



TECHNOLOGIE OVERDRACHT

8 oktober 1993

CWI, Kruislaan 413, 1098 SJ Amsterdam

Over dit thema organiseert het
Centrum voor Wiskunde en Informatica op vrijdag 8 oktober a.s.
de jaarlijkse manifestatie:

CWI IN BEDRIJF

Technologie Overdracht

Het benutten van het omvangrijke kennispotentieel van de Nederlandse universiteiten en onderzoeksinstituten door de industrie verloopt, als het al tot stand komt, niet altijd even vlekkeloos. Omgekeerd blijkt het voor de onderzoekswereld niet altijd eenvoudig om maatschappelijk belangrijke problemen te betrekken bij het formuleren van de onderzoeksdoelstellingen. Tegelijkertijd wordt meer dan ooit beseft dat een effectieve overdracht van kennis en technologie van levensbelang is voor onze op kennis gebaseerde economie.

Kortom, technologie overdracht is meer dan ooit noodzakelijk, maar de werelden van onderzoek en bedrijfsleven sluiten allerminst naadloos op elkaar aan.

Reden genoeg voor het CWI om een aantal belangrijke actoren in dit veld aan het woord te laten. Namens het bedrijfsleven zal de heer **Rinnooy Kan** zijn visie op het onderwerp geven, terwijl de heer **Slagmolen** specifiek vanuit de computerservice industrie zijn gedachten over technologie overdracht zal laten gaan.

Vanuit het onderzoek spreekt de heer **Van Oortmerssen**, terwijl ook de overheid haar kijk op het probleem zal geven in de persoon van de heer **Tindemans** van het Ministerie van Onderwijs en Wetenschappen.

Presentaties

Naast deze inleidingen over het onderwerp, wordt ook concreet aan technologie overdracht gedaan tijdens deze "CWI in Bedrijf".

Het terrein van de **software-verificatie** is bij uitstek een gebied waar veel wetenschappelijk onderzoek wordt gedaan en waar praktische toepassingen weliswaar veelbelovend, maar nog niet erg talrijk zijn. Ofschoon het evident mag lijken dat software correct moet zijn, is dat in de praktijk veelal niet het geval omdat de kosten van het opsporen en verwijderen van de fouten vele malen hoger zijn dan de klant kan en wil betalen. De presentatie zal met name ingaan op het belang van het gebruik van formele methoden bij het ontwikkelen en verifiëren van software.

Een onderwerp dat zeer in de belangstelling staat is dat van **elektronisch geld**. Op het CWI wordt al geruime tijd belangrijk **cryptografisch onderzoek** gedaan om elektronisch geld uit te rusten met de goede eigenschappen van het traditionele geld (anonimiteit en privacy bescherming) en van elektronisch betalen (veiligheid). Het CWI coördineert een groot Europees onderzoeksproject op dit gebied dat gericht is op het introduceren van één elektronisch betaalsysteem voor Europa.

Het is mogelijk om verbanden tussen gegevens in databases op het spoor te komen met behulp van een techniek die bekend staat als **datamining**. "*Haal meer uit uw eigen databestanden*" is het thema van de presentatie over datamining. Terwijl gebruikelijke statistische technieken slechts veronderstelde verbanden toetsen, gaat het bij datamining om het actief opsporen van verbanden door de database programmatuur zelf.

Op het gebied van **multimedia** werkt het CWI, in het kader van een groot ESPRIT-project, aan de ontwikkeling van een software-basis voor multimedia toepassingen. Daarnaast is op het CWI een belangrijke standaard ontwikkeld voor het creëren van transporteerbare multimedia documenten binnen een gespreide heterogene omgeving.

Demonstraties

De gehele dag door zullen demonstraties gegeven worden van lopend CWI-onderzoek. Zo kunt u zich op de hoogte stellen van recente ontwikkelingen op het gebied van het visualiseren van grote gegevensstromen, van het maken van compilers voor parallelle computersystemen, van systeem- en regeltheorie, van computer-algebra en nog veel meer.

Programma CWI in Bedrijf 8 oktober 1993

- 10.00 Ontvangst
- 10.25 Opening – Prof.dr. P.C. Baayen (wetenschappelijk directeur CWI)
- 10.30 Technologie overdracht (bezien vanuit de onderzoekswereld)
– dr.ir. G. van Oortmerssen
- 11.00 Technologie overdracht (bezien vanuit de software industrie)
– dr. M.H. Slagmolen (bestuur Cossio)
- 11.30 Pauze
- 12.00 Mensen, kennis en informatie - investeren in vaste activa
– dr. P.A.J. Tindemans (directeur onderzoek- en wetenschapsbeleid Ministerie van O & W)
- 12.30 Wetenschap- en Industriebeleid – dr. A.H.G. Rinnooy Kan (voorzitter VNO)
- 13.00 Lunch
- 14.30 Schatgraven in je eigen databestanden – dr. A.P.J.M. Siebes
- 15.00 Verificatie van een audio protocol – dr. F.W. Vaandrager
- 15.30 Pauze
- 16.00 Elektronisch geld – drs. R. Hirschfeld
- 16.30 Multimedia – drs. P.J.W. ten Hagen
- vanaf 17.00 uur Borrel

Wat is het CWI ?

Het Centrum voor Wiskunde en Informatica (CWI) is het onderzoeksinstituut van de in 1946 opgerichte Stichting Mathematisch Centrum, een 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 op deze gebieden naar de maatschappij in het algemeen en het bedrijfsleven en de industrie in het bijzonder.

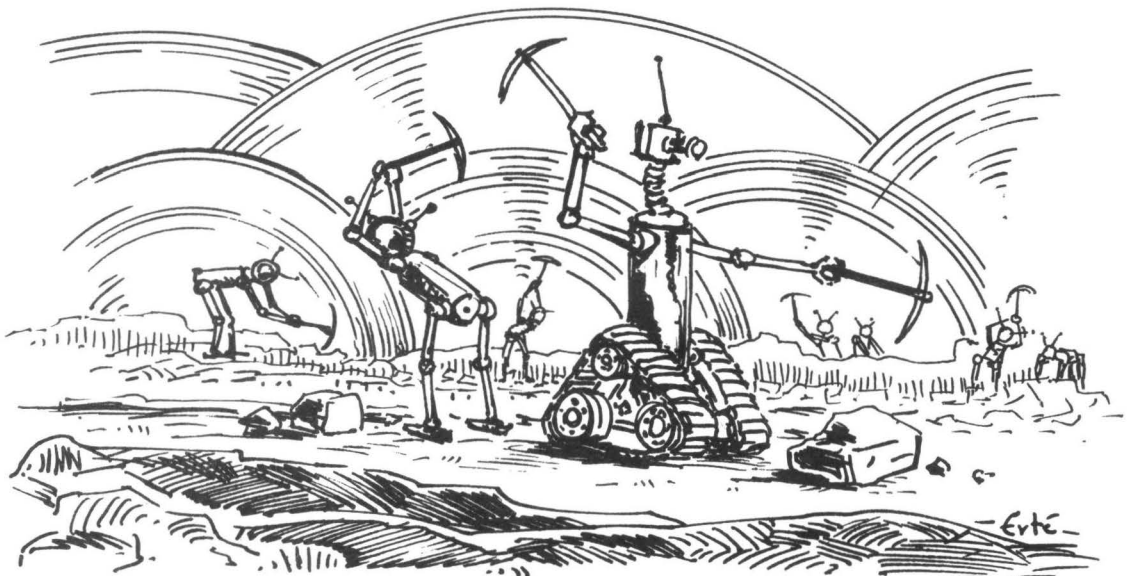


DATA MINING: SCHATGRAVEN IN DATABASES

Steeds meer gegevens worden opgeslagen in databases. Deze bevatten schatten aan strategische informatie, die echter met de gebruikelijke database management systemen moeilijk boven water komen. Dat is wel mogelijk met 'data mining', een recent in ontwikkeling gekomen techniek, die elementen uit de theorie van databases, statistiek en lerende machines in zich verenigt. Onlangs is op het CWI, dat beschikt over expertise op alle drie terreinen, een project Data Mining gestart.

Databases groeien zeer snel, zowel in omvang als in aantal. Schattingen van de groei in omvang lopen uiteen van een verdubbeling per drie jaar tot een vertienvoudiging per tien jaar. Naast de feitelijke in een database opgeslagen informatie is vooral ook de daaruit afgeleide informatie interessant. Neem bijvoorbeeld een verzekeringsmaatschappij die een database bijhoudt met alle informatie over haar autoverzekeringen. Zij kan dan heel eenvoudig nagaan hoeveel klanten ooit schade hebben gereden. Andere voor de maatschappij interessante informatie, bijvoorbeeld de risico-profielen, is wel impliciet aanwezig in deze database, maar veel moeilijker te vinden. Data mining is de techniek van het zoeken naar zulke karakteristieke patronen in een database. Eerst wordt de informatie in de database geclusterd, waarbij we bijvoorbeeld de brokkenmakers onderscheiden van de veilige rijders. Daarna wordt er gezocht naar een karakteristieke beschrijving van elke groep in de cluster. De zo verkregen regels geven strategisch inzicht in de inhoud en de samenhang van de database. De gevonden risico-profielen kunnen bijvoorbeeld worden gebruikt om de premie voor risico-groepen te verhogen, terwijl de premie voor de anderen wordt verlaagd.

Met data mining vinden we een hoog-niveau beschrijving van de database in de vorm van een indeling in groepen, elk met hun karakteristieke kenmerken. Dit soort beschrijvingen kan worden gebruikt om bijvoorbeeld regionale verschillen of trends te vinden. Stel dat onze autoverzekeringen database twee regio's beslaat, de Randstad en Friesland, en dat de ene regio relatief veel meer schade heeft dan de andere. Eerst maken we van elke regio zo'n hoog-niveau beschrijving in groepen met hun risico-profielen. Vervolgens vergelijken we deze beschrijvingen. Verklaringen voor de verschillen kunnen dan zijn dat de regio's verschillende groepen hebben, dat de relatieve grootte van de groepen verschillend is, of dat de risico-profielen van de groepen per regio verschillen. Door in plaats van regio's dezelfde database op verschillende tijdstippen te nemen, kunnen we op soortgelijke manier trends ontdekken in het tijdsverloop.



De huidige generatie database management systemen is niet geschikt voor data mining. Deze zijn wel te gebruiken om een vermeend risico-profiel te testen, maar de gebruiker zelf moet dit profiel opstellen. Als de gebruiker echter het profiel niet kent, dan zijn er veel te veel mogelijkheden om allemaal uit te proberen. Een data mine tool beperkt het aantal mogelijkheden door het menselijk inzicht (niet alle clusterings en lang niet alle patronen zijn zinvol) en 'slimme' algoritmen te combineren. Op deze wijze wordt het mogelijk om ook onbekende verbanden in de database te vinden.

Data mining wordt al in de praktijk toegepast. Zo kan IBM aanzienlijk besparen op het aantal laatste (dure) tests op disk-drives doordat zij een profiel hebben opgesteld waarmee men in een vroegtijdig stadium disk-drives kan herkennen die vermoedelijk in die laatste test zullen falen. Een ander voorbeeld is het Britse bankiershuis TSB, dat uit gegevens van oude leningen regels heeft afgeleid waarmee de kredietwaardigheid van nieuwe klanten beter kan worden beoordeeld.

Data mining heeft vier belangrijke facetten. De eerste is de clustering van de gegevens in de database. De kwaliteit van de gevonden regels hangt in hoge mate af van de gebruikte clustering. De gebruiker kan dan ook de computer sturen bij het vinden van een geschikte clustering. Als hij bijvoorbeeld is geïnteresseerd in het vinden van risico-profielen, dan moet hij het systeem laten clusteren op de hoogte van het schadebedrag. Na het clusteren moet er voor iedere groep een karakteristiek patroon worden gevonden, dat wordt uitgedrukt in een daartoe ontworpen representatietaal. Hoe rijker deze taal is, hoe nauwkeuriger de gevonden patronen zullen zijn, maar ook hoe langer het zoeken duurt en hoe moeilijker interpreteerbaar het resultaat zal zijn. Een van de zwaartepunten van het onderzoek is dan ook het ontwerpen van een representatietaal waarmee eenvoudig begrijpbare adequate beschrijvingen snel kunnen worden gevonden. Om de beste beschrijving te vinden gebruikt men een kwaliteitsfunctie die voor elk patroon aangeeft hoe goed die de cluster in kwestie beschrijft. De zoekruimte is nu voor te stellen als een heuvelandschap, waar de hoogte de kwaliteit aanduidt, en het doel is zo snel mogelijk de hoogste top te vinden. Hiertoe is een veelheid aan goede algoritmen bekend. De gebruiker kan dit zoekproces verder versnellen door bijvoorbeeld aan te geven dat sommige kenmerken onbelangrijk zijn voor het resultaat. Zo zal de naam van een verzekeringnemer geen rol spelen in een risicoprofiel. Het laatste facet is dat databases altijd onjuiste informatie (ruis) bevatten, bijvoorbeeld veroorzaakt door typefouten, en dat er soms informatie ontbreekt, omdat die op het moment van samenstelling niet van belang leek. Met behulp van statistische technieken, zoals het verwijderen van sterk afwijkende voorbeelden, kan de ruis grotendeels worden verwijderd. Bovendien blijkt dat data mining op een database met ruis toch vrij goed lukt. Het ontbreken van informatie is daarentegen in principe een onoverkomelijk probleem. De enige oplossing is hier te werken met waarschijnlijkheidsregels, die een uitspraak doen over de kans dat een object tot een klasse behoort, indien het aan bepaalde voorwaarden voldoet.

Medio 1993 heeft de onderzoeksgroep Databases van het CWI het project Data Mining gestart, met als doel een data mining omgeving te creëren voor moderne database management systemen. Centraal bij het ontwerp staat de integratie van resultaten uit de statistiek, data- en kennis-banken en machine learning, zowel om de efficiëntie van de data mining als om de betrouwbaarheid van de resultaten te garanderen. Omdat data mining een interactief proces is, krijgt ook het ontwerp van de user-interface ruime aandacht. Hierbij wordt bijvoorbeeld gedacht aan de inzichtelijkheid en presentatie van de gevonden informatie.

Data Mining (AA4)

Dr. A.P.J.M. Siebes, telefoon 020 - 592 4139

Ir. M. Holsheimer, telefoon 020 - 592 4134

Centrum voor Wiskunde en Informatica

Kruislaan 413

postbus 94079, 1090 GB Amsterdam

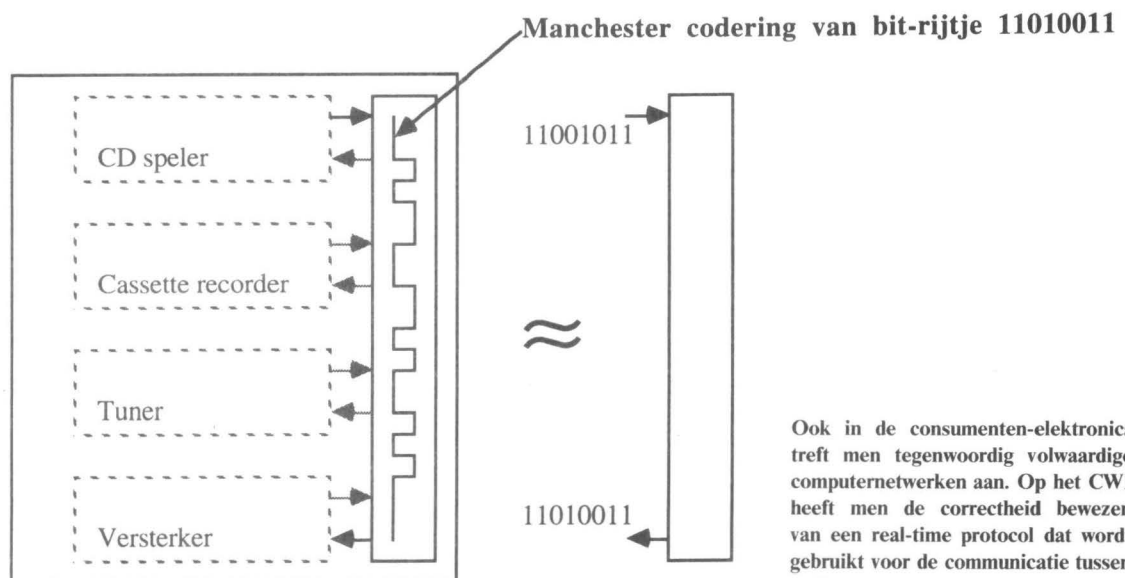
telefoon 020 - 592 9333, telefax 020 - 592 4199

september 1993

CORRECTE PROGRAMMA'S VOOR GESPREIDE EN REAL-TIME COMPUTERSYSTEMEN

Computersystemen groeien snel in omvang en complexiteit, teneinde aan de steeds hogere eisen te kunnen voldoen. Daarbij wordt een taak vaak verdeeld over verschillende gelijktijdig in werking zijnde, onderling verbonden (concurrente) processen. Deze situatie treft men aan in een computernetwerk, maar ook binnen één computer. Hierbij eist men steeds vaker dat een computersysteem in real-time kan opereren. De programmering van zo'n systeem stelt speciale eisen. Op het CWI zoekt men naar goede technieken om programma's voor gespreide en concurrente computersystemen te specificeren en verifiëren. Het onderzoek vindt grotendeels plaats in het kader van de Europese programma's RACE en ESPRIT.

De eerste stap bij het vinden van een geautomatiseerde oplossing van een probleem is een specificatie geven van dat probleem, dat wil zeggen een beschrijving in algemene termen, niet refererend naar bijvoorbeeld een bepaalde programmeertaal of computer. Nemen we als voorbeeld de specificatie van een computernetwerk. Deze zal typisch bestaan uit een lijst van eisen ten aanzien van het gewenste externe gedrag, zoals de eis dat elk bericht dat het netwerk wordt ingestuurd, hetzij bij de geadresseerde zal arriveren, hetzij zal terugkomen bij de zender met de vermelding dat er iets is misgegaan. De specificatie spreekt zich niet uit over de mogelijk zeer complexe route die het bericht aflegt binnen het netwerk, het feit dat sommige van de gebruikte kanalen niet betrouwbaar zijn, dat computers onderweg plat kunnen gaan, etc. De tekst van een specificatie kan nog diverse vormen hebben. In algebraïsche specificaties is deze gegeven in algebraïsche termen, waarbij axioma's regels geven voor de vereenvoudiging van uitdrukkingen en de betekenis (semantiek) van de constructies in die algebra vastleggen. Een specificatie levert criteria voor een te ontwerpen programma; als aan die criteria is voldaan heet het programma correct. De criteria worden geformuleerd in een specificatietaal. Men kan zo'n taal zien als een hogere systeemontwerptaal. Een specificatietaal wordt bij voorkeur zo abstract mogelijk gehouden en hoeft bijvoorbeeld niet executeerbaar te zijn. Afhankelijk van de aard van de specificatie zijn verschillende specificatietaalen ontworpen, die tot doel hebben de beoogde functionaliteit van software- en hardware-systemen te beschrijven. Gezien de toenemende omvang en complexiteit van de te automatiseren problemen gaat de aandacht tegenwoordig steeds sterker uit naar formele methoden zoals voornoemde algebraïsche specificaties (de weergave van een probleem in een stroomdiagram is een voorbeeld van een informele specificatie). De term 'formeel' duidt erop dat het gaat om een wiskundige systeembeschrijving, waartoe de specificatietaal moet worden voorzien van een formeel wiskundige semantiek. Formele specificaties hebben het voordeel dat alle aannamen expliciet worden genoemd, zodat vergissingen uitgesloten zijn, maar daardoor worden zij ook nogal lang.



