Ontwikkelingscentrum, Gouda

Het CWI heeft een haalbaarheidsstudie verricht naar het ontwikkelen van een rekenmethode voor een speciale klasse van vrije-randvoorwaarde problemen, namelijk bewegende grensvlakken tussen materialen, met toepassingen in gebieden als smeden, klotsen en explosies. Vooral het smeden stelt zeer hoge eisen aan de nauwkeurigheid waarmee het grensvlak in de berekening wordt meegenomen.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/mas2

Dr.ir. B. Koren
Telefoon: 020 - 592 4114
E-mail: Barry.Koren@cwi.nl

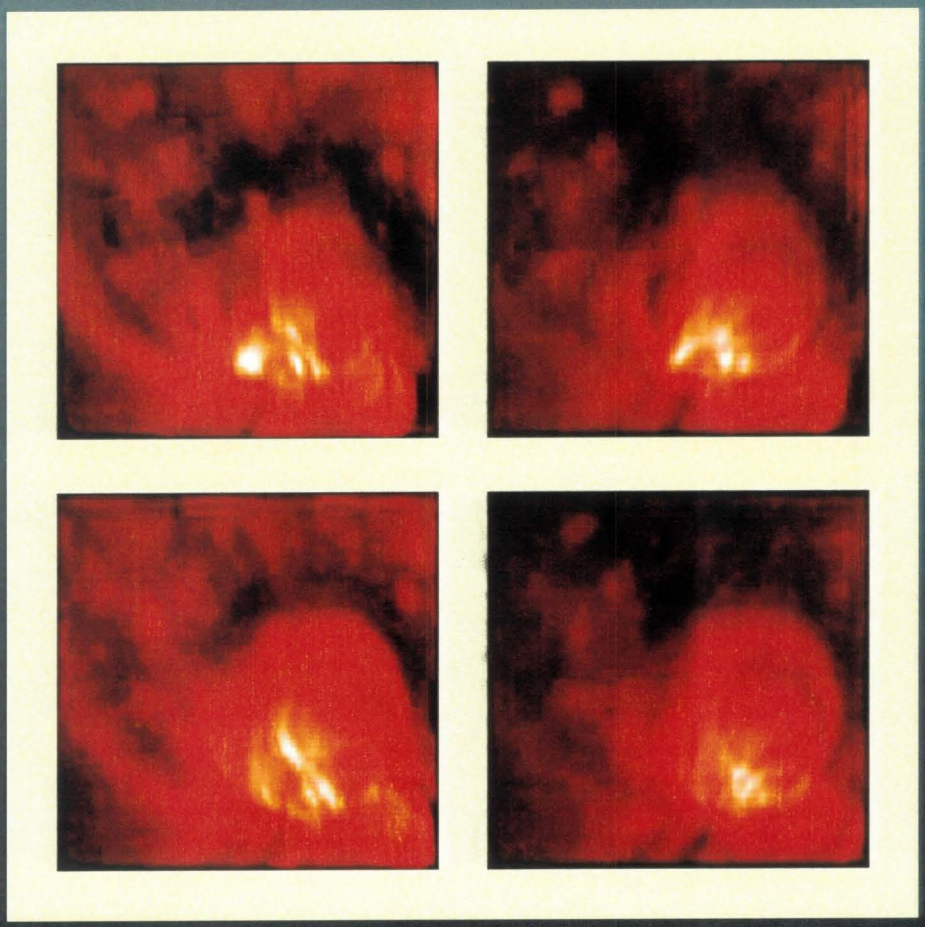
september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

GROOTSCHALIG REKENEN STEUNT OP PARALLELLE VERWERKING

De rekenkracht en het geheugen van de snelste computers zijn in de laatste twee decennia sterk toegenomen. Deze trend zal naar verwachting in het volgende decennium doorgaan en de toverformule luidt daarbij: massaal parallelle verwerking. De snelste computers van de toekomst zijn systemen en wereldwijde netwerken met vele duizenden parallelle processoren. Voor optimale benutting van zulke architecturen moeten nieuwe numerieke methoden ontwikkeld worden. Het CWI-onderzoek op dit terrein richt zich vooral op toepassingen in de stromingsleer en de cryptografie (getaltheorie).

De eerste parallelle (super)computer was de roemruchte ILLIAC IV, door Burroughs in 1972 aan het NASA Ames Research Center geleverd. De machine bestond uit een array van 64 floating-point processing elementen, ieder met een intern geheugen van 2048 woorden van 8 bytes: in totaal dus een geheugen van iets meer dan 1 M (miljoen) bytes. De klokperiode van de machine was 80 nanoseconden, wat overeenkomt met een snelheid van 12.5 MHz. De prijs van de toen zeer revolutionaire computer was oorspronkelijk begroot op 8 miljoen US dollars, maar liep uiteindelijk op tot 31 miljoen US dollars! Ter vergelijking: voor minder dan 4000 gulden koopt men nu een 2.0 GHz



Ontwikkeling van een actief gebied in de corona van de zon. Voor simulatie en bestudering van deze verschijnselen wordt gebruik gemaakt van parallelle algoritmen. (Foto: National Solar Obvervatory, Sacramento Peak.)

processor met 512 Mbytes intern geheugen. Snelheid en geheugen zijn dus met factoren van resp. 160 en 512 omhoog gegaan, terwijl de prijs met een factor van meer dan 30000 is gedaald (inflatie niet meegerekend).

Door deze enorme vooruitgang in snelheid en geheugen zijn de snelste en grootste computers van het ogenblik steeds beter in staat de werkelijkheid realistisch na te bootsen. Computersimulatie is zo een autonome derde richting van onderzoek geworden, naast de traditionele theoretische en experimentele richtingen. Op deze wijze kan men verschijnselen bestuderen die in het laboratorium een zeer lange tijd (duizenden jaren) of juist zeer korte tijd (enkele picoseconden) in beslag zouden nemen.

Toepassingen van grootschalige computersimulaties zijn bijvoorbeeld te vinden bij het ontwerpen van vliegtuigen, het ontwikkelen van nieuwe automodellen (botsingsproeven), de studie van de verspreiding van giftige stoffen in het milieu, wereldwijde klimaatstudies, het ontwikkelen van nieuwe geneesmiddelen, het doen van macro-economische voorspellingen, het ontwerpen van chips en het ontbinden in factoren van grote getallen (voor cryptografische toepassingen).

