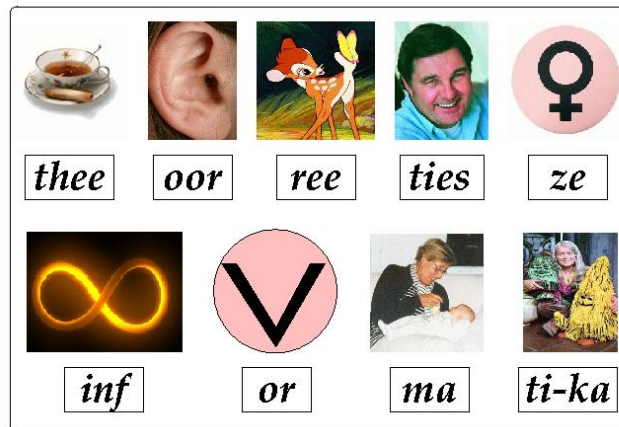


Thee Oor Ree Ties Ze Inf Or Ma Ti-ka: Deze Tijd Vraagt om Verificatie van Software

Wan Fokkink

6 maart 2007



Mijnheer de rector magnificus, dames en heren,

Ook op de universiteit zijn we er tegenwoordig van doordrongen dat PR een zeer belangrijke zaak is. De naam van een opleiding blijkt vaak belangrijker dan de inhoud ervan, als het gaat om het trekken van grote aantallen studenten. Ik heb, met deze les in het achterhoofd, getracht familie en vrienden naar mijn oratie te lokken, en daarbij verschillende aankondigingen rondgestuurd. Velen van u verwachten nu ten onrechte een voordracht onder de titel

Computers, Drugs en Rock & Roll

En de leden van mijn schaakclub Paul Keres zullen zich ondertussen wel realiseren dat de titel

Kunnen Computers Schaken ?

niet op waarheid berust. Hopelijk zult u mij dit niet al te kwalijk nemen, en de komende 45 minuten desalniettemin kunnen waarderen. De echte titel van mijn rede luidt

*Thee Oor Ree Ties Ze Inf Or Ma Ti-ka:
Deze Tijd heeft Behoeftē aan Verificatie van Software*

Deze titel is gebaseerd op een serie reclame-slogans van de VU, enkele jaren geleden, waarin een leesplankje figureerde tezamen met de leus “deze tijd heeft behoefte aan”.

In feite is een inaugurele rede een onmogelijke spagaat. Aan de ene kant is het de bedoeling om in de breedte, maar ook in de diepte, mijn visie te geven op de belangrijkste huidige en toekomstige ontwikkelingen in mijn vakgebied. Aan de andere kant varieert het publiek van naaste collega’s tot familie en vrienden. Gelukkig bleken Fokke en Sukke alsmede prinses Máxima bereid om op de slides te figureren. Hopelijk biedt mijn rede daardoor voor elk wat wils.

Is Informatica een Wetenschap ?

Allereerst wil ik graag ingaan op de fundamentele vraag of informatica een wetenschap is. De buitenwereld, en daar horen wetenschappers uit andere vakgebieden bij, heeft er grote moeite mee om informatica te zien als een wetenschappelijke discipline. Ze ziet de computer als een gebruiksvoorwerp, te vergelijken met een stofzuiger of een TV. Bij informatica denkt men aan een computer, beeldscherm, toetsenbord, printer en snoeren. Hiermee zou het belang van ons onderzoek zich beperken tot een storende kabel, een harde schijf, of de houdbaarheidsdatum van een programmeertaal. Nog afgezien van het feit dat één programmeur meer kan schrijven dan tien informatici kunnen doorgronden.

Mijn leerstoel heet, zoals in de echte titel van deze rede is verwerkt, Theoretische Informatica. Nu het steeds belangrijker wordt gevonden dat wetenschappelijke resultaten direct toepasbaar zijn in de industrie, is Theoretische Informatica bijna een geuzennaam geworden. Want wat is nou de theorie die ten grondslag ligt aan een gebruiksvoorwerp als een computer?

Het draait om drie centrale begrippen: informatie, berekening en communicatie. De computer is in staat om met enorme snelheid gigantische hoeveelheden data te verwerken. Het is echter aan de mens om de rekenregels voor de computer vast te leggen. Daarbij kan een imperatieve programmeertaal worden gebruikt, maar we kunnen bijvoorbeeld ook de rekenregels van onze hersencellen of evolutionaire principes als uitgangspunt nemen. Verder kunnen berekeningen gedistribueerd worden uitgevoerd, wat wil zeggen dat verschillende computers of processoren verschillende delen van de berekening voor hun rekening nemen. Tijdens deze berekeningen communiceren de computers onderling om hun deelresultaten aan elkaar door te geven.

Al deze zaken geven aanleiding tot moeilijke, vaak wiskundige problemen. Hoe kun je snel zoeken in enorme hoeveelheden data? Wat is het beste berekeningsmodel om een

gegeven probleem op te lossen? Heeft een stuk software het juiste gedrag? En hoe kunnen we programma's die op verschillende computers worden uitgevoerd goed en efficiënt laten samenwerken? Maar ook, hoe maak je software van hoge kwaliteit met een team van honderd man? Of, hoe kunnen computers op een goede manier in het bedrijfsproces geïntegreerd worden? Al deze vragen zijn niet alleen wetenschappelijk zeer uitdagend, maar hebben ook, zoals we allemaal ervaren, grote invloed op ons dagelijks leven. Informatica is overal: onzichtbare embedded systemen hebben onze samenleving massaal gepenetreerd, communiceren draadloos met elkaar, en dienen zich vaak zelfstandig te organiseren. Dit vereist onderzoek, veel onderzoek. Ik durf daarom te beweren dat informatica niet alleen een wetenschap is, maar sterker nog, één van de belangrijkste wetenschappen van deze eeuw zal blijken te zijn.