In het verlengde van de specificatie ligt de verificatie van de resulterende programmatuur, dat wil zeggen, bewijzen dat een programma een bepaalde eigenschap heeft. Met behulp van de wijd verbreide 'debugging' technieken kan men weliswaar fouten uit een programma halen, maar nooit aantonen dat het foutloos is, bijvoorbeeld dat het geen 'deadlocks' bevat. Ook verificatie kan men op tal van manieren aanpakken. Zo berust algebraïsche verificatie op het bewijzen van de equivalentie van twee programma's door ze te vergelijken, zoals ook de gewone algebra werkt met vergelijkingen. Het ideaal is natuurlijk dat samen met de constructie van een programma ook het correctheidsbewijs wordt geleverd. Dat blijkt in de praktijk echter nog zeer lastig te zijn.

Specificatie, ontwerp en verificatie van programmatuur bestaan al zolang er wordt geprogrammeerd. Met de opkomst van gespreide computersystemen en parallelle verwerking ontstond ook de noodzaak om op deze gebieden nieuwe technieken te ontwikkelen voor concurrente programma's. Dat bleek al gauw veel moeilijker te zijn dan in het geval van sequentiële programma's. Een van de problemen is bijvoorbeeld te bewijzen dat er niets mis loopt met de synchronisatie tussen concurrente processen. Een veelbelovende aanpak is het gebruik van procesalgebra, aan de ontwikkeling waarvan het CWI belangrijke bijdragen heeft geleverd. Hiermee kunnen concurrente processen op formele, algebraïsche wijze worden beschreven.

Veel van het CWI-onderzoek op dit gebied vindt plaats in het kader van Europese programma's. In het inmiddels afgesloten RACE-project SPECS (Specification and Programming Environment for Communications Software) is gekeken hoe het ontwerpen van telecommunicatie-software zo veel mogelijk kan worden geautomatiseerd en geoptimaliseerd. Het CWI speelde een sleutelrol in de ontwikkeling van de op procesalgebra gebaseerde specificatietaal μ -CRL. In het onlangs gestarte RACE-project BOOST (Broadband Object-Oriented Service Technology) wordt een software-omgeving ontworpen ten behoeve van de zich snel uitbreidende netwerkdiensten (bijvoorbeeld vluchtschema's van luchtvaartmaatschappijen). Verder wordt in het kader van het ESPRIT-project CONCUR onderzoek gedaan aan calculi en algebra's voor concurrente processen. Dat heeft onder meer geleid tot een aantal op procesalgebra gebaseerde softwarepakketten die hulp bieden bij de analyse van ingewikkelde programma's. Is de Europese aanpak sterk gericht op algebraïsche technieken, in de steeds belangrijkere samenwerking met MIT (VS) ligt het accent meer op assertionele methoden en simulatie-relaties. Daarbij wordt onder meer gewerkt met 'invarianten': uitspraken die bij het doorlopen van een programma geldig blijven, en die daar een functie vervullen vergelijkbaar met behoudswetten in de fysica.

Een belangrijke ontwikkeling, speciaal in verband met industriële toepassingen, is de uitbreiding van de tot nu toe ontwikkelde technieken voor specificatie en verificatie naar real-time systemen. Toepassingen vindt men in uiteenlopende terreinen als digitale horloges, gevechtsvliegtuigen en procesregelaars. Op het CWI kijkt men onder meer naar de ontwikkeling van een procesalgebra voor real-time systemen.

Dr. F.W. Vaandrager, Concurrency en real-time systemen (AP2)
telefoon 020 - 592 4232

*Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199
september 1993*

EUROPEES ONDERZOEK VERSCHAFT SOFTWARE BASIS VOOR MULTIMEDIA TOEPASSINGEN

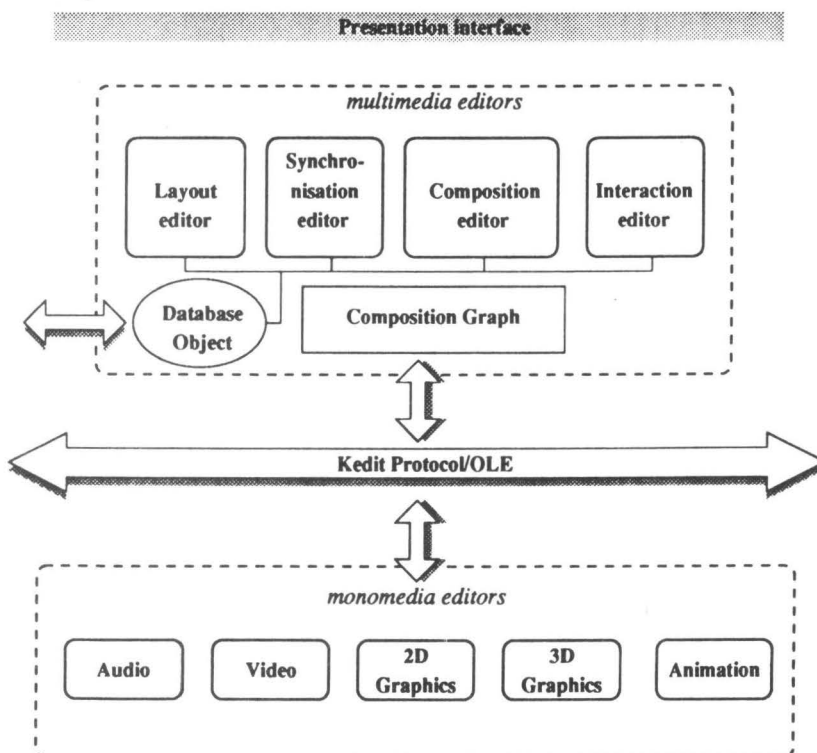
Snelle ontwikkelingen op het gebied van hardware hebben de mogelijkheden van multimediale presentaties, waarbij tekst, geluid en beeld zijn geïntegreerd, aanzienlijk vergroot. De bijbehorende software vertoont tot nu toe echter nog weinig samenhang. Speciaal vanuit de industrie dringt men aan op een uniforme aanpak en standaardisatie van multimedia basis-software. Onderzoek hiernaar vindt plaats in het ESPRIT-project MADE (Multimedia Application Development Environment). Het CWI is een der belangrijkste partners in dit grootschalige Europese project.

Bij het ontwerpen van multimedia toepassingen is men het aan zijn stand verplicht veel aandacht te geven aan de kwaliteit van de weergave, de samenstelling van het geheel en de hanteerbaarheid voor de gebruiker. De stem van Pavarotti mag niet worden verpest door een derde-rangs beeldkwaliteit. Bij het programmeren van multimedia toepassingen moet de programmeur dus uitdrukkelijk rekening houden met de relatie van zijn programma met de buitenwereld. Daarom treft men in een multimedia programmeeromgeving drie niveau's van programmering aan:

- de ontwikkeling van hulpmiddelen en technieken; dit is het technisch lastigste deel, waarvoor de expertise van de programmeur is vereist;
- 'authoring', dat wil zeggen de beschrijving van de organisatie van de ruwe multimedia informatie en de wijze waarop de gebruiker daarmee kan omgaan, min of meer zoals een krantenredacteur werkt met de binnenkomende kopij;
- de scenario's van de gebruiker, waarin hij specificeert hoe hij met de geautoriseerde informatie wil omgaan.

De laatste twee niveau's moeten zo ruim zijn opgezet dat zij het gehele spectrum bestrijken van zeer speciale toepassingen, zoals het ontwerpen van een handboek voor de reparatie van vliegtuigen, tot alleen op vrij algemene informatie gebaseerde systemen zoals het clubblad van een voetbalvereniging.

MADE (Multimedia Application Development Environment) is een ESPRIT-project, waarin een omvattend programmapakket wordt ontwikkeld voor alle drie bovengenoemde niveau's van programmering. In dit grootschalige, onder leiding van het Franse concern Bull staande project (1992-1995) is het CWI de belangrijkste van de zeven partners. Bij het ontwerp spelen twee begrippen een sleutelrol: integratie en standaarden.



Integratie

Elke media component (beeld, geluid, tekst) vereist een specifieke, vaak ook fysiek gescheiden aanpak voor de generatie, transmissie en opslag van informatie. Toch moet een multimedia compositie worden gegenereerd, verzonden, opgeslagen en gepresenteerd als één geheel, evenals haar behandeling in een interactieve omgeving. In MADE wordt deze integratie tot stand gebracht door toepassing van object-georiënteerde programmeertechnologie. De objecten zijn hier bijvoorbeeld stukken tekst, geluid en beeld, en het probleem is dan deze op de juiste wijze aan elkaar te koppelen, zodat bijvoorbeeld inkortingen technisch eenvoudig zijn te realiseren. Het te ontwikkelen programmeergereedschap moet de gebruiker in staat stellen met zo'n audio-visueel brokstuk te manipuleren. Een object bevat code voor zijn media-specifiek gedrag, bijvoorbeeld het geluidsaspect, onzichtbaar gemaakt voor de gebruiker (transparant) zodat die er geen last van heeft. Deze code wordt geactiveerd door instructies van buitenaf. Algemene, gemeenschappelijke eigenschappen van objecten worden geërfd van één moeder-object, dat ook vertelt hoe objecten aan elkaar moeten worden geknoopt. Verder werkt het systeem met delegatie van methoden aan prototype objecten. Als bijvoorbeeld een stuk tekst normaal is ontworpen voor A4-formaat, maar nu op A5 moet komen, dan wordt de omzetting gedelegeerd aan een speciaal object dat weet hoe dat moet. De aldus gerealiseerde integratie bepaalt de meerwaarde van het MADE-systeem ten opzichte van andere, vergelijkbare systemen.

Standaarden

Het MADE-systeem accepteert alle gangbare standaarden voor de interne representatie van media-informatie, zoals transmissiecodes (bijvoorbeeld de in de krantenwereld bekende JPEG standaard voor het overseinen van foto's), de opbouw van documenten en coderingen voor files (computing platforms, files bevinden zich in het algemeen verspreid over diverse installaties). Vooral vanuit het internationale bedrijfsleven wordt nu aangedrongen op nieuwe standaarden ten behoeve van de programmering van multimedia presentaties. Verkopers van hardware zien graag dat alle multimedia toepassingen op hun apparatuur kunnen lopen. Dergelijke standaarden moeten de overdraagbaarheid van die presentaties binnen netwerken en computing platforms garanderen. Zij vormen de basis voor de verbinding tussen klant en bediende in mediasystemen en voor multimedia archivering. Op het gebied van standaarden hebben zich enkele clusters gevormd, zoals de Amerikaanse Object Management Group, waarin software engineers en verkopers en gebruikers van software van zo'n 500 bedrijven zijn vertegenwoordigd, en de Interactive Multimedia Association. Daarnaast is de International Standards Organization ISO bezig met het formuleren van een internationale standaard voor multimedia programmeurs. Bij de ontwikkeling van deze standaard, PREMO (Programming Environment for Multimedia Objects), is het CWI actief betrokken. Het MADE-project haakt hierop in door de in het project geconstrueerde object-basis en prototypes van MADE-componenten ter beschikking te stellen van deze ontwikkelaars van standaarden. Door zo nauw betrokken te zijn bij de totstandkoming van de nieuwe standaarden verwacht men de marktmogelijkheden van het MADE-systeem te vergroten.

MADE (IS3)

Drs. P.J.W. ten Hagen, telefoon 020 - 592 4133

Dr. I. Herman, telefoon 020 - 592 4163

Centrum voor Wiskunde en Informatica

Kruislaan 413

postbus 94079, 1090 GB Amsterdam

telefoon 020 - 592 9333, telefax 020 - 592 4199

september 1993

TOEGEPASTE KANSREKENING VOORKOMT ERGERNIS BIJ WACHTEN

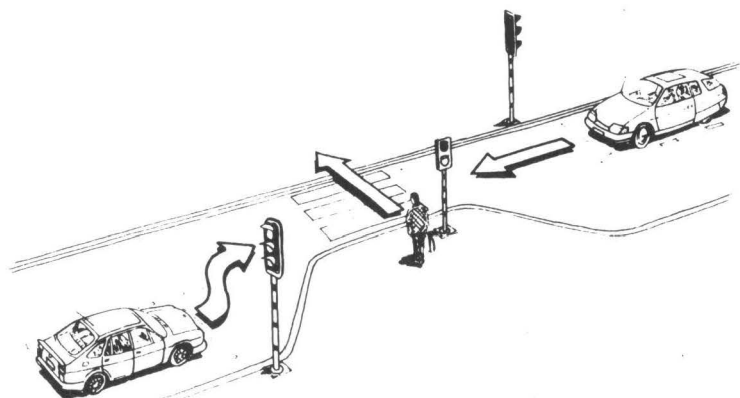
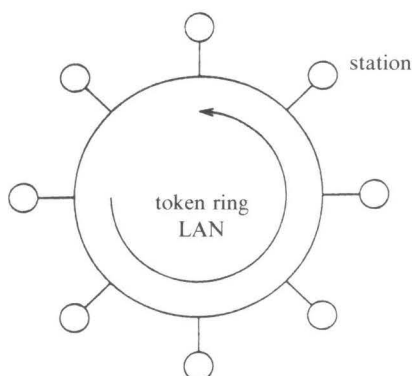
Wachten is zo algemeen dat de ergernis waarmee het gepaard gaat eveneens deel is gaan uitmaken van het dagelijks bestaan. Wachten in de file, op het postkantoor of het 'aantal wachtenden voor u' bij de telefoon lijkt bovendien steeds maar toe te nemen, terwijl in onze informatiemaatschappij tegelijkertijd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

Het wachtrijprobleem verheugt zich al sinds het begin van deze eeuw in de aandacht 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), het oplossen van problemen bij het wegverkeer en bij allerlei fabricageprocessen. Kort gezegd: daar waar een beperkte capaciteit voor 'dienstverlening' beschikbaar is voor elkaar concurrerende gebruikers. 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 functioneren moet een wiskundig model worden gemaakt van de manier waarop de wachtenden moeten worden bediend. Omdat het aankomstproces van de klanten en hun bedieningsvraag stochastische aspecten bevat, zijn ook de belangrijkste grootheden (het aantal wachtende klanten en de wachttijden) stochastisch: wachtrijtheorie is een onderdeel van de toegepaste kansrekening.

De groep Analyse en Besturing van Informatiestromen in Netwerken van het CWI doet al jaren fundamenteel onderzoek naar modellen en methoden uit de wachtrijtheorie. Het onderzoek spitst zich de laatste jaren toe op wachtrijmodellen voor prestatie-analyse van computers en communicatiesystemen, en de integratie van wachtrij- en betrouwbaarheidsaspecten in één model (bijvoorbeeld defecte onderdelen die wachten op reparatie of bedieners die zelf aan slijtage onderhevig zijn).

Zo doet de groep onderzoek naar de analyse en de optimalisering van zogenaamde pollingsystemen. Dit zijn wachtrijsystemen waarin een bediener afwisselend klanten bedient die in meerdere wachtrijen klaar staan. Een dergelijk systeem komt bijvoorbeeld voor bij bepaalde computernetwerken zoals het ringvormige 'Token Ring' local area netwerk. De token (bediener) reist de ring rond met een opdracht van een der zenders en is dan bezet.



Een multi-wachtrijprobleem met ringvormige bediening komt niet alleen vaak voor in verkeerssituaties, maar ook in computernetwerken. Op het CWI is een

behoudswet gevonden, waarmee men inzicht kan krijgen in gemiddelde wachttijden van alle soorten gebruikers in zulke systemen.

Op dit moment doet de groep onderzoek naar de mogelijkheden om de bediener binnen een dergelijk systeem volgens een vast, niet noodzakelijk cyclisch, patroon naar de wachtrijen te sturen. Getracht wordt een patroon te vinden dat de gemiddelde wachttijden minimaliseert. De CWI-groep werkt momenteel zowel theoretisch als in consultatieverband aan dit probleem.

Pollingsystemen worden ook toegepast in flexibele produktiesystemen, bij verkeersmodellen en bij machinale robots - als bedieners - die verschillende bewerkingen aan produkten kunnen verrichten. Hier zijn omschakeltijden en -kosten belangrijke factoren.

Daarnaast houdt de CWI-groep zich bezig met complexe systemen die bestaan uit een groot aantal aan slijtage onderhevige onderdelen, waarbij onderhoudsploegen het preventief en correctief onderhoud uitvoeren. Hierbij gaat het om een interactie van wachtrij- en betrouwbaarheidstheorie. In het onderzoek wordt naast de wiskundige analyse steeds meer het belang onderkend van ondersteunende softwarepakketten, zowel voor theoretisch onderzoek als voor consultaties. De groep beschikt over verschillende geavanceerde softwarepakketten en heeft in 1987 de gebruikersgroep QPASS opgericht die actief is op het gebied van de software voor wachtrij- en prestatie-analyse.

Tenslotte verricht de groep rechtstreeks toegepast onderzoek voor bedrijven en andere organisaties. Daarbij wordt er steeds 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.

Praktijk

ECT: Voor het containeroverslagbedrijf ECT is een wachtrij-analyse gemaakt voor het bepalen van de in te zetten apparatuur voor de afhandeling van containers. Achter de containerkranen maakt het bedrijf gebruik van Automatic Guided Vehicles die de opslagplaatsen achter de kranen bedienen en zorgen voor de verbinding met de loskade. Deze karretjes zijn toegewezen aan bepaalde kranen. Onderzocht is of het poolen van de karretjes (waardoor ze uitwisselbaar worden tussen de verschillende kranen) een positief effect kan hebben op de opslagstrategie.

PTT Telecom: Via glasvezelnetten lopen straks diverse vormen van communicatie, zoals het gesproken woord, data en beelden, die allemaal verschillende karakteristieken bezitten. Dat leidt tot interessante wachtrijproblemen. Dataverkeer mag in sommige gevallen wel even wachten, maar het gesproken woord meestal niet. In opdracht van de PTT zijn wachtrij-modellen ontwikkeld en doorgerekend voor de verkeerstechnische analyse van ATM-netten (Asynchronous Transfer Mode) zoals het nieuwe ISDN-net van PTT Telecom.

Prof.dr.ir. O.J. Boxma, Analyse en Regeling van Informatiestromen in Netwerken (BS2)
telefoon 020-592 4094

*Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199*

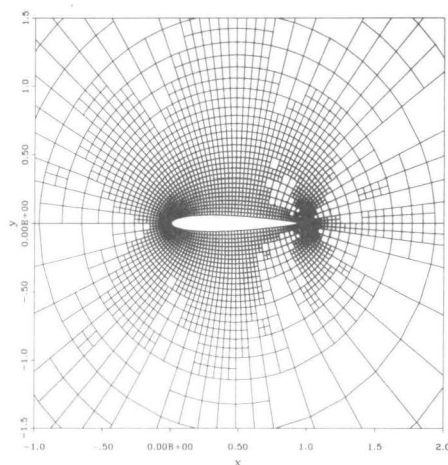
September 1993

MULTIROOSTERMETHODEN VERSNELLEN DE OPLOSSING VAN INGEWIKKELDE REKENPROBLEMEN

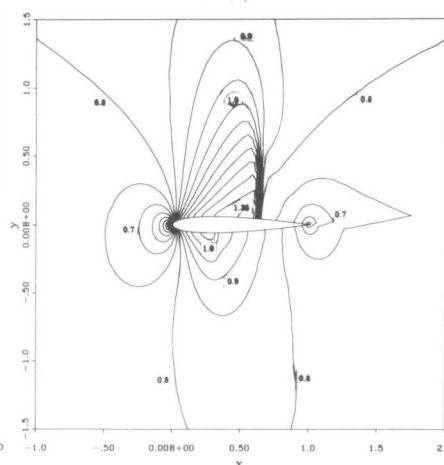
Stromingen van vloeistoffen en gassen (bijvoorbeeld in olievelden of om vliegtuigvleugels) of elektrische stromen in halfgeleiders (chips) worden wiskundig beschreven door *partiële differentiaalvergelijkingen (PDV's)*. Door deze vergelijkingen op te lossen vindt men het verloop van die stromingen in plaats en tijd. Inzicht in dit verloop is vaak van groot praktisch belang. De numerieke oplossing van PDV's vormt een ingewikkeld rekenprobleem. Het CWI heeft aanzienlijke ervaring met de *multiroostermethode* waarmee veel van zulke problemen succesvol zijn aan te pakken.