Met de door de natuur gestelde snelheidsgrenzen in zicht heeft men zich al geruime tijd geleden gerealiseerd dat er bij de bouw van toekomstige computersystemen alleen nog snelheidswinst valt te behalen door het gebruik van parallelle architecturen. Het doorrekenen van realistische wiskundige modellen vereist een dusdanige rekenkracht dat alleen zeer grootschalig parallellisme (machines met duizenden processoren) uitkomst kan brengen. Het grootste probleem is hierbij de communicatie: de rekenchips van al die processoren zijn zo snel dat de benodigde data niet snel genoeg kunnen worden aangevoerd. Ook het verwerken en analyseren van de resultaten stuit op grote problemen. Veel onderzoek wordt momenteel dan ook verricht naar grafische technieken voor het efficiënt zichtbaar maken van die resultaten. De voor massaal parallelle computers beschikbare software is over het algemeen nog van onvoldoende kwaliteit. De ontwikkeling van geschikte software tools komt langzaam op gang. Een bijkomend probleem is dat de hardware-ontwikkelingen zo snel doorgaan, dat tegen de tijd dat de software voor een bepaalde computer klaar is, deze al weer aan vervanging toe is. Portabiliteit (overdraagbaarheid) van software wordt daarom steeds belangrijker.

Vanaf 1984 doet het CWI onderzoek naar het optimaliseren van bestaande numerieke en getaltheoretische algoritmen voor vector- en parallelle computers en het ontwikkelen van nieuwe algoritmen. Daarbij wordt onder meer gebruik gemaakt van de bij SARA Reken- en netwerkdiensten opgestelde Cray C916 supercomputer en de IBM SP-2 en Parsytec CC-40 parallelle computersystemen, en van de bij de TU Delft opgestelde Cray T3E.

In het bijzonder onderzoekt het CWI parallelle algoritmen voor het berekenen van eigenwaarden van zeer grote ijle matrices, het gegeneraliseerde eigenwaardeprobleem, het oplossen van grote lineaire stelsels met minimalisatie van geheugengebruik, en multigrid-, en multi-precisie berekeningen. Toepassingen liggen onder andere op het gebied van de stromingsleer (bijvoorbeeld stromingen in ondiep water en rond vliegtuigvleugels) en in de magnetohydrodynamica (bijvoorbeeld de studie van verschijnselen in de corona van de zon en in kernfusiereactors). Ook bestudeert men het gebruik van software tools (zoals PVM en MPI) voor het op een machine-onafhankelijke wijze ontwikkelen en onderhouden van parallelle programmatuur.

Tenslotte heeft het CWI een wereldnaam opgebouwd met toepassingen van grootschalig rekenen in het zuiver wiskundig onderzoek, met deels zeer praktische implicaties (in de cryptografie). Zo werden uitvoerige berekeningen uitgevoerd aan de Riemann hypothese en aan de vermoedens van Mertens en Goldbach, drie klassieke wiskundige problemen; thans wordt onderzoek verricht naar snelle algoritmen voor het ontbinden van grote getallen in priemfactoren. Enkele malen heeft het CWI hierbij getallen van recordgrootte weten te kraken. In augustus 1999 is op dit gebied een grote doorbraak gerealiseerd: het is gelukt een 512-bits RSA sleutel in factoren te ontbinden. Dit type sleutel wordt momenteel veel gebruikt voor de beveiliging van dataverkeer over Internet. Aan dit onderwerp is een aparte fact sheet gewijd, met de titel: 'Ontbinding van grote getallen test veiligheid elektronisch dataverkeer'.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/mas2

Dr.ir. B. Koren
Telefoon 020 - 592 4114
E-mail: Barry.Koren@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

CWI

CLUSTER Information Systems

THEMA Multimedia and Human - Computer Interaction

NAAR DE AUTOMATISCHE CREATIE VAN HYPERMEDIA PRESENTATIES

Multimediatechnologie is inmiddels zo ver gerijpt dat duurzame elektronische publikaties van hoge kwaliteit, toegankelijk voor meerdere door een netwerk verbonden gebruikers, binnen handbereik zijn. Vanaf begin jaren negentig heeft de Multimedia and Human-Computer Interaction groep op het CWI methodes onderzocht om multimedia documenten te creëren en te presenteren waarmee het mogelijk is informatie slechts éénmaal te coderen en meerdere keren te gebruiken in de levenscyclus van het document.

Het onderzoek naar een grote diversitijd aan multimediatoepassingen stoelt op de grote ervaring van het CWI in de ontwikkeling van datamodellen, auteurssystemen en zogenaamde run-time ondersteuning voor heterogene afspeelomgevingen over computernetwerken met variabele bandbreedte. Een auteurssysteem wordt gebruikt om multimedia-documenten te organiseren; het is een soort opmaaksysteem voor documenten die tekst, illustraties, film en geluid bevatten. Concrete resultaten zijn het GR*i*NS auteurssysteem (dat geschreven is in de ook op het CWI ontwikkelde programmeertaal Python), het Amsterdam Hypermedia Model, dat grote interesse heeft gewekt in

Breedband Internet vergemakkelijkt de verspreiding van interactieve en gesynchroniseerde multimedia presentaties over het Web. De figuur laat een SMIL-presentatie zien van een van Rembrandts beroemdste schilderijen (met dank aan het Rijksmuseum Amsterdam).

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

onderzoekskringen en de taal SMIL -- een Recommendation van het World Wide Web Consortium (W3C) sinds juni 1998. Het GRiNS auteurssysteem werd in samenwerking met Europese partners in het kader van het EU-programma ESPRIT voortgezet en is daarna de commerciële wereld in gebracht door een nieuw bedrijf Oratrix Development b.v.

SMIL -- Synchronized Multimedia Integration Language -- is een specificatietaal ontwikkeld voor gesynchroniseerde interactieve multimedia presentaties op het Internet. SMIL vormt de eerste stap naar de toegang tot multimedia presentaties op het Internet in publieke formaten. Het is zowel mogelijk bestaande HTML browsers uit te breiden met een SMIL plug-in, als afzonderlijke SMIL-only browsers te maken. Het formaat, dat een XML toepassing is, is geschikt om eenvoudige multimedia presentaties met een standaard teksteditor te creëren. Voor ingewikkelder presentaties is een auteurssysteem, zoals GRiNS, gewenst. SMIL is ontworpen door de W3C werkgroep SYMM, waarin naast het CWI/Oratrix ook Canon, Compaq, CSELT, France Telecom, Gateway, GLOCOM, Intel, INRIA, Macromedia, Microsoft, NIST, Panasonic, Philips en RealNetworks hebben deelgenomen. De CWI-groep blijft in het kader van W3C actief bijdragen aan de verdere ontwikkeling van SMIL.

