

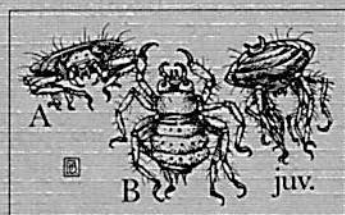
DOPO LE PAROLE

aangeboden aan

DR. A.K. LENSTRA

verzameld door

H.W. Lenstra, Jr., J.K. Lenstra en P. van Emde Boas



met platjes van Arjen

Amsterdam, 16 mei 1984



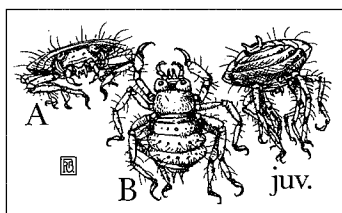
DOPO LE PAROLE

aangeboden aan

DR. A.K. LENSTRA

verzameld door

H.W.Lenstra, Jr., J.K.Lenstra en P.van Emde Boas



met platjes van Arjen

Amsterdam, 16 mei 1984

Voorwoord

Op het moment dat U als lezer deze bundel onder ogen zult krijgen zal geschied zijn datgene wat wij de afgelopen jaren als onvermijdelijk op ons af hebben zien komen. Arjen is doctor geworden - niet meer en niet minder. Dit noodlot heeft zich voltrokken waar wij allen bijstonden. Niemand van ons heeft ook maar een vinger uitgestoken om hiertegen iets te ondernemen. Nu is het te laat. De doctorale waardigheid met de daaraan verbonden verantwoordelijkheden met betrekking tot Koningin, Wetenschap en Vaderland is over hem gekomen en zal van hem nimmer meer wijken.

Diegenen die de totstandkoming van het door Arjen bewerkte proefschrift van nabij hebben mogen beleven zullen met ons eens zijn dat door een grillige speling van het lot werkelijk ieder element van noest spoorwerk dat aan dit werk ten grondslag zou moeten liggen is verdwenen dan wel op zijn minst aan het oog van de buitenwereld is onttrokken. In de voorbereidende fase, ten tijde van de doctorale studie, leek het alsof de opgelegde taak, inhoudende het voltooiën van een onvolledigheid in het werk van een ouder broertje, lastig zou zijn, althans gezien de ingewikkeldheid van de voorgelegde literatuur. Helaas bleek Arjen slimmer en bewees dat het makkelijk was. Het vinden van een promotor ging al even onconventioneel - voor de prijs van dertig zilverlingen mocht deze op het Mathematisch Centrum een briefje komen ondertekenen om Arjen uit de dienst te houden en de samenwerking was daarmee een feit. Incompetentie van collegae elders in den lande leidde ertoe dat het smalle pad der VLSI niet werd ingeslagen maar dat er in het verborgene rustig verder werd gewerkt aan priemgetallen en polynomen. Tegen de tijd dat het echt moeilijk leek te worden viel er juist een briefje van Lovász in de brievenbus dat het antwoord op alle vragen bleek te bevatten en kon Arjen rustig naar een concert gaan wetende dat hij de Bul in feite in zijn zak had. Het enige dat toen nog diende te geschieden was het schrijven van een coherente bundel artikelen op een zodanige wijze dat geen beoordelingscommissie daar problemen over zou maken, en dat was de kandidaat wel toevertrouwd. Het resultaat heeft U inmiddels allen gezien. Zelfs de stereotiepe zelfmoordpoging van de promovendus, om in de eindfase van het promotieonderzoek in verkering te gaan, heeft in dit geval geen vertraging mogen veroorzaken. Hoe stralend en gelukkig hebben wij Haar hedenmiddag naast Arjen zien staan.

Het moge duidelijk zijn dat deze voorgeschiedenis aanleiding geeft tot een gewetensvraag: moeten wij deze dag op feestelijke wijze vieren, of doen wij er beter aan dit gebeuren snel bij te schrijven in de statistieken die in steeds toenemende mate de ruimte voor onze wetenschappelijke existentie gaan bepalen. Zeker, deze Bul opent voor Arjen de weg tot het Wetenschappelijke Buitenland, en hij zal die zeker weten te vinden. Maar eenmaal zal hij wederkeren naar het Vaderland, om te ontdekken dat op basis van dit document en de tegen die tijd verworven vermaardheid een tiental Nederlandse instellingen voor Hoger Onderwijs staat te trappelen om hem aan te stellen als Kroondocent - uiteraard tegen minimumloon, want daar zullen Deet en zijn opvolgers tegen die tijd wel voor gezorgd hebben.

Anderzijds ervaren wij deze dag als een laatste kans. Vandaag kunnen wij nog met Arjen communiceren. De woorden die wij nu tot hem richten zullen wellicht nog tot hem doordringen. Morgen is hij geheel van buiten onze wereld - hij onderhoudt zich dan alleen nog maar met de Waarlijk Groten, of U zou zich tot hem moeten richten in de vorm van een op muziek gezette partituur.

Om deze reden hebben wij gemeend het gebruikelijke verzoek te doen uitgaan aan alle vrienden en bekenden van Arjen om datgene dat zij nog willen meegeven aan de jonge doctor nu aan het papier toe te vertrouwen en om niet tot morgen te wachten. De respons was gelijk te verwachten viel enorm, hetgeen tot grote problemen bij de technische verzorging heeft geleid, maar die waren dankzij de bijstand van Tobias en Dick oplosbaar.

Arjen, we beseffen het terdege: het heeft niet anders mogen zijn. Gedenk ons zwakkelingen in het uur van onze nood.

Hendrik W. Lenstra, Jr.

Jan Karel Lenstra

Peter van Emde Boas

Inhoud

- L.M. ADLEMAN, R.S. RUMELY, On distinguishing 89 from not 89.
D. ARNON, Ad Arjen K. Lenstra.
R.L. ARTZ, Een Ionisch polynoom.
P.C. BAAYEN, De ganzenboom.
F.J.M. BARNING, Reeds van zeer weleer.
J.A. BERGSTRA, J.W. KLOP, Een tegenvoorbeeld voor de Church-Rosser eigenschap van procespolynomen.
H. BODLAENDER, J. VAN LEEUWEN, A colorful proof of an obvious theorem.
J. BOESEWINKEL, Denkend aan Arjen.
B. CARMIGGELT, C. DE VRIES, Hou dat meneer Lenstra der veur de zoveulste moal uutbuult.
A.G.M. CIEREMANS, E. DEN BOER-CIEREMANS, J.E. VAN OUWERKERK-CIEREMANS, Amsterdam die grote stad.
L. CLASON, M. BELDEROK, Hommage aan de Friese doorloper.
H. COHEN, Some problems for Arjen and others.
P.A. DE GROOT, Arjen Klaas in zijn naam.
T.J. DEKKER, Parallelism in ALGOL68: the five dining philosophers revisited.
E. DOBBER, Vrije tijd of werken?
J. EBERGEN, Het perfide Zuiden.
G.M.M. FOEKEMA, Gustav Mahler en Richard Strauss.
W. HOFFMANN, Singuliere-waardenontbinding en datacompressie.
R. KANNAN, Best wishes.
E. KALTOFEN, On a theorem by R. Dedekind.
E. KOK-DE GROOT, Je moest wel.
D. KOZEN, A Ramsey theorem on infinitely many colors.
H.W. LABBERS, JR., Über die Unprimzähligkeit.
J.C. LAGARIAS, Oids and their ilk.
G. LAMAN, De boom van het onderscheid.
S. LANDAU, Ode to Arjen.
W.F. LANKAMP, M. LANKAMP-VAN DER ZEYDE, Rechtsvinding in het burendrecht.
F.C. LAUWAARS, A.J. LENSTRA, J. SCHOOTSTRA, Vonnis 13-9-1984.
A.K. LENSTRA, Het boek van vader en moeder Geit.
C.M. LENSTRA, Het gekke huis.
G.A. LENSTRA, Molto vivace.
H.W. LENSTRA, SR., Krachtige meetkunde.
J.A. LENSTRA, B.A. HUITEMA, Biologische informatica.
W.C.H. LENSTRA, De figurant.
K.C.E. LENSTRA-DE GROOT, Pas de problèmes.
M. LENSTRA-GERRITS, La cottura delle paste.
C.F. LENSTRA-VAN INGEN SCHENAU, Een vensterbank voor Arjen.
B.E. LUB, Het BELIAL project.
R.H. MAK, Over een jonge doctor, zijn bagage, en twee ringen.
A. MIOLA, Algorithms for symbolic determination of Laplace transform.
S.J. MULLENDER, Capability management in distributed operating systems.
F.A. MULLER, Het munten-weegprobleem.
G.J. MULLER, Toekomstvisioen.
J.L. NICOLAS, Être ou ne pas être un carré.
M.A. ODLYZKO, A disproof of the Reimann hypothesis.
A. PAZ, Some NP-hard problems connected with the extended Euclidean-algorithm for n-integers.
C. POMERANCE, Are there counter-examples to the Baillie-PSW primality test?
M. REM, Het Brouwerinstituut.
L.C. ROOKMAKER, De mathematische achtergrond van de rhinoceros.

E.W. ROSCAM ABBING, Een laatste stelling ter verdediging.
 C.P. SCHORR, A remark on the construction of short lattice elements.
 A. SCHÖNHAGE, Root finding in polynomial time.
 R.J. SCHOOF, L. WASHINGTON, Let p be the prime.
 A. SCHRIJVER, Ervaringen met L , L^2 en L^3 .
 D.C. SHANKS, Two conjectures about a_n .
 G.J. SIMMONS, Goede morgen.
 W. SIMONIS, Op feesten en verjaardagen.
 J. STERRINGA, Onwetenschappelijke observaties.
 H.J.J. TE RIELE, Over de laatste stelling.
 R. TIJDEMAN, La musica e le parole.
 G.M. TUYNMAN, De fysica van het openen van een deur.
 J. VAN DE LUNE, !? True .or. false ?!
 A.S. VAN DOBBENBURGH, Dichtwerck.
 L. VAN DOBBENBURGH, M. KROESE, Homo polynomo.
 W.G. VAN DOBBENBURGH, G.M. VAN DOBBENBURGH-VRIES, Eindelijk vrij!
 VAN DOBBENBURGH-FRENKEL, Je kwam, zag, en overwon.
 P. & B. VAN DOBBENBURGH-ROSSBERG, Badinage.
 A. & P. VAN DOBBENBURGH-SCHUT, De manier, waarop het onvermijdelijke zich
 voltrekt, is door inspanning.
 J. VAN WITSEN, Een zielige bijdrage.
 P. VAN EMDE BOAS, Photo quiz.
 K. VAN LEEUWEN, B.S. MIJLPAAL, A.D.S. DE SCHUITE, De top der Nederlandse
 informatica.
 P.M.B. VITÁNYI, Counting is easy.
 N.J. VRIES, Ontbinding van veeltermen per proefschrift.
 S.S. WAGSTAFF, JR., On the foundations of computer science; part I: what is
 a bit?
 P.J. WEINBERGER, Calculating with real numbers.
 Oplossingen.

On Distinguishing 89 From Not 89

by

Leonard M. Adleman and Robert S. Rumely

On The Awarding of A.K. Lenstra's Doctorate

It is now well known how to establish the primality of very large numbers [1], [2]. In this opus we make some rather dramatic progress on the still open problem of establishing the primality of very small numbers.

I. History

In recent years much progress has been made on the problem of finding fast algorithms for determining whether or not very large numbers are prime.

Initially these algorithms had the disadvantage that they only performed well in one small city in Monaco [4]. Later new algorithms were developed for which it was claimed no such geographical restriction existed.

We in the United States were skeptical of these claims, since all implementations of these algorithms here ran very slowly.

Finally in 1983 the issue was put to rest when A.K. Lenstra visited the United States. He brought with him a 200 digit number, the primality of which he had established in only five minutes of computation! Since an examination of his passport revealed that he had never been in SE France and it was clear that his coresearchers H. Cohen and H. Lenstra never got out of the house much; there was no other option but to conclude that the geographical problem had been overcome. The new primality algorithm would work anywhere in the world!

With the problem of establishing the primality of very large numbers solved, the authors turned to the related problem of establishing the primality of very small numbers.

In December of 1983 the breakthrough occurred. Rumely was able to establish the primality of 89 using the techniques which A.K. Lenstra had revealed. Rumely presented his results to an enthusiastic but admittedly small group at the West Coast Number Theory Conference in Asilomar, California. We welcome this opportunity to reach a larger audience.

II. The Proof Method (The Lenstra/Cohen Test (Square Free Version))

Given n :

1. Initial prime, Euclidean prime setup:

Take a sufficiently large initial segment of primes $I = \{2, 3, 5, \dots\}$ such that the product of the primes in the set

$$\mathcal{Q} = \{q : q = (\prod_{p \in \mathcal{S}} p) + 1 \text{ where } \mathcal{S} \subseteq I\} \text{ is greater than } n.$$

Throw away some of the primes in $\mathcal{Q}$, keeping only enough that the product is greater than n .

$$\text{Let } P = \prod_{p \in I} p, \text{ and let } Q = \prod_{q \in \mathcal{Q}} q.$$

2. Compute Jacobi Sums

For each pair (p, q) with $q \in \mathcal{Q}$ and $p \in I$, and $p|q-1$ compute an element

$$J_{p,q} \in \mathcal{Q}(\xi_p) \text{ to use in the pseudo-primality tests:}$$

If $p = 2$, put $J_{p,q} = -q$;

If p is odd, choose a character χ of $(\mathbb{Z}/q\mathbb{Z})^*$ having order p .

- For example, let g be a primitive root for $(\mathbb{Z}/q\mathbb{Z})^*$, and define χ by

$$\chi(g^x) = \xi_p^x \text{ where } \xi_p \text{ is a primitive } p^{\text{th}} \text{ root of unity. Also let } \chi(0) = 0.$$

$$\text{Then compute } J_{p,q} = \sum_{x \bmod q} \chi(x)\chi(1-x) \in \mathbb{Z}[\xi_p].$$

3. Pseudo-Primality Tests

For each pair (p, q) with $p \in \mathcal{I}$, $q \in \mathcal{Q}$, $p|q-1$ do the following:

If $p = 2$: compute $(J_{p,q})^{(n-1)/2} \bmod n$.

If $(J_{p,q})^{(n+1)/2} \not\equiv \pm 1 \bmod n$. Then n is composite.

If p is odd: compute $\prod_{a=1}^{p-1} \sigma_a(J_{p,q}^N) \bmod n\mathbb{Z}[\xi_p]$.

Here σ_a is the automorphism of $\mathcal{Q}(\xi_p)$ taking $\xi_p \rightarrow \xi_p^a$, and

$$N_a = \frac{n\{a^{-1}\} - \{na^{-1}\}}{p}$$

where a^{-1} is an inverse of $a \bmod p$, and $\{k\}$ means the least positive residue of $k \bmod p$.

If $\prod_{a=1}^{p-1} \sigma_a(J_{p,q}^N) \not\equiv \xi_p^b \bmod n\mathbb{Z}[\xi_p]$ for some b then n is composite.

4. Make p good for n .

In order for step (3) to be applicable, the following condition must be met for each $p \in \mathcal{I}$:

For each p , there must be a q for which the root of unity produced in step (3) is nontrivial (not $= 1$). Usually this condition will be met in the course of the tests in step (3). If it is not, carry out the test of step (3) for other randomly chosen q 's such that $p|q-1$ until a nontrivial root of unity occurs.

5. Test Possible Divisors

The possible divisors for n will be found among the least positive residues of

$$n^k \bmod \mathcal{Q}, \text{ for } k=1, \dots, P.$$

Test these numbers. If they are not proper divisors, then n is prime.

III. The Proof for 89

Step 1: (Setup)

Take $I = \{2, 3\}$. The numbers of the form $(\prod_{p \in S} p) + 1$, $S \subseteq I$ that are prime are

3, 7. Here $\sqrt{89} \simeq 9.4 < 3 \cdot 7 = 21$ so take $\mathcal{Q} = \{3, 7\}$. Therefore $P = 6$, $Q = 21$.

Step 2: (Compute Jacobi Sums)

$$J_{2,3} = -3 \quad J_{2,7} = -7$$

For $J_{3,7}$, note that 5 is a primitive root for $\mathbb{Z}/7\mathbb{Z}$, and write $\xi = \xi_3$. Then x_3 is given by

	0	1	2	3	4	5	6
x_3	0	1	ξ	ξ^2	ξ^2	ξ	1

$$J_{3,7} = \sum_{x=0}^6 x_3(x) x_3(1-x) = 0 \cdot 1 + 1 \cdot 0 + \xi \cdot 1 + \xi^2 \cdot \xi + \xi^2 \cdot \xi^2 + \xi \cdot \xi^2 + 1 \cdot \xi$$

$$= \xi + 1 + \xi + 1 + \xi = 2 + 3\xi$$

Step 3: (Pseudo Primality Tests)

Powers of -3:	n	0	1	2	4	8	16	32
mod 89	$(-3)^n$	1	-3	9	81	64	2	4

$$\frac{89-1}{2} = 44 = 32+8+4:$$

$$\boxed{(-3)^{44} \equiv 81 \cdot 64 \cdot 4 \equiv -1 \pmod{89}}$$

Powers of -7:	n	1	2	4	8	16	32
mod 89	1	-7	49	87	4	16	78

$$\frac{89-1}{2} = 44 = 32+8+4:$$

$$(-7)^{44} \equiv 87 \cdot 4 \cdot 78 \equiv -1 \pmod{89}$$

Powers of $2+3\xi$:	n	0	1	2	4	8	16
mod $89\mathbb{Z}[\xi]$	$(2+3\xi)$	1	$2+3\xi$	$-5+3\xi$	$16-39\xi$	$-19-10\xi$	$-6+13\xi$

$$N_1 = \frac{89\{1\} - \{89\}}{3} = \frac{89-2}{3} = 29 = 2(8+4+2)+1$$

$$N_2 = \frac{89\{2\} - \{89 \cdot 2\}}{3} = \frac{178-1}{3} = 59 = 2(29)+1$$

n	1	6	14	28	29	58	59
$(2+3\xi)^n$		$37+43$	$-40-50\xi$	$-10-13\xi$	$19-17\xi$	$-17-45\xi$	$12-6\xi$

Here in computing these we have used the relation $1+\xi+\xi^2 = 0$ and working mod $89\mathbb{Z}[\xi]$ means freedom to change each coordinate in a representation $a+b\xi$ by multiples of 89. For example to compute $(2+35)^6$ we multiply $(2+35)^2$ by $(2+35)^4$

$$\begin{aligned} & -5+3\xi \\ & 16-39\xi \\ & -80+48\xi \\ & +195\xi-117\xi^2 \\ & -80+243\xi-117\xi^2 \\ & +117+117\xi+117\xi^2 \text{ (i.e. adding 0)} \\ & 37+360\xi \end{aligned}$$

$$37+360\xi \equiv 37+360\xi-4(89)\xi = 37+4\xi \pmod{89\mathbb{Z}[\xi]}$$

We want to compute:

$$\sigma_1(J_{3,7}^{N_1}) \cdot \sigma_2(J_{3,7}^{N_2}) \bmod 89\mathbb{Z}[\xi]$$

$$\begin{array}{c}
\sigma_1(J_{3,7}^{N_1}) \cdot \sigma_2(J_{3,7}^{N_2}) \\
||| \\
\sigma_1((2+3\xi)^{29}) \cdot \sigma_2((2+3\xi)^{59}) \\
||| \\
\sigma_1(19-17\xi) \cdot \sigma_2(12-6\xi) \\
||| \\
(19-17\xi) \cdot (12-6\xi^2) \\
||| \\
(19-17\xi) \cdot (18+6\xi) \quad (\text{we added } 0 = 6+6\xi+6\xi^2) \\
||| \\
-1-\xi \\
||| \\
\xi^2 \quad (\text{We added } 0 = \xi^2 + \xi + 1) \\
\text{MOD } 89\mathbb{Z}[\xi]
\end{array}$$

Step 4: (Making p good for 89)

From the computation in step (3), both $p = 2$, $p = 3$ are good because nontrivial roots of unity appeared in the congruences.

Step 5: (Test possible divisors)

The powers of 89 and 21 are:

$89^1 \equiv 5 \pmod{21}$	$5 \nmid 89$
$89^2 \equiv 4 \pmod{21}$	$4 \nmid 89$
$89^3 \equiv 20 \pmod{21}$	$20 \nmid 89$
$89^4 \equiv 16 \pmod{21}$	$16 \nmid 89$
$89^5 \equiv 17 \pmod{21}$	$17 \nmid 89$
$89^6 \equiv 1 \pmod{21}$	improper divisor of 89

Hence 89 is a prime number.

IV. Conclusions

Since it took only 5 minutes to establish the primality of the 200 digit number, but at least an hour to establish the primality of 89, we conclude that the problem becomes

more difficult as the numbers get smaller. This raises the obvious open question:

**CAN THE PRIMALITY OF ARBITRARILY SMALL NUMBERS BE
ESTABLISHED IN A FINITE AMOUNT OF TIME?**

In [3] we have taken what we believe is an important step toward resolving this question.

V. References

1. Adleman, L.M., Pomerance, C. and Rumely, R.S., *On Distinguishing Prime Numbers From Composite Numbers*, Annals of Mathematics, 1983, pp. 173-206.
2. Cohen, H. and H.W. Lenstra, Jr., *Primality Testing and Jacobi Sums*, Mathematisch Instituut, University van Amsterdam, Report 82-18, October, 1982.
3. Adleman, L.M., Rumely, R.S., *An Application of Capacity Theory to the Primality Question for 51*, Journal of Unsettling New Knowledge, Vols. 22 through 67, to appear.
4. R. Solovay and V. Strassen, *A Fast Monte-Carlo Test for Primality*, SIAM J. Comput. (1977), 84-85; erratum, 7 (1978), 118.

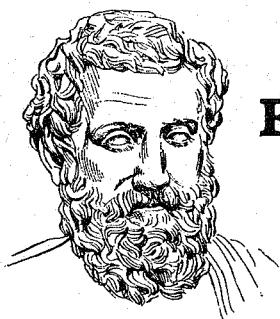
AD ARJEN K. TENSTRA

In occasione della difesa della sua tesi dottorale

**Bennis Arnon
Purdue University**

**S'intrecci il loto al lauro
Sui crin di Arjen
Nembo gentil di fiori
Stenda sul suo terminale un vel.
Danziam, informatici e matematici
Le mistiche carole,
Come d'intorno al sole
Danzano gli astri in ciel.**

(Con mille scuse ad Antonio Ghislanzoni)



EEN IONISCH POLYNOOM

Reinoutje Artz

Priamos van Milete

Toen Priamos van Milete rond het jaar 530 v. Chr. aan boord ging van het schip dat hem van zijn vaderstad naar Zuid-Italië zou brengen, kon hij niet weten dat deze stap in zijn leven tot in de twintigste eeuw van grote betekenis zou zijn voor de wiskunde.

Hij was één van de velen die Ionië ontvluchtten, omdat de perzische bezetter de Grieken die daar woonden steeds minder vrijheid liet, ook in hun denken. De intellectuelen onder deze vluchtelingen gingen naar plaatsen waar kunst en wetenschap bloeiden en niet aan banden werden gelegd, zoals Samos, Athene en de griekse steden in Zuid-Italië.

Priamos' bestemming was Kroton, waar kort tevoren een broederschap was opgericht door Pythagoras van Samos, die een geheel eigen getallenleer onderwees. In deze pythagoreïsche getallenleer wilde Priamos zich bekwaamen. Zijn kennis van filosofie en wiskunde was groot, naar de maatstaven van die tijd: als twaalfjarig jongetje was hij in de leer gegaan bij zijn beroemde tijdgenoot Thales van Milete en vergezelde die op zijn reis naar Babylon, waar de Chaldaëen hem nog een jaar verder wiskundeonderricht gaven. Aldus opgeleid begon Priamos na zijn terugkeer in Milete zijn eigen bijdragen te leveren aan de filosofische theorieën van zijn tijd. Hij zette die in hexameters op schrift in zijn werk 'περὶ φύσεως' waarvan slechts zulke kleine fragmenten bewaard zijn gebleven dat we er niet uit kunnen opmaken, wat zijn opvattingen waren in deze tijd.

Meer weten we van Priamos door zijn brieven, die hij gedurende zijn omzwervingen door Zuid-Italië en Etrurië naar zijn broer Hestiaeus in Milete schreef. Deze brieven, 97 in getal, zijn op een serie papyri bewaard gebleven, die in 1906 te Oxyrhynchus (in Egypte) is ontdekt. Hoewel de tekst vrij corrupt is overgeleverd geeft hij toch een tamelijk gedetailleerd beeld van het dagelijks leven in het Magna Graecia en Etrurië van de 6e eeuw v. Chr. Maar voor ik op de inhoud van enkele brieven inga, zal ik een korte schets geven van de ontwikkeling van filosofie en wiskunde tot in Priamos' tijd. Hierdoor is Priamos' verdienste op dit vlak beter op waarde te schatten.

Het begin van wijsgerig denken in het westen vinden we in Ionië. Hier begonnen in de 6e eeuw v. Chr. een aantal filosofen theorieën te formuleren over het ontstaan en de samenstelling van de wereld en van de hele kosmos. Verder probeerden zij een verklaring te vinden voor de veranderingen die zich in de waarneembare wereld voordoen. Zij worden daarom de Natuurfilosofen genoemd. Volgens hun theorie moesten alle verschijnselen terug te brengen zijn tot één oerstof, de ἀρχή, die overal aan ten grondslag ligt.

De oudste van deze filosofen waren Thales, Anaximander en Anaximenes, alledrie afkomstig uit Milete. Zij hielden zich bij hun onderzoekingen ook zeer intensief bezig met de astronomie. De wiskundige kennis die ze hiervoor nodig hadden deden ze op bij de Chaldaëen in Babylon.

Uit de natuurfilosofie kwam een school voort, waarvan Pythagoras de stichter was. Kenmerkend voor zijn theorie is dat de wiskunde er een vooraanstaande plaats in inneemt, doordat als ἀρχή het getal wordt gekozen, met als oergetal 1, waarvan alle andere zijn afgeleid. Alle betrekkingen, zo stellen de Pythagoraeërs, zijn in getallen uit te drukken. De praktische toepassing hiervan leidde tot een getallensymboliek als: 1 is het punt, 2 de lijn, 3 het vlak, 4 het lichaam, maar 1 is ook hoofd, 2 het hart, 4 de gerechtigheid etc.

Priamos van Milete was één van de eerste leerlingen van de Pythagoreïsche school, maar hij bleef er niet erg lang, waarschijnlijk slechts 15 maanden. Toen besloot hij, om ons onbekende redenen, de broederschap te verlaten. Het moet echter niet worden uitgesloten dat de oorzaak van zijn vertrek lag in de persoonlijke tegenstelling tussen hem en de als zeer eigenzinnig bekend staande Pythagoras. Dit gebeurde omstreeks 528 v. Chr. De eerste brief op de overgeleverde Oxyrhynchus papyrus dateert uit deze tijd. Hierin deelt Priamos zijn broer mee dat hij weggaat. Hij begint als volgt:

Ἐστίαίω τῷ ἀδελφῷ
 Κροτώνα ἔλιπον | | πεντεκαίδ<εκα> μῆνα
 | | σὺν ἑταίρῳ Κύνι, ὃν φλίψ<εν>¹⁾
 ὠνόμασα. (P. Oxy. 2202 fr. 1)

"Aan mijn broer Hestiaeus. Ik heb Kroton verlaten (lacune) 15 maanden (lacune), met als metgezel een hond, die ik Philipsen heb genoemd."

Na zijn vertrek uit Kroton heeft Priamos vele jaren een zwervend bestaan geleid. Hij werd, wat de Grieken noemden, een πολύνομος (lett. "iemand die veel verblijfplaatsen heeft".) De brieven uit de eerste jaren bevatten uitsluitend reisverhalen en geven geen enkele aanwijzing dat Priamos zich nog met wiskunde bezighield. Hij beschrijft de plaatsen die hij bezoekt, de mensen die hij ontmoet en de logementen waarin hij verblijft. Een karaktereigenschap van Priamos die in de brieven sterk naar voren komt, is zijn liefde voor dieren, vooral honden. De hond Philipsen blijft nog jaren in de brieven figureren. Priamos was zozeer aan hem gehecht geraakt, dat hij in tijden van armoede het eten uit zijn eigen mond spaarde om Philipsen in leven te houden. "Niets maakt mij zo gelukkig, als de kans om Philipsen zijn lievelingsmaal te geven: vis met brood en chocoladekoek. Ik koop dit bij een Phoeniciër, die zijn waren aanprijst in het Phoenicisch, Grieks en Oskisch door elkaar", vertelt Priamos in een brief uit een tijd waarin het hem financieel kennelijk beter gaat. De dierenliefde van deze St. Franciscus avant-la-lettre ging zelfs zo ver, dat hij zijn hond meenam wanneer hij naar het theater ging. En dat was zeer dikwijls, zo blijkt uit zijn brieven. Geen gelegenheid om een tragedievoorstelling bij te wonen liet hij ongebruikt voorbijgaan. Zonodig reisde hij er zelfs een aantal dagen voor om. Van elke tragedievoorstelling zendt hij een minutieus verslag aan zijn broer.

Priamos meldt, na talrijke omzwervingen, dat hij in Etrurië is beland en in Tarquinia bij een Corinthische pottenbakker, Demaratos, gastvrij onderdak heeft gevonden. De eerste brieven uit Tarquinia staan vol met beschrijvingen van de zeden en gewoontes van de Etrusken, die zeer afwijkend waren van die van de andere volkeren in Italië. Vooral de etruskische eetgewoontes vergden enige aanpassing van Priamos' zijde:

..."Zij eten verder een gekruide tonijnsaus²⁾ met tomaten, waar zij lange repen brood in weken. Bij het nuttigen hiervan pleegt mijn chiton vol druppels te raken, zodat ik, tot plezier van mijn gastheer, mij genoodzaakt heb gezien een schort³⁾ te dragen, wanneer dit gerecht ter tafel komt..." (P. Oxy. 2306)

Aan de eetgewoontes kon Priamos wel wennen maar waar hij nooit aan gewend raakte was het feit dat er in de etruskische steden nooit tragedievoorstellingen werden gegeven. We weten dat hij voor de opvoering van de "Phoenissae" van de dichter Phrynichus speciaal naar Cumae, de dichtstbijzijnde griekse stad, is gereisd.

