Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Egghead betegelt badkamer

Rede bij het afscheid als lector Mathematische Informatica aan de Universiteit van Amsterdam

DONDERDAG 25 MAART 2010

Dr. Peter van Emde Boas

Egghead betegelt badkamer

Rede bij het afscheid als lector Mathematische Informatica
aan de Universiteit van Amsterdam

25 maart 2010

Dr. Peter van Emde Boas

ILLC, FNWI, Universiteit van Amsterdam,
Bronstee.com Software & Services B.V., Heemstede
Dept. Comp. Sci. University of Petroleum,
Chang Ping, Beijing,
P.R. China

Geachte toehoorders

Geachte toehoorders. Het traditionele begin van een rede zal ik U niet onthouden, maar dat zal zo ongeveer het enige traditionele element in deze rede zijn.

Allereerst een verklaring voor de titel. Deze titel is ontleend aan de kop van een verslag over een door mij verzorgd college dat in april 1996 is verschenen in het studenten blaadje SUM [1]. Collega's van het ILLC en andere bezoekers van onze gang op de derde verdieping van het Euclides gebouw kunnen dit weten aangezien een kopie van dit stukje jarenlang naast mijn deur heeft gehangen.

De journalist was toevallig getuige geweest van mijn presentatie van een regelmatig terugkerend onderdeel van mijn onderwijs, te weten de meester-reductie van Turing Machine berekeningen tot betegelingen, en heeft bij die gelegenheid in ieder geval meegekregen dat dit soort, in het algemeen als lastige materie beschouwde, onderwerpen zich laten behandelen zonder daarbij de humor uit het oog te hoeven verliezen. De frase "Egghead" is ontleend aan een van mijn favoriete truien die ik tijdens dit college aanhad. Het betreft hier een stuk merchandise van een inmiddels verdwenen keten van computerwinkels, Egghead Software, die rond de jaren 1980-1990 actief was in Californië. Bij die winkel zijn vergelijkbare truien zijn aangeschaft voor de gehele familie.

Mijn exemplaar van de trui kunt U aantreffen op het staatsieportret dat onze Universitaire fotograaf Henk Thomas in het najaar van 1990 vervaardigde voor de destijds in Folia [2] verschijnende reeks portretten onder het motto "In Academia", een serie die het helaas niet lang heeft volgehouden. Dit portret vertoont iemand die weinig op lijkt te hebben met de standaarden van academische stijl en traditie, hetgeen vast de reden is geweest om mij destijds voor deze portrettenreeks te inviteren. De als aap uit de mouw verschijnende Rollei

illustreert uiteraard mijn rol als permanente fotograaf van activiteiten op het gebied van de Wiskunde en de Informatica en andere zaken waarbij ik betrokken ben.

Dat ik de trui ook echt heb gedragen blijkt uit een tweede staatsieportret dat Henk Thomas eerder dat jaar had vervaardigd ten behoeve van een interview in de Folia [3] over mijn bijzondere positie als de laatste lector aan de UvA. Naast de trui vertoont dit portret een aantal karakteristieke attributen zoals mijn dinosaurussen anti-roken mok. Ik heb destijds de gelegenheid misbruikt om Henk Thomas een groepsportret te laten vervaardigen van mijn toenmalige onderzoeksgroep (op kosten van de toenmalige vakgroep II waarvan ik de voorzitter was). Zoals U ziet liepen er in 1990 aan de UvA heel wat meer theoretische Informatici rond dan thans het geval is.

Ik heb mij regelmatig de vraag gesteld of ik soms een roeping heb gemist om te functioneren als Universitaire Hofnar. Dit is een functie die de Universiteit op dit moment niet kent maar invoering ervan valt zeker te overwegen in de context van de bestuurstructuur die de Universiteit zich sinds de invoering van de meest recente wet over de Universitaire organisatie heeft aangemeten, die men eerder neo-despotisch dan democratisch kan noemen. Echter: mij is met klem ontraden om deze rede te misbruiken met gemopper over de gang van zaken binnen de Universiteit dus ik zal dit onderwerp verder met rust laten.

In het komende Academische uur hoop ik U te kunnen meenemen op een tocht langs de diverse activiteiten waarmee ik gedurende mijn leven dat zich grotendeels rond het Roeterseiland heeft afgespeeld heb ingelaten. Wellicht dat ik ook nog iets van mijn beweegredenen over het voetlicht kan brengen. En ik wil laten zien hoe groot de invloed bij die activiteiten is geweest van toevalligheden waar onze organisatie geen greep op heeft.

Een afscheidscollege geven legt immers aan de orator een drietal taken op: uitleggen wat je zelf hebt gedaan, uitleggen wat er met je vak is gebeurd, en dit alles in verband brengen met de ontwikkelingen in de buitenwereld. Te veel om allemaal in de toegemeten tijd van 45 minuten te kunnen behandelen. Papier is echter geduldig, en daarom zult U bij het verlaten van deze zaal een gedrukte tekst ontvangen waarin ik de kans heb gegrepen om veel uitgebreider en volledige deze onderwerpen te bespreken.

Ik zal mij concentreren op de taak van het afleggen van verantwoording. De Nederlandse staat heeft mij gedurende een periode van 46 jaar, eerst op het toenmalige Mathematische Centrum, thans het Centrum voor Wiskunde en Informatica, en later via een reeks aanstellingen aan de Universiteit van Amsterdam als werknemer in diens gehad; eerst als assistent, later medewerker en uiteindelijk als lector Mathematische Informatica. U hoort het goed: ik

beschouw mij zelf nog steeds als lector, in het besef dat met mijn emeritaat na 30 jaar waarschijnlijk een einde is gekomen aan het bestaan van deze Universitaire functie in Nederland. Ik kan wel met tevredenheid constateren dat voor deze gelegenheid onze organisatie er in is geslaagd mijn positie op correcte wijze te vermelden op de verzonden uitnodigingen. De vraag mag gesteld worden wat de Nederlandse samenleving gedurende die periode heeft teruggekregen voor het salaris waarvan ik al die jaren het goede leven heb mogen genieten.

De jonge van Emde Boas

In mijn geval is er nooit sprake geweest van enige twijfel over mijn latere studiekeuze. Petertje had immers altijd iets met cijfers en niets met mensen. Gezichten en namen kon ik toen (en ook nu nog) niet onthouden. Als kleuter werd ik weerhouden van destructieve activiteiten door mij een telefoonboek in handen te stoppen want daar stonden een heleboel cijfertjes in.[1] Op de Montessori kleuterschool werden vele duizendrollen volgeschreven, en de legende wil dat op de lagere school het begrip voor het wiskundige Montessori materiaal bij mij groter was dan bij onze toenmalige onderwijzeres, een eigenschap die ik deelde met mijn toenmalige klasgenote en huidige echtgenote Ghica Lubsen.

1). Deze en andere gedragspatronen zouden mij heden ten dage ongetwijfeld een diagnose van een lichte vorm van Autisme hebben bezorgd, maar die kwaal was destijds gelukkig nog niet uitgevonden.

In die dagen beheersten wij naast de inmiddels verguisde staartdeling uiteraard ook de vergelijkbare algoritme om vierkantswortels uit grote getallen te trekken. Het enige probleem dat de school carrière van de jonge van Emde Boas leek te belemmeren lag op het gebied van de taal: Petertje kon niet spellen. Dit belette destijds een vroegtijdige overgang naar de Middelbare school, maar dit staaltje repressief gedrag van school en ouders vroeg om wraak en vergelding en zo geschiedde het. Op het Montessori Lyceum van Amsterdam hadden leerlingen in de laagste twee klassen immers alle ruimte om hun taken naar vrije keuze in te delen, vele decennia voordat onze onderwijsdeskundigen het studiehuis meenden uit te moeten vinden. Gedurende de eerste twee maanden op het Lyceum had ik, gebruik makende van deze vrijheid, bij een aantal vakken zover vooruit gewerkt dat de schoolleiding geen andere oplossing zag dan mij alsnog over te laten gaan naar de tweede klas, zodat ik het Gymnasium in vijf jaar kon voltooien.

Mijn voornaamste actie van puberale revolte bestond enkele jaren later uit het dreigement om via een keuze voor de alfa variant mijn toegang tot een studie in de exacte vakken te belemmeren, maar dank zij een compromis

waardoor ik via privé onderwijs ook op het onderwerp van de klassieken de nodige kennis kon opdoen is dat conflict destijds snel en efficiënt uit de wereld geholpen. Als geciviliseerd burger combineerde ik deze opleiding met het bespelen van een instrument (in mijn geval de viool) en het regelmatige bezoek aan concerten en andere culturele evenementen. Met sportactiviteiten in georganiseerd verband heb ik mij daarentegen nooit ingelaten, en afgezien van het latere lidmaatschap van het Amsterdam Studenten Corps en het eertijds nog levende dispuut APEDAS nam ik geen deel aan het uitgaansleven.

De studie wiskunde die ik begon in 1962 werd voltooid in de zeven jaar die destijds daarvoor normaal was. Van meet af aan vertoonde ik daarbij een thans minder gebruikelijk gedrag: ik stelde (soms tamelijk domme) vragen tijdens het college en vervoegde mij bij de docenten om na afloop dingen uit te zoeken die mij niet duidelijk waren geworden. Hiermee werkte ik mijzelf in het gezichtsveld van de toenmalige hoogleraar in de Topologie J. de Groot die mij medio 1964 uit de collegebanken pikte om mij een positie als technisch assistent (later, na mijn Kandidaats examen als student assistent) aan te bieden op het Mathematisch Centrum. Met het aanvaarden van deze functie verviel de meer gebruikelijke optie die de goede studenten destijds hadden om als derdejaars student assistent mee te lopen bij de wiskunde practica, en aansluitend als studentassistent mee te werken op het Mathematisch Instituut. Anders gezegd: de Groot had mij voor de neus van A. Heyting weggekaapt, die destijds verantwoordelijk was voor de selectie van de student assistenten.

Naast het bezoek aan de colleges op het Roeterseiland vertoefde ik dus vooral op het Mathematisch Centrum dat destijds op steenworp afstand was gevestigd in de tweede Boerhaavestraat (nabij genoeg om bij gelegenheid tijdens de pauze van een college even te profiteren van de gratis koffie die rond die tijd op het Centrum werd aangeboden). Op het Centrum werd ik al snel betrokken bij het onderzoek op de afdeling Zuivere Wiskunde o.l.v. Cor Baayen. Reeds in 1965 verscheen daar het eerste interne rapport dat ik geheel eigenhandig had geschreven.

Dit brengt mij op het punt van de resultaten van mijn onderzoek, onderwijs en andere activiteiten. Ik meen dat iemand in mijn positie toch op zijn minst een dozijn onderwerpen moet kunnen opvoeren onder het kopje relevante activiteiten. Zoals iedere wiskundige sinds de dagen van Cantor weet betekent dit dat je in staat moet zijn om een bijectie te construeren tussen deze verrichtingen en een andere willekeurig te kiezen verzameling van twaalf objecten. Voor deze laatste verzameling heb ik mijn keuze laten vallen op de werken van de Griekse Mythologische held Heracles. Kenners van de klassieke mythologie zullen kunnen beamen dat vanuit hedendaags perspectief gezien deze lijst van heldendaden eerder gezien moet worden als een zwartboek dat

aanleiding geeft tot strafvervolging van de held. Het betreft hier immers een reeks van gevechten met creaturen met al dan niet voor het beest dodelijke afloop waarbij het vaak handelt om zeldzame en ongetwijfeld inmiddels beschermde diersoorten; zijn omgangsvormen met betrekking tot de koningin van de Amazonen zijn bepaald vrouwonvriendelijk, en de wijze waarop de Augiasstal is gereinigd vormt ongetwijfeld een milieudelict van de derde categorie. Het is lastig om deze bijectie ook enige betekenis te geven, en hierbij is het helaas niet mogelijk gebleken om de canonieke ordening in de Mythologie van deze werken te respecteren.

Bij de bespreking van deze activiteiten gaat het mij uiteraard niet om de al dan niet aanwezige importantie (waarover ik het oordeel aan anderen overlaat), maar meer op de rol die het werken eraan heeft gespeeld voor mijn ontwikkeling als wiskundige en informaticus.

De leeuw van Nemea - *Verzamelingstheoretische Topologie*

De leeuw van Nemea was het eerste monster dat Heracles in dienst van Eurystheus, de koning van Argos, diende te verslaan, dus het is passend dit werk te koppelen aan mijn eerste schreden op het pad van de wiskunde.

Zoals hierboven aangegeven was het de hoogleraar J. de Groot die mij in 1964 vanuit de collegebanken naar het Mathematisch Centrum inviteerde. Zijn vakgebied betrof de verzamelingtheoretische topologie, een vakgebied dat U vandaag tijdens het symposium vertegenwoordigd hebt zien worden door mijn collega Jan van Mill van de Vrije Universiteit die ik nog altijd beschouw als de voornaamste wetenschappelijke erfgenaam van de Groot. Het vak is aan de eigen instelling helaas vrijwel geheel verdwenen. Toch hoef ik mij als lid van het ILLC er niet voor te schamen het ooit te hebben bedreven, aangezien het juist in de logica (en in mindere mate in de Informatica) nog de nodige toepassingen vindt.

De Groot was ook om een andere reden belangrijk voor het Mathematisch Instituut. Als een van de weinige hoogleraren wist hij over te brengen dat het beoefenen van de wiskunde ook leuk is, en reeds met betrekkelijk weinig technische voorkennis op zinvolle wijze kan worden bedreven, ook door studenten. Zijn vakgebied leende zich daar ook goed voor. Het zit vol met problemen die zich gemakkelijk laten uitleggen en die soms op eenvoudige wijze oplosbaar blijken te zijn, en soms grote technische vaardigheden vereisen om tot een oplossing te komen.

Mijn eerste artikel dat ooit in een tijdschrift is opgenomen (in dit geval het Nieuw Archief voor Wiskunde), is ontstaan naar aanleiding van het tentamen Topologie dat ik voor mijn kandidaats examen mondeling mocht afleggen bij de Groot. Een hierbij gestelde opdracht bestond uit het construeren van vijf

verschillende compactificaties van de reële halfrechte. In het bijzonder ging het om het bepalen van de restverzameling, de deelruimte van elementen die aan de ruimte moet worden toegevoegd om de compactificatie op te leveren. Aanleiding was een discussie die de Groot eerder met collega Kuiper had gehad over de rol van compactificaties in de verschillende vormen van meetkunde die de beide hooggeleerden bedreven. Kuiper hield zich immers bezig met de meetkunde van variëteiten.

Na het produceren van een viertal expliciete voorbeelden kwam het inzicht boven tafel dat voor dit probleem een generiek antwoord kon worden gegeven: ieder continuum kan als restverzameling optreden en omgekeerd zijn alle restverzamelingen continua. Tijd om de toenmalige medeweker Jan Aarts bij het gesprek te betrekken. Het uiteindelijke artikel [4] laat zien dat deze eigenschap voor een veel grotere klassen van niet compacte ruimten geldt en geeft voor deze klasse een volledige karakterisering. Opgemerkt dient te worden dat dit artikel ook voor Jan Aarts zijn eerste tijdschriftpublicatie was.

Het werk in de Topologie heeft een ander remarkabel resultaat mogen opleveren. In de traditionele beschrijving is een Topologie een oneindige hogere orde structuur: de collectie van open verzamelingen is een verzameling van deelverzamelingen van het domein die aan een aantal eenvoudige condities moet voldoen. Om topologieën te kunnen bepalen gebruikt men systemen van voortbrengers in de vorm van een basis: iedere open verzameling is een vereniging van basisverzamelingen. Een basis kan soms veel zuiniger zijn dan de topologie zelf. Voor een gebruikelijke ruimte zoals de reële rechte kan een basis aftelbaar zijn terwijl de topologie gelijkmachtig is met het continuum. Een basis kan op haar beurt worden gegenereerd door het vormen van eindige doorsneden uit een nog kleinere collectie open verzamelingen die men een subbasis noemt.

De vraag die ik mij stelde was hoe topologische ruimten er uit zien indien men aan een basis of een subbasis de extra conditie oplegt dat deze *minimaal* is: het verwijderen van een willekeurig element uit dit systeem van voortbrengers resulteert in een zwakkere topologie. Voor het geval van een basis bleekt deze conditie gevolgen te hebben voor de structuur van de ruimte, die geheel beschreven kan worden in termen van een partiële ordening en een voor deze ordening dichte deelverzameling. In het geval van de subbasis was het niet duidelijk of er (afgezien van een aantal evidente voorbeelden zoals de eindige ruimten en het Cantor discontinuum) Topologische ruimtes bestonden met een minimale subbasis. Een middag puzzelen op het Mathematisch Centrum leerde mij echter dat het mogelijk was voor de reële rechte een dergelijke minimale subbasis te construeren. Nadere analyse van de gebruikte methode toonde aan dat deze eigenschap geldt voor de gehele klasse van separabele metrische

ruimten, een klasse van ruimten die een groot deel van de topologische ruimten omvat waarmee een student in de beginjaren van zijn studie in contact zal komen. Al deze ruimtes hebben derhalve de onverwachte eigenschap dat het mogelijk is de topologie op een maximaal zuinige wijze te genereren.

Het resultaat was goed voor mijn eerste deelname aan een internationaal congres dat in Montenegro plaats vond in augustus 1968 [5]. Helaas heb ik nooit mogen vernemen dat het resultaat enige verdere toepassing in de wiskunde heeft gevonden.

Cerberus - *de Davenport Constante*

Cerberus - de Hellehond, is een driekoppig monster dat niet gedood maar alleen maar gevangen diende te worden om het aan de koning te presenteren; het uitvoeren van deze opdracht vereiste wel een afdaling naar de onderwereld. Het is passend dit werk te koppelen aan een probleem met verschillende verschijningsvormen dat in feite ook vandaag nog onopgelost is.

Beschouw een getal dat product is van minstens vier al dan niet gelijke priemfactoren. Dan bestaat er altijd een echte deler van dit getal waarvan het eindcijfer gelijk 0, 1, 5 of 6 is. Deze simpele getaltheoretische observatie van mijn toenmalige college op het Mathematisch Centrum, Dirk Kruyswijk, vormt het uitgangspunt voor een reeks rapporten die tussen 1965 en 1971 zijn verschenen op het Mathematisch Centrum geschreven door Kruyswijk, Cor Baayen, Evert Wattel en mijzelf in wisselende samenstelling over een combinatorisch probleem over eindige groepen en halfgroepen. De centrale vraag is hoe veel elementen van deze groep of halfgroep verzameld kunnen worden zonder dat het mogelijk is een niet leeg product (som) van deze elementen te vormen dat als resultaat het eenheidselement oplevert (resp. voor het geval van de halfgroepen, een idempotent element). De gegeven elementen kan men zich voorstellen als geplaatst in een rij, waarbij men zoekt naar een aaneengesloten deelwoord dat na uitvermenigvuldiging de gevraagde idempotent oplevert. Men kan ook denken aan een multiset waarbij men een willekeurige greep uit deze multiset kan kiezen. In het geval van deelwoorden hebben de elementen een vaste volgorde, terwijl voor een multiset de elementen in een willekeurige volgorde kunnen worden uitvermenigvuldigd, en daarom beperken wij ons voor deze versie van het probleem tot groepen waarvoor de volgorde er niet toe doet omdat de groep Abels is. Ik negeer in het vervolg van dit verhaal het geval van

het woordprobleem voor halfgroepen, echter niet zonder te vermelden dat mijn eerste zelfstandig geschreven rapport op het Mathematisch Centrum in 1965 [6] over een speciaal geval van dit probleem handelde.

Een eenvoudig geval van dit probleem is het geval van een eindige cyclische groep $Z/(n)$. Men kan een voortbrenger a kiezen en $n-1$ kopieën daarvan in een multiset stoppen zonder dat men op niet triviale wijze het eenheidelement 0 als som kan krijgen. Het is ook makkelijk in te zien dat men deze multiset niet kan uitbreiden en dat in het algemeen iedere multiset van n elementen wel voldoende materiaal voor een nulsom bevat (dit geldt overigens voor iedere groep van de orde n).

Eindige Abelse groepen kan men op canonieke wijze schrijven als direct product van een stel cyclische groepen waarvan de ordes een keten van delers vormen: $G \cong Z/(d_1) \oplus Z/(d_2) \oplus \ldots Z/(d_m)$ waarbij geldt dat $d_m | \ldots d_2 | d_1$. Als wij nu een grote multiset willen vinden zonder niet triviale nulsommen, dan ligt het voor de hand om van iedere factor een voortbrenger te kiezen en die even vaak als diens orde min 1 in de multiset op te nemen. De aldus geconstrueerde multiset omvat $d_1 + \ldots + d_m - m$ elementen en het is duidelijk dat zij niet kan worden uitgebreid zonder nulsommen te genereren. De vraag is of er alternatieve multisets zijn te vormen die geen nulsommen genereren die nog meer elementen bevatten. Wij koesterden het vermoeden dat dit niet het geval was.