Hoewel 'duurzame' elektronische publicaties al wel handmatig gemaakt kunnen worden, vergt het produceren van een hypermedia presentatie nog steeds aanzienlijke inspanning. Bij grote hoeveelheden gegevens, of als de gegevens snel veranderen (bijvoorbeeld een nieuwsrubriek) is het twijfelachtig of het maken van complexe presentaties voor een eindgebruiker wel zo veel inspanning waard is. Het doel van het onderzoek is om het maken van presentaties te vereenvoudigen door het ontwerpproces zo veel mogelijk te automatiseren.

Een voorbeeld: uitgaande van een uitgebreid geannoteerde hypermedia database zou men automatisch presentaties kunnen genereren die zijn toegesneden op het platform van de eindgebruiker, de browser software en de netwerkfaciliteiten. Op basis van dezelfde inhoud kunnen dan multimedia Web-presentaties automatisch worden aangepast aan PC-gebruikers met een langzaam analoog modem, aan gebruikers met toegang tot breedband Internet (zie figuur 1), of aan gebruikers met een klein-scherm apparaat zoals een mobiele WAP telefoon (zie figuur 2). Bovendien zou men, als het proces voldoende kennis heeft over zaken als taak en kennisniveau van de gebruiker, automatisch de presentatie kunnen aanpassen aan de informatiebehoefte van die gebruiker.

Momenteel stoelen automatisch gegenereerde Webpagina's op vaste templates ingevuld door de database backend van de server, of op eenvoudige lijsten van links die de resultaten van een zoekmachine weergeven. Werkelijk adaptieve hypermedia presentaties vereisen echter een veel grotere flexibiliteit. Bij zo'n flexibele benadering moet voor de verschillende media de layout, volgorde in de tijd en hyperlinks bepaald worden op basis van ontwerpregels die de presentatie op maat maken voor de individuele gebruiker.

Dit onderzoek vindt thans plaats in het kader van het ITEA-project RTIPA en de NWO-projecten 'Semi-automatische generatie van hypermediapresentaties' en ToKeN2000.

Klein-scherm apparaten zoals mobiele telefoons hebben speciale vereisten voor presentaties.

Voor nadere informatie over dit onderzoek:
www.cwi.nl/ins2

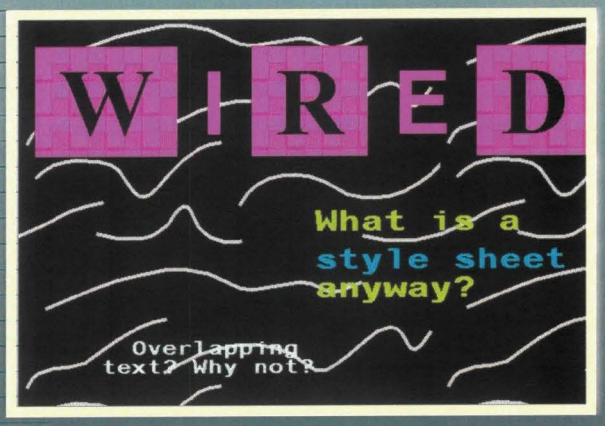
Prof.dr. L. Hardman
Telefoon: 020 - 592 4147
E-mail: Lynda.Hardman@cwi.nl

september 2001

Centrum voor Wiskunde en Informatica

WORLD WIDE WEB CONSORTIUM SCHEPT ORDE IN CHAOTISCHE INTERNET-WERELD

Door de explosieve wildgroei in het gebruik van Internet werd al snel de behoefte gevoeld aan een wereldwijde organisatie die de ontwikkelingen in goede banen leidt. Meer dan 500 bedrijven en instituten hebben daartoe het World Wide Web Consortium (W3C) gevormd. Het CWI, in 1988 al de eerste niet-militaire europese internet site, neemt als lid deel aan de activiteiten van W3C, ook via mede-lid ERCIM (het European Consortium for Informatics and Mathematics).



Schattingen lopen ver uiteen, maar gemiddeld schat men de huidige groei van Internet op een verdubbeling van de omvang elke 50 dagen, terwijl er elke 4 seconden een WWW homepage bijkomt. Deze groei gaat gelijk op met de groei in het aantal toepassingen die worden ontwikkeld voor het gebruik van Internet. Vroeger, toen Internet nog een kleine omvang had, werden de nieuwe ontwikkelingen geleid door de Internet Engineering Task Force IETF. In het razendsnelle WWW-tijdperk, waarin men al spreekt van 'Web-jaren' (zoals een hond-jaar, gelijk aan 7 mens-jaren), vond een stortvloed van nieuwe ontwikkelingen plaats buiten de tot dan formeel overeengekomen kanalen. Daardoor ontstond het gevaar dat Internet zou ontaarden in een broedplaats van concurrerende en tegenstrijdige protocollen zonder enige samenhang, waarmee een van de sterke punten van het World Wide Web zou worden teniet gedaan.

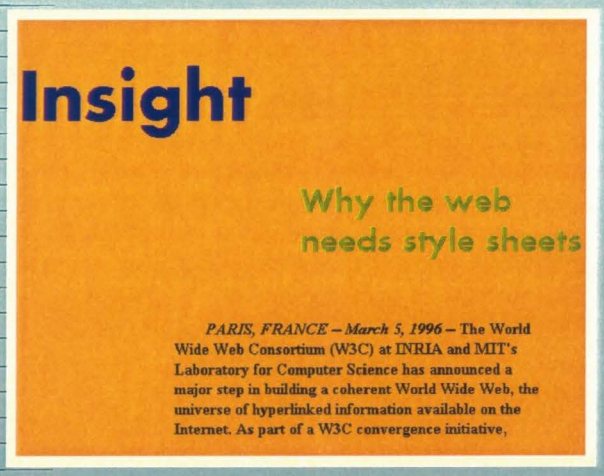
Om dit gevaar te bezweren is het World Wide Web Consortium W3C opgericht, volgens het model van het succesvolle X-consortium dat de ontwikkelingen van het X Window systeem coördineert. W3C bestaat thans uit meer dan 500 bedrijven en instituten die alle zijn geïnteresseerd in een ordelijke verdere ontwikkeling van WWW. Het consortium wordt vertegenwoordigd door het Institut National de Recherche en Informatique et Automatique (INRIA) in Europa, het Laboratory for Computer Science van het Massachusetts Institute of Technology (MIT/LCS) in de VS, en de Keio Universiteit in Japan. W3C heeft in verschillende landen kantoren gevestigd. In Nederland bevindt dit zich op het CWI.