Wat hem desondanks in Tarquinia hield, was zijn hernieuwde belangstelling voor wiskunde, waarschijnlijk opgewekt door de etruskische cultuur. De Etrusken waren namelijk zeer geavanceerde ingenieurs, meesters in het bouwen van bruggen en gewelven, waarbij ze ook hun wiskunde tot een hoog niveau hadden gebracht. Priamos begint zijn broer steeds vaker te schrijven over de gedachten die hem bezighouden m.b.t. de getallen en de pythagoreïsche getallentheorie, die hij kennelijk niet geheel had afgezworen. De ontdekking die voor de wiskunde van zoveel belang zou worden, deed Priamos omstreeks 510 v. Chr. Hij schreef toen namelijk aan zijn broer Hestiaeus:

Δοκοῦσιν β' γ' ε' γ' ια' ιγ' ιζ' ιθ'
ἀριθμοὶ τελείου εἶναι. (P. Oxy. 2217 fr. 2)



Fig. 1.

We zien hier voor het eerst in de pythagoreïsche traditie der getallentheorie verwoord dat er getallen zijn met de kenmerkende eigenschap dat ze 'volmaakt' zijn, zoals Priamos het nog uitdrukt. Met deze ontdekking brengt hij de Pythagoraeërs een stap verder in hun ontwikkeling van de wiskunde. Met hun grotere waardering van 'volmaakte' getallen boven de 'onvolmaakte' was voor hen Priamos' ontdekking baanbrekend.

Philolaos, een late Pythagoraeër (midden 5e eeuw v. Chr.) heeft het in zijn geschrift περὶ φύσιος over de Πριάμου ἀριθμοί, de getallen van Priamos, i.p.v. over de τελείου ἀριθμοί. Of hij hiermee de getallen uitdrukkelijk naar Priamos wilde noemen is niet met zekerheid vast te stellen. In elk geval is Philolaos' term 'Priamos-getallen' door de eeuwen heen gehandhaafd en wordt tegenwoordig nog steeds gebruikt, zij het in de verbasterde vorm 'priem getallen'. (In een bizantijns handschrift vinden we nog de tussenfase: 'priam-getallen').

In de laatste brief op de Oxyrhynchus papyrus beschrijft Priamos vol ontzetting en verdriet hoe de Pythagoraeïsche school in Kroton door tegenstanders in brand is gestoken en hoe daarna felle vervolgingen, ten dode toe, in heel Zuid-Italië volgden.⁴¹ Daarna

horen we niets meer van Priamos. Het is niet bekend

of deze brief ook zijn laatste is geweest. Hij moet over de 60 zijn geweest toen hij hem schreef, voor die tijd een respectabele leeftijd.

Ook uit andere litteraire bronnen is verder niets bekend over het einde van Priamos. Maar dat hij desondanks toch niet spoorloos van de aardbodem is verdwenen danken we behalve aan zijn brieven en aan Philolaos ook aan de beeldende kunst.

In Apulië is een lecythos gevonden (Fig. 1), waarop een fries met priemgetallen is aangebracht. Dit heeft er toe geleid dat men algemeen aanneemt dat de jager met de hond, die boven het fries zijn afgebeeld, Priamos en Philipsen voorstellen.

Wat gecompliceerder is het geval van de Tomba dei Leopardi in Tarquinia. Het plafond van deze grafkamer is geruit, wat gebruikelijk is voor etruskische graven uit die tijd. Niemand had echter enige speciale aandacht aan het ruitenpatroon besteed, totdat in de vijftiger jaren de engelse

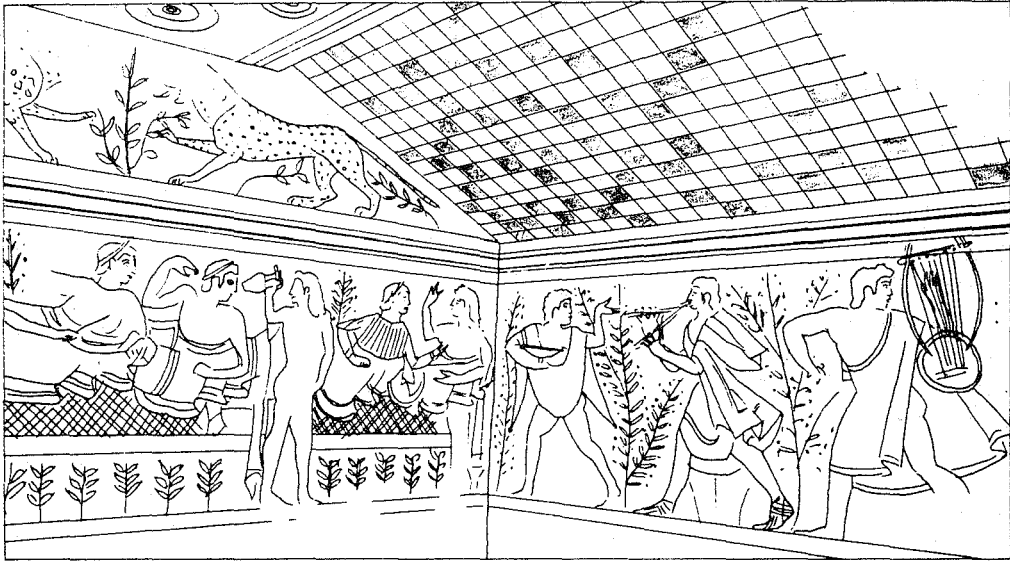


Fig. 2.

wiskundige Sir William Eldrie het graf bezocht en zag dat het plafond een priemgetallenpatroon vertoonde. (Fig. 2.)

Priamos maakte klaarblijkelijk veel indruk op zijn omgeving, iets wat niet gezegd kan worden van zijn leermeester Pythagoras, die de reputatie had een lichtgeraakte nurks te zijn. Gezien de totaal verschillende karakters van leerling en leermeester, is het dan ook niet verbazingwekkend dat Philolaos Priamos typeert als 'kweeling van Pythagoras'.

Noten:

- 1) Van de twee coniecturen $\Phi\lambda\iota\psi\sigma$ en $\Phi\lambda\iota\psi\epsilon\nu$ wordt de laatste algemeen het waarschijnlijkst geacht.
- 2) Men merke op dat Priamos het niet zo nauw nam met de pythagoreïsche leer van de zielsverhuizing ($\mu\epsilon\tau\epsilon\mu\psi\acute{\upsilon}\chi\omega\sigma\iota\varsigma$) die het eten van vlees, gevogelte en vis verbood.
- 3) Over de juiste betekenis van dit woord is men het niet eens. Het meest logisch zou het woord 'servet' zijn, maar deze betekenis is zonder parallel. Tegen de vertaling 'schort' pleit het argument dat Priamos ten tijde van dit schrijven een volwassen man was, die toch in staat geacht moet kunnen worden zich met een servet te behelpen en niet een heel schort nodig te hebben.
- 4) Deze gebeurtenissen zijn ook uit andere bronnen bekend en dateren de brief op ca. 500 v. Chr.

De vraag of iets vlees is of vis bezorgt ons geen slapeloze nachten. Meestal denken we het antwoord te weten (sommigen van ons blijven naïef), maar zelfs als dat niet het geval is roept het probleem zelden existentiële spanningen op.

Eens lag dat toch anders. In de middeleeuwen was het wel degelijk van groot belang, zowel voor de hongerige landman of gezel als voor de verfijnde levensgenieters, vorsten en abten en paters goedleven, te weten of men vis of vlees voor zich had, op Vrijdagen bijvoorbeeld en in de Vastentijd. Gelukkig - Dei Gratia - was er iets dat de smakelijker en voedzamer eigenschappen van vlees (van gevogelte, om precies te zijn) paarde aan de rituele reinheid van vis: de barrakylle, barnacle goose (1), brandgans of Anser Leucopsis (Branta leucopsis).

Wat dit te maken heeft met Arjen Lenstra, of met "Polynomial-time Algorithms for the Factorization of Polynomials"? Dat lijkt mij duidelijk, althans voor de doorsnee getaltheoreticus of econometrist. Wie zijn wiskunde even belangrijk acht als zijn dagelijkse of wekelijkse biefstuk of gehaktbal zal menige activiteit, uitgevoerd onder de informatica-vlag, als "fishy" afschrijven. Maar soms is ook hier vis even smakelijk en voedzaam als vlees. Laten we dus maar dankbaar zijn voor de ganzenboom!

Sinds de informatica in Nederland de zolang en zo vurig verbeide erkenning als zelfstandige studierichting verwierf, en de eeuwig in oprichting blijvende Stichting SION in het aardse paradijs der door ZWO erkende organen werd opgenomen, lijkt het ongepast te insinueren dat er intieme betrekkingen zouden kunnen bestaan tussen het wiskundig denken en het doen der rekentuig-wetenschappers. Over een instelling als het CWI, waar desondanks gelegenheid wordt gegeven tot niet-gechaperonneerde ontmoetingen, wordt dan ook bij tijd en wijle flink geroddeld. De goede naam van dit Centrum wordt zo bedreigd door factoren van ontbinding.

In deze delicate situatie verschijnt nu die verhandeling van een soi-disant informaticus over algoritmen voor ontbinding in factoren, een verhandeling waarin geen enkel programma is afgedrukt, niet in ALGOL 68 en evenmin in de uiterst gebruikersvriendelijke taal B, noch in de tekst noch in appendices, terwijl wel wordt verwezen naar HENSEL's lemma, gebruik gemaakt wordt van Meetkunde der Getallen, van p-adische waarderingen en van nog veel meer esoterische mathesis. Is this animal, vegetable or mineral? Wat moeten we hiermee aan?

Gelukkig is er een algoritme om de vraag naar het genus van "Polynomial algorithms....." bevredigend en snel te beantwoorden. In een recente "Mathematical Intelligencer" stond een gave recursieve definitie van een "wiskundige": *"Een wiskundige is iemand van wie een wiskundige vindt dat hij/zij een wiskundige is"*. Zoals iedere recursieve definitie heeft ook deze een basis nodig, en die wordt dan ook toegevoegd: *"Karl Friedrich GAUSS is een wiskundige"*. Deze definitie is uiteraard onmiddellijk overdraagbaar (portable) naar de informatica. De recursieve clause zal de intelligente lezer zelf wellicht kunnen formuleren. De basis-clause vergt echter enige subtiliteit: bij de startpositie *"E.W. DIJKSTRA is een informaticus"* krijgt men bepaald een andere bevolking in het aquarium dan bij de start-keuze *"Paul J.W. TEN HAGEN is een informaticus"*. Maar als aan de basis van de recursie voldoende zorg wordt besteed, zal blijken dat A.K. Lenstra (en wellicht zelfs P. van Emde Boas) een informaticus is. Voeg nu nog toe de regel *"informatica (resp. wiskunde) is alles waarvan een informaticus (resp. een wiskundige) meent dat het informatica (resp. wiskunde) is"*, en onze snelle algoritme ligt voor het grijpen.

Na deze handreiking zal van de lezers van dit gedenkboek de hierboven opgeroepen vraag, nl. of het proefschrift van Arjen Lenstra nu echt gave informatica is, of misschien toch (een klein beetje) wiskunde, ondubbelzinnig en definitief beantwoord zijn. Deze bijdrage ware dus voltooid te achten, ware het niet dat een enkeling mij reeds heeft laten weten toch nog iets meer achtergrondinformatie op prijs te stellen over die gevederde vis, de barnacle goose. Gaarne zal ik deze enkeling ter wille zijn. De anderen kunnen door naar de volgende bijdrage.

In de winter 1980-1981 hebben opmerkelijke parkeerders enkele malen een zevental brandganzen kunnen waarnemen die graasden op de ringdijk van de Watergraafsmeer, achter het parkeerterrein bij het begin van de lineaire versneller. Deze vogels, die in de zomer zich veel noordelijker plegen op te houden, bezoeken in de wintermaanden geregeld Ierland, Schotland en de kustgebieden van Noord-Europa.

De engelse barbier en chirurgijn John GERARD publiceerde in 1597 een kruidenboek of "Herball", waarvan de inhoud voor een belangrijk deel geplagieerd was uit het werk van DODOENS. Het laatste hoofdstuk echter, getiteld "The Goose Tree, Barnacle Tree, or the Tree bearing Geese", is bij DODOENS niet terug te vinden. Hierin schrijft GERARD onder meer:

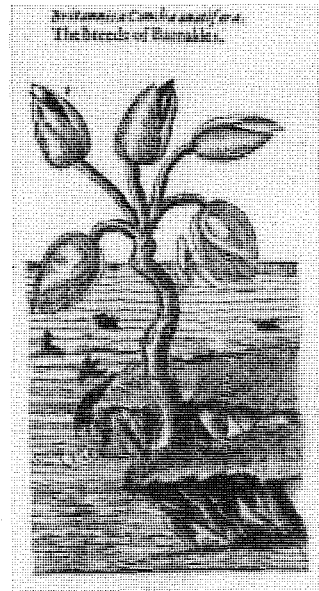
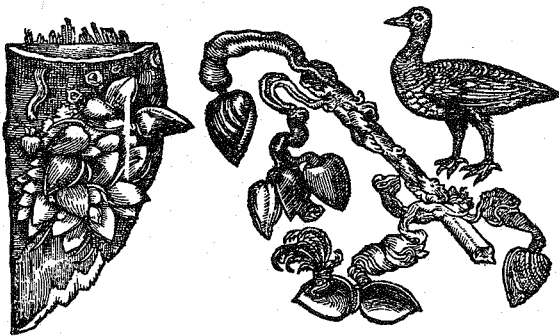


Het kruidboek van GERARD is vele malen herdrukt.
 Het bekendst is de heruitgave door Thomas JOHNSON in 1636,
 die veel nieuw materiaal bevatte.

"There are found in the North parts of Scotland and the Islands adjacent, called Orchades, certaine trees whereon do grow certaine shells of a white colour tending to russet, wherein are contained little living creatures: which shells in time of maturity doe open, and out of them grow those little living things, which falling into the water do become fowles, which we call Barnacles; in the North of England Brant Geese; and in Lancashire tree Geese: but the other that do fall upon the land perish and come to nothing. Thus much by the writings of others and also from the mouthes of people of those parts, which may very well accord with truth

But what our eyes have seen, and hands have touched we shall declare. There is a small Island in Lancashire called the Pile of Foulders, wherein are found the broken pieces of old and bruised ships, some whereof have beene cast thither vy shipwracke, and also the trunks and bodies with the branches of old and rotten trees, cast up there likewise; whereon is found a certaine spume or froth that in

time breedeth unto certaine shells, in shape like those of the Muske, but sharper pointed, and of a whitish colour; wherein is contained a thing in forme like a lace of silke finely woven as it were together, of a whitish colour, one end whereof is fastned unto the inside of the shell, even as the fish of Oisters and Muskles are: the other end is made fast unto the belly of a rude mass or lumpe, which in time commeth to the shape and forme of a Bird: when it is perfectly formed the shell gapeth open, and the first thing that appeareth is the foresaid lace or string; next come the legs of the bird hanging out, and as it groweth greater it openeth the shell by degrees, til at length it is all come forth, and hangeth onely by the bill: in short space after it commeth to full maturitie, and falleth into the sea, where it gathered feathers, and groweth to a fowle bigger than a Mallard, and lesser than a Goose, having black legs and bill or beake, and feathers blacke and white, spotted in such manner as is our Magpie, called in some places a Pie-Annet, which the people of Lancashire call by no other name than a tree Goose: which place aforesaid, and all those parts adjoyning do so much abound therewith, that one of the best is bought for three pence. For the truth hereof, if any doubt, may it please them to repaire unto me, and I shall satisfie them by the testimonie of good witnesses.



Moreover, it should seeme that there is another sort hereof; the History of which is true, and of mine owne knowledge: for travelling upon the shore of our English coast betweene Dover and Rumney, I found the trunke of an old rotten tree, which (with some helpe that I procured by Fishermens wives that were there attending their husbands returne from the sea) we drew out of the water upon dry land: upon this rotten tree I found growing many thousands of long crimson bladders, in shape like unto puddings newly filled, before they be sodden, which were very cleere and shining; at the nether end whereof did grow a shell fish, fashioned somewhat like a small Muske, but much whiter, resembling a shell fish that groweth upon the rockes about Garnsey and Garsey, called a Lympit: many of these shells I brought with me to London, which after I had opened I found in them living things without forme or shape; in others which were neerer come to ripeness I found living things that were very naked, in shape like a Bird: in others the Birds covered with soft downe, the shell halfe open, and the Bird ready to fall out, which no doubt were the Fowles called Barnacles. I dare not absolutely avouch every circumstance of the first part of this history, concerning the tree that beareth those buds aforesaid, but will leave it to a further consideration; howbeit, that which I have seene with mine eies, and handled with mine hands, I dare confidently avouch, and boldly put downe for verity".

Voorwaar een boeiend relaas, en ditmaal, zoals reeds opgemerkt, niet overgeschreven uit DODOENS of DE L'OBEL. Ik was dus jarenlang geneigd GERARD's verklaring "*what our eies have seen, and hands have touched, we shall declare*" serieus te nemen. Zelfs een chirurgijn zal toch bij tijd en wijle te vertrouwen zijn!

Maar vorig jaar verwierf ik mij de Penguin Classics uitgave van de "*Topographia Hibernica*" door Giraldus Cambrensis (vertaald uit het Latijn door John J. O'MEARA). Gerald de Barry, of Gerald van Wales, zal wel geen voorvader geweest zijn van Gerard de chirurgijn, want als jongste zoon in een adellijk geslacht was hij van de wieg af geroepen tot een geestelijk ambt (2). In 1183 vergezelde Gerald prins Jan (Zonder Land, weet u wel) naar Ierland, waar zo nodig de Pax Brittanica moest worden uitgedragen, en wat hij daar allemaal zag en meemaakte was ruim voldoende voor een leven lang vertellen bij het haardvuur. En wat lezen we in hoofdstuk II, getiteld

"Barnacles that are born of the fir-tree and their nation"?

"There are many birds here that are called barnacles, which nature, acting against her own laws, produces in a wonderful way. They are like marsh geese, but smaller. At first they appear as excrescences on fir-logs carried down upon the waters. Then they hang by their beaks from what seems like seaweed clinging to the log, while their bodies, to allow for their more unimpeded development, are enclosed in shells. And so in the course of time, having put on a stout covering of feathers, they either slip into the water, or take themselves in flight to the freedom of the air. They take their food and nourishment from the juice of wood and water during their mysterious and remarkable generation. *I myself have seen many times and with my own eyes more than a thousand of these small bird-like creatures hanging from a single log upon the sea-shore.* They were in their shells and already formed. No eggs are laid as is usual as a result of mating. No bird ever sits upon eggs to hatch them and in no corner of the land will you see them breeding on building nests. Accordingly in some parts of Ireland bishops and religious men eat them whithout sin during a fasting time, regarding them as not being flesh, since they were not born of flesh".

puero q̄ alui egtantib; salutifa. rufq;
in hodiernū diē tā salix illa q̄ alie ex
ea ēca cimitiū tñsplantate more po
meri. salicis tñ alias p oīa tā foliis q̄



Giraldus Cambrensis.
Illustratie uit "*Topographia Hibernica*",
manuscript MS. Royal 13 B VIII, British Library.

Zouden die "eigen ogen" van chirurgijn en herbalist John GERARD wellicht door de oogkassen van aartsdiaken GERALD hebben gekeken? In ieder geval moet Gerald betrouwbaar geacht worden. Hij was immers een hoge geestelijke, wiens vroomheid buiten kijf is. Zijn boven geciteerde ooggetuigenverslag wordt dan ook prompt gevolgd door een preek, met een vermanend opgeheven vingertje naar ... de Joden! "Pause, unhappy Jew! Pause - even if it be late (...) Blush! wretch. Blush!" Die joden, die de onbevleete ontvangenis ontkenden, omdat het biologisch onmogelijk zou zijn dat iemand slechts één ouder zou hebben, moesten maar eens letten op de barnacles, die ganzen die helemaal zonder ouders aan de ganzenboom groeiden!

De Middeleeuwse Joden tilden overigens ook zwaar aan het probleem of die brandgans nu vlees was of vis. Rabbi ISAAC van CORBEIL koos de veiligste weg: in 1277 verbood hij het eten van deze dieren aan zijn geloofsgenoten, omdat hij besliste dat zij geen van beide waren. Ook de Christenen waren het daar niet allemaal over eens. Paus Innocentius III - de geweldenaar die koning Jan-zonder-land en Keizer Otto IV in de ban deed, Frederik II de Grote maaakte, en vervolgens trachtte te breken, die de afschuwelijke kruistocht tegen de Katharen en Albigenzen in de Languedoc organiseerde en zegende, en die verantwoordelijk was voor de vierde kruistocht waarbij Constantinopel werd geplunderd en op de puinhopen het Latijnse Keizerrijk werd opgericht - paus Innocentius III, op het Lateraans Concilie van 1215, stelde zich voorzichtig op en verbood het eten van brandgans in de vastentijd. Maar latere pausen, zoals Pius II, kwamen hierop weer terug.

De overtuiging dat de "barnacle goose" uit de "barnacle shell-fish" (3) voortkomt (met variaties: in de Nederlanden was het de eidereend die zich uit de eendenmossel ontwikkelde) is ongetwijfeld veel ouder dan Geraldus Cambrensis. Een raadsel in het Exeter raadselboek (ca. 980) verwijst hiernaar, zoals algemeen wordt aangenomen (4), terwijl de woorden voor de gans en voor het schaaldier homonymen zijn in het Iers en het Gaelic (*guirann*) en in het Welsh (*gwyrrann*), reeds lang voor het jaar 1000.

ALBERTUS MAGNUS en ROGER BACON weerlegden de beweerde verwantschap en maakten deze belachelijk, maar nog in 1677 presenteerde Sir Robert MORAY voor de Royal Society een verhandeling "A Relation concerning Barnacles", gepubliceerd in de *Philosophical Transactions*, Januari/Februari 1678, waarin hij de oude beweringen wetenschappelijk meende te onderbouwen.

Wij twintigste-eeuwers, losgeraakt van de vasten, lopen niet meer zo warm voor de vraag naar het vis-of-vlees karakter van brandgans en eidereenden (hoewel, het groeiende aantal vegetariërs onder ons moet er toch maar eens over mediteren dat deze natuurproducten aan bomen groeien...). En die andere vraag, of "Polynomial-time Algorithms etc." informatica is of wiskunde, lopen we daar dan warm voor? Natuurlijk niet! Zolang het voedzaam is en goed te verteren, zo lang het smaakt naar meer, zolang willen we allemaal toch niets liever dan dat de ganzenboom nog vele vruchten werpen zal?

AANTEKENINGEN

- (1) Het woord "barnacle" betekende oorspronkelijk zowel de "barnacle goose", brandgans, Anser leucopsis, als de "barnacle shell-fish", eendenmossel, Lepas anatifera. De eendenmossel werd - zoals de Nederlandse naam aangeeft - beschouwd als een mossel, een schelpdier, een "shell-fish"; vandaar dat ook de gans tot de vissen werd gerekend. Charles DARWIN was er erg trots op dat hij in de eendenmossel een kreeftachtige herkende (terwijl de grote CUVIER die nog bij de weekdieren onderbracht). De eendenmossel wordt ingedeeld bij de Cirripedia of Rankpootkreeften, evenals bv. de zeepok.

- (2) Giraldus Cambrensis (c.1146-1223) kwam uit een illustere familie. Zijn oom (moeder's broeder) David FitzGerald was bisschop van St. David's, de positie waarnaar Gerald zijn lange leven vurig maar zonder succes streefde. Zijn moeder, Angharad, was een bijzonder intelligente vrouw, kleindochter van Rhys ap Tewdwr, prins van Zuid-Wales. Zijn vader, Willem van Barry, was een normandisch edelman; ook zijn oudere broers waren als ridders befaamd.

Zo vurig begeerde Gerald de positie die zijn oom bekleedde, dat hij andere benoemingen, zoals die tot bisschop van Bangor, of tot bisschop van Llandaff, en twee dergelijke aanbiedingen in Ierland, weigerde.

In zijn jonge jaren was Gerald van Wales een lange en knappe jongeman. Zoals hij zelf schrijft: "Eram autem tunc adolescens, statua procerus, facie quoque fragilique ac momentaneo naturae bono formae nitore praeclarus...." [Zie Lewis THORPE, inleiding tot "Gerald of Wales - The Journey through Wales and The Description of Wales", Penguin Books Ltd, Harmondsworth, Middlesex, 1978.]

- (3) De ethymologie van "barnacle" is onzeker. Samuel JOHNSON, in zijn "A Dictionary of the English Language" (London 1755) presenteert een afleiding die aansluit bij de oude verhalen, maar zoals zovele van JOHNSON's voorstellen is deze ethymologie onhoudbaar.

BA'RNACLE. *n. f.* [probably of bearn, Sax. a child, and aac, Sax. an oak.]

1. A bird like a goose, fabulously supposed to grow on trees.
Surely it is beyond even an atheist's credulity and impudence, to affirm that the first men might grow upon trees, as the story goes about *barnacles*; or perhaps might be the lice of some vast prodigious animals, whose species is now extinct.
Bentley's Sermons.

And from the most refin'd of faints,

As naturally grow miscreants,

As *barnacles* turn folan geese

In th' islands of the Orcades.

Hudibras, p. iii. c. ii.

2. An instrument made commonly of iron for the use of farriers, to hold a horse by the nose, to hinder him from struggling when any incision is made.
Farrier's Dict.

Oude vormen van "barnacle" zijn bernickle, berneka, barneca (GERVASE van Tilbury, c.1211). Het grote Oxford Dictionary geeft aarzeland als mogelijke afleiding bare-neck (vgl. ook de uit het engels overgenomen vormen bernaque (oudfrans), bernaca of barnaces (middeleeuws latijn), bernachi (spaans).

Max MULLER suggereert een assimilatie tussen bernicula < hibernicula, [gans] van Hibernica (Ierland), en bernacula < pernacula < perna, een soort schelpdier. Anderen wijzen op gaelic "bairneach" en welsh "brenig" met de betekenis "schaalhoorn". Een bezwaar tegen dit laatste voorstel is dat oorspronkelijk met barnacle bepaald de brandgans en niet de eendenmossel werd aangeduid (vg. NECKHAM 1227: "De ave que vulgo dicitur bernekke", of TREVISA 1387: "per beep bernakles foules licke to wyld gees; kynde bryngē hem forþ wonderliche out of trees").

- (4) De Codex Exoniensis (Exeter Book), vermoedelijk door een kopiïst afgeschreven in het laatste kwart van de tiende eeuw, is waarschijnlijk hetzelfde als het "mycel englisc boc be gehwylcum þingum on leoðwisan geworht" vermeld in de nalatenschap van bisschop Leofric van Exeter († 1072). Het tiende raadsel luidt, in de vertaling van Kevin CROSSLEY-HOLLAND:

My beak was bound and I was immersed,
the current swept round me as I lay covered
by mountain streams; I matured in the sea,
above the milling waves, my body
locked to a stray, floating spar.
When, in black garments, I left the waves
and the wood, I was full of life;
some of my clothing was white
when the tides of air lifted me,
the wind from the wave, then carried me far
over the seal's bath. Say what I am called.

Arjen,

Reeds van zeer weleer, een ogenlust

Je te zien spelend leren en lerend spelen in het pure,

Een UvA-assistent van groot allure.

Niets stond in de weg, dat ook deze

Lenstra

Erin zou slagen

Na een paar jaar een dissertatie aan te dragen.

Stug doorzettend, op niveau opererend,

Trouw wiskunde en informatica gezamenlijk vererend.

Rem op VLSI, maar toch een werk dat kreeg het fiat

Amice, proficiat!

FJMB

Een tegenvoorbeeld voor de Church-Rosser eigenschap van proces polynomen

(opgedragen aan Arjen Lenstra ter gelegenheid van zijn promotie)

door Jan Bergstra en Jan Willem Klop

In deze bijdrage beschrijven we een (voor ons) verrassend feit gelegen in het gebied waar abstracte data typen en term herschrijfsystemen overlappen. Meer specifiek betreft het het aan een proces algebra geassocieerde herschrijfsysteem, waarbij de proces algebra een 'fixed point algebra' is verkregen door een formele uitbreiding met elementen die aan zekere recursievergelijkingen voldoen; analoog aan bijvoorbeeld de constructie van $\mathbb{Q}[X]/X^2-2$.

Het volgende axiomastelsel PA beschrijft een simpele vorm van proces co-operatie: namelijk 'merge' of 'interleaving' ($\parallel$).

PA

$x + y = y + x$	A1
$x + (y + z) = (x + y) + z$	A2
$x + x = x$	A3
$(x + y) \cdot z = x \cdot z + y \cdot z$	A4
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	A5
$x \parallel y = x \parallel y + y \parallel x$	M1
$a \parallel x = a \cdot x$	M2
$ax \parallel y = a(x \parallel y)$	M3
$(x + y) \parallel z = x \parallel z + y \parallel z$	M4

(Hierbij zijn $a, b, \dots$ atomaire acties en x, y, z zijn variabelen.)

Zo is $a \cdot (b+c) \cdot a \cdot a \cdot a$, of simpel $a(b+c)a^3$, het proces dat als eerste stap 'a' doet, dan kiest of het 'b' of 'c' doet om te besluiten met drie a-stappen. Dit proces is gelijk aan $a(ba^3+ca^3)$. De 'merge' van proces a^2 met proces b zal opleveren $aa \parallel b = aa \parallel b + b \parallel aa = a(a \parallel b) + baa = a(a \parallel b + b \parallel a) + baa = a(ab+ba) + baa$.

We zijn nu geïnteresseerd in het adjungeren van formele processen aan algebras die aan PA voldoen. Bijvoorbeeld, de oplossing X van $X = aX$ stelt voor het proces $aaa \dots$. In het algemeen kan men een 'fixed point' X_0 definiëren door een stelsel van de vorm

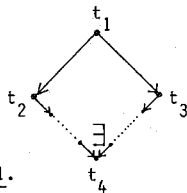
$$E_X: \begin{cases} X_0 = t_0(X_0, \dots, X_n) \\ \vdots \\ X_n = t_n(X_0, \dots, X_n) \end{cases}$$

waarbij de t_i ($i=0, \dots, n$) termen zijn over de signatuur van PA en variabelen uit $X = \{X_0, \dots, X_n\}$ kunnen bevatten.