Mooie Modellen

Waarom heeft informatica dan toch zo'n moeite met zijn beeldvorming naar buiten? Ten dele komt dit omdat het een relatief nieuw vakgebied betreft, dat tegelijkertijd zeer divers is. Er zijn raakvlakken met bijvoorbeeld electronica, bedrijfskunde, wiskunde en natuurkunde (denk aan nano-technologie), maar ook met psychologie (in de vorm van mens-machine interactie, oftewel, hoe gaat een mens om met een computer) en met biologie (bioinformatica is een combinatie van informatica en biologie waar ik straks meer over zal zeggen). Helaas hebben die verschillende disciplines binnen de informatica onderling te weinig waardering voor elkaar, zodat we niet alleen versnipperd zijn, maar ook nog eens geen front vormen. Hopelijk krijgt het nog niet zo lang geleden opgerichte Informatica Platform Nederland de kans om zich te ontwikkelen tot de broodnodige spreekbuis van de Nederlandse informatica-onderzoekers.

Echter, het belangrijkste probleem voor de beeldvorming is dat andere exacte wetenschappen, in tegenstelling tot de informatica, wel met mooie modellen van de werkelijkheid worden geassocieerd. Bij de natuurkunde dienen modellen ons universum zo dicht mogelijk te benaderen. De scheikunde draait om moleculen. En de wiskunde houdt zich bezig met een handvol modellen die allemaal eeuwigheidswaarde hebben, zoals de natuurlijke getallen. Voor de leek zijn al die modellen veel aantrekkelijker dan de printers en snoeren waarmee informatica wordt vereenzelvigd. Zo is er bij de Nationale Wetenschapsquiz nog nooit één informatica-vraag gesteld, afgezien van een historische, terwijl het wemelt van natuurkunde-, scheikunde- en wiskunde-vragen.

Echter, ook aan de informatica liggen modellen met een universeel karakter ten grondslag. Alan Turing formuleerde in 1936 de Turing-machine, bestaande uit een oneindige tape met nullen en enen, en een machientje dat over de tape loopt en daarop nullen en enen kan overschrijven. Turing-machines hebben dezelfde expressieve kracht als zelfs de meest geavanceerde programmeertalen. Derhalve kunnen fundamentele vraagstukken in de informatica, over expressiviteit en complexiteit, bestudeerd worden op het nivo van Turing-

machines.

Noam Chomsky, een wereldberoemde Amerikaanse linguïst, bestudeerde in de jaren '50 de (minder expressieve) klassen van finite-state machines en van pushdown automaten. Een finite-state machine beschrijft een eindige toestandsruimte. Bij een pushdown automaat hebben de toestanden daarbij ook nog een onbegrensd geheugen. Chomsky had als doel natuurlijke taal beter te begrijpen, maar finite-state machines en pushdown automaten bleken ook uitstekend geschikt om bijvoorbeeld lexicale analyzers voor programmeertalen te beschrijven, alsmede hardware-circuits. Bovendien werden ze in de jaren '60 gebruikt om softwaresystemen te specificeren en te analyseren.

Finite-state machines bleken uiteindelijk echter niet rijk genoeg om gedistribueerde systemen tot in detail te bestuderen. Ook het gebrek aan algebraïsche structuur bleek een serieuze beperking. De Britten Tony Hoare en Robin Milner ontwikkelden daarom in de jaren '70 zogenaamde procesalgebra's om systeemgedrag formeel te beschrijven. (Zij kregen mede voor dit werk in respectievelijk 1980 en 1991 de Turing Award, het informatica-equivalent van de Nobelprijs.) Met behulp van procesalgebra kan op symbolische, algebraïsche wijze worden geredeneerd over het gedrag van gedistribueerde systemen.

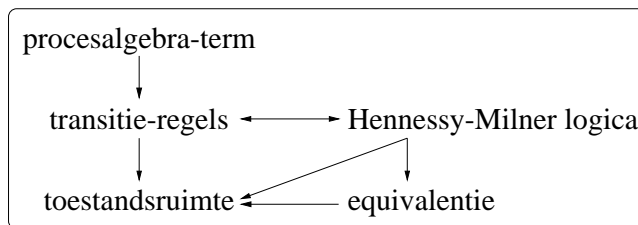
Het werk van Hoare en Milner kreeg begin jaren '80 navolging in Nederland. Eerst door Jaco de Bakker, die hierbij methoden uit de topologie gebruikte. Later door Jan Bergstra en Jan Willem Klop, die een alternatieve procesalgebra ontwikkelden. Ik ben een product van deze Nederlandse school. Jan Bergstra is mijn 1e promotor, en ik ben er trots op de leerstoelen van zowel Jaco de Bakker als Jan Willem Klop te mogen bekleden. Jaco de Bakker ging in 2001 met pensioen, waarna ik één dag in de week op de VU werd aangesteld. En de afgelopen 2,5 jaar ben ik in een dakpan-constructie vier dagen in de week op de VU aangesteld, als opvolger van Jan Willem Klop, die vorige week met pensioen is gegaan. Vandaar ook dat ik vandaag mijn oratie houd.

Ik zal nu eerst twee aspecten van mijn theoretische onderzoek belichten, gerelateerd aan procesalgebra. Vervolgens zal ik ingaan op de algoritmische ondersteuning bij het formeel modelleren en verifiëren van systemen. Daarna zal ik uitleggen hoe technieken uit de formele verificatie kunnen worden ingezet bij de modellering en analyse van ten eerste kwantitatieve aspecten van systemen, ten tweede security-protocollen, en ten derde biologische systemen. Tenslotte zal ik mijn visie geven op de toepasbaarheid van formele verificatie in de praktijk.

Procesalgebra

Vanuit de procesalgebra-beschrijving van een systeem, zijnde een procesalgebra-term, kan de bijbehorende toestandsruimte van het systeem worden gegenereerd. Dit gebeurt door middel van zogenaamde transitie-regels, inductieve bewijsregels die vertellen welke toestandsovergangen een procesalgebra-term kan uitvoeren. Er bestaat een rijke collectie van equivalenties om uit te drukken welke toestanden in een toestandsruimte hetzelfde gedrag

vertonen. Verder kunnen eigenschappen van deze toestanden worden uitgedrukt in wat heet Hennessy-Milner logica. En verschillende deelklassen van Hennessy-Milner logica corresponderen weer met verschillende equivalenties. Al enkele jaren doe ik samen met Rob van Glabbeek, en aanvankelijk ook Paulien de Wind, onderzoek naar het samenspel van procesalgebra-termen, transitie-regels, equivalenties, en Hennessy-Milner logica. Door een verrassende link te leggen tussen transitie-regels en Hennessy-Milner logica, zijn we in staat gebleken belangrijke eigenschappen voor procesalgebra's aan te tonen. We kunnen bepalen onder welke voorwaarden een equivalentie een congruentie is, wat wil zeggen dat de equivalentie behouden blijft door de operatoren van een procesalgebra. Dit is werk waar ik trots op ben. Niet alleen hebben we de machinerie ontwikkeld om dergelijke congruentieresultaten af te leiden, we hebben ook een dieper begrip gekregen waar en waarom deze resultaten gelden.