Vaak blijkt een numeriek probleem eenvoudig en goedkoop op te lossen via een stapsgewijze benadering (*iteratie*). Eerst vervangen we het ingewikkelde probleem door een probleem dat er wel wat op lijkt, en eenvoudig is uit te rekenen. Die oplossing wijkt dan natuurlijk wel af van de gezochte oplossing. Op basis van de gemaakte fout (het 'defect') corrigeren we het eenvoudige probleem, lossen het opnieuw op, enzovoort. Dit iteratieve proces leidt vaak snel en accuraat tot het doel. Een voordeel van dit type berekeningen is dat ze heel goed zijn te automatiseren. Deze manier van rekenen, de *defect-correctie methode*, is heel oud - de Babyloniërs gebruikten haar al. Zij is goed te vergelijken met het terugkoppelingsprincipe in de techniek, zoals dat bijvoorbeeld wordt toegepast in de temperatuurregelaar in een koelkast.

De numerieke oplossing op een computer van stromingsvergelijkingen zoals voornoemd gebeurt in twee stappen. Eerst brengen we in de ruimte een denkbeeldig rooster aan en bekijken het probleem alleen in de roosterpunten (*discretisatie*). Ook de tijdvariabele wordt vervangen door een aantal discrete tijdstippen. Deze discretisatie is nodig omdat een digitale computer nu eenmaal alleen in stapjes rekent. De oorspronkelijke continue differentiaalvergelijkingen worden zo vervangen door een (groot) aantal algebraïsche vergelijkingen, waarin de onbekenden de te berekenen grootheden zijn (temperatuur, druk, etc.) in de roosterpunten. Dit stelsel lossen we dan iteratief op, bijvoorbeeld met de defect-correctie methode. Als het gekozen rooster te grof blijkt voor een goede benadering, verkleinen we de maaswijdte en herhalen de hele berekening voor dit fijnere rooster. In de praktijk kan deze werkwijze echter een dure grap worden. Het gaat dan namelijk vaak om vele duizenden vergelijkingen, en een halvering van de maaswijdte levert al acht maal zo veel vergelijkingen op.



Adaptief multirooster patroon



Mach-verdeling

Transsonie stroming rond een vleugelprofiel (NACA0012). Berekening van de iso-lijnen van het getal van Mach met behulp van een adaptief multirooster algoritme.

In dit soort gevallen kan de rekentijd worden teruggebracht door toepassing van de *multirooster-methode*. Het slimme van deze methode schuilt daarin dat, ook als we uitgaan van een behoorlijk fijn rooster, bij de tussenstappen van het iteratieve oplossingsproces vaak kan worden volstaan met berekeningen op grovere roosters, die aanzienlijk minder rekentijd vergen. De methode is dan ook vooral tijdbesparend voor berekeningen op fijne roosters. De multiroostermethode is in de jaren zestig voor het eerst gepubliceerd in de Sovjet-Unie, maar er bleken de eerste jaren nog geen praktische toepassingen voor te vinden. Die kwamen pas ruim tien jaar later, waarna in de jaren tachtig de grote groei volgde. In Nederland was het CWI er al vroeg bij. De groep Randwaardeproblemen, Multigrid en Defectcorrectie van CWI's afdeling Numerieke Wiskunde heeft in de loop der jaren uitgebreide kennis opgebouwd in het gebruik van de multiroostermethode en heeft haar reeds succesvol toegepast bij diverse praktische problemen, ook in opdracht van derden.

Praktijk

De volgende voorbeelden geven een indruk van het brede toepassingsgebied van deze rekenmethode.

HERMES - Europa is nu, naar aanleiding van een Frans initiatief, binnen haar ruimtevaartprogramma bezig met de bouw van een eigen shuttle. Het ruimteveer HERMES zal misschien omstreeks het jaar 2000 de ruimte ingaan en vervolgens weer op aarde terugkeren. Bij terugkeer in de dampkring treden stromingen op die vele malen sneller dan de geluidssnelheid kunnen zijn. Omdat de Europese shuttle kleiner zal zijn dan de Amerikaanse krijgen we met andere en - enigszins verrassend - moeilijker problemen te maken. Simulatie in een windtunnel is in dit geval niet goed mogelijk. Daarom is gekozen voor een wiskundige aanpak. Onder leiding van de Franse fabrik Dassault wordt onderzocht welke van een aantal berekeningsmethoden de beste benadering van het re-entry probleem geeft. Op het CWI is met de multiroostermethode aan dit probleem gewerkt.

BRITE - Voor het Europese onderzoekprogramma BRITE worden thans in samenwerking met Belgische, Italiaanse, Zweedse en Deense universiteiten, en onder belangstelling van een aantal Europese vliegtuigbouwers, berekeningen uitgevoerd aan luchtstromen rond de vleugels van vliegtuigen. Hoewel dit probleem veel lijkt op dat van de HERMES, verloopt de oplossing anders. Hier maken we gebruik van *adaptieve* roosters: waar nodig worden de roosters plaatselijk verfijnd. Hierdoor worden tijdens de berekeningen nieuwe vergelijkingen toegevoegd. In feite gaat het hier om een uitbreiding van de multiroostermethode.

Chips - Ook voor het bepalen van de elektrische stromen in een transistor is het simuleren met behulp van een wiskundig model beter - en goedkoper - dan het uitvoeren van een experiment. Het CWI-onderzoek dat is gedaan op dit terrein werd gefinancierd door het Innovatief Onderzoek Programma IC-Technologie en had (uiteeraard) de belangstelling van Philips. Kennis van deze elektrische stromen is belangrijk voor het verkrijgen van kennis over het gedrag van een chip tijdens het toenemen van de door die stromen veroorzaakte warmte.

Veel van het wiskundig onderzoek met behulp van de multiroostermethode wordt uitgevoerd voor de industrie, omdat juist deze methode bij rekenintensieve numerieke problemen voor veel tijdswinst kan zorgen en daarmee geld bespaart.

Prof.dr. P.W. Hemker, Randwaardeproblemen, multigrid en defectcorrectie (NW2)
telefoon 020 - 592 4108

Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199

september 1993

VEILIG ELEKTRONISCH BETALEN MET PRIVACY IN EUROPA

Het verwachte massale aanbod en gebruik van diensten via een computernetwerk stelt hoge eisen aan de veiligheid van het netwerk en de privacy-bescherming van de gebruikers. Het CWI coördineert het ESPRIT-project CAFE (Conditional Access for Europe), dat tot doel heeft een Europees betalingssysteem te ontwerpen dat aan deze eisen voldoet.

Een algemeen heersende opvatting is dat men niet tegelijk de veiligheid van het systeem en de privacy van de gebruiker in voldoende mate kan garanderen. Dit is echter onjuist: met behulp van recent ontwikkelde technieken in de cryptologie (de wetenschap van informatiebeveiliging), waaraan het CWI belangrijke bijdragen heeft geleverd, blijkt dat wel degelijk mogelijk. In het project CAFE worden, in nauwe samenspraak met potentiële eindgebruikers, deze technieken beproefd op hun praktische waarde.

In het tot nu toe meest gebruikte cryptografische systeem, de Data Encryption Standard (DES), heeft iedere deelnemer een geheime sleutel voor codering en decodering, terwijl de methode van omzetting openbaar is. DES is goedkoop en gemakkelijk te implementeren, maar is niet geheel veilig en kan geen privacy garanderen. Ook maakt het snel toenemende verkeer via elektronische netwerken met vaak vele duizenden deelnemers het gebruik van een aparte geheime sleutel voor elk paar deelnemers praktisch ondoenlijk. Eind jaren zeventig gaven de wiskundigen Rivest, Shamir en Adleman (RSA) aan hoe het enkele jaren daarvoor geopperde idee om ook openbare sleutels te gebruiken, in de praktijk zou zijn te realiseren. In het RSA-systeem heeft iedere deelnemer een geheime sleutel (twee grote priemgetallen van zo'n honderd cijfers) en een openbare sleutel (hun produkt). De veiligheid van het systeem berust op het gegeven dat uit het produkt de samenstellende priemfactoren praktisch niet zijn af te leiden. Het blijkt dat op RSA gebaseerde systemen wel privacy kunnen garanderen. Tot nu toe is echter het gebruik van RSA in de praktijk, bijvoorbeeld bij geldtransactiesystemen, nogal ingewikkeld gebleken, zeker als men ook privacy wil inbouwen. Er zijn ook andere systemen met openbare sleutels ontwikkeld, die berusten op soortgelijke principes. Een ervan is de 'discrete log' methode, die ook werkt met grote priemgetallen. Tot nu toe was deze methode niet erg efficiënt. Onderzoek op het CWI heeft echter een weg aangegeven hoe de oorzaken hiervan zijn te vermijden. In het kader van het CAFE-project worden nu, met dit gegeven als uitgangspunt, nieuwe wegen ingeslagen om met deze methode een praktisch werkbaar systeem te maken.



In een voorafgaand ESPRIT-project van de Europese Gemeenschap, CRYPTO IC-CARD, is een 'veilige' chip ontworpen, waarin speciale hardware is opgenomen die het gebruik van codeertechnieken met openbare sleutels mogelijk maakt. Om de mogelijkheden van zulke coderingen optimaal te benutten is het zaak om uitgekende protocollen te ontwerpen. Zo'n protocol is een wiskundig vraag-en antwoordspel, waarmee twee of meer deelnemers elkaar kunnen overtuigen van hun betrouwbaarheid zonder enige andere informatie prijs te geven. Verder is voor gebruik in de praktijk inbouw van zo'n chip in een zakformaat werkstation noodzakelijk. Deze problemen zullen in het kader van CAFE worden aangepakt. Het project houdt nadrukkelijk rekening met de behoeften en wensen van eindgebruikers, dienstverleners, financiële instellingen, overheidsinstellingen en consumentenorganisaties. Zo zal er een proefsysteem worden ontworpen voor praktijktests op een aantal Europese lokaties.

CAFE betekent op het gebied van veiligheid en privacy een belangrijke stap vooruit vergeleken met bestaande IC-kaarten. Om dit te bewerkstelligen zal er gebruik worden gemaakt van moderne technologie op het gebied van crypto IC-kaarten en zakcomputers. Cryptografische technieken waarmee elektronische privacy kan worden gegarandeerd, zijn onder andere beschreven door David Chaum in de Scientific American (augustus 1992).

Het CAFE-project duurt drie jaar (1993-1995). De coördinatie berust bij het CWI. De andere leden van het CAFE-consortium zijn: Digicash en PTT (Nederland); Cardware (UK); Gemplus, SEPT en Ingenico (Frankrijk); SINTEF-Delab (Noorwegen); Institut für Sozialforschung Frankfurt, Institut für Informatik Hildesheim en Siemens (Duitsland); en de Universiteiten van Aarhus (Denemarken) en Leuven (België).

R. Hirschfeld (Technical Manager CAFE), Cryptologie (AA2)
telefoon 020 - 592 4169

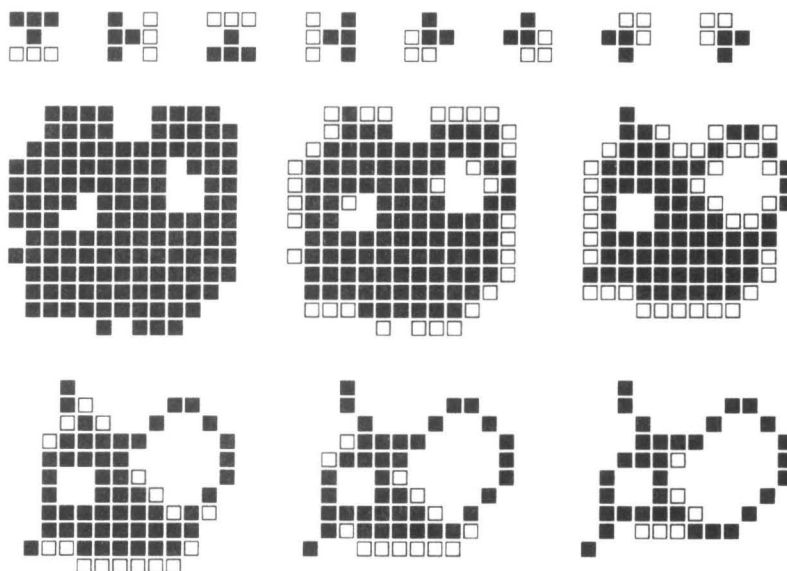
*Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199
september 1993*

BEELDVERWERKING: ONMISBARE SCHAKEL TUSSEN GEGEVENS EN ONDERZOEK

Beeldverwerking is een niet meer weg te denken deel van het wetenschappelijk onderzoek. De door computers geproduceerde enorme hoeveelheden digitale gegevens zijn vaak alleen te analyseren door ze in beeld te brengen. Ook zijn de gegevens zelf vaak al in de vorm van beelden (remote sensing, tomografie, seismiek, microscopie, etc.). De komst van snelle grafische werkstations heeft essentieel bijgedragen aan de ontsluiting van dit vakgebied. Het CWI legt zich toe op de wiskundige aspecten van de beeldanalyse, in het bijzonder statistische en meetkundige aspecten.

Door het massale gebruik van de computer bij het wetenschappelijk onderzoek krijgt de onderzoeker te maken met grote stromen van gegevens, die hij moet analyseren en waaruit hij conclusies probeert te trekken. Het beeld neemt hierbij een steeds belangrijker plaats in. Gegevens kunnen zelf al de vorm van een beeld hebben, zoals satelliet- en Röntgen-foto's, of in ruwe vorm zo onoverzichtelijk zijn dat er alleen door visualisatie iets mee is te beginnen. Het beeld kan ook bestaan uit een ruimtelijk patroon, dat niet direct visualisatie behoeft, maar dat men statistisch wil analyseren, bijvoorbeeld de groei van bepaalde planten in een veld. Bij het onderzoek gaat het om een combinatie van aspecten als de herkenning, analyse, verwerking en reconstructie van beelden. Deze aspecten komen in tal van toepassingen aan de orde, bijvoorbeeld bij remote sensing opnamen van het aardoppervlak, microscoopbeelden van biologische weefsels, robot-visie, het automatisch lezen van documenten, visualisatie van numerieke gegevens, archivering van bouwtekeningen en visuele communicatie (hypermedia). Het manipuleren met beelden geeft ook nieuwe uitdagingen aan het onderzoek in de wiskunde en informatica, bijvoorbeeld het ontwerpen en toepassen van statistische en meetkundige methoden. Het huidige onderzoek op het CWI richt zich vooral op morfologie, stochastische meetkunde en statistische beeldanalyse.

Morfologie is een meetkundige methode van beeldanalyse, waarbij een beeld wordt opgevat als een verzameling in de pixel-ruimte (een pixel is de raster-eenheid op een beeldscherm), die door operatoren op die verzameling kan worden getransformeerd. Een beeld wordt in kaart gebracht door het af te tasten met een vaste 'mal', bijvoorbeeld een schijfje of een vierkantje. Het doel is om door een serie van dergelijke meetkundige operaties het oorspronkelijke beeld zo te transformeren - er bijvoorbeeld als het ware een karikatuur of 'skelet' van te maken - dat bepaalde interessante karakteristieken naar voren komen. Meestal bevat een beeld namelijk ook een grote hoeveelheid ongestructureerde informatie, die alleen maar storend is bij de analyse. Zo reduceert men bij optische symboolherkenning elk symbool tot een skelet met een dikte van één pixel. Dit kan de opslag en reproductie van documenten aanzienlijk economiseren.



Skeletvorming in de morfologie. Een beeld wordt afgetast met acht malen. Elke mal heeft een voorgrond-(zwart) en een achtergrond-(wit) deel. Als het zwarte deel binnen het beeld valt en het witte erbuiten, wordt de centrale pixel van de mal uit het beeld verwijderd (per iteratie met wit aangegeven).

Andere toepassingen liggen in de robotica (herkenning van obstakels), diagnostiek (is een weefsel gezond of ziek?) en beeldverbetering. De morfologie is zo'n dertig jaar geleden voortgekomen uit onderzoek naar automatische beeldanalyse in de mineralogie (Serra en Matheron, Ecole de Mines Paris). Het CWI heeft de laatste jaren een vooraanstaande positie op dit gebied verworven. Naast theoretisch werk aan de algebra van morfologische operatoren en aan recursieve en iteratieve methoden is in het kader van een SION-project (Stichting Informatica Onderzoek Nederland) onder meer gekeken naar de toepassing van morfologische methoden op beelden weergegeven als een hiërarchie van grafen.

Stochastische meetkunde betreft de toepassing van kansrekening op door het toeval bepaalde ruimtelijke patronen. Hiertoe behoort de stereologie, het statistisch schatten van de omvang van een willekeurig voorwerp op basis van een aantal doorsnijdingen met een vaste meetkundige structuur. Verwant hiermee is het reconstrueren van een ruimtelijk voorwerp uit een aantal doorsnedes (computertomografie). Door haar eenvoud en geldigheid voor willekeurige vormen is de stereologie direct toepasbaar op vele problemen in de geneeskunde, anatomie, materiaalkunde en geologie, bijvoorbeeld bij de bestudering van microscopische structuren of van breuklijn patronen in de aardkorst. Het CWI-onderzoek richt zich vooral op fundamenteel onderzoek naar toepasbare stochastische modellen in de beeldanalyse, onder meer naaste-nabuur Markov puntprocessen. In een consultatieproject met de Australian Coal Industry Research Laboratories en de afdeling Wiskunde & Statistiek van CSIRO te Sydney is gekeken naar de voorspelling van breuklijnpatronen en de daaruit af te leiden veiligheid en opbrengst van een potentiële mijn uit gegevens van bestaande mijnen in de omgeving.

Statistische beeldanalyse wordt onder meer gebruikt voor het verwijderen van ruis in een beeld. Dat is niet alleen aan de orde bij het scherper maken van foto's, maar ook bijvoorbeeld bij het zien in het donker (militaire operaties). Het beeld wordt dan beschreven in termen van een statistisch model. Zo'n model kan parametrisch zijn (bijvoorbeeld een Poisson-model), waarbij de geschatte parameterwaarden als het ware het beeld samenvatten. Een voorbeeld is de weefselstructuur van een tapijt. In de beeldanalyse is het echter meestal beter niet een parametrisch model te gebruiken, maar een patroon in kaart te brengen door statistiek te bedrijven op een aantal eenvoudige aspecten ervan. Daarbij kan de aanpak van Bayes nuttig zijn. In het statistisch model wordt dan al bepaalde voorkennis ingebouwd, bijvoorbeeld dat naast een punt in de oceaan meestal een ander punt in de oceaan ligt. Het beste kansmodel voor dit soort verschijnselen is het 'Markov random field'. Deze aanpak bleek zeer succesvol, met algoritmen voor de classificatie van satellietbeelden, het verwijderen van ruis in videobeelden en de reconstructie van 3D-beelden in de medische tomografie. Op het CWI onderzoekt men met deze methode onder meer patroonherkenning in een grijswaarden-beeld, met toepassingen in het lezen van documenten zoals muziekpartituren en in de industriële robotica.

