NE PROBENTUR ORACULA

Dr. P. van EMDE BOAS

NE PROBENTUR ORACULA

REDE

Uitgesproken bij de aanvaarding van het ambt van
Gewoon Lector in de Mathematische Informatica
in de Faculteit der Wiskunde en Natuurwetenschappen
aan de Universiteit van Amsterdam
op Maandag 18 April 1980

door

Dr. P. van EMDE BOAS

MC

Mathematisch Centrum - Amsterdam - 1980

Dames en Heeren Bestuurderen van deze Universiteit,
Dames en Heeren Hoogleraren, Lectoren, Docenten, Assistenten en anderszins aan deze Universiteit werkzamen,
Dames en Heeren Studenten,
Beste Bekenden en verwanten,
en voorts Gij allen, die deze plechtigheid met Uw tegenwoordigheid vereert,

Zeer gewaardeerde toehoorders

Ne probentur oracula, quae semper mentiantur;[1]

Niets bewijzen de Orakelen die altijd liegen .

In tegenstelling tot hetgeen U wellicht zult denken, dateren deze in het Latijn neergeschreven woorden uit het begin van deze Eeuw. Toen Igor Strawinsky de behoefte gevoelde een Oratorium te componeren op basis van de Oedipus legende, heeft hij door Jean Cocteau een compacte samenvatting van het drama laten vervaardigen; deze Franstalige tekst is nadien in het Latijn vertaald om aldus een verstarring ervan teweeg te brengen. De geciteerde tekst wordt aan het begin van de tweede acte van het resulterende Oratorium "Oedipus Rex" gezongen door Jocasta. Hoezeer deze van het feilen der orakelen overtuigd is blijkt wel uit het vervolg : *Ne probentur Oracula; Mentita sunt Oracula. Niets bewijzen de orakelen; de orakelen hebben altijd gelogen .*

Het is opmerkelijk te moeten constateren dat woorden van deze strekking niet te vinden zijn in de tragedie van Sophocles, die aan de Strawinsky versie ten grondslag ligt. De corresponderende passage in de Griekse tekst loopt als volgt:

Σὺ νυν λφεἰσ σεαυτὸν ὢν λέγεισ πέρι ἐμου 'πάκουσον καί μάθ' ὑνεκ' ἐστί · σοι βρότειον οὐδὲν μαντικησ ἔχον τέχνησ.[2]

In de vertaling van P.C. Boutens luidt deze passage:

Zet gij die dingen van u af, waarvan gij spreekt, en naar mij luister en laat u beleren dat geen enkel sterfelijk wezen deelt in zienerskunst.[3]

De Pinguin editie met een vertaling van E.F. Watling levert ons de volgende versie:

Then absolve yourself at once. For I can tell you, No man possesses the secret of divination.[4]

De argumenten die Jocasta aanvoert mogen U bekend zijn. In het verleden is door een orakel aan haar gewezen echtgenoot Laios de voorspelling gedaan dat deze door zijn eigen zoon zou worden gedood. Welnu; zoals iedereen weet is Laios op een driesprong vermoord door rovers.

Achteraf kunnen we gemakkelijk de fout in deze redenering aanwijzen. Gebrek aan volledige informatie. Het hele Oedipus drama is erop gericht te laten zien dat de uitspraken van het orakel uitkomen; sterker nog; de pogingen om de vervulling ervan te voorkomen scheppen de noodzakelijke voorwaarden om de verwerkelijking van de voorspelling te laten plaatsvinden.

In de Oedipus legende treedt het orakel driemalig op. Laios krijgt de voorspelling dat hij gedood zal worden door zijn zoon. Effect: hij besluit zijn zoon te laten doden, maar de uitvoerder van deze opdracht voert deze op inadequate wijze uit - Oedipus wordt met doorgesneden pezen te vondeling gelegd, gevonden en groeit op aan een ander hof.

Later ontvangt Oedipus van het orakel de voorspelling dat hij zijn vader zal doden en zijn moeder zal huwen. Effect: hij verlaat zijn vermeende geboorteplaats, en heeft vervolgens de, voor Laios fataal aflopende, ontmoeting op de driesprong. Hierna verlost hij Thebe van de Spynx en krijgt als beloning de Koningin weduwe, waarvan hij niet weet dat zij zijn moeder is, tot echtgenote.

Ten derde male grijpt het orakel in door te eisen dat de moordenaar van Laios gevonden wordt, opdat Thebe verlost zal worden van de pest. Dit bevel leidt ertoe dat de ware toedracht wordt onthuld. Het is tevens van de genoemde orakeluitspraken de enige waarvan de legende niet vermeldt of zij is uitgekomen; wij weten niet of na afloop van het drama de pest inderdaad uit Thebe is vertrokken, alhoewel wij op epidemiologische gronden kunnen vermoeden dat zulks na kortere of langere tijd is gebeurd.

Vanwaar nu mijn voorkeur voor de neo-klassieke variant van deze tekst als gebruikt door Strawinsky ? Het is duidelijk dat in de klassieke passage Jocasta een zwakkere bewering in de mond krijgt gelegd. Het feit dat geen mens de mogelijkheid heeft om in de toekomst te kunnen zien zegt niets over het waarheidsgehalte van orakel voorspellingen, die immers regelrecht van de Goden afkomstig worden geacht te zijn. Door het orakel zelf tot leugenaar te bestempelen wordt ook deze laatste mogelijkheid om tot voorspellingen te komen ontkend. Het is deze sterkere bewering die ik tot thema van mijn rede wil kiezen.

Waarde toehoorders

Wellicht zullen een aantal onder U thans het idee hebben gekregen dat zij getuige zijn van de verkeerde oratie. Wat immers heeft de mathematische informatica te maken met legendarische uitspraken van een orakel ? Ik wil echter met deze rede aansluiten op het pad dat voor mij betreden is door mijn Rotterdamse collega Alexander Rinnooy Kan. Deze heeft immers in zijn oratie, vandaag precies twee jaar en één dag geleden gehouden aan de Erasmus Universiteit, het beeld geschilderd van de wetenschapper als Hogepriester en/of Magier van deze tijd [5]. Het zal dan duidelijk zijn dat in dit licht bezien het tegenwoordig alom gehanteerde hulpmiddel - de Computer - gezien moet worden als het Orakel van onze eeuw. Het is dan ook alleszins gerechtvaardigd ons opnieuw de vraag te stellen of wij de uitspraken van dit hedendaagse Orakel mogen geloven.

Daarnaast is het interessant te zien dat juist in het vak der mathematische informatica, in het bijzonder in de door mij bedreven theorie der berekenbaarheid, het orakel als hulpmiddel voor wiskundige begripsvorming weer helemaal in zwang is. Vele medewerkers, studenten en collegas hebben mij bij andere gelegenheden diverse malen over het orakel horen spreken.

In het vervolg van deze rede wil ik U dan ook een uiteenzetting geven van de rol die het orakel speelt in de theorie der berekenbaarheid, die tenslotte een substantieel deel van het door mij vertegenwoordigde wetenschapsterrein vormt. Nadien keer ik terug tot de cruciale vraag: Indien wij de computer zien als het orakel van deze tijd, mogen wij dan de uitspraken ervan geloven ? Voordat het echter zover komt keren wij eerst terug tot de Griekse Oudheid.