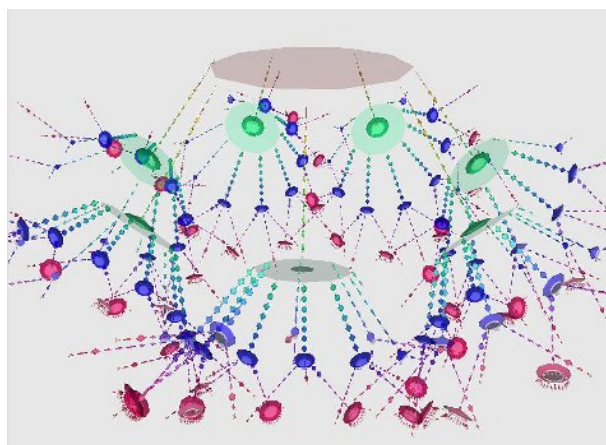


Gegeven een equivalentie, kan een stelsel van vergelijkingen uitdrukken welke procesalgebra-termen equivalent gedrag vertonen. Ik geef enkele voorbeelden van zulke vergelijkingen, en geniet ervan, want de volgende twee slides bevatten de enige formules die u vanmiddag zult zien. Bijvoorbeeld, $x + x = x$. Nu zult u denken, komt er een formule, en dan is hij fout, want $x + x$ is toch $2x$? Maar hier staat de plus niet voor optelling maar voor keuze in het gedrag van zijn twee argumenten. Aangezien $x + x$ tweemaal dezelfde keuze geeft, is het gelijk aan x . Nog een voorbeeld: $x + y = y + x$. Dit geldt toevallig ook voor de optelling van natuurlijke getallen. Maar hier betekent het, de keus tussen het gedrag van x of y is hetzelfde als de keus tussen het gedrag van y of x . Een laatste voorbeeld: $x \parallel y = y \parallel x$. Hier is de dubbele streep een algebraïsche operator die parallellisme uitdrukt. x en y zijn twee gedistribueerde componenten die onafhankelijk van elkaar opereren, maar wel met elkaar kunnen communiceren. De vergelijking zegt dat het niet uitmaakt in welke volgorde componenten parallel gezet worden. Dit zijn slechts drie van een veel grotere collectie vergelijkingen, waarmee de procesalgebra-beschrijving van een systeem equationeel gelijk kan worden bewezen aan de procesalgebra-beschrijving van het gewenste gedrag. Door de jaren heen heb ik binnen de procesalgebra zowel onderzoek gedaan aan de onderliggende equationale logica, als equationele correctheidsbewijzen geleverd voor concrete systemen.

Een belangrijke openstaande vraag op dit terrein, waar velen hun tanden al op hebben stukgebeten, betreft de axiomatisering voor formele talen van Arto Salomaa uit 1966. Robin Milner poneerde in 1984 de vraag of deze axiomatisering, minus twee axioma's, volstaat voor de zogenaamde bisimulatie-equivalentie. Ik heb hier al een heleboel energie in gestoken, maar zoals gezegd, deze vraag staat nog steeds open.

Verificatie-Tools

Ik zal nu ingaan op de ondersteuning van formele verificatie van systemen met behulp van geautomatiseerde tools. Een systeem kan op twee verschillende nivo's geanalyseerd worden, symbolisch als bijvoorbeeld een procesalgebra-term, of expliciet als een toestandsruimte. Voor beide nivo's bestaat tool-ondersteuning om het verificatie-proces te automatiseren. Op symbolisch nivo zijn dit zogenaamde theorem provers, en voor toestandsruimtes zijn dit zogenaamde model checkers. Dergelijke tool-ondersteuning is onontbeerlijk bij systeem-verificatie, omdat correctheidsbewijzen met de hand veel te arbeidsintensief en foutgevoelig zijn. Beide aanpakken hebben echter ook nadelen. Theorem provers vereisen nu nog veel menselijke inspanning. En model checkers gaan gebukt onder het feit dat toestandsruimtes van gedistribueerde systemen gigantisch groot worden.



Maar de ontwikkeling van deze tools gaat snel. Ik voorspel dat over 25 jaar wiskundige bewijzen alleen nog door de wiskundige gemeenschap geaccepteerd zullen worden als ze door een theorem prover zijn geverifieerd. Mijn collega Herman Geuvers zal daar in zijn inaugurele rede aan de Radboud Universiteit, komende vrijdag, vast meer over zeggen. En om de onstuimige groei van toestandsruimtes de baas te kunnen, is er een hele reeks technieken in ontwikkeling om toestandsruimtes efficiënt te representeren, of slechts gedeeltelijk te genereren, of al tijdens de generatie ervan te verkleinen.

Zoals gezegd, goede tools zijn erg belangrijk voor systeem-verificatie. Maar er is wel een wezenlijk probleem bij het onderzoek naar dergelijke tools. In de praktijk blijken resultaten met verificatie-tools, die in artikelen worden geclaimd, niet reproduceerbaar. Het tool werkt bijvoorbeeld slechts op één enkel operating systeem, of het tool danwel de betreffende case studie wordt door de auteurs zelfs helemaal niet vrijgegeven. En als een reproductie wel mogelijk blijkt, komen de uitkomsten vaak niet overeen met de door de auteurs geclaimde resultaten. Zojuist heb ik met nadruk betoogd dat informatica een wetenschap is, maar deze gang van zaken is natuurlijk zeer onwetenschappelijk, en belemmert de voortgang. Mijns

inziens zouden belangrijke conferenties op dit gebied, zoals CAV en TACAS, eigenlijk alleen tool-artikelen moeten accepteren waarvan de resultaten daadwerkelijk reproduceerbaar zijn.