Prof.dr. A.J. Baddeley, Beeldanalyse (BS4)

Centrum voor Wiskunde en Informatica

Kruislaan 413

Postbus 94079, 1090 GB Amsterdam

telefoon 020-592 9333, telefax 020-592 4199

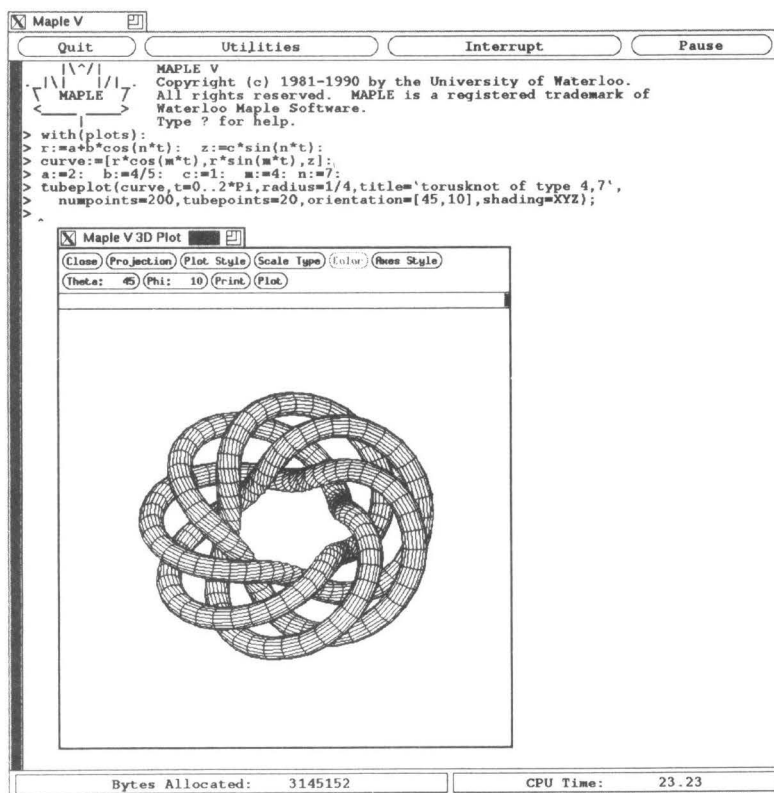
september 1993

SYMBOLISCH REKENEN OP DE COMPUTER IN OPMARS

Ruim tien jaar geleden was er een maatschappelijke discussie gaande of kinderen op de basisschool uitsluitend met behulp van (zak)rekenmachines zouden moeten (leren) rekenen of vooral uit hun hoofd. Vandaag geldt eenzelfde soort vraag voor het voortgezet en hoger onderwijs met betrekking tot het hanteren van wiskundige formules. In feite kunnen namelijk alle formele ingewikkelde wiskundige handelingen, zoals integratie en differentiatie, de reeksontwikkeling van functies en de berekening van matrices worden opgelost via zogenaamde computeralgebra-systemen, die ook wel symbolische manipulatieprogramma's worden genoemd.

Na het numerieke rekenen op de computer heeft nu ook het symbolisch rekenen op de computer de plaats van papier en potlood en de gedrukte tabellen overgenomen. Inmiddels zijn voor alle standaardbewerkingen programma's ontwikkeld in het symbolisch rekenen. Dat is gedeeltelijk een gevolg van het beschikbaar komen van de juiste programmatuur, maar vooral een gevolg van het veel krachtiger worden van de computers. Binnenkort zullen dergelijke programma's gemeengoed worden op alle opleidingsniveau's vanaf HAVO/VWO. De verwachting is dat de effecten voor het wiskunde-onderwijs veel drastischer zullen zijn dan die van de rekenmachine. Veel van de huidige tentamens zijn met behulp van deze pakketten uitvoerbaar door het intypen van enkele opdrachten.

Het werken met computeralgebra programma's biedt drie duidelijke voordelen: allerlei routinehandelingen worden machinaal uitgevoerd, waardoor er meer tijd overblijft voor het (echte) beoefenen van de wiskunde en bovendien worden rekenfouten en vergissingen vermeden. Je kunt daarnaast veel meer met wiskunde experimenteren, dus allerlei vermoedens testen of doorrekenen en functies onderzoeken



In moderne computeralgebra-systemen zijn de numerieke, symbolische en grafische aspecten van het wetenschappelijk rekenen samengebracht. De foto toont een torus-knoop van het type (4,7) gegenereerd door het software-pakket Maple.

via bijvoorbeeld visualisatie (grafieken). Computeralgebra is in de jaren zestig van de grond gekomen vanuit een behoefte in de natuurwetenschappen. Een van de eerste programma's, genaamd 'Schoonschip', is in 1965 ontworpen door de Nederlandse natuurkundige M. Veltman en dat jaar geldt dan ook min of meer als een omslagpunt. Inmiddels lijkt het met de computeralgebra net zo te gaan als indertijd met de tekstverwerking. Op de universiteiten zijn het vooral de jonge onderzoekers die er gebruik van maken, maar de toepassing van computeralgebra dringt ook door op middelbare scholen. Er zijn zowel algemene pakketten voor de meest voorkomende wiskundige handelingen (bijvoorbeeld voor het factoriseren van een getal of het maken van grafieken), als speciale pakketten voor specifieke algoritmen (bijvoorbeeld voor het uitvoeren van berekeningen in de hoge energiefysica en op het gebied van de wiskunde in de groepentheorie, algebraïsche meetkunde en commutatieve algebra).

CAN

Voor het doen gebruiken en verspreiden van pakketten en de benodigde ondersteuning daarbij is in 1989 de stichting Computer Algebra Nederland (CAN) opgericht, een platform voor alle computeralgebra gebruikers in Nederland. Deze stichting heeft een expertisecentrum binnen het CWI (er zijn op initiatief van NWO inmiddels ongeveer twintig van dergelijke centra in Nederland) en tussen beide bestaat een directe relatie. De stichting bevordert de ontwikkeling van de computeralgebra, coördineert seminaria en werkt case studies uit voor ingenieursbureau's, researchlaboratoria en voor in de industrie.

Het expertisecentrum houdt zich onder meer bezig met de aanleg van een programmabibliotheek en de verkoop van programma's. In feite is er al een aantal programma's beschikbaar voor het voortgezet onderwijs, en allerlei scholen, vooral HTS-en, blijken zeer geïnteresseerd te zijn.

RIACA

In 1993 is het Research Institute for Applications of Computer Algebra (RIACA) opgericht. Dit is een samenwerkingsverband tussen CAN, de Stichting Mathematisch Centrum (waartoe het CWI behoort) en het Kurt Gödel Instituut in Linz (Oostenrijk). Het is de bedoeling dat RIACA zal uitgroeien tot een Europees onderzoekscentrum voor toepassingen van computeralgebra.

Programma's

Een voorbeeld van een algemeen symbolisch rekenprogramma is 'Maple', een Canadees computeralgebra systeem dat meer dan 2000 verschillende mathematische bewerkingen aan kan. Maple kan bijvoorbeeld (stelsels van) vergelijkingen oplossen, functies integreren en differentiëren, Fourier-analyse uitvoeren, differentiaalvergelijkingen analytisch oplossen, werken met machtreeksen en limieten van functies, rekenen met Legendre-polynomen en met matrices (met symbolische coëfficiënten). Met behulp van Maple zijn ook numerieke benaderingen mogelijk en kunnen de formules die als eindproduct op het scherm verschijnen, worden vertaald naar andere programmeertalen voor een snelle en accurate numerieke verwerking.

Een ander voorbeeld is 'Derive', eveneens een algemeen programma dat speciaal voor de PC is gemaakt. Beide programma's kunnen door het CAN-expertisecentrum worden geleverd, terwijl de stichting opleidingsmogelijkheden aanbiedt.

Expertisecentrum CAN

Kruislaan 419
1098 VA Amsterdam
telefoon 020-592 6050, telefax 020-592 4199

september 1993

DYNAMISCHE SYSTEMEN LABORATORIUM ONDERSTEUNT NIET-LINEAIR ONDERZOEK

De meeste natuurverschijnselen worden wiskundig beschreven door niet-lineaire vergelijkingen. Bij de bestudering van deze vergelijkingen is de computer een onontbeerlijk hulpmiddel. Bij onderzoekers uit uiteenlopende disciplines bestaat er grote behoefte aan ondersteuning op dit gebied. Ook zijn vele aspecten van niet-lineaire (of dynamische) systemen nog nauwelijks onderzocht. Het CWI heeft daarom onlangs een Dynamische Systemen Laboratorium opgericht, waar onderzoekers computer-experimenten kunnen uitvoeren en ook terecht kunnen met hun problemen.

Onderzoek naar niet-lineaire dynamische systemen heeft de laatste twee decennia een explosieve groei gekend. De brede belangstelling voor dit onderwerp blijkt ook uit het feit dat enkele aspecten, zoals *fractals* en *chaos*, zeer populair zijn geworden in de media. Een dynamisch systeem is een stelsel vergelijkingen waarmee men, in principe, uitgaande van het verleden de toekomst kan voorspellen. Bij een lineair systeem hebben kleine oorzaken ook kleine gevolgen. Is het systeem daarentegen niet-lineair, dan kunnen kleine wijzigingen in de begintoestand de eindtoestand compleet veranderen. Hoewel het systeem deterministisch is, dat wil zeggen op elk tijdstip volkomen bepaald door de vergelijkingen, kan er schijnbaar willekeurig 'chaotisch' gedrag ontstaan. Het besef dat een deterministisch systeem zich in de praktijk toch onvoorspelbaar kan gedragen is pas vrij recent gemeengoed geworden. Wiskundigen onderzoeken al bijna een eeuw dynamische systemen. Pioniers waren onder anderen Poincaré, Lyapunov, Markov en Birkhoff. De jaren zestig en zeventig gaven diverse doorbraken te zien, zowel op wiskundig gebied (bijvoorbeeld het theorema van Kolmogorov, Arnol'd en Moser over kleine storingen van een 'integreerbaar' systeem, zoals een om de zon draaiende asteroïde) als daarbuiten. Een dynamisch systeem is een zeer algemeen begrip en komt dan ook in de natuur in vele vormen voor. Geen wonder dus dat enkele van de belangrijkste doorbraken hun oorsprong hadden in gebieden als de meteorologie (lange-termijn weersvoorspelling, Lorenz), astronomie (planetenbanen, Hénon) en biologie (insectenplagen, May). Al snel ontdekte men dat ook een zeer eenvoudig systeem als een slinger (het symbool van regelmaat!) vergelijkbaar chaotisch gedrag kon vertonen.

Men kan een niet-lineair dynamisch systeem op verschillende wijzen bestuderen. Een ervan is de bijbehorende differentiaalvergelijkingen oplossen. Heel soms kan dit met de hand, maar meestal zijn numerieke of symbolische (computer algebra) berekeningen nodig. Dit heeft onder meer geleid tot een aantal ontdekkingen, zoals het bestaan van vormvaste oplossingen (solitonen). Vaak krijgt men echter meer inzicht via andere wegen. Een dynamisch systeem bezit een aantal vrijheidsgraden, de 'coördinaten' van het systeem, en kan worden beschreven door het tijdsverloop te bepalen van deze coördinaten en hun bijbehorende snelheden. Coördinaten en snelheden vormen samen de 'faseruimte' van het systeem. Een vlakke slinger heeft bijvoorbeeld één vrijheidsgraad, een fiets heeft er vijf.



De kern van het dobbelspel bestaat uit de praktische onvoorspelbaarheid van de eindtoestand (welke zijde komt boven?) uit een gegeven begintoestand.

Elke toestand van een systeem correspondeert met een punt in de faseruimte en zijn ontwikkeling in de tijd met een kromme in die ruimte. Een wrijvingsloze slinger keert steeds terug in zijn begintoestand (periodieke beweging) en het 'fase-portret' is dan een gesloten kromme. Zo'n regulier fase-portret is het kenmerk van exact oplosbare ('integreerbare') systemen. Met wrijving vertoont het systeem al karakteristieke chaotische eigenschappen en wordt het fase-portret ingewikkeld. Bestuuring hiervan, bijvoorbeeld visueel op een goed kleurenscherm, geeft vaak kwalitatief inzicht in het gedrag van het systeem, dat niet of nauwelijks is te krijgen door naar de vergelijkingen zelf te kijken.

Een derde, zeer vruchtbaar gebleken aanpak is uit de vergelijkingen een 'iteratieve kaart' te maken door een volgend stadium in de ontwikkeling van een systeem te beschrijven in termen van een voorgaand stadium: $x_{t+1} = F(x_t)$, waar de 'tijd' t een natuurlijk getal is. De functie F bevat een of meer varieerbare parameters, bijvoorbeeld een wrijvingscoëfficiënt, en men kijkt naar de verzameling limietpunten ($t \rightarrow \infty$) voor allerlei parameterwaarden. Door met een zakcomputer de iteratieve kaart van de door May bestudeerde logistieke vergelijking uit de populatiebiologie door te rekenen - een model met één vrije parameter - , vond Feigenbaum dat er boven een bepaalde waarde van die parameter twee limietpunten zijn in plaats van één ('periode-verdubbeling' of 'bifurcatie'), dat dit verschijnsel zich bij hogere parameterwaarden met steeds kortere tussenruimtes herhaalt en dat er relaties tussen deze bifurcatiepunten bestaan die in geheel andere dynamische systemen precies dezelfde zijn ('universaliteit'). Deze overgang van regelmaat naar chaos kan men ook zien als een soort fase-overgang. Er zijn overigens ook nog andere wijzen waarop die overgang kan plaatsvinden. Van speciaal belang zijn gebieden in een fasediagram waar het systeem een zekere voorkeur voor heeft ('aantrekkers'). Bij niet-lineaire systemen vormen die gebieden vaak zulke grillige patronen dat men spreekt van 'vreemde aantrekkers'. Meetkundig hebben die patronen dan een fractale structuur, dat wil zeggen een niet-geheeltallige dimensie.

De studie van niet-lineaire dynamische systemen heeft grote praktische waarde omdat veel natuurverschijnselen als zodanig kunnen worden gemodelleerd. Zo wil men soms voorkomen dat een systeem chaotisch gedrag gaat vertonen. Voorbeelden zijn te vinden in uiteenlopende situaties zoals elektrische schakelingen, chemische reacties, stromingen (turbulentie), de hartslag en de effectenbeurs. Kennis over het ontstaan van chaos is dan nodig om dit door een geschikte systeemregeling te voorkomen. Ook is soms inbouw van een zekere mate van chaos gewenst, bijvoorbeeld ter bestrijding van geluidshinder door versnellingsbakken in personenauto's. Tot nu toe zijn voornamelijk systemen met slechts enkele vrijheidsgraden onderzocht. Uitbreiding tot systemen met meer vrijheidsgraden behoort tot de onderzoeksprioriteiten van de komende jaren.

De spectaculaire opbloei van dit vakgebied zou ondenkbaar zijn geweest zonder gebruik van de computer als 'laboratorium', waar experimenten helpen de richting van het verdere onderzoek te bepalen. De problemen waarmee men op dit gebied in verschillende disciplines te maken krijgt vertonen veel overeenkomsten. Het is dan effectief om kennis en computerfaciliteiten te bundelen op een centrale plaats voor dienstverlening en onderzoek. Het Dynamische Systemen Laboratorium (DSL) op het CWI, gestart in 1993, zal zo'n functie in Nederland gaan vervullen. De activiteiten zullen nauw aansluiten bij het NWO Prioriteitsprogramma Niet-Lineaire Systemen (1991-1998). Deze activiteiten omvatten:

- het onderhouden van een gespreid netwerk van hoogwaardige grafische werkstations;
- het regelen van de toegang tot centrale parallele computerfaciliteiten;
- de beschikbaarstelling van een gebruiksvriendelijke experimenteer-omgeving, inclusief diverse software pakketten, ten behoeve van onderzoekers;
- fungeren als centrum voor gast-onderzoekers;
- ondersteuning van concrete onderzoeksprojecten en onderzoekers elders.

Dr. J.A. Sanders, prof.dr. M. Hazewinkel, Dynamische Systemen Laboratorium
telefoon 020 - 592 4051, 020 - 592 4204

Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199
september 1993

WISKUNDE ONMISBARE BASIS VOOR MILIEUMODELLEN

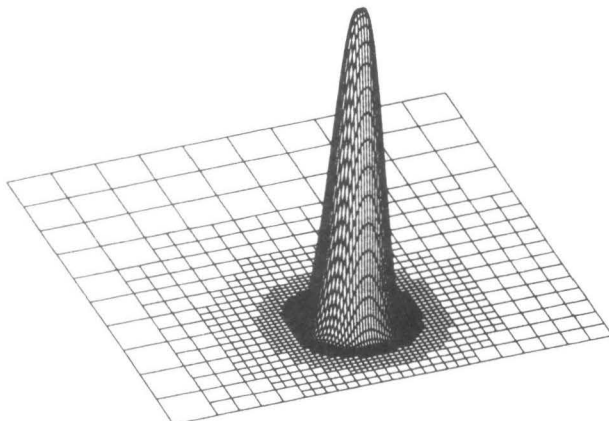
Aan het milieu-onderzoek wordt bijgedragen vanuit zeer veel wetenschapsgebieden. Wiskunde en informatica nemen daarbij een speciale plaats in. Met veel van de te bestuderen systemen kan men namelijk niet experimenteren. Wiskundige modellen en computersimulaties zijn dan de aangewezen middelen om inzicht te krijgen in het gedrag van die systemen. Ook binnen de wiskunde en informatica spelen hierbij diverse disciplines een rol. Het CWI is in 1992 gestart met een multidisciplinair onderzoekprogramma Wiskunde & Milieu, waarin verschillende groepen binnen en buiten het CWI samenwerken.

Enkele voorbeelden van milieuproblemen, waarbij men is aangewezen op modellering en simulatie, zijn: aantasting van de biosfeer, verspreiding van ziekten binnen populaties, plaatselijke luchtverontreiniging, schone en veilige energievoorziening, verspreiding van schadelijke stoffen (bijvoorbeeld door grondwaterstromingen) en klimaatveranderingen op wereldschaal. Hieraan ziet men hoe breed het spectrum der betrokken wetenschapsgebieden is: meteorologie, oceanografie, hydrologie, geologie, biologie, natuurkunde, scheikunde en - last but not least - wiskunde en informatica. Binnen de laatste twee disciplines wordt vooral een beroep gedaan op: numerieke wiskunde (speciaal vloeistofdynamica), grootschalig rekenwerk op super- en parallelle computers in combinatie met visualisering en massale gegevensverwerking, beeldreconstructie, inverse methoden en parameter-identificatie, dynamische systeemtheorie en chaos, statistiek, besliskunde, optimalisering en regeltechniek, en biomathematica.

Het multidisciplinaire programma Wiskunde & Milieu brengt al het lopende en geplande CWI-onderzoek op milieugebied onder één noemer.

Luchtvervuiling

Het transport van vervuiling door de lucht wordt beschreven door zogenaamde LRTAP-modellen (Long-Range Transport of Air Pollution). De vergelijkingen - één voor elke chemische stof - beschrijven advection (transport onder invloed van wind), diffusie en de onderlinge chemische reacties. Realistische LRTAP-modellen behoren tot de omvangrijkste en in computergebruik duurste ter wereld. In het project EUSMOG ontwikkelt het CWI in samenwerking met het RIVM efficiënte algoritmen voor luchtvervuilingsmodellen ten behoeve van regionale smog-voorspelling op Europese schaal.



De Molenkamp test is een veel gebruikte methode voor het testen van de betrouwbaarheid van numerieke modellen voor luchtvervuiling, zoals de uitstoot van gassen door fabrieken.

In het project CIRK werkt het CWI samen met IMAU (Instituut voor Meteorologie en Oceanografie, Rijksuniversiteit Utrecht), RIVM en KNMI aan de wiskundige modellering van de veranderingen in chemische samenstelling van de troposfeer op wereldschaal, als gevolg van de verspreiding van vervuillende stoffen. Het specifieke doel is een 3D model te maken van de troposfeer, waarin uitwisseling met de stratosfeer is ingebouwd, ten behoeve van voorspellingen op lange termijn. Omdat efficiënte algoritmen en grote rekenkracht hier essentiële voorwaarden zijn, krijgen in het onderzoek HPCN-aspecten (High Performance Computing and Networking) grote aandacht.

Verspreiding van infecties

Bij het onderzoek naar de verspreiding van ziekten binnen de veestapel kunnen wiskundige modellen meer inzicht geven in de effecten van individuele karakteristieken op de populatie als geheel. Samen met het Centraal Diergeneeskundig Instituut (CDI) in Lelystad heeft het CWI theoretische onderzoeksresultaten toegepast op bepaalde dierziekten, in het bijzonder de ziekte van Aujeszky bij varkens. De effectiviteit van maatregelen ter beheersing van epidemieën bij (ketens van) veefokkerijen is bestudeerd met behulp van evolutiemodellen van gestructureerde populaties. Verder zal, in samenwerking met CDI, RIVM en de Rijksuniversiteit Leiden, soortgelijk onderzoek beginnen naar de geheimzinnige virusziekte die regelmatig de zeehondenpopulatie in het Waddengebied treft.