Het maximale aantal elementen is uiteraard een constante die slechts afhangt van de structuur van de groep en dus geheel bepaald wordt door de eerder genoemde rij delers. Zij staat bekend (zoals wij later hebben ontdekt) onder de naam *Davenport Constante* en speelt een rol in de Algebraische getaltheorie.

Ons onderzoek liet zien dat het vermoeden geldt voor alle groepen waarvan de orde een macht van een priemgetal is, ongeacht het aantal cyclische factoren. Het vermoeden geldt ook voor alle groepen die het product zijn van twee cyclische factoren hetgeen zich laat bewijzen via een inductie naar het aantal optredende priemfactoren in de maximale orde. Helaas bleken beide resultaten reeds bekend te zijn in de literatuur: de wiskundige Olson was ons voor geweest.

In 1969 vond Cor Baayen geheel onverwacht een tegenvoorbeeld voor een groep met vijf cyclische factoren. Dirk Kruyswijk wist dit aantal later tot vier te reduceren. Dit maakte de vraag of het vermoeden geldt voor groepen met drie cyclische factoren nog interessanter, en ik moet helaas constateren dat veertig jaar later dit probleem nog steeds open staat. Wij hebben destijds via een analogon van ons inductie bewijs voor dimensie 2 een aantal positieve resultaten bewezen voor dimensie 3, maar waren daarbij bij het gebruik van de inductieve constructie beperkt tot ordes opgebouwd uit de priemfactoren 2, 3,

5 en 7 omdat het inductiebewijs structurele eigenschappen van de te componeren elementaire groepen nodig heeft die slechts voor deze kleine priemgetallen te verifieren waren (voor p=7 heb ik daar ooit nog eens uitgebreid aan mogen rekenen in Algol 60 op de EL X8 machine van het Mathematisch Centrum).

Helaas zijn onze resultaten nooit gepubliceerd buiten deze reeks rapporten. Publish or Perish gold in die dagen nog niet. Jarenlang heb ik een meesterkopie op mijn kamer bewaard om de verzoeken om overdrukken te kunnen honoreren die toch met enige regelmaat binnenkwamen.

Met betrekking tot dit project moet ik nog een aantal zaken vermelden. Onze resultaten voor het drie dimensionale geval zijn inmiddels uitgebreid: in de jaren 90 kwam ik in contact met een Chinees Weidong Gao die onze collectie kleine priemgetallen heeft weten uit te breiden met de eerstvolgende vier priemgetallen; helaas was zijn methode gecompliceerd en gaf geen duidelijke aanwijzing hoe dit verder dient te worden aangepakt. Het contact resulteerde wel in een invitatie voor een bezoek aan China in 2000; aan dit bezoek heb ik nog een eervolle benoeming als visiting professor aan de Petroleum University of China in Chang Ping over gehouden.

Het onderzoek vormt ook de basis van mijn doctoraalscriptie [7]. De verdediging daarvan in juni 1969 viel net in de periode dat nieuwe resultaten werden behaald zodat op het examen vooral is gesproken over een tweetal daags tevoren geschreven nieuwe rapporten en de scriptie zelf niet meer aan de orde kwam. Examens vonden in die dagen nog achter gesloten deuren plaats, zodat van dit feit vandaag nog slechts een verdere getuige in leven is: de toenmalige hoogleraar Frans Oort die ik vandaag in het publiek hoop aan te mogen treffen.

Tussen de reeks rapporten is er een die handelt over een uitbreiding van het probleem naar oneindige groepen, waarvoor uiteraard de vraagstelling dient te worden aangepast. Dit rapport is vermeldenswaardig omdat het hier de eerste publicatie in de wiskunde betreft van Hendrik Lenstra [8]. Van groter belang is een lemma van de hand van Kruyswijk dat in ons laatste rapport [9] is opgenomen dat vele jaren later een rol heeft mogen spelen in het bewijs van het bestaan van oneindig veel Carmichael getallen [10]. Als co-auteur van dit rapport sta ik dus (ten onrechte) bekend als iemand die een bijdrage heeft geleverd aan de oplossing van dit probleem uit de getaltheorie.

De hinde van Cerynea - *Abstracte Complexiteitstheorie*

De hinde van Cerynea was van grote schoonheid en kon pas door Heracles worden gevangen door haar in een sneeuwhoop te jagen. Alle reden dus om dit werk te koppelen aan een theorie van grote schoonheid.

Inmiddels had ik in juli 1969 het doctoraal examen behaald en was ik per 1 oktober 1969 zowel aan de Universiteit als aan het Mathematisch Centrum verbonden als medewerker - op beide plaatsen voor de halve werktijd. Ik was nog steeds werkzaam op het gebied van de zuivere wiskunde en het was de bedoeling dat ik zou promoveren bij Aida B. Paalman de Miranda en Frans Oort op een onderwerp dat in lag tussen de topologie en de algebra, meer specifiek binnen het vakgebied Algebraïsche Meetkunde.

Gedurende de hierop aansluitende twee jaren heb ik een aantal wandaden bedreven die tegenwoordig dodelijk zouden zijn geweest voor een Universitaire loopbaan. Mijn belangstelling was gewekt voor de meer theoretische aspecten van het gebruik en programmeren van computers. Het feit dat Ghica, inmiddels mijn vrouw, haar studie wiskunde een jaar na haar kandidaats had afgebroken en in plaats daarvan per oktober 1969 als programmeur in dienst was getreden bij de IBM, bezorgde mij een venster op deze wereld. Evenzeer de doorlopende contacten met mijn studiegenoot W.P de Roever die inmiddels na enige rondzwervingen door de zuivere wiskunde terecht was gekomen bij de Informatica hoogleraar van de Riet aan de Vrije Universiteit trok mij ook in de richting van dit vakgebied. Overigens gebruik ik hier de term “Informatica” ten onrechte want dat woord kende wij destijds niet. Voor zover er een onderzoeksgebied werd onderkend noemde men dat destijds gewoon Computer Science, en het is een tragische fout van de geschiedenis dat men deze laatste term niet heeft gehandhaafd, maar in plats daarvan is gevallen voor een

Gallicisme - nog afgezien van het feit dat het invoeren van een naam voor een vakgebied tot op de huidige dag niet heeft mogen leiden tot consensus over de inhoud ervan.

Het onderzoek naar krommen met een groot aantal automorfismen kwam hiermee niet van de grond, en na twee jaar viel er dan ook weinig vooruitgang te rapporteren.[2] Het gevaar dreigde dat ik mijn recht op promotie-uitstel voor de vervulling van de militaire dienstplicht ging verspelen. Gelukkig heeft het Mathematisch Instituut mij uit deze penibele toestand gered door mij in de zomer van 1971 een van de zeldzame onmisbaarheidverklaringen te bezorgen, en wel in een periode dat het allerminst duidelijk was of ik ooit nog een rol van betekenis voor dit instituut zou gaan spelen. Met deze onmisbaarheidverklaring werd uitstel uiteindelijk afstel, zodat ik mij nooit onledig heb hoeven te houden met het graven van schuttersputjes en vergelijkbare nutteloze zaken.

2). In feite is dit alleen maar gunstig geweest - het gezochte resultaat bleek naderhand reeds elders te zijn verkregen.

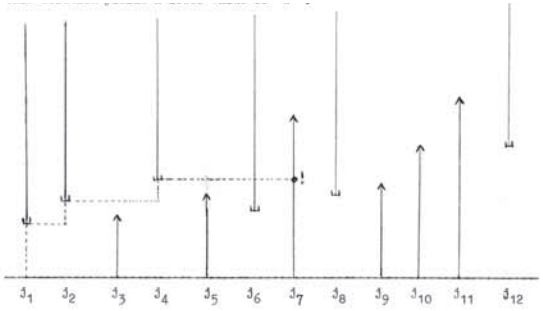
Voor haar werk werd Ghica regelmatig uitgezonden naar verre landen. Voorjaar 1971 moest zij voor 6 weken naar het IBM laboratorium in Endicott in upstate New York. De IBM regels verschaften haar een gratis retour voor een tussentijds bezoek aan huis. Wij wisten het zo te regelen dat in plaats daarvan ik zelf van de IBM een gratis retour kreeg in de omgekeerde richting om verder op eigen kosten daar een maand door te brengen. De universiteit van Cornell was dicht in de buurt en gezien mijn inmiddels verschuivende belangstelling had ik bedacht dat ik ter plekke een bezoek wilde brengen aan de afdeling Computer Science aldaar. Een bezoeker van de Groot, de hoogleraar Anderson, kende ter plekke de hoogleraar Juris Hartmanis en was bereid mij te introduceren. Het gevolg was dat ik eind maart 1971 mijn opwachting kon maken in een voor mij nieuw land en een mij geheel onbekende instelling bij deze mij geheel onbekende expert op het gebied van de Theoretische Informatica, in het bijzonder de Complexiteitstheorie.

Samen met John Hopcroft had Hartmanis zojuist de laatste hand gelegd aan een overzichtsartikel [11] over het onderzoeksgebied Abstracte Complexiteitstheorie. Dit vak is te zien als een uitbreiding van de Recursietheorie (een mij destijds wel bekend onderwerp) met een tweetal door Manuel Blum geïntroduceerde axioma's die het mogelijk maken om binnen de meest abstracte modelvorming voor berekenbaarheid die de binnen de Computer Science wordt gebruikt, inhoud te geven aan de intuïtie dat rekenen tijd kost en ruimte gebruikt voor opslag van gegevens.

Het artikel introduceerde mij in de destijds in Nederland volledig onbekende wereld van de Complexiteitstheorie. Het trok mijn volledige aandacht, niet alleen omdat het goed geschreven was, maar vooral omdat ik (zoals zal blijken een terugkerend thema) tegen een hinderlijke fout aanliep in de meest complexe algoritme die in het artikel wordt beschreven: de diagonalisatie

procedure die optreedt in het bewijs van de *Naming Theorem* bewezen door Mc Creight en Meyer in een artikel gepresenteerd op de STOC 1 in 1969 [12]. De fout bleek reparabel; in feite is niet meer nodig dan een zeer liberale interpretatie van datgene wat de auteurs hadden opgeschreven. Het koste mij echter gedurende de zomer van 1971 na terugkeer uit de USA vele weken alvorens ik de bewuste algoritme geheel had doorzien, en begreep hoe de fout diende te worden gerepareerd en ook hoe op basis van een strikte lezing een tegenvoorbeeld tegen de constructie kon worden verkregen. De gedurende dit onderzoek verkregen inzichten zijn deels verwoord in het voorwoord voor de leek in mijn proefschrift [13] en deels in het artikel gewijd aan de toepassingen van deze Mc Creight - Meyer algoritme dat ik heb geschreven voor TCS [14]. Maar de helderste illustratie van dit inzicht is naar mijn mening het onderstaande plaatje dat de berekening van de essentiële subroutine in deze algoritme illustreert; deze versie van de afbeelding komt uit een van mijn manuscripten voor mijn proefschrift.

This solution yields a lower value of z.



Deze ontmoeting met de Theoretische Informatica heeft er uiteindelijk toe geleid dat ik de traditionele zuivere wiskunde heb verlaten en mij heb kunnen storten in de destijds in Nederland onbekende complexiteitstheorie. Ik ben mijn toenmalige broodheren zeer dankbaar dat zij mij hebben toegestaan niet alleen dit staaltje van hoogverraad te plegen maar mij ook bij de realisering ervan hebben ondersteund. Ter geruststelling kan ik nog vermelden dat inspectie van artikelen die ik veel later heb geproduceerd zoals bij voorbeeld het overzicht over de theorie van de complexiteit van bilineaire vormen [15] aantoont dat de algebraicus in mij nog vele jaren heeft voortgeleefd.

Promoveren op dit onderwerp gaf uiteraard logistieke problemen. Toen ik voldoende resultaten had behaald die een proefschrift rechtvaardigden, zocht en vond ik een promotor in de persoon van een van de weinige Informatici die onze Universiteit destijds rijk was: prof. A van Wijngaarden. Cor Baayen was bereid als co-promotor de relevante bewaking van het proces op zich te nemen

terwijl de wetenschappelijke inhoud is bewaakt door de eerder genoemde Juris Hartmanis als co-referent - een inmiddels helaas afgeschafte rol bij het promoveren (de hedendaagse leescommissie is beslist geen adequate vervanging voor deze externe deskundige). Initiële resultaten kon ik reeds in 1972 presenteren op het eerste ICALP congres te Versailles (niet na reguliere selectie, maar via een ter plekke geregelde reserveplaats op de sprekerslijst). Een korte samenvatting is opgenomen in de proceedings van dit congres [16].

Inhoudelijke consultaties met Hartmanis waren niet frequent want het internet moest nog worden uitgevonden: de Atlantische Oceaan lag ertussen. Maar gedurende het jaar 1971-72 had Hartmanis een sabbatical in Bonn, alwaar ik hem twee keer heb mogen bezoeken, en hij is een keer op bezoek geweest in Amsterdam. In 1973 bezocht ik hem voor een week in Cornell om vast te stellen dat de inhoud toereikend was en daarna was het een kwestie van schrijven en volgde de verdediging in deze zaal op 18 september 1974. Het werk bezorgde mij een invitatie als spreker op de MFCS conferentie in 1975 in Tsjechoslowakije [17].

Achteraf moet ik helaas constateren dat mijn proefschrift een van de laatste dissertaties is geweest over dit onderwerp in de wereld: Albert Meyer heeft nog enkele studenten opgeleverd, in Jena, DDR, is Gerhard Lischke er op gepromoveerd, en daarna is er nog een student van Bob Soare geweest, Victor Bennison, die erin is geslaagd het vak zozeer te verwoorden in de terminologie van de klassieke recursietheorie dat het daarmee voor een simpele informaticus ontoegankelijk dreigde te worden. Daarnaast was inmiddels de hoofdstroom van de onderzoekers tot het inzicht gekomen dat deze prachtige abstracte theorie nooit het antwoord kon geven op de concrete vragen waarmee de Informatica destijds worstelde, zoals het inmiddels beruchte P vs NP probleem. Anders gesteld: toen ik erop promoveerde was het vak op sterven na dood, en het is dus geen groot verlies voor de mensheid geweest dat ik mijn toezegging om het proefschrift uit te werken tot een tweedelige uitgave in de MC Tract reeks niet ben nagekomen. Zoals ik reeds eerder aangaf is dit een fase van mijn leven geweest waarin ik nogal wat wandaden heb bedreven.

Het zwijn van Erymanthus - *de Stratified Trees*

Bij de uitvoering van dit werk werd Heracles gestoord door buitenstaanders. Wellicht is het dus passend dit werk te koppelen aan een onderwerp waarbij een kanttekening van een buitenstaander de inhoud van de publicaties aanzienlijk heeft beïnvloed.

Medio de zeventiger jaren, toen ik mijzelf nog beschouwde als wiskundige, combineerde ik een keer het nuttige met het aangename met een bezoek aan Parijs ter gelegenheid van het Seminaire Bourbaki. Ik herinner mij bij die gelegenheid een ontmoeting te hebben gehad met de wiskundige Zassenhaus. Dit was een remarkabele ontmoeting omdat het hier een onderzoeker betreft waarvan wij de naam slechts kenden uit een naar hem vernoemd lemma in de groepentheorie dat wij in ons tweede studiejaar waren tegengekomen. Het is bevreemdend om een wiskundige wiens resultaten je kent uit het basisonderwijs te ontmoeten, want in het algemeen hangen de namen die je in deze context tegenkomt aan wiskundigen uit een ver verleden en die plegen niet meer op de wereld rond te lopen.

De gelaagde bomen (stratified trees - in de wereld ook bekend onder de naam van Emde Boas bomen) treden op in een stuk onderzoek dat mij in de omgekeerde positie plaatst tegenover jonge Informatici, in het bijzonder in de USA: bij mijn bezoeken aan OOPSLA trof ik regelmatig jonge studenten aan die verbaasd waren de ontdekker in levende lijve tegen te komen van een gegevensstructuur die hen is onderwezen bij het basisonderwijs. Ik kan ook verwijzen naar de laatste editie van het standaardwerk van Cormen ea. [18] verschenen in 2009, waarin het gehele hoofdstuk 20 is gewijd aan de naar mij vernoemde bomen; de gebruikte 30 pagina's zijn er precies evenveel als die in het oorspronkelijke artikel [19].

De oorsprong van dit werk ligt andermaal in Cornell. In september 1974 had ik mijn proefschrift verdedigd, en in die tijd werden jonge Informatici aangemoedigd voor kortere of langere tijd zich verder te ontwikkelen aan de overkant van de Oceaan. NWO had daar destijds een speciaal programma van subsidies voor. Aldus ondersteund verbleef ik van oktober tot december 1974 te Cornell terwijl Ghica die drie maanden een uitgebreide interne nascholingscursus van de IBM volgde in het destijds nieuwe (en inmiddels opgeheven) IBM Education Centre in La Hulpe nabij Brussel. De zorg voor de twee katten en schildpadden in ons huis werd toevertrouwd aan de toenmalige gastbezoeker aan de VU, Ira Pohl en zijn toenmalige partner Tana Sommer.

Doel van het bezoek aan Cornell was om na de abstracte complexiteitstheorie ook kennis op te doen over het zich snel ontwikkelende gebied van de algoritmiek. Het klassieke leerboek van Aho e.a. [20] was net verschenen, en het leek mij een goede gelegenheid om in de omgeving van de medeauteur John Hopcroft mij te gaan verdiepen in dit onderwerp.

Bij het doorwerken van dit boek liep ik al in het vierde hoofdstuk aan tegen interessante problemen. Het gaat in dit hoofdstuk over gegevensstructuren voor het manipuleren van eindige verzamelingen.

U dient te beseffen dat in de Informatica, in tegenstelling tot de wiskunde, de verzameling geen basisbegrip is. Verzamelingen worden weliswaar uitgebreid gebruikt binnen het ontwerp en de implementatie van algoritmen, maar de visie erop wijkt sterk af van de visie van een wiskundige. Om te beginnen zijn verzamelingen altijd eindig, anders passen ze niet in een computer. Verder kijkt men in het algemeen naar verzamelingen met een daarop gedefinieerde lineaire ordening. En ten slotte is het niet de verzameling zelf maar de er op uit te voeren bewerkingen die bepalen hoe men de verzameling zal gaan representeren.

Een representatief voorbeeld is een priority queue. Dit is een structuur waarop men de volgende twee operaties moet kunnen uitvoeren: het toevoegen van een element, en het verwijderen van het kleinste element (aannemende dat de verzameling niet leeg is). Voor de hand liggende opslag methoden die ieder programmeur zal kennen, zijn arrays en lijsten, maar beide zijn voor deze toepassing minder geschikt: binnen een array kan men elementen invoeren en verwijderen, maar het lokaliseren van het kleinste element is problematisch, terwijl bij een gesorteerde lijst het juist weer lastig is een element toe te voegen als men niets weet over de positie die dat element in de ordening zal gaan innemen.

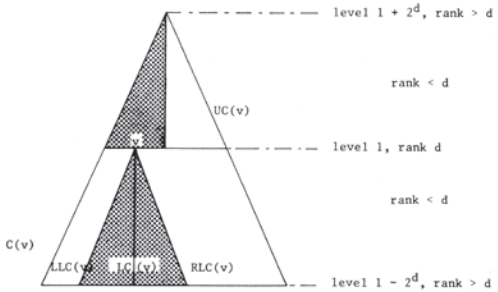
Er was in die dagen een aantal gegevensstructuren bekend waarmee beide operaties redelijk efficiënt zijn uit te voeren. Deze structuren die in het algemeen gebruik maken van binaire boomstructuren ondersteunen beide operaties

in een tijd orde $O(log(n))$ waarbij n de grootte van de verzameling is. Deze overhead $log(n)$ valt ook te verklaren als men zich realiseert dat gebruik makende van deze twee instructies een verzameling kan worden gesorteerd, en iedereen weet (en dat was ook in 1974 al bekend) dat sorteren van n elementen tijd $\Omega(n.log(n))$ kost.

Bij de gelaagde bomen kijken wij echter naar een speciaal geval. Wij beschikken over de extra informatie dat de elementen die in de verzameling terecht zullen komen allemaal behoren tot een vast universum gevormd door de getallen $0...u-1$. De gevensstructuur die ik in het najaar van 1974 ontdekte maakt het mogelijk om de genoemde operaties (in feite een veel uitgebreider repertoire aan instructies) uit te voeren in tijd $O(loglog(u))$, hetgeen een verbetering geeft in situaties waarin n groot is in vergelijking tot $log(u)$.