Functionele en Niet-Functionele Eigenschappen

Eigenschappen van systeemgedrag kunnen worden geklassificeerd als functioneel of niet-functioneel. Functionele eigenschappen beschrijven de relatie tussen de inputs en de outputs van een systeem. De afgelopen jaren was een flink deel van mijn onderzoek gericht op het bewijzen van functionele eigenschappen van gedistribueerde algoritmes, communicatie-protocollen en industriële systemen, met gebruik van theorem provers en model checkers. Dit onderzoek was vaak in samenwerking met mijn voormalige promovendus Jun Pang, die nu werkzaam is aan de Universiteit van Oldenburg. Zo hebben we bijvoorbeeld een reeks verificaties uitgevoerd van de embedded controller in een gedistribueerd liftstelsel voor zware voertuigen, dat door een bedrijf in Amersfoort is ontworpen.

Hier wil ik echter in vogelvlucht het onderzoek naar niet-functionele eigenschappen van systemen belichten. Daarbij kan het gaan om kwantitatieve aspecten zoals de tijd die het een systeem kost om een bepaalde uitkomst te berekenen, of de kans dat zo'n berekening convergeert naar de correcte uitkomst. Ook kan het gaan om security, dat wil zeggen, hoe goed is een systeem beveiligd tegen hackers. Ik zal inzoomen op het werk van drie van mijn promovendi en een afstudeerder, om aldus de diversiteit van mijn onderzoeksgebied voor het voetlicht te brengen. Tegelijkertijd zijn er vier telkens terugkerende thema's. Ten eerste het ontwikkelen van formalismes om de te analyseren systemen en de te verifiëren eigenschappen in uit te drukken. Ten tweede het bedenken van algoritmes en het inzetbaar maken van bestaande wiskundige technieken, om deze verificaties uit te kunnen voeren. Ten derde het implementeren van deze technologie in verificatie-tools. En ten vierde het toepassen op case studies.

Performance Analyse

Eerst zal ik ingaan op de analyse van de performance van systemen, zoals bijvoorbeeld de productiecapaciteit van een machine. In een NWO-project genaamd TIPSy werken onderzoekers op de Technische Universiteit Eindhoven en op het Centrum voor Wiskunde en Informatica, afgekort tot CWI, samen om een brug te slaan tussen enerzijds performance analyse en anderzijds de verificatie van functionele eigenschappen. In Eindhoven is het tool χ ontworpen voor de analyse van performance aspecten van een systeem. En op het CWI is het tool μCRL ontwikkeld voor de verificatie van functionele eigenschappen. De input-talen van zowel χ als μCRL zijn gestoeld op procesalgebra. χ baseert zijn analyse echter op grootschalige simulaties, terwijl μCRL zich op zowel model checken als theorem proving baseert. Mijn promovendus Anton Wijs op het CWI heeft onder andere een vertaling gemaakt van χ naar μCRL , waardoor een directe brug is geslagen tussen performance en

functionele analyse. Ook heeft hij meegeholpen om een raamwerk te ontwikkelen waarbinnen performance analyse kan worden uitgevoerd met behulp van een tijdloze model checker. En hij heeft de zogenaamde beam search methode uit de artificiële intelligentie, die dient om een toestandsruimte slechts gedeeltelijk te doorzoeken, toepasbaar gemaakt voor kwantitatief model checken.

Roddel-Protocollen



Nu zal ik ingaan op de formele verificatie van zogenaamde roddel-protocollen. Bij een roddel-protocol wordt informatie door een groot computernetwerk verspreid op dezelfde manier als hoe een roddel alle mensen in het dorp bereikt, of een epidemische ziekte een bevolking infecteert. Het basisprincipe van een roddel-protocol is dat een knoop in het netwerk op gezette tijden informatie uitwisselt met één of meer willekeurige naburige knopen. Als dit maar vaak genoeg gebeurt is de kans dat een stukje informatie alle uithoeken van het netwerk bereikt op den duur bijna 100%. Het grote voordeel van dergelijke roddel-protocollen is dat ze een heel eenvoudige structuur hebben. Met name werken ze daardoor goed in heterogene omgevingen als het internet, waarin knopen op onvoorspelbare momenten kunnen crashen of aan het netwerk kunnen worden toegevoegd. Maar de analyse van roddel-protocollen is lastig, omdat de eigenschappen probabilistisch zijn (zoals “de kans is groot dat een stukje informatie binnen een bepaalde periode alle knopen bereikt”), en ook omdat deze eigenschappen geverifieerd dienen te worden ten opzichte van grootschalige netwerken. Tot nu toe worden eigenschappen van roddel-protocollen voornamelijk bepaald door middel van emulaties. Maar dit geeft geen zekerheid over eigenschappen als robuustheid (oftewel, hoe goed werkt het protocol in een dynamische omgeving) en convergentie (oftewel, hoe snel bereikt het protocol gemiddeld een stabiele toestand).

Onlangs is binnen de VU een onderzoeksproject gestart, als samenwerking van Maarten van Steen, Henri Bal en mijzelf. Promovenda Rana Bakhshi zal in dit project onderzoeken hoe verificatie-algoritmes en wiskundige technieken kunnen worden toegepast bij de analyse van roddel-protocollen. Aangezien het gaat om probabilistische eigenschappen ten opzichte van grootschalige netwerken, vergt dit veel reken capaciteit. Daarom zal getracht worden om de in dit project toegepaste verificatie-algoritmes zoveel mogelijk te paralleliseren, wat wil zeggen dat de berekeningen in parallel op verschillende processoren worden uitgevoerd. Hiervoor zal de nieuwe DAS3 gridcomputer worden ingezet.

Zowel in het TIPSy-project over performance analyse als in het VU-project over roddel-protocollen gaat formele verificatie hand in hand met het toepassen van wiskundige technie-

ken zoals differentiaalvergelijkingen en Markov-ketens. Met een Markov-keten kan, op basis van een gegeven kansverdeling, berekend worden hoe die kansverdeling zich door de tijd heen zal ontwikkelen. Een grote uitdaging voor mijn vakgebied is om uiteindelijk te komen tot een naadloze integratie van formele verificatie en dergelijke wiskundige methoden.