Identificatie van compartiment-systemen

In nauwe samenwerking met het RIVM onderzoekt het CWI de wiskundige onderbouwing van beslissingen over kwesties als de wijze van opbergen en bewaren van kernafval, de toelaatbare hoeveelheid zwaveldioxyde uitstoot en de beperking van schadelijke stoffen in voedingsmiddelen en industriële produkten. Zulke vragen zijn wiskundig goed te formuleren met de theorie van 'compartiment-systemen', een speciaal soort dynamische systemen met veel toepassingen in de biologie en de wiskunde. Uitgaande van begrippen uit de systeem- en regeltheorie richt het CWI-onderzoek zich vooral op systeemidentificatie.

Sediment transport in ondiep water

In het EG-programma NOWESP (NORTH West European Shelf Program) bestudeert men onder meer het vervuilingseffect van de Rijn en andere grote Europese rivieren in het Continentaal Plat. Op het CWI zijn 3D parallelle gevectoriseerde stromingsmodellen ontwikkeld en geïmplementeerd op een Cray Y-MP supercomputer, die worden gebruikt bij het onderzoek naar sediment-transport. Dergelijke fysische verschijnselen zijn sterk lokaal van aard. Daarom is het CWI, in samenwerking met Rijkswaterstaat en de universiteit van Delft, bezig adaptieve roostertechnieken te ontwikkelen voor gebruik op parallelle vectorcomputers ten behoeve van het 3D model TRIWAQ voor het Continentaal Plat. Ook hier krijgen HPCN aspecten grote aandacht.

Dr. J.G. Verwer, Wiskunde & Milieu
telefoon 020 - 592 4095

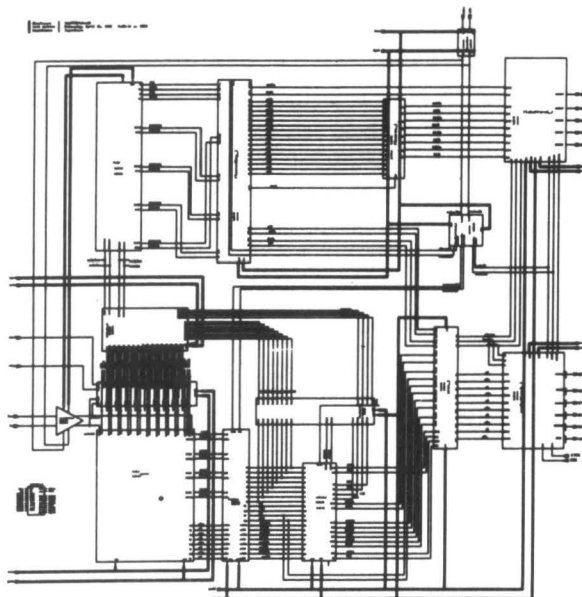
Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199
september 1993

NUMERIEKE MODELLERING VAN EVOLUTIEPROCESSEN

In de natuur en in de techniek komen veel tijdsafhankelijke processen voor, die vanuit maatschappelijk of industrieel oogpunt van belang zijn om te bestuderen. Voorbeelden zijn de verspreiding van verontreinigingen in grondwater, oppervlaktewater en de atmosfeer en het verloop van elektrische stromen in ingewikkelde circuits. Simulatie van dergelijke 'evolutieprocessen' via wiskundige modellen verdringt steeds meer het werken met schaalmodellen. Op het CWI zijn diverse numerieke algoritmen ontwikkeld en onderzocht voor het effectief oplossen van de vergelijkingen die de grondslag vormen van dergelijke wiskundige modellen.

Veel processen in natuur en techniek, waarbij continue veranderingen optreden, worden wiskundig beschreven door differentiaalvergelijkingen. Als hierin naast de tijd ook andere variabelen voorkomen, zoals plaatscoördinaten, spreekt men van partiële differentiaalvergelijkingen (PDV's). Voorbeelden zijn de ondiep-watervergelijkingen en de poreuze-mediumvergelijkingen, die respectievelijk de waterbeweging in ondiepe zeeën en grondwaterstromen beschrijven. Het opstellen van dergelijke vergelijkingen heet wiskundige modellering. Door de tijd- en plaatsvariabelen op rekenroosters te discretiseren verkrijgt men een numeriek model dat vervolgens benaderd wordt opgelost op de computer. Door de grote rekencapaciteit van de huidige super- en parallelle computers is dit 'numeriek modelleren' tegenwoordig vaak vele malen goedkoper dan het bouwen van traditionele schaalmodellen. Daarnaast zijn er vele processen die met een schaalmodel niet goed zijn na te bootsen, zoals de verspreiding van verontreiniging in lucht, bodem en water.

Het numeriek oplossen van PDV's is zeer rekenintensief. Discretisering in de plaatscoördinaten leidt tot een reusachtig stelsel van gewone differentiaalvergelijkingen, waarin alleen de tijd nog als continue variabele voorkomt. Daarna wordt de tijdvariabele gediscrèteiseerd en het stelsel stap voor stap opgelost met behulp van een numerieke integratieformule die uit de oplossing op het tijdstip t_0 de oplossing op het tijdstip $t_0 + \Delta t$ berekent. De keuze van de formule hangt af van de stabiliteit (gevoeligheid van het evolutieproces voor verstoringen), de gewenste nauwkeurigheid van de benadering, en de efficiëntie van het hele rekenproces in termen van rekestijd en geheuegebruik.



Circuit diagram van de Philips TDA8760 AD converter, met meer dan 2600 transistors, 400 weerstanden en 6 capaciteiten (bron: Philips Research Laboratories). Simulaties van elektrische circuits zijn zo rekenintensief dat alleen gebruik van parallelle computerarchitecturen en daarop afgestemde numerieke algoritmen uitkomst biedt.

Ook de stabiliteit van de integratieformule zelf is een belangrijk criterium. Bij numerieke instabiliteit wordt de benaderingsfout al snel overvleugeld door een geweldige accumulatie van afrond- en discretiseringsfouten. Met betrekking tot de stabiliteit zijn er twee soorten integratieformules: impliciete en expliciete. Impliciete formules zijn in het algemeen voldoende stabiel, maar zeer duur in het gebruik, omdat hierbij grote stelsels algebraïsche vergelijkingen iteratief moeten worden opgelost. Expliciete formules zijn zeer goedkoop per tijdstip (er hoeven geen stelsels te worden opgelost), maar zijn meestal alleen stabiel als men zeer veel tijdstappen neemt. De afweging expliciet/impliciet integreren vormt een kernthema in de numerieke analyse van evolutieprocessen.

Het CWI-onderzoek aan het stabiliseren van expliciete integratieformules heeft een verscheidenheid van algoritmen opgeleverd die ook voor grote praktijkproblemen een oplossing bieden. We noemen hier: gestabiliseerde Runge-Kutta formules voor warmte- en diffusieproblemen, bijzondere expliciete/impliciete formules voor ondiep-watervergelijkingen, en 'split-technieken' die toepasbaar zijn op ruime klassen van PDV's. Het onderzoek concentreert zich thans op het gebruik van adaptieve roostertechnieken voor zeer rekenintensieve problemen, op de numerieke modellering van ondiep-water vergelijkingen, op algoritmen voor de simulatie van transport van luchtverontreiniging, en op de integratie van gewone differentiaalvergelijkingen op parallelle computers, vooral gericht op toepassingen in circuitanalyse en regeltechniek.

Praktijk

Het onderzoek in de groep Numerieke Modellering van Evolutieprocessen heeft vele raakvlakken met de praktijk, zoals onderstaande recente voorbeelden duidelijk maken.

Parallele methodes voor circuitanalyse en regeltechniek - Real-time computertoepassingen in de circuitanalyse en regeltechniek vereisen een hoge verwerkingssnelheid, die kan worden verkregen door uitbuiting van de mogelijkheden tot parallelle verwerking op nieuwe computerarchitecturen. In plaats van bestaande oplossingsmethoden voor de omvangrijke stelsels niet-lineaire differentiaal-/algebraïsche vergelijkingen te paralleliseren, beloven geheel nieuwe, speciaal voor parallelle computers ontworpen methoden een veel grotere snelheidswinst. In een STW-project ontwikkelt het CWI, in samenwerking met Philips (PRLE, Eindhoven) en de universiteiten van Twente en Amsterdam zulke nieuwe methoden.

Ondiep water - Voor Rijkswaterstaat is een efficiënt rekenmodel voor drie-dimensionale ondiep-watervergelijkingen (multilayer model) ontwikkeld. Dat model vormt een uitgangspunt voor de simulatie van watervervuiling, sediment-transport en andere biologische of chemische processen, die alleen op de krachtigste parallelle supercomputers kunnen worden gemodelleerd.

Luchtvervuiling - Het transport van vervuiling door de lucht wordt beschreven door LRTAP-modellen (Long-Range Transport of Air Pollution). Deze behoren tot de omvangrijkste en in computergebruik duurste ter wereld. In het project EUSMOG ontwikkelt het CWI in samenwerking met het RIVM efficiënte algoritmen voor luchtvervuilingsmodellen ten behoeve van regionale smogvoorspelling op Europese schaal. Verder werkt het CWI in het project CIRK samen met IMAU (Instituut voor Meteorologie en Oceanografie, Rijksuniversiteit Utrecht), RIVM en KNMI aan de wiskundige modellering van de veranderingen in chemische samenstelling van de troposfeer op wereldschaal, als gevolg van de verspreiding van vervuilende stoffen.

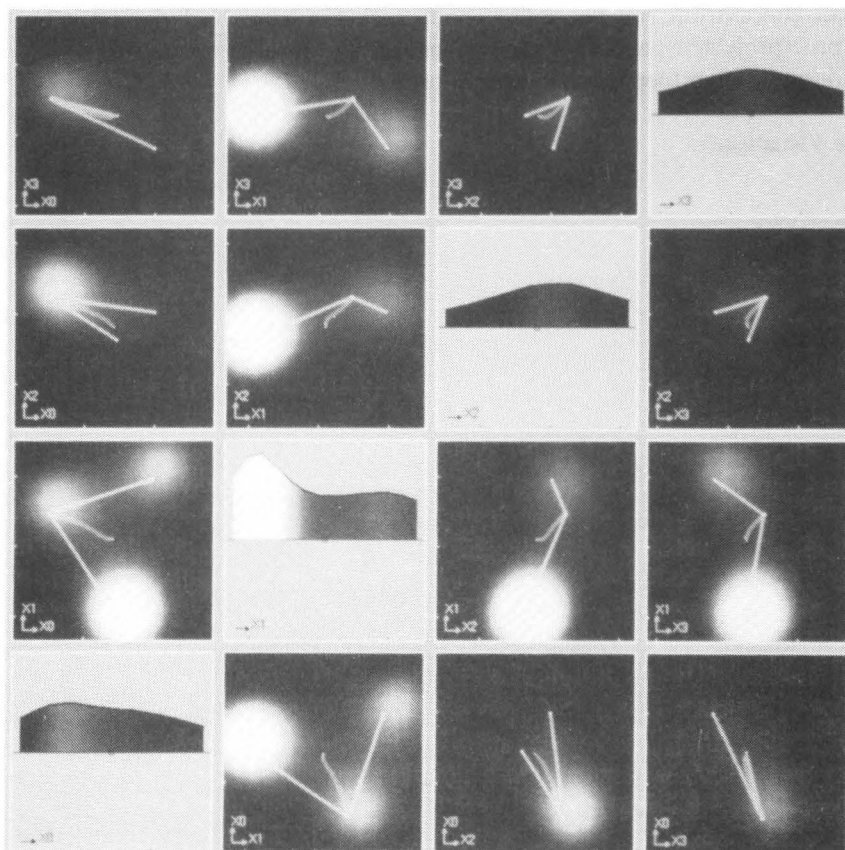
Prof.dr. P.J. van der Houwen, dr. J.G. Verwer
Numerieke Modellering van Evolutieprocessen (NW1)
telefoon 020 - 592 4083, 020 - 592 4095

Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199
september 1993

VISUALISATIE VAN GEGEVENS GEEFT EXTRA DIMENSIE AAN ONDERZOEK

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 is daarom onlangs een project Wetenschappelijke Visualisatie gestart.

Het is bijna ondoenlijk om uit een grote hoeveelheid gegevens, in de vorm van bijvoorbeeld getalwaarden, 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 meer zegt 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. Het komt echter ook vaak voor dat het te bestuderen verschijnsel wordt beschreven in een ruimte van meer dan drie dimensies, waarvan we ons niet direct een visuele voorstelling kunnen vormen. Een voorbeeld is de clusteranalyse in de statistiek, waar van een groot aantal individuen bepaalde karakteristieken worden gemeten, en vervolgens weergegeven als een verzameling punten (elk punt correspondeert met één individu) in een ruimte met een dimensie gelijk aan het aantal karakteristieken. De enige manier om in zulke gevallen iets 'zichtbaar' te maken is aan de hand van een aantal visualiseerbare doorsneden van hooguit drie dimensies.



Visualisatie met HyperSlice (CWI-ECN) van een scalaire functie van vier variabelen als een matrix van orthogonale 2D-doorsneden, gecentreerd om een punt in de 4D-ruimte dat de gebruiker met de muis kan variëren.

Door de snel toegenomen rekenkracht en grafische mogelijkheden van computers zijn thans 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 bewaken van structuren die anders verborgen zouden blijven.

Op het CWI wordt in het project Wetenschappelijke Visualisatie 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 met aangepaste invoergegevens wordt herhaald. 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 'navigatie'. De onderzoeker varieert zijn invoer als functie van de tijd en volgt een bepaald plan om een doel te bereiken, bijvoorbeeld 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 gewenste 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.

In samenwerking met het visualisatiecentrum van het Energieonderzoek Centrum Nederland (ECN) wordt op het CWI in enkele proefprojecten gekeken naar het visueel specificeren en bewaken van invoergegevens. In een later stadium komen toepassingen aan de orde.

R. van Liere, Wetenschappelijke Visualisatie
telefoon 020-592 4118

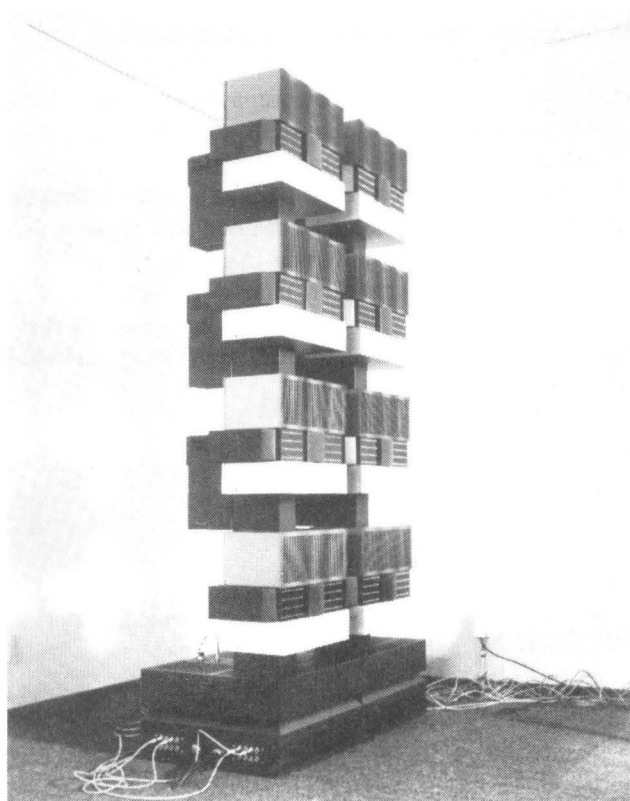
Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199
september 1993

GROOTSCHALIG REKENEN STEUNT OP PARALLELE VERWERKING

De rekenkracht en het geheugen van de snelste computers zijn in de jaren tachtig sterk toegenomen. Deze trend zal naar verwachting dit decennium onverminderd doorgaan. De toverformule achter de huidige groei luidt: massaal parallelle verwerking. De snelste computers van de toekomst zijn systemen met vele duizenden parallelle processoren. Optimale benutting van zulke architecturen vergt de ontwikkeling van nieuwe numerieke methoden. Het CWI-onderzoek op dit terrein heeft vooral toepassingen in de stromingsleer en de cryptografie (getaltheorie).

De snelste computers van het ogenblik zijn steeds beter in staat de werkelijkheid realistisch na te bootsen. Deze werkwijze kan aanzienlijk goedkoper uitvallen dan het werken met schaalmodellen, bijvoorbeeld bij het ontwerpen van vliegtuigen, of het fysisch experimenteren, zoals botsingsproeven bij het ontwikkelen van nieuwe automodellen. Het is zelfs de enige manier om processen te bestuderen waarbij realistische experimenten onmogelijk zijn, zoals bij de verspreiding van giftige stoffen in het milieu. Het grootschalig rekenen is in vele takken van wetenschap uitgegroeid tot een aparte discipline. Enkele voorbeelden: de studie van stromingen van vloeistoffen en gassen rond schepen c.q. vliegtuigvleugels, het ontwikkelen van nieuwe geneesmiddelen, macro-economische voorspellingen, het zoeken naar olie en gas, wereldwijde klimaatstudies, het ontwerpen van chips en het ontbinden in factoren van grote getallen.

Een belangrijk aspect bij deze toepassingen is de simulatie, zo belangrijk dat men in dat opzicht kan spreken van een autonome derde richting van onderzoek, tussen de traditionele theoretische en experimentele richtingen. Met behulp van een (super)computer kan men zo verschijnselen bestuderen die in het laboratorium een zeer lange tijd (duizenden jaren) of zeer korte tijd (enkele picoseconden) in beslag zouden nemen. Daarbij kan het model vaak zonder veel moeite een beetje worden veranderd, en de 'waarnemingen' worden niet beïnvloed door het apparaat waarmee de metingen worden uitgevoerd.



De bij SARA opgestelde Parsytec GCel-3/512 massaal parallelle computer.
Foto: Bram de Hollander.

Met de door de natuur gestelde snelheidsgrenzen in zicht is er bij de bouw van toekomstige computersystemen alleen nog snelheidswinst te halen door andere, met name parallelle, architecturen. Het doorrekenen van realistische modellen vereist een dusdanige rekenkracht dat alleen parallellisme (machines met honderden, in de nabije toekomst duizenden processoren) uitkomst kan brengen. Het grootste probleem is hierbij de communicatie: de rekenchips van al die processoren zijn zo snel dat de hiervoor 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 staat nog in de kinderschoenen. 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 algoritmen voor vector- en parallelle computers en het ontwikkelen van nieuwe algoritmen. Daarbij wordt onder meer gebruik gemaakt van de bij de Stichting Academisch Rekencentrum Amsterdam (SARA) opgestelde Cray Y-MP4 supercomputer en het Parsytec GCel massaal parallelle computersysteem. Een deel van het werk op de Parsytec gebeurt in het kader van het onlangs opgerichte 'Interdisciplinary Centre for Computer based Complex Systems Research Amsterdam' (IC3A), een samenwerkingsverband van de Universiteit van Amsterdam en het CWI, waarbij ook de industrie wordt betrokken.

Meer in het bijzonder besteedt het CWI aandacht aan algoritmen voor matrix decompositie, domein decompositie, het bepalen van enkele eigenwaarden van zeer grote ijle matrices, het gegeneraliseerde eigenwaardeprobleem, het oplossen van grote lineaire stelsels met minimalisatie van geheugengebruik, multigrid-, en multi-precisie berekeningen. Toepassingen liggen onder andere op het gebied van de stromingsleer (bijvoorbeeld stromingen in ondiep water en rond vliegtuigvleugels). Ook bestudeert men thans het gebruik van 'software tools' (zoals PVM en CONDOR) voor het op een machine-onafhankelijke wijze ontwikkelen en onderhouden van parallelle programmatuur. In dit verband wordt ook gekeken naar 'Problem Solving Environments', waarin verscheidene componenten, zoals numerieke methoden, symbolisch rekenen en visualisering zijn geïntegreerd.