W3C stelt zich ten doel voor het Web gemeenschappelijke specificaties te vinden, waardoor veel bedrijven onder de voortdurende snelle en dramatische veranderingen toch op hun eigen terrein kunnen opereren, daarbij bouwend op het door het Web gevormde globale informatiekader. Omdat de bij het Web gebruikte technologie zeer snel verandert, moet het W3C Consortium efficiënt en flexibel opereren, teneinde tijdig in te kunnen spelen op de behoeften van de gebruikersgemeenschap. Tevens moet W3C zich duidelijk profileren als een neutraal forum, waarbij geen enkel lid a priori een zwaarder gewicht heeft dan de andere leden.

Het W3C consortium richt zich vooral op de volgende onderzoeksgebieden:

- nieuwe versies van Web protocollen en data formats, zoals HTTP, XML, XHTML, Style Sheets, graphics formats en fonts;
- real time: audio en video;
- internationalisering van protocollen en data formats;
- Content Rating protocollen, waarmee niet alleen bijvoorbeeld materiaal als 'voor volwassenen' kan worden aangemerkt, maar de inhoud op elke schaal en met betrekking tot elk onderwerp kan worden gewaardeerd;
- privacy en demografie;
- digitale handtekeningen;
- elektronische handel en veilige elektronische betaalsystemen;
- rechten van intellectueel eigendom;
- toegang voor gehandicapten.

PARIS A-H
LESPAGES JAUNES


Insight

Why the web needs style sheets

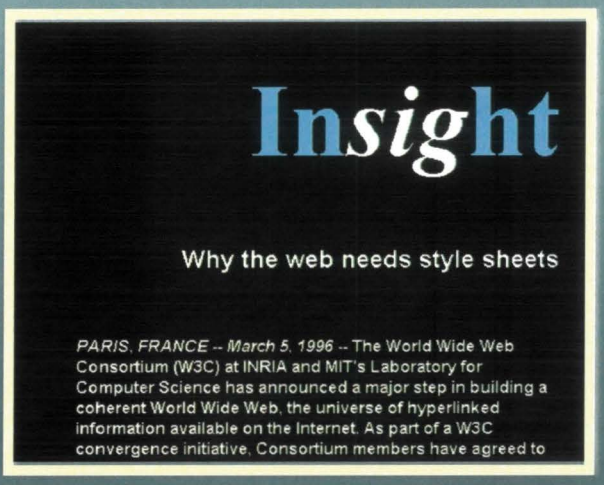
PARIS, FRANCE – March 5, 1996 – The World Wide Web Consortium (W3C) at INRIA and MIT's Laboratory for Computer Science has announced a major step in building a coherent World Wide Web, the universe of hyperlinked information available on the Internet. As part of a W3C convergence initiative,

Het CWI werkt actief mee in een aantal W3C-werkgroepen, zoals CSS (Style Sheets), HTML en Forms (beide voorgezeten door Steven Pemberton) en Multimedia. Zo had het CWI een belangrijk aandeel in het ontwikkelen van de specificatietaal SMIL, die in juni 1998 een officiële W3C Recommendation werd (zie de fact sheet 'Multimedia auteurs-systemen voor duurzame elektronische publikaties'). Ook neemt het CWI deel in de activiteiten van het W3C consortium door het detacheren van onderzoekers bij de Europese W3C-vertegenwoordiger INRIA en via W3C-lid ERCIM (European Research Consortium for Informatics and Mathematics, in 1989 opgericht door CWI, INRIA en het Duitse GMD).

Style Sheets vormen een voorbeeld van het soort werk dat tot het terrein van W3C behoort. HTML is de taal waarmee de structuur van over het Web verzonden documenten wordt beschreven, in de trant van: dit is een kop, dit is een alinea, enzovoorts. De taal legt echter niet vast hoe het document er op het scherm of in afdruk uitziet. De Style Sheet notatie CSS (Cascading Style Sheets) is een afzonderlijke, maar verwante notatie waarmee kan worden aangegeven hoe een document of groep documenten er op het scherm of op een pagina zou moeten uitzien. Daarbij kan de gebruiker beslissen over zaken als fonts, kleur en positionering. CSS heeft als groot voordeel boven de tot nu toe gebruikte, enigszins willekeurige methoden voor het opmaken van Web-documenten dat het zeer snel is te laden vergeleken met de thans in gebruik zijnde grote en ingewikkelde beeld-files. Bovendien geeft CSS controle over het uiterlijk van een complete website vanuit een enkele plaats. Wie de huisstijl wil aanpassen hoeft dit slechts eenmaal te doen, waarna alles meeverandert; de documenten zelf kunnen onaangeroerd blijven. Nu de twee grote browser producenten, Microsoft en Netscape, browsers op de markt hebben gebracht die deze Style Sheet technologie bevatten, gevolgd door een groot aantal 'embedded' browsers, gebruikt nu meer dan 95% van alle gebruikers een CSS-enabled browser.

CSS is een technologie die XML mogelijk heeft gemaakt. XML is een nieuw, aanbevolen gegevensformaat voor het versturen van documenten over het Web. Het is een vereenvoudigde versie van SGML, de metataal gebruikt voor de definitie van HTML. Door die vereenvoudiging is XML veel gemakkelijker te implementeren, en ligt daarom dichter onder bereik van de doorsnee Web-gebruiker.

Met XML kan men zijn eigen data-talen (zoals HTML) definiëren, waardoor de vroegere problemen, waar de producenten van browsers elk hun eigen HTML-tags uitvonden, tot het verleden behoren. Nu kan iedereen nieuwe tags definiëren zonder dat daarvoor een nieuwe browser nodig is. Omdat deze nieuwe tags echter geen basis-presentatie hebben, wordt CSS essentieel voor het vertonen van documenten met gebruik van de nieuwe tags.