Security op het Internet

Als derde voorbeeld van niet-functionele eigenschappen zal ik het nu hebben over security op het internet. Sinds 9-11 heeft het onderzoek naar security binnen de informatica een grote vlucht genomen. Het streven is om bij elektronisch verkeer zoals internet-bankieren of stemmen per computer te garanderen dat er geen fraude gepleegd kan worden. Ik ben betrokken bij twee onderzoeksprojecten, een NWO-project en een onderdeel van het Bsik-project BRICKS, waarin het ontwerp en de verificatie van security-protocollen centraal staan. Zo'n protocol legt vast op welke manier de verschillende partijen in een elektronische handeling met elkaar dienen te communiceren. Een security-protocol dient de betrokken partijen te beschermen tegen een indringer, die de berichten in het netwerk afluistert. Deze berichten zijn in principe cryptografisch gecodeerd, maar de indringer kan de berichten hergebruiken om zich als een ander voor te doen, en kan proberen berichten te decoderen.

De grote uitdaging bij security-protocollen is om te laten zien dat fraude daadwerkelijk is uitgesloten. Fraude kent verschillende vormen, die vaak met kennis of geloof te maken hebben. Bijvoorbeeld, als de ene partij beweert dat zij een bericht verstuurd heeft, kan de ontvangende partij dan misschien toch ontkennen dat het bericht is aangekomen? En is het gegarandeerd dat de ontvangende partij uit dit bericht geen geheime informatie kan afleiden? Het formeel uitdrukken en verifiëren van dergelijke eigenschappen is een kunst op zich.

Mijn promovendus Mohammad Torabi Dashti doet op het CWI onderzoek naar het ontwerp en de analyse van security-protocollen. Hij werkt hierbij samen met onderzoekers op de VU en op de Universiteit Twente. Doel van dit NWO-project, genaamd ACCOUNT, is om security-protocollen ontwikkeld aan de VU, in de groep van Andy Tanenbaum en Bruno Crispo, formeel te verifiëren. Aldus zijn inmiddels vijf security-protocollen mede met hulp van formele technieken ontwikkeld. Ten eerste een fair payment protocol voor internet-bankieren. Ten tweede een non-repudiation protocol, waardoor de versturende en de ontvangende partij van een boodschap niet ten onrechte kunnen ontkennen dat een boodschap is verstuurd. Ten derde een digital rights management protocol voor de bescherming van bijvoorbeeld digitale muziekbestanden waar copyrights op rusten. Ten vierde een protocol voor een public-key infrastructuur. En ten vijfde een protocol voor de bescherming van emails. Ook heeft Mohammad samen met Jan Cederquist methodes ontwikkeld om zogeheten liveness-eigenschappen voor security-protocollen te verifiëren. Met zo'n liveness-eigenschap kan worden uitgedrukt dat uiteindelijk altijd iets goeds zal gebeuren, zoals bijvoorbeeld een elektronische betaling.

Electronisch Stemmen is Onveilig

In aansluiting hierop wil ik graag ingaan op het gebruik van stemcomputers, die momenteel veel in het nieuws zijn. In Nederland gaan we steeds meer over op het stemmen per computer. De ophef over stemcomputers, die bij de afgelopen Tweede Kamerverkiezingen is aangezwengeld door de actiegroep *Wij Vertrouwen Stemcomputers Niet*, maakt pijnlijk duidelijk dat zowel politici als ontwerpers van stemcomputers zich tot nu toe niet lijken te realiseren hoe gevoelig stemcomputers zijn voor fraude. Veel gevaarlijker dan het op afstand affluisteren van een stemcomputer, waar iedereen zich nu zo druk over maakt, is de mogelijkheid tot manipulatie van de uitslag van een verkiezing. De mens heeft van nature een heilig vertrouwen in de uitkomst van een computer, maar dat is lang niet altijd terecht. Onderzoekers van de Radboud Universiteit lieten zien dat een stemcomputer op eenvoudige wijze kan worden omgezet in bijvoorbeeld een schaakcomputer. Electronisch stemmen zoals het nu wordt uitgevoerd is de natte droom van iedere dictator. Knokploegen en fraude met stembiljetten zullen niet langer nodig zijn, het beheersen van de software van stemcomputers is voldoende. Zelfs grote teams internationale waarnemers kunnen een dergelijke verkiezingsfraude bijna niet achterhalen. In Italië loopt al enige maanden een onderzoek of Silvio Berlusconi bij de Italiaanse parlementsverkiezingen in april 2006 ruim een miljoen blanco stemmen met een simpel computerprogrammaatje om heeft laten zetten in stemmen voor hemzelf. De enige aanwijzing hiervoor is overigens dat er bij die verkiezingen onwaarschijnlijk weinig blanco stemmen zijn uitgebracht.

Toevallig stond afgelopen woensdag op de voorpagina van het NRC Handelsblad een artikel onder de titel *Stemmen blijft 'linke soep' met software van kleine monopolist*. De software voor stemcomputers blijkt door één driemansbedrijfje te worden ontwikkeld, en hierover is niet of nauwelijks controle. Enkele Tweede Kamerleden hebben nu aan de bel getrokken. Zoals te verwachten valt heeft het ministerie van Binnenlandse Zaken hierop sussend gereageerd; deze situatie zou “nooit accuut gevaar” hebben opgeleverd. Maar hopelijk begint de politiek zich nu toch eindelijk te realiseren dat stemcomputers, zoals ze nu worden gebruikt, een wezenlijke bedreiging vormen voor de democratie.



David Dill van de Universiteit van Stanford heeft in Amerika de Verified Voting Foundation opgericht, die misstanden bij elektronisch stemmen aan de kaak stelt. Deze stichting pleit voor een stemproces waarin de uitslag van een elektronische verkiezing daadwerkelijk gecontroleerd kan worden. In de academische wereld wordt al hard gewerkt aan stemprotocollen die dit kunnen realiseren. Binnenkort zal Cynthia Maasbommel bij mij afstuderen op een formele verificatie van het zogenaamde RIES stemprotocol, ontwikkeld aan de Technische Universiteit Delft. Bij dit stemprotocol krijgt iedere kiezer over de post een persoonlijke geheime sleutel toegestuurd, die kan worden gebruikt om via het internet één stem uit te brengen, en ook achteraf door de kiezer om te controleren of zijn of haar stem op de juiste manier is meegeteld. Dit stemprotocol voor het internet is al ingezet bij de laatste Tweede Kamerverkiezingen, voor kiezers in het buitenland.