De aan de structuur ten grondslag liggende gedachte berust op een decompositie van het universum in een cluster van melkwegstelsels; ieder melkwegstelsel bevat een aaneengesloten interval van $\sqrt{u}$ elementen en het aantal melkwegstelsels is daarmee ook gelijk $\sqrt{u}$. Vervolgens kun je inzien dan met deze decompositie iedere actie op de verzameling zich laat ontleden in vergelijkbare acties op het niveau van de cluster of een individueel melkwegstelsel. Daarbij is het zo gesteld dat een van beide individuele deelacties altijd eenvoudig is en daardoor in constante tijd kan worden uitgevoerd. Bijvoorbeeld, om een element in te voegen kijk je in welk melkwegstelsel het element terecht moet komen; als dat stelsel niet leeg is volstaat een invoeging in het bewuste stelsel maar behoeft de cluster geen aanpassing. Zo nee, dan is het invoeren van een eerste element in het melkwegstelsel eenvoudig, maar daarna moet het stelsel zelf worden ingevoerd in de cluster.

In termen van de bomen laat deze constructie zich illustreren door een (binaire) boom te splitsen in een topboom waarvan ieder blad de wortel is van een bodem boom; top- en bodem bomen hebben de halve hoogte van de oorspronkelijke boom. U ziet deze splitsing afgebeeld in de onderstaande figuur, afkomstig uit de FOCS 16 presentatie van mijn resultaten. De figuur verwijst naar een nog te complexe methode: de splitsing in linker en rechter subbomen die de figuur illustreert is geheel overbodig en die is in latere versies dan ook niet meer terug te vinden.



The canonical subtrees of v. R(v) is the shaded area.

Deze decomposities geven voor alle relevante bewerkingen een recurrentie voor de rekentijd $T(u)$ van de vorm $T(u) = T(\sqrt{u}) + O(1)$ waarvan de oplossing wordt gegeven door $T(u)=O(loglog(u))$.

Helaas kon ik deze gedachte in 1974 nog niet zo helder over het voetlicht tillen. De methoden maken duidelijk gebruik van recursie, maar als je het oorspronkelijke rapport uit Cornell [21] ter hand neemt moet je constateren dat ik destijds nog geen elegante recursieve definitie voor een van de belangrijke operaties (het verwijderen van een element) wist te geven.

Een ernstiger probleem werd veroorzaakt door een kritische opmerking van Hopcroft: in mijn originele aanpak gebruik ik een tweedimensionaal array, maar om dat te adresseren moet een computer beschikken over een vermenigvuldigingsinstructie en die is (overigens op goede gronden) niet opgenomen in het bij deze theorie gebruikte machinemodel van de Random Access Machine. Om aan dit bezwaar tegemoet te komen besloot ik alle berekeningen die niet waren toegestaan te vervangen door het opzoeken van het resultaat ervan in een bijbehorende collectie tabellen, met het onaangename gevolg dat zowel het geheugenbeslag van mijn gegevensstructuur als de initialisatie tijd ervan toenamen tot $O(u.loglog(u))$ gemeten in computer woorden resp. instructies.

Teruggekeerd in Nederland verzorgde ik samen met de toenmalige hoogleraar informatica Th.J. Dekker een cursus onder de naam Programmeermethoden. In deze cursus konden de betrokken docenten aandacht besteden aan door hen zelf te kiezen speciale onderwerpen (voor mij was dat uiteraard een stukje algoritmiek en complexiteitstheorie), terwijl de studenten werden geacht een klein project uit te voeren. Ik heb bij een andere gelegenheid [22] uitgebreider kunnen ingaan op de fraaie resultaten die uit deze cursus zijn voortgekomen. De implementatie van mijn gegevensstructuur is een van deze producten.

Ik was bepaald niet tevreden over de door mij ontworpen pseudocode voor de verschillende instructies; in het bijzonder het ontbreken van een recursieve versie van de Delete instructie was mij een doorn in het oog. Goede redenen derhalve om een paar studenten aan het werk te zetten en die vond ik bij het college programmeermethoden in de personen van de heren Rob Kaas (thans hoogleraar bij de Economen aan deze instelling) en Erik Zijlstra. Zij hebben zich op gepaste wijze gekweten van hun taak zodat ik bij de presentatie op het FOCS congres in 1975 te Berkeley [23] gebruik heb kunnen maken van hun code. Zij zijn ook medeauteurs geworden van het uiteindelijke tijdschriftartikel [24], hetgeen voor beide een eerste publicatie is geworden (en tevens voor ons drieën een belangrijke bron van citaties - iets waaraan onze behoorden tegenwoordig nogal belang schijnen te hechten). In Google scholar zult U bij het invoeren van de naam van Emde Boas dit artikel bovenaan in de lijst aantreffen.

Om het superlineaire geheugenbeslag weg te werken was nog een extra idee nodig. Opnieuw wordt het Universum opgesplitst maar nu in stelsels van orde $loglog(u)$. De cluster gebruikt de oude structuur maar omdat het aantal elementen inmiddels is gereduceerd tot $u/loglog(u)$ komt het geheugen uit op $O(u)$. Voor de stelsels kan men een willekeurige domme implementatie kiezen (zoals een eenvoudige lijst); de grootte van een stelsel is zo gering $O(loglog(u))$, dat zelfs met lineaire overhead de rekentijd voor de gehele structuur begrensd blijft tot de gezochte $O(loglog(u))$.

Ik moet bekennen dat ik met de publicatie van deze verbetering in Information Processing Letters [25] een domme fout heb gemaakt, en wel het niet onderkennen van de mogelijkheden van de door mij gebruikte methode. Deze techniek is in de late jaren 70 uitgebreid gebruikt o.a. in het werk van mijn collega's Jan van Leeuwen en Mark Overmars.

Verder valt op dat het theoretische bezwaar van Hopcroft voor vele informatici geen enkele rol blijkt te spelen. Diverse auteurs meenden mijn resultaat te kunnen verbeteren door de adresberekeningen uit te voeren in plaats van ze te coderen in een tabel. Mijn oorspronkelijke implementatie kan worden gezien als een implementatie op een pointermachine en voor dat model is bewezen dat mijn structuur optimaal is. Ten slotte kan ik niet nalaten te vermelden dat een bekend citaat van D.E.Knuth over programmacorrectheid: *Beware of bugs in the above code; I have only proved it correct, not tried it* terug is te vinden in een classroom note waarin hij mijn gegevensstructuur bespreekt.

De stier van Kreta - *Semantiek van programma's*

De stier van Kreta was een cadeau van Poseidon aan koning Minos, bestemd om te worden geofferd. Minos was echter zo perfide een andere stier te offeren, waarna Poseidon het origineel trof met razernij, zodat deze het eiland verwoestte totdat Heracles met grof geweld het beest tot de orde wist te roepen. Zo is de semantiek van programma's een probleemgebied waarin de Informatica zich regelmatig van haar dolle kant laat kennen.

In 1969 ontwikkelden Dana Scott en Jaco de Bakker de op domeintheorie gebaseerde semantiek [26] voor recursieve procedures die het uitgangspunt vormde voor een uitgebreid onderzoeksprogramma op de Informatica afdeling van het Mathematisch Centrum. Mijn studiegenoot W.P de Roever was in die periode aan deze afdeling verbonden waar hij bij de Bakker zijn promotie-onderzoek heeft uitgevoerd over de polyadische relationele semantiek voor recursieve programma's. Ik was naast mijn aanstelling aan de UvA gedurende deze periode nog steeds verbonden aan de afdeling Zuivere Wiskunde en als zodanig in principe slechts een toeschouwer bij dit onderzoeksprogramma.

Op een voor mij gebruikelijke wijze ben ik echter na 1972 toch bij dit programma betrokken geraakt. Ik was in die periode deelnemer van een Theoretisch Informatica symposium dat door G. Rozenberg werd georganiseerd in Utrecht, alwaar regelmatig recent onderzoek over semantiek van programma's werd gepresenteerd. Wat mij uit die periode is bijgebleven is de indruk die ik ervaar bij vele onderzoekers bij hun eerste kennismaking met dit onderwerp: Hoe kunnen mensen zo moeilijk doen over kwesties die intuïtief zo duidelijk lijken te zijn... .

De directe aanleiding om mij actiever met dit onderwerp te gaan bemoeien is een artikel van de Bakker [27]: zijn bijdrage aan het symposium in januari

1972 t.g.v. van het 25 jarig bestaan van het Mathematisch Centrum (bijna een jaar eerder) en het 25-jarige ambtsjubileum van mijn Promotor A. van Wijngaarden op het Mathematisch Centrum. Ik bezocht dit symposium, en na afloop nam ik de proceedings mee als vakantielitteratuur bij een reis naar het nieuw gebouwde vakantieverblijf van de familie Lubsen in Carezza in de Dolomieten.

Aldaar trachtte ik mijn ega te overtuigen van de schoonheid van deze theorie (die ook voor haar als programmeur bij IBM relevant zou moeten) zijn door haar dit artikel te laten lezen. Helaas liep zij vast in de technische details, en dat was niet ten onrechte, aangezien ik al vrij snel tegen een problematische maar reparabele fout in het bewijs aan liep. Een goede reden om na terugkeer contact met de Bakker op te nemen, die, na de nodige initiële twijfels zich liet overtuigen van mijn gelijk. Dit was de eerste van een reeks consultaties die wij de daarop volgende jaren hebben gehad, waarbij ik een groot aantal van zijn artikelen mocht doorspitten voordat ze de wereld in werden gestuurd.

In de vroege jaren 70 kwamen regelmatig bezoekers op het Mathematisch Centrum die zich elders bezig hielden met programma semantiek. Zo konden wij in het najaar van 1976 V. Pratt verwelkomen die ons liet kennismaken met de zojuist aan MIT ontwikkelde Dynamische Logica. In dezelfde tijd waren wij op de afdeling Zuivere Wiskunde, mede op instigatie van mijn toenmalige opvolger als student assistent Theo Janssen, ons gaan verdiepen in de Montague grammatica voor de natuurlijke taal.

In deze tijd worstelde men met een lastig technisch probleem binnen de semantiek van programma's: het geven van een correcte semantiek in de stijl van Hoare voor toekenningsopdrachten aan array elementen en pointers. Voor zover daar al regels voor waren voorgesteld waren deze complex en weinig intuïtief, zodat het lastig was om de correctheid ervan in te zien.

In de voordracht van Pratt werd naast een aantal andere onderwerpen ook een voorstel om dit probleem op te lossen gepresenteerd. Na afloop van de voordracht kwam Theo met de suggestie dit probleem aan te pakken door toepassing van de Intensionele logica uit de Montague semantiek op de artificiële wereld van de computer toestanden. Het voorstel bleek levensvatbaar. Wij konden met onze methode het probleem van assignments aan pointers en array elementen behandelen, en wij besloten onze bevindingen in te zenden naar de ICALP conferentie in 1977 te Turku. Om door de selectieprocedure te komen moesten wij nog wel een scherpzinnige referee tevreden stellen door een aanmerkelijk complexer model in ons artikel op te nemen, maar dat probleem bleek na enige onderlinge twisten en worstelpartijen oplosbaar [28]. Het is dit project geweest dat voor Theo aanleiding is geweest mij als een van zijn promotors te kiezen en aldus een van mijn vroege promovendi te worden.

Gedurende de daarop aansluitende vijf jaren kwamen wij meer en meer tot het inzicht dat de aantrekkelijkheid van de Montague semantiek in vergelijking met andere vormen van semantiek voor de natuurlijke taal gelegen was in het feit dat in deze semantiek het principe van de compositionaliteit op strikte wijze wordt gehanteerd. Theo ontwikkelde een scherpe intuïtie om een correspondentie te leggen tussen mislukte pogingen om het fragment van Montague uit te breiden met nieuwe taalelementen en inbreuken tegen de compositionaliteit die in deze uitbreidingen terecht waren gekomen. In Theo's uiteindelijke proefschrift staat dan ook het thema compositionaliteit centraal en is de toepassing op programmasemantiek niet meer dan het laatste hoofdstuk. Onze samenwerking aan dit project heeft mij echter voor jaren binnen de theoretische gemeenschap de status van profeet van de compositionaliteit bezorgd.

De paarden van Diomedes - *Epistemische Logica*

Paarden die in zodanige mate carnivoor zijn dat ze met mensenvlees gevoederd dienen te worden strookt niet met onze kennis van de biologie. Maar mogen wij uit het feit dat wij weten dat deze legende daarom wel onwaar moet zijn ook concluderen dat zij onwaar is…

Velen onder U zullen bekend zijn met de puzzel van de bemodderde kleutertjes (ook wel bekend als de puzzel van de ontrouwe echtgenoten). Een geciviliseerde weergave van deze puzzel is als volgt te formuleren: U staat met uw partner in een afgesloten ruimte terwijl een perfide experimentator op uw beider voorhoofden een positief geheel getal heeft geschreven. Ieder van U beiden kan het getal van de partner lezen, maar het eigen getal is onzichtbaar ten gevolge van de beperkingen die de menselijke anatomie met zich meebrengt; verder zijn er ook geen spiegels in de ruimte aanwezig.

De opgave is de waarde van het eigen getal te achterhalen, waarbij iedere vorm van rechtstreekse communicatie met uw partner is verboden. Dit is een onmogelijke opgave, ware het niet dat de bedenker van deze tortuur U een belangrijke aanwijzing heeft gegeven: de twee getallen zijn opeenvolgend. Als uw partner met het getal 53 rondloopt, weet U dus dat uw eigen getal 54 of 52 is. Ook met deze kennis lijkt de opgave vooralsnog onoplosbaar. In het verdere verloop van dit experiment vraagt de sadistische experimentator iedere minuut of een van U beide reeds het juiste antwoord kan geven, want eerder zal hij U niet laten vertrekken. U wordt hierbij beiden geacht een rationeel en tot perfect redeneren opgevoed individu te zijn.

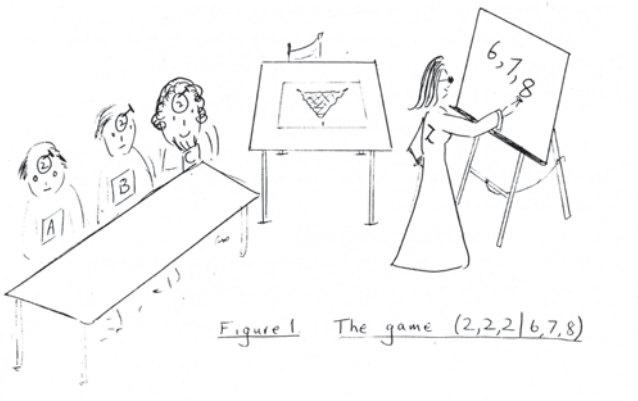
Het probleem doet zich nu voor dat een wiskundige analyse van dit probleem een oplossingsmethode aandraagt, die strijdig lijkt te zijn met onze intuïtie. De methode leert ons dat in het geval dat de getallen gelijk 53 en 54

zijn (dus U draagt het grootste getal) U na 52 vragen van de experimentator onbeantwoord te hebben gelaten kunt melden dat U hebt vastgesteld met het getal 54 rond te lopen en daarmee een einde te maken aan deze beproeving. De methode schrijft voor dat in de situatie (k,k+1) de drager van het getal k+1 op de k-e vraag van de experimentator het juiste antwoord geeft. De correctheid van deze methode bewijzen wij met het principe van de volledige inductie. Als het paar (1,2) optreedt weet diegene die de 1 ziet dat hijzelf niet het getal 0 kan dragen want dat is immers niet positief. Hij kan dus de eerste vraag van de experimentator reeds correct beantwoorden. Als iemand die bij zijn partner een 2 ziet constateert dat deze partner niet bij de eerste vraag reageert, kan hij constateren dat hijzelf geen 1 kan dragen, dus moet hij wel met 3 rondlopen. In de inductiestap geldt dat iemand die bij zijn partner het getal k ziet, op grond van het feit dat de partner geen antwoord geeft bij de k–1-e vraag, kan concluderen dat hij niet rondloopt met het getal k–1 en daarom moet zijn getal wel gelijk k+1 zijn.

Het vervelende is dat naarmate de getallen groter worden een naïeve redenering ons leert dat het zo toch niet kan werken. Als U een 53 ziet is het eenvoudig in te zien dat noch uw partner, noch uzelf bij het begin van het spel beschikt over voldoende informatie om het spel te kunnen beëindigen; sterker nog: U kunt beargumenteren dat U beide intelligent genoeg bent om dat voor elkaar vast te stellen, zodat U van te voren al weet dat geen van U beide in de eerste ronde zal reageren. Wat heeft het dan voor zin om deze eerste ronde te spelen als U toch al beide weet dat er niets zal gebeuren…?

Het moge duidelijk zijn dat de twee redeneringen leiden tot conclusies die met elkaar in strijd zijn, dus een van beide redeneringen moet wel fout zijn. Het probleem is om te bepalen welk van beide argumentaties niet deugt.

Een wat uitgebreidere versie van deze paradoxale puzzel is te vinden in het liber amicorum dat in 1977 werd aangeboden aan Hendrik Lenstra bij de gelegenheid van zijn promotie aan deze instelling [29]. In dit geval gaat het om drie slachtoffers die de informatie meekrijgen dat de som van de getallen die zij dragen behoort tot een verzameling van drie gegeven getallen. De originele afbeelding uit het artikel is hiernaast afgedrukt.



Aangezien ik een van de vijf redacteuren van deze bundel was (samen met J.K. Lenstra, F. Oort, A.H.G. Rinnooy Kan en T.J. Wansbeek) bleef deze puzzel in mijn gedachten rondspoken. Met het onderwerp epistemische logica hielden wij ons in die dagen echter niet bezig in Amsterdam zodat de gedachte dat in die richting wellicht een antwoord te vinden zou zijn niet bij ons opkwam.

Rond 1978 ontwikkelden de heren Stokhof en Groendendijk, beide deelnemers en activisten in ons Montague Seminar, hun theorie over de betekenis van vragen gebaseerd op partities in plaats van proposities waarop zij later zijn gepromoveerd (ik heb destijds in ons seminar met een gemeen tegenvoorbeeld tegen een eerdere versie van de theorie de beide heren nog een zet in de goede richting mogen geven). Geconfronteerd met deze theorie vroeg ik de beide heren of zij wellicht in staat zouden zijn met gebruikmaking van hun systeem te komen tot een formele beschrijving van de situatie in de puzzel die de juistheid van het inductie antwoord niet alleen begrijpelijk maar ook wiskundige noodzakelijk en bewijsbaar zou maken. Ik hoopte en verwachte in het bijzonder technieken uit de theorie over programmacorrectheid te kunnen gebruiken. De vraag viel in vruchtbare aarde en leidde uiteindelijk tot een gezamenlijke presentatie op het derde Amsterdam Montague Colloquium in 1979 [30].

Als er een onderwerp in mijn loopbaan geweest is waarvan ik moet constateren (achteraf) de boot te hebben gemist dan betreft het inschatten van het belang van deze puzzel en de oplossing die wij ervoor trachtten te vinden. In onze visie op de wetenschap ging het over een totaal onbelangrijk en irrelevant onderwerp: een puzzel uit de recreatieve wiskunde. Recreatieve wiskunde werd niet serieus genomen en hetzelfde gold voor meer wiskunde die met spelletjes te maken had.

Het vervolg van deze geschiedenis speelt zich af op het ICALP congres in 1984 te Antwerpen. In die tijd had zich een traditie gevormd dat ik op dat congres de organisatie op mij nam van de zogeheten "wildcat session", een uurtje waarin iedereen die nog wat wilde presenteren daartoe de gelegenheid kreeg. De (enige) belangstellende in 1984 was een vertegenwoordiger van IBM San Jose Research, Ron Fagin, die graag van de gelegenheid gebruik wilde maken om iets te laten zien van een prachtige theorie die hij samen met zijn collega's Moshe Vardi en Joe Halpern en diens student Yoram Moses aan het ontwikkelen was over het redeneren over kennis.

Tijdens deze voordracht werd ik verrast door het feit dat, zeker in de eerste helft ervan, alles wat Fagin vertelde afkomstig had kunnen zijn uit mijn eigen presentatie van 5 jaar eerder: motivatie, probleemstelling en plan van aanpak. Echter, voor deze IBM'ers was de motivatie geen recreatieve wiskunde maar harde informatica, te weten de theorie van gedistribueerde berekeningen.

Hierbij gaat het over het redeneren over protocollen voor communicatie en het nemen van beslissingen door een systeem van computers in een netwerk waarbij niet mag worden verondersteld dat communicatie altijd feilloos verloopt. Boodschappen kunnen worden vertraagd, zoekraken, of in het ergste geval worden verwisseld of willekeurig worden gewijzigd. Het was gebruikelijk om correctheidsanalyses over deze protocollen te voeren in termen van kennis die een processor heeft over de toestand van een andere processor, waaronder inbegrepen de kennis van deze andere processor over de toestand van een derde processor en zo voort. Deze redeneringen waren echter inherent informeel, en kenden aan computersystemen antropomorfe eigenschappen toe die deze systemen volstrekt niet bezitten. De uitdaging was desalniettemin een formeel acceptabele basis voor deze redeneringen te geven.