Het Orakel van Delphi

Bij het optreden van het orakel in de Oedipus legende, zullen de meesten onder U denken dat het hier handelt om het Orakel te Delphi. Van alle Orakelen in de Oudheid is dit verreweg het bekendste; deze faam genoot het bovendien in de oudheid zelf in ruime mate. Het is het orakel van Delphi waarvan wij vroeger bij Oude Geschiedenis hebben geleerd dat het de voorspelling aan Koning Croesus heeft uitgesproken dat hij, indien hij de Halys zou oversteken, een groot rijk zou vernietigen. Even bekend is de voorspelling dat houten muren de stad Athene zouden beschermen tegen de inval der Perzen. Wij herinneren ons allemaal het beeld van de priesteres, Pythia geheten, gezeten op een driepoot boven een spleet in de bodem van de Apollo tempel waaruit vulkanische dampen opstijgen, die bedwelmd door deze uitwasemingen uit het binneste der aarde onsamenhangende kreten uitstoot die vervolgens door deskundige priesters op liefst zo dubbelzinig mogelijke wijze worden verklaard en begrijpelijk gemaakt aan de afgezanten van koningen,vorsten en helden.

Dank zij een boekbespreking in het Februari nummer van Scientific American van dit jaar [6], werd ik gewezen op het bestaan van het boek *"The Delphic Oracle, Its Responses and Operations with a Catalogue of Responses"* van de hand van Joseph Fontenrose [7]. Bestudering van dit boek leert ons dat alle bovengenoemde jeugdherinneringen naar het rijk der Fabelen dienen te worden verwezen.

Het Orakel van Delphi was actief gedurende een periode beginnende in de achtste eeuw voor Christus, en eindigende in de late Romeinse tijd toen aan het einde der vierde eeuw de, inmiddels tot het Christelijk geloof bekeerde, Romeinen de nog bestaande Orakelen, met alle andere vormen van waarzeggerij van de aardbodem lieten verdwijnen. Het zal U namelijk bekend zijn dat het Christendom niets op heeft met lieden die de toekomst menen te moeten voorspellen. Raadpleging van Trommius[8] leert ons dat het woord "orakel" in de Heilige Schrift in het geheel niet voorkomt. Andere vormen van waarzeggerij worden incidenteel vermeld, in het algemeen in een ongunstige contekst; een duidelijk en bekend voorbeeld is de passage waarin Saul kort voor zijn dood een waarzegster raadpleegt, terwijl hij zelf een bevel heeft doen uitgaan alle waarzeggers te doen doden. De visitatie leidt tot een ontijdige herkenning en een herhaling van al het onheil dat hem reeds eerder was aangezegd (1 Samuel 28).

Op grond van deze datering alleen al kan worden aangetoond dat de orakelvoorspellingen uit de Oedipus legende nooit afkomstig geweesd kunnen zijn van het Orakel te Delphi; de Oedipus legende betreft gebeurtenissen uit dezelfde legendarische oudheid als de Trojaanse Oorlog (± 1200 voor Christus) .

Joseph Fontenrose verdeelt de lijst van orakel uitspraken die worden toegeschreven aan het Orakel van Delphi in vier categorieën, afhankelijk van de wijze waarop de vermelding van de uitspraak in de wereld is geraakt. Een uitspraak wordt gezien als *Historisch* indien zij vermeld wordt door een auteur die zelf in leven was gedurende de periode waarin de uitspraak moet zijn geschied, hetgeen overigens geenszins zou impliceren dat de weergave juist en correct zou moeten zijn. In zijn lijst zijn 74 uitspraken opgenomen die in deze categorie vallen.

De tweede categoerie, die 268 uitspraken bevat, zijn de *Quasi-historische* uitspraken. Dit zijn orakeluitspraken die moeten hebben plaats gevonden gedurende de historische periode van na 800 voor Christus, maar waarvoor geen vermelding van een tijdgenoot bekend is. Het is uiteraard lastig van deze uitspraken uit te zoeken of ze al dan niet authentiek zijn.

Categorie drie, de *Legendarische* uitspraken, wordt gevormd door 176 voorspellingen die hetzij voor 800 voor Christus zouden moeten zijn uitgesproken, hetzij slechts bekend zijn uit tijdloze volksvertellingen en fabels. Tenslotte zijn er nog 16 voorspellingen die het predicaat *Fictief* hebben meegekregen; dit zijn uitspraken die zichtbaar zijn uitgevonden door dichters en schrijvers ter verfraaing van hun producten.

Een onderverdeling naar onderwerp, strekking en formulering van de verschillende uitspraken laat een aantal opvallende verschillen zien tussen de uitspraken in de verschillende categorieën. Zo blijkt 73 % van de Historische antwoorden betrekking te hebben op godsdienstige handelingen (offers, sanctionering van het instellen van een cultus etc.) terwijl slechts 29 % van de legendarische antwoorden in deze groep vallen. Mensenoffers worden daarentegen alleen maar genoemd in legendarische antwoorden; er is geen historische uitspraak bekend die vraagt om een mensenoffer. Van de Legendarische uitspraken heeft 67 % betrekking op wereldlijke en/of huis,tuin en keuken aangelegenheden terwijl dit slechts geldt voor 13.5 % van de Historische antwoorden. Er zijn geen Historische dubbelzinnige antwoorden bekend, terwijl van de 176 Legendarische uitspraken er 20 kunnen worden gebrandmerkt als dubbelzinnig.

Het blijkt dan ook zo te zijn dat de drie voorspellingen uit de Oedipus legende thuis horen in de Legendarische groep (L. 17, 18 & 19 in de lijst van Fontenrose), terwijl de antwoorden aan Croesus en aan de Atheners Quasi-Historisch worden genoemd (Q. 100 en Q . 146 resp.); deze beide laatste uitspraken komen overigens mede tot ons via de Historieën van Herodotus, maar gegeven het feit dat deze zelf de inval van de Perzen niet heeft meegemaakt, is dit onvoldoende grond om de laatstgenoemde voorsplelling te beschouwen als historisch; Fontenrose heeft dan ook diverse argumenten om te vermoeden dat de uitspraak niet historisch is.

De weergave van het ritueel boven de spleet blijkt eveneens een verzinsel van slecht lezende historici te zijn. In de historische teksten is er sprake van een inspirerende πνευμα die niets te maken heeft met dampen uit de aarde. Geen klassiek auteur heeft het ooit over een spleet in de bodem en hedendaagse geologen hebben er ook geen spoor van kunnen vinden. We mogen aannemen dat de Pythia geheel bij haar eigen zinnen de bezoekers van het orakel in duidelijke bewoordingen heeft toegesproken; in het algemeen deed zij dit in proza teksten; als er sprake is van antwoorden in versvorm dan was dit een kwestie van hetzij voorkennis omtrent de te stellen vraag, hetzij vakmanschap bij het sneldichten.

Ik hoop U met deze samenvatting van enkele opvattingen, zoals deze door Fontenrose op heldere en overtuigende wijze zijn weergegeven in zijn zeer lezenswaardige boekwerk, niet zozeer te hebben overtuigd van de onbetrouwbaarheid van het Orakel van Delphi zelve, als wel van het twijfelachtige gehalte van al hetgeen wij er in onze geschiedenis lessen over hebben geleerd. Om het Orakel te kunnen beoordelen moeten wij beginnen met te twijfelen aan alles wat wij erover dachten te weten.

Het Orakel van Turing

Ik wil nu met U een sprong in de tijd nemen die ons voert naar het begin van deze eeuw. Onderzoekingen in de grondslagen der wiskunde hadden het noodzakelijk gemaakt te komen tot een goede definitie van het begrip "effectief berekenbaar" . Gedurende de dertiger jaren van deze eeuw is een dergelijke definitie van de grond gekomen. Het begrip berekenbaarheid bleek zich op diverse manieren te laten beschrijven, terwijl nadien de gelijkwaardigheid van de verschillende beschrijvingsmethoden kon worden aangetoond.

Een van de meest overtuigende en tot op de huidige dag in zwang zijnde beschrijvingsmethoden is in 1936 gegeven door de Britse Wiskundige A.M. Turing. Deze lanceerde in een artikel[9] zijn ontwerp voor de thans naar hem genoemde Turing Machine. Wij kunnen ons dit abstracte model van een computer dat is ontwikkeld in een tijd dat de voorlopers van onze huidige computers nog ontwikkeld dienden te worden (de vroegste automatische digitale rekenautomaten dateren uit de veertiger jaren van deze eeuw), ongeveer als volgt voorstellen[10].