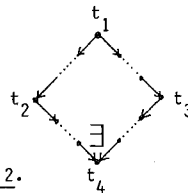
Met enige goede wil en voor deze gelegenheid, kunnen we termen over $PA + E_X$ 'proces polynomen' noemen. (Bijvoorbeeld, $aX_0^3 + bX_0^2 + cX_0 + d$ is een dergelijke term.) Jammer genoeg betreft ons probleem niet het factoriseren van dergelijke polynomen, maar het reduceren ervan, als volgt.

Bij een uitbreiding $PA + E_X$ hoort op natuurlijke wijze een term herschrijfsysteem, namelijk door de '=' te vervangen door '+' behalve in de regels A1, A2, A5 (associativiteit en commutativiteit). (In feite werken we dan met reducties van de equivalentieklassen gegenereerd door deze axioma's.)

Het is niet moeilijk na te gaan dat de reductie '+' voldoet aan de *zwakke confluentie eigenschap* (of zwakke Church-Rosser eigenschap) gesuggereerd in Figuur 1; i.e. elke twee divergente stappen vanuit term t_1 kan men (eventueel in meer stappen) weer doen convergeren. Voor verdere theorie zou het nu zeer plezierig zijn als ook *volledige confluentie* (of Church-Rosser eigenschap) zou gelden, zoals in Figuur 2.



Figuur 1.



Figuur 2.

Merkwaardig genoeg, en tegen onze verwachting in, is het mogelijk een stelsel E te geven zodanig dat er een term t_1 is die gereduceerd kan worden naar t_2 , t_3 zonder gemeenschappelijk reduct t_4 . Namelijk:

$$E = \begin{cases} X \rightarrow a + aX \\ Y \rightarrow XY \end{cases}$$

(Hierbij zijn X,Y proces namen voor de specifieke oplossingen van E, niet te verwarren met x,y,z die variëren over alle processen.)

STELLING. Het reductiesysteem bij $PA + E$ is niet confluent.

BEWIJS: $Y \rightarrow XY \rightarrow (a + aX)Y \rightarrow aY + aXY \rightarrow aXY + aXY \rightarrow aXY$.

Dus, met de notatie $t \twoheadrightarrow t'$ voor $t \rightarrow \dots \rightarrow t'$, hebben we

- (1) $Y \twoheadrightarrow aXY$
- (2) $XY \twoheadrightarrow aXY$
- (3) $XY \twoheadrightarrow XaXY$ (uit (1)).

Zou nu $PA + E$ confluent zijn, dan moeten de reducten $t_2 = aXY$ en $t_3 = XaXY$ van $t_1 = XY$ weer een gemeenschappelijk reduct hebben (notatie: $aXY + XaXY$).

Echter, gelet op de reductie

$$XaXY \twoheadrightarrow aaXY + aXaXY$$

kunnen we nu stellen:

$$\begin{aligned} aXY + XaXY &\Leftrightarrow \\ aaXY + aXaXY &\twoheadrightarrow aPQ \text{ voor zekere } P, Q \Leftrightarrow \\ aaXY + aXaXY &\Leftrightarrow \\ aXY + XaXY. \end{aligned}$$

Maar dit laatste is juist het oorspronkelijke probleem!

Natuurlijk zou het nog wat meer vergen om dit bewijs voor 100% waterdicht te maken, maar dat laten we over

aan Arjen.

A COLORFUL PROOF OF AN OBVIOUS THEOREM

Hans Bodlaender & Jan van Leeuwen

Department of Computer Science, University of Utrecht
P.O. Box 80.012, 3508 TA Utrecht, the Netherlands

Abstract. We provide a proof of the following "folk" theorem in (three-dimensional) VLSI-theory: given a $v \times w \times 1$ rectilinear block of the three-dimensional grid ($v \leq w \leq 1$), its minimum bisection width is at least vw .

Keywords and phrases: VLSI-theory, minimum bisection width, A.K. Lenstra.

1. Introduction. A VLSI-circuit can be defined as a finite graph of nodes (gates) and edges (wires) that satisfy certain additional constraints. Thompson's model of a 2-layered VLSI-chip assumes that circuits are laid out in a 2-dimensional grid, with nodes occupying single cells of the grid and wires running horizontally or vertically (ninety-degree bends allowed). At most two wires can cross in a single cell, and only "orthogonal" crossings are allowed. For details see Thompson [2]. The model is easily extended for multilayered ("three-dimensional") VLSI-chips, leading to embeddings in the 3-dimensional grid. For details see e.g. Rosenberg [1].

Lowerbound proofs for VLSI-circuits typically make use of the following argument. Consider a cutset D consisting of (say) d edges, and let it dissect the circuit in two parts Y and B . {This means that every path between a Y -node and a B -node must contain an edge in D .} If one can determine or estimate the information transfer I (in bits) required for Y and B in the course of the computation, then under reasonable assumptions I/d will be a lowerbound on the computation time of the circuit. Traditionally one tries to find a cutset of a smallest possible number of edges that dissects the circuit in two balanced halves.

Definition. Let $G = \langle V, E \rangle$ be a finite (undirected) graph and $S \subseteq V$.

We say that $D \subseteq E$ bisects S in G if there are $Y, B \subseteq V$ such that

(i) $Y \cup B = S$ and $Y \cap B = \emptyset$,

(ii) $|Y| \leq |B| \leq |Y| + 1$,

(iii) every path between a Y -node and a B -node contains an edge of D .

The minimum bisection width of S in G , notation: $mbw(G, S)$, is the number of edges in the smallest D that bisects S in G .

If $S \equiv V$ we speak of the minimum bisection width of G , notation:

$mbw(G)$. The nodes of Y will be called "yellow" and of B "blue".

Necessarily $|Y| = \lfloor \frac{1}{2}s \rfloor$ and $|B| = \lceil \frac{1}{2}s \rceil$, with $s = |S|$.

Thompson [2], p.52 notes that the mbw of a $w \times w$ square block of the 2-dimensional grid is $w + (w \bmod 2)$ but gives no proof of this fact. As the result is intuitively obvious it has become a folk theorem in this part of VLSI-theory. Yet we feel that a rigorous proof is required. In this note we show the following more general result. Let G be a $v \times w \times 1$ rectilinear block of the 3-dimensional grid with $v \leq w \leq 1$, then $mbw(G) \geq vw$.

Definition. $G(v, w, 1) = \langle V, E \rangle$ is the graph $\subseteq \mathbb{Z}^3$ with node-set $V = \{(i, j, k) \mid 1 \leq i \leq v \text{ \& } 1 \leq j \leq w \text{ \& } 1 \leq k \leq 1\}$ and an edge between every two nodes that differ by 1 in exactly one coordinate.

2. The folk theorem. Consider a minimum bisection of $G(v, w, 1)$ into parts Y and B , using a set $D \subseteq E$ of d edges ($d \equiv$ the minimum bisection width). Let nodes in Y and B be called "yellow" and "blue" respectively. An edge will be called yellow or blue if it connects two yellow or two blue nodes, respectively. An edge will be called "green" if it connects a yellow node and a blue node. {By definition every path from a Y -node to a B -node must contain a green edge. It also follows that all green edges belong to D .} We will estimate the number of green edges in $G(v, w, 1)$. View G as a collection of v "planes" of size $w \times 1$, with $w \leq 1$. {Thus a plane is a $w \times 1$ rectangle of the two-dimensional grid.}

Lemma 2.1. Suppose a plane contains at least x nodes from Y and x nodes from B . Then it contains $\geq \min \{w, 2\sqrt{x}\}$ green edges.

Proof.

Let the plane be P . One can view P as a collection of w or 1 "parallel" lines. A line will be called yellow or blue if it contains yellow or blue edges only. A line will be called green if it contains at least one green edge. Consider the lines in one direction. If all lines are green, then we have at least as many green edges and the estimate of $\min \{w, 1\} = w$ follows. Suppose in both directions there is at least one yellow or blue line. Because the lines intersect they must both be yellow or both be blue. Assume they are both yellow (without loss of generality), which implies that there can be no blue lines. It follows that every blue node must lie on the intersection of two green lines. Because there are at least x blue nodes there are at least as many intersections of green lines. Suppose there are x_1 green lines in one direction and x_2 in the other. The number of green edges will be $\geq x_1 + x_2$, whereas for the number of intersections $x_1 x_2 \geq x$. Under the latter constraint $x_1 + x_2 \geq 2\sqrt{x}$. $\square$

Proposition 2.2. The minimum bisection width of a $w \times l$ rectilinear block of the two-dimensional grid with $w \leq l$ is $w + (l \bmod 2)$, for $w > 1$.

Proof.

Let the block be G . Clearly G can be bisected by a "vertical" cut using a number of edges as stated. Only when l is odd there will be one "zig zag" in the vertical cut, accounting for the one extra cutting edge. For a lowerbound apply lemma 2.1. with $x = \lfloor \frac{1}{2}wl \rfloor$. When l is even (hence $l \geq 2$) we have $x = \frac{1}{2}l.w$ and the number of green edges is bounded by $\min \{w, 2\sqrt{\frac{1}{2}lw}\} = w$, using that $l \geq w$. Thus the upper- and lower-bound on the mbw match. Let l be odd. The same argument would still result in a lowerbound of w , although $\lceil 2\sqrt{x} \rceil = \lceil 2\sqrt{\lfloor \frac{1}{2}wl \rfloor} \rceil \geq w+1$ in this case. {We exclude the degenerate case that w equals 1.} Consider the first part of the proof of lemma 2.1. again. Distinguish the following cases:

(i) all w lines in one direction are green. This leads to at least w green edges in (say) the horizontal direction. The l vertical lines

cannot be all yellow or blue, or else we would not have a proper bisection (l odd). Thus at least one vertical line is green, and the estimate of the number of green edges becomes $w + 1$.

(ii) all l lines in the other direction are green. This leads to at least 1 green lines in the vertical direction. Either w is even and the estimate becomes $l \geq w + 1$, or w is odd and the same argument as before shows that there must be at least one extra green line in the horizontal direction and (hence) at least $l + 1$ green edges total. Thus at least $w + 1$ green edges are required when l is odd, and again the upper- and lowerbound on the mbw match. $\square$

Observe that proposition 2.2. proves Thompson's remark that the minimum bisection width of a $w \times w$ block is $w + (w \bmod 2)$ ([2], p.52).

Theorem 2.3. The minimum bisection width of a $v \times w \times l$ rectilinear block of the three-dimensional grid with $v \leq w \leq l$ is at least vw .

Proof.

View $G(v, w, l)$ as a stack of v planes $P_1, \dots, P_v$ of size $w \times l$ each. Let P_i ($1 \leq i \leq v$) contain y_i yellow nodes and hence $wl - y_i$ blue nodes. Let t be a threshold value with $0 < t \leq wl$, t not necessarily integer. We will fix t at $t = \frac{1}{2}w^2$. Divide the planes into the following three categories:

$$X_1 = \{P_i \mid 0 \leq y_i \leq t\}$$

$$X_2 = \{P_i \mid t < y_i < wl - t\}$$

$$X_3 = \{P_i \mid wl - t \leq y_i \leq wl\}$$

and let $x_i = |X_i|$ ($1 \leq i \leq 3$). Clearly $x_1 + x_2 + x_3 = v$. Also note that the division of the planes into categories based on the number of blue nodes is symmetric to the current one. Define $\bar{\alpha} = \min \{y_i \mid P_i \in X_1\}$ and $\bar{\alpha} = \max \{y_i \mid P_i \in X_1\}$, $\bar{\beta} = \min \{y_i \mid P_i \in X_2\}$ and $\bar{\beta} = \max \{y_i \mid P_i \in X_2\}$, and $\bar{\gamma} = \min \{y_i \mid P_i \in X_3\}$ and $\bar{\gamma} = \max \{y_i \mid P_i \in X_3\}$. We estimate the number of green edges in the graph. Consider the planes in X_1, X_2 , and X_3 .

Planes in X_1 :

There are at least $\bar{\alpha}$ yellow nodes and $wl - \bar{\alpha}$ blue nodes in every plane in X_1 . Because $\bar{\alpha}, \bar{\alpha} \leq t$ and $t \leq \frac{1}{2}wl$ it follows that every plane contains at least $\bar{\alpha}$ yellow nodes and $\bar{\alpha}$ blue nodes, and lemma 2.1. can be applied. This leads to an estimate of $\min \{w, 2\sqrt{\bar{\alpha}}\} = 2\sqrt{\bar{\alpha}}$ green edges in every plane of X_1 (using that $2\sqrt{\bar{\alpha}} \leq 2\sqrt{t} = w$).

Planes in X_2 :

By their very definition planes in X_2 contain at least t yellow nodes and t blue nodes each. By lemma 2.1. it follows that every plane in X_2 contains at least $\min \{w, 2\sqrt{t}\} = w$ green edges.

Planes in X_3 :

There are at least $\bar{y}$ yellow nodes and $w_1 - \bar{y}$ blue nodes in every plane of X_3 , hence at least $w_1 - \bar{y}$ nodes of each kind. By lemma 2.1. it follows that every plane in X_3 contains at least $\min \{w, 2\sqrt{w_1 - \bar{y}}\} = 2\sqrt{w_1 - \bar{y}}$ green edges (using that $w_1 - \bar{y} \leq t = \frac{1}{4}w^2$).

The remainder of the argument is tedious. If $x_1 = x_3 = 0$ then $x_2 = v$ and the bound of vw green edges follows (because the planes in X_2 contribute w edges each). Thus we may assume that $x_1 \neq 0$ or $x_3 \neq 0$, and without loss of generality we can take $x_1 \neq 0$. We distinguish the following three cases.

Case I: $x_1 \geq \frac{1}{2}w$.

If all planes would belong to X_1 (i.e., $x_1 = v$) then the number of yellow nodes would be bounded by $\frac{1}{2}vw^2$ and be less than $|Y| = \lfloor \frac{1}{2}vw \rfloor$, a contradiction. Thus $x_1 < v$, and we can define $\bar{\delta} = \max \{y_i | P_i \in X_2 \cup X_3\}$ ($\neq 0$). By slightly extending the argument above, a plane $P_i \in X_1$ contains at least $2\sqrt{y_i}$ green edges. Because $y_i \leq \frac{1}{4}w^2$ we can estimate this at $\frac{4}{w}y_i$ green edges per plane. Considering the w_1 lines perpendicular to the planes it can be noted that at least $\bar{\delta} - \bar{\alpha}$ must be green and thus account for as many additional green edges. Now let $Y_1 = \sum_{P_i \in X_1} y_i$, $Y_2 = \sum_{P_i \in X_2} y_i$, and $Y_3 = \sum_{P_i \in X_3} y_i$, and observe that $\bar{\delta} \geq \frac{(Y_2 + Y_3)}{v - x_1} \geq \frac{2}{w} (Y_2 + Y_3)$ by using the assumed bound on x_1 . The total

number of green edges can be estimated at:

$$\begin{aligned} \sum_{P_i \in X_1} \frac{4}{w} y_i + \bar{\delta} - \bar{\alpha} &\geq \frac{4}{w} Y_1 + \frac{2}{w} (Y_2 + Y_3) - \bar{\alpha} = \\ &= \frac{2}{w} (Y_1 + Y_2 + Y_3) + \frac{2}{w} Y_1 - \bar{\alpha} = \frac{2}{w} \lfloor \frac{1}{2}vw \rfloor + \frac{2}{w} Y_1 - \bar{\alpha}. \end{aligned}$$

Note that $\frac{2}{w} \lfloor \frac{1}{2}vw \rfloor \geq v_1 - \frac{1}{w}$, and that $\frac{2}{w} Y_1 - \bar{\alpha} \geq \frac{2}{w} x_1 \bar{\alpha} - \bar{\alpha} \geq 0$.

Thus the bound becomes v_1 ($\geq vw$) green edges, using that the bound is integer.

Case II: $x_1 < \frac{1}{2}w$ (but $x_1 \neq 0$) and $x_3 = 0$.

As before it can be argued that $x_1 < v$ and (hence) that $x_2 > 0$. The planes of X_1 contain at least $2\sqrt{\bar{\alpha}} \geq \frac{4-\bar{\alpha}}{w}$ green edges each, and the planes of X_2 at least w green edges each. The lines perpendicular to the planes account for an additional $\bar{\beta} - \bar{\alpha}$ green edges. Observe that

$\bar{\beta} \geq \frac{1}{v} \lfloor \frac{1}{2}vw \rfloor \geq \frac{1}{2}wl - \frac{1}{2v}$ and (hence) that $\bar{\beta} \geq \frac{1}{2}wl$. {Clearly we can exclude the case $v = 1$.} The number of green edges can be estimated at

$$\begin{aligned} \frac{4-\alpha}{w}x_1 + x_2w + \bar{\beta} - \bar{\alpha} &= x_1 \left(\frac{4-\alpha}{w} + \frac{\frac{1}{2}wl - \bar{\alpha}}{x_1} \right) + x_2w + \bar{\beta} - \frac{1}{2}wl \geq \\ &> x_1 \left(\frac{4-\alpha}{w} + 1 - \frac{2-\alpha}{w} \right) + x_2w + \bar{\beta} - \frac{1}{2}wl \geq \\ &\geq x_1 + x_2w \geq \\ &\geq vw \end{aligned}$$

(using that $x_1 + x_2 = v$).

Case III: $x_1 < \frac{1}{2}w$ (but $x_1 \neq 0$) and $x_3 \neq 0$.

The planes of X_1 contain at least $2\sqrt{\bar{\alpha}} \geq \frac{4-\alpha}{w}$ green edges each, the planes of X_2 at least w green edges each, and the planes of X_3 at least $2\sqrt{wl-\bar{\gamma}} \geq \frac{4}{w}(wl-\bar{\gamma}) = 4l - \frac{4\bar{\gamma}}{w}$ green edges each. The lines perpendicular to the planes account for an additional $\bar{\gamma} - \bar{\alpha}$ green edges. By symmetry we may assume that $x_3 < \frac{1}{2}w$. The number of green edges can be estimated as follows

$$\begin{aligned} \frac{4-\alpha}{w}x_1 + x_2w + x_3(4l - \frac{4\bar{\gamma}}{w}) + \bar{\gamma} - \bar{\alpha} &= \\ &= x_1 \left(\frac{4-\alpha}{w} + \frac{\frac{1}{2}wl - \bar{\alpha}}{x_1} \right) + x_2w + x_3 \left(4l - \frac{4\bar{\gamma}}{w} + \frac{\bar{\gamma} - \frac{1}{2}wl}{x_3} \right) \geq \\ &\geq x_1 \left(\frac{4-\alpha}{w} + 1 - \frac{2-\alpha}{w} \right) + x_2w + x_3 \left(4l - \frac{4\bar{\gamma}}{w} + \frac{2\bar{\gamma}}{w} - 1 \right) \geq \\ &\geq x_1 + x_2w + x_3(3l - \frac{2\bar{\gamma}}{w}) \geq \\ &\geq x_1 + x_2w + x_3 \geq \\ &\geq vw. \end{aligned}$$

It follows that in all cases a lowerbound of vw green edges can be shown and thus that the minimum bisection width of $G(v,w,l)$ is at least vw ($v \leq w \leq l$). $\square$

It follows in particular that for l even the minimum bisection width of a $v \times w \times l$ block ($v \leq w \leq l$) is precisely vw .

3. References.

- [1] Rosenberg, A.L., Three-dimensional VLSI: a case study, J. ACM 30 (1983) 397 - 416.
- [2] Thompson, C.D., A complexity theory for VLSI, Ph.D. Thesis, Techn. Rep. CMU-CS-80-140, Dept. of Computer Science, Carnegie-Mellon University, Pittsburgh, 1980.

DENKEND AAN ARJEN

Wanneer ik aan Arjen denk, komen meteen zijn ogen in mijn gedachten.
Vanaf de eerste keer dat ik hem ontmoette, werd ik daardoor getroffen.

Zelden ontmoet je nog medemensen met zulk een onbevangen blik.
Het is net of er kleine lampjes zitten die schitteren.

Toch heeft het niet te maken - wat vaak daarmee in verband gebracht wordt - met onnozelheid. Integendeel, Arjen verbaast mij juist door zijn "weten", voorzover zo iets mogelijk is, en dat is voor een mathematicus iets bijzonders. Dat is geen verwijt aan andere mathematici. Neen, verscheidenheid moet er zijn, het is zelfs vaak ontroerend.

Arjen, gelukgewenst en het ga je verder ook nog goed in het leven.

(Joep Boesewinkel)

Wanneer ik aan Arjen denk
zie ik slechts zijn ogen
alsof ze nimmer zijn bedrogen
en zulks is een groot geschenk.

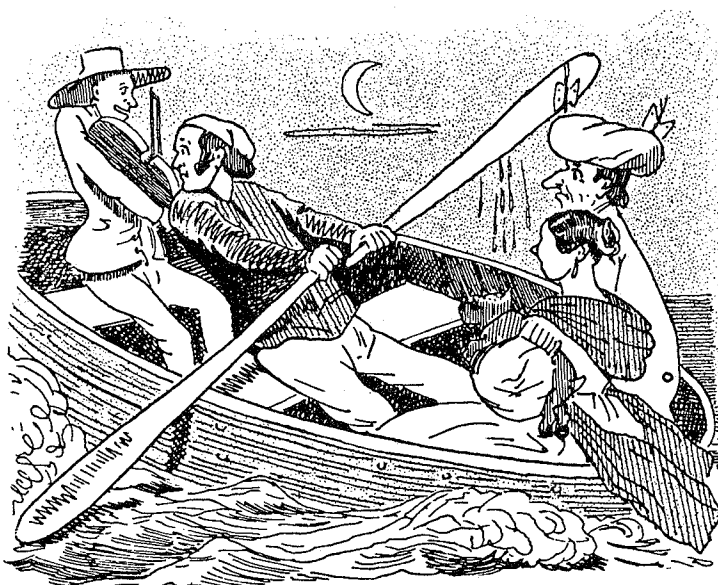
Het zijn lampjes in duisterheid
die fonkelend je ontmoeten
je lichtend groeten
in onbevangenheid gevlijd.

Let wel, hij leeft al "wetend",
meestal vreemd aan mathematici
die zo verwant zijn aan flegmatici,
het levend leven vaak vergetend.

Maar, dergelijk goed is dan slechts goed
wanneer het tussen anderen gedijt
zich van andere 'wijzen' onderscheidt,
het diverse ... dat ontroert.

(berijming Monique Greveling)

HOU DAT MENEER LENSTRA DER VEUR DE ZOVEULSTE MOAL UUTBUULT



"Dizze raais komt 't veur mekoar,
Pefester ligt op ain oor.
Niks meer zeggen, gain geluud
en din bulen wie der uut!"

Gaauw in 't bootje, hier vandoan!
Speulman wil vot fiedeln goan.
Lenstra het 't slim benaauwd,
vint 't moar zunegaan vertraauwd.

AIN GOUDE RAAIZE
NOAR AMMERIKOA !

Bettie en Cees.

Zo af en toe gebeurt er wat
In Amsterdam die grote stad,
Wel niet altijd even mooi,
Want soms is het er een zooi,
Maar er wonen ook studieballen,
Die met gemak door examens rollen!
Ook Arjen is één van dat soort
Dat bij de uitblinkers behoort.
Dus ging hij als Lenstra-spruit
Wetenschap'lijk goed vooruit,
Waardoor aldus ten langen leste
Een doktorsgraad hem restte.
Toch waren er ook andere zaken
Die naast studie hem konden vermaken:
Daartoe behoorden opera, muziek en lekker eten,
Waarbij de pudding niet werd vergeten!
Zelf pudding maken was voor hem geen toer,
Maar vormen bezat nòch hij, nòch zijn broer!
Dit feit werd in Breda vernomen,
Zodat die toch in Amsterdam zijn gekomen;
Daarom vroegen de Lenstra-heren
De Bredase familie te dineren.
Natuurlijk moest het slot van 't festijn
De zelfgemaakte pudding zijn.
De hele maaltijd al met al
Was een goed geslaagd geval,
Waaruit valt te concluderen,
Dat Arjen meer kan dan goed leren!
Verder is de kans niet klein
Dat hij eens prof zal kunnen zijn,
Waarmee hij kan bereiken
Dat prof. en doctor voor zijn naam mogen prijken.

De drie van Breda

Hommage aan de Friese doorloper

Het is algemeen bekend dat Arjen goed in wiskunde is. Maar slechts weinigen weten dat Arjen ook op sportief gebied uitstekend presteert. Daarvan willen wij hier verslag doen.

In het winterseizoen 79/80 uitte Arjen spontaan de wens om eens een avondje mee te gaan met een groepje enthousiaste schaatsers. Hij zorgde zelf voor de uitrusting: een warme muts met pompoen, een lange zwarte jas en een sjaal van enkele meters lang. De schaatsen, houten Friese doorlopers, leende hij van de vader van Liesbeth. Na het eerste wankel begin raakte Arjen al snel gehecht aan de vaste schaatsavonden op woensdag.

Deze begonnen altijd met een maaltijd van stampot in een Diemense studentenkeuken. Na de afwas fietsten de schaatsers gezamenlijk door de bittere kou naar de Jaap Edenbaan. Daar werden op een wiebelig bankje de schaatsen ondergebonden. Dan het ijs op: zo snel mogelijk vooruit en zo min mogelijk onderuit. De krabbelaars, en Arjen, bewogen zich langs de buitenkant van de baan. Arjen had daar steun en gezelschap van andere beginnelingen als Barbara, Helie, Liesbeth en Marian. Aan de binnenkant van de baan flitsten de ervaren schaatsers langs: Jos Jansen, Peter Jensen, Ans Reuvers en Ben Knip. Daar tussenin schaatsten de middenmoters als Rudolf, Monique Abels, Jan Lankelma, Jan Hogervorst en Karin Stevens.

Natuurlijk werd er regelmatig gerust en bijgepraat op een bankje langs de baan. De ervaren rijders gaven daar de beginnelingen adviezen over zijwaarts afzetten en diep gebogen knieën en ruggen.

Wanneer iedereen koude tenen had was het tijd voor een beker warme chocolademelk (met of zonder jenever) in de kantine. Daarna ging iedereen nog even het ijs op voor de laatste rondjes en de laatste botsingen en valpartijen. Na sluitingstijd fietste men naar de bar in Diemen om de avond

te besluiten met een glaasje berenburg.

Arjen maakte snelle vorderingen en stapte na een paar avonden van de Friese doorlopers (waar zouden die dingen gebleven zijn, heeft Arjen ze als souvenir boven zijn bed gehangen?) over op gehuurde ijshockeyschaatsen. Hij leerde van Rudolf de techniek van "pootje-over". Arjen schaatste zo goed, dat hij een bewonderaarster kreeg, een meisje van twaalf dat gezellig babbelend naast "die leuke lange meneer" schaatste.

Maar helaas, naarmate Arjens rondetijden korter werden, werden de dagen langer. Het voorjaar brak aan en de Eden-baan sloot. Voor zover wij weten betekende dit het einde van Arjens schaatscarrière.

Natuurlijk stellen wij ons de vraag waarom Arjen die winter zo enthousiast geschaatst heeft.

Had hij behoefte aan ontspanning na zijn zware taak als assistent bij het praktikum numerieke wiskunde?

Of probeerde hij te leven volgens het motto "mens sana in corpore sano"?

Misschien gebruikte hij het schaatsen wel als excuus om op een doordeweekse dag jenever en berenburg te drinken.

Of kroop toch zijn Friese bloed waar het niet gaan kon?

In dat geval kunnen wij Arjen aanraden zich deze zomer eens bezig te houden met polsstokspringen, zeilen of kaatsen.

Liesbeth Clason

Marian Belderok

Some problems for Arjen and others

by Henri COHEN

Problem 1. - Let $\lambda \geq 0$ be fixed and let D be the operator

$$D = \frac{d}{dx} + \lambda \left(\frac{d}{dx} \right)^3 .$$

Assume that f is a C^3 function on an open set containing an interval $[a, b]$ and that

$$f(a) = f(b) = 0 .$$

Is it true that there exists $c \in [a, b]$ such that $Df(c) = 0$? (the case $\lambda = 0$ is Rolle's theorem). If so, generalise to other differential operators.

Problem 2. - Assume the Riemann hypothesis and let

$$f_1(s) = (s-1) \zeta(s+1) + 2\pi \zeta(s-1)$$

$$f_2(s) = (s-1) \zeta(s+1) - 2\pi \zeta(s-1)$$

$$f_3(s) = s(s+1) \zeta(s+1) + 2\pi(s-2) \zeta(s-1)$$

$$f_4(s) = s(s+1) \zeta(s+1) - 2\pi(s-2) \zeta(s-1) .$$

Then f_1, f_2, f_3, f_4 have trivial zeros for $s = -1 - 2n$, ($n \geq 0$ for f_3 and f_4 , $n \geq 1$ for f_1 and f_2).

Is it true that apart from these zeros all the other zeros of the f_i are on the critical line $\text{Re } s = \frac{1}{2}$?

Problem 3. - (See Edwards, Riemann's zeta function, page 166). Denote by $0 \searrow 1$ a path of integration which is of slope -1 , crosses the real axis between 0 and 1 and directed from upper left to lower right. Set

$$f(s) = \int_{0 \searrow 1} \frac{e^{-i\pi x^2} x^{-s} dx}{e^{i\pi x} - e^{-i\pi x}}$$

Compute some zeros of f outside the trivial zeroes $-2n$, $n \geq 1$. Are they all in the half plane $\operatorname{Re} s \geq 1/2$?

Enkele van de bovengenoemde problemen hebben me erg geamuseerd. Ik zal ze je doorgeven, want ik denk dat ze jou ook zullen interesseren, evenals een paar van je collega's.

Een paar heb ik opgelost en andere niet... natuurlijk zeg ik niet welke.

Elk antwoord is welkom. En van harte gefeliciteerd !

Mathématiques et Informatique
L. A. au C.N.R.S. n° 226
Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX, France

ARJEN KLAAS IS ZIJN NAAM

Vorige maand werd mijn vrouw en mij schriftelijk aandacht gevraagd in een vertrouwelijke kwestie. Een gerucht dat onze neef Arjen zich binnenkort met de doctorshoed kan tooien. Welk gerucht wij reeds kenden.