Het was uiteraard minder aangenaam te zien dat de IBM'ers verder waren gekomen op het punt waar wij vijf jaar eerder waren vastgelopen. Hun voornaamste stuk gereedschap was het gebruik van de Kripke semantiek voor de epistemische logica als een speciaal geval van een multi-modale logica; tegenwoordig in onze omgeving standaard kennis, maar rond 1979 deden wij daar nog niet erg veel aan. Omgekeerd was Fagin zeer verrast door mijn mededeling dat wij reeds vijf jaar eerder in Amsterdam met deze problematiek bezig waren geweest.

Het resulterende contact heeft belangrijke gevolgen gehad voor de verdere ontwikkelingen. Onze Amsterdamse onderzoekers zijn vanaf het begin intensief betrokken geweest bij de opzet van de congres serie TARK (destijds een afkorting voor Theoretical Aspects of Reasoning about Knowledge), begonnen in 1986, die in eerste instantie substantieel is ondersteund vanuit IBM; de toepassing op de theorie van gedistribueerde systemen transformeerde de

wiskundige studie van deze modellen van kennis in een klap van irrelevante recreatieve wiskunde en filosofie tot goed gesubsidieerde Informatica, waarvoor veel geld beschikbaar kwam. De eerste vijf bijeenkomsten van deze serie in Asilomar heb ik allemaal mogen bijwonen, en de eerste bijeenkomst buiten de USA hebben wij in 1996 in Nederland mogen organiseren in Renesse. Het onderwerp heeft jarenlang een centrale rol gespeeld in het programma van het ILLC (en haar voorganger ITLI dat rond 1985 vorm begon te krijgen).

Toen in 1995 de resultaten van de IBM'ers hun neerslag vonden in het standaard leerboek van de genoemde vier auteurs [31] hebben wij dat boek uiteraard gebruikt bij ons eigen onderwijs. Ook de hedendaagse focus op spelen en hun relatie tot de logica en de taal ligt in het verlengde van deze eerdere revolutionaire verandering van de positie van de epistemische logica voor de Informatica en de taalkunde.

De roofvogels van Stymphalus - *Roosters en Roosterreductie*

De roofvogels van Stymphalus waren tamelijk onaangename creaturen met koperen bekken en snavels die Heracles uiteindelijk wist te overwinnen met giftige pijlen - een werk derhalve dat zich gemakshalve laat koppelen aan een geschiedenis die deels berust op een keten van fouten…

Roosters zijn discrete ondergroepen van maximale rang in de additieve groep van een algebraisch getallenlichaam, en roosterreductie is een rekenmethode om voor een dergelijk rooster een prettige basis te vinden. U zult zich wellicht afvragen hoe een dergelijk onderwerp te plaatsen valt in een fase in mijn leven waarin ik de zuivere wiskunde al een kleine tien jaar niet meer had bedreven. Het betreft hier dan ook een onderwerp waar het feitelijke werk is verricht door anderen: de gebroeders Hendrik en Arjen Lenstra en Laszlo Lovász. Het resultaat is de bekende LLL algoritme voor roosterreductie en de toepassing daarvan in een polynomiale tijd algoritme voor de factorisatie van polynomen [32].

Toen in 2007 in Caen een congres werd georganiseerd om de 25e verjaardag van deze algoritme te vieren ben ik in de gelegenheid geweest om deze geschiedenis in details uit te leggen aan het publiek, daarbij gesteund door de drie auteurs van het beroemde artikel die ieder verslag deden van hun eigen inbreng. Een weergave van deze history session van het LLL+25 congres is te vinden in het artikel van Ionica Smeets [33]. Ik zal het bij deze gelegenheid dus maar kort houden.

De oorsprong van mijn participatie aan de totstandkoming van dit resultaat ligt deels in het al eerder genoemde college Programmeermethoden dat ik in de jaren 70 samen met Dekker verzorgde aan de Universiteit van Amsterdam. Hendrik Lenstra had voor zijn eigen promotieonderzoek een lijst van

polynomen geproduceerd waarvan hij zich afvroeg of sommige daarvan wellicht eenzelfde getallenlichaam voortbrachten en dit probleem kon worden opgelost door polynomen te factoriseren over algebraische getallenringen, een destijds uitgebreid onderzocht onderwerp. Om Hendrik te steunen leek mij dit een passend project voor opname in de lijst projecten bij Programmeermethoden, en het werd in dankbaarheid aanvaard door een drietal studenten waaronder Arjen Lenstra.

Zelf raakte ik enige tijd later geïnteresseerd in de complexiteit van een aantal problemen over lineaire vergelijkingen over verschillende getaldomeinen. Resultaten over dit probleem stonden op verstrooide plaatsen in de literatuur en ik wilde ten behoeve van een geinviteerde voordracht op het FCT congres in 1979 in Wendisch Rietz, DDR, deze resultaten in een helder schema samenvatten. Ik meende bovendien een open entry in dit schema te hebben opgelost.

Gedurende dit jaar bleek er helaas van alles mis te zijn met mijn inmiddels ingediende bijdrage voor dit congres [34]. Het open geval bleek reeds eerder te zijn gepubliceerd, zij het buiten de informatica. Een aantal velden in mijn schema bevatten versies van het Lineaire programmeringprobleem waarvan juist dat jaar door Khachiyan was aangetoond dat het oplosbaar was in polynomiale tijd, waarmee de status "equivalent met LP" uit het schema kon worden verwijderd. Enkele storende typo's in mijn manuscript volstonden om de ramp te completeren.

Voor de presentatie op het congres had dit geen fatale gevolgen; ik kon mijn tijd nuttig besteden door de congresgangers te informeren over de hun nog niet bekende Elipsoide methode van Khachiyan, gebruik makend van een heldere presentatie van deze algorime van de hand van Gacz en Lovázs die als Stanford rapport was verschenen [35].

Later in 1979 ontving ik een brief van de Italiaan A. Marchetti-Spaccamela, met vragen over mijn artikeltje en een herinnering aan het feit dat ik een openstaande uitnodiging had voor een reis naar Rome. Tijdens deze reis naar Rome hebben we zitten puzzelen over het probleem om te bepalen of een gegeven driehoek in het platte vlak al dan niet een geheeltallig punt omvat. Een probleem waarin ik meende iets te herkennen van kettingbreuken. Na terugkeer legde ik het neer bij Hendrik Lenstra die mij ter plekke liet zien dat het probleem reeds was opgelost door Gauss. Ik heb deze oplossing in een brief doorgestuurd naar Marchetti maar die bleek later dat jaar mijn brief niet te hebben begrepen, weshalve wij andermaal op bezoek gingen bij Hendrik voor nadere uitleg. Naar aanleiding van dit bezoek ontdekte Hendrik zijn Roosterreductiealgoritme, die een bouwsteen vormt voor een polynomiale oplossing van geheeltallige lineaire programmeringproblemen in vaste dimensie. Lovász

liet een jaar later zien dat het roosterreductie gedeelte van deze oplossingsmethode polynomiaal is voor willekeurige dimensie. Arjen Lenstra had inmiddels een factorisatiemethode ontwikkeld waarvoor roosterreductie de hoofdmoot van de rekentijd vraagt, zodat hij, na ontvangst van de brief van Lovász kon vaststellen dat polynoomfactorisatie van geheeltallige polynomen in polynomiale tijd mogelijk is (modulo het irritante subprobleem van het factorisren van het gehele getal dat bekend staat als de inhoud van het polynoom).

De details van deze geschiedenis kunt U nalezen in het genoemde artikel van Ionica Smeets. Mijn voornaamste rol gedurende de zomer van 1981 bestond uit het verkondigen van Hendriks resultaat over de geheeltallige lineaire programmering op een aantal instituten en congressen die ik dat jaar heb bezocht. Een tweede bijdrage is het stellen van een probleem: de complexiteit van het beslissingsprobleem of in een rooster een niet nul vector bestaat waarvan de lengte een gegeven grens niet te boven gaat. Dit probleem is NP volledig als de lengte van een vector gemeten wordt in de max-norm maar het geval voor de Euclidische norm is een open probleem gebleven. Nadat Hendrik de fout had gevonden in mijn manuscript waarin ik meende te hebben bewezen dat het probleem ook voor de Euclidische norm NP-volledig was resteerde slechts een NP-volledigheidsbewijs voor het inhomogene geval (bestaat er een roosterpunt binnen gegeven afstand van een gegeven punt in de ruimte).

Deze resultaten werden opgeschreven in een rapport [36] van het Mathematisch Instituut vooruitlopende op de spoedig verwachte finale oplossing. Dit rapport is een van mijn meest frequent opgevraagde ongepubliceerde resultaten; in Google scholar verschijnt het op de derde positie als U de naam van Emde Boas invoert. Daarom heb ik enkele jaren geleden, nadat al mijn exemplaren op een meester-kopie na waren uitgedeeld, het rapport maar gedigitaliseerd en op mijn website geplaatst samen met het al evenmin gepubliceerde origineel van Hendriks oorspronkelijke artikel over de geheeltallige lineaire programmering waarin zijn oorspronkelijke roosterreductie algoritme is te vinden - in de tijdschrift versie gebruikt hij immers de roosterreductiemethode van Lovász.

Ik wil bij deze gelegenheid graag een tweetal kanttekeningen herhalen die ik ook heb uitgesproken in mijn voordracht te Caen.

Alle onderzoekers die bij dit project betrokken zijn geloofden aanvankelijk dat de gevonden polynomiale factorisatiemethode niet kon bestaan; de gangbare opvatting was dat dit probleem exponentiële rekentijd zou vragen maar dat onze kennis ontoereikend was om dat te bewijzen. Arjen heeft het op dit punt over de *Zassenhaus trap*. Toen de resultaten in de richting van het tegendeel wezen is er ook uitgebreid gezocht naar de fout in het zich ontwikkelende bewijs; de conclusie kon immers niet waar zijn. U moet zich voorstellen wat de

gevolgen zijn van een dergelijke appreciatie van het probleemgebied gezien tegen de achtergrond van het huidige klimaat van projectgebaseerd onderzoek. Een onderzoeksvoorstel om te zoeken naar een polynomiale factorisatiemethode zou, met de kennis van 1980, genadeloos worden afgekeurd. Het is derhalve goed om te constateren dat er nog altijd resultaten worden gevonden die tegen de heersende opvattingen ingaan en buiten de traditioneel gesubsidieerde projecten worden behaald.

Verder wil ik in herinnering brengen dat ik in mijn voordracht te Caen een veelheid van oude documenten kon vertonen (allemaal op papier) die, gesteld dat ik over 25 jaar een vergelijkbare voordracht zou willen geven over onderzoek dat heden wordt uitgevoerd, mij niet tot beschikking zouden staan. Dit soort informatie is tegenwoordig allemaal digitaal en we zullen ongetwijfeld moeten constateren dat over 25 jaar de bewuste files weggegooid, onvindbaar, of vanwege veranderingen in de software onleesbaar zullen blijken te zijn. Mijn collega die tegen die tijd een verhaal wil houden over ons onderzoek van rond 1980 verkeert helaas in weinig betere omstandigheden - bij de recente verhuizing van ons instituut zijn immers grote delen van de daartoe noodzakelijk te bewaren archieven ten prooi gevallen aan de opruimwoede opgeroepen door de opdracht te verhuizen naar een nieuwbouwcomplex waarbinnen geen ruimte beschikbaar is voor een ordentelijke privébibliotheek, en zeker niet voor dit soort artefacten uit het verleden. Ik kan niet nalaten te vermelden dat ik heb getracht mijn eigen archieven voor het grootste deel te redden, maar die liggen thans opgeslagen in 180 dozen in een Shurgardloods in mijn woonplaats, uiteraard op mijn eigen kosten, en zij zijn daarmee helaas slecht toegankelijk.

De gordel van Hippolyte - *Prolog en Databases*

Volgens de overlevering was Heracles bepaald niet handig in zijn omgang met de dames. Ik heb daar gelukkig minder problemen mee gehad.

Het nu te bespreken onderzoek komt voort uit een project dat ik heb mogen uitvoeren in samenwerking met Ghica. De wortel ligt in de revival die het in de zeventiger jaren op sterven na dood verklaarde gebied van de Artificiele Intelligentie in de jaren tachtig mocht ondergaan op basis van de initieel goede resultaten behaald met Expert Systemen en, niet in het minst, het propagandaoffensief dat gevormd werd door het vijfde generatie project waarmee Japan zich trachtte omhoog te werken naar de top in de Informatica. Ik kan het verhaal bij deze gelegenheid beperkt houden aangezien dit een stuk geschiedenis betreft waarover ik 12 jaar geleden reeds uitgebreid heb gerapporteerd in een geinviteerde voordracht op de SOFSEM in Jasna, Slovakije in 1998 [37].

Het onderwerp van de Deductieve Databases is gelegen op het overgangsgebied tussen de Database technologie, de Kunstmatige Intelligentie en het Logisch Programmeren in de taal Prolog. Bezien vanuit de laatste twee perspectieven gaat het om het ontwikkelen van programmatuur voor logische inferenties binnen een goed hanteerbaar en efficient te implementeren fragment (de Horn Clause logica) dat voor een ruime klasse van toepassingen voldoende uitdrukkingskracht blijkt te bezitten. Vanuit Database perspectief gaat het erom om de bestaande technologie van de gegevensbanken op een hoger niveau van abstractie aan te spreken met behoud van de voordelen die deze technologie te bieden heeft op de aspecten van efficientie, persistentie van de gegevens, en de bruikbaarheid in een multi-user omgeving. In de ideale wereld zou het mogelijk moeten zijn het ondervragen van een gegevensbank te programmeren in Prolog, waarna het resulterende programma mechanisch vertaald wordt naar code die regelrecht door het gegevensbanksysteem kan worden geïnterpreteerd.

In de vroege jaren 80 is er uitgebreid onderzoek verricht op het thema *Logic and Databases*, maar dat betrof primair theoretisch werk. In principe wisten de onderzoekers op dit gebied tot in details hoe een dergelijke vertaling van logica naar database programma's er uit zou moeten zien, maar het leek onmogelijk om een dergelijk systeem ook echt te realiseren. En voor zover men al iets implementeerde was dit gebaseerd op de *tuple at a time* aanpak, die vanzelfsprekend wel moest resulteren in een systeem dat de rekenkracht van de database volstrekt onvoldoende zou aanspreken.

Achteraf gezien meen ik te moeten stellen dat de reden waarom dit idee niet reeds eerder was gerealiseerd samenhangt met de specifieke aard van de destijds dominante gegevensbankensystemen. Het relationele model en de relatiealgebra zijn prima ingrediënten voor dit project, maar de uitdrukkingsmiddelen die de toenmalig in zwang zijnde versies van de taal SQL te bieden had waren ontoereikend voor dit doel. Op dit punt deden zich de gelukkige omstandigheden voor dat Ghica in die periode betrokken was bij de ontwikkeling van het inmiddels naar de geschiedenis verwezen IBM Database Systeem BS12, ontwikkeld in de luwte van de laboratoria in Peterlee, UK en Uithoorn, dat (wellicht mede beïnvloed door de adviezen van de toenmalige adviseurs Blauw en Duyvesteijn) wel voldoende uitdrukkingskracht te bieden had.

Gevolg was dat wij in Uithoorn wel in staat waren een op compilatie gebaseerde brug te slaan tussen Prolog en BS12. Het in 1984 uitgevoerde stageproject van de heer CFJ Doedens leverde een werkend prototype op, waarmee deze student zich in de geschiedenisboeken van deze instelling heeft weten te plaatsen als een van het duo studenten dat op 14 december 1984 de eerste doctoraalbullen Informatica in ontvangst mochten nemen [38]. Een ander resultaat was het gezamenlijke artikel van Ghica en ondergetekende in een Industrieel tijdschrift [39]. Het fragment is later uitgebreid met termen door een andere UvA stagiair Bas Elbers [40].

Voorzien van deze nieuwe inzichten verbleven wij in 1985 voor 8 maanden op het IBM Research Laboratorium te San Jose (thans gevestigd te Almaden), waar ik binnen het Office Automation project van Peter Lucas mocht nadenken over een declaratieve taal om business rules te specificeren. De door mij ontworpen taal **RL** voldoet aan de eis van declarativiteit; de semantiek is gebaseerd op een combinatie van elementen van het Logisch Programmeren, relationele databases en het later populair geworden onderwerp Constraint Logic Programming [41]. Aan een implementatie heb ik niet gewerkt. Bij mijn vertrek verwachtten mijn IBM collega's daarvoor wel twee jaar nodig te hebben, en nadien is er niets meer mee gedaan, mede omdat het gehele Office Automation project werd getermineerd.

Na terugkeer in Amsterdam werd ik al vrij snel opgezadeld met het voorzitterschap van de Examencommissie Informatica - een taak die ik met veel plezier gedurende 22 jaar heb mogen vervullen, maar daarover later meer. In de stijl van de traditie van de vakgroep Numerieke Wiskunde en Informatica van de de subfaculteit Wiskunde, had de Informatica als onderdeel van het examen de verdediging van het afstudeerwerk in het openbaar in volle glorie gehandhaafd, met het gevolgd dat ik vanaf die datum automatisch inzicht kreeg in het afstudeerwerk van al onze studenten.

Een van die studenten was de heer Sieger van Denneheuvel die in een project van Bob Wielinga een virtueel laboratorium had gebouwd waarmee experimenteel onderzoek naar studieprestaties van studenten verricht diende te worden. Hij maakte daarbij gebruik van een algebraïsch systeem om vergelijkingen op te lossen - precies het soort technologie wat nodig was om mijn taal te realiseren.

Ik heb Sieger deze worst slechts één keer voor zijn neus hoeven hangen. Een week later vervoegde hij zich bij mij met de wens om mijn taal te implementeren, en konden wij hem een plaats als AIO in de toenmalige theoriegroep aanbieden (dat soort aanstellingen waren destijds nog gemakkelijk te regelen…). Sieger slaagde erin om binnen korte tijd een eerste werkend prototype aan de praat te krijgen.

Tot medio jaren negentig hebben een reeks van mijn promovendi (naast Sieger van Denneheuvel waren dit Karen Kwast, Zhisheng Huang, Fred de Geus, en Ernest Rotterdam) zich bezig kunnen houden met theoretische aspecten en toepassingen van mijn taal **RL** en de eraan ten grondslag liggende relationele semantiek. De taal is zelfs gedurende korte tijd gebruikt voor productspecificatie bij Syllogic, het bedrijf van mijn toenmalige promovendus en huidige collega Pieter Adriaans. In de buitenwereld waren inmiddels de Objecten in zwang gekomen, en daar heeft mijn groep (in dit geval Ernest Rotterdam en Erik de Haas) zich ook nog mee bezig mogen houden.

Ten slotte hebben deze projecten er toe geleid dat ik in de negentiger jaren ben ingezet bij het onderwijs over gegevensbanken aan deze instelling, een taak waarvan ik mij heb gekweten tot 1999 toen ik na enige omzwervingen langs Object Technologie, Design Patterns en Agent Technologie de perverse actie heb ondernomen om deze plaats in het onderwijsprogramma te gaan misbruiken voor onderwijs in de speltheorie.

De Augiasstal - *Invariantie en Machinemodellen*

In de Augiasstal viel het een en ander op te ruimen; het is passend om dit werk te koppelen aan activiteiten die samenhangen met het afrekenen met een irritante slordigheid in de standaardliteratuur.

Het eerste verhaal in mijn geheugen waarin een duidelijk overzicht werd gegeven van de voor de algoritmiek en complexiteitstheorie relevante machinemodellen heb ik niet zelf mogen verzorgen. In 1976 organiseerde de afdeling Besliskunde van het Mathematisch Centrum in samenwerking met de afdeling Informatica een bijeenkomst onder de titel *Interfaces between Computer Science and Operations Research* (ICSOR) [42] waarbinnen de complexiteitstheorie een centrale rol speelde. Betrokkenen waren onder anderen de toenmalige promovendi van Gijs de Leve: Alexander Rinnooy Kan en Jan Karel Lenstra die een half jaar later beide hun proefschrift over de theorie van machinevolgorde problemen zouden verdedigen. Mij viel de taak ten deel iets te vertellen over de ontwikkelingen op het gebied van efficiente gegevensstructuren zodat ik niet meer inzetbaar was voor het daaraan voorafgaande stuk theorie over de vergelijking van Machinemodellen dat werd verzorgd door de toenmalige bezoeker Walter Savitch.[3] Ik kreeg zelf vier jaar later de kans een dergelijke inleiding te verzorgen tijdens de studieweek Getaltheorie en Computers die door Rob Tijdenman en Hendrik Lenstra op het Mathematisch Centrum was georganiseerd [43, 44].