De machine bestaat uit een eindig controleorgaan, waarin een eindig programma ligt opgeslagen, en een (potentieel oneindige) band bestaande uit cellen waarin een symbool uit een eindige collectie kan worden geschreven. Gemakshalve kunnen wij zelfs veronderstellen dat er, naast het blanco symbool waarmede de band die vers uit de fabriek komt wordt geacht te zijn beschreven, slechts twee verschillende symbolen zijn die wij zullen aanduiden met 0 en 1 . Het programma kent een zevental verschillende typen van instructies, te weten:

schrijf een 0
schrijf een 1
beweeg naar links
beweeg naar rechts
spring naar adres i
spring naar adres i als het thans gelezen symbool een 0 is
stop

Het adres waarheen eventueel gesprongen dient te worden is als label aangebracht voor de eerste van de reeks instructies waar de uitvoering van het programma dient te worden voortgezet.

Het berekenen van een functie met deze machine verloopt als volgt: Men brengt een codering van de invoer gegevens aan op een overigens blanco band, men voert deze in in de machine zodanig dat de machine het eerste beschreven symbool leest, en men start de machine in een daartoe gemarkeerde startinstructie. Hierna vertelt op ieder tijdstip het programma in de machine wat er moet gebeuren. Indien (hetgeen altijd gehoopt wordt) de situatie optreedt dat een stop-instructie wordt uitgevoerd beschouwt men de berekening als beëindigd; het resultaat van de berekening staat dan in gecodeerde toestand op de band.

Het is een moeizaam, doch voor de studenten leerzaam, betoog waarin de docent theoretische informatica waar moet maken dat met het boven beschreven uiterst simpele machine model in principe alles kan worden gedaan wat wij tegenwoordig op onze grote computers plegen uit te rekenen. Dit bewijs wordt in de practijk dan ook zelden tot nooit gegeven. Men volstaat met aan te tonen dat in dit reken model alles berekend kan worden wat berekenbaar is volgens alternatieve definities van bv. Church of Kleene[11] terwijl de omkering hiervan eveneens waar is. Vervolgens laat men zien dat het mogelijk is de programmas van een Turing machine op een zodanige wijze te coderen dat men een Universele machine kan construeren die, gegeven als invoer een programma i en een argument x, de berekening van de Turing machine met programma i op argument x simuleert. De hiertoe benodigde technische truukjes imponeren de student voldoende om hem te doen geloven dat al het overige ook wel zal kunnen.

Op dit punt aangekomen is het eenvoudig geworden een voorbeeld te geven van een probleem dat het vermogen van de Turing machine te boven gaat: het beruchte "stop-probleem". Kan men op effectieve wijze vaststellen of een gegeven berekening, indien eenmaal gestart, er ooit toe zal overgaan een stop-instructie uit te voeren ? Het antwoord op deze vraag luidt ontkennend. Met gebruik making van een hypothetische machine die het termineren van berekeningen voorspelt, kan men de universele machine overvoeren in de diagonaliserings machine, die op invoer i nagaat of programma i op invoer i al dan niet zal termineren; is dit niet het geval dan termineert de diagonaliserins machine met antwoord nul ; is het echter wel zo dat machine i op invoer i termineert dan zal de diagonaliserings machine deze berekening tot het einde toe simuleren, om vervolgens met een ander antwoord te voorschijn te komen. Het gevolg is dat de diagonaliserings machine voor iedere invoer stopt, en daarnaast zich verschillend gedraagt van de Turing machine met programma i op invoer i, wat dit ook voor programma moge zijn. Er kan dus nooit een Turing machine bestaan die doet wat de diagonaliserings machine doet.

Deze tegenspraak laat zien dat onze hypothetische machine, die het stop-probleem voor ons moest oplossen niet bestaat. Als wij willen weten of een bepaalde berekening al dan niet stopt dan zullen wij deze moeten uitvoeren.

Het blijkt dat deze laatste bewering nog wat kan worden verscherpt. Niet alleen is het mogelijk terminatie van een berekening te voorspellen, maar het is ook niet mogelijk om de terminatie van een berekening vast te stellen in wezenlijk minder veel rekentijd dan de Turing machine waar het over gaat er zelf voor nodig zou hebben. Deze "afgeknotte" versie van het stop-probleem speelt in de complexiteitstheorie eenzelfde rol als het originele stop-probleem in de recursietheorie.

Gegeven de aanwezigheid van berekenbare en niet berekenbare functies kan men zich de vraag stellen of sommige niet berekenbare functies minder berekenbaar zijn dan andere. Beschouw bijvoorbeeld de volgende twee verzamelingen van Turing machine programmas :

Halt = de verz. van programmas die voor geschikte invoer stoppen

Total = de verz. van programmas die voor iedere invoer stoppen

Het blijkt dat de verzameling Halt beter berekenbaar is dan de verzameling Total ; men kan namelijk, gegeven een programma i op effectieve wijze dit programma overvoeren in een programma s(i) dat niets anders doet dan het zoeken naar een geschikte invoer waarvoor programma i stopt. Als i een element is van de verzameling Halt zal dit zoekproces altijd termineren zodat s(i) een element is van de verzameling Total , terwijl bij het ontbreken van een geschikte invoer voor programma i het zoeken van s(i) eveneens tot in het oneindige zal voortduren. Voor de recursietheoreticus betekent dit dat wij in feite een reductie van het probleem Halt tot het probleem Total hebben aangegeven. Het is nu precies bij de wiskundige formalisering van dit reductie begrip dat wij opnieuw het orakel tegenkomen.

Om te modelleren wat het betekent een berekening uit te voeren waarbij men kan beschikken over extra informatie, voorzag Turing zijn machine van een orakel[12]. Er kwam een nieuw type instructie bij dat voorzag in een vraag aan het orakel:

spring naar adres i op grond van het orakel

Uitvoering van deze instructie houdt in dat in één eenheid van rekentijd de gehele inhoud van de band wordt beschouwd door het orakel; behoort deze tot een verzameling die het orakel wenst te accepteren dan spring de machine naar adres i , zonee dan gaan wij verder bij de volgende instructie.

Merk op dat het helemaal niet gezegd is dat de taak van het orakel niet door een machine kan worden over genomen. Het kan evengoed de bedoeling zijn het orakel in te schakelen om alleen maar tijd te besparen. In deze laatste vorm is het orakel van Turing op gaan treden in de hedendaagse complexiteitstheorie. Een markant voorbeeld hiervan moge dit illustreren.

Bij onze beschrijving van Turing machine programmas zijn we er gemakshalve van uitgegaan dat een adres dat genoemd wordt in een sprong-instructie slechts op één plaats in het programma als label optreedt. Laten wij deze eis vallen dan belanden wij in een klasse van machines die de mogelijkheid hebben zelfstandig tijdens de loop van de berekening keuzes te maken - als er naar een meervoudig optredend label gesprongen moet worden kiest de machine zelf een van de optredens. Uitreaard mag U deze keuze ook toeschrijven aan uw ergste vijand, de Duivel of iedere andere hogere macht die U zich hierbij voor de geest wilt halen. De aldus verkregen klasse van machines noemt men *Non-Deterministisch* .

Het is mogelijk bij een non-deterministische machine een deterministische variant te bouwen die onder controle van een programma alle mogelijke berekeningen van de gegeven machine afzoekt om te kijker of één van deze mogelijke berekeningspaden tot het gewenste doel voert. Op deze wijze kan men aantonen dat non determinisme niet leidt tot een uitbreiding van de rekencapaciteit. Wel dient te worden opgemerkt dat deze simulatie erg veel tijd zal kosten. Als de oorspronkelijke machine in polynomiaal begrensde tijd kan termineren heeft zijn deterministische variant er in het beroerdste geval exponentiele rekentijd voor nodig om de goede oplossing te vinden.