Insight

Why the web needs style sheets

PARIS, FRANCE -- March 5, 1996 -- The World Wide Web Consortium (W3C) at INRIA and MIT's Laboratory for Computer Science has announced a major step in building a coherent World Wide Web, the universe of hyperlinked information available on the Internet. As part of a W3C convergence initiative, Consortium members have agreed to

Ondanks de komst van XML is er nog steeds een duidelijke behoefte aan een standaard markup. Daarom wordt er een nieuwe versie van HTML gedefinieerd, die XML gebruikt en XHTML wordt genoemd. De eerste versie, XHTML 1.0, is een overgangsversie die werkt voor zowel bestaande browsers als met nieuwe XML browsers. XHTML 1.1 is een opgeschoonde versie, waaraan markup voor Aziatische talen is toegevoegd. XHTML Basic is een versie vvor kleine apparaten zoals telefoons. Een volledig herziene versie is in voorbereiding. Daarin zijn vele nieuwe ontwikkelingen, zoals nieuwe vormen van elektronische handel, geïntegreerd.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/ins0, www.w3.org

Steven Pemberton (voorzitter HTML Working Group)
Telefoon: 020 - 592 4138
E-mail: Steven.Pemberton@cwi.nl

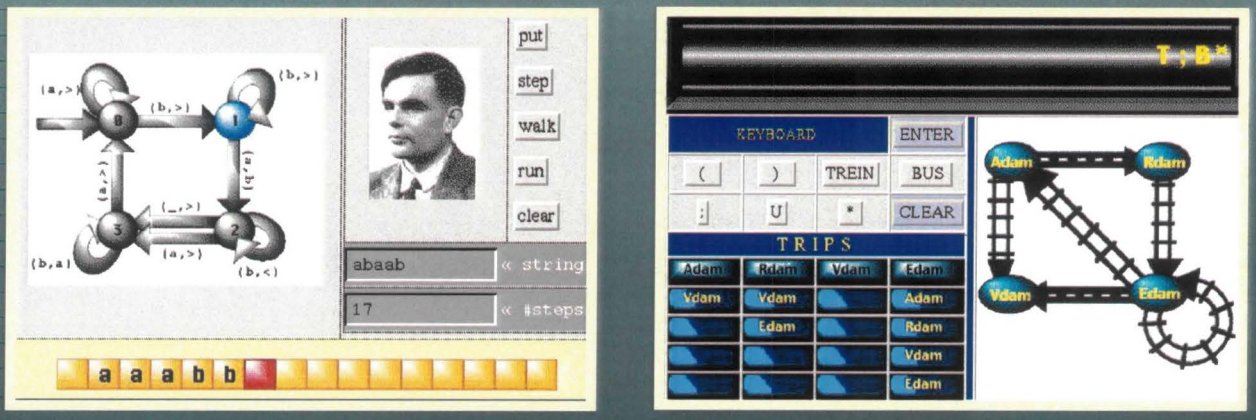
september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

LOGICA EN BEREKENING – DISSEMINATIE VAN DE KERNIDEEËN

Evenals het differentiaal- en integraalrekenen de kern was van de natuurwetenschappelijke revolutie uit de zeventiende eeuw, vormt de logische theorie over berekenbaarheid en bewijsbaarheid de kern van de informatierevolutie waar we nu middenin zitten. De hoofdideeën van het mechaniseren van redeneren en rekenen verdienen een plaats in het denken van iedere geïnteresseerde burger met een bêtaachtergrond. Logici en informatici slaan de handen ineen om ervoor te zorgen dat de kern van hun denkwereld het algemene publiek bereikt.



Twee voorbeelden van interactief logica onderwijs via Internet: een Turing-machine (links) en een vereenvoudigd Kripke model voor de trein- en busverbindingen tussen vier steden (rechts).

Het succes van de natuurwetenschappelijke revolutie van de zeventiende eeuw was in niet geringe mate te danken aan het feit dat de manier van denken van Newton, Leibniz en Huygens het algemene wereldbeeld beïnvloedde. Voltaire maakte reclame voor Newton's Principia. Differentiëren en integreren werden binnen enkele generaties opgenomen in het middelbare school curriculum. Het mechanistische wereldbeeld werd gemeengoed. Ons informatiseringstijdperk heeft dezelfde potentie om het wereldbeeld te beïnvloeden, en het is de taak van informatie-wetenschap in het algemeen, en logica in het bijzonder, om te zorgen dat de logisch/mathematische kijk op informatie, informatiegroei, informatieverwerking en informatieoverdracht een plaats krijgt in het denken van iedereen die aan het begin van de eenentwintigste eeuw een middelbare of universitaire opleiding geniet.

De fragmentatie van kennis die wordt veroorzaakt door overspecialisatie draagt bij aan de slechte naam van wetenschap bij het algemene publiek, en die slechte naam betekent voor een op wetenschap gebaseerde democratische samenleving als de onze een ernstig gevaar. Wetenschapsbeoefenaars kunnen helpen de fragmentatie van kennis een halt toe te roepen door wetenschappelijk inzicht geïntegreerd toegankelijk te maken voor een breed publiek. Dit creëert dan tevens het broodnodige maatschappelijk draagvlak voor verdere steun aan wetenschappelijk onderzoek.

Logica en Berekening — Disseminatie van de kernideeën' is een samenwerkingsprogramma van het CWI en het ILLC (Institute for Logic, Language and Computation) van de Universiteit van Amsterdam. Het maakt deel uit van het SPINOZA-programma Logic in Action onder leiding van prof.dr. J. van Benthem (Universiteit van Amsterdam), dat wordt gefinancierd door de Nederlandse organisatie voor Wetenschappelijk Onderzoek NWO. Doel van het samenwerkingsprogramma is een systematisch perspectief uit te dragen op ons werkterrein als geheel, door middel van een reeks boeken met multimedia ondersteuning via internet. Voor dit doel is samenwerking gezocht met AUP (Amsterdam University Press), om een boekjes-serie 'informatie in context' op te zetten.

Het eerste deeltje in deze reeks, 'Computers, Rekenen, Redeneren' is geschreven door Jan van Eijck, Jan Jaspars, Jan Ketting en Marc Pauly, met internet-toepassingen geschreven door Jan Jaspars.

Hier volgt wat nadere informatie over deeltjes (met internet ondersteuning) die nog op stapel staan.