3). Deze bijeenkomst vormt een belangrijke scheidslijn in mijn professionele loopbaan: op dit symposium ben ik begonnen systematisch fotos te maken van alle sprekers op alle bijeenkomsten waaraan ik deelneem, een activiteit waar ik nooit meer mee ben opgehouden.

Bij de bewuste modellen handelt het om Turing Machines in vele vormen en soorten, von-Neumann achtige modellen zoals de Random Access Machine, al dan niet met een modificeerbaar programma (RAM en RASP), verschillende modellen van pointermachines en modellen gebaseerd op graafmanipulatie en/of term herschrijving. Daarnaast bestaan circuit gebaseerde modellen, maar die

werken in het algemeen slechts voor invoer van een gegeven vaste lengte en geven aldus aanleiding tot een familie van circuits wat een non-uniform model oplevert. De collectie modellen wordt nog veel uitgebreider als men ook de parallelle versies van deze modellen in beschouwing neemt.

In de wiskunde en de logica speelde de exacte keuze van een model geen rol. Men had van alle bestaande modellen immers vastgesteld dat zij gelijkwaardig waren met betrekking tot de dingen die je ermee kunt doen: alle modellen berekenen de volledige klasse van partieel recursieve functies, indien je bereid bent de in- en uitvoer maar te coderen in een formaat dat door het desbetreffende model wordt begrepen. Voor de bestaande modellen was dit bewezen en het heilige geloof dat het voor andere nog uit te vinden modellen niet anders kan en zal zijn staat bekend als de These van Church-Turing.

Echter, zoals reeds eerder gemeld bij de bespreking van de Abstracte Complexiteitstheorie, houdt de recursietheorie geen rekening met het feit dat berekeningen tijd kosten, en geheugen gebruiken. Het door Blum ontwikkelde abstracte model leert ons helaas niets over de wereld waarin wij dagelijks aan het rekenen zijn. Daarvoor gebruiken wij de genoemde concrete modellen, en dat roept onmiddelijk de vraag op of de keuze van het machinemodel al dan niet invloed heeft op de uitspraken die wij kunnen doen over de feitelijke complexiteit van problemen.

Een voorbeeld van dit probleem heeft U reeds kunnen zien in de behandeling van de van Emde Boas bomen: het bezwaar dat Hopcroft maakte tegen mijn oorspronkelijke aanpak berust op het feit dat in het standaard RAM model geen instructie bestaat om het product van twee getallen te berekenen, en de prijs die ik daarvoor moest betalen was dat een structuur die lineair geheugen had moeten innemen meer dan lineair geheugen vereist. Collega's die mij schreven dat het toch echt in lineair geheugen kon gebruikten een ander machinemodel.

Waarom is de studie van deze afhankelijkheid belangrijk? Dit hangt samen met het feit dat in de Algoritmiek en in de standaard Complexiteitstheorie gebruik wordt gemaakt van een hiërarchie van fundamentele complexiteitsklassen: LOGSPACE $\subseteq$ NLOGSPACE $\subseteq$ P $\subseteq$ NP $\subseteq$ PSPACE $\subseteq$ EXPTIME $\subseteq$ EXPSPACE …. Een hiërarchie die, naar behoefte uitgebreid met een veelheid van andere klassen, wordt bestudeerd in de Structurele Complexiteitstheorie, een vorm van Theoretische Informatica die men kan zien als de natuurlijke erfgenaam van de Abstracte Complexiteitstheorie. Deze fundamentele klassen worden gedefinieerd in termen van de rekentijd en het geheugengebruik van een programma voor een Turingmachine, en het is dus belangrijk vast te stellen dat het gebruik van de RAM als basis model niet onverhoeds aanleiding kan geven tot een totaal andere familie van fundamentele complexiteitsklassen.

Dit probleem laat zich goed oplossen door gebruik te maken van simulaties. Als men een berekening op een Turingmachine kan naspelen op een RAM zonder dat dit veel extra rekentijd kost (overhead) en idem dito in de omgekeerde richting dan is er geen probleem. Acceptabel is een polynomiale overhead in rekentijd, I.E., rekentijd van $T(n)$ stappen op model 1 simuleren op model 2 kost niet meer dan $O(T(n)^c)$; hierbij is c meestal een klein getal als 2 maar ook overhead $O(T(n)log(T(\mathrm{n})))$ komt vaak voor. Voor geheugengebruik geldt een zwaardere eis: de overhead mag hier niet meer zijn dan vermenigvuldiging met een vaste constante.

Het algemene inzicht rond 1980 was dat het voor de gebruikte sequentiële modellen wat betreft de rekentijd allemaal wel in orde was. Inleidende leerboeken over Algoritmiek bespraken het probleem en gaven aan welke simulaties men kon gebruiken.

Helaas lieten deze zelfde leerboeken achterwege om te valideren dat het met het geheugen ook goed zat, waarschijnlijk omdat niemand op dat punt een probleem vermoedde.

Een ander aspect betrof de parallelle modellen. Daar onderkende men een patroon dat bekend staat onder de naam *Parallel Computation Thesis*: een parallel model heeft in polynomiale tijd dezelfde rekenkracht als een sequentieel model in polynomiaal geheugen, en het maakt niets uit of de parallelle machine nondeterministisch is; in formule //PTIME = //NPTIME = PSPACE.

Maar was het nu wel in orde met betrekking tot het geheugengebruik? Een incident had mij moeten waarschuwen. In 1980 lag er voor de ICALP die dat jaar in Noordwijkerhout werd gehouden, en waarvoor ik lid was van de Program commissie, een inzending op tafel uit de toenmalige DDR waarin werd aangetoond dat een tweedimensionale Turing Machine band met constante overhead in geheugen kan worden gesimuleerd op een lineaire tape. “Triviaal” riepen de deskundigen en de inzending werd afgewezen. Op mijn vraag waar het resultaat dan te vinden was kreeg ik geen antwoord, en dat was terecht, want, achteraf gezien, kan ik slechts constateren dat het hier een bevinding is die behoorde tot de algemene folklore kennis van de onderzoekers die met het onderzoek naar de complexiteit van Turing machines zijn begonnen medio jaren 60; helaas was de benodigde simulatie wat ingewikkeld en die hebben ze dus nooit opgeschreven. Onze Oost Duitser was met zijn geheel ontoegankelijke rapport vermoedelijk toch de eerste auteur die wel een bewijs op papier zette, en de verwijzing naar dit rapport in het ook in Oost Duitsland gepubliceerde Encyclopedische verzamelwerk van de heren Wagner en Wechsung [45] is voor zover ik kan nagaan de eerste gedrukte uitgave waarin het resultaat traceerbaar is terug te vinden.

Begin jaren 80 kwam mijn toenmalige assistent Leen Torenvliet mijn kamer binnen met een vraag over dit onderwerp, en ik stelde hem gerust met het uitspreken van de bewering die later bekend zou worden als de *Invariance Thesis: Redelijke Sequentiële Machinemodellen simuleren elkaar met een polynomiale overhead in tijd en een constante factor overhead in geheugen.* Echter toen Leen de kamer uit liep begon ik te twijfelen of ik hem niet had belazerd; hoe moet je immers een RAM op een Turingmachine simuleren met een constante factor overhead in geheugen?

De vraag hangt samen met de wijze waarop het geheugengebruik op de RAM wordt gemeten. Op een Turingmachine hebben de geheugencellen eindige opslagcapaciteit: er past een symbool in uit een voor de machine vastliggend eindig alfabet. Op een RAM kan een geheugenwoord in principe een willekeurig groot getal bevatten en daarom is het eerlijk om een geheugenwoord slechts te belasten voor de bits die feitelijk worden gebruikt, hetgeen neerkomt op het aanslaan van een woord voor de kosten gelijk aan de logaritme van de inhoud van dat woord. De RAM heeft ook de speciale eigenschap dat woorden niet aaneengesloten worden gebruikt - dat is nu net het gemak van het Random Access concept dat de machine haar naam geeft. Daarom is het ook eerlijk om een woord dat in de berekening niet wordt gebruikt niet mee te tellen bij de bepaling van het geheugengebruik.

Hiermee opent zich echter de mogelijkheid een gemene truc uit te halen: door in een woord met een hoog adres M het getal 1 op te slaan kan ik informatie opslaan waarmee ik het getal M kan terugvinden. Ik heb dit gedaan ten koste van slechts 1 bit geheugengebruik, en het is allerminst duidelijk is of ik dat op een Turingmachine kan naspelen zonder meer dan een constante hoeveelheid geheugen te gebruiken.

Er bestaat voor dit probleem een eenvoudige remedie: men moet bij de definitie van het geheugengebruik op de RAM ook de lengte van het adres van een gebruikt geheugenwoord meetellen, en dat maakt het simuleren van de RAM op een Turingmachine met constante factor geheugenoverhead triviaal; dat onder deze definitie de simulatie in omgekeerde richting lastiger wordt laat ik maar even onbesproken.

Het remarkabele feit doet zich nu voor dat in de toenmalige literatuur niemand gebruik blijkt te maken van deze voor de hand liggende definitie voor het geheugengebruik op de RAM. De reden hangt ongetwijfeld samen met het algemeen geaccepteerde idee dat het met het geheugen wel goed zit. Als er al definities in de literatuur staan dan meten ze te weinig (door het adres niet mee te tellen) of te veel (door ook de ongebruikte woorden voor minstens een bit te belasten).

Ik had hiermee echter nog niet bewezen dat deze definities echt fout waren. Wellicht bestaat er een andere simulatie waarmee de inhoud van het RAM geheugen op een alternatieve wijze op een Turingmachine kan worden gecodeerd waarbij de ruimte voor de adressen niet nodig is. Een op het eerste gezicht lastige puzzel en derhalve tijd om er weer eens een student op te zetten.

De student had in dit geval de toepasselijke naam Cees Slot. Als deelnemer aan onze CWI, UvA, RUU working group on Complexity Theory die ik samen met Paul Vitányi en Jan van Leeuwen organiseerde had hij kennis gemaakt met recente resultaten op het gebied van de theorie van perfect hashing, en op een goede dag kwam hij met de verassende boodschap dat hij hierin een mogelijkheid zag om de onvermoede simulatie te construeren. De noodzakelijke conditie voor zijn simulatie was dat wij een, voor een relevante kleine verzameling adressen, perfecte hash functie in een voldoende kleine hoeveelheid geheugen konden coderen, maar een recent gepubliceerd artikel van de heren Komlos en Szemeredi bood ons voldoende uitgangspunten om deze constructie door te kunnen voeren.

Het resultaat: voor online bewerkingen is gemakkelijk in te zien dat de simulatie onmogelijk is, maar voor het deterministische offline geval kan het wel: er bestaat een simulatie van de RAM op een Turingmachine die het geheugen met niet meer dan een constante factor opblaast, ook als we de verkeerde definitie van het geheugengebruik hanteren. Helaas loopt de rekentijd bij deze simulatie volstrekt uit de hand zodat we niet aan een meer orthodoxe lezing van de Invariance Thesis voldoen waarbij vereist wordt dat de simulatie tegelijkertijd de eisen met betrekking tot rekentijd en geheugengebruik vervult.

Het leverde ons een gezamenlijk artikel op het ACM symposium Theory of Computing in Washington DC in 1984 [46] waarvan een tijdschrift versie pas vier jaar later verscheen [47]. Het bewuste tijdschrift had graag de congresversie ongewijzigd willen opnemen, maar slaagde er niet in de rechten bij de ACM los te peuteren zodat we het artikel in zijn geheel hebben moeten herschrijven. Vermeldenswaardig is nog dat ik op het congres er in slaagde de Amerikanen de stuipen op het lijf te jagen door de Invariance Thesis te verkopen geformuleerd in termen van de Declaration of Independence.

Een overzichtsverhaal over Parallelle machinemodellen dat ik in eerste instantie had gepresenteerd op een CWI colloquium medio jaren 80 vormde de basis voor een reeks artikelen waarin ik liet zien in welke mate de parallelle modellen nu echt voldeden aan de Parallel Computation Thesis. Een versie van dat artikel is gepresenteerd in het najaar van 1985 en opgenomen in een bundel van het Banach Center in Warschau [48].

Op basis van de genoemde artikelen ontving ik de eervolle uitnodiging het openingshoofdstuk over machinemodellen te schrijven voor het tussen 1985 en

1990 geproduceerde Elsevier Handbook of Theoretical Computer Science [49]. Helaas was ik ook dit keer te laks om de ingeslagen weg te vervolgen zodat een denkbaar standaard leerboek over machinemodellen van mijn hand nooit is verschenen.

De appels van de Hesperiden - *Betegelingen*

Een taak waarvoor Heracles alle uithoeken van de Aarde heeft moeten bezoeken. Een overbodige reis, aangezien de hier te bespreken artefacten zich gewoon bij mij thuis bevinden.

Ik ben U nog de uitleg schuldig hoe dat nu precies zat met dat betegelen van badkamers waarmee ik kennelijk bezig was toen die journalist mij in Utrecht heeft betrapt. In een moeite door kan ik U dan ook vertellen over een eerder betegelingsproject waarvan een resultaat is verwerkt in de uitnodiging die de Faculteit heeft doen uitgaan.

De afbeeldingen die U op de uitnodiging kunt zien zijn afkomstig van opnames van een van de parketvloeren die in 1977 zijn aangelegd in onze woning te Heemstede waarheen wij in dat jaar zijn verhuisd. Hoewel wij nu niet meer in dat huis wonen is de waarheid van de bewering dat deze parketvloer zich in mijn huis bevindt onveranderd; bij onze verhuizing in 1991 hebben wij deze vloeren immers mee laten verhuizen.

Het motief om deze ongebruikelijke actie te ondernemen is uiteraard dat wij hier te maken hebben met een artefact dat uniek is in de wereld. De bewuste parketvloeren vertonen drie mathematische patronen. Het best bekende patroon is dat van de verdeling van de priemgetallen in de ring van gehele getallen van Gauss - een patroon dat ook is gebruikt voor een theedoek uitgedeeld op het IMU congres in Amsterdam in 1954, waarvan het Koninklijk Wiskundig Genootschap ter gelegenheid van het 5e Europese Wiskunde Congres dat in 2008 in Amsterdam werd georganiseerd een heruitgave heeft verzorgd. Het tweede patroon vertoont de exponenten van de eerste 27 Mersenne priemgetallen in een formaat geconcipieerd door Hendrik Lenstra. Dit patroon is ook terug te vinden in een tweetal prenten van Tobias Baanders,

waarvan er een is gebruikt als briefkaart van het Mathematisch Instituut en (in groter formaat) als present voor de sprekers van het Algemeen Wiskunde Colloquium. Het laatste patroon is gebaseerd op een stuk getaltheorie uit het proefschrift van Hendrik Lenstra: de minimale Euclidische Algoritme voor de getallen van Gauss. Dit patroon bestaat voor zover mij bekend verder alleen nog in de vorm van een quilt vervaardigd door mijn schoonmoeder en kussentjes geborduurd door onze helaas het afgelopen jaar overleden collega Elly Dobber.

Deze vloeren danken hun bestaan aan het feit dat ik destijds bij de verhuizing naar Heemstede slechts bereid was akkoord te gaan met de door Ghica begeerde parketvloeren als deze vloeren een wiskundig patroon zouden vertonen. Dat het mogelijk was invloed uit te oefenen op het patroon danken wij aan het bestaan van de firma Rowi Parket die in dat jaar op de huishoudbeurs parket in de aanbieding had in de vorm van stroken van 1 tot 6 vierkantjes van 6 bij 6 cm in verschillende houtsoorten, en dat geeft alle ruimte die een mens nodig heeft om interessante patronen te realiseren. Dat het hier om tropisch hardhout gaat - met de kennis van nu dus foute boel - moet U maar voor lief nemen. Uiteraard was dit een project waarbij wij geen fouten konden tolereren, maar onder het scherpe toezicht van de geestelijke vader Hendrik Lenstra (die overigens niet te beroerd was om zelf de hamer ter hand te nemen bij de aanleg) werd dit project foutloos voltooid. U kunt op mijn website een uitgebreid verslag vinden van dit project in de vorm van een presentatie die ik op 8 oktober 2000 mocht houden voor scholieren op de Wetenschapsdag waarvan het thema was *Huis- tuin- en keuken wetenschap* [50]. U kunt een indruk krijgen van het gebruikte materiaal en de constructiewerkers (in dit geval Henrik Lenstra en Arthur Rietveld) op de onderstaande foto.

Deze vloeren hebben echter niets te maken met de betegelingen waar onze Egghead zich mee bezig heeft gehouden. Het gaat in dit laatste geval over het gebruik van betegelingen voor een meesterreductie van Turingmachine berekeningen tot een combinatorisch probleem.

Voor de oorsprong van deze toepassing moeten wij andermaal terug naar de jaren 70 van de vorige eeuw. De bewuste tegels zijn vierkante tegels die door de beide diagonalen verdeeld zijn in vier driehoeken. Een tegeltype ontstaat door deze vier driehoeken te voorzien van een kleur uit een eindige collectie kleuren. Betegelingen ontstaan door tegels naast en onder elkaar te plaatsen waarbij de conditie geldt dat driehoeken die een kant van een tegel delen dezelfde kleur moeten hebben. Het is gemakkelijk in te zien dat dit altijd kan - ook als men maar over een enkel tegeltype beschikt, maar er geldt nog een extra conditie: de tegels mogen niet worden gedraaid. Zoals ik het altijd uitleg aan mijn studenten: de firma Mosa die de bewuste tegels produceert heeft de vreemde gewoonte in iedere tegel een staafmagneet te bakken, en helaas is het Aardmagnetische veld een factor 10000 sterker dan het in onze wereld is. Spiegelen is ook niet toegestaan: dit zou er op neer komen dat de tegels worden omgedraaid maar dan komt de ongeglazuurde kant boven te liggen en dat is om hygiënische redenen niet verantwoord.

Deze tegels zijn in de wiskunde en logica populair geworden omdat het mogelijk is om voor een gegeven Turing Machine een collectie tegeltypen te ontwerpen zodanig dat er een correspondentie bestaat tussen legale betegelingen en (fragmenten van) het Tijd-Geheugen diagram van berekeningen van de bewuste machine. Als wij nu ook nog de mogelijkheid krijgen om via het opleggen van een randconditie af te dwingen dat de gecodeerde berekening er een is op de gewenste invoer die eindigt in een accepterende toestand is het duidelijk dat hier sprake is van een meesterreductie: het rechtstreeks vertalen van berekeningen naar combinatorische puzzels.

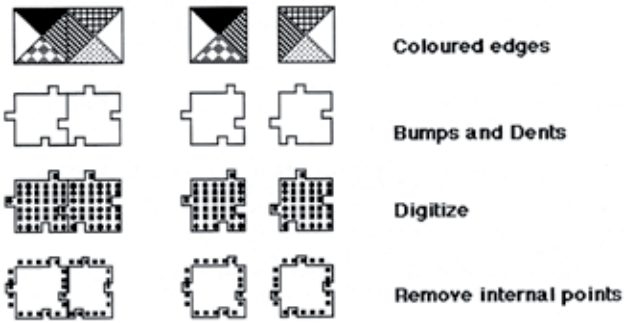
In de context van de berekenbaarheidstheorie is deze gedachte voor het eerst uitgewerkt door Wang. Een fundamentele stelling die uitspreekt dat het bestaan van een betegeling van het gehele vlak - zonder extra randconditie - een onbeslisbaar probleem is bewezen door Berger en Robinson. De constructie is complex en vereist de constructie van een collectie tegeltypes waarmee het vlak wel te betegelen is maar alleen met aperiodieke betegelingen: er bestaat geen grote betegelde rechthoek zo dat het vlak wordt overdekt met bij elkaar passende verplaatste kopieën van deze rechthoek.

Tot de huidige dag zijn collega's (in het bijzonder in Frankrijk) bezig om het bewijs van deze klassieke stelling te vereenvoudigen en begrijpelijker te maken, maar ik wil daar verder bij deze gelegenheid niet op ingaan. Ik beperk mij hier tot het gebruik van deze techniek binnen mijn eigen activiteiten.

Het gebruik in de complexiteitstheorie vinden wij voor het eerst bij H.Lewis in 1977. Zelf ben ik mij er in 1980 mee gaan bezig houden naar aanleiding van een introductie over de elementaire reductietheorie die ik moest houden in het kader van een CWI cursus over de cryptografie. Het stond mij tegen dat de standaard behandeling die resulteert tot het voor dit vakgebied relevante resultaat dat het Knapsack probleem NP-volledig is een voor dit publiek onaangename omweg bevat. Men introduceert het vervulbaarheidsprobleem (Satisfiability) en bewijst volgens de klassieke methode van Cook en Levin dat dit een NP-volledig probleem is (hier zit de meesterreductie in deze route); vervolgens reduceren wij Satisfiability tot een combinatorisch probleem zoals Set Cover, en vandaar komen wij door de verzamelingen te coderen als bitstrings (hetgeen de facto binair geschreven getallen zijn) tot het Knapsack probleem. Bij het gebruik van deze methode introduceren wij dus het Satisfiability probleem alleen maar met het doel datzelfde probleem weer zo snel mogelijk te doen vergeten.