Ten halve waren de beide ondertekenaars van dit schrijven bekend. Neef Hendrik W. Jr. De ander - Peter - veronderstelde ik, afgaande op de achternaam, zoon of neef te zijn van een man die ik nooit zal vergeten nadat ik hem jaren geleden een zich nieuw aandienend medisch specialisme op brilante wijze had horen verdedigen voor het daarvoor in aanmerking komend machtig en kritisch college, en met succes. Zo'n échte nieuwlichter geniet mijn respect.

Hendrik en Peter vroegen een bijdrage voor de publicatie van een vriendenalbum als tastbaar blijk van waardering voor de wetenschappelijke inspanningen van Arjen. Deze staan buiten kijf. Vandaar dit verzoek om een bijdrage welke volgens de initiatiefnemers bij ontbreken als een lacune door Arjen ervaren zou kunnen worden. Een dergelijke a.h.w. mentale, mankerend ruimtelijke bewustwording moet natuurlijk hoe dan ook voorkomen worden.

Vandaar de "van harte" gedane uitnodiging enig eigen geschrift af te staan om dit album volgens de toegewijde ondertekenaars tot een succes te maken. Suggesties worden hiertoe zelfs aangedragen. Een lyrisch lofdicht of ode op Arjen. Een wetenschappelijke beschouwing. Een kroniek of mémoires over of zonder Arjen zijn welkom. Zelfs kwinkslagen en mystificaties. Kortom een scala van schriftuurlijke mogelijkheden. Mits de eigenhandige pennevrucht, hoe en welke dan ook, aan enkele technische eisen tout court voldoet. A4-formaat papier met vrije marge onder, boven, links, rechts en blanco ommezijde.

Deze vertrouwelijke kwestie en vraag bereikte mij gekluisterd aan een ziekenhuisbed met een, versneld ademend door een dubbelzijdige longontsteking, zuurstofsonde in de neus. "En van harte beterschap" voegde Hendrik aan zijn vrijwel onleesbare handtekening meelevend toe. Sindsdien heb ik geen ogenblik slechter noch beter geslapen en ben toch - na een aanvankelijk onverwachte miskleun waardoor ik vier da-

gen

gen na een eerste ontslag opnieuw met bekwame spoed in het ziekenhuis belandde - voorspoedig ~~genezen~~. Die dokters moeten tegenwoordig wél in de gaten gehouden worden zou je haast zeggen.

Aan odes, kronieken, ~~mémoires~~ ben ik echter in mijn leven - 67 jaar zijnde - nimmer toegekomen. Evenmin waag ik mij - andere suggestie - aan mystificaties. Sinds ik namelijk als kleine jongen een voor mij volslagen mystificerend en onbegrijpelijk gebeuren voor de eerste keer onder toezicht van mijn moeder meemaakte, zijn bij mij uit dergelijke plechtige academische zittingen tot zekere hoogte a.h.w. haat/liefde- of beter afkeer/eerbiedgevoelens gegroeid. Ongetwijfeld later méde, eerlijk gezegd, in het besef dat ik zelf in eigen discipline nooit aan een dergelijke tópprestatie toe kom.

Al zal Arjen niet verwachten dat ik zijn studie onder mijn kussen heb liggen, ik heb zijn proefschrift wel degelijk trachten te lezen. Dit is mij dit keer minder dan ooit gelukt. Intussen is het familiehoekje in mijn boekenkast als vrucht van evenzovele wetenschappelijke inspanningen en reikend van pentateuch tot thans factorization of polynomials wél uitgedijd. Aan de vorige studie van neef Hans over pancreatic ribonuclease beeldde ik mij in nog enige affiniteit te hebben. Doch Arjens dissertatie deed de deur dicht, dát heeft hij mij wel ingepriemd. Tot zekere hoogte maakte zich na deze vergeefse poging een lijdzaamheid, gelatenheid of hoe dit innerlijk gebeuren ook nader psychisch omschreven kan worden, van mij meester. Eine sanfte Ruhe. Berusting. La résignation est le courage de l'impuissance, mag ik - sinds twee jaar als A.O.W.-er geleidelijk uit de circulatie genomen wordende - misschien opmerken.

Ook Fortran moge van mij gerust lang leven. Zelfs Arjens laatste stelling dat zijn 220-cijferig getal een priem is aanvaard ik zonder morren of tegensputteren. Nogal voor de hand liggend - alhoewel niet bewezen uiteraard - zou ik zeggen als 19 niet alleen aan het begin maar ook nog aan het eind van dit reüzencijfer staat.

Over reüzen gesproken! Maar dan, ook buiten de happy few van betrokkenen exacte wetenschappers, daadwerkelijk zicht- en tastbaar gemaakt! Even een kleine nevensprong. Reüzen. Een adembenemend schouwspel biedt Future World's Land pavillion van Epcot Centre in Florida.

Werkelijkheid

Werkelijkheid welke door mensenvernuft in planten- en dierenrijk mogelijk is geworden. Tomaten zo groot als bloemkolen, forellen als reuzenkarpers en "in de lucht hangende" slapplanten in drie weken volgroeid. Aan het einde van deze imposante show (waar met een klein bootje doorheen gevaren wordt) kan men een typisch Amrikaanse understatement lezen. "Only Robinson Crusoe could have done everything by Friday". Een troostende bemoediging voor de velen die dit ondermaanse gedurig verder trachten te doorgronden of ook dito ontmoediging.

Voor Arjens album blijft, wat mij althans betreft, volgens beide initiatiefnemers nog als bijdrage een wetenschappelijke beschouwing over. Ook zonder hierover in en later buiten het ziekenhuis lang te hebben liggen peinzen, heb ik deze suggestie wel overwogen. Mij daarbij afgevraagd wat ik met een dergelijk, in de loop der jaren verricht, veelal min of meer toegepast wetenschappelijk onderzoek van mijn hand in dit album mijn neef zou aandoen? Om enkele onderwerpen te noemen: Kala azár among Bushnegroes in Dutch Guiana. Medical audit en utilisation review in Nederlandse ziekenhuizen. Der Ärztliche Beitrag zum Krankenhausbau. Cuban - Netherlands Co-operation in the Public Health sector. Soins de de santé primaires aux îles des Comores. Comparison of hospital care in Finland, Scotland and the Netherlands. En onlangs: Programme d'urgence sanitaire à la capitale du Tchad.

Maar heb ik mijn neef in dit album - ter gelegenheid van zo'n uitzonderlijk hoogtepunt in zijn leven - niet iets meer te zeggen? Ik wil Arjen toch iets schrijven dat hem aan gaat, op hem zelf is afgestemd. Zo kwam ik na terugkeer en bekomen te zijn van het ziekenhuis waar morbide gedachten gemakkelijker overheersen, op de gedachte over Arjens beide voornamen te schrijven. Mijn onderwerp in zijn album is daarom: Arjen Klaas is zijn naam. Geen bijdrage. Nog minder een stamboomverhaal maar een klein document humain op Arjen toegesneden. Een personal story alshetware over zijn beide voornamen. Slechts met één beperking: voorzover deze voornamen in de familie van zijn moeder, mijn eigen en enige zuster, voor komen en waarover ik misschien iets wetenswaardigs voor Arjen kan vertellen.

Voor al in de laatste decennia blijft dikwijls, naar het klassieke spreekwoord

woord, in de schoot der goden verborgen hoe en waarom ouders tot de naamgeving van hun nieuw boreling komen. Dit moge met Arjen Klaas ook zo zijn. Van enige voorkeur bij het ouderpaar in kwestie voor de naam Arjen blijkt reeds bij de vorige zoon Johannes Arjen. Toch mogen in deze petite histoire - van weten is beslist geen sprake - enige veronderstellingen in dit opzicht door een naast familielid wellicht geuit worden. Ik mag dan - op eigen risico doch mijn zwager kennend - de veronderstelling uitspreken dat Arjens tweede voornaam met die van zijn moeder samenhangt. Dat zou mij allerminst verbazen omdat Arjens moeder als eerste voor-naam Klaasje heeft. En zeker weet ik van mijn ouders - in dit opzicht spraakzamer dan mijn zuster en zwager - dat mijn zuster vernoemd is naar haar vaders grootmoeder, wier huwelijkskennisgeving hieronder staat weergegeven.



Arjens overgrootmoeder Klaasje moet een bijzondere vrouw geweest zijn. Als kind jong verweesd werd zij - in 1843 geboren in Sint Jacoba Parochie boven Leeuwarden - opgevoed door haar moeders grootouders. Een gelovige en verstandige vrouw en een echte moeder voor haar kinderen - allen geboren op de boerderij in Pieterzijl bij Grijpskerk - waarvan zij er drie mocht zien opgroeien. Naar haar grootmoeder is Arjens moeder dus vernoemd, die ook haar kerkboek bezit. En als enige kleindochter destijds in de familie ook een poederdoos, tegelijk met een sigarettenkoker uit haar oorijzers later vervaardigd tot niet geringe ontsteltenis overigens, ondanks het geschenk aan hun dochter, van mijn ouders. Terwijl ik dit schrijf ligt de trouwbijbel van Arjens betovergroot-

ouders

ouders voor mij. Een stevige boerenbijbel voor dagelijks gebruik. Met twee degelijke knippen waarop resp. een zaaiende boer en een pap kokende boerin staan afgebeeld en met vier sterke scharnierplaten op elk waarvan een jong kind staat. Een echte boerenbijbel waarop de menselijke verlangens van die tijd rechttoe rechtaan staan weergegeven. Deze betovergrootvader van Arjen heette eveneens Arjen en door hem is de naam Arjen in de familie de Groot gekomen. Mijn 's vaders enig overlevende en oudere broer heette namelijk eveneens Arjen naar zijn moeders grootvader met de stevige bijbel. Deze broer van mijn vader heeft als 16-jarige boerenzoon het ouderlijk landbouwbedrijf de rug toegekeerd. In vier jaar tijds heeft hij het gymnasium doorlopen en in even vier jaar de medische studie volbracht. Hij is de laatste student van de vorige eeuw geweest die aan de Universiteit van Amsterdam tot arts werd beëdigd en tegelijk in de kortste studietijd. Na bestudering van Hahnemanns homeopathie in Berlijn - welke rond de laatste eeuwwisseling erg in de belangstelling stond - vestigde hij zich als huisarts in Utrecht waar hij in 1936 in de kracht van zijn leven is overleden. Een boeiende man evenals in ander opzicht - kleine zij-sprong - zijn zwager Bart de Lig, collega en geestverwant van de befaamde predikant in het Friese Nijebeets Domela Nieuwenhuis. Schrijver deze regelen heet met zijn tweede voornaam naar zijn oom.

Dit familieverhaal voor mijn neef Arjen besluit ik met nog iets over zijn grootvader van moederszijde Johannes te vertellen. Een levensblijve, krachtige man hoewel hij reeds jong menselijk leed en lijden aan den lijve heeft ervaren. Op 12-jarige leeftijd werd zijn linkeroog namelijk door een steen getroffen. Na jarenlange behandeling moest dit oog zes jaar later, om totale blindheid te voorkomen, worden weggenomen. Desondanks ook een sportsman. Voortreffelijk zeiler, liefst in de Friese boeier en een sterk schaatser

ser op doorlopers. Van jongsaf een ervaren ruiter. Wat goed te pas kwam toen hij tegen het einde van zijn studententijd vòòr de eerste wereldoorlog aan een archeologische expeditie van de universiteit van Göttingen van een half jaar door het tegenwoordige Jordanië en Israël deelnam. In de latere jaren van zijn leven - hij is 56 jaar geworden - reed hij paard met zijn enige dochter, Arjens moeder. Hij was een enige vader voor zijn drie kinderen. Een echte verhalenverteller. Zelfs mijn oudere broertje en ik zelf luisterden graag mee naar de grappige avonturen van Petronella van Constantinopel die hij elke avond opnieuw wist op te dissen voor zijn kleine dochtertje Ina - zijn oogappel - gezeten in de geliefde Amerikaanse schommelstoel met de kleine Ina op schoot, hangend aan zijn lippen.

Ook een voortreffelijk goochelaar wat hij in zijn Groningse studententijd geleerd had. Goochelen was het hoogtepunt van menig kinderverjaarspartijtje.

Een echte schaker net als zijn vrouw, zijn broer Arjen en de befaamde Oom Jan. In later jaren ook een goed bridgespeler.

Een doorvorser van talmoed, bijbel en koran welke hij dagelijks las.

De laatste zoals gebruikelijk hardop tot mijn constant verdriet omdat mijn kamer boven de studeerkamer lag. Ook een kenner van Dostojewski en van Rilke. Een ruim denkend man met ondanks zijn eenogigheid een verre blik. Een man door wie geloof en wetenschap met vanzelfsprekendheid en liefde gediend werden. Zoals hij zelf eens gezegd heeft: "Wij moeten onze talenten zo gebruiken dat het onze naaste gemakkelijk wordt gemaakt in God te geloven".

Pier Arjen de Groot Johanneszoon

PARALLELLISM IN ALGOL68: THE FIVE DINING PHILOSOPHERS REVISITED

by

T. J. Dekker *)

1. INTRODUCTION.

The purpose of this paper is to (dis-) prove the following proposition:

There exists parallelism in ALGOL68.

In section 2 we give a theoretical disproof, in section 3 an experimental disproof, and in section 4 an experimental proof of this proposition.

The theoretical disproof is based on quotations from the Revised Report on ALGOL68, Van Wijngaarden et al. (eds) [3].

The experiments are based on the well-known paradigm of the five dining philosophers, presented by Dijkstra [2].

The experiments were performed in the ALGOL68 - system on the CD CYBER 750 installation of SARA.

The experimental proof in section 4 uses a technique to obtain fairness, presented by Apt & Olderog [1].

ACKNOWLEDGEMENT.

The author is grateful to Dr Peter van Emde Boas and Drs Jan Kok for stimulating discussions and valuable suggestions which have influenced the final shape of this paper.

REFERENCES.

- [1] K. R. Apt & E.- R. Olderog, Proof rules dealing with fairness; Lecture Notes in Computer Science nr 131 (D. Kozen, ed.), p. 1 - 8
- [2] E. W. Dijkstra, Hierarchical ordering of sequential processes; Acta Informatica 1 (1971) 115 - 138
- [3] A. van Wijngaarden et al. (eds), Revised Report on the algorithmic language ALGOL68; Mathematical Centre Tracts nr 50, Amsterdam 1976

2. THEORETICAL DISPROOF.

The proposition is disproved by the following quotations from [3]: from o.c. section 3.3. Collateral and parallel clauses:

"Collateral-clauses allow an arbitrary merging of streams of actions. Parallel-clauses provide, moreover, levels of coordination for the synchronisation (10.2.4) of that merging." ;

from o.c. section 3.3.2. Semantics:

"The elaboration of a void-collateral-clause or void-parallel-clause consists of the collateral elaboration of its constituent units and yields empty." .

From these quotations, especially the second one, it immediately follows that there is no true parallelism in ALGOL68.

3. EXPERIMENTAL DISPROOF.

The proposition is disproved by the following ALGOL68 program and its results which show that the void-parallel-clause of the program is elaborated sequentially.

*) Mathematisch Instituut & Vakgroep Informatica, Universiteit van Amsterdam, Roetersstraat 15, 1018 WB Amsterdam.

```

BEGIN    #   ALGOL68 program dining philosophers nr 1, TJD 84.4.11  #
        #   Reference : E. W. Dijkstra , Hierarchical ordering of  #
        #   sequential processes; Acta Informatica 1(1971)115-138  #

INT lifetime=6, thinkmax=30, eatmax=10;
INT thinking = 0, hungry = 1, veryhungry = 2, eating = 3;
INT n=5;                                     # number of philosophers #
[[[] CHAR name=("arjen ", "andries", "hans ", "hendrik", "jan ");
SEMA mutex:= LEVEL 1;
[1:n] SEMA prisem; [1:n] INT st;
    FOR j TO n DO prisem[j]:= LEVEL 0; st[j]:= thinking OD;

PROC toss = ( INT max) INT: ENTIER(max * random) + 1;

PROC next = ( INT j) INT: IF j=n THEN 1 ELSE j+1 FI;

PROC prev = ( INT j) INT: IF j=1 THEN n ELSE j-1 FI;

PROC test = ( INT k, horvh) VOID:
    IF st[k] > thinking
    THEN IF st[prev(k)] <= hungry AND st[next(k)] <= hungry
        THEN st[k]:= eating; UP prisem[k]
        ELIF st[prev(k)] = eating OR st[next(k)] = eating
        THEN st[k]:= horvh
    FI
    FI;                                     # end of test #

PROC thinkoreat = ( INT k, max, STRING s) VOID:
    BEGIN INT period = toss(max);
        TO period DO SKIP OD;
        print((newline, " philosopher ", name[k], " has been "
            + s + " during", whole(period, -4), " time units "))
    END ;

PROC think = ( INT k) VOID: thinkoreat(k, thinkmax, "thinking");

PROC eat = ( INT k) VOID: thinkoreat(k, eatmax, " eating");

PROC cycle = ( INT w) VOID:
    TO lifetime
    DO think(w);                             # philosopher w is thinking #
        DOWN mutex;
        st[w]:= hungry;                     # philosopher w is hungry #
        test(w, hungry);                   # or very hungry #
        UP mutex;
        DOWN prisem[w];
        eat(w);                             #philosopher w is eating #
        DOWN mutex;
        st[w]:= thinking;                 # philosopher w is thinking #
        test(next(w), veryhungry); test(prev(w), veryhungry);
        UP mutex
    OD ;                                     # end of cycle #

PAR BEGIN cycle(1), cycle(2), cycle(3), cycle(4), cycle(5) END
END

```

The results of this program are displayed on the next page.

[illegible]

4. EXPERIMENTAL PROOF.

The proposition is proved by the following ALGOL68 program and its results.

Parallellism is obtained by a technique to implement fairness presented by Apt & Olderog [1].

A key role is played by the routine variez which enables redirection of control to another process.

Routine sortie forces redirection of control, and routine entree neutralises this effect.

The status of the five philosophers is encoded in the fractional digits of the number of time units as follows:

0 = thinking, 1 = hungry, 2 = very hungry, 3 = eating.

```
-----
BEGIN      # ALGOL68 program dining philosophers nr 2, TJD 84.4.12 #
           # Reference : E. W. Dijkstra , Hierarchical ordering of #
           # sequential processes; Acta Informatica 1(1971)115-138 #

INT lifetime=6, thinkmax=30, eatmax=10;
INT thinking = 0, hungry = 1, veryhungry = 2, eating = 3;
INT n=5;                                     # number of philosophers #
[[[]] CHAR name=("arjen  ","andries","hans  ","hendrik","jan   ");
SEMA mutex:= LEVEL 1;
[1:n] SEMA prisem; [1:n] INT st;
      FOR j TO n DO prisem[j]:= LEVEL 0; st[j]:= thinking OD;

PROC toss = ( INT max ) INT: ENTIER(max * random) + 1;

# Declarations and initialisations to obtain fairness. Reference: #
# K. R. Apt & E.- R. Olderog, Proof rules dealing with fairness; #
# Lecture Notes in CS nr 131 (D. Kozen, ed.), p. 1 - 8.          #

INT waitmax = 2 * n, seminf = maxint OVER 2;
[1:n] SEMA turn; [1:n] INT z; turn[1]:= LEVEL 1; z[1]:= waitmax;
      FOR j FROM 2 TO n
        DO turn[j]:= LEVEL 0; z[j]:= toss(waitmax)
        OD;

PROC mindex = INT:
  BEGIN INT min:= maxint, inx:= 0;
        FOR j TO n
          DO IF (z[j]-:= 1) < min THEN min:= z[j]; inx:= j FI
          OD;
        inx
  END;

PROC variez = ( INT k) VOID:
  IF INT inx = mindex; z[inx] <= 0 OR z[k] > waitmax
  THEN z[inx]:= toss(waitmax); UP turn[inx]; DOWN turn[k]
  FI;
                                     # end of variez #

PROC entree = ( INT k) VOID : z[k]-:= seminf;

PROC sortie = ( INT k) VOID : (z[k]+:= seminf; variez(k));

# End of declarations and initialisations to obtain fairness #
-----
```

Program text continues on next page.

Continued text of ALGOL68 program nr 2, TJD 84.4.12

```
PROC next = ( INT j) INT: IF j=n THEN 1 ELSE j+1 FI;
PROC prev = ( INT j) INT: IF j=1 THEN n ELSE j-1 FI;
PROC test = ( INT k, horvh) VOID:
  IF st[k] > thinking
  THEN IF st[prev(k)] <= hungry AND st[next(k)] <= hungry
        THEN st[k]:= eating; UP prisem[k]; entree(k)
        ELIF st[prev(k)] = eating OR st[next(k)] = eating
        THEN st[k]:= horvh
  FI FI;                                     # end of test #

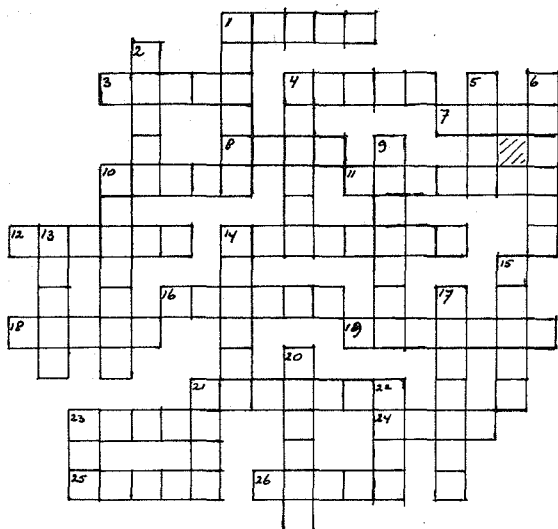
PROC thinkoreat = ( INT k, max, STRING s) VOID:
  BEGIN INT period = toss(max); REAL d = 10; PRIO + = 7;
    TO period DO variez(k) OD;
    REAL pst = st[1]*d+st[2]*d+st[3]*d+st[4]*d+st[5]/le5;
    print((newline, " philosopher ", name[k], " has been " +s,
           " during", fixed(period+pst, -9, 5), " time units "))
  END ;

PROC think = ( INT k) VOID: thinkoreat(k, thinkmax, "thinking");
PROC eat = ( INT k) VOID: thinkoreat(k, eatmax, " eating");
PROC cycle = ( INT w) VOID:
  BEGIN DOWN turn[w];
    TO lifetime
      DO think(w);                               # philosopher w is thinking #
        DOWN mutex;
        st[w]:= hungry;                          # philosopher w is hungry #
        test(w, hungry);                         # or very hungry #
        UP mutex;
        sortie(w); DOWN prisem[w];
        eat(w);                                  #philosopher w is eating #
        DOWN mutex;
        st[w]:= thinking;                        # philosopher w is thinking #
        test(next(w), veryhungry); test(prev(w), veryhungry);
        UP mutex
      OD ;
    UP turn[w]; sortie(w)
  END;

PAR BEGIN cycle(1), cycle(2), cycle(3), cycle(4), cycle(5) END
END
```

The results of this program are displayed on the next page, the last page of this paper.

philosopher	arjen	has	been	thinking	during	12.00000	time	units
philosopher	arjen	has	been	eating	during	7.30000	time	units
philosopher	jan	has	been	thinking	during	12.00000	time	units
philosopher	andries	has	been	thinking	during	17.00003	time	units
philosopher	jan	has	been	eating	during	8.03003	time	units
philosopher	andries	has	been	eating	during	5.03000	time	units
philosopher	arjen	has	been	thinking	during	9.00000	time	units
philosopher	arjen	has	been	eating	during	2.30000	time	units
philosopher	andries	has	been	thinking	during	4.00000	time	units
philosopher	hans	has	been	thinking	during	21.03000	time	units
philosopher	hendrik	has	been	thinking	during	29.03100	time	units
philosopher	andries	has	been	eating	during	5.03130	time	units
philosopher	hendrik	has	been	eating	during	5.00230	time	units
philosopher	hans	has	been	eating	during	2.00300	time	units
philosopher	andries	has	been	thinking	during	13.00000	time	units
philosopher	hans	has	been	thinking	during	7.03000	time	units
philosopher	jan	has	been	thinking	during	29.03100	time	units
philosopher	andries	has	been	eating	during	6.03103	time	units
philosopher	jan	has	been	eating	during	6.00303	time	units
philosopher	hans	has	been	eating	during	5.00300	time	units
philosopher	hendrik	has	been	thinking	during	24.00000	time	units
philosopher	hendrik	has	been	eating	during	1.00030	time	units
philosopher	hans	has	been	thinking	during	9.00000	time	units
philosopher	arjen	has	been	thinking	during	30.00300	time	units
philosopher	arjen	has	been	eating	during	3.30300	time	units
philosopher	hans	has	been	eating	during	7.00300	time	units
philosopher	jan	has	been	thinking	during	20.00000	time	units
philosopher	andries	has	been	thinking	during	28.00003	time	units
philosopher	jan	has	been	eating	during	7.03003	time	units
philosopher	andries	has	been	eating	during	1.03000	time	units
philosopher	hendrik	has	been	thinking	during	24.00000	time	units
philosopher	jan	has	been	thinking	during	5.00030	time	units
philosopher	arjen	has	been	thinking	during	27.00031	time	units
philosopher	hans	has	been	thinking	during	16.30031	time	units
philosopher	arjen	has	been	eating	during	4.30131	time	units
philosopher	hendrik	has	been	eating	during	6.00132	time	units
philosopher	jan	has	been	eating	during	6.00303	time	units
philosopher	hans	has	been	eating	during	9.00300	time	units
philosopher	arjen	has	been	thinking	during	11.00000	time	units
philosopher	andries	has	been	thinking	during	22.30000	time	units
philosopher	arjen	has	been	eating	during	4.31000	time	units
philosopher	jan	has	been	thinking	during	7.03000	time	units
philosopher	andries	has	been	eating	during	2.03003	time	units
philosopher	hans	has	been	thinking	during	9.00003	time	units
philosopher	hans	has	been	eating	during	4.00303	time	units
philosopher	jan	has	been	eating	during	9.00003	time	units
philosopher	jan	has	been	thinking	during	1.00000	time	units
philosopher	hans	has	been	thinking	during	5.00003	time	units
philosopher	jan	has	been	eating	during	6.00303	time	units
philosopher	hendrik	has	been	thinking	during	25.00300	time	units
philosopher	arjen	has	been	thinking	during	14.00310	time	units
philosopher	andries	has	been	thinking	during	15.30310	time	units
philosopher	hans	has	been	eating	during	8.31310	time	units
philosopher	hendrik	has	been	eating	during	3.32030	time	units
philosopher	arjen	has	been	eating	during	7.32000	time	units
philosopher	andries	has	been	eating	during	6.03000	time	units
philosopher	hendrik	has	been	thinking	during	30.00000	time	units
philosopher	hendrik	has	been	eating	during	7.00030	time	units
philosopher	hendrik	has	been	thinking	during	15.00000	time	units
philosopher	hendrik	has	been	eating	during	7.00030	time	units



horizontaal:

1. vrije tijd of werken ?
3. een leuk feest.
4. helft van een bekend paar.
7. opera op het M.I.
8. Jack de Ripper is haar laatste vriend.
10. niet zo,n leuk feest.
11. niet aardig, zeggen ze, maar goed in z'n vak.
12. een gekke meid.
14. hierom draait alles.
16. inwoner van 19.
18. schepper van 20.
19. woonplaats van 16.
21. zij geeft veel inspiratie.
23. hebbelijke vrouw.
24. is zijn koning koud ? welnee.
25. zij wordt gemeen voor de gek gehouden.
26. trouw tot in de dood.

verticaal:

1. niet aardig voor z'n vrouw.
2. ongelukkige moeder
4. wat een verdriet heeft hij !
5. zij sterft een natuurlijke dood.
6. voor haar een happy ending.
9. men begint vaak met haar.
10. hij is enkelvoud van zichzelf.
13. alweer een gekke meid.
14. schepper van 22 en 26.
15. zij treft het slecht met haar vader.
17. voor haar wordt trouw beloond.
20. wispelturige dame.
21. zij heeft niet veel kijk op mannen.
22. haar wantrouwen brengt ongeluk.
23. ladder in New-York.

Beste Arjen

ik hoop dat je dit cryptogram met plezier oplost.
De meeste omschrijvingen slaan op onze gemeen-
schappelijke liefde, de opera !

Elly Dobber

HET PERFIDE ZUIDEN

Er wordt op de deur geklopt.

Ik schrik wakker.

"Ja?"

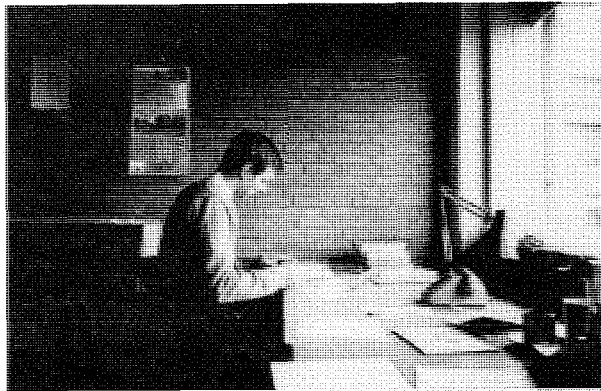
De deur gaat open.

Een net geklede jongeman steekt zijn hoofd naarbinnen.

"Krokettentijd!" gebiedt hij.

Hij trekt de deur weer dicht en vervolgt gehaast zijn weg.

Na luttele seconden dringt de situatie tot me door. Snel breng ik mijn bureau in orde, berg wat spulletjes op en ga mijn rustverstoorder achterna. Zo gaat het bijna elke dag. Hij is mij weer eens komen roepen voor de lunch. Om 11.55 precies komt hij ons "losweken uit ons kot", zoals hij het noemt.



het voormalig kot van dr. A.K. Lenstra

Lunchtijd betekent voor hem krokettentijd. Deze warme snacks vormen zijn primaire voedselvoorziening tijdens de lunch. Mits ze natuurlijk op het menu staan, en liefst niet met een kip-kerrie smaak.