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 zeer uitvoerige berekeningen uitgevoerd aan de Riemann hypothese en aan de vermoedens van Mertens en Goldbach, drie klassieke wiskundige problemen; thans wordt onderzoek verricht naar de geschiktheid van moderne factorisatiemethoden (voor het ontbinden van grote getallen in priemfactoren) voor vector- en parallelle computers. Enkele malen heeft het CWI hierbij getallen van recordgrootte weten te 'kraken'. Met name wordt gekeken naar de praktische bruikbaarheid van de theoretisch snelste methode, de Number Field Sieve, alsmede naar het oplossen van zeer grote stelsels lineaire vergelijkingen over eindige lichamen (bijvoorbeeld de natuurlijke getallen). Bij dit onderzoek wordt nauw samengewerkt met de Rijksuniversiteit Leiden.

Dr.ir. H.J.J. te Riele, Grootschalig Rekenen (NW3)
telefoon 020-592 4106

Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199

september 1993

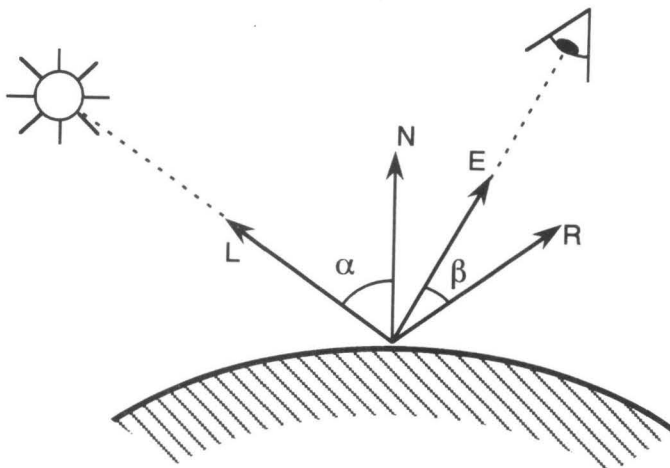
SNELLE BEELDMANIPULATIE OP RASTERSCHERMEN

Het presenteren en manipuleren van beelden op een grafisch beeldscherm kost nog altijd zo veel rekenwerk, dat dit gemakkelijk de gehele capaciteit van het werkstation opslokt. Aanzienlijke verbetering in visuele communicatie blijkt mogelijk door betere faciliteiten te scheppen voor *interactie* met beelden. Het CWI heeft hiertoe een nieuwe werkstation-architectuur ontworpen, waarin speciale, zeer krachtige chips (VLSI) zijn opgenomen, die samen met de Universiteit Twente in een STW-project zijn ontwikkeld.

Het afbeelden van voorwerpen op een computerbeeldscherm is technisch nog steeds een groot probleem. Tot voor kort kwam men niet veel verder dan het tonen van een 'draadstructuur', die tegelijkertijd het eindprodukt was van de berekeningen. Tegenwoordig zijn de goede werkstations weliswaar standaard uitgerust met hoge-resolutie beeldschermen en snelle processoren, en leiden de gegenereerde beelden tot een betere visuele communicatie, maar tegelijkertijd legt dit een zwaar beslag op de computercapaciteit. Bovendien zal er nog aanzienlijk meer capaciteit nodig zijn als men ook de gewenste aandacht wil geven aan zaken als de verlichting van de getoonde objecten, schaduwwerking en textuur. Als men ook nog hiermee in real-time wil manipuleren, dan blijkt de capaciteit van de meeste werkstations daarvoor volstrekt ontoereikend.

Rasterschermen zijn ontworpen om er realistische, ruimtelijke beelden op te kunnen tonen. Het scherm is verdeeld in een groot aantal (in de orde van een miljoen) 'puntjes' (pixels). Elk puntje kan men een kleur toewijzen; er zijn vele miljoenen mogelijke kleuren. De puntjes worden elke zestigste seconde ververst vanuit een pixelrepresentatie. Hierbij zijn de kleurenwaarden van individuele pixels opgeslagen in een 'frame-buffer', omdat het doorlopen van de pijplijn meer tijd neemt dan de aanwezigheid van de betreffende pixel op het beeldscherm. Bij real-time animatie verandert de inhoud van de frame-buffer ongeveer twintig maal per seconde van waarde. Afgezien van het grote geheugenbeslag stelt dit hoge eisen aan de organisatie van het tot stand komen en veranderen van beelden.

Voor de opbouw van een beeld moet een serie grafische handelingen worden verricht, zoals beeldprojectie, belichtingsberekening, zichtbaarheidsbepaling en pixelgeneratie. Wil men interactief met zo'n beeld kunnen werken, dan is het zaak om die serie (de 'grafische pijplijn') zo snel mogelijk te doorlopen (korte responstijd). De gebruikelijke aanpak is om die handelingen die de meeste kans op vertraging geven, te versnellen door het inbouwen van speciale hardware.



Belichtingsberekeningen zijn zeer rekenintensief. Voor interactieve grafische toepassingen is daarom nog veel onderzoek nodig op dit gebied. De berekeningen berusten op de invalshoek α ten opzichte van de normaal N en de reflectiehoek β ten opzichte van de kijkrichting E .

Het onderzoek van de CWI-groep Computergrafiek heeft aangetoond dat nog veel meer is te winnen door gebruik te maken van het feit dat het niet nodig is om voor elke interactie de hele grafische pijplijn te doorlopen. Hiertoe zijn de interacties, afhankelijk van welk deel van de pijplijn wordt doorlopen, ingedeeld in klassen, en is de architectuur van het hele grafische systeem daarop afgestemd. Een belangrijke eigenschap van deze architectuur is de opslag van tussenresultaten op handig gekozen niveau's. Op het laagste, voor interactie meest veelvuldig benodigde niveau zijn alleen alle volledig zichtbare gedeelten van voorwerpen opgeslagen op een als zodanig herkenbare manier. Het tweede niveau bevat (groepen van) objecten, bijvoorbeeld een geheel vlak met dezelfde eigenschappen, terwijl de volledige 3D scene het hoogste niveau vormt. Opslag in de vorm van pixels blijkt in deze architectuur niet noodzakelijk. De gebruiker is nu in staat om alleen bepaalde delen van een beeld te veranderen, waardoor het tijdrovende steeds weer opnieuw vullen van de frame-buffer wordt vermeden.

Bij het ontwerpen van een nieuwe architectuur is een geheel nieuw algoritme ontwikkeld, dat een beeldrepresentatie van het laagste niveau oplevert (voor kenners: een rooster-onafhankelijk incrementeel hidden surface removal algoritme). Hierdoor kan men met het object in de ruimte manipuleren, veranderingen aanbrengen zonder het gehele object opnieuw op te bouwen en bovendien transparante objecten hanteren. Ook zijn nieuwe belichting-berekeningsmethoden ontwikkeld en zijn diverse bestaande algoritmen verbeterd en vaak aanzienlijk sneller gemaakt.

Voor de aansturing van het beeldscherm door middel van een vanuit het laagste niveau gegenereerd videosignaal zijn op basis van het CWI-onderzoek door een team van de Universiteit van Twente speciale chips ('full custom VLSI') ontworpen, met een pixel-generatiesnelheid van 12 nanoseconden per pixel. Hiermee kan men niet alleen real-time realistische beelden van ruimtelijke vormen op het scherm krijgen, maar ook bijvoorbeeld raster-onafhankelijke lettertypen ten behoeve van 'document previewing', met een tot nu toe ongekende snelheid en beeldkwaliteit.

De chips worden, in samenwerking met de vakgroep Informatica van de Universiteit van Amsterdam, ingebouwd in een prototype werkstation, waarbij speciale grafische functies, zoals belichtingsberekeningen en het veranderen van de gezichtshoek, worden toegewezen aan afzonderlijke parallele processoren. Hiermee komt een werkomgeving binnen bereik waarin met ruimtelijke vormen wordt gemanipuleerd zoals nu desk top publishers met illustraties in documenten manipuleren. Zoals gebruikelijk bij STW-projecten is de industrie vanaf het begin betrokken geweest bij het onderzoek.

Drs. A.A.M. Kuijk, Computergrafiek (IS1)
telefoon 020 - 592 4160

Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199
september 1993

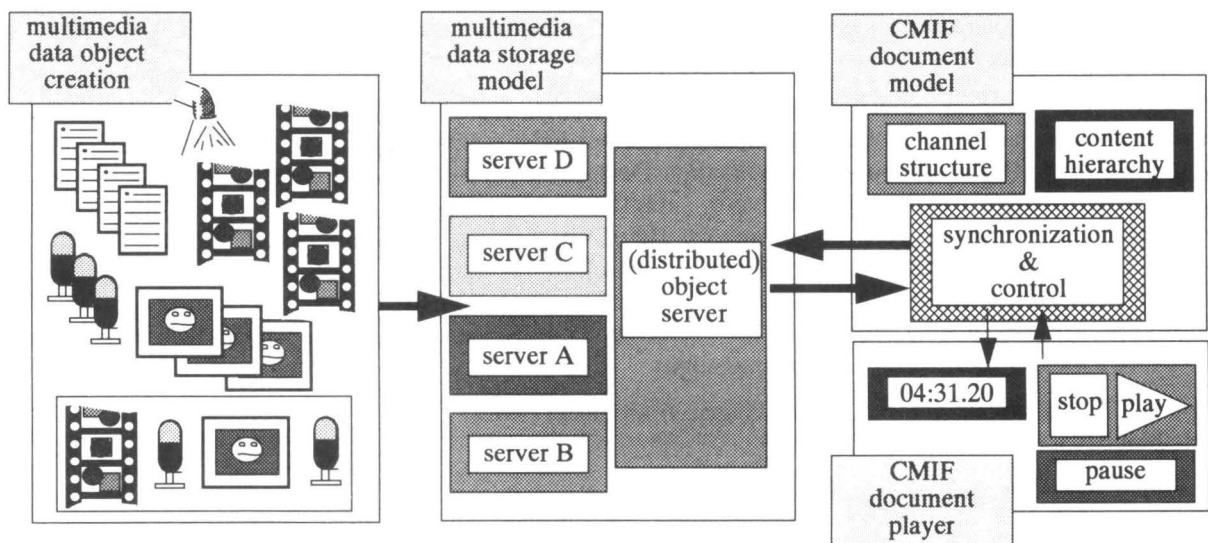
MULTIMEDIA: FUNDAMENTEEL ONDERZOEK MOET WILDGROEI VOORKOMEN

Multimedia behelst het geïntegreerd aanbod van tekst, beeld en geluid via een computersysteem. Ondanks de snelle technische vooruitgang blijft een aantal fundamentele problemen vooralsnog onopgelost: datastromen zijn onvoldoende gestructureerd, de huidige systemen zijn ongeschikt voor gebruik in een heterogeen netwerk van werkstations, en synchronisatie tussen de componenten van een multimedia-document is systeem-afhankelijk. Omdat bij het onderzoek verschillende disciplines in de informatica en wiskunde zijn betrokken, heeft het CWI in 1991 een multidisciplinair programma Multimedia gestart, dat al het CWI-onderzoek op dit gebied bundelt.

Informatiesystemen zullen in toenemende mate multimediaal zijn. Dat wil zeggen dat de informatie beschikbaar is in een geïntegreerde vorm van tekst, beeld en geluid. Door de snelle technische ontwikkelingen en de daarop inhakende reclametechnieken krijgt de gebruiker al gauw het idee dat op dit terrein binnenkort alles mogelijk zal zijn. Niets is echter minder waar. Weliswaar kan men op een PC al bewegende beelden stilzetten, bewerken en in een andere omgeving plaatsen, heeft muziek die is opgewekt via een PC toetsenbord al vaak CD-kwaliteit. Maar de juist door haar snelheid ook ongestructureerde groei van het gebied zorgt in de praktijk nog voor grote problemen. Representatie en betekenis van multimedia data moeten worden ontkoppeld teneinde inhoudelijke bewerkingen te kunnen uitvoeren (voor tekst is dit nauwelijks een probleem). Verder bevat de gangbare programmatuur geen inherente timing-mechanismen. Tenslotte zullen multimediasystemen pas gemeengoed worden als zij aanzienlijk minder omslachtig worden in het gebruik.

Multimedia onderscheidt zich van klassieke vormen van invoer/uitvoer door de gelijktijdige aanwezigheid van een aantal datastromen, waartussen een nauwstekende synchronisatie moet plaatsvinden en die samen één geïntegreerd systeem vormen. Bij dit gelijktijdig en in onderlinge samenhang verwerken van tekst, beeld en geluid doen zich verschillende problemen voor die nog maar zeer ten dele zijn opgelost.

Wat momenteel op de markt beschikbaar is gaat niet verder dan dat bijvoorbeeld bij een stuk tekst een beeld van die tekst (zoals een fax) wordt meegezonden. Kenmerkend is hier de ongestructureerde datastroom. Voor het verkrijgen van de noodzakelijke flexibiliteit in het manipuleren met die data is het nodig om meer controle te krijgen over de inhoud van de datastroom door toevoeging van informatie over de structuur van die data.



Multimedia datastromen en hun synchronisatie worden beschreven in de vorm van data objecten. Een object server verwerkt de objecten volgens de regels van een CMIF document. De CMIF-speler levert het multimedia document af bij de gebruiker.

Deze object-gerichte benadering levert diverse voordelen op: betere foutendetectie/-verbetering, eenvoudiger synchronisatie en efficiëntere gegevensopslag. Een volgende cruciale stap is verband te leggen tussen de inhoud van de datastromen, bijvoorbeeld de toevoeging aan een tekst van gesproken commentaar met ingebouwde betekenis.

Het CWI-onderzoek is gericht op de problemen bij het gebruik van multimedia in een *gespreide, heterogene omgeving*. Dat wil zeggen dat de data en de verwerkingsroutines zijn gespreid over een computernetwerk met onderling verschillende werkstations (afmetingen van het scherm, kleurmogelijkheden, etc.). Het onderzoek is multidisciplinair, met als zwaartepunten het modelleren van complexe data, datamodellen voor gesynchroniseerde datastromen, gebruikersinterfaces, gespreide bedrijfssystemen voor de verdeling van taken in een netwerk, en netwerkprotocollen voor gesynchroniseerde communicatie.

Het door het CWI beoogde systeem voor de opbouw van een multimedia-document in een gespreide, heterogene omgeving kent de volgende fasen:

- Verzameling van data in de vorm van objecten in een database. Zo'n object kan een gescand beeld zijn, maar ook het programma dat zo'n beeld samenstelt.
- Constructie van het document, bestaande uit gestructureerde verwijzingen naar datablokken, inclusief informatie over de synchronisatie tussen blokken.
- Aanwijzingen omtrent de weergave van het document (virtuele presentatie-omgeving).
- Het aanbrengen van filters die de algemene multimedia-gegevens geschikt maken voor een specifiek werkstation.
- Regeling van de gebruikerstoegang tot het document.

Het CWI heeft op vele aan multimedia verwante gebieden in de loop der jaren een grote expertise opgebouwd en vaak een leidende rol gespeeld. Wij noemen hier: gespreide bedrijfssystemen, integratie van computergrafiek en beeldverwerking, en patroonherkenning. Ook de aanwezige kennis van de prestatie-analyse van computersystemen is van belang bij het ontwerpen van multimediastelsels. Een voorbeeld is het onderzoek naar de beheersing van verschillende typen datastromen binnen ISDN-netwerken.

Het CMIF project (CWI Multimedia Interchange Format), gestart in 1991 onder de naam VANGOGH, behelst het ontwikkelen en testen van datamodellen, auteurssoftware en systeemsoftware voor transportabele multimedia presentaties in een heterogene netwerkomgeving. Het eerste model, het Amsterdam Hypermedia Model, vormde de basis voor een prototype auteursstelsel, gebouwd met gebruikmaking van Python, een op het CWI ontwikkelde, geïnterpreteerde taal voor de ontwikkeling van prototypes. Python is hiervoor uitgebreid met diverse algemeen toepasbare multimedia modules. Ervaring met het gebruik van het prototype heeft geleid tot diverse verfijningen in het Amsterdam Hypermedia Model.

MADE - De Europese industrie heeft grote behoefte aan een uniforme aanpak van de multimedia basissoftware. Daarom is in 1992 in het kader van het EG-programma ESPRIT een grootschalig project gestart (MADE = Multimedia Application Development Environment). Doel is de bouw van een object-georiënteerde softwarebasis voor multimediatoepassingen en het verschaffen van programmeergereedschap voor de gebruikers. Het CWI, dat een der belangrijkste partners is in dit onder leiding van de Franse firma Bull staande project, zal het basis object-model ontwikkelen, de database interfaces modelleren en - samen met Bull - zorgen voor de complete software basis en de integratie van multimedia-objecten. Vier deelnemende Europese industrieën zullen de ontwikkelde software als basis gebruiken in hun toepassingen.

Dr. D.C.A. Bulterman, drs. P.J.W. ten Hagen, Multimedia (MR2)
telefoon 020 - 592 4147, 020 - 592 4133

Centrum voor Wiskunde en Informatica
Kruislaan 413

postbus 94079, 1090 GB Amsterdam

telefoon 020 - 592 9333, telefax 020 - 592 4199

september 1993

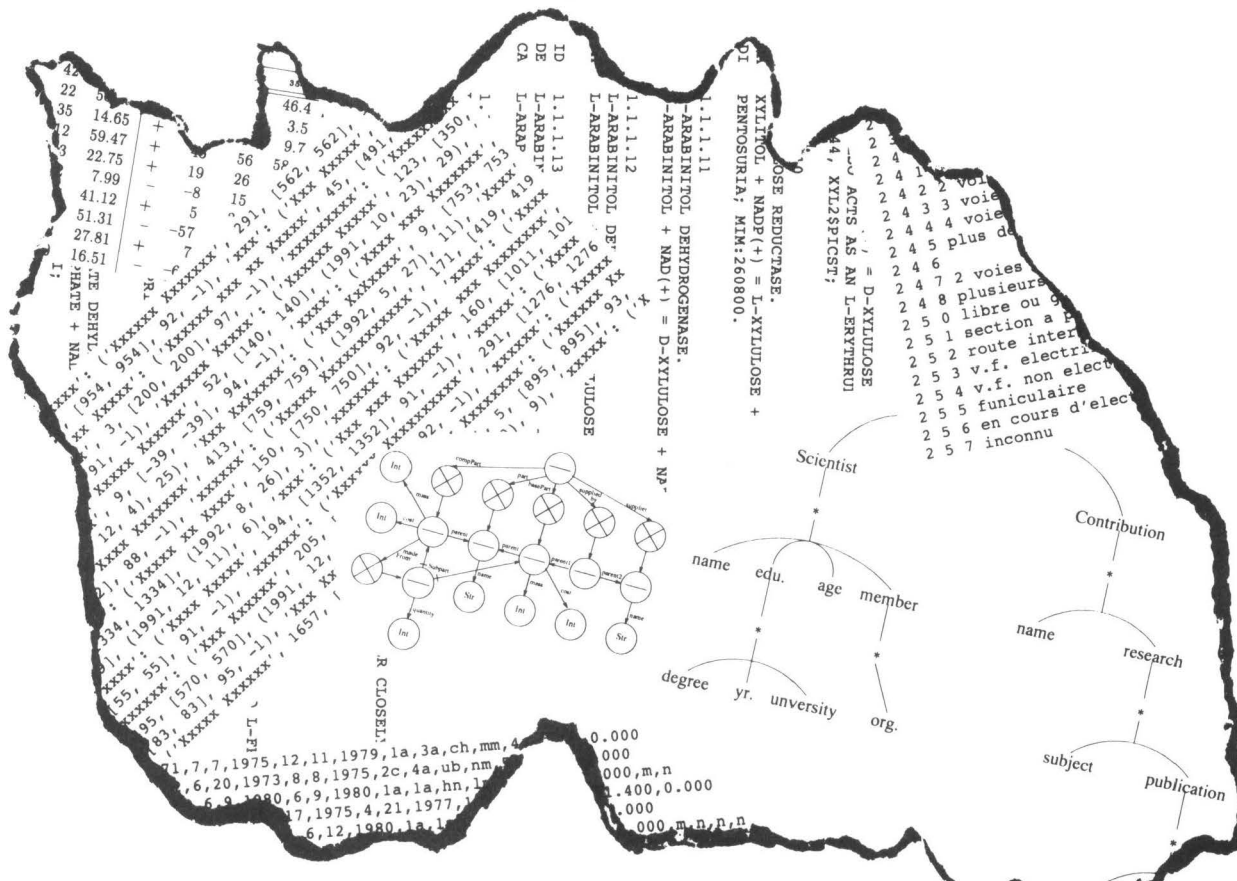
KWALITEIT EN EFFICIËNTIE VAN DATABASE MANAGEMENT SYSTEMEN

Informatiesystemen ter ondersteuning van bedrijfsprocessen of ten behoeve van wetenschappelijk onderzoek zijn onderhevig aan snel wisselende eisen met betrekking tot het gebruik. Dit vereist van deze systemen grote flexibiliteit en betrouwbaarheid. Het CWI levert belangrijke bijdragen aan de studie naar datamodellen en architecturen voor database management systemen (DBMS) geschikt voor parallelle en gespreide computersystemen. Het onderzoek gebeurt zowel in nationaal als in Europees verband.