Bij het voorbereiden van deze presentatie zag ik dat het met gebruik van betegelingen mogelijk is een meesterreductie te geven die zich rechtstreeks laat doorvertalen naar Set Cover, zodat wij deze cryptografen niet langer hoeven lastig te vallen met de voor hen niet relevante logische taal van de propositielogica. De reductie (die in feite berust op het idee om fotos op te slaan in pixels) laat zich bovendien uitstekend illustreren aan de hand van het eenvoudige plaatje dat U hieronder ziet afgebeeld. Deze versie van deze figuur die in mijn artikelen over dit onderwerp terugkeert is afkomstig van een van de latere versies van dit artikel [51].

Reducing tilings to EXACT COVER.



Gewapend met dit resultaat vroeg ik mij af of het wellicht mogelijk zou zijn om het Satisfiability probleem op vergelijkbare wijze te elimineren uit de vijf overige standaard reducties in het standaardwerk over NP-volledigheid van de heren Garey en Johnson [52]. Eens te meer tijd om een student aan het werk

te zetten, in dit geval de heer Martin W.P. Savelsbergh. Ook deze student heeft zich op bekwame wijze van zijn taak gekweten; alle vijf overige reducties lieten zich uitvoeren met betegelingen als uitgangspunt, zij het dat het Hamiltonian Circuit geval complex blijft (maar dat is het vanuit Satisfiability ook). Altijd nog goed voor een gezamenlijke presentatie op het 2e Frege Memorial Congres in Schwerin in 1984 [53].

In oktober 1982 bezocht ik een workshop te Paderborn waar ik geconfronteerd werd met recent werk van Jones en Matiasevitch over het Hilbert 10 probleem. Zij hadden een vereenvoudiging gegeven van het bewijs dat Turing Machine berekeningen zich laten reduceren tot de vraag naar de oplosbaarheid van exponentieel-diophantische vergelijkingen. Dit is het combinatorische deel van het bewijs van de onbeslisbaarheid van de oplosbaarheid van Diophantische vergelijkingen - de tweede stap waarbij met gebruik van de Pell vergelijking de exponentiële functies worden geëlimineerd blijft bij dit bewijs nodig. In zijn voordracht poneerde Jones de bewering dat het gebruik van registermachines voor deze methode noodzakelijk was - uitgaande van Turingmachines zou het niet kunnen.

Deze uitspraak vroeg uiteraard om weerlegging. Jones had zijn voordracht op maandag gegeven en in mijn eigen voordracht later die week kon ik laten zien dat de methode die ik eerder gebruikt had voor de Cryptografen ook hier werkt [54]. Ik ben van mening dat het resulterende bewijs voor de combinatorische helft van de Hilbert 10 stelling het meest transparante bewijs is dat wij kennen. Omdat het oorspronkelijke congresverslag nogal ontoegankelijk is heb ik dit resultaat naderhand nog eens gepubliceerd in een bundel voortkomende uit het Europees gesteunde project COLORET waar ons instituut aan heeft deelgenomen in de jaren 1993-97 [51].[4] In dit artikel zult U alle verwijzingen naar de literatuur aantreffen die ik in de huidige tekst achterwege heb gelaten.

4. Dit project is een directe voorganger van ons huidige CiE netwerk.

Dit optreden had nog een gevolg, waar ik verder geen invloed op heb gehad. Tussen de toehoorders zat mijn collega David Harel, die na afloop evenzeer tot het gebruik van betegelingen bleek te zijn bekeerd. Gebruik makend van het recurrente betegelingsprobleem (kan het vlak zodanig worden betegeld dat een specifiek vermeld tegeltype oneindig vaak wordt gebruikt) slaagde hij erin om voor een twintigtal programmalogica's in een slag te bewijzen dat ze in hoge mate onbeslisbaar zijn (hun complexiteit valt buiten de aritmetische hiërarchie in de recursietheorie). Op dit artikel berust het nu algemeen geaccepteerde inzicht dat een logica die krachtig genoeg is om de structuur van een twee dimensionaal rooster te coderen deze hoge graad van onbeslisbaarheid moet bezitten.

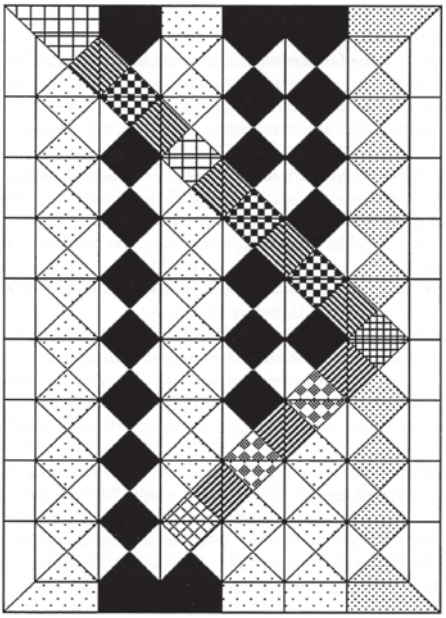
Bij al mijn presentaties van deze methode om de reductietheorie te baseren op betegelingen heb ik altijd gebruik gemaakt van hetzelfde voorbeeld van een

Turingmachine: de successor machine die eerst het rechtereinde van een binair getal opzoekt en vervolgens het laatste blok enen door nullen vervangt waarna de daarvoorstaande nul of blanco symbool wordt overschreven door een 1 waarna de machine termineert. Met twee toestanden en drie symbolen levert dit een catalogus van 15 verschillende tegeltypes op die gebruikt worden in de reductie.

In 1992 kon ik de directie van de Faculteit Wiskunde en Informatica ervan overtuigen dat het de moeite en het geld waard was om de aldus gedefinieerde puzzel in hardware te realiseren om deze te gebruiken op open dagen voor de studie, wetenschapsdagen en dergelijke gelegenheden. Voor het demonstreren was het wenselijk dat het te betegelen bord verticaal staat, zodat het nodig is iets te verzinnen waardoor de tegels er niet afvallen. Om tegelijkertijd af te dwingen dat de tegels niet gedraaid kunnen worden bedacht de constructeur van deze puzzel, Ankie Houtkooper - Visser een constructie waarbij iedere tegel op zijn plaats wordt gehouden met twee spijkertjes die passen in twee gaten in de houten tegel. De tegels zijn beplakt met folie bedrukt met de benodigde vier gekleurde driehoeken die vervaardigd zijn op een van de eerste kleurenprinters die onze faculteit destijds bezat. Ik ben daarbij nog geholpen door Edoh Dooijes om de printer zo ver te krijgen dat deze dit kon afdrukken.

Het was het plan om de puzzel officieel in te wijden op de Wetenschapsdag in 1992, maar toehoorders die de geschiedenis goed kennen weten dat deze editie van de Wetenschapsdag is afgelast vanwege de Bijlmerramp. De puzzel is daarna wel regelmatig gebruikt bij open dagen, en ik heb hem ook een keer kunnen vertonen op een bijeenkomst van de Nederlandse Vereniging voor Logica. Jarenlang heeft het bord op mijn kamer gestaan tot er een keer een oekaze van de brandweer kwam dat er geen losse objecten in onze kamers mochten rondslingeren. De laatste jaren vertoefde de puzzel in de kelder van Euclides, en zou zeker bij de verhuizing zijn weggegooid als ik mij niet erover had ontfermd en hem thuis had opgeslagen. Het betreft hier immers een uniek object. Ik meen dat het de meest inefficiënte computer is die de mensheid ooit heeft gebouwd. Het uitvoeren van de berekening 11 + 1 = 12 vraagt minstens vijf minuten werk van een gemiddelde scholier, en het aantal bewerkingen dat je ermee kunt uitvoeren is ook nogal beperkt. Inmiddels is de puzzel ook beschikbaar in de vorm van een computersimulatie die Ghica dit voorjaar heeft ontwikkeld ter gelegenheid van ons bezoek aan China. U kunt dit vinden via de URL www.squaringthecircles.com/turingtiles/.

Het patroon wat resulteert als de puzzel is opgelost is door mijn schoonmoeder verwerkt in een quilt die onze gang opsiert. Diegenen onder U die ook voor het diner vanavond zijn uitgenodigd hebben het patroon kunnen zien op de gedrukte uitnodiging. Een oudere versie van deze betegeling (bedoeld om in zwart-wit te worden afgedrukt) is te zien in de onderstaande figuur afkomstig uit [51].



A tiling representing the computation 11 + 1 = 12.

De runderen van Geryones - *de Fotocollectie en de gelegenheden waar deze gemaakt zijn*

Als wij de overlevering mogen geloven was Heracles bij dit werk primair actief als veedief in combinatie met doodslag op een reus. Diefstal roept uiteraard de associatie op met alle beelden van collega's die ik de afgelopen 40 jaar heb gestolen.

Na deze tien onderwerpen uit de wiskunde en informatica te hebben besproken wil ik het voorlaatste werk koppelen aan activiteiten die niet rechtstreeks iets met onderzoek te maken hebben maar wel degelijk een onderdeel vormen van de reputatie die ik heb opgebouwd.

Het gaat hier in de eerste plaats om de fameuze fotocollectie.

Ter gelegenheid van het eerder genoemde EMS congres in 2008 in Amsterdam heb ik (met steun van de publicatiedienst van het CWI en van Herman te Riele) een kleine expositie van vroege opnamen uit deze collectie kunnen verzorgen.

Voor september 1976 had ik incidenteel wel eens een wiskundige op de prent gezet tijdens een conferentie, of bij een bezoek aan mijn huis. Te beginnen bij het ICSOR symposium ben ik systematisch te werk gegaan en heb ik waar mogelijk alle sprekers die ik voor mij zag staan op de prent gezet. Regelmatig nam ik ook voorzitters en interessante toehoorders mee. Oorspronkelijk werkte ik met een Olympus OM1, maar nog veel vaker met een van de ongeveer 15 Rollei 35 camera's die ik in de loop van 40 jaar heb bezeten. Het merendeel daarvan leeft niet meer; vele raakten onbruikbaar door slijtage, intensief gebruik, zijn gestolen of verloren op straat. De meest dramatische wijze om een van mijn Rollei's te verliezen was het feit dat op vakantie in Idro (Italië) mijn oudste zoon er eentje in het meer heeft gegooid (zulks als reactie op een uitdrukkelijke opdracht een dergelijke euvele daad niet te plegen - so much

voor onze educatieve en pedagogische vaardigheden). Zoals kenners weten is het model reeds geruime tijd buiten productie, en op de tweede handsmarkt brengt een goede Rollei vandaag meer op in Euro's dan het origineel destijds in guldens heeft gekost. Gelukkig heb ik nog een aantal bruikbare exemplaren ter beschikking.

De wereld van de fotografie is zoals mijn collega Arnold Smeulders mij zo treffend heeft weten uit te leggen echter totaal veranderd door de komst van de digitale camera. Ik heb lang de vooruitgang bestreden maar mensen in mijn omgeving zullen inmiddels hebben gemerkt dat ik op dit punt inmiddels om ben gegaan. Een nadeel van een digitale camera is echter dat je nog veel meer foto's maakt dan in het analoge verleden.

Het voornaamste probleem met de collectie is het ontbreken van een index. Tot ongeveer 1996 zitten de binnenlandse opnamen in fotoalbums (in principe chronologisch). Wat buitenlandse bijeenkomsten betreft is de achterstand nog een acht jaar groter. Over de periode van 11 jaar daarna zijn tenminste de negatieven nog chronologisch geordend, en daarna heb ik de afdrukken niet eens meer uitgepakt. De digitale bestanden zitten onbeschreven in folders te traceren op datum. Gevolg is dat ik in het algemeen verzoeken om opnames uit een verder verleden makkelijker kan honoreren dan vragen naar opnamen van de laatste tien jaar, waarbij ik moet melden dat een dergelijk verzoek vrijwel onuitvoerbaar is als ik er niet een indicatie bij krijg van een datum waarop de gezochte persoon een voordracht gehouden heeft waarbij ik mogelijk aanwezig ben geweest.

Om deze collectie te ontsluiten en te preserveren voor het nageslacht (wat duidelijk mijn doel is - zij is bestemd om toe te vallen aan het Koninklijk Wiskundig Genootschap) zal ik dus alles moeten beschrijven in een nader vast te stellen ontologie, en uiteraard dient het oude analoge materiaal te worden gedigitaliseerd. Als U weet dat een grove schatting mij leert dat het om ruim 100.000 opnames gaat, ziet U dat hier nog veel en tijdrovende arbeid op ons ligt te wachten, en zult U het met mij eens zijn dat ik voorlopig meer dan genoeg te doen zal hebben.

Deze opnames zijn voor het overgrote deel gemaakt bij voordrachten van anderen en als bijbehorende activiteit wil ik dan ook vermelden de actieve aanwezigheid bij presentaties, ongeacht of dit colloquium voordrachten, conferenties, colleges, promoties of scriptieverdedigingen op een examen zijn.

Ik heb aan het begin van deze rede reeds vermeld dat ik als jonge student de gewoonte had om sprekers lastig te vallen met vragen en dat ben ik gedurende mijn gehele loopbaan bij alle in aanmerking komende gelegenheden blijven doen.

Een noodzakelijke voorwaarde voor een zinnige interactie met sprekers is dat je als toehoorder in staat bent de spreker te blijven volgen. Niet alle sprekers bieden het gehoor daartoe de mogelijkheid, maar in het verleden was het zo dat ik het vaak langer vol wist te houden dan de meeste mensen in mijn omgeving (althans voor vele onderwerpen - er zijn ook onderwerpen waarbij ik het wel direct kon opgeven). Ik zag het dan als mijn taak om te vragen om verduidelijking als ik dacht dat het publiek daar baat bij zou hebben, en foutjes te corrigeren als ik meende dat andere toehoorders door deze fouten in verwarring zouden kunnen geraken. Regelmatig gebeurde het dat ik een aantal stappen vooruit had gedacht zodat ik vroeg naar de inhoud van een van de komende slides.

Bij congressen is het ook wenselijk dat na afloop van een voordracht vragen gesteld worden, en als de zaal dat niet doet rust de taak op de schouder van de voorzitter om een vraag te genereren. Dat dit niet altijd eenvoudig is heb ik ervaren want ik heb deze rol regelmatig mogen vervullen, zeker bij conferenties waarvoor ik eerder had mogen deelnemen aan de selectie binnen het programma comité. Helaas tref ik maar al te vaak sprekers die op een congrespresentatie niets duidelijk over het voetlicht weten te brengen; op dit punt dient onze gemeenschap bij voortduring nader te worden opgevoed.

Bij examens en promoties is het stellen van vragen uiteraard geen mogelijke actie maar een opgelegde verplichting. De cultuur die wij in onze instituten tot de huidige dag hebben weten te handhaven waarbij de verdediging van een scriptie een serieus en openbaar evenement is, vraagt van de leden van de examencommissie dat zijn voldoende kennis hebben genomen van de inhoud van het geschrevene en daar een zinnige en relevante vraag over kunnen stellen. Als voorzitter van de Examencommissie Informatica heb ik deze taak mogen vervullen bij zeker 650 van de 700 Informatici die gedurende mijn voorzitterschap in de periode 1986 tot 2009 zijn afgestudeerd. Daarbij komen uiteraard studenten in andere opleidingen waarvoor ik deze functie heb mogen bekleden zoals de Master Software Engineering en de Master of Logic. Incidenteel mocht ik opdraven bij andere opleidingen zoals Kunstmatige Intelligentie en Wiskunde, en uiteraard was ik ook voor 1986 regelmatig betrokken bij examens van de toenmalige vakgroepen binnen de subfaculteit wiskunde. Het is dus plausibel dat ik in de loop van de afgelopen veertig jaren een kleine duizend examens heb mogen bijwonen, en een navenant aantal doctoraalscripties heb mogen doorlezen.

Het aantal bijgewoonde promoties valt wat lager uit - ik schat ergens tussen de 300 en 400, waarvan ik zeker de afgelopen 20 jaar de meeste heb mogen bijwonen in de rol van voorzitter en vervanger van de rector. In 1991 kreeg ik deze taak geheel onverwacht toegeschoven toen onze toenmalige

decaan zijn agenda niet op orde had, en na afloop van dit incident vond deze decaan dat een zo goede oplossing dat ik deze taak heb mogen blijven vervullen gedurende zijn decanaat, en vervolgens ook gedurende de decanaten van zijn opvolgers. Daarmee was het enige motief dat mij ooit had kunnen overtuigen zelf decaan te worden (dat je daardoor promoties mag voorzitten) van tafel, en ik prijs mij dan ook gelukkig dat dit soort bestuurlijke ambten mij bespaard zijn gebleven. Ik denk ook dat ik daar totaal ongeschikt voor ben en mijn collega's, die mij er nooit voor hebben gevraagd zijn dat kennelijk met mij eens geweest.

Nu zult U terecht opmerken dat de voorzitter niet geacht wordt zich bezig te houden met het stellen van vragen op een promotie, maar ik heb mij daar nooit door geremd gevoeld. Ik denk juist dat het getuigd van respect voor de promovendus als ook de voorzitter kenbaar maakt zich met belangstelling te hebben verdiept in de voorliggende dissertatie en daar via het stellen van een vraag daar acte van geeft. Het logistieke feit dat de voorzitter niet zichzelf kan onderbreken om het tijdschema na te leven is geen probleem zolang deze zich maar positioneert aan het einde van de plechtigheid want dan maakt onze pedel er wel een einde aan.

Uiteraard heb ik ook in deze rol gebruik gemaakt van mijn camera (zonder flitsapparatuur - een reden te meer om gebruik te blijven maken van mijn Rollei's aangezien praktisch alle andere compact camera's voorzien waren van een automatische flits die zich niet laat uitschakelen). Wat mij nog niet is gelukt is om aan het einde van de plechtigheid deze zo krachtig af te hameren dat ik de hamer wist te breken, maar dat blijft vooralsnog een lopend project.

Ik realiseer mij dat het hier allemaal om activiteiten gaat die men niet pleegt op te voeren in het CV, en die U ook niet zult terugvinden in de academische jaarverslagen. Geheel ten onrechte want het gaat er in de academische wereld tenslotte niet alleen om dat er kennis wordt geproduceerd en opgeschreven, maar ook dat deze kennis vervolgens wordt geconsumeerd. Ik vrees met grote vreze dat op dat punt de balans in onze wereld totaal zoek is. Er wordt steeds meer gepubliceerd en gepresenteerd terwijl het aantal actieve lezers alleen maar lijkt af te nemen, zeker als het materiaal alleen maar beschikbaar is via digitale media die het mogelijk maken in korte tijd erg veel materiaal te zien, maar waarbij het extra vermoeiend is om het ook echt te lezen.

De Hydra - *de spelletjes*

De Hydra had de onaangename eigenschap dat zij voor iedere afgeslagen kop een nieuwe kop wist te genereren. Heracles wist uiteindelijk met inzet van massavernietigingswapens dit proces te onderbreken, maar waarom zou een mens dat doen als het afhakken van koppen nu juist ervaren wordt als een aangename bezigheid.

Er resteert nog een laatste werk, dat het in zich heeft oneindig lang te kunnen worden voortgezet. Wij zullen dit werk dus maar koppelen aan het speelkwartier waarin ik mij vooral de laatste tien jaar heb mogen vermaken: het gebruik van spelen als modellen voor onderzoek in de Informatica.

Het is zo dat de eerste wiskundige stelling die ik ooit meen zelfstandig te hebben bewezen het terminatie bewijs is voor het kaartspelletje Napoleon Patience dat ik als kind geleerd heb van mijn grootmoeder. Tijdens mijn schooljaren heb ik mij afgevraagd hoe het komt dat je bij dit spel niet onbeperkt met kaarten kunt blijven schuiven, en uiteindelijk vond ik het bewijs dat ik tegenwoordig aan mijn studenten vraag te reconstrueren in een van mijn standaardopgaven bij het college Games en Complexity [55].

Met de kennis van nu zie ik dat de gebruikte bewijsmethode zich laat onderkennen als de Moeder van alle terminatiebewijzen (definieer een geheeltallige niet negatieve functie op de mogelijke configuraties die bij iedere beweging alleen maar kleiner wordt). Echter, in deze fase van mijn leven had ik nog nooit een computer gezien, de wiskunde studie lag nog in de toekomst, en het woord Informatica diende nog te worden uitgevonden.

U moet bedenken dat lange tijd gedurende het begin van mijn wiskundig actieve leven het bestuderen van alles wat met spelletjes te maken had geen activiteit was waarmee de wiskundige werd geacht zich serieus in te laten. Dit was

ook de tijd dat onderzoekers die zich bezig hielden met schaakprogramma's of programma's voor andere spelen zoals checkers, dammen of backgammon amper erkend werden als serieuze onderzoekers op het gebied van de Kunstmatige Intelligentie.