Een dergelijk stemprotocol, waarbij een kiezer achteraf de elektronisch uitgebrachte stem kan verifiëren, brengt overigens weer andere gevaren met zich mee. Hiermee wordt bijvoorbeeld omkoping of afpersing in de hand gewerkt. Want de kiezer kan dan mogelijk niet altijd verdonkeremanen welke stem hij of zij via het internet heeft uitgebracht. Dit is sowieso strijdig met het stemgeheim, dat is vastgelegd in de kieswet. Promovendus Hugo Jonker op de Technische Universiteit Eindhoven doet in het eerder genoemde BRICKS-project onderzoek naar deze aspecten van stemmen via internet.

Concluderend zijn er veel haken en ogen aan elektronisch stemmen, de ideale procedure hiervoor is nog niet uitgedacht. Maar de politiek lijkt rigoreus door te denderen naar algehele Tweede Kamerverkiezingen via het internet. De VVD pleitte hier in 2005 al voor, en er is reeds speciale wetgeving geïntroduceerd die dit mogelijk moet maken. Als dit zo doorgaat zal over een aantal jaren ongetwijfeld blijken dat de introductie van kamerverkiezingen via het internet falikant is misgegaan. Het lijkt me raadzaam dat men nu alvast begint met het formeren van de parlementaire enquetecommissie die dit te zijner tijd kan gaan onderzoeken.

De Cel als Mini-Computer

Als laatste onderzoeksonderwerp zal ik nu ingaan op een vrij nieuw onderzoeksgebied, de bioinformatica. Zoals de naam al suggereert ligt dit op het snijvlak van de biologie en de informatica. Het gaat hierbij om het ontwikkelen van algoritmes en computationele technieken voor het beheer en de analyse van biologische data. Meerdere Nederlandse universiteiten hebben de afgelopen jaren onderzoeksgroepen in de bioinformatica opgericht, en ook op de VU hebben we zo'n groep, geleid door Jaap Heringa. Wetenschappelijke vragen zijn onder andere het opslaan en doorzoeken van enorm lange DNA-sequenties, computationele analyse van genen, biomedische beeldverwerking, en systeem-biologie.

Dat laatste, systeem-biologie, houdt zich bezig met het bestuderen van de interacties van een biologisch systeem, en hoe deze interacties aanleiding geven tot het gedrag van het gehele systeem. Eén van de grote uitdagingen is het modelleren van celgedrag. Cellen zijn complexe, zelforganiserende machientjes die grote aantallen biochemische reacties uitvoe-

ren. Tot nu toe werden voornamelijk differentiaalvergelijkingen gebruikt om celgedrag te beschrijven, maar daar kleven bezwaren aan. Zo geven differentiaalvergelijkingen op zichzelf een nogal grove benadering van het werkelijke celgedrag. Ook is het lastig de experimentele data te verkrijgen die als input voor de differentiaalvergelijkingen moet dienen. En de resulterende differentiaalvergelijkingen zijn zo ingewikkeld dat het zeer moeilijk is om ze op te lossen of te simuleren.

De laatste jaren is men gaan inzien dat een cel in feite een mini-computer is, met een aantal verschillende processoren die asynchroon met elkaar communiceren. En cellen onderling kunnen ook weer communiceren, zodat ze een gedistribueerd netwerk vormen. Zoals ik al eerder zei, informatica draait nu juist om informatie, berekening en communicatie. Het modelleren en analyseren van cellen blijkt voor mijn vakgebied een nieuwe en prachtige uitdaging. David Harel, een grootheid in de theoretische informatica, formuleerde in 2005 een zogenaamde Grand Challenge, namelijk, geef een formele modellering van een rondworm, zijnde een diertje van één millimeter lang dat in de biologie als modelorganisme wordt gebruikt.



Onlangs zijn de eerste procesalgebra's gedefinieerd waarmee bepaalde aspecten van celgedrag formeel kunnen worden beschreven. In deze procesalgebra's spelen bindingen tussen verschillende componenten een prominente rol, maar ook stochastiek, en ruimtelijke aspecten. Want de locatie van bijvoorbeeld een celkern in een cel, of van een cel in een stuk weefsel, heeft grote invloed op de gedragmogelijkheden ervan. Het zoeken is nog naar een overkoepelend formalisme, waarin alle belangrijke aspecten van cellen tot hun recht komen. Serieuze vraag daarbij is hoe we zeker kunnen zijn dat de formele beschrijving van celgedrag in zo'n procesalgebra overeenstemt met de werkelijkheid. En de grote uitdaging is om vervolgens aan de hand van zo'n formele beschrijving een daadwerkelijke simulatie en analyse van celgedrag te kunnen uitvoeren. Dit is grotendeels een braakliggend onderzoeksgebied. Jaap Heringa, Henri Bal en ik zijn bezig hier gezamenlijk twee promovendi op aan te stellen.

Samenvattend, bij kwantitatieve analyse, dat wil zeggen de analyse van performance en van probabilistische aspecten, zijn de formalismes om systemen te specificeren en om eigenschappen uit te drukken reeds goed uitgekristalliseerd. De nadruk van het onderzoek ligt hier op het ontwikkelen van verificatie-algoritmes en het integreren van wiskundige technie-

ken. Bij security-protocollen zijn de formalismes nog minder ver ontwikkeld, vooral waar het gaat om het uitdrukken van security-eigenschappen, Tenslotte, bij het formeel beschrijven en analyseren van cel-gedrag zijn we nog maar net uit de startblokken vertrokken.

Het Virtuele Blok Beton

Ik zal nu iets zeggen over de toepasbaarheid van formele methoden in de informatica. In de oratie van Jos Baeten werd ooit een mooie parallel getrokken tussen informatica en bouwkunde. Want net als gebouwen en bruggen vergen ook computerprogramma's een conceptueel constructieplan. Groot verschil is echter dat in de bouwkunde het ontwerpproces in meerdere opzichten verder is ontwikkeld dan in de informatica: er worden architectuurtekeningen gemaakt, er worden vooraf op papier sterkteberekeningen uitgevoerd, en er zijn standaardcomponenten (zoals bakstenen en ramen) voorhanden. Idealiter zouden formele methoden uiteindelijk eenzelfde rol gaan spelen in de informatica als sterkteberekeningen dat nu doen in de bouwkunde.