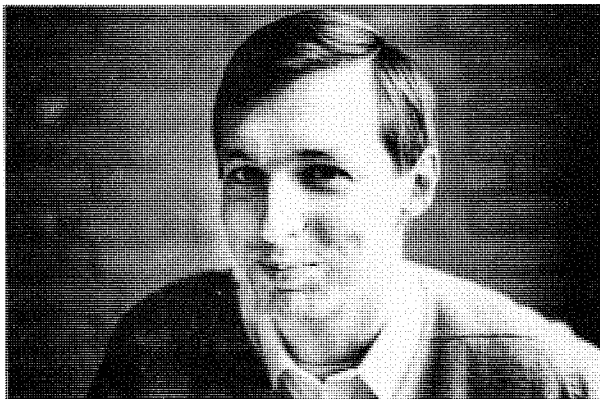
"Nee, dank je feestelijk," zou hij zeggen als je hem deze kroketten warm zou aanbevelen.

Het kroketten eten heeft Arjen verheven tot een kunst. Laat mij U deze schetsen. Men neme de volgende werktuigen en ingrediënten:

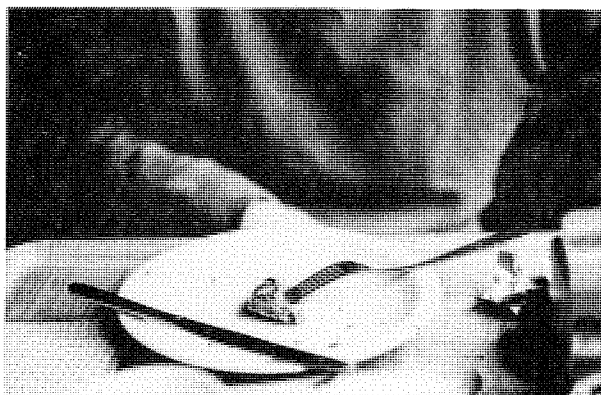
1. De kroket. Deze moet vanzelfsprekend warm, maar niet te heet, en van goede kwaliteit zijn, dus geen kip-kerrie kroket.
2. Sneetje bruin brood.
3. Tube mosterd.
4. Bord, mes en vork.

Leg het sneetje brood op Uw bord. Plaats midden op het sneetje brood de kroket. Snijd met het mes de kroket in de lengterichting middendoor zonder daarbij het brood doorte snijden. Als men de kroket doorsneden heeft, draaie men de kroket een kwartslag zodat de open zijde op het brood komt te liggen, en wel door het lemmet van het mes tegen de open zijde van de kroket te drukken en een vingertop (voorzichtig!) tegen de korst te houden. Druk daarna met de vingers de kroket stevig, doch niet te doortastend, op de snee brood en haal het mes onder de kroket uit, daarbij het

lemmet meteen schoonvegend aan brood en kroket. Handig en efficiënt! Doe hetzelfde met de andere helft. Pers een dun laagje mosterd op beide helften van de kroketen strijk daarna met Uw mes de mosterd egaal over de kroket. Snijd met vork en mes het brood in de lengterichting door en daarna elk der helften in kleinere stukjes. Men zorgt dat men bij het doorsnijden van de kroket deze niet uitperst. Dus laat het (scherpe!) mes zachtjes door de kroket glijden. Smaak en aroma blijven zo zoveel mogelijk behouden. De stukjes brood met kroket zijn nu gereed voor consumptie (met vork!).



Indien men de kunst van het kroketten eten niet snel genoeg onder de knie kan krijgen, kan men deze creatieve bezigheid in eigen persoon gaan aanschouwen tijdens de lunch bij dr. A.K. Lenstra. Smakelijk eten!



Niet alleen zijn voedselvoorziening maar ook zijn woordkeus is vaak weloverwogen, zoals moge blijken uit de volgende fragmenten.

Tijdens het tafelen bespreken we wel eens de 'kwaliteit' van sommige café's. Zo vroeg ik eens aan Arjen:

"Ken je café X? Ik heb gehoord dat daar de hogere standen van Amsterdam vertoeven." (Om beleefdheidsredenen, en zonder verlies van algemeen-

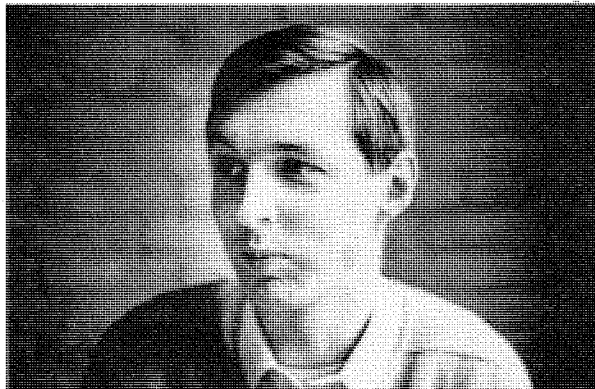
heid, zullen we dit café aanduiden met de letter X).



"Wat?!" riep Arjen uit. "Café X? Dat is een proletencafé! Het grauw en gepeupel komt daar."

Dat is tenminste duidelijke taal, vindt U niet?

Ook schertst Arjen vaak over "het gepeupel van beneden de rivieren". Dat men daar soms wetenschappelijke notities schrijft i.p.v. typt, is wel eens onderwerp van zijn scherts. Als ik daags na een bezoek aan Eindhoven Arjen tijdens de lunch tegenkom, is zijn opmerking steevast:



"En hoe was het in het perfide Zuiden?"

Wat zou ik daarop moeten antwoorden?

"Vertrouwer dan in het 'hoge' Noorden."

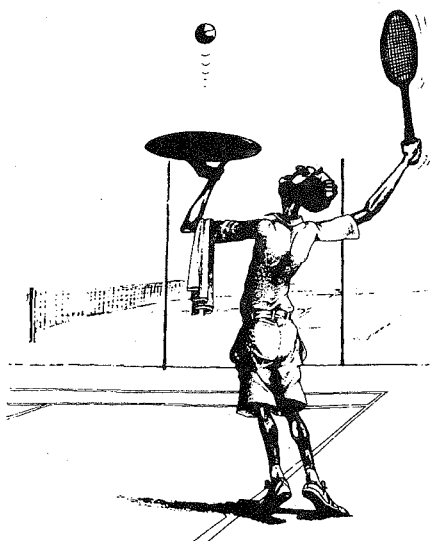
In de zomer van '83 hebben Arjen en ik af en toe tennis gespeeld, dat wil zeggen "de kunst, om staande op fijn gemalen dakpannen een bal over een grofgehaakt lapje te slaan, met zo weinig mogelijk spelregels, zodat ook de hogere standen het nog kunnen volgen" (G. Komrij).

Wij speelden op het trainingsveld van de voetbalclub "Zeeburgia". Geen echt tennisveld dus. Ons speelveld zou beter beschreven kunnen worden als een veld van grofgemalen bakstenen waar hier en daar diepe voren en kuilen in waren aangebracht. Als het zeer heet was geweest, en dat was het vaak afgelopen zomer, was het maalsel zeer droog. Als men dan een snel sprintje trok en daarna krachtig remde, moest men gehuld in een dikke mist van stof de weg op de tast terugzoeken. Een paar sprintjes waren voldoende om alle lijnen volledig onzichtbaar te maken. Maar ja, die hadden we toch niet nodig? Zonder lijnen ging het veel beter.

De spelregels, al waren ze eenvoudig, schaften we zoveel mogelijk af. De lijnen hadden we al afgeschaft. Serveren deden we ook niet, dat was te moeilijk. Het net hebben we maar laten zitten. Anders was de lol er af. Verder mocht je een zo groot mogelijk speelveld nemen als je zelf wilde, de enige beperkende regel daarbij was dat we de bal moesten kunnen raken. Er bleef uiteindelijk maar één spelregel over: je moest elkaar de bal over het net toeslaan. En dat vonden we al moeilijk genoeg. Dat er zo weinig spelregels overbleven lag niet aan onze standen, zoals Komrij suggereert. Het was louter een kwestie van spelvreugde: hoe minder regels, hoe meer plezier we in het spel hadden.

Uitgesproken 'geoefende' spelers waren we dus niet. Als we elkaar de bal meer dan twee keer konden toeslaan vonden we dat al een hele prestatie. Dat lag niet alleen aan onze onbekwaamheid. De eerlijkheid gebiedt mij te zeggen dat ook de slechte gesteldheid van het speelveld hier mede toe bijdroeg.

Befaamd waren onze lobs. Een lob is een hoge bal die men over de tegenstander heen plaatst, maar binnen het speelveld. "Hoe hoger hoe mooier" was ons devies. Verscheidene malen belandde de bal, inderdaad onbereikbaar voor Arjen, in de hoofdtribune van de voetbalvereniging Zeeburgia. We hebben wat afgelopen in die tennisuurtjes.



Jo Ebergen

Gustav Mahler en Richard Strauss.

Beste Arjen,

In jouw studententijd leerden wij elkaar kennen als consumenten van muziek. Niet als gewone consumenten maar als super-consumenten. Veel mensen, ik denk vooral aan uitvoerende musici, weten veel meer van muziek af dan wij, maar op het consumptie-vlak zijn wij moeilijk te overtreffen.

De meeste tijd die wij samen luisterend doorbrachten is ongetwijfeld aan Wagner besteed, maar meer nog associeer ik onze muzikale relatie met de heren Mahler en Strauss. Twee tijdgenoten, twee collega's, twee kinderen van het oude Europa, maar vooral twee verschillende mensen die verschillende muziek schreven.

Bij het luisteren naar Mahler verbaas ik mij er nog vaak over, dat het oude, vertrouwde symfonie-orkest zo kan klinken. Sommige vaklieden vinden Mahler geen echte muziek, misschien wel omdat ze mijn verbazing delen. Maar ik heb de tijd mee gehad met mijn grote voorkeur voor Mahler: in de jaren zestig is er een Mahler-renaissance begonnen die geleid heeft tot een ware explosie van het aantal uitvoeringen van al zijn werken, zowel in de concertzaal als op de grammofoonplaat.

Bij het luisteren naar de orkestwerken van Strauss denk ik nog steeds: wat is het Europese symfonie-orkest toch groot, en mooi, en hol. Maar bij het luisteren naar zijn opera's verbaast het me telkens weer, dat operamuziek zo doorwrocht en zo natuurlijk kan klinken. Hoe is het mogelijk dat er wel tien van zulke opera's slechts af en toe worden uitgevoerd en zo weinig op de plaat zijn opgenomen.

Mijn eerste voorkeur is Mahler, en ik kom als consument tegenwoordig voor de volle honderd procent aan mijn trekken. Jouw eerste voorkeur is Strauss, en met een behoorlijk aantal van zijn opera's kom je als consument maar matig aan je trekken. Er is een grote vergissing gaande. Ik wens jou en alle opera-liefhebbers een Strauss-renaissance toe.

Amsterdam, 24 maart 1984.

Gerard Foekema.

Singuliere-waardenontbinding en datacompressie

door

Walter Hoffmann

1. Singuliere-waardenontbinding

Voor het oplossen van problemen uit de lineaire algebra met behulp van een computer wordt gewoonlijk gebruik gemaakt van een voor dat probleem geschikte matrixfactorisatie. Zo wordt voor het oplossen van stelsels lineaire vergelijkingen met een reguliere coëfficiënten-matrix, deze matrix (evt. na verwisseling van rijen) geschreven als het product van een onderdriehoeks-matrix en een bovendriehoeks-matrix. Daarna kan de oplossing van het stelsel lineaire vergelijkingen verkregen worden door twee keer een stelsel op te lossen met een coëfficiënten-matrix in driehoeksvorm. Deze methode is nauw verwant aan zgn. Gauss-eliminatie.

Een methode voor het oplossen van stelsels differentiaalvergelijkingen maakt gebruik van de spectraaldecompositie van de (vierkante) coëfficiënten-matrix. Daartoe moet de matrix een volledig stelsel eigenvectoren hebben, hetgeen niet voor iedere matrix het geval is.

Nauw verwant aan de spectraaldecompositie is de singuliere-waardenontbinding die gedefiniëerd is voor willekeurige $m \times n$ matrices. Eenvoudigheidshalve beperken we ons hier tot matrices over $\mathbb{R}$. Neem aan dat de symmetrische matrix $A^T A$ precies p (positieve) eigenwaarden $\neq 0$ heeft: $\sigma_1^2, \dots, \sigma_p^2$; de bijbe-

horende orthonormale eigenvectoren zijn $v_1, \dots, v_p$. Zij V de $n \times p$ matrix van eigenvectoren dan geldt dus:

$$\text{diag}(\sigma_1^2, \dots, \sigma_p^2) = \Sigma^2 = V^T (A^T A) V = (AV)^T AV.$$

De matrix AV is dus een orthogonale $m \times p$ matrix waarbij σ_j de 2-norm van de j -de kolom is. De matrix U , gedefiniëerd door

$$U = A V \Sigma^{-1},$$

is dus een orthonormale $m \times p$ matrix. Deze laatste relatie wordt ook wel weergegeven als

$$A V = U \Sigma.$$

Daar alle kolommen van V loodrecht op de nulruimte van A staan en samen met een basis van die nulruimte de $\mathbb{R}^n$ opspannen, geldt

$$A V V^T = A.$$

De singuliere-waardenontbinding kan nu gedefiniëerd worden als

$$A = U \Sigma V^T.$$

Deze factorisatie kunnen we ook opvatten als som van p matrices, elk van de rang 1 als volgt:

$$U \Sigma V^T = \sum_{i=1}^p \sigma_i u_i v_i^T.$$

Deze ontwikkeling blijkt in volgende zin optimaal te zijn.

Definiëer

$$A_k = \sum_{i=1}^k \sigma_i u_i v_i^T.$$

Voor A_k geldt dat deze matrix de beste benadering (in de 2-norm) van A is door een matrix van de rang k . In formule:

$$\min_{\text{rang}(B)=k} \|A - B\|_2 = \|A - A_k\|_2 = \sigma_{k+1}; \quad k = 1, 2, \dots, p-1.$$

Voor het (eenvoudige) bewijs hiervan verwijzen we naar:

G. H. Golub, Ch. F. van Loan, Matrix Computations; North Oxford

Academic Publ. Co. 1983.

2. Toepassing van singuliere-waardenontbinding in datacompressie

Een toepassing van de singuliere-waardenontbinding, kortweg svd genoemd, wordt gevonden in datacompressie. We denken daarbij aan een foto die onderverdeeld is in $m \times n$ vierkante vakken. Voor elk vakje kan de "grijswaarde" worden weergegeven d.m.v. een getal dat ligt tussen bijv. min (geheel wit) en max (volledig zwart). Meestal is daarbij $\min = 0$ en $\max = g^e - 1$, voor zeker grondtal g en exponent e . In het door ons uitgewerkte voorbeeld geldt $g = 2$ en $e = 7$. Van de dan ontstane matrix wordt de svd bepaald. Aan de berekende singuliere waarden kan afgelezen worden hoe nauwkeurig A door A_k benaderd wordt. Er geldt immers

$$\frac{\|A - A_k\|_2}{\|A\|_2} = \frac{\sigma_{k+1}}{\sigma_1}$$

Voor het "recht toe recht aan" opslaan van de elementen van de oorspronkelijke matrix A zijn $m \times n$ plaatsen nodig. Voor het opslaan van de gegevens waaruit een rang-1 matrix kan worden berekend zijn $m + n + 1$ plaatsen nodig; m plaatsen voor de elementen van u_i , n plaatsen voor v_i en een voor σ_i . De elementen van A_k kunnen dus berekend worden uit de informatie die is opgeslagen in $k \times (m+n+1)$ plaatsen. We moeten hier echter opmerken dat de elementen van de matrix A geheeltallig verondersteld waren. De elementen van de matrix uit het volgende voorbeeld kunnen in 7 bits worden opgeslagen. Indien we voor de elementen van u_i en van v_i en voor σ_i ook 7 bits ter beschikking stellen, zal een afrondfout gemaakt moeten worden. Voor de afgeronde elementen $\tilde{u}_i$, $\tilde{v}_i$ en $\tilde{\sigma}_i$ zal niet meer gelden

$$A = \sum_{i=1}^R \tilde{\sigma}_i \tilde{u}_i \tilde{v}_i^T.$$

Gewoonlijk zal de datareductie worden toegepast in een situatie waarbij een fout σ_{k+1} / σ_1 geaccepteerd wordt die aanzienlijk groter is dan de fout die ontstaat door A_k slechts in eindige precisie weer te geven.

In het voorbeeld waarin de beschreven techniek is toegepast, is uitgegaan van een foto van Arjen waar hij nadenkt over een antwoord op een interruptie tijdens een van zijn voordrachten. De foto werd opgedeeld in 130×104 vakken waaruit een 130×104 matrix geconstrueerd is met elementsgewijs als waarde de grijswaarde van het overeenkomstige vak op de foto.

Dit leverde 13520 getallen tussen 0 en 127 (de uiterste waarden bleken 8 en 117 te zijn).

De ontstane matrix is vervolgens tamelijk "grof" afgebeeld, in grote trekken op de volgende manier. Het traject van 8 tot 117 is verdeeld in elf gelijke intervallen G_i . Aan elk interval is een symbool of combinatie van symbolen toegevoegd die een steeds grotere mate van "zwarteheid" geven. Hiermee is een in 10 stappen verlopende schaal van wit tot zwart gecreëerd. Voor elk van de 13520 elementen van de matrix is steeds door de schrijfmachine het symbool afgedrukt dat overeenkomt met het interval waartoe het betreffende element behoort. Achtereenvolgens zijn negen benaderingen A_k afgedrukt, gevolgd door de oorspronkelijke matrix A .

In de volgende tabel wordt voor de negen benaderingen aangegeven hoe groot k was in de betreffende benadering A_k ; hoeveel plaatsen nodig waren om alle informatie waaruit A_k berekend kan worden op te slaan; hoeveel procent dit is van 13520 en hoe groot de relatieve

fout σ_{k+1} / σ_1 is.

k	# plaatsen	% van 13520	σ_{k+1} / σ_1
1	235	1.7	.57
2	470	3.5	.26
3	705	5.2	.23
5	1175	8.7	.15
8	1880	13.9	.097
11	2585	19.1	.068
15	3525	26.1	.046
20	4700	34.8	.031
30	7050	52.1	.016

3. Verantwoording

Aan de tot stand koming van deze afdrukken is medewerking verleend door:

Dr P. van Emde Boas, subf. wiskunde, die enige negatieven waar

Arjen op voorkwam ter beschikking stelde;

Dr P. C. Diegenbach, subf. biologie, wiens met behulp van een mi-

croscop verkregen digitalisering van een negatiefbeeld

door een te grove korrelstructuur in het fotografisch ma-

teriaal helaas niet bruikbaar bleek;

Dr Ir J. Smith, fac. geneeskunde, die m.b.v. videocamera, andere

electronica en geschikte software een uitvergroting kon

digitaliseren en de informatie op een magnetische schijf

kreeg;

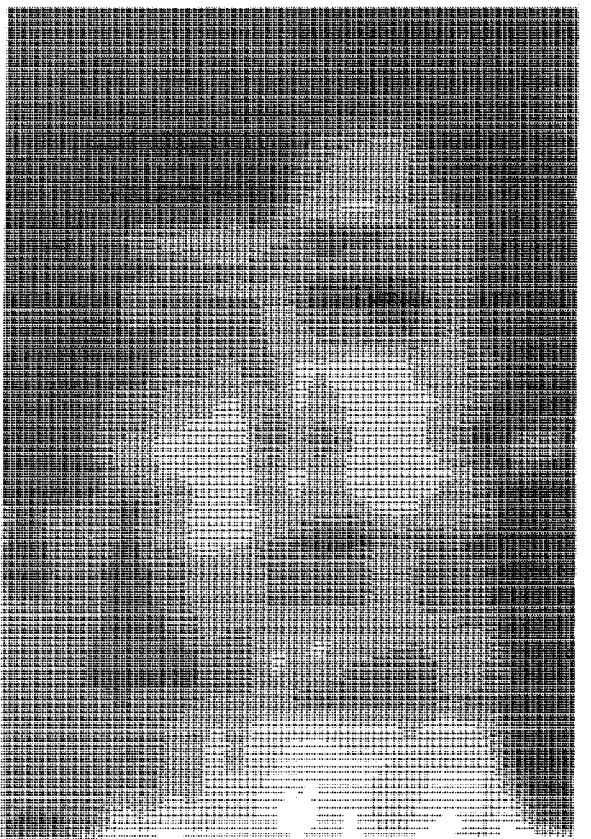
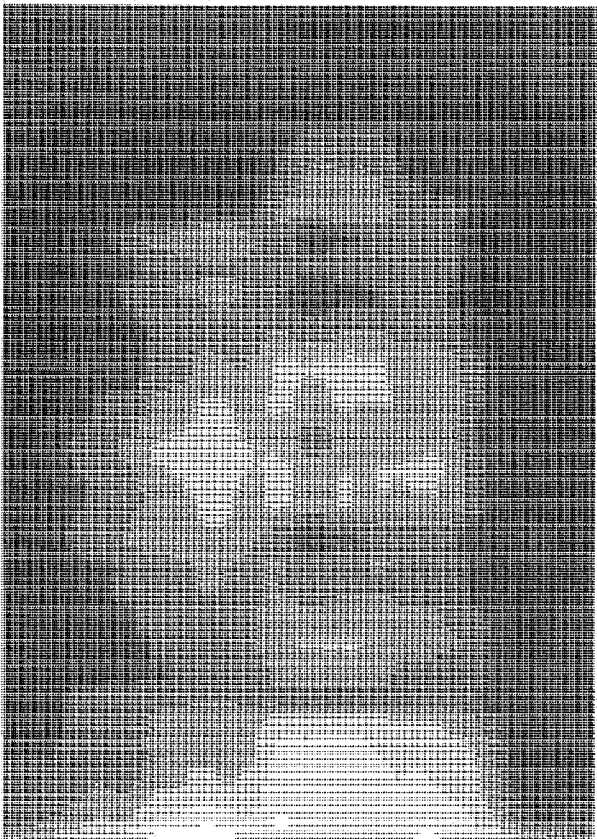
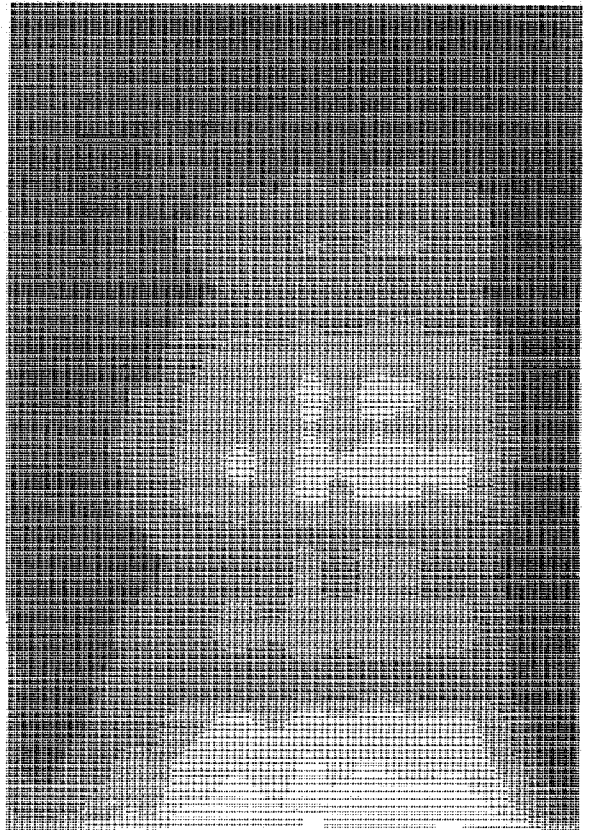
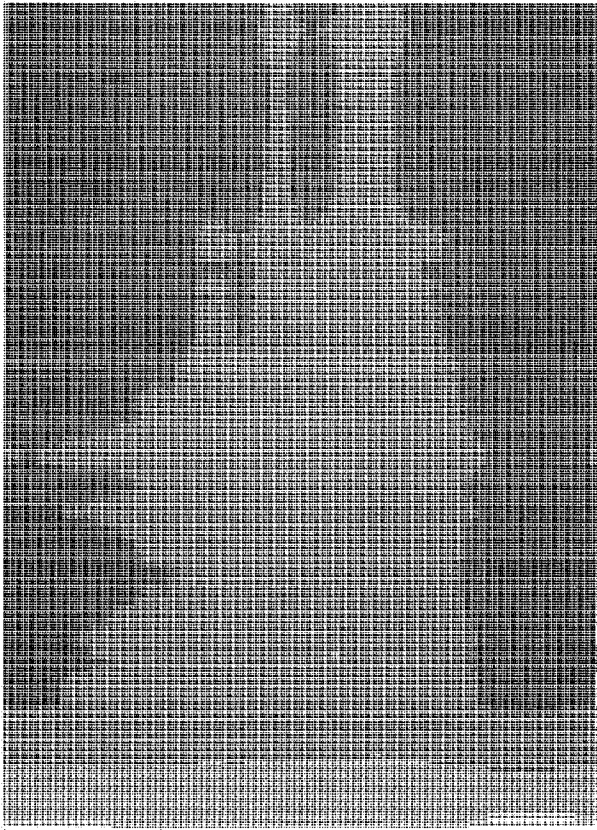
Drs W. L. Posthumus, fac. geneeskunde, die de informatie van de

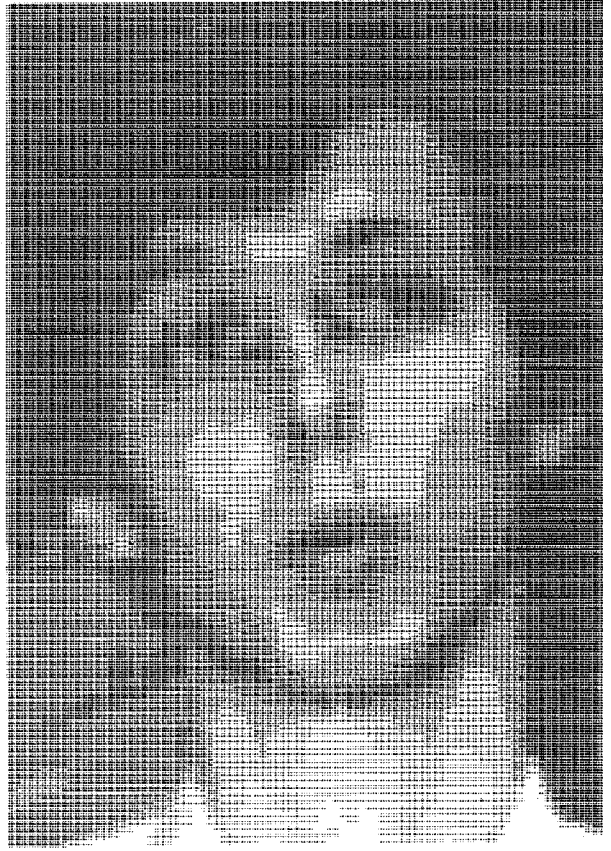
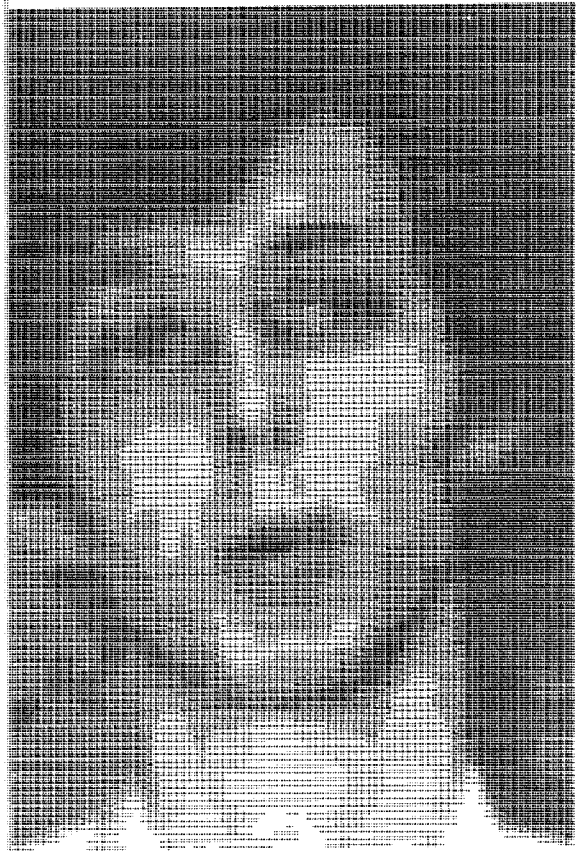
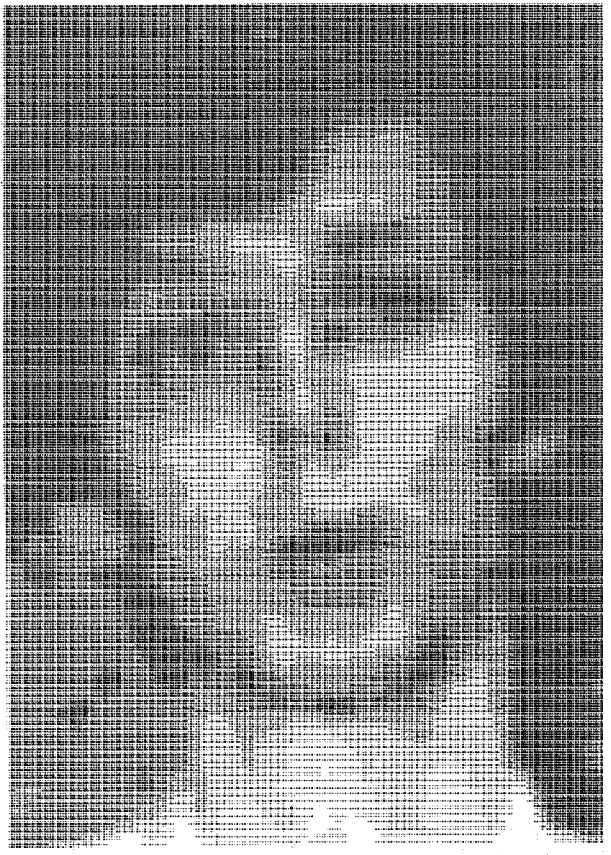
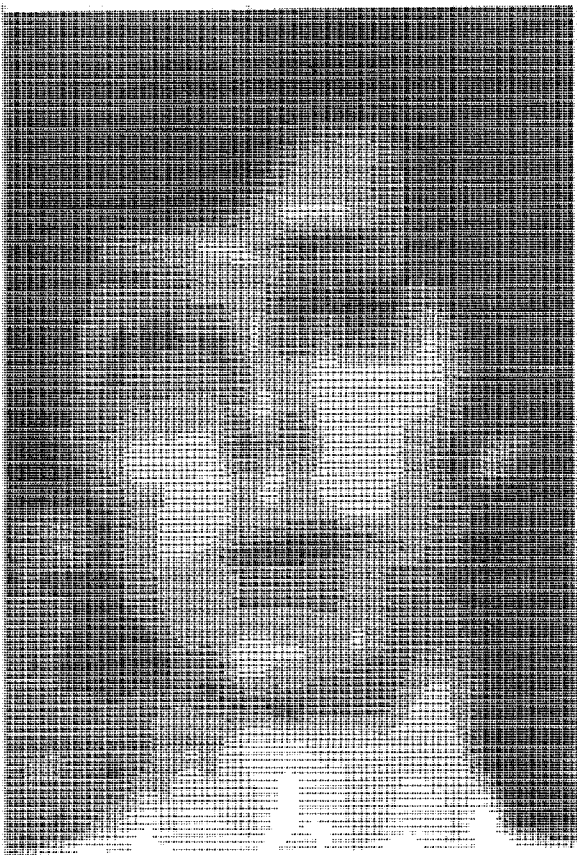
schijf naar de SARA-computer kon transporteren;

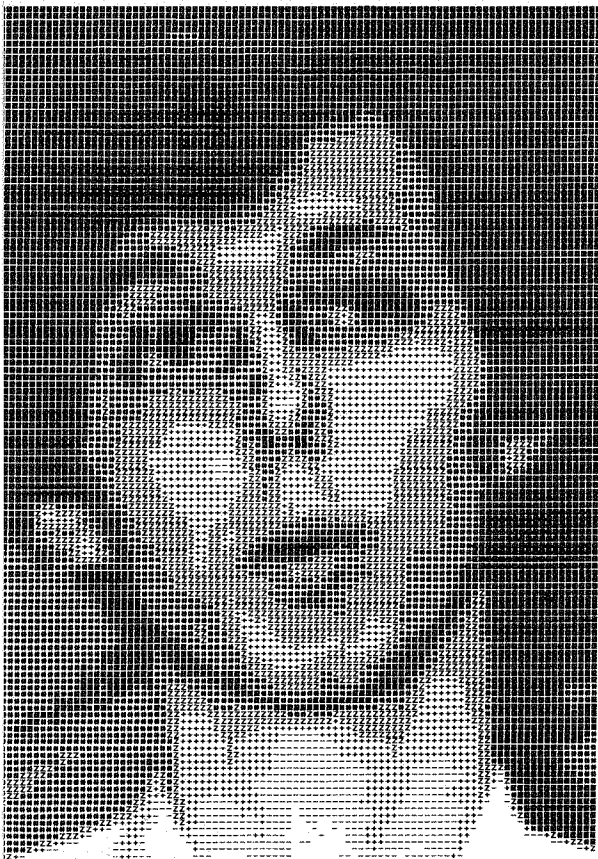
P. P. M. de Rijk, subf. wiskunde, die programma's voor de svd en

voor het afdrukken schreef, en draaide.