Er waren enkele uitzonderingen. Gedurende de latere jaren 70 ontwikkelde Conway zijn rekenkunde van eindige tweepersoons spelletjes, en definieerde hij de door D.E. Knuth gepopulariseerde Surreal numbers: een systeem van getallen die met een soort herhaalde Dedekind constructie worden opgebouwd uit de lege verzameling. Deze getalklasse laat zich herkennen als een maximale non-standaarduitbreiding van de bekende reële getallen. Samen met Guy en Berlekamp schreef hij een standaardwerk over deze eindige tweepersoons-spelletjes. Wij bestudeerden deze ontwikkelingen in de combinatoriek werkgroep onder leiding van Jack van Lint op het Mathematisch Centrum maar meer als afleiding tussen het echte werk door dat gelegen was op het gebied van combinatoriek en coderingstheorie, dan dat wij het zagen als serieuze wiskunde.

Ik heb U reeds uitgelegd hoe de studie van een spelletje uit de recretatieve wiskunde ons rond 1979 op het spoor heeft gebracht van de epistemische logica, maar ook toen is het onderwerp van de speltheorie niet op de onderzoeksagenda geplaatst. Daarna valt nog een periode dat de (computer) spelletjes waar mijn zonen zich mee bezig hielden een rol gingen spelen bij het onderwijs over gegevensbanken dat ik medio jaren 90 heb verzorgd. Enkele jaargangen studenten zijn bezig gehouden met het maken van informatiemodellen voor de artificiële werelden van Civilization en Warhammer omdat ik daar grote voordelen in zag in vergelijking met de standaard voorbeelden in de literatuur. Ik heb deze gedachte ooit nog eens mogen propageren in een aflevering van het kort levende tijdschrift Athenaeum Illustre, uitgegeven door onze Universiteit [56]. Internationaal heb ik dit mogen bepleiten op een workshop bij de OOPSLA in Denver 1999 [57].

Geconstateerd kan worden dat toen ik in 1999 uiteindelijk begon met een echt college speltheorie dit precies op het juiste moment is gebeurd. Niet alleen waren spelletjes in zicht gekomen in het werk over dynamische epistemische logica in de omgeving van mijn collega van Benthem (die in dezelfde periode begon met zijn cursus Logic and Games), maar datzelfde voorjaar werden wij op de STACS bijeenkomst in Trier aangenaam verrast door de voordracht van de Noam Nisam [58] over mechanismen om agenten in het Internet bij de leest te houden (werk verricht samen met R. Ronen). Hier herhaalde zich de gang van zaken met betrekking tot de epistemische logica van 15 jaar eerder: omdat de Informatica de speltheorie kon toepassen werd dit onderwerp in zeer korte tijd gepromoveerd van een exotisch thema bestudeerd door enkele verdwaalde economen, wiskundigen, logici en filosofen, tot een goed gesteund centraal

thema binnen onze onderzoeksdisciplines. Het succes van het eerder dit jaar afgesloten Gloriclass project spreekt in deze boekdelen.

Deze hernieuwde belangstelling voor spelletjes is voor mij primair een onderwijsactiviteit gebleven. Het cursusmateriaal, in vele vormen toegankelijk via mijn website [59], heeft mij geïnspireerd om er tien jaar lang aan te blijven sleutelen om het te verbeteren, en wellicht zal ik het ooit nog eens kunnen bewerken tot het leerboek dat ik tenslotte ooit nog eens hoop te schrijven. Bij de vele onderzoeksprojecten waarbij spelletjes in rol spelen in mijn omgeving heeft mijn rol zich beperkt tot die van een actieve toeschouwer die af en toe de onderzoekers een idee mocht toespelen.

Ik hoop met mijn cursus over deze onderwerpen gedurende de afgelopen tien jaar een generatie studenten te hebben vermaakt, en bij hen belangstelling te hebben opgewekt voor dit leuke en nog steeds in belang toenemende onderwerp. Het zal U weinig moeite kosten om mijn studenten te herkennen: iedereen die de Warhammer helden Thorgrim en Urgat als spelers in een spel opvoert moet wel een student van mij zijn geweest.

Mentita sunt oracula

Onze held Heracles was na het voltooien van zijn twaalf werken nog niet uitgeleefd; zo wachtte hem nog een ongelukkig huwelijk dat eindigde in een pijnlijke dood, maar ik wil U niet verder lastig vallen met eigen activiteiten die aan dit deel van de mythologie kunnen worden gekoppeld. Het is thans tijd om in te gaan op de ontwikkeling van het vak en de wereld gedurende de dertig jaren die verlopen zijn sedert ik eerder op deze plaats U mocht toespreken in mijn oratie [60] *Ne Probentur Oracula.*

Ik wil meteen deze gelegenheid gebruiken om twee grove fouten die ik 30 jaar geleden gemaakt heb te corrigeren. In de eerste plaats is mijn vertaling van de Latijnse titel geheel fout: de betekenis is niet dat de orakelen niets bewijzen (zoals de gedrukte tekst stelt), maar dat men de orakelen niet moet raadplegen; zij hebben immers altijd gelogen. De tweede fout is de datum die in de gedrukte versie van de oratie is afgedrukt: de voorpagina vermeldt dat de rede is uitgesproken op maandag 18 april maar een blik op een eeuwigdurende kalender, dan wel een exemplaar van het jaar 2008, zal U leren dat de bewuste maandag op 21 april viel. Dat komt ervan als je een dergelijk stuk drukwerk geheel zelfstandig gaat uittypen.

De boodschap die ik dertig jaar geleden wilde meegeven is dat wij de resultaten die het gebruik van de computer ons oplevert dienen te benaderen met een gezonde dosis wantrouwen. De vraag is of wij op dit punt dertig jaar later er anders over moeten denken.

De technische vooruitgang gedurende deze periode is overweldigend geweest. In 1980 hadden wij geen algemeen toegankelijk internet, geen email, geen web, geen Windows systemen, geen mobieltjes, en, uitgezonderd een gering aantal hobbyisten, geen privé computers in de huiskamer.

Tekstverwerking met de computer stond in de kinderschoenen, en zelf schreef ik al mijn artikelen en brieven op een IBM schrijfmachine met verwisselbare koppen. Computer uitvoer verscheen op een regeldrukker waarmee in een taal als Fortran gemene trucs konden worden uitgehaald, en grafische terminals waren dure apparaten voor experimenteel onderzoek. Kleuren op een beeldscherm was een zeldzaamheid.

Als wij niet contant betaalden dan ging dat niet met een bankpas maar met een Eurocheque. Wij beschikten over een uitgebreide bibliotheek met papieren edities van tijdschriften, en wij ruilden rapporten met bevriende instituten overal in de wereld. Verder leefden wij in een Europa dat in twee stukken was verdeeld door het IJzeren Gordijn.

Ik reken mij bepaald niet tot een vroege gebruiker van de nieuwe technologie.[5] Kort voor mijn vertrek naar de USA kreeg ik in december 1984 een eerste Mac op mijn werkplek. De eerste laserprinter voor mijn groep moet rond 1987 zijn geplaatst toen wij op de vijfde verdieping van het gebouw B/C van het Roeterseiland woonachtig waren. De zegeningen van email heb ik mogen ervaren tijdens mijn Amerikaanse verblijf in 1985 waar ik binnen IBM de luxe positie had om verbonden te zijn aan het Research Laboratorium te San Jose, een van de weinige IBM instellingen waar de medewerkers vrije toegang hadden tot het groeiende internet, en via dit medium heb ik met het thuisfront kunnen communiceren. Ik heb tijdens dat verblijf ook voor het eerst artikelen geschreven op een computer. Na de verhuizing naar de Plantage Muidergracht heb ik gebruik mogen maken van een reeks steeds groter wordende Mac's, ook nadat rond 1990 er een van mijn kamer is gestolen. Aan de zegeningen van het web heb ik mij pas in de latere jaren 90 blootgesteld. Ik moet bekennen dat ik nooit op mijn inmiddels tien jaar oude Windows laptop gebruik heb gemaakt van wireless verbindingen. Ik gebruik deze laptop tegenwoordig alleen om er Powerpoint presentaties op te prepareren of af te spelen, en om er Civilisation II op te spelen.

5. Het is dan ook een ironie van de geschiedenis dat het drukwerk voor de uitnodiging voor deze bijeenkomst een van de eerste gelegenheden is geweest waarin onze Faculteit de nieuwe huistijl van de UvA heeft mogen gebruiken.

Thuis had ik wel toegang tot meer geavanceerde technologie, aangezien Ghica wel tot de vroege gebruikers kan worden gerekend. Soms kon ik daarvan gebruik maken; zo heb ik rond 1984 benoemingsrapporten kunnen schrijven op de BBC/Acorn computer thuis die primair bestemd was om er spelletjes voor de zonen op te programmeren, dan wel de klassieke spelletjes zoals Pacman te spelen die in die dagen daarvoor verkrijgbaar waren. De floppen waar deze rapporten op staan zal ik nog wel ergens hebben liggen, maar apparatuur om ze te lezen hebben we niet meer in werkende vorm. Bij het opruimen vorig jaar trof ik nog enkele transparanten aan die geschreven zijn op de BBC, en vervolgens zijn afgedrukt en op plastic zijn gekopieerd. Handheld computer spelletjes verschenen rond 1982 in huis, tien jaar later gevolgd door

6. Afleveren kun je het amper noemen; Ghica trof op een avond bij thuiskomst een stel dozen aan in de tuin van de buren, waarvan de inhoud destijds een waarde vertegenwoordigde van een middenklasse auto

de eerste Nintendo. De eerste IBM PC/AT werd begin 1986 afgeleverd.[6] Nadien zijn er elke drie tot vier jaar nieuwe computers in huis gekomen, en nam het aantal computers ook geleidelijk toe dank zijn de komst van portables, en uiteraard later de laptops. Op dit moment staan er thuis twee desktop computers naast twee laptops en twee netbooks; de oudere apparatuur die niet meer wordt gebruikt maar wel wordt bewaard tel ik hierbij niet mee.

Ik kan U een simpele vraag stellen die laat zien hoezeer de computer tegenwoordig is doorgedrongen tot ons dagelijkse leven. De vraag luidt: *Hoeveel computers heeft U vanmiddag bij U?* Voor mij persoonlijk is het antwoord op deze vraag: 10. U ziet, dan wel weet de aanwezigheid van de laptop waarmee ik U de afbeeldingen vertoon, maar onder mijn toga zit als vanouds een camera, die vanwege haar digitale karakter een computer bevat. Mijn mobieltje zit in het heuptasje, tezamen met de overige zeven computers die verscholen zitten in verschillende bankpassen, creditcards en een kortingskaart van de NS. Het aantal is nog redelijk laag omdat ik niet ook nog met organisers e.d. rondloop, en geen spelcomputer in mijn achterzak hoef mee te nemen om kleinkinderen zoet te houden want die hebben wij nog niet.

Onze nieuwe auto bevat een onbekend aantal computers om het apparaat te besturen, en hetzelfde geldt voor een groot aantal van onze huishoudelijke apparaten.

Wij mogen dus constateren dat wij in ons dagelijkse leven tegenwoordig in veel grotere mate afhankelijk zijn van computers dan zich dertig jaar geleden liet voorzien. En de vraag is of deze computers of meer specifiek de daarop gebruikte programma's tegenwoordig betrouwbaarder zijn dan dertig jaar geleden.

De Software crisis waarmee wij dertig jaar geleden werden geconfronteerd is allerminst opgelost. Wel is er op het gebied van de programmatuur die verwerkt zit in apparaten zoals auto's en vliegtuigen grote vooruitgang geboekt op het gebied van de verificatie ervan door middel van Model Checking technieken, een technologie die gefundeerd is op uit de Theoretische Informatica afkomstige begrippen zoals eindige automaten en de temporele logica. Echter, het correct modelleren en implementeren van bestuurlijke en bedrijfskundige processen en procedures in de samenleving is tot vandaag toe voor de informatici, ongeacht of het theoretici, practici, of programmeurs betreft, een maatje te lastig gebleven. Hetzelfde geldt voor het correct houden van de bedrijfssystemen op onze standaardapparatuur getuige de maandelijkse updates die wij toegezonden krijgen via het internet.

Oorzaak van dit verschil zal ongetwijfeld zijn dat wij het gewenste gedrag van een auto of een vliegtuig beter begrijpen dan het gedrag van de samenleving of een onderdeel ervan. Ik zal hier verder niet op ingaan want deze problematiek valt immers buiten mijn eigen domein van competentie.

Er zitten aan deze ontwikkeling een tweetal aspecten die mij grote zorgen baren, en waarvan ik mij afvraag of de ontwikkelingen niet veel te ver zijn doorgeslagen. Beide aspecten vinden hun wortel in de observatie dat onze samenleving de nieuwe technologie veelal hanteert als vervanging van in plaats van uitbreiding van het bestaande.

Een voorbeeld. Tien jaar geleden deed een bedrijf aangifte voor de belastingen op een formulier, maar tegenwoordig moet dat via digitale aangifte. Privé personen hebben gelukkig nog niet de verplichting opgelegd gekregen hun aangifte digitaal te verzorgen; zij mogen het wel (en het is nog maar de vraag hoelang het zal duren voordat digitale aangifte ook verplicht zal zijn voor particulieren).

Ik heb mij altijd de vraag gesteld of een samenleving die nog steeds het gebruik van computers en het functioneren ervan in de maatschapij geen duidelijke plaats heeft gegeven in de basisopvoeding, het recht heeft om van ondernemers en/of andere burgers te eisen dat zij van deze hulpmiddelen gebruik maken. Het lijkt op een aan de burger opgelegde verplichting zich per auto te verplaatsen, zonder dat de overheid die de verplichting oplegt ook de verantwoordelijkheid op zich neemt om het nodige rijonderwijs te verzorgen.

In onze samenleving geldt dat er geen verplichting bestaat om een bankrekening te hebben maar het dagelijkse leven wordt echter wel erg problematisch voor de burger die er geen bezit. Maar ook binnen het betalingsverkeer zijn wij hard bezig de klassieke middelen te vervangen door de digitale, in plaats van de digitale technieken te gebruiken als verrijking van de samenleving. Overal treffen wij tegenwoordig apparaten aan die geen (munt)geld meer accepteren. Niet zo lang geleden werd mij bij een bezoek aan een kantine bij onze zusterinstelling in Utrecht duidelijk gemaakt dat ik werd verondersteld te betalen met plastic. Men kon nog wel een uitzondering maken en met klassiek geld afrekenen omdat men nu eenmaal rekening moest houden met al die buitenlandse bezoekers die geen chipkaart hebben die overweg kan met ons Nationale digitale betalingssysteem.

Ik vind dit een ontwikkeling die strijdig is met het primaire doel waarvoor onze voorouders in een ver verleden het geld hebben uitgevonden: het moet een universeel geaccepteerd betaalmiddel zijn. En ik ben ongevoelig voor het argument dat het reduceren van de hoeveelheid contant geld dat in de samenleving circuleert help om de misdaad te bestrijden en de veiligheid te vergroten. Digitale betaalmiddelen worden ook gekraakt, regelmatig worden in ons land skimmers gegrepen, en de handel in gestolen creditcardgegevens tiert welig. En waarom zouden wij ons op het punt van de inrichting van onze samenleving de wet moeten laten voorschrijven door criminelen.

Wij zien deze ontwikkelingen op meerdere gebieden. De reiziger die een willekeurige plek in Nederland bezoekt moet zich afvragen of hij ter plekke wel in staat is de plaatselijke parkeermeter te betalen, zeker als hij uit het buitenland komt. Vergelijkbare omstandigheden zullen zich voordoen bij het gebruik van het openbare vervoer als onze OV Chipkaart landelijk is ingevoerd, aangezien ik niet verwacht dat de daar gebruikte betaalapparatuur wel universeel zal zijn.

Het komt er uiteindelijk op neer dat in onze samenleving een deel van de mensheid wordt uitgesloten als zij om welke reden dan ook geen gebruik kunnen maken van deze gedigitaliseerde transactiestromen, hetzij omdat zij van elders komen en tijdelijk in ons land willen verblijven, hetzij omdat zij de apparaten niet kunnen hanteren vanwege lichamelijke of geestelijke beperkingen of ouderdom, dan wel ze niet willen gebruiken omdat ze de boel niet vertrouwen. Wantrouwen dat geheel wordt gerechtvaardigd door de voortdurende stroom van berichten waarin gemeld wordt dat er weer een fout is opgetreden of een systeem is gekraakt. De verantwoordelijkheid voor het opleggen van deze systemen ligt uiteraard niet bij de technici die naar eer en geweten deze systemen ontwikkelen, maar bij de bestuurderen die met onvoldoende gevoel voor technologie de mogelijkheden ervan overschatten terwijl ze tegelijkertijd de bezwaren ervan onderschatten.

Mijn tweede zorg heeft betrekking op het behoud van de artefacten van onze cultuur in de gedigitaliseerde wereld. Als U toegang heeft tot een digitaal bestand heeft U niets zolang U niet beschikt over de software om dit bestand te kunnen lezen of bekijken, en de apparatuur om deze software te kunnen verwerken. Helaas is in de soft- en hardware industrie tegenwoordig de levensduur van een producttype vaak korter dan de houdbaarheid van het opslagmedium waarop deze producten hun informatie plegen op te schrijven. Gevolg: het oude apparaat of de oude computer mag niet worden weggegooid voordat de opgeslagen gegevens zijn geconverteerd naar het formaat dat het nieuwe product ook kan verwerken. Dit beginsel in volle gestrengheid naleven vereist een grotere discipline dan wij gewoonlijk op plegen te brengen, en niemand heeft behoefte aan een samenleving die zodanig is ingericht dat het tijdig converteren van de gegevens kan worden afgedwongen, want deze mate van disciplinering zal ongetwijfeld de installatie van een dictatuur vragen.

Met betrekking tot de houdbaarheid van gegevens is het overigens opmerkelijk te constateren dat deze in de loop van de geschiedenis alleen maar achteruit lijkt te zijn gegaan. Kleitabletten uit Mesopotamië kunnen na 4000 jaar nog steeds worden gelezen; papyrus rollen houden het ook duizenden jaren uit, en perkament heeft ook een langere levensduur dan het papier dat wij na de Industriële revolutie zijn gaan gebruiken. De levensduur van slecht papier is

nog altijd langer dan die van een diskette of een magneetband. Hoe het zal gaan met Cd-roms en USB sticks is nog onduidelijk.

Het is dus niet alleen zo dat de nieuwe hulpmiddelen ons in staat stellen steeds meer informatie te verzamelen en op te slaan (een ontwikkeling die er op zich zelf al toe zal leiden dat wij in deze informatie zullen verdrinken), maar wij zullen ook keer op keer ervaren dat de informatie waarover wij meenden te beschikken ontoegankelijk is geworden. Dit gaat veel sneller dan men denkt. Een voorbeeld uit onze directe omgeving: Ongeveer 15 jaar lang hanteerde de Mac een afwijkend opslagformaat voor 3.5 inch diskettes. De machine die ik rond 1998 op mijn bureau kreeg kon dat formaat nog lezen naast het standaard formaat waarop de Mac destijds overging; de modellen die rond 2003 werden aangeleverd konden dat niet meer, een aanpassing waaraan destijds amper ruchtbaarheid werd gegeven.

Aangezien een deel van de documenten van ons instituut waren bewaard op de klassieke Mac diskettes was toegang tot een verouderde computer noodzakelijk toen deze documenten na tien jaar voor een of andere evaluatie gebruikt moesten worden. Gelukkig was ik destijds zoals gebruikelijk traag met de vervanging van mijn apparatuur zodat mijn oudere computer nog aanwezig was.

Digitalisering speelt ook een belangrijke rol binnen onze bibliotheek. Eind jaren 90 heeft onze instelling, zoals vrijwel alle instellingen het naar mijn mening onzalige besluit genomen om de papieren abonnementen op tijdschriften die in de digitale bibliotheek beschikbaar zijn af te stoten, en daarbij de aanwezige exemplaren die de uitgevers gedigitaliseerd aanbieden te verwijderen uit de bibliotheek om deze (uitgezonderd een laatste exemplaar in Amsterdam dan wel Nederland) weg te gooien. De motieven zullen ongetwijfeld van financiële aard zijn geweest: minder kosten, minder personeel, minder vloeroppervlak. Dat het niet handelt om de kosten van aanschaf blijkt wel uit het inmiddels gevolgde beleid dat schenkingen van boeken en/of tijdschriften van medewerkers niet meer geaccepteerd mogen worden. Allemaal ontwikkelingen die mij zo zeer tegenstonden dat ik rond die periode mijn betrokkenheid met de bibliotheek heb beëindigd (ik was gedurende een periode van ca 15 jaar de voorzitter van de bibliotheekcommissie voor Wiskunde en Informatica aan onze instelling). Of na deze digitaliseringslag de informatie toegankelijk is gebleven is nog maar de vraag: informanten vertellen mij dat zij wiskundige artikelen zijn tegengekomen die op een zodanige resolutie zijn ingescand dat een aantal van de super-super-indices niet meer te lezen zijn, hetgeen de juiste interpretatie van de afgedrukte formules ernstig bemoeilijkt.