- *Computers, rekenen, redeneren:* Korte geschiedenis van het mechanisch rekenen. Binaire representatie, rekenen en verbanden met propositielogica. Modellen van mechanische berekening. Programmeren en complexiteit van problemen.

- *Logica en Bewijs:* Bewijs is een kernbegrip in het wiskundig redeneren. Wat is de algemene structuur van een wiskundig bewijs? Hoe helpt logica om deze structuur te doorzien?

- *Programmeren en Redeneren:* Welke ingrediënten hebben programmeren en redeneren gemeen? Hoe kun je logica gebruiken om programma's beter te begrijpen, en hoe kun je omgekeerd, de activiteit van logische bewijsvoering programmeren?

- *Logica, Grammatica en Betekenis:* Hoe kan taalstructuur worden beschreven met formele middelen? Wat zijn de overeenkomsten tussen ontleden en bewijsvoeren? Hoe kan de betekenis van een zin worden afgeleid uit de betekenissen van de samenstellende delen?

- *Kennis, Informatiegroei en Leren:* Hoe vallen de processen van kennisverwerving en leren op grond van ervaring formeel (wiskundig precies) te begrijpen?

- *Codes en Geheimschrift:* Van een korte geschiedenis van cryptografie en cryptanalyse naar een overzicht van de huidige stand van zaken.

Kerndoel van Logica en Berekening — Disseminatie van de kernideeën' is om de banden tussen universitair en voorbereidend wetenschappelijk onderwijs op ons terrein weer nauwer aan te halen. Op nationaal vlak wordt hiertoe samengewerkt met de Stichting Vierkant voor Wiskunde, een initiatief om het wiskunde onderwijs in Nederland een nieuwe impuls te geven. Internationaal wordt samengewerkt in het kader van COMPULOG (een door de EU gefinancierd Network of Excellence) met verscheidene initiatieven op het gebied van courseware ontwikkeling in computationele logica.

Voor nadere informatie over dit CWI-onderzoek:
`www.cwi.nl/ins0/`

Prof.dr. J. van Eijck en Marc Pauly M.Sc.
Telefoon 020 - 592 4052/4227
E-mail: Jan.van.Eijck@cwi.nl, Marc.Pauly@cwi.nl

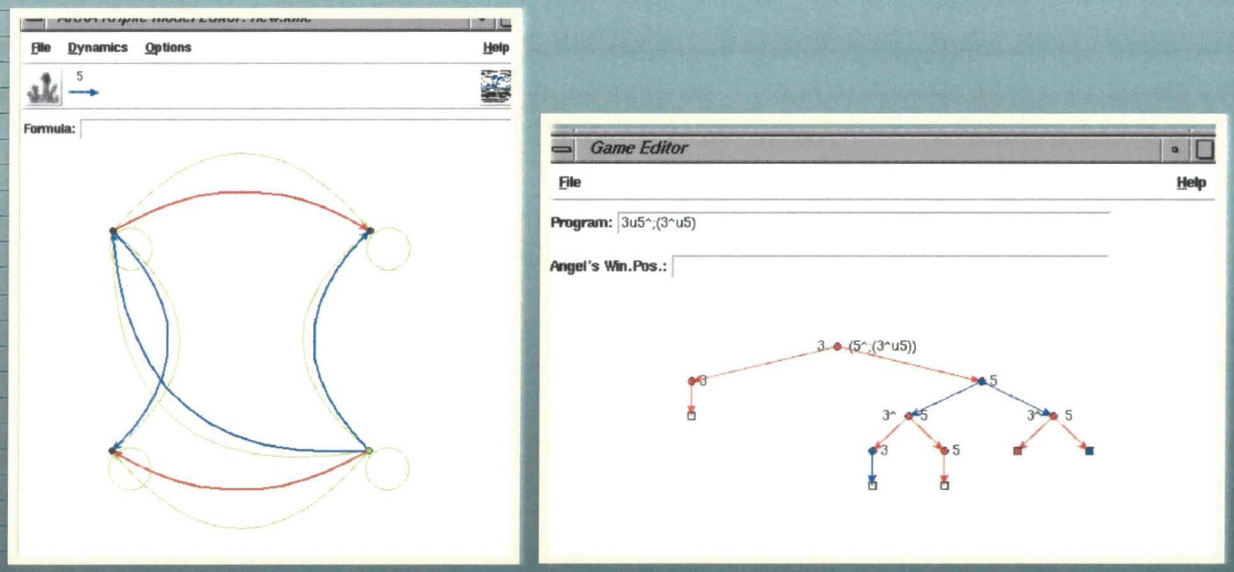
september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

Centrum voor Wiskunde en Informatica

INFERENTIEMACHINES DRIJVENDE KRACHT ACHTER REDENEERPROCESSEN

Inferentiemachines zijn redeneerprogramma's die onderdeel uitmaken van bijvoorbeeld programmeertalen, elektronische boeken en dergelijke. Automatisering van redeneren is een vorm van toegepaste logica. Het CWI wil inferentiemachines onder meer inbouwen in modern cursusmateriaal op het gebied van logica.



Spelboom (rechts) behorend bij een niet-deterministisch proces (links). De computer kan op vele manieren worden ingeschakeld bij het onderwijs en onderzoek in de logica.

In inferentiemachines worden verschillende technieken gebruikt:

Resolutie redeneertechnieken - De resolutieregel stelt ons bijvoorbeeld in staat om uit (A of B of C) en (niet C of D of E) te concluderen tot (A of B of D of E). Resolutie is in feite een iets andere verschijningsvorm van de bekende redeneerregel Modus Ponens. Immers, de tweede premisse in bovenstaande redenering is equivalent aan: (C → (D of E)).

Tableaux redenering, modelconstructie en modeltoetsing - Een tableaux redenering is een vorm van systematisch zoeken naar een tegenvoorbeeld om een redenering te weerleggen. Zo'n tegen voorbeeld is een logisch model - een situatie waarin zekere elementaire feiten waar zijn en andere onwaar - waarin de premissen van de redenering waar zijn, terwijl de conclusie onwaar is.