Sinds een tiental jaren is het inzicht ontstaan dat een probleem, wil het practisch oplosbaar zijn, moet kunnen worden opgelost met gebruikmaking van een algoritme waarvan de rekentijd niet harder groeit dan een polynomiale functie in termen van de lengte van de invoer. Nu bestaan er in de practijk vele duizenden typen van problemen waarin gevraagd wordt naar het bestaan van een zekere deelstructuur in een grotere gegeven structuur. Zo kan men bijvoorbeeld vragen of er in een gegeven graaf (dat is een wiskundig model van bv. een landkaart met knopen die steden modelleren en kanten als verbindingswegen) een Hamilton-circuit, dat is een pad dat alle knopen precies één keer aandoet en dan in zijn startpunt terugkeert, kan worden gevonden. Dit probleem laat zich non-deterministisch makkelijk oplossen: laat de machine eerst een pad raden en vervolgens verifieren dat het pad inderdaad alle punten eenmalig aandoet.

Als we op de standaard wijze het non deterministische programma proberen te vervangen door een deterministische versie, leidt dit tot de triviale oplossing "probeer alle paden en kijk of er een goed pad bij zit" (Ακουε παντων, ἐκλεγε δε ἃ συμφερει σ[13]) . De vraag is dan ook gerechtvaardigd of dit niet wat efficienter kan. Het noodlot wil nu echter dat deze vraag reeds tien jaar onopgelost bekend staat als het P = NP probleem[14] . Het genoemde probleem van het bestaan van een Hamilton-circuit in een graaf is een van de tienduizend bekende vormen van een NP-volledig probleem. Als we dit probleem op efficiente wijze kunnen oplossen (en efficient betekent in dit geval "in polynomiaal begrensde tijd") dan is daarmede de gehele klasse NP als probleem gekraakt.

Een van de pogingen die gedaan zijn om dit probleem te kraken bestond uit het onderzoeken van het P = NP probleem voor Turing machines met een orakel. Helaas bleek het antwoord, gelijk men van een orakel verwachten kan, dubbelzinnig: het bleek mogelijk een orakel A te construeren waarvoor $P^A = NP^A$, terwijl voor een ander orakel B geldt $P^B \neq NP^B$ [15] .

Hoe het orakel van Turing zijn zegenbrengende arbeid verricht is hierboven geheel in het midden gelaten. In het klassiek bekende geval van een orakel voor het stop-probleem heeft Charles H. Bennet recentelijk een uiterst compacte vormgeving beschreven[16] . Beschouw opnieuw een universele Turing machine die nu ecter zijn invoer bitsgewijs binnen krijgt. Deze machine rekent totdat hij een nieuw invoer symbool nodig heeft, en zal daar dan om vragen. Sommige invoerstromen zullen aanleiding geven tot een terminerende berekening. Gegeven een rij nullen en enen zijn er nu drie mogelijkheden:

1) na verwerking van deze rij symbolen vraagt de machine om verdere invoer
2) na verwerking van deze rij symbolen stopt de machine
3) de machine stopt voordat het laatste symbool van de invoer gelezen is

Geven wij nu een rij van k nullen en enen gewicht 2^{-k} , en tellen we alle gewichten van rijen op waarvoor 2) geldt, dan kan men laten zien dat de som convergeert naar een getal Ω gelegen tussen de getallen nul en één. Dit getal wordt het *Chaitin getal* genoemd. Men kan het beschouwen als de kans dat bij koppeling van de machine aan een random generator die willekeurig nullen en enen genereert, de machine tot rust komt.

Kennis van de decimale ontwikkeling van het Chaitin getal vormt de sleutel tot de oplossing van vele wiskundige problemen. Zo kunnen wij het bestaan van een zesde Fermat priemgetal[17]eenvoudig als volgt oplossen:

Ontwerp een programma dat zoekt naar het zesde Fermat priemgetal. Vorm de bijbehorende rij nullen en enen die bij invoer in de universele machine dit programma zullen laten uitvoeren, en laat de lengte van deze rij k zijn. Ga vervolgens met een universele simulator alle mogelijke berekeningen uitproberen en vorm daarbij de som van alle gewichten van rijen invoersymbolen die aanleiding geven tot een terminerende berekening. Ga hiermee door totdat de som minder dan 2^{-k} verschilt van de (tot op die precisie bekend verondersstelde) benadering van het Chaitin getal. Als tegen die tijd (die zeker zal aanbreken want de som convergeert per definitie naar het Chaitin getal), het programma dat naar F_6 zoekt nog steeds niet getermineerd is kunnen we concluderen dat F_6 niet bestaat, en in het andere geval hadden we het reeds gevonden.

Bennet heeft helaas vergeten de waarschuwing uit te spreken dat de voor dit proces benodigde rekentijd van de zelfde orde van grootte is als de "nijvere Bijen functie" (Buzy Beaver Function)[18] voor $n = k$; aangezien deze functie voor n groter dan 8 reeds onvoorstelbare waarden aanneemt dienen wij het project vermoedelijk als onwereldlijk van de hand te wijzen. Dit neemt overigens niet weg dat de kabalist in het Chaitin getal de oplossing van al zijn problemen kan aantreffen. Ook als invoer voor de Lotto is het ideaal - het is onmogelijk om met positieve winstverwachting op de uitkomst van een nul of een één in de binaire ontwikkeling van het Chaitin getal te gokken.

Het Orakel van Rabin

Een laatste serieuze vorm van een orakel in de wiskunde, die ik met U wil behandelen betreft het gebruik van probabilistische hulpmiddelen bij het beantwoorden van problemen die welliswaar ook op deterministische wijze kunnen worden opgelost maar dan wellcht te veel rekentijd zouden vergen. De grote protagonist voor deze aanpak is Michael O. Rabin, die in 1976 de nodige wenkbrouwen liet fronsen met zijn voorstel voor het vinden van grote priemgetallen[19] .

De bedoelde methode voor het herkennen van primaliteit van getallen is gebaseerd op het kenmerk van Fermat: als p priem is geldt voor ieder getal a tussen 1 en p dat a^{p-1} congruent 1 modulo p is. Helaas geldt van deze stelling niet de omkering; schrijven wij echter $p-1 = 2^k.n$ met n oneven en is p niet priem dan moeten er getallen a bestaan waarvoor geldt :

hetzij $a^{p-1} \not\equiv 1 \pmod{p}$

hetzij er is een $j < k$ zodat voor $b = a^{n.2^j}$ geldt dat $b \not\equiv -1 \pmod{p}$ terwijl toch $b^2 \equiv 1 \pmod{p}$

Een getal a met deze eigenschap noemt men een getuige voor de non-primaliteit van p . Gegeven een getuige kan men de test of het inderdaad een getuige is goedkoop uitvoeren; de benodigde machtsverheffingen modulo p vragen een rekentijd die begrensd wordt door een polynoom in $\log(p)$. Resteert de vraag hoe wij aan een getuige moeten komen.

Gary Miller[20] heeft laten zien met gebruikmaking van resultaten uit de klassieke analytische getaltheorie, dat er een constante C bestaat zodanig dat de kleinste getuige voor de non-primaliteit van p kleiner is dan $C.(\log(p))^2$; hierbij wordt echter wel een beroep gedaan op een gegeneraliseerde Riemann Hypothese, iets waarvoor de Zuivere Wiskundigen terugschrikken.