Allen dank ik hartelijk voor hun bereidwillige medewerking.







BEST WISHES

Arjen

Congratulations on your Ph.D.

Continue to produce great results.

Ravi Kannan

On a Theorem by R. Dedekind

Erich Kaltofen
Department of Mathematical Sciences
Rensselaer Polytechnic Institute
Troy, New York 12181

To Arjen K. Lenstra

On the occasion of his successful doctoral thesis defense

1. Introduction

A lemma by C. F. Gauss [3, article 42] states that if a polynomial over a unique factorization domain is irreducible it remains irreducible over the field of quotients of this domain. This theorem does not hold, in general, if the coefficient domain is the ring of algebraic integers $\mathcal{O}_K$ of a number field K . Using an old generalization of Gauss' lemma by R. Dedekind [1] it is shown in [8] that the additional denominator needed to express the factorization of a univariate polynomial over K can be chosen equal to the leading coefficient of the polynomial to be factored. Several papers on factoring multivariate polynomials over algebraic number fields [4, 5, 6, 7, 8] have made reference to this fact without showing that the univariate lemma generalizes. In section 2 we will prove a multivariate version of first Dedekind's theorem and then a slightly more general multivariate version of the theorem in [8] designating possible denominators. Since the leading coefficient of a multivariate polynomial is not uniquely determined, we can further optimize the choice of a sufficient denominator needed to express the multivariate factors, a phenomenon which seems not to have been noticed before.

2. Main Results

We first state and prove Dedekind's generalization of Gauss' lemma.

But first we need to clarify our notation. We say that an algebraic integer $a \in \mathcal{O}_K$ divides $b \in \mathcal{O}_K$, $a|b$, iff there exists a number $c \in \mathcal{O}_K$ such that $ac = b$.

Theorem 1 [1]: Let K be a number field, $f(x) = a_\ell x^\ell + \dots + a_0$, $g(x) = b_m x^m + \dots + b_0 \in \mathcal{O}_K[x]$, $h(x) = f(x)g(x) = c_n x^n + \dots + c_0$, $n = \ell + m$, and let $d \in \mathcal{O}_K$ such that $d | c_k$ for all $0 \leq k \leq n$. Then $d | a_i b_j$ for all $0 \leq i \leq \ell$ and $0 \leq j \leq m$.

Proof [2, Sec. 4]: We first prove that $d | a_\ell b_j$ for all $0 \leq j \leq m$. For $j = m$, $d | c_n = a_\ell b_m$ by assumption. Let $\zeta_1, \dots, \zeta_m$ be the roots of $g(x)$ and $\zeta_{m+1}, \dots, \zeta_{m+\ell}$ the roots of $f(x)$. Multiplying $g(x)$ by a_ℓ ,

$$a_\ell g(x) = c_n x^m + a_\ell b_{m-1} x^{m-1} + \dots + a_\ell b_0$$

we see that

$$(-1)^{m-j} \frac{a_\ell b_j}{c_n} = s_{m-j}(\zeta_1, \dots, \zeta_m)$$

where s_i denotes the i -th basic symmetric function

$$s_i(\zeta_1, \dots, \zeta_m) = \sum_{1 \leq m_1 < \dots < m_i \leq m} \zeta_{m_1} \dots \zeta_{m_i}.$$

Now, with $t = n!$, the coefficients of

$$z^t + e_{t-1} z^{t-1} + \dots + e_0 = \prod_{\sigma \in S_n} (z - s_{m-j}(\zeta_{\sigma(1)}, \dots, \zeta_{\sigma(m)})),$$

S_n the set of permutations on $\{1, \dots, n\}$, are symmetric functions in $\zeta_1, \dots, \zeta_n$.

Moreover, each individual ζ_k occurs to power $t - i$ in e_i . By the fundamental theorem on symmetric functions, e_i can be written as an integral polynomial in

$$s_1(\zeta_1, \dots, \zeta_n) = -\frac{c_{n-1}}{c_n}, \dots, s_n(\zeta_1, \dots, \zeta_n) = (-1)^n \frac{c_0}{c_n}$$

of total degree $t - i$. Therefore, $d^{t-i} \mid c_n^{t-i} e_i$ and

$$\left(\frac{c_n z}{d}\right)^t + \frac{c_n e_{n-1}}{d} \left(\frac{c_n z}{d}\right)^{t-1} + \dots + \frac{c_n^t e_0}{d^t} = 0$$

for $z = s_{m-j}(\zeta_1, \dots, \zeta_m)$ and has coefficients in $\mathcal{O}_K$. Thus

$c_n s_{m-j}(\zeta_1, \dots, \zeta_m)/d = (-1)^{m-j} a_\ell b_j/d \in \mathcal{O}_K$. For arbitrary $a_i b_j$ the theorem now follows by induction on ℓ . For $\ell = 0$, $d \mid c_j = a_\ell b_j$, $0 \leq j \leq m$, by assumption. By our previous conclusions, the coefficients of

$$(f(x) - a_\ell x^\ell) g(x) = (c_{n-1} - a_\ell b_{m-1}) x^{n-1} + \dots + (c_\ell - a_\ell b_0) x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_0$$

are divisible by d , thus by induction hypothesis, are the products $a_i b_j$, $0 \leq i \leq \ell-1$, $0 \leq j \leq m$. $\square$

We next show that theorem 1 generalizes to multivariate polynomials.

Theorem 2: Let K be a number field,

$$f(x_1, \dots, x_v) = \sum_{0 \leq i_j \leq \ell} a_{i_1, \dots, i_v} x_1^{i_1} \dots x_v^{i_v} \in \mathcal{O}_K[x_1, \dots, x_v],$$

$$g(x_1, \dots, x_v) = \sum_{0 \leq i_j \leq m} b_{i_1, \dots, i_v} x_1^{i_1} \dots x_v^{i_v} \in \mathcal{O}_K[x_1, \dots, x_v],$$

$$h = f g = \sum_{0 \leq i_j \leq n} c_{i_1, \dots, i_v} x_1^{i_1} \dots x_v^{i_v}, \quad n = \ell + m,$$

and let $d \in \mathcal{O}_K$ be such that $d \mid c_{i_1, \dots, i_v}$ for all $0 \leq i_j \leq n$.

Then $d \mid a_{i_1, \dots, i_v} b_{k_1, \dots, k_v}$ for all $0 \leq i_j \leq \ell$, $0 \leq k_j \leq m$.

Proof: We use Kronecker's homomorphism on f , g and h , that is we substitute

$$y^{(n+1)j-1} \quad \text{for } x_j, \quad 1 \leq j \leq v.$$

Thus,

$$f(y) = f(y, y^{(n+1)}, \dots, y^{(n+1)(v-1)}) = \sum a_{i_1, \dots, i_v} y^{i_1 + (n+1)i_2 + \dots + (n+1)(v-1)i_v}$$

has as its coefficients 0 or the individual $a_{i_1, \dots, i_v}$. Similarly, we map g and h to $\bar{g}(y)$ and $\bar{h}(y) \in \mathcal{O}_K[y]$. Theorem 1 now applies to $\bar{f} \bar{g} = \bar{h}$ and proves our statement. $\square$

We finally prove a multivariate version of Lemma 7.1 in [8]. However, we shall use a weaker notion for monicity which yields a slight improvement to the denominator prediction methods discussed later. We first define:

The polynomial $h(x_1, \dots, x_v) \in K[x_1, \dots, x_v]$, K a number field, is called weakly normalized if one of its coefficients ($\in K$) is a unit in $\mathcal{O}_K$.

Theorem 3: Let K be a number field and let $h(x_1, \dots, x_v) \in (1/r)\mathcal{O}_K[x_1, \dots, x_v]$ with $r \in \mathcal{O}_K$, $r \neq 0$. Assume that $f g = h$ with $f, g \in K[x_1, \dots, x_v]$ weakly normalized. Then $f, g \in (1/r)\mathcal{O}_K[x_1, \dots, x_v]$.

Proof: Let $f, g \in (1/s)\mathcal{O}_K[x_1, \dots, x_v]$, $s \in \mathcal{O}_K$, such that $r \mid s$ (i.e. s may not be optimal). Then $s^2 h = (sf)(sg)$ with $sf, sg \in \mathcal{O}_K[x_1, \dots, x_v]$ and s^2/r divides all coefficients of $s^2 h$. By theorem 2, s^2/r must divide all products

$(sa_{i_1, \dots, i_v})(sb_{k_1, \dots, k_v})$ of coefficients $a_{i_1, \dots, i_v}$ of f and $b_{k_1, \dots, k_v}$ of g . This, in turn, is equivalent to

$$ra_{i_1, \dots, i_v} \cdot b_{k_1, \dots, k_v} \in \mathcal{O}_K$$

which, if we choose $a_{i_1, \dots, i_v}$ the unit coefficient in f or $b_{k_1, \dots, k_v}$ the unit coefficient in g , shows that

$$ra_{i_1, \dots, i_v}, rb_{k_1, \dots, k_v} \in \mathcal{O}_K \quad . \quad \square$$

In the univariate case ($v = 1$) it is sufficient to choose f, g and h monic in order to enforce the weak normalization assumption. In the multivariate case one sufficient condition is that the non-zero monomials in f, g and h of maximum exponent vector with respect to a lexicographical ordering are normalized to 1. In fact, besides lexicographical orderings, any linear ordering on the exponent vectors of the monomials which satisfies

$$(\dagger) (i_1, \dots, i_v) \prec (j_1, \dots, j_v) \implies (i_1+k_1, \dots, i_v+k_v) \prec (j_1+k_1, \dots, j_v+k_v)$$

could be selected. One such ordering is

$$\begin{aligned} (i_1, \dots, i_v) \prec (j_1, \dots, j_v) \text{ iff } & i_1 + \dots + i_v < j_1 + \dots + j_v \text{ or} \\ & i_1 + \dots + i_v = j_1 + \dots + j_v \text{ and} \\ & (i_1, \dots, i_v) \prec_{\text{lexico}} (j_1, \dots, j_v). \end{aligned}$$

3. Application to Factorization Algorithms

Factorization algorithms for polynomial over an algebraic number field K have been devised by several authors. Theorem 3 enters when estimates for occurring rational numerators and denominators are sought. The following representation for the coefficient domain K is usually adopted. First we choose $\alpha \in \mathcal{O}_K$ such that $\mathbb{Q}(\alpha) = K$ by virtue of its minimal polynomial $\mu(\alpha) \in \mathbb{Z}[\alpha]$. The polynomial f to be factored then can be transformed by multiplication with a rational integer to an element

$$f(x_1, \dots, x_v) \in (\mathbb{Z}[\alpha]/(\mu))[x_1, \dots, x_v].$$

However, unlike in the integral case, the factorization of $f = g_1 \dots g_t$,

$g_1 \in \mathcal{O}_K[x_1, \dots, x_v]$, may not have an associate factorization in $(\mathbb{Z}[\alpha]/(\mu))[x_1, \dots, x_v]$.

The reasons are twofold.

1) $\mathbb{Z}[\alpha]$ can be a proper subset of $\mathcal{O}_K$. One can prove, however, that

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \left(\frac{1}{d}\mathbb{Z}\right)[\alpha] \subseteq \left(\frac{1}{D}\mathbb{Z}\right)[\alpha]$$

where $D = \text{discriminant}(\mu) = \mp \text{resultant}(\mu, \mu')$ and $d^2 \mid D$. In fact, $D = d^2 \Delta$ with Δ being the discriminant of K .

2) $f \in \mathcal{O}_K[x_1, \dots, x_v]$ may factor in $K[x_1, \dots, x_v]$ but not in $\mathcal{O}_K[x_1, \dots, x_v]$. One

example, taken from [8], is $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ ($-5 \equiv 3 \pmod{4}$), $f(x) = 2x^2 + 2x + 3 = \frac{1}{2}(2x + 1 + \sqrt{-5})(2x + 1 - \sqrt{-5})$. Applying theorem 3 to $x^2 + x + \frac{3}{2}$

with $r = 2$ both monic linear factors must be elements in $\left(\frac{1}{2}\mathbb{Z}[\sqrt{-5}]\right)[x]$ which

they are: $x + \frac{1+\sqrt{-5}}{2}$, $x + \frac{1-\sqrt{-5}}{2}$.

This example shows that, in the univariate case ($v=1$), monicity is one way of enforcing the weakly normalization assumption. But it is not the only possibility: E.g., we could have applied theorem 3 to $\frac{2}{3}x^2 + \frac{2}{3}x + 1 = (\frac{1+\sqrt{-5}}{3}x+1)(\frac{1-\sqrt{-5}}{3}x+1)$ choosing the constant coefficients 1 ($r = 3$).

In the multivariate case, one has even more choices. Let

$a_{k_1, \dots, k_v}(\alpha) \in \mathbb{Z}[\alpha]$ be the coefficient of $x_1^{k_1} \dots x_v^{k_v}$ in $f(x_1, \dots, x_v)$ such that $(k_1, \dots, k_v)$ is maximal with respect to some ordering $<$ satisfying (+). We now multiply f with $a_{k_1, \dots, k_v}(\alpha)^{-1} \bmod \mu(\alpha)$ and get $a_{k_1, \dots, k_v}(\alpha)^{-1} f(x_1, \dots, x_v) \in (1/r \mathbb{Z}[\alpha])[x_1, \dots, x_v]$ with $r \in \mathbb{Z}$. Therefore, applying theorem 3 to a factorization of $f = g_1 \dots g_t$ such that all non-zero monomials of maximum order w.r.t $<$ have coefficient 1, we get $g_i \in 1/r \mathcal{O}_K[x_1, \dots, x_v]$.

It might not be apparent, at this point, why the minimization of r is of computational advantage. It mainly depends at which moment in the multivariate Hensel algorithm one switches from the mod p^k representation of numeric coefficients back to rational ones. [4] suggests doing this before lifting the minor variables, whereas [6, 7, 8] at the very end for the recovery of the true factors. In the first case, comparing the denominators of the univariate factorization of $f(w_1, \dots, w_{v-1}, x_v)$, $w_i \in \mathcal{O}_K$, to rD (or rd , if d is known) might help discover some extraneous factors, but we believe this is not too helpful. Keeping the mod p^k representation of rationals to the very end, just before the trial divisions, seems a much better idea. One thus can keep p^k small by firstly working with the minimal r and secondly, one can recover the true denominators dr with $d^2 | D$ by computing a continued fraction approximation of the residues and p^k .

REFERENCES

- [1] Dedekind, R.: Über einen arithmetischen Satz von Gauss. Mitteilungen der mathematischen Gesellschaft zu Prag, 1892.
- [2] Fricke, R.: Lehrbuch der Algebra, Bd. 3. Braunschweig: Friedr. Vieweg & Sohn, 1928.
- [3] Gauss, C. F.: Disquisitiones Arithmeticae. Leipzig, 1801.
- [4] Kaltofen, E.: Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization. SIAM J. on Comp., to appear.
- [5] Landau, S.: Factoring Polynomials over Algebraic Number Fields is in Polynomial Time. Siam J. on Comp., to appear.
- [6] Lenstra, A. K.: Factoring Multivariate Polynomials over Algebraic Number Fields. Manuscript, 1983.
- [7] Wang, P.: Factoring Multivariate Polynomials over Algebraic Number Fields. Math. Comp. 30, 324-336 (1976).
- [8] Weinberger, P. and Rothschild, L.: Factoring Polynomials over Algebraic Number Fields. ACM Trans Math. Software, 2, 335-350 (1976).

Zoetermeer 12 april 1984.

Beste Wifje,

Om wij gehoord hebben, dat je de graad van doctor gaat behalen, verbaast ons dit niet! Je moest wel. Je had niet achterblijven bij je broertjes. Zo doe je je ouders nog eens een plezier.

Ik realiseer mij nu ook, dat ik ouder word: als je ziet hoe de kinderen opgroeien en zelfs gaan promoveren.

We hebben elkaar natuurlijk steeds ontmoet in de afgelopen jaren, maar onze contacten lagen toch vooral in je kinderjaren: toen Arnoud een peutertje was en een liefdevol onderdak vond bij zijn onvolprezen tante Ina en oom Hendrik. In die tijd, en dat is de tijd, dat ik je het beste gekend heb, was jij een jaar of tien.

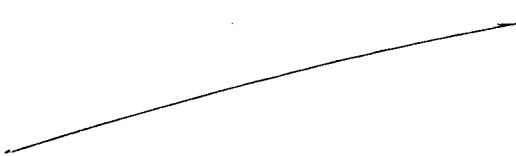
Je hebt toen meebijgedragen aan het geven van een warme thuis haven voor Arnoud.

hij Arnold bijna achttien jaar is, heeft
hij nog altijd fijne herinneringen aan
die tijd: de gezellige dagen en avonden
met de traditionele spelletjes, de wandel-
lingen in het bos en op het strand.
We wensen je van harte geluk met je
behaalde graad!

Ik ben blij, dat ik destijds een aanstaande
promovendus nog in een korte brief
heb zien spelen.

Veel succes in je verdere leven!

Els, mede namens Arnold
en Theun.



A RAMSEY THEOREM ON INFINITELY MANY COLORS

Dexter Kozen
IBM Research
Yorktown Heights, NY 10598, USA

For Arjen, on the occasion of his graduation

Let C be a finite set of colors, and let $[A]^n$ denote the family of subsets of A of cardinality n . Ramsey's Theorem states that for any coloring $\chi: [\omega]^n \rightarrow C$ there exists an infinite $A \subseteq \omega$ such that $[A]^n$ is monochromatic, i.e., the set $\{\chi(x) \mid x \in [A]^n\}$ has cardinality 1. The following simple generalization arose in the author's work on program logics, where it turns out to have some useful applications. For $x, y \subseteq \omega$, define $x \ll y$ if $a < b$ for all $a \in x, b \in y$.

Theorem. Let C be a (possibly infinite) set of colors, and let

$$\chi: [\omega]^{m+n} \rightarrow C$$

be a coloring such that for all $x \in [\omega]^m$, the set

$$\{\chi(xuy) \mid y \in [\omega]^n, x \ll y\}$$

is finite. Then there exists an infinite $A \subseteq \omega$ such that for all $x \in [A]^m$, the set

$$\{\chi(xuy) \mid y \in [A]^n, x \ll y\}$$

has cardinality 1.

Remark. The theorem asks for infinitely many Ramsey theorems, one for each $x \in [\omega]^m$, and solves them all at once with a single $A \subseteq \omega$. Ramsey's Theorem is obtained by taking $m = 0$. Note that χ , even restricted to $[A]^{m+n}$, may have infinite range.

Proof. The proof follows [1, p. 145]. Fix a nonprincipal ultrafilter U on ω . Extend χ inductively to $x \in [\omega]^k$, $m \leq k < m+n$, by taking

$$x/c = \{a \mid x \ll \{a\}, \chi(x \cup \{a\}) = c\}, \quad c \in C,$$

$$\chi(x) = \text{the unique } c \text{ such that } x/c \in U.$$

It follows inductively from the assumption of the theorem that at most finitely many of the x/c are nonempty, therefore $\chi(x)$ exists.

Define a_i inductively to be the least element of

$$\cap \{x/\chi(x) \mid x \in [\{a_0, \dots, a_{i-1}\}]^k, m \leq k < m+n\} \in U.$$

Then $A = \{a_0, a_1, \dots\}$ is the desired infinite set: for $x \in [A]^k$, $m \leq k < m+n$, and $a \in A$, $x \ll \{a\}$, let i be the least number such that $x \in [\{a_0, \dots, a_i\}]^k$. By construction, $a \in \{a_{i+1}, a_{i+2}, \dots\} \in x/\chi(x)$, therefore $\chi(x \cup \{a\}) = \chi(x)$. Thus $\chi(x \cup y) = \chi(x)$ for any $x \in [A]^m$, $y \in [A]^n$, $x \ll y$. This completes the proof. $\square$

R. L. Graham [2] has observed that the theorem fails if the condition $x \ll y$ is weakened. For example, if $m = 2$, $n = 1$, $x = \{x_1, x_2\}$, $y = \{y_1\}$, and both $x_1 < y_1 < x_2$ and $x_1 < x_2 < y_1$ are allowed, color the triple $\{z_1 < z_2 < z_3\}$ with color z_2 .

References

- [1] Chang, C.C. and H.J. Keisler. Model Theory. North Holland, 1973.
- [2] Graham, R.L., correspondence.

Über die Unprimzähligkeit

Hosia W. Labbers, Jr.

Arjen K. Lenstra zugewidmet



1. Einleitung.

Die Unendlichkeit der Menge der Primzahlen, kurz die *Unprimzähligkeit* genannt, ist Gegenstand einer der ältesten Sätze der Zahlentheorie. In diesem Absatz möchte ich drei neue Unprimzähligkeitsbeweise erbringen mit dem Absicht, den angewandten Zahlentheoretiker mit einer Verschiedenartigkeit mathematischer Beweisverfahren vertraut zu machen und auf dieser Weise seine Anwendungsfähigkeit besser den gesellschaftlichen Erfordernissen abzustimmen. Hauptsatz 2 meiner bekannten primzahlo-metrischen Arbeit [1] möge hier als jüngeres Beispiel einer Unprimzähligkeitsanwendung vorgeführt werden.

2. Erster Unprimzähligkeitsbeweis.

Mein erster Unprimzähligkeitsbeweis verwendet nur den marksteinsetzenden, allen Informatikern wohlvertrauten L3-Algorithmus [2]. Die nur wenige Seiten vor meinem musikalischen Motto anzutreffende Formel (3.8) dieser Arbeit besagt dass

$$\prod_{q < p, q \text{ prim}} q > e^{Ap}$$

für alle $p > 2$; hier bedeutet A eine positive Weltkonstante, (Die L3-sche Voraussetzung dass p prim sei wird beim (3.8)-schen Beweis nicht benötigt.) Die Unprimzähligkeit ist unmittelbare Folge der angeführten Formel.

3. Zweiter Unprimzähligkeitsbeweis.

Der zweite Unprimzähligkeitsbeweis entspricht dem Bedürfnis arbeitsloser Algebraiker, die die Sozialrelevanz der Ringenlehre zu betönen wünschen.

Ich brauche zwei Hilfssätze, deren Zweite selbständiges Interesse beansprucht.

Hilfssatz 1. Es sei K ein Körper und $x \in K$.

(a) Wenn $\#K \neq 2$, so gibt es zwei Einheiten in K mit Summe x , und es gibt auch drei Einheiten in K mit Summe x .

(b) Wenn $\#K = 2$, so gibt es entweder zwei oder drei Einheiten in K mit Summe x .

Beweis: Klar.

Hilfssatz 2. Es sei R ein semilokaler Ring, d.h. ein kommutativer Ring mit nur endlichvielen maximalen Idealen. Es sei vorausgesetzt dass R höchstens ein maximales Ideal $\underline{m}$ hat mit $\#R/\underline{m} = 2$. Dann gibt es für jeden $x \in R$ zwei oder drei Einheiten mit Summe x .

Beweis: Nach dem (EUKLID noch nicht zugänglichen!) chinesischen Restsatz ist die kanonische Abbildung $f: R \rightarrow R' = \prod_{\underline{m}} R/\underline{m}$ surjektiv; hier durch-

läuft $\mathfrak{m}$ alle maximale Ideale von R . Für $a \in R$ gilt weiter, dass a Einheit ist wenn und nur wenn $a \notin \mathfrak{m}$ für alle $\mathfrak{m}$, so wenn und nur wenn $f(a)$ Einheit in R' ist. Diese Bemerkung reduziert das Problem von R auf R' , und da R' ein Produkt von Körpern ist kann man zur Beendigung des Beweises Hilfssatz 1 anwenden.

Gesetzt nun, es gäbe Primzähligkeit. Dann wäre $R = \mathbb{Z}$ ein semilokaler Ring, und die Voraussetzung meiner zweiten Hilfssatzes ist erfüllt. Also wäre jeder ganze Zahl Summe von zwei oder drei Einheiten. Aber in $\mathbb{Z}$ gibt es nur die Einheiten $+1$ und -1 . Auf dieser Weise fände man $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3\}$. Widerspruch!

Mein Kollege Herr L.C. WASHINGTON, wem mein Dank für eine Berichtigung in obigem Beweise gebührt, hat bemerkt dass der Schlusswiderspruch für gewisse primitive Stämme nicht zutrifft. Da es aber mehr als drei Primzahlen gibt - zum Beispiel $2, 3, 2^2+1, 2^3-1$ - ist auch für solche Stämme die Unprimzähligkeit bestätigt.

3. Dritter Unprimzähligkeitsbeweis.

Der dritte Beweis erfordert bewertungstheoretische Hilfsmittel [3], ist aber dafür auch ganz kurz. Wenn es nur endlichviele Primzahlen gäbe, so würde der rationale Zahlkörper auch nur endlichviele Primdivisoren haben [3, §1.4]. Der Produktformel [3, 1.4.2(ii)] besagt, dass diese endlichviele Primdivisoren abhängig sind, was nach dem Approximationssatz unmöglich ist [3, 1.2.3].

4. Abschliessende Bemerkungen.

In diesem Absatz habe ich drei neue Unprimzähligkeitsbeweise erbracht mit dem Absicht, den angewandten Zahlentheoretiker mit einer Verschiedenartigkeit mathematischer Beweisverfahren vertraut zu machen und auf dieser Weise seine Anwendungsfähigkeit besser den gesellschaftlichen Erfordernissen abzustimmen. Wir regen den Leser an nach denselben Prinzipien meinen noch nicht publizierten Theorem über die Unendlichkeit der Menge der nicht-Primzahlen zu beweisen.

Literaturhinweise.

1. H.W. Labbers, Jr., TOM und die Primzahlometrie, in: *Tamelijk briljant, opstellen aangeboden aan Dr. T.J. Wansbeek, verzameld door A.K., H.W. en J.K. Lenstra*, Amsterdam, 5 juni 1980.
2. A.K. Lenstra, H.W. Lenstra, Jr., und L. Lovász, Factoring polynomials with rational coefficients, pp. 27-46 in: A.K. Lenstra, *Polynomial-time algorithms for the factorization of polynomials*, Centrum voor Wiskunde en Informatica, Amsterdam 1984.
3. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York 1963.

OIDS AND THEIR ILK

by

J. C. Lagarias

1. The Number of the Beast

It is said that children adapt to whatever environment they grow up in, no matter how bizarre, treating it as normal and as a matter of fact, simply because it never occurs to them that they have any alternative. Through many years of schooling, one becomes a mathematician, or a computer scientist, or whatever. And in this process what peculiar things does one adapt to and take for granted, without noticing?

I speak of commonplaces, of words, of expressions, of concepts. For example, “skid row” is an expression used for a final destination of alcoholics, the end of the line. Where did “skid row” come from? Well, in Portland, Oregon (or was it Seattle, Washington?) there was a steep road called Skid Road, down which logs were skidded to the river for transport to a sawmill. On the weekends the loggers would come to town, get drunk, and sleep it off, in the bushes near Skid Road. By some process Skid Road eventually became “skid row.” This story sounds good, doesn’t it? Perhaps I made it up. (Actually it was told to me by a friend.) A more homely example: what is the origin of the expression “dead end”?