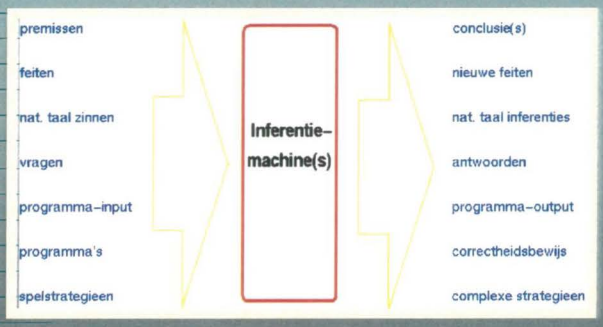
Dynamische logica redeneertechnieken - Dynamische logica is de logica van acties en hun begin- en eindvoorwaarden. Voorbeelden van premissen in dynamische logica zijn: 'steeds nadat actie a is uitgevoerd is A het geval en steeds nadat actie b is uitgevoerd is B het geval'. Volgt hier nu uit: 'Steeds nadat acties a en b zijn uitgevoerd zijn A en B het geval'? Niet zonder meer: het resultaat kan bijvoorbeeld afhangen van de volgorde waarin a en b worden uitgevoerd, of van de vraag of er interactie is tussen de twee acties a en b.

Term-unificatie - Unificatie van uitdrukkingen is een techniek om uitdrukkingen die variabelen bevatten aan elkaar gelijk te maken door het toepassen van een geschikte substitutie. De termen a(b,Y) en a(Z,f(Z)) worden geünificeerd door de substitutie van b voor Z en f(b) voor Y.

Term-herschrijving - Herschrijving is het maken van elementaire rekenstappen door een uitdrukking te vervangen door een eenvoudiger uitdrukking met dezelfde betekenis. Zo kan (1+3)+5 worden herschreven tot 4+5, en die nieuwe vorm is een stukje dichter bij de uitkomst 9. Een meer geavanceerde vorm is nodig voor de studie van functionele programma's zoals het volgende: een = '1': een. Uitvoering van dit

programma levert een oneindige stroom 1-en op het scherm. Dit valt als volgt te begrijpen. 'een' staat hier voor een proces dat bestaat uit twee onderdelen: ten eerste een '1' schrijven, en ten tweede het 'een' proces opnieuw uitvoeren. Zo'n proces is ook weer te geven in een graaf. De theorie over de reductie van dit soort uitdrukkingen heet dan ook wel graaf-herschrijving.

Lambda reductie en type-inferentie - Lambda notatie is een universele notatie voor functionele uitdrukkingen. De actie '3 erbij optellen' ziet er in deze notatie uit als $\lambda x.x+3$. Als je deze functie toepast op het getal 5 is de uitkomst 5+3. De reductie van $(\lambda x.x+3)(5)$ tot 5+3 heet lambda reductie of conversie. In principe kan elk rekenproces als een proces van opeenvolgende lambda conversie stappen worden gezien.



Inferentiemachines spelen een rol in de volgende toepassingen:

- Instructie-programma's in wiskunde en logica
- Presentatie van wiskunde en logica in elektronische studieboeken
- Analyse van natuurlijke taal
- Automatische verificatie van bewijzen en van programmatuur
- Ontwikkeling van functionele en logische programmeertalen.

Het CWI onderneemt een aantal activiteiten op dit terrein:

Cursusontwikkeling Redeneren en Rekenenen

In samenwerking met de UvA (Dr. Kees Doets, ILLC) wordt gewerkt aan een cursus 'Logic, Representations and Proofs', waarin inleiding in de mathematische bewijsvoering hand in hand gaat met representatie van formele definities als functionele programma's.

Programmatuur voor Practicum Computationele Semantiek

In samenwerking met de Universiteit van Amsterdam (Yde Venema, ILLC) werd een practicum computationele semantiek ontwikkeld, gebaseerd op implementaties van een reeks mini-programmeertalen voor imperatief, functioneel en logisch programmeren. Dit practicum is een integraal onderdeel van een doctoraalcollege Computationele Semantiek voor studenten informatica en wiskunde.

Spellogica's

Marc Pauly werkt op het CWI aan een proefschrift over logische perspectieven op spelen. Onderwerpen zijn onder andere de interactie tussen de spelers en hun strategieën, het construeren van complexe spelen uit simpele spelen en verbanden tussen spel-theoretische noties zoals determinisme en logische wetten, bijvoorbeeld de wet van de uitgesloten derde.

LoLaLi Exemplar

In samenwerking met Elsevier Science BV wordt gewerkt aan een exemplarisch elektronisch handboek 'Logic and Language', waarin inferentiemachines aan het werk worden gezet om nieuwe ontwikkelingen in Logica en Taalanalyse te demonstreren.

Dynamo: Programmeren met Dynamische Logica

Dynamo, ontwikkeld door Jan van Eijck, is een programmeertaal gebaseerd op een dynamische interpretatie van eerste-orde logica (DPL). Aangezien DPL een logica voor het modelleren van natuurlijke taal voorstelt, wordt verwacht dat Dynamo als inferentiemachine zowel voor eerste-orde logica als voor natuurlijke taal kan worden gebruikt. Een prototype van Dynamo werd in Haskell geïmplementeerd.

Deze activiteiten worden mede gesteund vanuit NWO, het SPINOZA programma 'Logic in Action' onder leiding van prof. J. van Benthem (Universiteit van Amsterdam) en Elsevier.

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/ins0/

Prof.dr. J. van Eijck
Telefoon 020 - 592 4052
E-mail:Jan.van.Eijck@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl

ONTBINDING VAN GROTE GETALLEN TEST VEILIGHEID ELEKTRONISCH GEGEVENSVERKEER

Op 22 augustus 1999 werd op het CWI een getal van 512 bits (155 cijfers) in factoren ontbonden. Zo op het oog niets meer dan de zoveelste ontbinding in een lange reeks, waarin het CWI de laatste vijftien jaar diverse malen wereldrecords brak. Hier was echter sprake van een mijlpaal: voor het eerst was een getal gekraakt dat model staat voor een populaire sleutel voor de beveiliging van het Internet en van bijvoorbeeld transacties in de financiële wereld.

De uitvinders van het RSA cryptosysteem in 1978: R.L. Rivest, A. Shamir en L. Adleman (van links naar rechts). Foto: RSA Data Security Inc.