Toch kunnen we niet verwachten dat alle software uiteindelijk zo solide en doordacht gebouwd zal worden als een huis. Daarvoor is er veel te veel software nodig, en zijn er te weinig standaard oplossingen. Bij het intikken van een stel regels code zal men bovendien niet snel een blok beton op zijn hoofd krijgen. Strenge controle van miljoenen regels code is moeilijk, miserabele kwaliteit van software kan eenvoudig achter een mooie interface worden verborgen, en de klant weet meestal te weinig van het product. Ook zijn ontwerpers van software over het algemeen nauwelijks bekend met het toepassen van formele methoden.

Gelukkig onstaat in de industrie wel steeds meer het bewustzijn dat het ontwerp van een computerprogramma hecht doortimmerd dient te zijn. En bij het ontwerpen van risicovolle systemen zoals in de ruimtevaart en in de vliegtuigindustrie worden formele methoden nu al veel toegepast. Zo is Gerard Holzmann, die de veelgebruikte model checker Spin heeft ontwikkeld, sinds enkele jaren hoofd van het Laboratory for Reliable Software binnen NASA. En bij de spoorwegen zijn er de Europese Cenelec-standaarden, die voor de hoogste veiligheidsnivo's het gebruik van formele methoden verplicht stellen. Door de jaren heen heb ik regelmatig samengewerkt met ProRail en Movares, voorheen onderdelen van de NS. Er wordt veel gescholden op de spoorwegen, en eerlijk gezegd doe ik daar als reiziger ook aan mee. Maar ze hebben wel een hele lange traditie in degelijke ontwikkeling van complexe en toch veilige computersystemen om treinen over het drukbezette spoor te leiden. De spoorwegen gaan door een spannende periode, mede omdat de nationale spoorwegorganisaties intensief moeten gaan samenwerken op Europees nivo. Dit heeft onder andere tot gevolg dat er in plaats van allemaal verschillende nationale veiligheidslogica's voor het spoor, in feite één Europese veiligheidslogica nodig is. De traditionele manieren waarop deze veiligheidslogica's voor het spoor werden ontwikkeld voldoen niet meer, waardoor de deur is opengezet voor de inzet van formele methoden.

Concluderend, formele verificatie van software is een belangrijk onderzoeksgebied, waarin nog veel voortgang geboekt kan worden. Gerard Holzmann kreeg in december een ere-doctoraat van de Universiteit Twente. Tijdens een interview met het universiteitsblad UT Nieuws, ter gelegenheid van dit ere-doctoraat, zei hij: “Ik heb het geluk dat ik in het juiste vakgebied werk, waarin correctheid van software het belangrijkste ‘open’ probleem is. Dit is moeilijk en uitdagend”. Ik kan dit alleen maar onderschrijven.

Microkredieten voor Onderzoek

Tenslotte wil ik graag mijn visie geven op enkele onderwerpen die een sterke invloed hebben op de huidige context voor onderzoek en onderwijs waarbinnen wij opereren. Onderzoek doen in de informatica betekent werken in een snel veranderend landschap. Binnen het onderzoeksgebied zelf gaan de ontwikkelingen razendsnel. Daar komt nog bij dat de universiteiten een stormachtige tijd beleven. Onderwijs internationaliseert, financieringsstromen veranderen, en de overheid probeert voortdurend veranderende visies op te leggen. Sommige van die veranderingen zijn beslist verbeteringen, en leveren nieuwe kansen op. Zo is de steeds grotere nadruk op multidisciplinair onderzoek voor de informatica buitengewoon gunstig, aangezien het, zoals al eerder gezegd, veel raakvlakken heeft met andere onderzoeksgebieden.

Maar helaas pakken veranderingen vaak niet positief uit. Zo heeft de continue onderwijsvernieuwing bij het middelbaar onderwijs de afgelopen vijftien jaar een schandalige uitholling van het beta-onderwijs opgeleverd. Tegelijkertijd blijft informatica op de middelbare school een ondergeschoven kindje. Dit alles heeft een zeer negatief effect op de kwaliteit en kwantiteit van de studenteninstroom bij onze afdeling. En de vermarkting van universiteiten, gepredikt door Mark Rutten in zijn vorige leven als staatssecretaris van onderwijs, waarbij de student vooral als consument wordt gezien, getuigt mijns inziens van een compleet gebrek aan inzicht wat goed onderwijs werkelijk inhoudt. Verder worden de onderzoeksscholen IPA, ASCI en SICS, die de afgelopen tien jaar met veel inspanning tot belangrijke platforms zijn geworden voor het opleiden van promovendi in de informatica, nu met een penne-streek vervangen door graduate schools. Ook zou ik hier een klaagzang kunnen afsteken over hoe de IND het voor buitenlandse kenniswerkers steeds moeilijker maakt om naar Nederland te komen, met mijn promovenda Rana Bakhshi uit Azerbaidjan als recent treurig voorbeeld. Ik wil hier echter iets dieper ingaan op de manier waarop informatica-onderzoek in Nederland tegenwoordig wordt gefinancierd.

Wat velen zich niet realiseren is dat onderzoek, net als bijvoorbeeld turnen en kunstschaatsen, een jurysport is. Onze wetenschappelijke artikelen worden bij conferenties en tijdschriften beoordeeld door anonieme collega’s, die er cijfers aan toekennen. En financiering voor onderzoek moeten wij binnenslepen bij verschillende nationale en internationale geldpotten, door onderzoeksvorstellen in te dienen, die ook weer door anonieme collega’s worden beoordeeld. Net als bij turnen en kunstschaatsen is hun oordeel subjectief, en dus

grillig en onvoorspelbaar.