Het voorstel van Rabin komt er op neer dat de getuige gevonden dient te worden via loting. Het is immers zo gesteld (en dat kan men bewijzen zonder een beroep te doen op enige extra hypothese) dat meer dan $\frac{3}{4}$ van alle getallen beneden p getuige moeten zijn als p tenminste niet priem is. Als het dus zo is dat na het uitproberen van 50 aselect gekozen getallen er nog steeds geen getuige gevonden is, mogen wij p als een priemgetal beschouwen. De kans dat ons orakel een foute uitspraak heeft gedaan is dan immers kleiner dan 2^{-100} en daar kunnen we in de practijk mee leven.

Voor de zuivere wiskundige is dit voorstel een nog groter gruwel dan het eerder genoemde voorstel van Miller. De uitspraak " p is met kans groter dan $1 - 2^{-100}$ een priemgetal" is immers onzin. Het getal p is priem of het is niet priem. De kans betreft niet de primaliteit van p zelve, maar het feit of de uitspraak die wij daarover doen al dan niet juist is. Uitspraken die niet gegarandeerd correct zijn kunnen in de empirische wetenschap dan nog zo nuttig zijn, in de wiskunde horen zij niet thuis.

Aan de andere kant dient te worden opgemerkt dat gebruik van deze Rabin-priemgetallen voor bv. het ontwikkelen van onbreekbare codes volgens het Adleman - Rivest-Shamir schema[21] niet op bedenkingen van de wiskundigen stuit. Mocht blijken dat een getal ten onrechte als priemgetal is aangemerkt dan blijkt dit vanzelf bij het gebruik van de code, en kan men overgaan tot het aanmaken van een nieuw priemgetal.

De computer als Orakel

Geachte toehoorders

Ik wil U thans uitnodigen om plaats te nemen op de andere helft van mijn leerstoel, te weten de meer toegepaste aspecten der informatica. Het is immers zo gesteld dat, voorzover U met de computer te maken zult hebben dit in het algemeen geschiedt via toepassingen buiten de wiskunde. In de meest zware vorm kan dit voortkomen uit het feit dat de computer over onze hoofden een atoomoorlog laat uitbreken[22] , in minder ernstige gevallen betreft dit het onvangen van drukwerkjes in duplo in banderollen, waarop de computer uw naam met de nodige spelfouten benevens enkele onduidbare letter- of cijfercombinaties heeft afgedrukt.

In zijn oratie gehouden op 25 september 1972 heeft mijn collega proximus, Th. J. Dekker reeds een waslijst van computer toepassingen de revue laten passeren[23];ik wil U vandaag daarmede niet lastig vallen en ik volsta derhalve met een representatief voorbeeld.

De Nobel prijs voor medicijnen voor het jaar 1979 is toegekend aan G.N. Hounsfield en A.M. Cormack voor hun bijdrage aan de ontwikkeling van de CAT-scan[24].Dit is een apparaat waarmede het mogelijk is opnamen van het inwendige van schedels of andere organen te maken, zonder hetzij via chiruchische ingrepen, hetzij via het inbrengen van constrast vloeistoffen met alle schadelijke gevolgen van dien, de patient te benadelen. Dit apparaat is ondenkbaar zonder de aanwezigheid van de computer die het mogelijk maakt de vele berekeningen (waarvan het principe reeds langer bekend is)[25] in een voldoend korte tijd uit te voeren.

In een voorbeeld als hierboven genoemd kunnen wij de computer zien als een verlengstuk van een meetapparaat. De verantwoordelijkheid voor de interpretatie van de opnamen die ermee vervaardigd worden blijft berusten bij de arts die het apparaat gebruikt. In een situatie als deze kunnen echter ook problemen optreden als de gebruiker, in casu, de arts, geconfronteerd wordt met een verveelvoudiging van het aantal gegevens op grond waarvan hij zijn beslissingen neemt. Ik denk hierbij aan de problemen die moeten gaan optreden als de thans ontwikkelde analyse apparaten die in één meting de resultaten van 20 tot 40 verschillende analyses op een bloedmonster tegelijk opleveren algemeen in gebruik komen; het is bijvoorbeeld ondenkbaar dat bij iedere overschrijding van een 5% waarde tot nader onderzoek wordt over gegaan, aangezien om zuiver kanstheoretische redenen het aantal "normale" monsters tot nihil zal worden gereduceerd. Gelukkig zijn er artsen die hiermee te maken krijgen en die zich deze problematiek bewust zijn.

Bij andere toepassingen fungeert de computer als bron van informatie; zij levert ons bv. die gegevens uit een administratief bestand, die nuttig zijn om bepaalde beslissingen te nemen. Een dergelijk systeem wordt gebruikt door de boekhouding van de Universiteit die ons maandelijk op de hoogte stelt van de toestanden van onze diverse budgetten. Zo vernemen wij jaarlijks bij het gereedkomen van de eindafrekening voor het bibliotheek crediet over het afgelopen jaar dat deze uitgaven aanleiding geven tot een tekort van vele tonnen over het komende jaar, omdat de computer niet beter weet dan dat uitgaven waarover hij in Februari rapporteert met een factor 12 vermenigvuldigd dienen te worden om tot een prognose op jaarbasis te komen. Soms zijn de gegevens zelfs helemaal onzinnig: het overzicht van het hulpmiddelencrediet van October 1978 vertoonde een voorziene uitgave van *f* 596 502 810.81 voor het lopende jaar, uit te geven aan krijtjes, papier, enveloppen etc. . Uiteraard kregen wij een week later een briefje met de excuses van de boekhouding - de computer had een fout gemaakt. Ongelukkig echter de boekhouder die een niet ontdekte fout van enkele tientjes - waarvan wij mogen aannemen dat zij even goed kan optreden - uit eigen zak mag bijbetalen.

In het verlengde hiervan liggen de toepassingen waarbij de computer cijfermateriaal oplevert waarvoor de berekeningen zo gecompliceerd zijn dat de rol van de menselijke beslisser vrijwel lijkt te zijn uitgeschakeld. Zo zullen bij de bepaling van de cijfers van het Centraal Planbureau, waarop de regering haar beleid baseert, ongetwijfeld de nodige computers zijn ingeschakeld. Bij een dergelijke toepassing is er een interactie van empirisch verzamelde gegevens, al dan niet juiste economische modellen, al dan niet correcte computer implementaties hiervan, en politiek gemotiveerde interpretatie van de uitkomsten. Dit alles ontrekt zich aan het oog van de burger, die de resultaten van het hierop gebaseerde beleid dagelijks in de krant leest of in zijn portemonnaie voelt.

In hoeverre kunnen wij in een situatie als hierboven geschetst, de computer zien als het hedendaagse orakel ? Allereerst dient te worden opgemerkt dat het feit dat de gegevens uit de computer komen te gemakkelijk wordt aangevoerd als legitimatie voor de correctheid ervan. Dit is geheel ten onrechte. In de aan de computer berekening voorafgaande keten van modelvorming en interpretatie zitten in het algemeen zoveel benaderingen en/of menselijke fouten dat we de uitkomsten met een korreltje zout dienen te nemen - zeker aangezien wij geen inzicht in de feitelijke gang van zaken hebben.

Wij kunnen echter wel stellen dat vermoedelijk de berekening in de computer in de gehele procedure de meest betrouwbare stap is, waarbij ik het tot stand komen van de gebruikte programmatuur expliciet uitsluit. Computers falen zelden op technische gronden. In het verleden toen de technologie minder volmaakt was stond er wel eens een bit fout. Tegenwoordig zien wij ons opnieuw geconfronteerd met het probleem van deze "bit-flippertjes"[26] maar dat is nu een gevolg van de ver voortgeschreden miniaturisatie. Wij kunnen dit probleem echter oplossen op de zelfde wijze als voorheen, via het gebruik van fouten corrigerende codes.