To digress further, there are several schools of mathematical philosophy. One such philosophy, often put forth as a straw man by competing philosophies, is that of *Platonism*, which I shall formulate as the assertion that mathematics consists of eternal truths. In practice it is necessary to formulate those truths using language; that is, to represent them as strings of symbols, often called *words*. (Binary encoding is also permitted.) And these words, representing would-be eternal concepts, each has an origin and a history. I argue instead that it is the *words* themselves that are eternal (for all practical purposes), while the concepts themselves, unhampered by a symbolic representation, change, transmogrify, run rampant. (See the discussion in LAKATOS [2].) It’s a few such *words* I shall now examine.

2. A Bestiary of Mathematical Terminology

- (1) *Fluxions* and *fluents*. Ahhh, the sweet sad melancholy of concepts that have flowered, flourished, and passed away. The heady days of that battle between the titans, NEWTON and LEIBNIZ, or rather between their camps of followers, over who did what, when, and where (a subject now called journalism). The dots and double dots versus the dx 's. A war fought and forgotten, now fossilized in the differing notation of mathematicians and physicists.
- (2) *Poles*. The Riemann zeta function has one, and where did it come from, the name I mean? I don't know. Perhaps it was DESARGUES' unread book with its botanical metaphors, which eventually spread to algebraic geometry and graph theory: trees, branch points, forests.
- (3) *Septic residues*. A term from number theory, a seventh power residue: 12 is a septic residue of 29. Of impeccable Latin parentage, it has since fallen into unsavory company assuring the Anglo-Saxons.
- (4) *Morasses*. A recent term, invented by a logician with a penchant for hyperbole. Is it a contraction of "miasmic mess"? Applying Occam's razor, I assert that the originator of the term is from Louisiana.
- (5) *Matroids*. This word was coined by WHITNEY [4] in 1935 to name an abstract notion of linear dependence. It was constructed by grafting the *Greek* suffix $-οειδης$ (meaning: like, resembling) onto the *Latin* word *matrix* (meaning: mother, source, origin). Some people, including myself, find the word matroid disturbing without being sure exactly why. Gian-Carlo ROTA began a campaign to replace this term with (the more apt but longer word) *Combinatorial Geometry*. However *matroid*, with its 40 year head start, has taken firm root, and indeed seems to be flourishing, cf. WELSH [3]. This leaves me with little more to say, except to inquire how the term *matrix* came to be applied to those little boxes with numbers in them.
- (6) *Oids*. The end product of a process of abstraction that has successfully spawned: Ovoids, Monoids, Matroids, Greedoids etc. A theory of Oids, nonexistent until now (I believe) is developed in § 3. One may object that the term "Oid" suffers from the drawback of being unnecessarily short, which renders it unfit to be a truly bad choice of terminology. Strictly speaking, the objects defined in § 3 are *Quasi-Oids*;

this overcomes the notational convenience of shortness. The alternate term *Lenstroids* was suggested by a friend who wishes to remain anonymous; this was rejected as being too euphonious.

3. Towards a Theory of Oids

Mathematicians have paid far too much attention in the past to concepts possessing structure. This is no doubt a consequence of their preference for discussing things they can say something about. The area of *structureless mathematics* (not to be confused with *computer science*) cries out for further exploration. Following these cries, I consider here one such direction.

The first obstacle one encounters is that a truly structureless concept has the property of not being describable in the English language. (The generalization to other languages would require another paper.) One may call such structureless concepts *ineffable*. It follows that ineffability, being definable in the English language, has the property of not being a member of the collection of all ineffable concepts, which therefore entitles it to membership in B. Russell's nonexistent set consisting of sets which are not subsets of themselves. This connection to classical mathematics rules out its further study in this paper.

As a fallback we may consider instead structured concepts concerning structureless objects. The argument above, *mutatis mutandis*, would seem to eliminate this category as well from serious consideration. Moreover *non-recursively enumerable sets* of integers, which possess at least one desirable desideratum of structurelessness, have been studied fairly extensively by mathematicians, though at least (out of delicacy) no one has exhibited any such sets explicitly.

The theory of Oids ought by all rights to be concerned with explicitly structureless objects. As I find I am unable to bring myself beyond the brink of such disquisitions, I shall instead expostulate on a theory of *Quasi-Oids*. This theory involves a structured

concept: Quasi-Oids*, concerning a structured object: Quasi-Oids*, having at least the merit of *not much structure*. A *Quasi-Oid* is a set with a single binary operation $\bullet$, called *ultiplication*, which is required to be neither commutative nor associative, in the very strong sense that, for any pattern of parentheses, the product is unequal to any other possible such product. For example, if

$$((x_1 \bullet x_2) \bullet x_3) \bullet (x_4 \bullet x_5) = x_6$$

then

$$x_6 \neq x_1, \dots, x_5, \quad x_1 \bullet x_2, \quad (x_1 \bullet x_2) \bullet x_3, \quad \text{etc.}$$

This eliminates the annoying possibility of an identity element in a Quasi-Oid. In what follows, I call Quasi-Oids *Oids* for short.

Examples.

- (1) The empty Oid ϕ . (This is called the *void*.)
- (2) The free Oid F_1 on one generator. (This is called the *Froid*.) The ultiplication table is a fruitful source of new elements:

$$x_1 \bullet x_1 = x_2, \quad (x_1 \bullet x_1) \bullet x_1 = x_3, \quad x_1 \bullet x_2 = x_4, \quad \text{etc.}$$

Elements of the free Oid are called *woids*. Only sticklers will insist that this construction be made well-defined.

Exercise. Show there are $2^{\aleph_0}$ distinct free Oids F_1 (*Hint:* I have not defined isomorphism of Quasi-Oids.)

* This non-distinction between the mathematics and the metamathematics is a satisfactory part of the theory.

A truly satisfactory theory of Oids would be vacuous. In this sense the theory of Quasi-Oids is defective, as I now show.

Theorem 1. *A group is not a Quasi-Oid.*

Proof. A group possesses an identity element, which is already too much. ■

Most other algebraic structures fall by the wayside in their attempts for containment in the collection of Quasi-Oids. Monoids come close, but overshoot by a few letters.

Theorem 2. *The property of Quasi-Oidness is not finitely axiomatizable in first order logic.*

Proof. Imitate Barwise [1], page 9. ■

The following result promises better things to come, a desirable non-closure property.

Theorem 3. *Homomorphic images of Quasi-Oids need not be Quasi-Oids.*

Proof. Take a free Oid F_1 and identify all elements $x_1 = x_2 = \dots$. The resulting object $\mathcal{O} = \{x_1\}$ is (God forbid!) a group, hence not a Quasi-Oid by Theorem 1. ■

The nonassociative nature of a Quasi-Oid leads to some difficulty in writing down its multiplication table. An associative object such as a group has its multiplication table compactly represented by a (possibly infinite) matrix.

Open Problem. *Is it possible to write down the multiplication table of a non-void Quasi-Oid in a satisfactory way? (Hint: Tensor products are allowed.)*

This brief prolegomenon to a theory of Quasi-Oids provides merely a tantalizing glimpse of a general theory of Oids. And beyond this, glimmering in the far distance like a mirage, lie *Fuzzy Oids*.

References

- [1] J. Barwise, *A Handbook of Mathematical Logic*, North-Holland, 1977.
- [2] I. Lakatos, *Proofs and Refutations*, Cambridge University Press.
- [3] J. A. Welsh, *Theory of Matroids*, Academic Press.
- [4] H. Whitney, On the abstract properties of linear dependence, *Am. J. Math.* **57** (1935), 509-533.

sc. De boom van het onderscheid

G. Laman

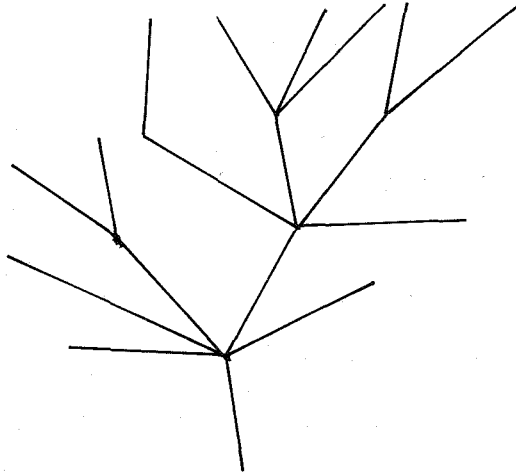
Dat Arjen Lenstra op 28 maart 1984 op het algemeen colloquium over algoritmen voor de Factorisatie van polynomen sprak was niet verwonderlijk gezien zijn activiteiten op dat terrein. Wel verbaasde het mij aanvankelijk dat hij dat deed in termen van goed en slecht. Naderhand kwam ik geleidelijk tot het inzicht dat het hier gaat om een veel wijder verbreid verschijnsel.

Een ander voorbeeld ervan kan men aantreffen bij L. Lovász die "characterizations" indeelt in "good" en "non-good" ¹⁾. K. Appel en W. Haken leveren een derde voorbeeld met hun "geographically good configurations" ²⁾. Opvallend is in dit verband de onzekerheid bij de diverse auteurs over de tegenhanger van goed resp. "good". Lenstra houdt het op slecht en Lovász introduceert het woord "non-good" in het Engels, dat noch in de grote Webster, noch in The Oxford Universal Dictionary voorkomt en zelfs niet in de lijst met duizenden samengestelde woorden met non- in The Random House Dictionary. Appel en Haken vermijden het invoeren van een ander woord helemaal. Bovendien beïjveren Lenstra en Lovász zich de tegenstelling te relativiseren.

Het kost niet veel Fantasie om op het idee te komen dat de auteurs het moeilijk hebben met goed en kwaad. Bij de buitenlanders onder hen blijft het

natuurlijk gissen wat daarachter zit, maar bij Lenstra rijst het vermoeden dat het theologische bloed kruipt waar het niet gaan kan³). Een teer punt daarbij zou zijn verhouding met zijn promotor geweest kunnen zijn, die immers bekend is om zijn bijbelse parafrasen in geschrift⁴), maar meer nog in mondelinge uitspraken.

Als dit alles zo zou zijn, dan zou wellicht een concept uit de graphentheorie uitkomst bieden, sc. de boom van het onderscheid. In navolging van een millenia-oude traditie (Gen 2:9) neme men een boom om alle nuances tussen goed en kwaad mee te beschrijven. Recht omhoog is dan helemaal goed (en dus onbereikbaar?), horizontaal is gewoon fout. Daartussenin zijn alle gradaties denkbaar. Zo'n boom van het onderscheid zou er dan aldus uit kunnen zien.



Welke hoek de algoritme van Berlekamp-Hensel in zo'n boom met de verticaal maakt, laat ik graag ter beoordeling aan meer deskundigen over.

1. L. Lovász, Combinatorial Problems and Exercises, North-Holland Publishing Company, Amsterdam-New York-Oxford 1979.
2. K. Appel & W. Haken, The existence of unavoidable sets of geographically good configurations, Ill. J. Math. 20 (1976) p. 218-279.
3. J. K. van Drunen in Een pak met een korte broek (Eds P. v. Emde Boas e.a.) Amsterdam 1977.
4. P. van Emde Boas, Ibid.

Ode to Arjen

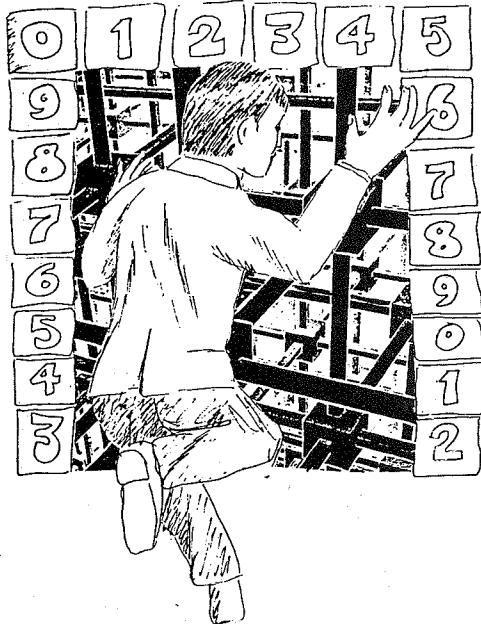
Arjen glanced upon a polynomial fair,
And saw it trapped in an exponential lair.

Guarded by a dralgorithm of non-deterministic height
Of Henselian girth and combinatorial might,



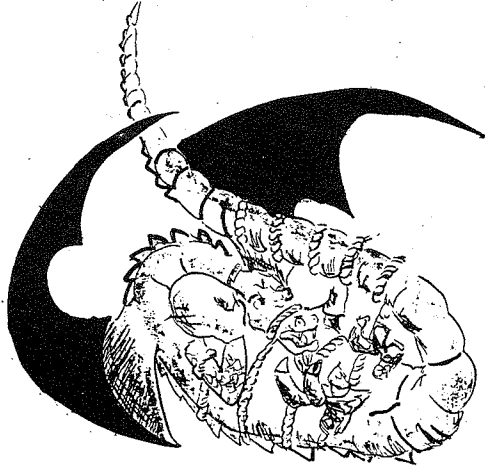
Modular tricks were to no avail
Others had foundered on that explosive trail.

The combinatorial devils had many confused,
But Arjen saw that it was all a ruse.



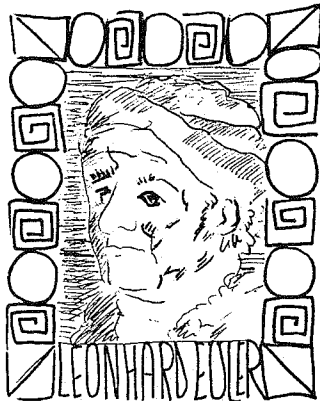
"A way can be found, a way must be found," Arjen pondered,
And into an integer lattice he sauntered.

He sought a basis small and round,
For the dralgorithm to bound.



With basis reduction at his disposal,
He tied up the dralgorithm from nose to toes-1.

Arjen broke open the exponential lair,
And rescued all the polynomials fair.



For this does he receive a Ph.D. crown,
To great applause, and world renown.

Susan Landau

RECHTSVINDING IN HET BURENRECHT

weiszt du was du sahst?

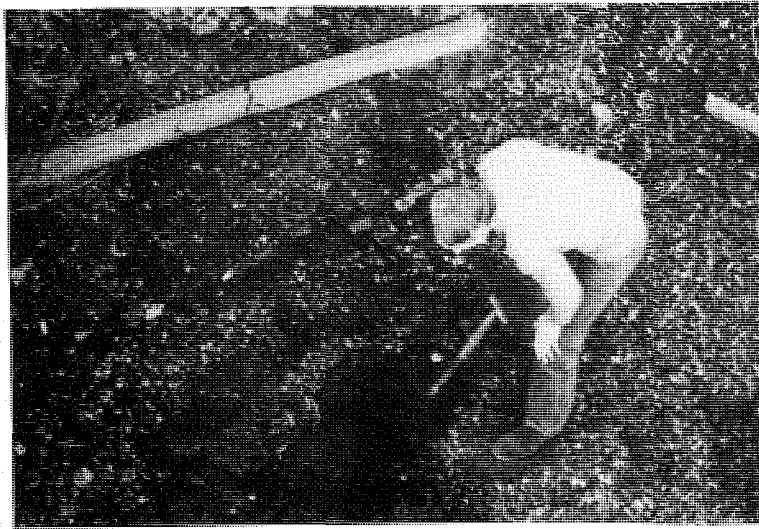
du siehst das ist nicht so...

Gurnemanz tot Parsifal

Wie zich onrustig voelt omdat hij of zij de nederlandse wet nog niet kent en wel eens gehoord heeft dat de wetgever dit van hem verwacht, neemt het Burgerlijk Wetboek (B.W.) ter hand en zet zich tot lezen. Met enig doorzettingsvermogen komt hij vanzelf in het derde boek terecht en dan kan van verveling geen sprake meer zijn, want hier wacht een boeiend hoofdstuk, titel vier: *"Van de regten en verplichtingen tussen eigenaars van naburige erven"*. Men noemt het ook wel het burenrecht.

De verwachtingen van een stadsburger raken nu hoog gespannen, eindelijk immers zal hem worden ontvouwd wat hem te doen of te laten staat met betrekking tot zijn naasten. De wetgever zal het wel uitputtend geregeld hebben.

Grote bewondering maar ook een lichte verontrusting ervaart weldra de lezer. Het verbale repertoire van de wetgever bereikt hier een hoogtepunt, maar het gaat niet over mensen die in een stad wonen in flats of in huizen naast elkaar.



art. 674 Die eene waterbron op zijn erf heeft mag daarvan, naar goeddunken, gebruik maken, behoudens het regt hetwelk de eigenaars van lager gelegen erven, hetzij door enigen titel, hetzij door verjaring, mogten verkregen hebben.

Ons B.W. dateert van 1838 en sommige artikelen zijn rechtstreeks uit de Code Civil vertaald. Het *recht van klaauwengang en stoppelweide* wordt genoemd (art. 680), een vertaling van *droit au parcours et vaine pâture* en het betekent het recht om beesten te laten weiden op onbebouwde gronden. We bevinden ons midden in situaties die op het platteland voorkomen; zo bepaalt art. 563 dat *onroerend door bestemming* onder meer zijn de *konijnen in de konijnenwarande*. Het wordt nog verwarrender; we lezen over voorbijstromend en aflopend water, gemene regenbakken, grachten en sloten, noodweg, buurweg en uitzicht, ladderrecht en waterbronnen. Maar, soms ontstaat een waterbron door dat de afvoer van een buurman op een antiek polderriool niet meer werkt. Dan is scheppen en pompen geboden om te overleven. Helpt titel 4 van boek 3 hier? Het lijkt er niet op. Eens werd een schutting voor een oneigenlijk doel gebruikt en dat hinderde vele burens.



Het bouwwerk bleek zonder vergunning opgetrokken te zijn en bouw- en woningtoezicht vorderde afbraak. De Hinderwet schiet ons te binnen, maar deze wet geeft alleen administratiefrechtelijke regels en schrijft voor dat men voor het vestigen van een industrie of andere werkplaats die gedreun, slechte lucht, trillingen of andere stoornis voor de omgeving ten gevolge heeft, vergunning van het gemeentebestuur moet hebben. Maar iemand die een vergunning heeft gekregen kan toch met de rechter in aanraking komen, omdat hij een ander in het gebruik van zijn huis of tuin belemmert, hetgeen een onrechtmatige daad kan opleveren.

art. 1401 Elke onrechtmatige daad, waardoor aan een ander schade wordt toegebracht, stelt dengene, door wiens schuld die schade veroorzaakt is, in de verplichting om deze te vergoeden.

In 1919 heeft de Hoge Raad(H.R.) het begrip onrechtmatige daad ontwikkeld; er wordt sindsdien onder verstaan "een handelen of nalaten dat óf inbreuk maakt op eens anders recht óf in strijd is met des daders rechtsplicht óf indruist hetzij tegen de goede zeden hetzij tegen de zorgvuldigheid, welke in het maatschappelijk verkeer betaamt ten aanzien van eens anders persoon of goed".

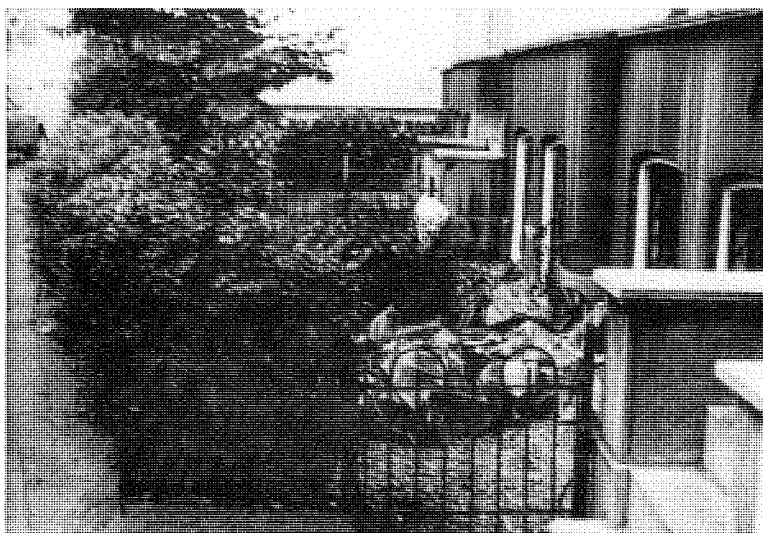
Later, in 1936, heeft de H.R. het begrip misbruik van recht geïntroduceerd door interpretatie van het begrip onrechtmatige daad. Een conflict tussen burens was hiertoe de aanleiding en heeft geleid tot het watertoren-arrest.

A plaatste een paal met oude lappen op zijn eigen terrein, maar zó dat buurman B het goed kon zien. Het mocht niet van de rechtbank, want er was geen enkel redelijk belang voor A en het was duidelijk de bedoeling om B te ergeren. Op de plaats van de paal verscheen toen een watertoren, maar er was geen aansluiting op water. Om dezelfde reden stelde de rechtbank A in het ongelijk. Toen sloot A de toren aan op water en de rechtbank besliste dat de toren er rechtmatig stond, omdat er een redelijk belang aanwezig kón zijn, hoewel ook de bedoeling tot benadeling aanwezig kón zijn. In hoger beroep en in cassatie werd B in het gelijk gesteld.

Misbruik van recht, kan dat eigenlijk wel? Hoe kan iemand een recht hebben en het tegelijkertijd misbruiken? Eigendom werd tot nu toe als het meest volledigerecht beschouwd, inviolable et sacré. Dat is niet zo, ontdekte de H.R. en zag de lijn van ontwikkeling naar een norm die een maatschappelijk bevredigend resultaat geeft en billijk is. Hij zag de woorden van de wet als tekens die voor "iets anders" staan en liet dat "andere", de billijkheid, zien door het eigendomsrecht te plaatsen in de verhouding van individu tot gemeenschap. Rechtsvinding: het verleden zien en ontdekken dat woorden in een wetstekst niet altijd concrete rechtsvragen kunnen oplossen; het zien dat loslaten van de letter van de wet geen rechtsonzekerheid hoeft te scheppen voor diegene die het teken herkent. Onrechtmatig werd méér dan onwetmatig en hinder werd méér dan toebrengen van alleen materiële schade. Misbruik van recht werd jaren na het watertoren-arrest méér dan handelen zonder redelijk doel met het oogmerk een ander te benadelen. In 1970 zag de H.R. nog verder en kwam tot een afweging van belangen: zelfs al streeft buurman A een voor zich zelf redelijk doel na, dan toch kan er sprake zijn van misbruik van recht, als hierdoor het nadeel voor buurman B onevenredig groot wordt. In het ontwerp voor een nieuw B.W. staat een algemeen hinder-artikel en niet bij het burensrecht, maar bij eigendom, want daar gaat het om en daar hoort het dan ook thuis. Ook de criteria voor onrechtmatige daad en misbruik van recht hebben er een plaats gekregen, zodat er rechtstreeks beroep op kan worden gedaan.

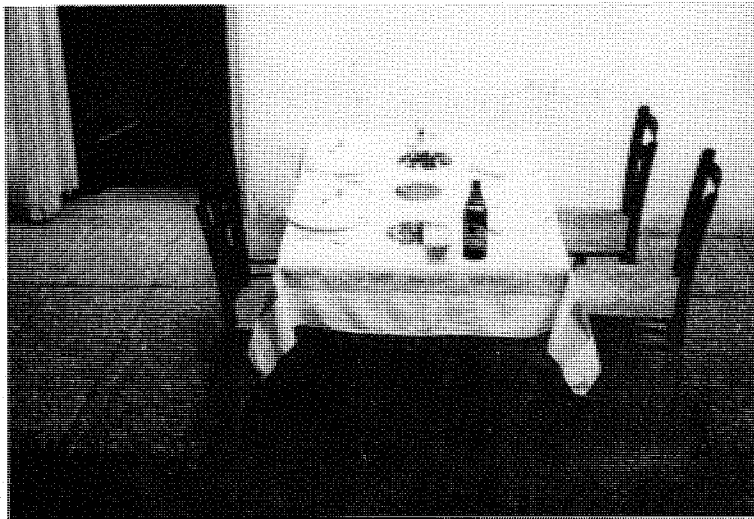
Aan geluidshinder heeft de wetgever van 1838 begrijpelijkerwijze nooit gedacht.

In Amsterdam woonde eens iemand aan een kade die regelmatig oerwoudmuziek en sportberichten de buurt in zond. Zijn naasten burenen wensten zich vele malen burenen toe die opera's ten gehore zouden brengen en ziet ... een wonder geschiedde. Het huis werd verkocht en op een avond hoorden die burenen nieuwe voetstappen en een paar seconden later klonk muziek, die richtige, und keine Fragen! So flieszt die helle stille Singelgracht uns beim Haus vorbei und hat uns das gebracht. Het was niet te geloven. Struikelend over de stoelen repten de burenen zich naar de gemene muur om nog beter te kunnen horen. Parsifal. Hij weet zijn naam niet te noemen, het allereerste teken niet. Maar iets moet hij toch weten? Kan het misschien iets harder? Geluiden die we graag horen hinderen toch immers nooit? Prima la musica, dopo le parole; zo is dat ook toen gegaan en deze nieuwe burenen inspireerden tevens tot enkele voorstellen ter correctie en aanvulling van enige termen in het burenenrecht. Het is echter twijfelachtig of de wetgever deze wijzigingen in het nieuwe B.W. zal opnemen.



1. Het gebruik van een met gemene toestemming tot buurweg bestemde voortuin is niet beperkt tot de personen der geburen.
2. Het uiten van schutting-woorden betekent niet in alle omstandigheden het bezigen van onwelvoegelijke taal, maar soms het uitwisselen van nieuws of het maken van afspraken met de burenen.

3. Een aanaard-ploeg is niet alleen een ploeg met dubbel rister, waarmee men de op rijen geteelde veldgewassen aanaardt, maar ook een ploeg burens die tot taak heeft aarde, zo nodig ook grint, ter ophoging van het tuinpeil aan te dragen.
4. Het recht van worteltrekken en delen is het recht om de wortels van bomen en struiken die op het erf van de nabuur doorschieten, weg te trekken en aan te wenden voor aanplant in eigen tuin.
5. Het recht van overboeking is een hoogst persoonlijk recht en kan slechts worden uitgeoefend door een buurman - boekhandelaar die boeken en dergelijke over de schutting levert.
6. Onder de erfdienstbaarheid van drop (art. 729) verstaat men niet alleen het recht om schoon water te doen uitlopen, maar ook de plicht een pond gemengd zout en een puntzakje camille aan een verkouden buurman te brengen.



7. Het recht van aanscharing is een wederkerige, voortdurende en zichtbare erfdienstbaarheid.

W.F.Lankamp
M.Lankamp-van der Zeyde

DE PRESIDENT VAN DE ARRONDISSEMENTSRECHTBANK TE AMSTERDAM,
RECHTSPREKENDE IN KORT GEDING in de zaak

rolnummer <*> van :

Andries Johannes LENSTRA,

wonende te Amsterdam,

e i s e r bij dagvaarding van 28 augustus 1984,

procureur mr J.Schootstra ing.,

t e g e n :

Arjen Klaas LENSTRA,

wonende te Amsterdam,

g e d a a g d e ,

procureur mr drs K.C.E.Lenstra-De Groot.

Gehoord partijen en gezien de stukken.

OVERWEGENDE TEN AANZIEN VAN DE F E I T E N :

Eiser heeft ter terechtzitting van 3 september 1984 gesteld en gevorderd overeenkomstig de dagvaarding, waarvan de inhoud geacht wordt hier ingevoegd te zijn. Gedaagde heeft verweer gevoerd en geconcludeerd tot afwijzing van de gevraagde voorzieningen. Na verder debat hebben partijen de stukken, waaronder beiderzijds pleitaantekeningen en zijdens eiser één productie, overgelegd ter fine van vonnis.

OVERWEGENDE TEN AANZIEN VAN HET R E C H T :

1. In dit vonnis wordt uitgegaan van de navolgende feiten:

a) Omstreeks maart 1984 heeft gedaagde zijn proefschrift "Polynomial-time algorithms for the factorization of polynomials" aan circa 350 familieleden waaronder eiser, vrienden, vakgenoten en daarvoor in aanmerking komende instanties toegezonden ter kennisname c.q. beoordeling.

b) In bovengenoemd proefschrift komt onder het hoofd "Stellingen" voor stelling nr. 9, luidende

"19201518202706126283527151627010214271805110514091407142113130518275482423212
72201142701281128271205141920180127200527011319200518040113270514270409140727
130505271401011827040527061244284527060505192016180905131618091019 is priem."

c) Toepassing van de volgende code:

01 = A ; 02 = B ; enzovoort, tot en met 26 = Z ; 27 = spatie ;
28 = . (punt) of , (komma)

op het getal in bovengenoemde stelling leidt tot de volgende zinsnede:

"STORT FL6,35 OP ABN REKENINGNUMMER 548242321 VAN A.K. LENSTRA
TE AMSTERDAM EN DING MEE NAAR DE FL44,45 FEESTPRIEMPRIJS" .

d) Eiser heeft f 6,35 gestort op ABN rekeningnummer 548242321
van A.K.Lenstra te Amsterdam.

e) Aanwijzing van een winnaar van de "feestpriemprijs" heeft
niet plaatsgevonden, noch heeft eiser de genoemde f 6,35 terug-
ontvangen.

2. Op de bij dagvaarding uiteengezette en bij pleidooi nader toege-
lichte gronden vordert eiser dat Wij gedaagde zullen bevelen "over
te gaan tot aanwijzing van de winnaar van de "feestpriemprijs" in
tegenwoordigheid van eiser of diens gemachtigde binnen één maand na
betekening van dit vonnis, een en ander op verbeurte van een dwang-
som van f 44,45 voor elke dag waarop gedaagde nalatig blijft aan bo-
venstaand bevel te voldoen".

3. Eiser legt aan zijn vordering ten grondslag dat in stelling 9 van
genoemd proefschrift een uitnodiging tot het meedingen naar een prijs
is vervat, aan de toekenning waarvan gedaagde gehouden is uitvoering
te geven nu eiser is ingegaan op deze uitnodiging door het storten
van genoemd bedrag van f 6,35 op de onder 1 d) genoemde bankrekening.