De huidige DBMS zijn goed opgewassen tegen hun taken in een traditionele, sequentiële computeromgeving. Ook op het terrein van administratieve toepassingen zijn er geen fundamentele technische problemen. Zolang men de database alleen als een grote 'kaartenbak' wil gebruiken zijn de beste beschikbare DBMS efficiënt en hebben een goed prestatieniveau.

Dat wordt anders bij meer geavanceerde toepassingen. DBMS presteren nog onder de maat in bijvoorbeeld een CAD/CAM of een multimedia omgeving. Men weet hier de aanwezige structuur nog niet goed uit te buiten. In de praktijk ontbreekt er in een database vaak informatie, hetgeen tot inconsistenties kan leiden. Hoe een DBMS op een consistente manier met onvolledigheid moet omgaan is nog een open vraag. De hedendaagse gebruiker is niet meer tevreden met 'passieve' databases; hij wil dat het DBMS als het ware met hem meedenkt. Het onderzoek naar actieve databases is nog grotendeels onontgonnen terrein.

Daarbij komt nog dat de computeromgeving waarin een database is ondergebracht tegenwoordig vaak bestaat uit een netwerk van onderling verschillende werkstations. Het onderzoek naar DBMS in een gespreid, heterogeen computersysteem vormt een belangrijk onderdeel van het CWI-onderzoek. Een der aandachtspunten is het bijhouden van consistente kopieën, van belang voor de betrouwbaarheid van het systeem. Ook is het economisch van groot belang om vóórinformatie te hebben over de prestatie van een DBMS in een zo complexe omgeving. Daartoe worden nieuwe testmethoden ontwikkeld.



Een ontwikkeling die eveneens van invloed is op toekomstige DBMS is dat in het komende decennium het interne RAM-geheugen (Random Access Memory) van de computers sterk zal groeien. Deze geheugens zullen een capaciteit in de orde van 1 Gigabyte en een snelheid van meer dan 1000 tps (transactions per second) bereiken en qua prijs moeiteloos kunnen concurreren met schijfgeheugens. Het is dan aanzienlijk voordeliger om gegevens direct in het RAM-geheugen te bewaren, in plaats van op magneetschijf, zoals heel lang gebruikelijk was. Tegelijkertijd zal de snelheid van de gegevensverwerking toenemen door het gebruik van meerdere parallele processoren. Deze nieuwe machine-architectuur stelt nieuwe, hoge eisen aan het DBMS.

Praktijk

Het CWI heeft de afgelopen jaren in een aantal nationale en Europese programma's deelgenomen aan fundamenteel en strategisch onderzoek naar database management systemen.

PYTHAGORAS - Het CWI is coördinator van een grootschalig ESPRIT III project (1992-1995) dat een vroegtijdige kwaliteitsbeoordeling van nieuwe DBMS mogelijk moet maken. Nieuwe systemen vertonen nog vaak constructiefouten en knelpunten in de prestatie die pas in de praktijk aan het licht komen. Een belangrijk onderdeel van PYTHAGORAS is het ontwikkelen van een Software Testpilot die het mogelijk maakt met beperkte inspanning de betrouwbaarheid en kwaliteit van een DBMS te testen. PYTHAGORAS bouwt voort op projecten als PRISMA en TROPICS (zie hieronder). Naast het CWI nemen zeven instellingen in Frankrijk en Engeland deel in PYTHAGORAS.

Goblin - Een DBMS voor toepassingen zoals CAD/CAM, cartografie en kantoorautomatisering moet in staat zijn complexe datastructuren efficiënt te verwerken. Het Goblin-project heeft tot doel de kern van een nieuwe generatie DBMS zo te ontwerpen dat de mogelijkheden voor datacompressie, data-opslag en parallele verwerking maximaal worden benut. In dit project (1990-1993), gefinancierd door de stichting SION, werkt het CWI samen met drie Nederlandse universiteiten.

ISDF - In het kader van het Nationale Faciliteit Informatica-programma wordt gewerkt (1990-1993) aan een raamwerk voor de formele beschrijving van het ontwerpen van informatiesystemen en de analyse van zulke beschrijvingen (ISDF = Integrated Systems Design Framework). Dit project bouwt voort op eerder CWI-onderzoek (1985-1989) naar de formalisering van object-georiënteerde datamodellen. Het onderzoek gebeurt in samenwerking met vier Nederlandse universiteiten.

PRISMA - In opdracht van Philips Natuurkundig Laboratorium en in samenwerking met vier Nederlandse universiteiten is onderzoek verricht (1986-1990) naar een relationeel DBMS dat kan werken op een parallele machine (PRISMA = PaRallel Inference and Storage MAchine). Bij afronding van het project was er een relationeel DBMS met SQL interface ontwikkeld, alsmede een machine met 100 processoren, elk met 4 Mbyte geheugen en gekoppeld aan 50 harde schijven. De aansluitende deelname in het ESPRIT II project TROPICS (1989-1990) was er vooral op gericht om dit DBMS mede geschikt te maken voor cartografische en kantoor-systemen.

Dr. M.L. Kersten, Databases (AA4)
telefoon 020 - 592 4066

*Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199*

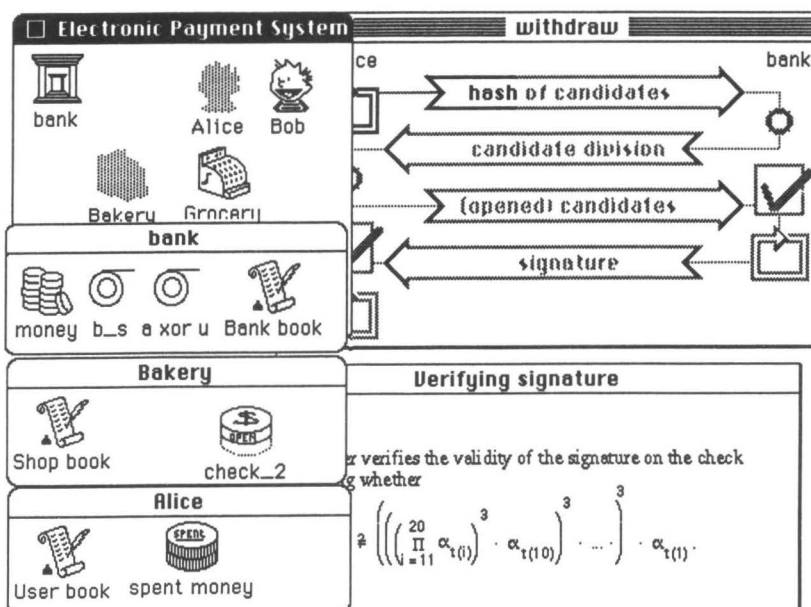
september 1993

CRYPTOLOGIE BESCHERMT ELEKTRONISCH GEGEVENSVERKEER

Tegenwoordig worden grote hoeveelheden gegevens verstuurd over computernetwerken en opgeslagen in (elektronische) gegevensbanken. Deze gegevens bevatten niet alleen technologische en commerciële informatie, maar zijn vaak ook van persoonlijke aard. Misbruik kan worden voorkomen door toepassing van cryptologie. Het cryptologisch onderzoek op het CWI is vooral gericht op de privacy van de gebruiker.

Met de beveiliging van geautomatiseerde systemen (bijvoorbeeld een computernetwerk) zijn belangen van de gebruiker zowel als van de beheerder gemoeid. Veel organisaties beheren grote bestanden met privé-informatie over hun klanten, waartoe die klanten zelf geen toegang hebben, noch het gebruik kunnen controleren. In zo'n situatie is het dan bijvoorbeeld denkbaar dat, als in de nabije toekomst elektronische transactiesystemen met 'smart cards' gemeengoed worden, aan een gebruiker bepaalde faciliteiten worden ontzegd op basis van transacties - bijgehouden in een computer-logboek - die in een totaal andere context plaatsvonden. Bij grootschalige toepassing zou dat een 'Big Brother' maatschappij nabij kunnen brengen. Anderzijds wil men het systeem beschermen tegen bijvoorbeeld geknoei van gebruikers met de besturingsprogrammatuur of tegen het zich als iemand anders voordoen. Gegevensbeherende instanties krijgen het steeds moeilijker met zulke vormen van misbruik. Dit leidt tot strengere veiligheidsmaatregelen, waardoor de privacy van de gebruiker nog verder in het gedrang komt.

Een algemeen heersende opvatting is dat men niet de belangen van beheerders en gebruikers simultaan kan beschermen. Niet zelden wordt daarom de privacy van de gebruikers opgeofferd aan de veiligheid van het systeem voor de beheerder. Dit berust echter op een misvatting. Met behulp van cryptologie kan men systemen ontwerpen die zowel veiligheid als privacy waarborgen.



PC-versie van een elektronisch betalingssysteem, ontwikkeld op het CWI. Rechts het te volgen cryptologisch protocol voor de geldopname van de klant.

Cryptologie is de wetenschap van informatiebeveiliging. Haar werkterrein is de communicatie tussen twee of meer partijen die elkaar niet à priori vertrouwen, zoals een bank en zijn cliënten. Met behulp van cryptologische technieken kunnen opgeslagen of verstuurde gegevens onleesbaar worden gemaakt voor personen die daartoe niet gerechtigd zijn (privacy), en men kan gegevens van een 'digitale handtekening' voorzien (authenticatie). Een sleutelrol is hierbij weggelegd voor het ontwerp van cryptologische protocollen. Dit zijn voorschriften voor de communicatie, berekeningen en vercijferingen van de deelnemers, die zijn bedoeld om hun belangen te beschermen. Hierbij is de inbreng van met name getaltheorie, complexiteitstheorie en discrete wiskunde onmisbaar. Deze protocollen zijn gebaseerd op het idee van een 'eenrichting-functie'. Een voorbeeld is het produkt van twee grote priemgetallen. Vermenigvuldigen is eenvoudig, maar de oorspronkelijke getallen terugvinden uit het produkt is bijna ondoenlijk.

De groep Cryptologie van het CWI - in haar huidige vorm ontstaan in het Orwell-jaar 1984! - heeft zich in de loop der jaren een vooraanstaande positie in de wereld verworven. Er is onder meer onderzoek gedaan naar elektronisch geld, geheime stamschema's, bescherming van bestandsgegevens, digitale groepshandtekeningen, berichten met onbekende en niet op te sporen afzender, en communicatie zonder kennis prijs te geven (zero-knowledge protocollen). Transactiesystemen gebaseerd op bij het CWI ontwikkelde technieken zijn niet alleen fraudebestendig, maar garanderen ook privacy.

Een veelbelovende recente ontwikkeling betreft onderzoek op het CWI naar het gebruik van een soort smart-card in de vorm van een zakcomputertje met ingeplugde 'waarnemers'. In tegenstelling tot andere ontwerpen heeft de gebruiker hier volledige controle over de smart-card. De waarnemer waarborgt de veiligheid van de beheerders en de zakcomputer van de gebruiker zijn privacy. De maatschappelijk snel stijgende interesse voor dit soort onderzoek blijkt onder meer uit het verschijnen in de Scientific American van een artikel van D. Chaum, leider van de CWI-groep ('Achieving Electronic Privacy', augustus 1992, pags. 96-101).

Praktijk

De groep Cryptologie heeft zich onder andere met de volgende projecten beziggehouden:

Rijkswaterstaat:

In opdracht van Rijkswaterstaat zijn voor het rekeningrijden-project de in aanmerking komende elektronische betalingssystemen gekarakteriseerd en vergeleken.

DigiCash:

Uit de groep Cryptologie van het CWI is het bedrijf DigiCash voortgekomen, dat zich bezighoudt met de ontwikkeling en implementatie van elektronische betalingssystemen.

Europese programma's:

In het kader van het EG-programma RACE, was het CWI in de periode 1989-1992 hoofdaannemer van het project RIPE (RACE Integrity Primitive Evaluation). Doel van het project was het evalueren van cryptologische beveiligingsmethoden voor gebruik in EBC (European Broadband Communication). In het ESPRIT-project CAFE (Conditional Access For Europe) ontwikkelen onder leiding van het CWI twaalf partners uit zeven landen een geavanceerd Europees elektronisch betaalmiddel met zakcomputers.

Dr. D. Chaum, Cryptologie (AA2)
telefoon 020 - 592 4169

*Centrum voor Wiskunde en Informatica
Kruislaan 413
Postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199*

september 1993

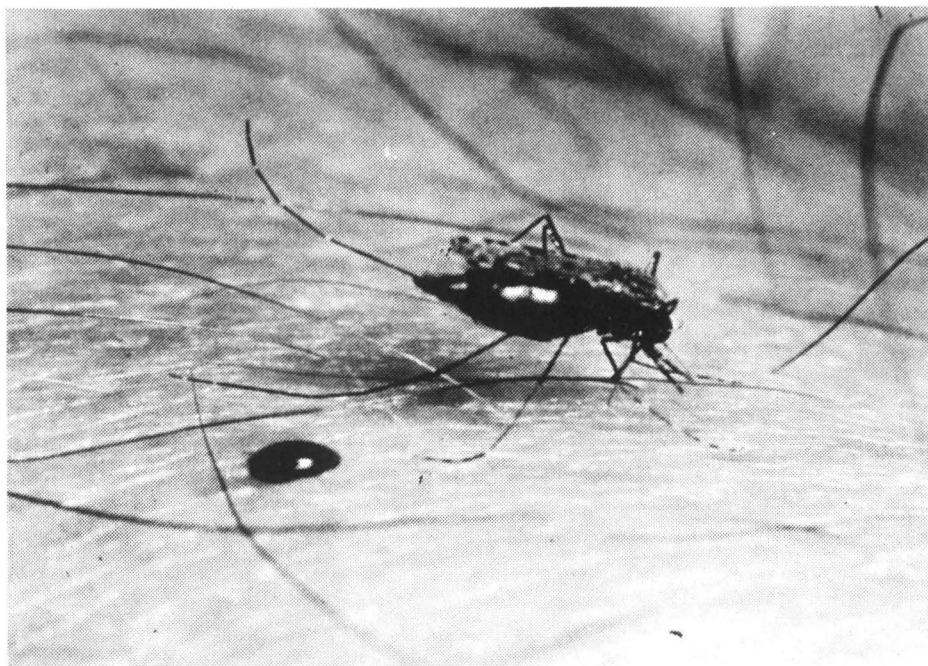
EPIDEMIEËN WISKUNDIG BESTREDEN

Wat is de beste manier om verspreiding van een besmettelijke ziekte te verhinderen? Om daar achter te komen is het nodig een realistisch wiskundig model te maken van de ontwikkeling van zo'n ziekte binnen een populatie. Verschillen tussen individuen blijken daarbij belangrijk te zijn. Op het CWI bestudeert men in het bijzonder de dynamica van gestructureerde populaties. Het onderzoek is theoretisch, maar er zijn diverse raakvlakken met de praktijk.

Wetenschappelijk onderzoek naar de effecten van externe invloeden op een gegeven populatie van mensen, dieren of planten is van groot praktisch belang. Denk bijvoorbeeld aan de invloed van schadelijke stoffen, het optreden van plagen of de verspreiding van besmettelijke ziekten. Meestal is experimenteren niet goed mogelijk vanwege de hoge kosten, de grote hoeveelheid werk of uit ethische overwegingen. Het werken met wiskundige modellen kan dan uitkomst brengen.

In de natuur vertoont elke populatie een bepaalde fysiologische structuur: individuen verschillen in kenmerken als leeftijd, grootte, seksueel gedrag, vatbaarheid voor een besmettelijke ziekte, etc. Tot voor kort werkten ecologen en epidemiologen veelal met modellen waarin alleen de *gemiddelde* eigenschappen van de individuen in een populatie zijn verwerkt. In tal van gevallen, bijvoorbeeld als men wil weten of de introductie van een ziekteverwekker tot een epidemie zal leiden, is dit niet de juiste methode van middelen en heeft men gestructureerde modellen nodig, waarbij met onderlinge verschillen van de individuen wordt rekening gehouden. Een tweede argument voor gestructureerde modellen is dat, vooral ook in reactie op veranderende omstandigheden in de leefomgeving, de gemiddelde eigenschappen behoorlijk kunnen variëren in de loop van de tijd.

In het onderzoeksprogramma Mathematische Modelling en Analyse op het CWI bestudeert men de dynamica van gestructureerde populaties. De wiskundigen van het CWI werken daarbij nauw samen met biologen, speciaal met het Instituut voor Theoretische Biologie van de Rijksuniversiteit Leiden. Bij de modellering van een gestructureerde populatie is het belangrijk de juiste variabelen te kiezen. Watervlooien bijvoorbeeld planten zich pas voort als ze een bepaalde grootte hebben. Het bereiken van die grootte hangt niet af van de leeftijd, maar wel van het voedselaanbod. Hier is dan 'grootte' het relevante kenmerk van de individuen, terwijl de leefomgeving wordt gekenmerkt door het voedselaanbod. Bij de beschrijving van de verspreiding van een ziekte als de mazelen daarentegen is de leeftijd een belangrijke variabele ter onderscheiding van de individuen.



Malariamuskiet zuigt zich overvol (overtollige bloeddrupeer aan de achterkant). Zo wordt de malariaparasiet overgedragen. Met behulp van wiskundige modellen wordt op het CWI de verspreiding van besmettelijke ziekten bestudeerd. Foto: H.J. van der Kaay, RU Leiden.

In gestructureerde modellen wordt verband gelegd tussen de eigenschappen van de individuen en het gedrag van de populatie als geheel. De vergelijkingen die de ontwikkeling van de populatie beschrijven, worden verkregen door eenvoudige boekhouding: tellen hoeveel individuen er in een bepaalde toestand zijn en de veranderingen in die hoeveelheden bepalen aan de hand van formules die de oorzaken van die veranderingen beschrijven. De resulterende vergelijkingen zijn tamelijk ingewikkeld, en vanuit wiskundig oogpunt nog grotendeels onontgonnen terrein. (Voor de kenners: het gaat om eerste orde niet-lineaire partiële functionaal-differentiaalvergelijkingen, die oneindig-dimensionale dynamische systemen beschrijven.)

Naast de theoretische studie van dit type vergelijkingen heeft de CWI-groep, in nauwe samenwerking met biologen, veel aandacht besteed aan onderzoek dat direct verband houdt met de praktijk. Enkele recente activiteiten van de groep zijn:

R_0 - Het drempelgetal R_0 , dat het gemiddeld aantal nieuwe gevallen van een ziekte aangeeft dat wordt veroorzaakt door één besmettelijk persoon, speelt een sleutelrol in de wiskundige epidemiologie ($R_0 > 1$ betekent een epidemie). Op het CWI is, in samenwerking met de Rijksuniversiteit Leiden, een theorie ontwikkeld waarmee R_0 kan worden gedefinieerd en uitgerekend voor gestructureerde populaties. Deze theorie is toegepast op enkele praktijkgevallen, waaronder de verspreiding van AIDS onder homoseksuelen bij eventuele aanwezigheid van een tweede seksueel overgedragen ziekte, die de besmettingskans sterk beïnvloedt.