Dat er bij het gebruiken van een groot computer systeem voortdurend van alles mis gaat - een waarheid waarmee ieder student, medewerker of andere SARA gebruiker dagelijks te maken heeft[27] - ligt aan fouten in de systeemprogrammatuur, die op hun beurt te wijten zijn aan het menselijk onvermogen om complexe systemen te begrijpen en te programmeren, in het bijzonder als het er om gaat om naast elkaar verlopende processen op correcte wijze te laten samenwerken.

In de informatica zijn wij inmiddels vertrouwd geraakt met het begrip "software crisis" ; de apparatuur wordt spotgoedkoop, de programmatuur wordt duurder en blijft fouten vertonen. Ik reken mijzelf niet tot de optimisten die geloven dat dit probleem kan worden opgelost door onze studenten beter te leren programmeren - wij mogen op zijn best hopen hierdoor aan de oplossing van dit nijpende probleem een redelijke bijdrage te leveren door de meest opvallende gruwelen te helpen uit te bannen. Wij hebben echter ook te maken met een samenleving waarin het ontbreekt aan standaardisatie van apparatuur, programmeertalen, en programmatuur. Veel detailkennis die wij onze studenten meegeven zullen zij zich bij hun latere broodheer opnieuw dienen te verwerven. Terecht tooit een tijdschrift over programmeertalen, Computer Languages, zich op zijn voorpagina met een Breugheliaanse toren van Babel.

Het Verkiezings Orakel

Ter illustratie van de bovengeschetste problematiek wil ik U confronteren met een praktijk voorbeeld waar ik persoonlijk mee te maken heb gehad. Het betreft hier het samenstellen van de subfaculteits raden aan deze universiteit. Zoals bekend worden de vertegenwoordigers van de wetenschappelijke staf in deze raden verkozen volgens het stelsel van de enkelvoudig overdraagbare stem. De werking van dit stelsel is gedefinieerd in ons kiesreglement[28] . Bij lezing van de te volgen procedure wordt het al snel duidelijk dat het vast stellen van de uitslag van een verkiezing zoveel rekenwerk vraagt dat de computer hierbij te hulp dient te worden geroepen. Dit is temeer nodig aangezien ons centrale stembureau in korte tijd de uitslag moet vaststellen voor een groot aantal raden. Het is mij ook bekend dat in het verleden, toen de uitslagen nog per subfaculteit door plaatselijke deskundigen met de hand werden vastgesteld, soms gebruik is gemaakt van methoden waarvan men vermoedde dat zij met de bedoeling van het stelsel overeenkwamen, terwijl dit in feite niet het geval is[29] .

In het jaar 1975 raakte ik geintersseeerd in de vraag hoe het programma dat het centrale stembureau gebruikte voor het vaststellen van de verkiezingsuitslag er uit zag. Navraag leverde een listing op van een uit Delft afkomstig ALGOL 60 programma dat de sporen vertoonde van de nodige conversies van een computer systeem naar een ander. Commentaar en structuur was verre van aanwezig. Bovendien bleek de in het programma opgenomen lotings procedure de candidaten waartussen geloot diende te worden ongelijke kansen te geven, terwijl het gebruik van real-arithmetiek op sommige plaatsen twijfels met betrekking tot de juiste werking bleek te rechtvaardigen. Op grond van deze bedenkingen besloot ik, in samenwerking met mijn collega H.W. Lenstra jr. maar eens een bezwaarschrift tegen de vaststelling van de verkiezingsuitslag in te dienen[30] . Dit bezwaar werd later door de betrokken instanties op deskundige wijze onder de tafel gewerkt[31] . Nog steeds betreur ik dat de publiciteit die wij in een later stadium aan deze zaak hebben gegeven niet heeft geleid tot het over deze boeg uitvechten van enkele universitaire vetes.

Een en ander heeft er wel toe geleid dat sinds 1976 onze universiteit gebruik maakt van een programma dat, mede onder mijn toezicht, is geschreven door G.M. Tuynman, thans assistent aan ons instituut. Wij hebben gehoopt dit programma zodanig te structureren dat het mogelijk is op eenvoudige wijze vast te stellen dat het in overeenstemming is met het reglement. Bovendien is bij het ontwikkelen van het programma gebleken dat het reglement op bepaalde punten nadere uitleg behoeft; deze punten met hun bijbehorende interpretatie zijn zorgvuldig verwoord in de documentatie die bij het programma is geschreven[32] . Het is tevens mogelijk gebleken op eenvoudige wijze wensen van het Centrale stembureau met betrekking tot de behandeling van niet geheel correct uitgebrachte doch niet ongeldige stemmen in het programma te verwerken.

Ik wil met het bovenstaande aantonen dat de beantwoording van de vraag of het computer orakel dient te worden geloofd niet afhangt van de computer zelve, maar van de kennis die wij hebben over de aan de computer-toepassing ten grondslag liggende analyses en modelvormingen, en het vertrouwen dat wij hebben in de deskundigheid van de ontwerpers en programmeurs die bij het project zijn ingeschakeld. Tot nog toe zijn de structuren in de samenleving zodanig dat de leek op geen van beide punten informatie kan verkrijgen. Op grond hiervan kan dan ook gerust gesteld worden dat wij het orakel niet dienen te geloven.

Het bovenstaande impliceert geenszins dat ik de stelling van Jocasta dat de orakelen altijd liegen wens te onderschrijven. Het is immers bekend dat een orakel dat altijd liegt even bruikbaar is als een dat altijd de waarheid spreekt[33] . Ik vraag slechts om een gezonde dosis wantrouwen bij de betrokkenen en dat zijn wij allemaal.

Als onderwijzer in de informatica zou ik mij geroepen dienen te voelen de taak op mij te nemen mijn studenten te leren correct, helder en foutloos te programmeren. Ik geloof echter niet dat ik in staat ben deze taak te vervullen - daartoe is mijn skepsis over de feilbaarheid van de mens te groot. Ik vindt het derhalve belangrijker mijn leerlingen te wijzen op de gevolgen die dit heeft voor henzelve en de rest van de samenleving. Inzicht in het gebeuren binnen een computer, en de voor het begrijpen hiervan benodigde begrippen is daarom minstens zo belangrijk als elementaire programmeervaardigheid. Diegenen onder mijn studenten die derhalve menen te kunnen volstaan met het voldoende doorlopen van het practicum doen zichzelve en hun latere broodheren te kort.

Geachte toehoorders

Gij hebt het in deze toespraak moeten stellen zonder een pleidooi voor het belang van de informatica in het algemeen en het eigen vakgebied in het bijzonder. Ik laat dit gaarne aan anderen over. Ik wil wel met genoegen constateren dat wij dit jaar eindelijk het vak informatica hebben zien opnemen in het Academisch Statuut, en dat er, hopelijk met de nodige voortvarendheid, gewerkt gaat worden aan een zelfstandige studierichting informatica in de regio Amsterdam. Ik hoop aan dit project mijn passende bijdrage te kunnen geven.

Het is buiten Amsterdam een goede gewoonte op dit punt in een inaugurele rede dank te betuigen aan Hare Majesteit de Koningin voor de ontvangen benoeming. Ik wil mij gaarne bij deze gewoonte aansluiten, temeer aangezien ik mij nog juist in de gelegenheid zie deze rede uit te spreken tijdens de regeerperiode van de Koningin die mij heeft willen benoemen tot lector aan deze Universiteit.

Mijne Dames en Heeren bestuurderen van deze Universiteit

Ik dank U voor het in mij gestelde vertrouwen. Ik voorzie dat wij in de komende tijden elkaar nog dikwijls aan de nodige vergaderingstafels zullen treffen als het gaat om de inrichting van de nieuwe informatica studie. Ik ben er hierbij echter van overtuigd op uw welwillende medewerking te mogen rekenen.