Ik heb geen enkel vertrouwen dat een digitale bibliotheek op de langere termijn een werkbare oplossing zal zijn voor onze informatievoorziening. Er is

een fundamenteel verschil. De bezitter van een tijdschrift bezit een stuk papier dat van nature de neiging heeft te blijven bestaan, zolang de bezitter een redelijke mate van zorg betracht en de stad niet tegelijkertijd bezig is een ondergrondse te laten aanleggen door een door criminelen geïnfiltreerd bouwbedrijf zoals we het afgelopen jaar hebben kunnen beleven bij onze Oosterburen. De bezitter van een digitaal document heeft een recht verworven en rechten kunnen in deze wereld nu eenmaal spontaan verdampen. Er is geen garantie dat de commerciële uitgever waarmee wij vandaag een contract sluiten inhoudende de eeuwige toegang tot de huidige jaargangen van een tijdschrift niet over enkele jaren blijkt te zijn overgenomen door een stelletje geldwolven die hun speculatieve handel combineren met de fundamentalistische opvatting van de krijgsheer die na de inname van Alexandrie over de daar gevestigde Wereldbibliotheek het oordeel velde: *als het in de Koran staat is het overbodig, als het niet in de Koran staat is het schadelijk, dus de brand er in.* Ongeacht of deze fabel al dan niet historisch waar is, meen ik te moeten constateren dat er genoeg godsdienstfanaten van verschillende religies in deze wereld rondlopen die vergelijkbare opvattingen over de relatie tussen geloof, wetenschap en waarheid koesteren, en die daarnaast over voldoende kapitaal beschikken om een dergelijke acquisitie te kunnen plegen.

Kort samengevat: de eigenaar van een klassiek papieren boek of document, weet wat hij bezit en heeft goede redenen om te mogen geloven dat hij dat object ook over tien jaar nog steeds bezit en het over tien jaar nog steeds kan lezen en begrijpen. De eigenaar van het recht op digitale toegang weet amper meer wat hij bezit, laat staan dat hij er op mag vertrouwen dat hij over tien jaar er nog steeds bij kan, en om het te lezen zonder zijn ogen te vermoeien door het staren naar een beeldscherm, moet hij er alsnog een afdruk op papier van maken (die hij dan uiteraard weer tien jaar lang kan bewaren, maar dat vereist wel meer organisatie dan het plaatsen van een rijtje tijdschriften in een boekenkast en meer opslagruimte op de werkplek dan onze broodheren ons in de nieuwbouw te bieden hebben). Welke garantie hebben wij dat wij over tien jaar nog steeds toegang hebben tot onze huidige bestanden en dat die met de dan aanwezige apparatuur nog steeds leesbaar zijn, en wat zijn deze garanties nog waard als de economische crisis echt toeslaat?

Terwijl de persistentie van de toegankelijkheid tot het canonieke archief van de wetenschap in de knel komt zien wij dat tegelijkertijd de hoeveelheid informatie waar wij toegang toe hebben gigantisch toeneemt. Via het internet kan immers iedereen aan iedereen informatie beschikbaar stellen, maar de betrouwbaarheid van deze informatie valt niet te garanderen. Het verschil tussen de wetenschappelijk geaccepteerde feiten en de beweringen die dagelijks circuleren op het internet is voor de gemiddelde burger onzichtbaar geworden.

Overheden en andere gezagdragers weten zich geen raad met dit verschijnsel, en verliezen hun geloofwaardigheid. Dit vertaalt zich uiteindelijk in falende vaccinatie campagnes en onuitroeibare broodje-aap verhalen. De waarschuwing van Jokaste blijft even geldig als dertig jaar geleden: *Ne Probentur Oracula.*

De gevolgen van deze ontwikkeling zullen op langer termijn zichtbaar worden. Mijn favoriete wijze om deze gevolgen te schetsen is de fundamentele vraag waar de archeologen in de 24e eeuw mee zullen worstelen: *Hoe is het mogelijk dat een hoog ontwikkelde samenleving aan het begin van de 21e eeuw plotseling is opgehouden documenten en archieven achter te laten zonder dat er sprake was van wereldomvattende Natuurrampen of een Wereldoorlog?*

Over de eigen Instelling

Dertig jaar geleden moest de opleiding Informatica aan deze instelling nog worden opgestart. Met een betrekkelijk kleine groep medewerkers waarvan ik toch hoop er vandaag een aantal in de zaal aan te mogen treffen, hebben wij een programma opgezet en zijn wij in 1980 met ongeveer zestig studenten van start gegaan. In het tweede jaar werd het programma al weer ingekort van vijf naar vier jaren, een ontwikkeling die veel later weer is teruggedraaid toen de exacte studies terug gingen naar vijf jaar. Het aantal studenten in toegenomen tot boven de honderd in de begin jaren 90 en nadien weer ingestort. De studie is opgesplitst in drie onafhankelijke programma's door de afsplitsing van Bestuurlijke Informatica en AI. Vervolgens kwam de invoering van de Bachelor Master structuur en de invoering van de eenjarige Masters Software Engineering en Systeem en Netwerk Beheer.

Gedurende diezelfde periode is de inrichting van de Universiteit meerdere malen gereorganiseerd: MI/ITW werden samengevoegd met het Instituut voor Propedeutische Wiskunde, de Facultaire Vakgroep Informatica werd opgericht en ging na drie jaar op in de Faculteit Wiskunde en Informatica, die via een kortlevende fusie met Natuur en Sterrenkunde is opgegaan in onze huidige faculteit FNWI. Toen het op dit punt rustig werd begon men aan de onderwijsinstituten, bachelor- en masterscholen en onderzoeksinstituten. Het zal U wellicht niet verbazen als ik U vertel dat het mij gedurende het laatste jaar dat ik optrad als voorzitter van verschillende examencommissies niet meer duidelijk was waar deze commissies inmiddels in het organogram geplaatst dienden te worden. Dat was ook niet belangrijk want het was mij duidelijk wat mijn taak was en hoe ik die diende uit te voeren.

Een ontwikkeling op dit gebied die ik alleen maar als positief kan ervaren is de officiële oprichting van ons ILLC als onderzoeksinstituut. Dertig jaar

geleden was er een groep samenwerkende taalfilosofen en wiskundige logici die, versterkt met een afvallige wiskundige die zich had omgeschoold tot informaticus, de taak op zich hebben genomen om een voor de wereld van de Mathematische logica een volstrekt alternatief perspectief op dit klassieke vakgebied te bieden en daar een onderzoeksinstituut rond te willen opbouwen. Het perspectief dat de logica er niet alleen is ter groter glorie van de wiskunde en zichzelf, maar veeleer als richtinggevend instrument op alle gebieden waar informatie wordt verwerkt, in het bijzonder de taalkunde en de Informatica, maar ook in Sociale wetenschappen en in de Economie. Het is mij een groot genoegen om de totstandkoming van dit instituut te hebben mogen meebeleven, en ik hoop dat het instituut zal standhouden in de zware tijden die op ons afkomen. Het moet kunnen: de formule is goed.

De afgelopen tien jaar heb ik alleen nog maar vakken verzorgd voor master studenten en betrof het vakken die voor geen enkel programma verplicht waren. Dit heeft er ongetwijfeld toe geleid dat ik geen zuiver beeld meer heb gehad op de studenten populatie als geheel. Ter compensatie kan ik natuurlijk stellen dat ik in feite ieder student aan het einde van diens studie te zien kreeg op het examen. Dit geeft echter een vertekend beeld want de studenten die het niet hebben gehaald blijven zo ongezien en dat zijn er meer dan ons en de instelling lief is.

Ik kan wel met genoegen constateren dat de kwaliteit van het werk dat mij door deze geslaagde studenten wordt voorgelegd mij goed is bevallen, en het heeft mij geholpen de ontwikkeling van het vakgebied Informatica met al haar toepassingen te blijven volgen, niet geremd door de begrenzingen van mijn eigen specialisme. De kwaliteit van onze studenten moge ondermeer blijken uit het feit dat drie keer de door mij voorgedragen kandidaat winnaar is geworden van de prestigieuze prijs uitgereikt door de Koninklijke Hollandse Maatschappij voor Wetenschappen voor het beste afstudeerwerk van het lopende jaar in de Informatica in Nederland. Aan deze landelijke competitie doen alle landelijke opleidingen mee. Een andere afstudeerder is bekroond met de afstudeerprijs aan de eigen instelling.

De traditie wil dat aan het einde van deze rede ruimte wordt gegeven aan een of meerdere woorden van dank gericht aan personen en instellingen die het leven van de emeritus hebben veraangenaamd. Ik zal deze traditie niet volgen, aangezien dit in mijn geval onbegonnen werk is. Vele personen die in het al dan niet uitgesproken gedeelte van deze voordracht zijn genoemd ben ik dank verschuldigd, en voor zover uw naam vanmiddag niet is uitgesproken kunt U nog altijd de gedrukte versie nalezen om te zien of U tot de gelukkigen behoort die in de tekst zijn vermeld.

Ik wil hierop een uitzondering maken en het is een collectief dat hiervoor in aanmerking komt: de 22 doctores die ik als promotor of medepromotor heb mogen helpen opvoeden. Dank ben ik hun verschuldigd voor het in mij gestelde vertrouwen en het plezier wat ik heb mogen beleven aan de samenwerking die ik met hen heb mogen bedrijven. Ik beken: door mijn keuze voor van Wijngaarden als promotor heeft U slechts weinig voorouders in de promotie genealogie, aangezien de promotor van van Wijngaarden, Biezeno zelf geen doctorsgraad bezat voordat hij een eredoctoraat mocht ontvangen uit handen van zijn zoon van Wijngaarden. In het bijzonder valt U buiten de boom van nazaten van Korteweg die het merendeel van de Nederlandse Wiskundigen en Informatici omvat. Korteweg is zoals U wellicht recentelijk weer hebt kunnen nalezen de eerste doctor aan deze Universiteit. U mag U echter verheugen in de aanwezigheid van een redelijk aantal broeders en zusteren, en een inmiddels groeiend aantal al dan niet incestueuze kinderen, neven en nichten.

En daarmee, geachte toehoorders, laat ik U over aan de verpozing die de receptie U pleegt te bieden.

References

[1] van Willigenburg, *Egghead betegelt badkamer*, SUM, Specifiek Universitair Magazine, 6(2), april 1996, 42.

[2] Folia, 44(15) Nov 30 1990, pag 9.

[3] Folia, 43(23) Feb 02 1990, pag 7.

[4] J. Aarts & P. van Emde Boas, *Continua as remainders in Compact Extensions*, Nieuw Archief voor Wiskunde (3) 15, 1967, 34-37.

[5] P. van Emde Boas, *Minimally generated Topologies*, Proc Int. Symp. Topology and its applications, Herceg-Novi, Aug 1968, Beograd 1969, pp. 146-152.

[6] P. van Emde Boas, *A combinatorial problem in the semigroup of all finite transformations of a finite set.*, Rep. MC-ZW-09-65.

[7] P. van Emde Boas, *A Combinatorial Problem on Finite Abelian Groups II*, Rep. MC-ZW-07-69

[8] H.W. Lenstra & P. van Emde Boas, *A transfinite generalization of a combinatorial problem on finite Abelian groups*, Rep. MC-ZN-29-69.

[9] D. Kruyswijk & P. van Emde Boas, *A combinatorial problem on finite Abelian groups III*, Rep. MC-ZW-08-69.

[10] W.R. Alford, A. Granville & C Pommerance, *there are infinitely many Carmichael numbers*, Annals Math. 140 (1994), 703-722.

[11] J. Hartmanis & J.E. Hopcroft, *An overview of the theory of computational complexity*, JACM 18 (1972) 444-475.

[12] E.M. Mc Creight & A.R. Meyer, *Classes of computable functions defined by bounds op computation*, Proc ACM STOC 1 (1969), 79-88.

[13] P. van Emde Boas, *Abstract Resource Bound Classes*, Proefschrift Sep 18 1974.

[14] P. van Emde Boas, *Some applications of the Mc Creight-Meyer algorithm in Abstract Complexity Theory,* TCS 7, 1978, 79-98.

[15] P. van Emde Boas, *Berekeningscomplexiteit van bilineaire vormen*, in Colloquium Complexiteit en Algorithmen, MC Syllabi 48.2, 1982, pp. 3-68.

[16] P. van Emde Boas, *A comparison of the properties of complexity classes and honesty classes*, proc ICALP 1, Versailles 1972, North Holland Publ. cie. 1973, pp. 391-396.

[17] P. van Emde Boas, *Ten Years of Speed-up*, proc MFCS 4, Sep 1975, Springer LNCS 32 , 1975, pp. 13-29.

[18] Th.H. Cormen, Ch.E. Leiserson, R.L. Rivest & C. Stein, *Introduction to Algorithms,* third edition, MIT press, 2009.

[19] P. van Emde Boas, R. Kaas & E. Zijlstra, *Design and Implementation of an efficient priority queue*, Math. Syst. Theory 10, 1977, 99-128.

[20] A.V. Aho, J.E. Hopcroft & J.D. Ullman, *The design and Analysis of Computer Algorithms*, Addison Wesley, 1974.

[21] P. van Emde Boas, *An O(nloglogn) On-line Algorithm for the Insert-Extract Min problem*, Cornell Rep. TR 74-221, Dec 1974, online availbale at http://techreports.library.cornell.edu:8081/Dienst/UI/1.0/Display/cul.cs/TR74-221.

[22] P. van Emde Boas, *Computer Science education and the VIN; looking back 30+ years*, presentation at the symposium on the retirement of dr. Walter Hoffmann, 20090116.

[23] P. van Emde Boas, *Preserving order in a forest in less than logarithmic time*, Proc IEEE FOCS 16, 1975, 75-84.

[24] P. van Emde Boas, R.Kaas & E. Zijlstra, *Design and implementation of an efficient priority queue*, Math. Syst. Theory 10, 1977, 99-128.

[25] P. van Emde Boas, *Preserving order in a forest in less than logarithmic time and linear space*, Inf. Proc. Letters 6 (1977) 80-82.

[26] D. Scott & J.W. de Bakker, *A Theory of programs*, unpublished notes, IBM Seminar, Vienna 1969.

[27] J.W. de Bakker, *Recursion, Induction and Symbol Manipulation*, proc. MC-25 Informatica Symposium, MC tracts 37, 1971, pp. 1.1-1.30.

[28] T.M.V. Janssen & P. van Emde Boas, *On the proper treatment of referencing, dereferencing and assignment*, proc. ICALP 4, Jul 1977, Springer LNCS 52, 1977, pp 282-300.

[29] J.H. Conway, M.S. Paterson & U.S.S.R. Moscow, *A headache-causing problem, in Een pak met een korte broek*, papers presented to H.W. Lenstra, jr. Amsterdam, 19770518.

[30] J. Groenendijk, M. Stokhof & P. van Emde Boas, *The Conway Paradox: its solution in an epistemic framework*, proc 3rd Amsterdam Conf. *Formal methods in the study of langauages*, MC Tracts 135, 1980, pp. 87-111.

[31] R. Fagin, J.Y. Halpern, Y. Moses & M.V. Vardi, *Reasoning about Knowledge*, MIT Press, 1995.

[32] A.K. Lenstra, H.W. Lenstra & L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261(4), 1982, 515-534.

[33] I. Smeets, in collaboration with Arjen Lenstra, Hendrik Lenstra, László Lovász and Peter van Emde Boas, *the History of the LLL-Algorithm*, in Phong Q. Nguyen & Brigitte Vallée (eds.), *The LLL Algorithm*, Springer 2010, pp. 1-17.

[34] P. van Emde Boas, *The complexity of linear problems*, Proc. FCT 2, Wendisch Rietz, sep 1979, L. Budach ed., Akademie Verlag, Berlin DDR, 1979, pp. 117-120.

[35] P. Gács & L. Lovász, *Khachian's Algorithm for Linear Programming*, rep. STAN-CS-79-750, July 1979.

[36] P. van Emde Boas, *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*, rep. MI-UvA-81-04.

[37] H. van Emde Boas - Lubsen & P. van Emde Boas, *Compiling Horn-Clause Rules in IBM's Business System 12; an Early Experiment in Declarativeness*, Proc. SOFSEM'98, Springer LNCS 1521 , 1998, pp. 68-88.

[38] C.F.J. Doedens, *Logic Programming and Business System 112*, rep. TR 13.198, IBM INS-DC Uithoorn, 1984.

[39] H. van Emde Boas & P. van Emde Boas, *Storing and evaluating Horn-clause rules in a relational database*, IBM J. of Research and Development 30(1), 1986, 80-92.

[40] SJC Elbers, *De compilatie van willekeurige Prolog structuren in een relationele database*, rep. TR 13.206, IBM INS-DC Uithoorn 1986.

[41] P. van Emde Boas, RL, *a language for enhanced rule nases database processing*, working document, rep. IBM research, RJ 4869 (51299), 1986.

[42] J.K. Lenstra, A.H.G. Rinnooy Kan & P. van Emde Boas, *Interfaces between Computer Science and Operations Research*, MC Tracts 99 , 1978.

[43] P. van Emde Boas, *Machinemodellen en Berekeningscomplexiteit*, Studieweek getaltheorie en compuets Sep 01-05 1980.

[44] P. van Emde Boas, *Computational Complexity and Number Theory*, in H.W. Lenstra & R. Tijdeman eds., *Computational Methods in Number theory,* MC Tracts 154, 1983, pp 133-161.

[45] K. Wagner & G. Wechsung, *Computational Complexity*, Mathematische Monographien 19, VEB Deutscher Verlag der Wissenschaften, DDR, 1986.

[46] C. Slot & P. van Emde Boas, *On Tape versus Core, an application of space efficient perfect hash functions to the invariance of space*, proc ACM STOC 16, May 1984, pp 391-400.

[47] C. Slot & P. van Emde Boas, *The problem of space invariance for sequential machines*, Inf. and Comp. 77 (1988) 93-122.

[48] P. van Emde Boas, *The Second Machine Class 2, an Encyclopaedic View on the Parallel Computation thesis*, in H. Rasiowa, ed., *Mathematical Problems in Computation Theory*, Banach Center Publications 21, 1988, pp. 235-256.

[49] P. van Emde Boas, *Machine Models and Simulations*, in J. van Leeuwen ea. eds., *Handbook of Theoretical Computer Science*, vol A, *Algorithms and Complexity*, Elsevier, Amsterdam, 1990, pp. 1-66.

[50] P. van Emde Boas, *Die lui van het computerparket*, Presentatie gehouden op de wetenschapsdag 8 Oct 2000, http:staff.science.uva.nl/ peter/vloeren/lieden.ppt.

[51] P. van Emde Boas, *The Convenience of tiling*, in A. Sorbii ed., *Complexity, logic and recursion theory*, lect. notes in pure and appl math. 187, 1997, pp. 331-363. Preprint beschikbaar op www.illc.uva.nl/Publications/ResearchReports/CT-1996-01.text.ps.gz

[52] M.R. Garey & D.S. Johnson, *Computability and Intractability; a guide to the theory of NP-completeness*, Freeman 1979.

[53] M.W.P. Savelsbergh & P. van Emde Boas, *BOUNDED TILING, an alternative to SATISFIABILITY?*, Proc. 2nd Frege memorial Conf. Schwerin sep 1984, Acad Verlag, math. Forschung 20, 1984, pp. 401-407.

[54] P. van Emde Boas, *Dominoes are forever*, Proc 1st GTI Workshop, Paderborn, Oct 1982, Rheie Theoretische Informatik UGH Paderborn, 1983.

[55] Excercises page for Games and Complexity toegankelijk via URL: http://staff.science.uva.nl/ peter/teaching/gac09exc.html

[56] P. van Emde Boas, *Computerspelen en de identificatie van objecten*, Athenæum Illustre, 8, dec 1996, 13-16.

[57] P. van Emde Boas, *games in the classroom*, Workshop 2 at OOPSLA'99, *Quest for Effective Examples*, ed. J. Börstler & A. Fernández, UMINF 00.03, Umea University, dept CS. 2000, pp. 37-50.

[58] N. Nisan, *Algorithms for Selfish Agents*, Proc STACS'99, Springer LNCS 1563, 1999, pp. 1-15.

[59] Cursusmateriaal toegankelijk via URL: http://staff.science.uva.nl/ peter/teaching/gac09.html

[60] P. van Emde Boas, *Ne Probentur Oracula*, Oratie Apr 21 1980.