Een veel gebruikte versleutelingsmethode is RSA, ruim twintig jaar geleden bedacht door Rivest, Shamir en Adleman op het MIT in de VS, en sindsdien op grote schaal gebruikt in hardware en software voor de beveiliging van gegevensstromen. Deze 'public-key' methode berust op de moeilijkheid om, gegeven het produkt van twee goed gekozen 'grote' priemgetallen, die priemgetallen weer terug te vinden. De vraag is nu: hoe groot is groot genoeg om dat terugvinden inderdaad vrijwel onmogelijk te maken? Zo'n tien jaar geleden dacht men nog met priemgetallen van zo'n 50 cijfers wel goed te zitten, maar de ontwikkelingen verliepen veel sneller dan voorzien. Het is dan ook een hachelijke zaak op dit gebied kwantitatieve voorspellingen te doen. Rivest daagde in 1977 de wereld uit om RSA-129, een getal van 129 cijfers uit een speciale lijst, te kraken. Hij schatte dat met de toen bestaande rekentechnieken en computersystemen dit 10^{16} jaar zou duren. Zeventien jaar later werd de klus in acht maanden geklaard in een wereldwijde samenwerking.

Hierbij moet men overigens bedenken dat het nog altijd mogelijk is dat er een rekenmethode wordt gevonden waardoor factoriseren niet meer een 'moeilijk' probleem is (bijvoorbeeld quantum computing, als er ooit een werkende quantumcomputer wordt gerealiseerd).

Public key cryptografie is vooral geschikt voor systemen met vele gebruikers, zoals het Internet. Bij deze methode kiest iedere gebruiker twee priemgetallen en een zogenaamde exponent (allemaal 'grote' getallen) en maakt alleen de exponent en het produkt van de priemgetallen bekend (de 'public key'). Iedereen die hem een boodschap wil sturen vercijfert deze boodschap met behulp van het bekend gemaakte produkt en de exponent. Die vercijfering zit zodanig in elkaar dat alleen wie de oorspronkelijke priemgetallen kent, de boodschap kan ontcijferen. (Een belangrijk onderdeel van de truc berust op modulair rekenen, 'klokrekenen'.) Daarmee hangt de veiligheid van deze methode af van de mogelijkheid van anderen om het produkt in factoren te ontbinden.

Het ontbinden in factoren is heel lang een zuiver wiskundige aangelegenheid geweest, zonder enige praktische toepassing. Het eenvoudigst is gewoon de rij priemgetallen 2, 3, 5, ... aflopen en kijken welke het te factoriseren getal delen. Dat is echter niet erg economisch en er zijn inmiddels veel betere methoden. De nieuwste, de Quadratic Sieve (QS) en de Number Field Sieve (NFS), berusten op een oud idee van Pierre de Fermat (1601 -- 1665), die constateerde dat elk oneven samengesteld getal N is te schrijven als het verschil van twee kwadraten: $N = x^2 - y^2 = (x+y)(x-y)$. Hebben we zulke getallen x en y gevonden, dan heb-

ben we dus ook factoren van N te pakken. Dat vinden gebeurt met een zeefproces (vandaar de term Sieve), waarin mogelijke waarden van x en y worden uitgesloten. Het zeefproces bestaat uit het op zeer efficiënte wijze verzamelen van 'relaties': getalparen a en b, die alleen 'kleine' priemfactoren bevatten, en zodat N een deler is van het verschil a - b. Voor grote N zijn in het algemeen zeer veel relaties nodig om de factoren te vinden (voor RSA-130 bijvoorbeeld 70 miljoen). Bij QS bestaan de relaties uit gewone getallen, bij NFS zijn dat algebraïsche getallen (bijvoorbeeld $3+2\sqrt{2}$).

De RSA-getallen behoren tot een lijst opgesteld door het Amerikaanse bedrijf RSA Data Security, Inc., dat licenties en produkten verkoopt die gebaseerd zijn op de RSA-methode. Zo hoopt het bedrijf goed zicht te houden op de kracht van ontbindingsmethoden en het kraken van getallen op deze lijst is een graadmeter voor de veiligheid van RSA. Van getallen met een speciale structuur, bijvoorbeeld van de vorm $a^b \pm 1$, zijn er al met een aanzienlijk hoger aantal cijfers ontbonden. Het CWI is ook hier wereldrecordhouder: in april 1999 werd $(10^{211} - 1)/9$, een getal van 211 cijfers, gekraakt met de Special Number Field Sieve, een versie van NFS die speciaal geschikt is voor dit soort getallen.

De inspanning hiervoor was vergelijkbaar met het kraken van RSA-140. De gebruikte methoden vormden een vingeroefening voor het kraken van RSA-155, dat gebeurde met de General NFS, de krachtigste methode tot nu toe.

Voor RSA-155 stonden zo'n 300 zeer snelle SGI en SUN workstations en Pentium II PC's in totaal 35 jaar te rekenen. Doordat dit grotendeels parallel gebeurde nam de klus slechts zeven kalendermaanden. Computertijd werd ter beschikking gesteld door Citibank (VS), CWI (Nederland), École Polytechnique (Frankrijk), Entrust Technologies (Canada), Centre Charles Hermite (Frankrijk), Lehigh University (VS), Microsoft Research (UK), Sun Microsystems (UK) en de University of Sydney (Australië). Daarnaast is op de Cray C916 supercomputer van het academisch rekencentrum SARA een essentiële stap van het rekenwerk verricht die extreem veel intern geheugen vroeg. Deze job kon in ongeveer in tien kalenderdagen worden voltooid. Tegenwoordig zijn er al gespreide rekenprojecten met tienduizenden PC-bezitters. Dit, en parallellisering van de rekenstap op de supercomputer (nog in onderzoek), doet verwachten dat de factorisering van getallen van 512 bits binnenkort nog slechts enkele dagen zal vergen.

RSA-155 =

**109417386415705274218097073220403576120037329454492059909138421314763499842889\
347847179972578912673324976257528997818337970765372440271467435315933543338 97**
=
102639592829741105772054196573991675900716567808038066803341933521790711307779
*****
106603488380168454820927220360012878679207958575989291522270608237193062808643

Voor nadere informatie over dit CWI-onderzoek:
www.cwi.nl/mas2/

Dr.ir. H.J.J. te Riele,
tel. 020 - 592 4106
e-mail: Herman.te.Riele@cwi.nl

september 2001

CWI - Centrum voor Wiskunde en Informatica Kruislaan 413 1098 SJ Amsterdam Telefoon 020 592 9333 Telefax 020 592 4199 http://www.cwi.nl