Bij geldgevers bestaat steeds meer een voorkeur om vooral grote onderzoeksprojecten te financieren, omdat één groot project voor de geldgever een betere beeldvorming naar buiten levert, en makkelijker te organiseren is dan meerdere kleine projecten. Ook eisen geldgevers steeds vaker fikse inmenging van de industrie. Op zich is een link van onderzoek met de praktijk natuurlijk toe te juichen. Maar we zijn bezig door te schieten. De overheid denkt ten onrechte dat onderzoek maakbaar is, en dat de industrie in staat zou zijn om de belangrijke onderzoeksvragen voor de informatica te dicteren. Geldstromen voor informatica-onderzoek worden als gevolg daarvan steeds meer geleid via afgebakende programma's, die tezamen een onoverzichtelijke lappendeken zijn gaan vormen. Ambtenaren van economische zaken krijgen steeds meer zeggenschap over de verdeling van dit geld, alhoewel zij weinig verstand blijken te hebben van hoe onderzoek gefinancierd dient te worden. Via bijvoorbeeld de FES-gelden komen op onvoorspelbare momenten grote hoeveelheden geld vrij, die binnen korte tijd verdeeld moeten zijn. Zo wordt lobbyen belangrijker dan goed onderzoek, als het gaat om het binnenhalen van onderzoeksfinanciering.

Daar staat tegenover dat bij de Open Competitie van informatica bij het NWO, bedoeld voor kleinere onderzoeksprojecten, elk jaar meer voorstellen binnenkomen. Bovendien zijn ze gemiddeld van hoge kwaliteit. Het percentage geaccepteerde voorstellen bij de Open Competitie is intussen gezakt naar zo'n 20%. Op deze manier wordt heel veel energie verkwist aan het schrijven van goede onderzoeksplannen die uiteindelijk in de prullenbak verdwijnen. Ook wordt het voor beginnende onderzoekers steeds moeilijker om financiering te krijgen.

De Bengaalse econoom Muhammad Yunus heeft onlangs de Nobelprijs voor de vrede gekregen vanwege microkredieten, waarbij veel kleine leningen worden verstrekt voor zeer specifieke doeleinden. In ons eigen land is prinses Máxima hier een warm pleitbezorgster van. In navolging van deze microkredieten pleit ik ervoor om meer geld te reserveren voor relatief kleine onderzoeksprojecten, en met meer kansen voor beginnende onderzoekers. Ook zou het accent moeten verschuiven van zware jurering van onderzoeksvoorstellen vooraf naar serieuze beoordeling van de behaalde resultaten achteraf. Geef een beginnend onderzoeker op basis van een relatief kort onderzoeksvoorstel een budget, en evalueer na een aantal jaren zorgvuldig wat daarmee is gedaan. En durf gevestigde onderzoekers budget te geven op basis van hun grote staat van dienst. De vernieuwingsimpuls van het NWO ligt in deze lijn, en is de afgelopen jaren een groot succes gebleken. Maar in plaats van de vernieuwingsimpuls uit te breiden, wordt het naar het zich nu laat aanzien helaas niet gecontinueerd. Gelukkig lijkt er via het nieuwe Ideas programma een vernieuwingsimpuls op Europees nivo te gaan ontstaan.

Al met al vind ik dat ambtenaren van economische zaken, het Centraal Planburo, en ook het nog niet zo lang geleden opgerichte ICTRegie Orgaan, in Nederland een te zware rol krijgen bij het verdelen van onderzoeksgeld. Door de jaren heen hebben STW en met name het NWO bewezen uitstekend in staat te zijn om onderzoeksgelden te verdelen, en in samenspraak met de betrokken partijen een onderzoeksagenda te bepalen. Ik pleit ervoor

het NWO een sterkere en meer centrale rol te geven bij het verdelen van onderzoeksgeld. Ik realiseer me terdege dat dit voorlopig vechten tegen de bierkaai is, maar ik wil het in ieder geval gezegd hebben.

Dankwoord

Graag wil ik tot slot een aantal mensen bedanken. Opmerkelijk genoeg hebben de meeste collega's die ik zal noemen een voornaam die begint met een J.

Jan Bergstra, John Tucker, Jaco de Bakker en Jan Willem Klop heb ik ooit in een liber amicorum omschreven als Vier Vaderlijke Figuren. Jan trok me met zijn aanstekelijke enthousiasme de informatica in, en was voor mij als promovendus op het CWI en als postdoc in Utrecht een belangrijke bron van inspiratie. John stelde me in Swansea aan als universitair docent, en hielp om me te vormen tot een volwassen onderzoeker en docent. Jaco speelde een sleutelrol in mijn aanstelling als themaleider op het CWI, en Jan Willem en Jaco spannen zich samen in voor mijn aanstelling op de VU. Ze hebben me daarna met raad en daad terzijde gestaan. Ik ben ze daar zeer erkentelijk voor.

Het CWI heeft mij vele jaren, tot op de dag van vandaag, een uitmuntende onderzoeksomgeving geboden. Jaco van de Pol wil ik graag hartelijk danken voor de nauwe en prettige samenwerking de afgelopen jaren. Enkele van de genoemde promovendi worden mede door hem begeleid. Ook met Jan Friso Groote en Jos Baeten is er een goede en langdurige samenwerking.

Mijn collega's op de VU, in het bijzonder van de sectie Theoretische Informatica, ben ik dankbaar voor het geschonken vertrouwen en, ondanks een ingrijpende reorganisatie binnen onze afdeling, de goede werksfeer in de afgelopen 2,5 jaar. Ik voel me bevoorrecht om bij de afdeling informatica van de VU te werken. Er is gebleken dat die voor mij veel mooie kansen op samenwerking biedt. Met Henri Bal op het gebied van parallelle algoritmes voor verificatie, met Maarten van Steen op roddel-protocollen, met Bruno Crispo op security-protocollen, met Jaap Heringa op het modelleren van celgedrag, en ook met Jan Treur op het bewijzen van eigenschappen voor zogeheten coördinatietalen.

Mijn familie is steeds heel belangrijk voor me geweest. Mijn ouders hebben me altijd gestimuleerd positief en ondernemend te zijn. De eerste 25 jaar van mijn leven ben ik "het broertje van" geweest, grote broer Robbert ging me voor in schaken, een studie wiskunde aan de UvA, en een promotie. Zus Annemarie bedank ik voor haar warmte en enthousiasme. En bovenal, Judi, bedankt voor je steun en liefde.

Ik heb gezegd.