Dames en Heeren docenten, medewerkers, assistenten en overige verbondenen aan het Mathematisch Instituut en het Instituut voor toepassingen der Wiskunde

Het lijkt mij in de gegeven omstandigheden onjuist om U te danken voor de wijze waarop U mij heeft willen ontvangen na mijn benoeming. Deze volgde immers na een periode van ruim 15 jaar waarin ik in Uw midden ben opgegroeid van beginnend student tot lector. Ik moet U derhalve danken voor al hetgeen U sinds October 1962 heeft bijgedragen tot mijn ontwikkeling. Diegene onder U die met name genoemd had dienen te worden, wegens de ingreep die mij op beslissende wijze op het pad der wetenschap heeft gezet, Prof. J. de Groot, is ons helaas in 1972 ontvallen, maar het doet mij een groot genoegen zijn invloed en zijn omgeving totop de huidige dag te zien voortleven binnen de wiskunde aan ons instituut en elders in Amsterdam.

Bij mijn onderzoek en verdere werkzaamheden heb ik met zeer velen van U regelmatig te maken. Dit hangt mede samen met de merkwaardige ontwikkelingen in het vak van de complexiteitstheorie, waar ik alle uithoeken der wiskunde in toegepaste vorm tegenkom. Ik zie dan ook een deel van mijn taak als permanent verzamelpunt en doorgeefluik voor recente wetenschappelijke informatie, en het doet mij dan ook een genoegen om mij nauw verbonden te weten met diverse communicatiekanalen tussen ons instituut en de rest van de wiskundige wereld.

Dames en Heeren Leden van de vakgroep Propaedeutische Wiskunde

Mijn benoeming tot lector hield tevens in een aanstelling in Uw instituut, en wel in een bijzondere positie. Gedurende de afgelopen drie jaren heeft U mij de gelegenheid gegeven te komen tot een onderwijspakket informatica voor uw afnemers, waarvan ik hoop dat het overeenstemt met uw eigen filosofie omtrent wiskunde voor niet wiskundigen. Ik realiseer mij dat een onderwijsonderdeel in de informatica voorturend zal moeten worden bijgesteld, al was het maar vanwege de voortdurende veranderingen in de gebruikte apparatuur en programmatuur. Het ziet er naar uit dat zelfs het aloude FORTRAN 4 vervangen zal worden , hetgeen zekerlijk zal leiden tot een nieuwe syllabus.

Bij mijn komst in uw midden heb ik de vraag gesteld of U niet bezig was met het binnenhalen van het spreekwoordelijke paard van Troje. Na drie jaar moet ik constateren dat de scheidsmuren tussen de twee afdelingen waartussen mijn leerstoel verdeeld is, inderdaad worden geslecht. Dit gebeurt echter op geheel vreedzame wijze, en het is eerder onder de druk der omstandigeheden dan dat ik mij zelve een duidelijke rol wens toe te delen. Ik vrees echter dat mijn persoonlijke voordeel, te worden verlost van het ontvangen van universitaire post in duplo, niet zal worden geëffectueerd - een oprichting van een facultaire groep voor de informatica lijkt niet te ver in de toekomst te liggen, en een nieuwe dubbele aanstelling valt daarom te verwachten.

Ik ben U echter dankbaar voor de steun die U mij gedurende de afgelopen drie jaar hebt gegeven, en ik kan U dan ook melden dat het in Uw secretariaat is dat deze rede is samengesteld.

Dames en Heeren bestuurderen van en medewerkers aan het Mathematisch Centrum

Gedurende bijna 12½ jaar was ik in een of andere functie officieel aan uw instituut verbonden. Sinds mijn benoeming aan deze Universiteit hebben wij gemeend de samenwerking op officieuze wijze voort te moeten zetten hetgeen tot nog toe tot bevredigend verloopt. Wekelijks bezoek ik uw instituut enkele malen. U geeft gastvrijheid aan twee door mij bezochtte werkgroepen die beide een unieke vorm van landelijke samenwerking te zien geven op het terrein der Complexiteitstheorie en het terrein der Montague-grammatica.

Het moge eenieder duidelijk zijn dat ik de huidige positie nooit bereikt zou hebben zonder uw ondersteuning die mij in staat heeft gesteld om van beginnend Topoloog met wat zijdelingse interessen in onderdelen der Algebra, via een abortieve poging tot het bedrijven der Algebraische meetkunde te belanden in de theoretische Informatica. In het bijzonder wil ik hier danken Prof. P.C. Baayen, onder wiens leiding deze rondedans door de wiskunde heeft plaats gevonden. Als in de toekomst de betrokkenheid met de Linguistiek zal toenemen zal hij daar ook niet vreemd aan zijn.

Mijn dank aan het Mathematisch Centrum strekt zich tevens uit tot de niet wiskundige afdelingen. Zo ben ik het Centrum ervoor erkentelijk dat ik deze rede via hun drukkerij heb mogen uitgeven, waarbij ik de Heeren Zwarst en Baanders wil danken voor hun bijdragen aan de technische verzorging.

Mijne Dames en Heeren informatici in Amsterdam

Schoorvoetend zijn wij bezig te komen tot een samenwerkingsverband van informatici binnen de universiteit van Amsterdam. Het moge echter duidelijk zijn dat de informatica studie in de regio dient te worden georganiseerd; ik hoop dan ook met U allen goed te kunnen samenwerken.

Mijne Dames en Heeren Wiskundigen en Informatici in Nederland

Veel van mijn activiteiten spelen zich af buiten Amsterdam. Ik bezoek liever een wetenschappelijke bijeenkomst elders dan een vergadering in mijn eigen instituut. Ik hoop dat dit in de toekomst zo zal blijven. Ik moet echter constateren dat de tijden somber zijn; er zijn organisatorische veranderingen op komst die ons wel tot een landelijke samenwerking zullen dwingen. Ik vrees dat wij een periode tegemoet gaan waarin de machtigen ons

weinig welgezind zullen zijn. De overheid belijdt in woorden het belang van een hoogstaand onderwijs en geavanveerd onderzoek, zulks in het kader van een hoog cultuurniveau, maar lijkt ondertussen op weg via voortdurende reorganisaties van onderwijs en onderzoek de vrijheden die wij totop heden gekend hebben in te perken, in naam van de vergroting van de productiviteit. Enerzijds zie ik niet hoe deze reorganisaties kunnen worden doorgevoerd als een groot deel der direct betrokkenen zich daartegen verzet; anderzijds verwacht ik niet dat op de langere duur de veranderingen steeds opnieuw worden uitgesteld, zoals dit de afgelopen jaren is gebeurd. Met betrekking tot het onderzoek zie ik het belang van landelijke samenwerkingsverbanden en het tot stand komen van een zwaartepuntsbeleid. Activiteiten te dienaangaande plaats vinden verdienen onze actieve steun, en in ieder geval onze serieuze aandacht. Een verantwoorde verslaglegging van onze resultaten is ook een vereiste.

Overigens ben ik van mening dat de wegen der wiskunde en informatica niet gescheiden dienen te worden.

Mijne Dames en Heeren Studenten

In mijn rede heb ik U reeds enkele inzichten willen geven in het materiaal dat ik U hoop bij te brengen. Informatica is een vak van veel zelfstandig werken en dingen leren te begrijpen door het te doen. De inhoud van een programmeer-handboek bij een machine of een taal laat zich het beste begrijpen door te kijken wat er gebeurt als men de regels in het manual volgt, dan wel bewust overtreedt. Alles heeft ergens wel een logische verklaring, al blijkt die vaak moeilijk te vinden.

Tegen de tijd dat U een programma aan de praat heeft gekregen zult U dikwijls moeten constateren dat de oorspronkelijk zo fraaie structuur bij het aanbrengen der noodzakelijke "patches" zwaar te lijden heeft gehad. Ik wil U in dit verband wijzen op de volgende passage uit de Kalevala[34] . Het handelt hier in dit Finse nationale epos (wat ik U in een Engelse vertaling moet voorleggen aangezien ik het Fins niet machtig ben) over de smid Ilmarinen, bezig met het volvoeren van zijn levenswerk - het smeden van de Sampo.