Varkensziekten - In opdracht van het Centraal Diergeneeskundig Instituut (CDI) in Lelystad doet het CWI onderzoek naar de verspreiding van de ziekte van Aujeszky op varkensfokkerijen. Met behulp van bovengenoemde theorie wordt nagegaan welke vaccinatiestrategie en welke organisatie van de fokkerijen, zowel intern als regionaal, zullen leiden tot het uitsterven van de ziekte.

Niet-lineaire systemen - Het breed opgezette Prioriteitsprogramma Niet-lineaire Systemen van NWO (1990-1998), gecoördineerd door O. Diekmann (CWI/RU Leiden) en anderen, omvat ook onderzoek op het terrein van de populatiedynamica. Zo maakt het CWI, in samenwerking met de vakgroep Fundamentele en Toegepaste Oecologie van de Universiteit van Amsterdam, modellen voor de interactie van spintmijten en roofmijten in een veelheid van lokale kolonies (onder meer van belang bij de biologische bestrijding van spintmijtplagen in kassen). In dit kader wordt ook gewerkt aan de opbouw van een 'Dynamisch Systeem Laboratorium'.

SCIENCE - Samen met zeven andere Europese instellingen neemt het CWI deel in een Europees SCIENCE programma ter bevordering van de onderlinge contacten op het terrein van evolutie-systemen, in het bijzonder deterministische en stochastische evolutievergelijkingen, regeltheorie en mathematische biologie (1990-1993).

ESF - De CWI-groep maakt deel uit van het European Science Foundation Network 'Dynamics of Complex Systems in Bio-Sciences' dat de Europese samenwerking op dit gebied versterkt door het organiseren van workshops.

Prof.dr. O. Diekmann, Mathematische Modelling en Analyse (AM3)
telefoon 020 - 592 4208 (CWI) of 071 - 27 4912 (RU Leiden)

Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020 - 592 9333, telefax 020 - 592 4199

september 1993

VOLGORDEPROBLEMEN KOMEN OVERAL VOOR

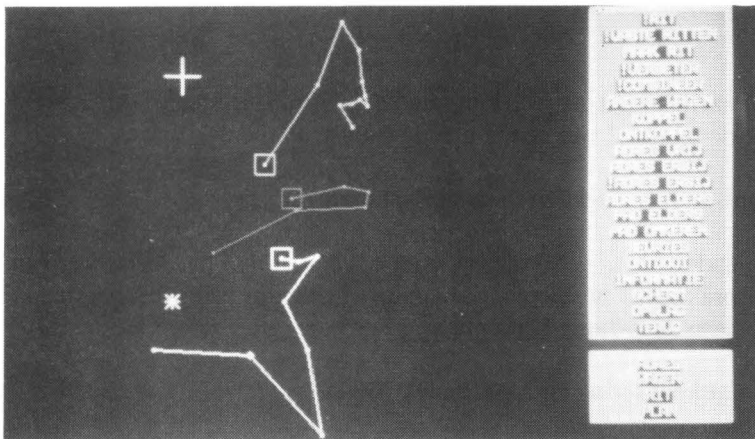
In de praktijk doen zich vaak problemen voor die betrekking hebben op het bepalen van de beste volgorde van een aantal taken of het maken van de beste keuze van produktiemiddelen. Voorbeelden zijn het vaststellen van vestigingsplaatsen van een bedrijf, het opstellen van produktieschema's, roosters en 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.

De groep Combinatorische Optimalisering en Algoritmiek 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 besturen 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 1000 'steden' worden opgelost. Bovendien heeft het onderzoek verschillende nieuwe wiskundige technieken opgeleverd, die toepasbaar blijken bij vele verwante problemen.



CAR (Computer Aided Routing) is een interactief software-pakket dat door het CWI is ontwikkeld als hulpmiddel bij de fysieke distributie. Ontwerp en ontwikkeling gebeurden in samenwerking met Van Gend & Loos.

De onderzoekers van de groep Combinatorische Optimalisering en Algoritmiek maken gebruik van een aantal van deze technieken, zoals optimaliserende algoritmen voor onderdelen van problemen en benaderingsalgoritmen of 'heuristieken' voor grote problemen (bijvoorbeeld een verkort aftelproces). Deze algoritmen lenen zich goed voor praktische vraagstukken als machinevolgordeproblemen of het 'schedulen' van programma's op computers die werken met parallelle processoren, meetkundige methoden afkomstig uit de lineaire programmering met toepassingen bij VLSI-ontwerp, patroonherkenning en robotiek.

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 ondertussen het oplossingsproces -interactief- kan blijven sturen met de computer als hulpmiddel.

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

- Voor **Van Gend & Loos** is een beslissingsondersteunend systeem ontwikkeld voor de routing van hangend confectievervoer (CAR = Computer Aided Routing). Het vervult alle functies, van kladblok en geheugensteuntje tot en met het genereren van volledige planningen. Ten tijde van de ontwikkeling (1984-1988) was nog geen enkel softwarehuis in staat om een dergelijk systeem te maken.
- Voor **ECT/Nedlloyd** is een interactief planningssysteem gemaakt voor het wereldwijd of regionaal beheer van containers, waarbij computers ter ondersteuning van plannersdeskundigen zijn ingeschakeld.
- In het kader van een **SPIN**-project, het overheidsprogramma op het terrein van fundamenteel onderzoek in de informatica, zijn methoden geanalyseerd en ontworpen voor de 'scheduling' van parallelle computers (ParTool).
- In samenwerking met het **TNO-Vezelinstituut** is een interactief planningssysteem ontwikkeld (KLIPP) voor de productieplanning in de naaizaal van een confectie-industrie.

Daarnaast zijn voor verschillende organisaties roosters en personeelsplanningen opgesteld.

De onderzoekers van het CWI hebben zodoende 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.

Prof.dr. A. Schrijver, Combinatorische Optimalisering en Algoritmiek (BS1)
telefoon 020-592 4087

Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199

september 1993

INTELLIGENT REGELEN KAN NIET ZONDER WISKUNDIGE ONDERSTEUNING

Van een rol papier is het gewicht per oppervlakte-eenheid een belangrijke maat voor de kwaliteit. Dat gewicht fluctueert altijd een beetje. De spreiding van het gewicht rond het gemiddelde (de variantie) is daarom een tweede kwaliteitsmaat. Bij het regelen van de productie komt het er daarom op aan deze spreiding zo klein mogelijk te maken en te houden. Variantie-minimalisering is een veel voorkomend probleem in de procesindustrie.

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. Zonder deze kennis is het bijvoorbeeld niet mogelijk om een robotarm een schroef te laten oppakken en die vervolgens in een plaat te laten draaien, of een korte-termijn voorspelling te doen van de afname van elektrische energie of van de toename van de luchtvervuiling binnen een bepaalde periode.

Deze en andere problemen worden op het CWI aangepakt op de afdeling Besliskunde, Statistiek en Systeemtheorie, met name door de onderzoeksgroep Systeem- en Regeltheorie. Enkele andere voorbeelden van regelproblemen zijn: het besturen van schepen, de regeling van het autoverkeer via het geven van signalen aan de bestuurders en de regeling van een chemisch proces volgens een temperatuurpad. Signaalverwerkingsproblemen zijn bijvoorbeeld: de korte-termijn voorspelling van luchtverontreinigingsconcentraties (voor het nemen van adequate maatregelen) en de schatting van de dikte en de eigenschappen van lagen in de aardkorst voor het opsporen van mineralen. Op het CWI is vooral kennis opgebouwd van stochastische systemen (wiskundige modellen voor verschijnselen met onzekerheid) en lineaire processen 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 te beïnvloeden zijn afhankelijk van de beoogde regeling. Het heeft ook uitgangen: bepaalde variabele waarden die veranderen afhankelijk van het ingangssignaal. Bovendien bevat het model een aantal toestandsvergelijkingen. Het ideaal is dat een model de werkelijkheid zo dicht mogelijk benadert en tegelijkertijd zo eenvoudig mogelijk van opzet is.

Afhankelijk van het probleem worden regeldoelen geformuleerd zoals: een korte responstijd, stabiliteit, minimalisering van regelenergie, robuustheid en dergelijke. Omdat het niet mogelijk is om aan al deze regeldoelen in gelijke mate te voldoen, is een afweging nodig. Die afweging wordt bijvoorbeeld gemaakt met behulp van optimale regeltheorie door het minimaliseren van kosten.



Uitgaande van een model voor de stroming van vloeistoffen ontwikkelde het CWI, in samenwerking met het Ministerie van Verkeer en Waterstaat, algoritmen voor de beheersing van verkeersstromen.

Voor de oplossing van een regelprobleem wordt een regelwet opgesteld (ook wel regelaar genoemd), gebaseerd op het terugkoppelingsprincipe: het verschil tussen het actuele uitgangssignaal en het gewenste uitgangssignaal wordt gebruikt om het ingangssignaal zodanig aan te passen dat dit verschil wordt verkleind. Tenslotte wordt de regelaar in de praktijk getest.

De oplossing van een signaalverwerkingsprobleem begint eveneens met het maken een dynamisch model. Voor het schatten, of het voorspellen van een uitgangssignaal wordt vervolgens een filteralgoritme ontworpen en uitgebreid getest met behulp van de door de potentiële gebruiker geleverde praktijkgegevens. Een voorbeeld is het voorspellen van luchtverontreinigingsconcentraties op korte termijn, bijvoorbeeld van zwaveldioxyde in het Rijnmondgebied voor een periode van 12 tot 24 uur. De concentratiegegevens worden in een landelijk netwerk verzameld. In combinatie met de weersverwachting levert het model dan een voorspelling waarop actie kan volgen.

Praktijk

De groep Systeem- en Regeltheorie heeft de afgelopen jaren vrij veel ervaring opgedaan met toegepast en toepassingsgericht onderzoek:

Rijkswaterstaat: In samenwerking met de Dienst Verkeerskunde is onderzoek gedaan naar het effect van adviessnelheden op het verkeersgedrag. Het bleek dat bij hoge verkeersdichtheden de verkeersstroom werd bevorderd door informatie te geven via het verkeerssignaleringssysteem. Het regelprobleem bestond uit de bepaling van de verkeersdichtheid bij welke de adviessnelheid op de matrixborden moet worden getoond. Voor dit probleem hebben wij een model opgesteld en een regelaar ontworpen. Een door Rijkswaterstaat nader uitgewerkte regelaar werd in 1992 uitgetest op de A2 tussen Utrecht en Amsterdam.

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. De CWI-groep heeft fundamenteel onderzoek verricht naar toelatingsregelingen voor communicatiesystemen. Voor specifieke problemen ontwerpt en analyseert zij gepaste regelalgoritmen.

Nederlandse Spoorwegen: De groep heeft een korte termijn voorspellingsalgoritme opgesteld voor de afname van elektrische energie bij de onderstations van de spoorwegen. Piekbelasting is namelijk heel duur en met behulp van deze voorspellingen is het mogelijk om te besparen op energie door, voorafgaand aan piekperioden, energie op te slaan en die vervolgens te gebruiken om pieken af te vlakken.

Prof.dr.ir. J.H. van Schuppen, Systeem- en Regeltheorie (BS3)
telefoon 020 - 592 4085

*Centrum voor Wiskunde en Informatica
Kruislaan 413
postbus 94079, 1090 GB Amsterdam
telefoon 020-592 9333, telefax 020-592 4199*

september 1993

Deelnemers 'CWI in bedrijf' - 8 oktober 1993

Anthony	S.	Rijkswaterstaat/Dir. Noord-Holland
Baaten	L.P.W.	RIKS
Baayen	P.C.	Directie CWI
Bakker	J.W. de	CWI
Bartelds	G.	NLR
Beeks	A.J.	KLM
Beer	A. de	SHELL
Belderbos	C.N.M.	TNO-Defensieonderzoek
Berkhoff	J.C.W.	ECN
Biesboer	F.	Tijdschrift Zeno
Bijlsma	J.	NNI/NEC
Boesveld	A.	PTT Nederland
Boot	J.L.J.	KNMI
Boxma	O.J.	CWI
Brouwer	M.W.	CWI
Bruins	J.	Ministerie van Economische Zaken
Bunje	A.de	PHILIPS Natlab.
Cabo	P.G.	Rijksuniversiteit Groningen
Chanowski	M.M.	MediaCab BV
Clercq	J.C. le	COSSO
Coehoorn	D.J.	Transferpunt Vrije Universiteit Amsterdam
Cuijlenborg	R.H. van	Hollandse Signaalapparaten
Dasselaar	M.R.	SENER
Diekmann	O.	CWI
Dillo	I.G.	Ministerie van O & W
Dits	H.P.	Nederlands Forum voor Techniek en Wetenschap
Drazen	P.J.	RIKS
Duinker	W.	ING Bank
Eck	A.A.	Tulip Computers Int.
Ehrhardt	J.J.	PAO-Informatica
Everaars	C.Th.	CWI
Feijs	L.M.G.	PHILIPS
Gaemers	K.J.F.	NIKHEF-H
Gastel	L. van	CAN
Geise	J.B.J.	IBM Nederland
Goosens	F.A.L.M.	SARA
Goudsbloem	F.J.G.	CWI
Griffin	P.	CWI
Hagen	P.J.W. ten	CWI
Hantke	T.	CWI
Hazewinkel	M.	CWI
Heck	A.	CWI
Heideman	J.J.H.	CONVEX Computer BV
Hemker	P.W.	CWI
Hendriks	P.R.H.	SERC
Hirdes	F.P.	TechForce BV
Hirschfeld	R.	CWI
Hoeve	J. ten	St. Coördinatie Maritiem Onderzoek (CMO)
Holsheimer	M.	CWI
Hoorn	M. van	Flax Technology
Houwen	P.J. van der	CWI
Huijbregts	J.M.	Ministerie van Economische Zaken
Ikink	H.	Journalist
Jansen	A.J.	CWI

Jong	M.T. de	STW - Stichting voor de Technische Wetenschappen
Kampfraath	A.A.	Emiritus hoogleraar
Kersten	M.L.	CWI
Kessler	W.J.A.	SENER/CISB
Kester	J.A.T.G. van	Stichting Cadans
Klint	P.	CWI
Kokosky Deforchaux	P.T.A.	Stichting SURF
Koning	N.	Rabobank Nederland
Kos	N.J.	NWO-GBE
Kramer	Ch.	VNU Business Publications (Hoofdredacteur)
Kruithof	H.	Technische Universiteit Delft
Kuperus	M.	NWO-GBE (voorzitter)
Kwakkel	F.	CWI
Liere	R. van	CWI
Lindijer	G.J.H.	SARA - Stichting Academisch Rekencentrum Amsterdam
Loon	M. van	CWI
Lut	H.J.A.	Assist Multimedia B.V.
Machielse	W.J.M.	Datatraffic BV
Meijs	C.	Landbouw Universiteit Wageningen
Mettrop	M.W.	CWI
Meulen	G.J. van der	Wiener Telecommunication Systems
Miltenburg	P.G.M.	Rijkswaterstaat/Vervoer & Leefbaarheid
Molenaar	J.	Technische Universiteit Eindhoven
Mom	P.A.M.	Journalist
Mullender	K.S.	CWI
Mynett	A.E.	Waterloorkundig Laboratorium
Neessen	J.T.A.	TNO IT&T initiatief
Nieland	H.M.	CWI
Niesten	P.L.J.P.	ABN AMRO Bank
Nieuwland	G.Y.	SMC
Niewind	A.C.	Ministerie van O&W/OWB/IZ
Noot	H.	CWI
Offeyran	A.	Digital Equipment
Okx	J.P.	TAUW Infra Consult
Ooms	M.J.S.	Directie Materieel Koninklijke Marine
Oortmerssen	G. van	Directie CWI
Op den Brouw	J.	Ministerie O&W/OWB/IZ
Os	A.G. van	Waterloorkundig Laboratorium
Overboom	G.K.	SHELL Research BV
Paassen	A.C. van	EG-Liaison
Pemberton	S.	CWI
Philippo	A.	STW - Stichting voor de Technische Wetenschappen
Pool	J.C.	Artifex Information Systems BV
Raat	J.	St. Coördinatie Maritiem Onderzoek (CMO)
Ree	M. van	Creative Graphics
Riele	H.J.J. te	CWI
Rienstra	S.W.	Technische Universiteit Eindhoven
Rinnooy Kan	A.H.G.	VNO
Rixon	S.	KLM/Automatisering
Roebbers	H.W.	Universiteit Twente/Regeltechnisch Laboratorium
Romeijn	E.F.	SENER
Roodzant	M.	ACE
Roos	F.A.	CWI
Rossum	G. van	CWI
Sanders	J.A.	CWI
Schelleman	A.A.	Computer Business Applications
Schippers	F.H.	DR&D
Schuppen	J.H. van	CWI

Sevenster	A.	Elsevier Science Publishers
Shair-ali	S.	IBM-Uithoorn
Siebes	A.P.J.M.	CWI
Sips	H.J.	Technische Universiteit Delft
Slagmolen	M.H.	COSSO
Sluis	A. van der	SMC
Snijders	F.A.M.	CWI
Spekreijse	S.P.	NLR
Sprij	W.K.	SION - Stichting Informatica Onderzoek Nederland
Steenbrink	J.H.M.	Katholieke Universiteit Nijmegen
Steenge	R.J.	KLM
Stijn	Th.L. van	Rijkswaterstaat/Dienst Getijdewateren
Stork	F.C.	Cray Research
Stortelder	W.	CWI
Sunter	J.P.E.	Universiteit Twente/Regeltechnisch Laboratorium
Taale	H.	Rijkswaterstaat
Tax	A.A.M.	Katholieke Universiteit Nijmegen
Temme	N.M.	CWI
Tindemans	P.A.J.	Ministerie van O&W
Vaandrager	F.W.	CWI
Vasbinder	J.W.	Consultium
Verboom	G.K.	Waterloopkundig Laboratorium
Vernimmen	E.J.B.	Kramers en Ruys
Verwer	J.	CWI
Vlasblom	G.	Cap Volmac
Vries	P.J. de	Twijnstra Gudde
Wapenaar	W.P.	PTT Telecom/Kabel- en Radioverbindingen
Weiss	P.	NLR
Werkhoven	L.D.C. van	EG-Liaison
Wielinga	R.F.	SENER
Wiener	R.F.	Wiener Telecommunication Systems
Wiggers	L.W.	NIKHEF-H
Willems	H.	NINT/NCWT
Wolters	J.A.M.	IBM Nederland



TECHNOLOGIE OVERDRACHT

8 oktober 1993

CWI, Kruislaan 413, 1098 SJ Amsterdam

Onder dit thema organiseert het CWI op vrijdag 8 oktober a.s.
haar jaarlijkse manifestatie:

CWI IN BEDRIJF

Het thema zal uit algemene hoek belicht worden door vertegenwoordigers van overheid, bedrijfsleven en onderzoek.

Daarnaast wordt CWI onderzoek op een aantal gebieden gepresenteerd in de vorm van voordrachten om daarmee ook concreet een bijdrage te leveren aan de overdracht van resultaten van onderzoek naar toepassingen.

De gehele dag door zullen demonstraties van lopend onderzoek gegeven worden.

INLEIDINGEN

A. Rinnooy Kan, VNO
G. van Oortmerssen, CWI
P.A.J. Tindemans, Ministerie van O&W
M.H. Slagmolen, COSSO

ONDERZOEKSPRESENTATIES

Software Verificatie
Cryptografie
Aktieve databases
Multimedia

DEMONSTRATIES

Testen van software, systeem- en regeltheorie, computer-algebra, visualisatie van wetenschappelijke gegevens, dynamische systemen, multimedia, compiler-constructie, etc.

Voor nadere informatie en indien u de definitieve programma gegevens wilt ontvangen kunt u contact opnemen met:

CWI, Margriet Brouwer, Postbus 4079, 1009 AB Amsterdam

Telefax (020) 592 4199 / Telefoon (020) 592 4253 / E-mail margriet@cw.nl