On the first day of their labor
He himself, smith Ilmarinen
Stooped him down, intently gazing,
To the bottom of the furnace,
If perchance amid the fire
Something brilliant had developed.
From the flames there rose a crossbow,
Golden bow from out the furnace;
'Twas a gold bow tipped with silver,
And the shaft shone bright with copper.
And the bow was fair to gaze on,
But of evil disposition,
And a head each day demanded,
And on feast-days two demanded.

He himself, smith Ilmarinen,
Was not much delighted with it,
So he broke the bow to pieces,
Cast it back into the furnace,
Made his servants work the bellows,
to the half of all their power.

Ge ziet het, men doet er soms goed aan het werk zijner handen geheel af te breken en het met de verworven kennis nog eens te proberen. Het smeden der Sampo gelukte ook pas bij de vijfde poging.

Beste Dennis, Beste Theo

U beiden, in uw functie als as. promovendus stel ik aansprakelijk voor de plechtigheid die thans een einde gaat nemen. Het spoedig gereed komen van uw werkstukken, gecombineerd met mijn idee fixe, dat het uitwendig tonen der universitaire waardigheidssymbolen slechts verdiend kan worden via het houden van een toespraak, vormde mijn voornaamste motivatie na drie jaar over te gaan tot het schrijven van een oratie. Ik wil echter met U alle overige aanwezigen danken voor hun aandacht.

Ik heb gezegd.

Noten

1 Igor Strawinsky, *Oedipus Rex* . Libretto Jean Cocteau, Vert. J. Danielou.

2 Sophocles, *Oedipus Tyrannus*. Ed. A.M. van Erp Taalman Kip / W.J.H.F. Kegel Tjeenk Willink 1978 (2e druk). Vrs. 707-709.

3 Sofokles, *Koning Oidipoes*, Vert. P.C. Boutens, Verz. werken deel 5. Joh. Enschedé & Zn. 1951, pag 90.

4 Sophocles, *The Theban Plays, King Oedipus*, transl. E.F. Watling, Puinguin Books 1947, pag 45.

5 A.H.G. Rinnooy Kan, *Vraag en aanbod op de Wetenschapsmarkt*, Oratie Erasmus Universiteit Rotterdam, Apr. 20 1978. H.E. Stenfert Kroese, Leiden 1978, pag 20.

6 Philip Morrison, *Books* (boekbesprekingen), Sci. Amer. 242 (1980), iss. 2 (feb), 22-24.

7 Joseph Fontenrose, *The Delphic Oracle, Its Responses and Operations, with a Catalogue of Responses*, University of California Press, Berkeley 1978, Chapt. 1,3,4 & 7 .

8 Abraham Trommius, *Nederlandse Concordantie van de Bijbel*, 18e grondig herziene en veel vermeerderde druk, bewerkt naar de originele uitgave. J.N. Voorhoeve, den Haag.

9 A.M Turing, *On Computable Numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. II 42 (1936), 230-265.

10 De hier behandelde beschrijving is niet de origineel van Turing afkomstige; zij is gebaseerd op H. Wang, *A variant to Turing's Theory of Computing Machines*, J. Assoc. Comput. Mach. 4 (1957) 63-92.

11 Voor een historisch overzicht van het tot stand komen der verschillende definities voor het begrip berekenbaarheid zie bv. S.C. Kleene, *Origins of Recursive Function Theory*, Proc 20th Symp. Foundations of Computer Science, (invited talk), IEEE, Oct 1979 Puerto Rico, pp. 371-382.

12 A.M. Turing, *Systems of Logic Based on Ordinals*, Proc. London Math. Soc II 45 (1939), pp 161-228.

13 Amsterdamse Studentenalmanak, Jaargangen 1954-1970.

14 M.R. Garey & D.S. Johnson, *Computers and Intractability, a guide to the theory of NP-completeness*, Freeman, San Francisco 1979.

15 T. Baker, J. Gill & R. Solovay, *Relativizations of the P =? NP question*, SIAM J. Comput. 4 (1975) 431-442.

16 C.H. Bennet, *On Random and Hard-to-describe Numbers*, rep. RC 7483 (#32272) IBM Watson Research Center, Yorktown Heights, NY 10598, Jan 1979.
Zie ook, Martin Gardner's Mathematical Games rubiek in Sci. Amer. 241, Nov 1979.

17 Een Fermat priemgetal is een priemgetal van de vorm $2^k + 1$; men kan bewijzen dat k zelf van de vorm 2^m moet zijn. Voor m = 0,1,2,3 en 4 is 2^{2^m} een priemgetal; andere waarden van m waarvoor 2^{2^m} priem is zijn tot op heden niet bekend.

18 T.Rado, *On non-computable functions*, Bell System Technical J. 41 (1962), 877-884. Voor een hedendaagse toepassing van deze functie zie R. Daley, *On the Simplicity of Buzy Beaver Sets*, Rep. DCS, Univ. of Pitsburgh, TR 76-6, July 1976.

19 M.O. Rabin, *Probabilistic Algorithms*, in J.F. Traub, ed., Algorithms and Complexity, New directions and recent results, Acad. Press 1976, pp 21-40.

20 G. Miller, *Riemann's Hypothesis and Tests for Primality*, J. Comput. Systems Sci. 13 (1976) 300-317.

21 R.L. Rivest, A. Shamir & L. Adleman, *A method for obtaining Digital Signatures and Public-key Cryptosystems*, Comm. Asoc. Comput. Mach. 21 (1978) 120-126.

22 NRC, 10 nov. 1979.

23 Th. J. Dekker, *Automatisch Rekenen*, Oratie Univ. van Amsterdam, Sep 25 1972. van Gorkum & Comp. N.V., Assen 1972.

24 ACM President's letter, Comm. Asoc. Comp. Mach. 22 (1979) 587-588.

25 Een voorbeeld van een wiskundige behandeling van dit probleem is te vinden in het artikel van G.T. Herman, A. Lent & P.H. Lutz, *Relaxation Methods for Image Reconstruction*, Comm. Asoc. Comput. Mach. 21 (1978), 152-158. Ook de filmopnamen van een kloppend hart die op basis van deze techniek verkregen zijn die G. Herman tijdens een voordracht op het Mathematisch Centrum heeft vertoond waren zeer overtuigend.

26 Bad Bits, in Science and the Citizen, Sci. Amer. 242 iss. 2 (feb), 63-64.

27 Zie bijvoorbeeld het maandelijkse overzicht van storingen in het SARA bulletin.

28 Kiesreglement van de Universiteit van Amsterdam, hoofdstuk X, afd. 5 (versie 1978).

29 Het betreft hier de methode om alle candidaten die de kiesdeler hebben gehaald gelijktijdig gekozen te verklaren.

30 Brief vEB/vw/237.75, dd. 16 mei 1975.

31 De droevige afloop van dit protest en vele andere wetenswaardigheden over deze affaire zijn te vinden in het artikel van A. Bijlsma: *Geblunder in Maagdenhuis*, Propria Cures 86 iss. 26 (10 Apr. 1976) pag 1 & 4.

32 G.M. Tuynman, *Documentatie bij het verkiezingsprogramma, editie 1979*, Uitgave Math. Inst. Univ. van Amsterdam (in voorbereiding).

33 Dit thema ligt ten grondslag aan de bekende leugenaarspuzzels. Een rijke verzameling hiervan kunt U vinden in de uitgave: R. Smullyan, *What is the name of this book ? The riddle of Dracula and other logical puzzles*, Prentice-Hall Inc., Englewood Cliffs, New Jersey 1978.

34 Kalevala, Runo X, Vs. 319-338. Vert. W.F. Kirby. Everyman's Library, Dent, London 1907, editie 1974.