4. Gedaagdes primaire verweer komt er op neer dat stelling 9 van
meergenoemd proefschrift niets anders inhoudt dan vaststelling van de
primaliteit van genoemd getal.

Subsidiair stelt gedaagde dat de onder 1 c) vermelde zinsnede als
grap bedoeld was en in redelijkheid als zodanig door eiser opgevat
had moeten worden.

5. Naar Ons oordeel faalt het primaire verweer van gedaagde aanstonds.
Immers, het feit dat toepassing van een eenvoudige code - welke toe-
passing zelfs eiser vermocht te volbrengen - op stelling 9 van meer-
genoemd proefschrift oplevert een samenhangende zin, waarin bovendien
twee referenties aan gedaagde voorkomen, te weten diens naam en diens

bankrekeningnummer, leidt onontkoombaar tot de conclusie dat toeval uitgesloten moet worden geacht, zodat Wij van oordeel zijn dat gedaagde de litigieuze mededeling heeft gedaan.

6. Voorzover gedaagde met het subsidiaire verweer bedoelt te stellen dat hij de intentie niet heeft gehad met de litigieuze mededeling uit te nodigen tot het meedingen naar een prijs, dient ook dat verweer te worden verworpen, nu volgens vaste jurisprudentie niet de werkelijke bedoeling van gedaagde te dezen juridisch relevant is, maar de bedoeling zoals eiser die had kunnen en mogen begrijpen uit de gedane mededeling.

7. Wij begrijpen voorts uit gedaagdes verweer dat dit de verder gaande strekking heeft dat eiser niet had mogen afgaan op de door de litigieuze zinsnede gewekte schijn.

Ook dit betoog faalt naar Ons oordeel.

Immers het feit - zoals door eiser gesteld en door gedaagde niet weersproken - dat het gebruik van de code waarvan onder 1 c) sprake is in samenhang met priemgetallen bij eiser zowel als gedaagde bekend was en naar eiser mocht veronderstellen ook bekend kon zijn bij een aantal ontvangers van eerdergenoemd proefschrift, omdat - naar hij onweersproken stelt - dit gebruik van genoemde code in samenhang met priemgetallen een soort standaardgrap is van de broer van eiser en gedaagde, de hooggeleerde H.W.Lenstra, jr., welke laatste zich er regelmatig van placht te bedienen ter gelegenheid van lezingen voor wiskundigen, waaronder ontvangers van het proefschrift en in sommige gevallen gedaagde, alsmede het feit dat de in de litigieuze zinsnede genoemde bedragen van een voor de gemiddelde wiskundige bevatelijke omvang kunnen worden geacht, leiden tot de conclusie dat eiser op de door gedaagde opgewekte schijn mocht afgaan. Dit klemmt te meer nu het van algemene bekendheid is dat tenminste één stelling van een proefschrift een humoristisch karakter dient te hebben.

8. Tenslotte voert gedaagde nog aan dat eiser geen belang heeft bij de vordering nu het mededingen naar een prijs in casu niet beantwoordt aan de formaliteiten van de Loterijwet, zodat uitbetaling van de hoofdprijs niet in rechte afdwingbaar zou zijn. Wij kunnen ons ook met dit verweer niet verenigen omdat - daargelaten of de Loterijwet eisen stelt aan de onderhavige loterij - er toch in ieder geval voor

gedaagde een natuurlijke verbintenis overblijft tot het uitbetalen van de "feestpriemprijs".

9. Eisers vordering is derhalve toewijsbaar.

10. Ten overvloede zij opgemerkt dat deze zienswijze ook strookt met recente rechtspraak van ons hoogste rechtscollege waarin een gelijk-luidend gemotiveerd vonnis van een Onze ambtgenoten, waarbij een hoogleraar tot f 10.000,- schadevergoeding werd veroordeeld omdat hij een collega had uitgemaakt voor "1492023920", als niet onbegrijpelijk en voldoende aan de eraan te stellen motiveringseisen werd beschouwd; dat voorts volgens vaste rechtspraak vonnissen, zoals het te dezen te wijzen, aan het slot waarvan de namen van rechters in vorenbe-doelde code worden vermeld niet strijden met hetgeen daaromtrent in artikel 59 lid 2 van het Wetboek van Burgerlijke Rechtsvordering is bepaald.

11. Gedaagde wordt te dezen in de kosten van het geding veroordeeld als de verliezende partij.

Wij hechten eraan op te merken dat naar Ons oordeel de gehele pro-cedure als overbodig is aan te merken, gelet op het inferieure karak-ter van gedaagdes weren.

R E C H T D O E N D E :

1. Beveelt gedaagde om binnen een maand na betekening van dit vonnis over te gaan tot aanwijzing van de winnaar van de "feestpriemprijs" in het bijzijn van eiser of diens gemachtigde, op verbeurte van een dwangsom van f 44,45 voor elke dag dat hij aan dit bevel niet vol-doet.

2. Verklaart dit vonnis tot zover uitvoerbaar bij voorraad.

3. Veroordeelt gedaagde in de kosten van het geding aan de kant van eiser tot op heden begroot op f 2.463,- , waaronder f 250,- wegens griffierecht.

Gewezen door mr 062803281201212301011819, fungerend president van de arrondissementsrechtbank te Amsterdam, en uitgesproken ter open-bare terechtzitting van donderdag 13 september 1984 in tegenwoordig-heid van de griffier.

Coll.: <handtekeningen c.q. paraaf: *>

<*) reproductie om formele redenen niet toegestaan >

Het Boek Van Vader En Moeder Geit

gescreven
door anjen
plaatjes door
anjen.

deel 1

deel 1.....de wolf

deel 2.....op reis

deel 3.....naar het bos

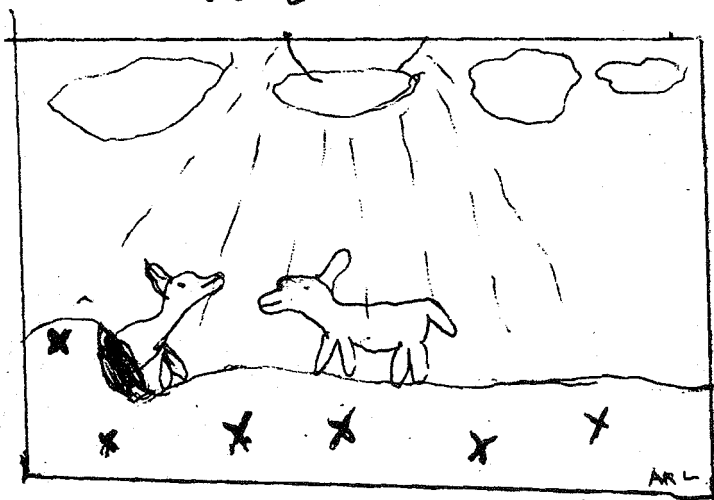
deel 4.....trip en trap

deel 5.....de jagen

deel 6.....naar school

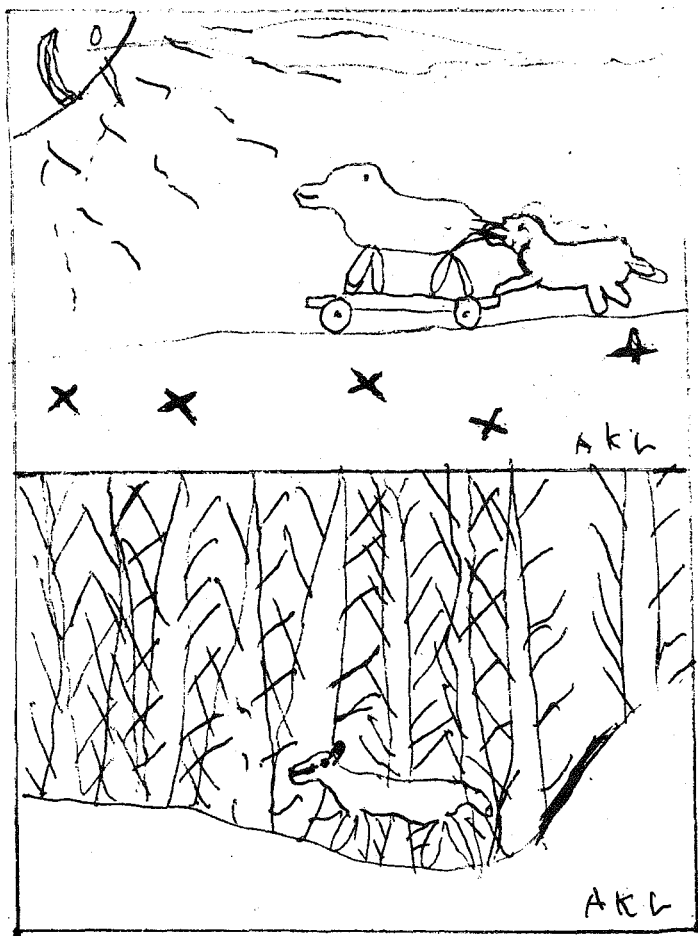
hoofdstuk 1 op de wei

Op een grote wei daar
wonen een vader geit en
en een moeder geit. En in
het bos daar woonde de wolf.
De geiten wonen er niet
gerustig. De geiten die
hebben van een val van de
wolf een hol gemaakt. De
wolf eek haken en kringen.
De geiten eten gras. De wolf
wil de geiten opeten. Hij kan
ze niet krijgen. Hun opaas en
omaas wonen in groningen by
een boer.

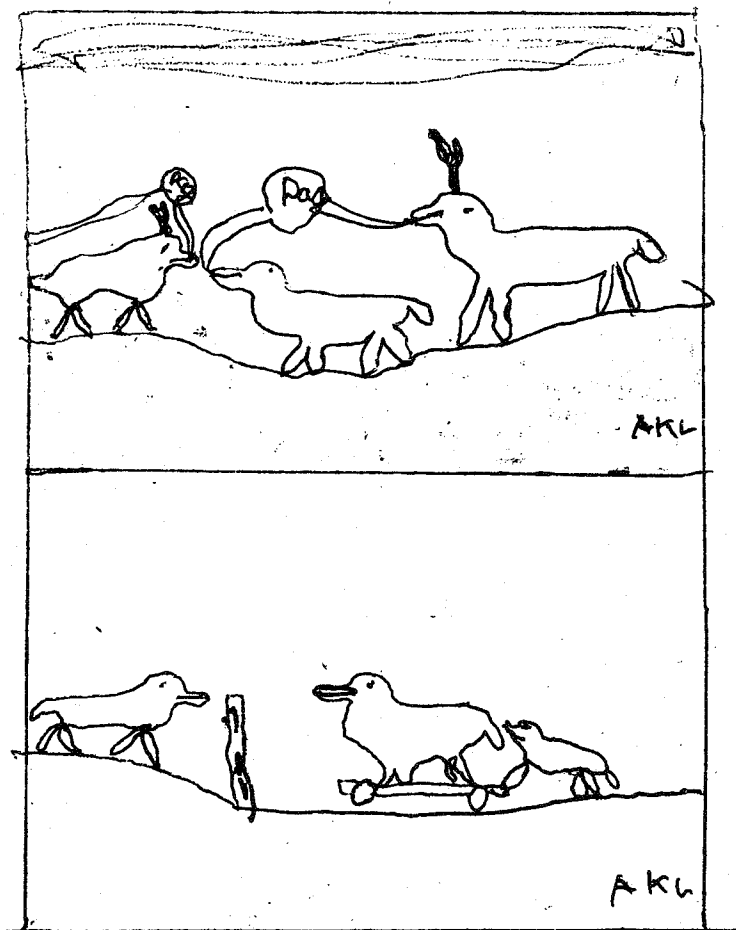


ARL

ze gaan er wel eens
met een oude kar naar
toe. hij wonen er 300 meter
van af.

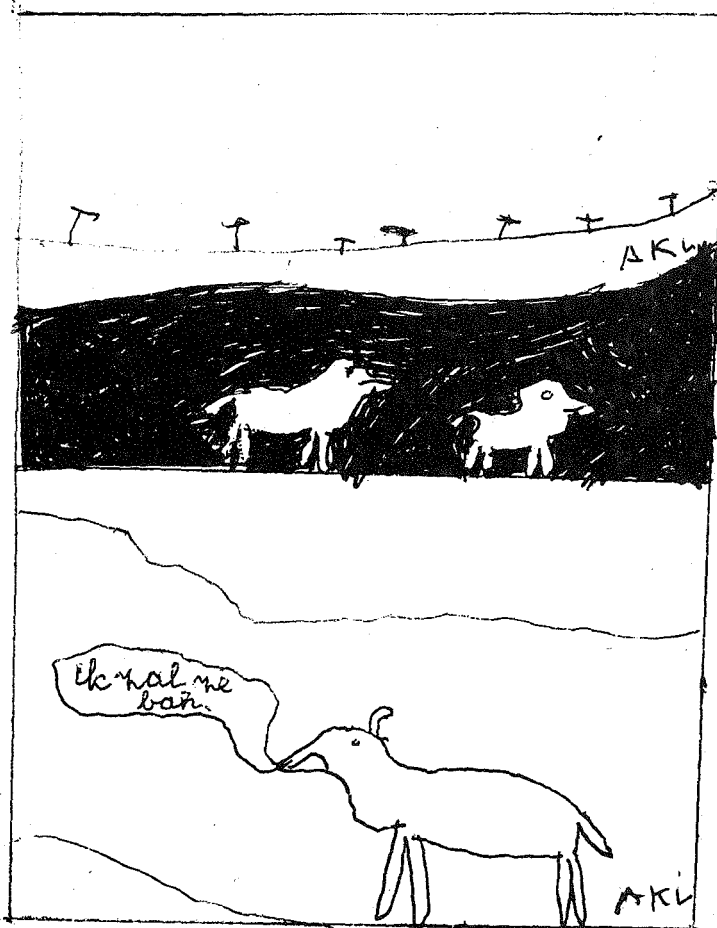


De boer kent 'ne wel.
Hij weet wel dat het
familie is. daarom
mogen 'ne bij 'em op de
wee.



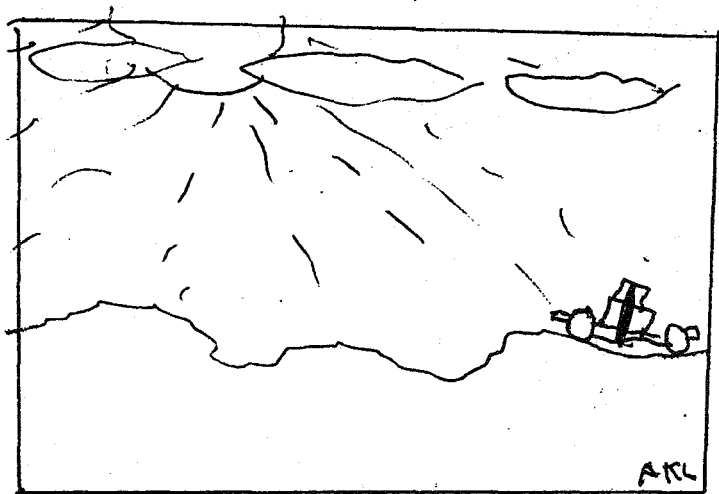
Maan ne rijn in hun hol.

De wolf nit boos in rijn
hol. De geiten nikken blij
in hin hol. ne nikkengras
te eten in hun hol



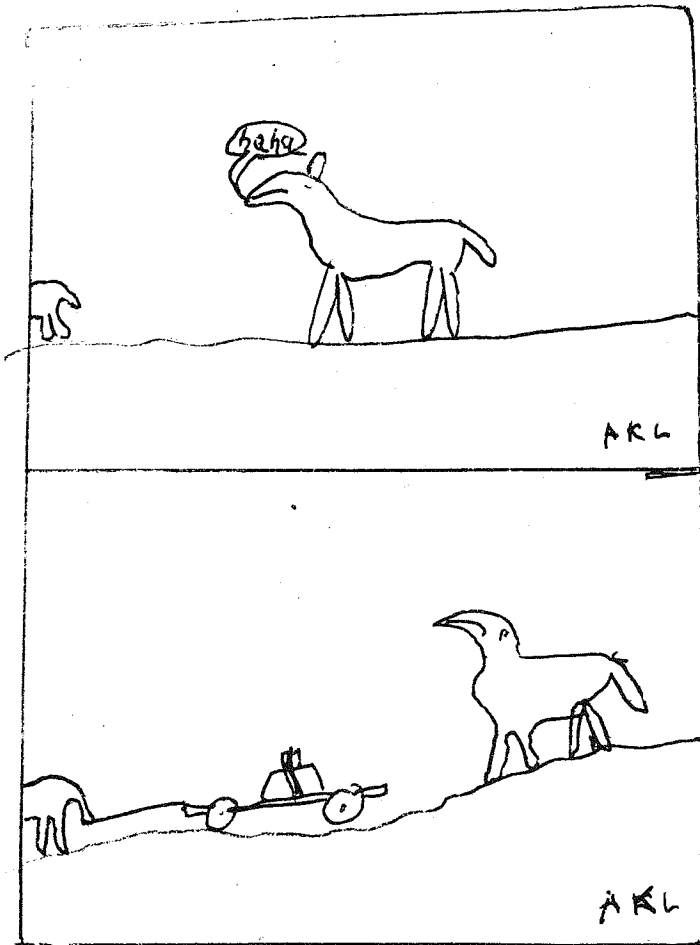
als het eten op is dan zegt
papa welk we over 10 weken
naar opa en oma gaan. ja!!!!!!

hier zijn de koffers. ik ga
al vast inpaken. goet.
ik weet wat we gaan over 10 da-
gen. ja!! dat doen we. waar zijn
jou kleren. hier. ik maak de
kar met een paar spijkers.
en dan maak ik voor de koffers
een paar riemen. voor ze
vast te maken.

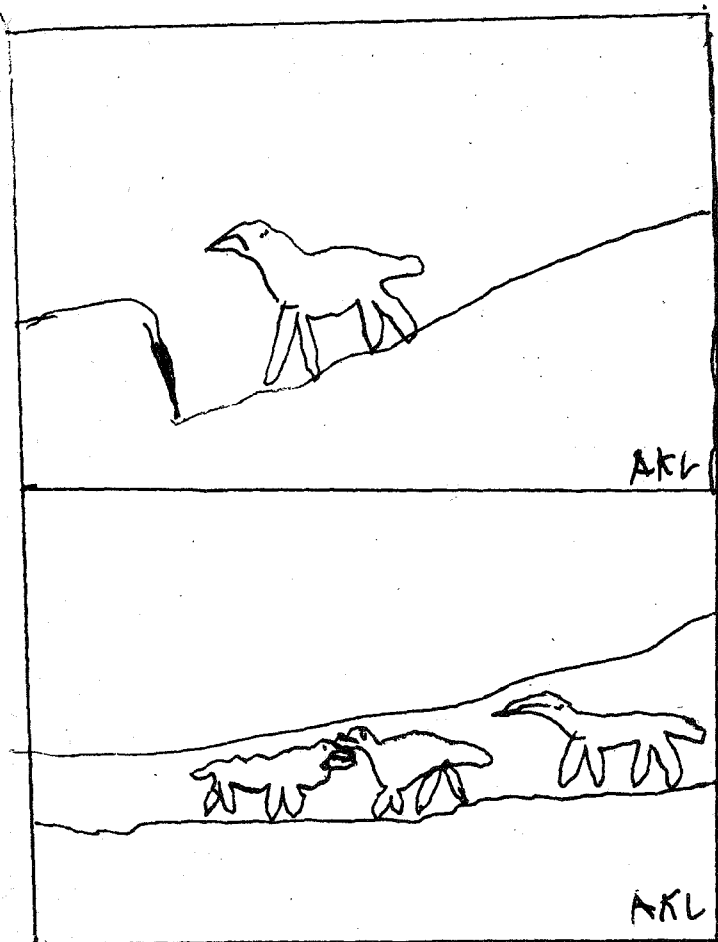


hoofdstuk twee
de wolf komt

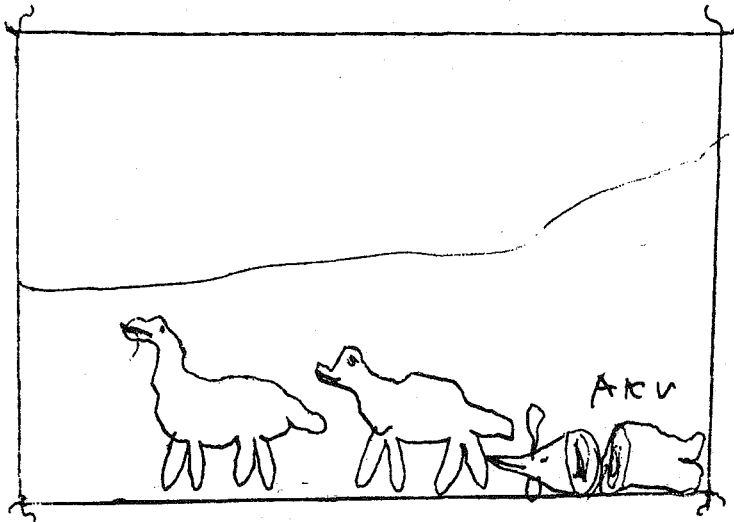
kijk daar komt de wolf
aan, in het hol gromm



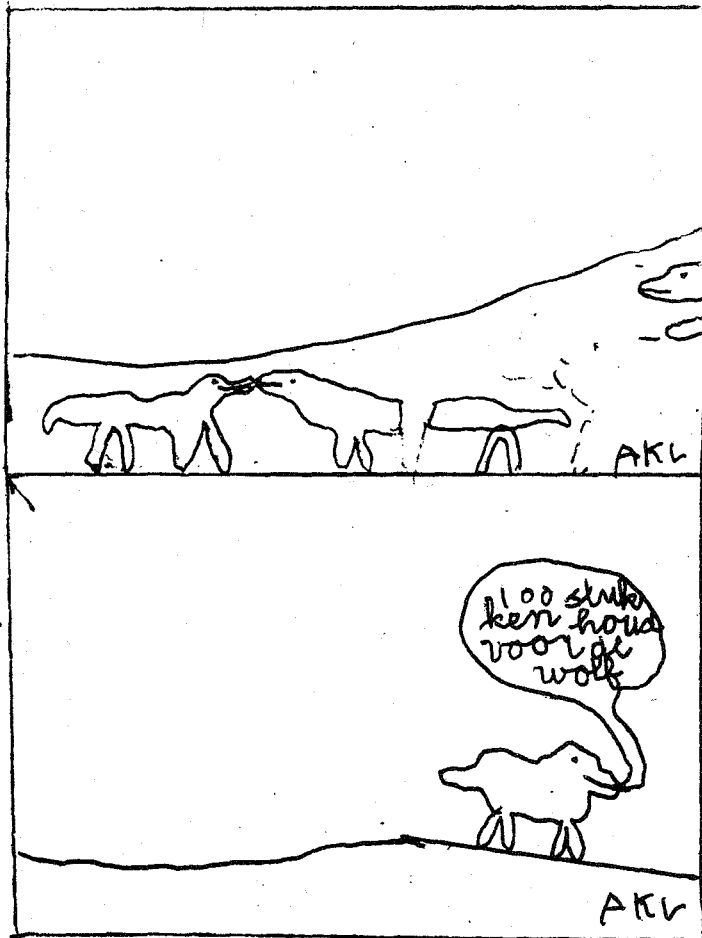
H₂H₂, dat was op het nippertje
help mij even met inpaken. Je
goed. nou ik ben benieuwd
hoe je het maken.



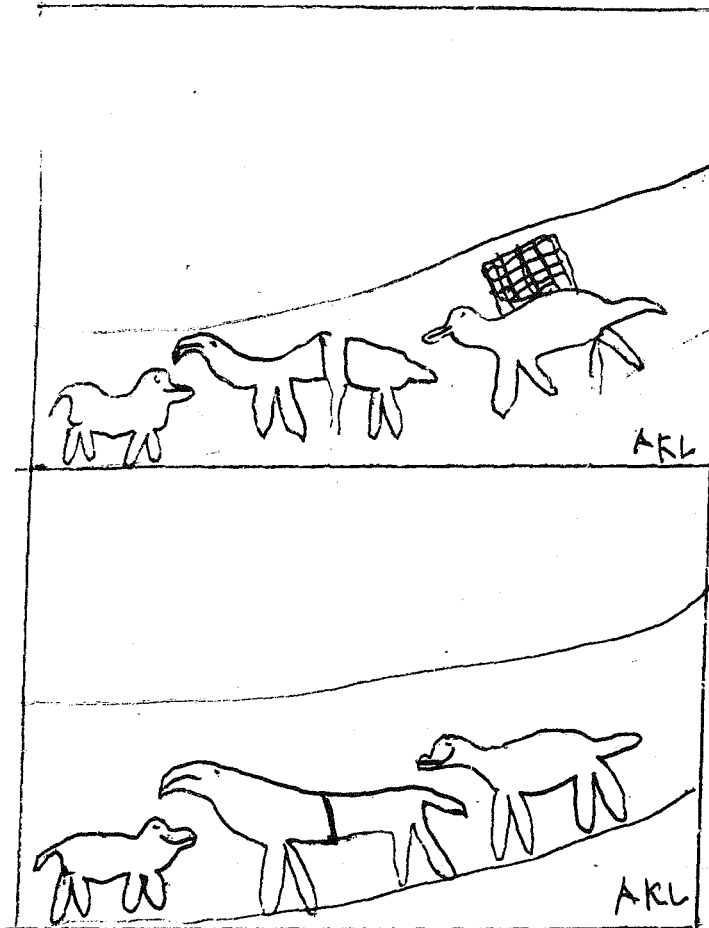
Maar de wolf wild ü
ons niet opeten. jawel ik
eek juli wel op HayHay.
ach waarom nou. HayHay
ik eek juli op HayHayHay,
nee nee, nee nee, ja ja, ja,
en hij al de vader geit
op. maar de moeder geit
had een mes. en sne de
slapende wolf door. en
de vader geit spronger
uit



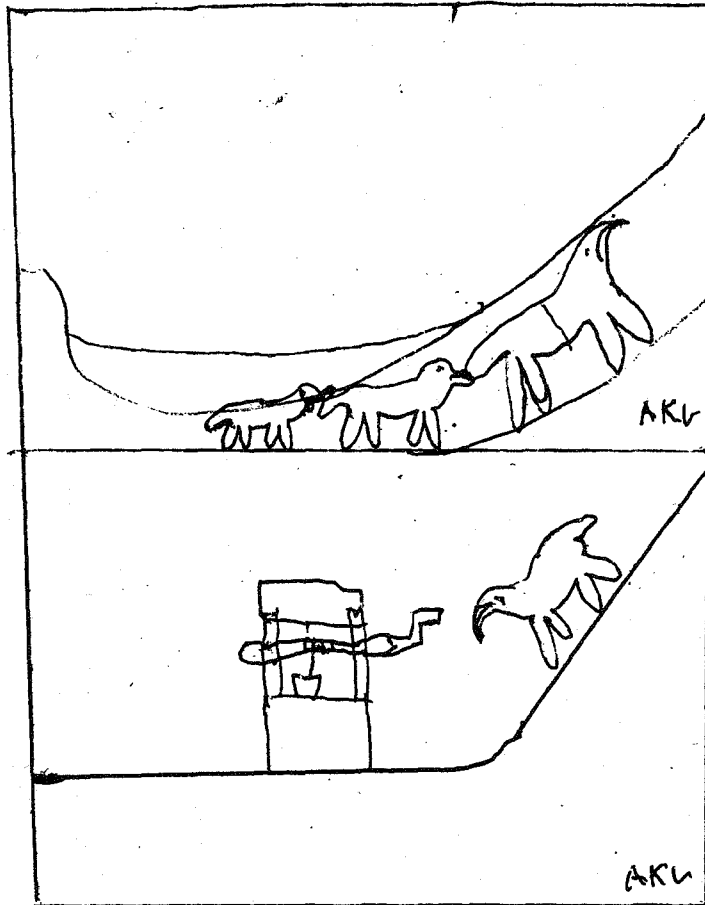
je doen in de buik van
de wolf een heleboel hout.
haal jij eens 100 stukken
hout. waarom? om in de buik
van de wolf te doen.



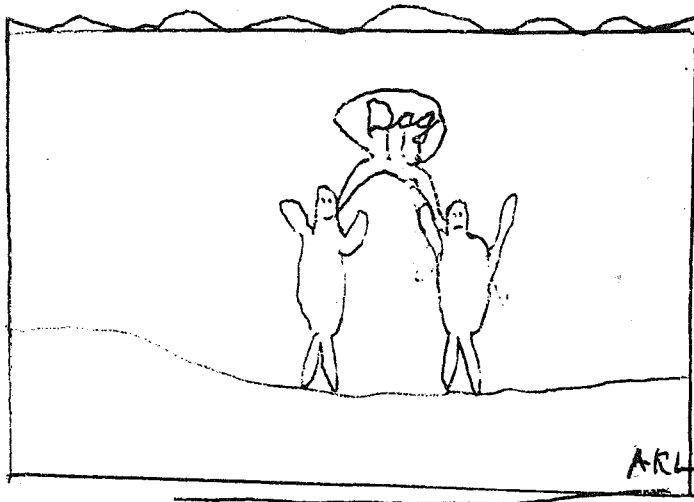
goed ik ga al 100 he ja.
3 uur gaat om
he waarom komt hij nou.
de wolf is dood. HayHayHa,
nu rilt hij het is van
de andere kant



haa ben je daan kom maar
gamme hier. De wolf is nu
lood: noo ny weer bigt mae
jen



no nu is het al dicht nu
moeten wij hem waker
maken. waarom, dan gaat
hij eten en dan knold hij
uitelkaar. ja. nou ga er
maar op stomppen goed.
stomp maar ~~stomp~~ door.
no nu is hij waker. hij
loopt al weg



het eerste boek is uit



Het gekke huis

C.M. Lenssen.

Er was eens een huis dat al 60 jaar stond!

Het riep altijd: boe, boe, boe,!

Alle mensen die voorbij kwamen zeiden: wat gek dat dat huis kan praten!! Weet je

wa-er mee dat huis was?? Dat huis was

een prins die betovert was door een heks.

Weet je waarom? Die prins had een klein

meisje geholpen. Over 100 jaar zou hij

weer een mens worden. Op een dag

kwam de heks langs, ze kreeg er spijt

van! Ze vond het niet eerlijk van haar!

Die prins had het meisje geholpen. Het was

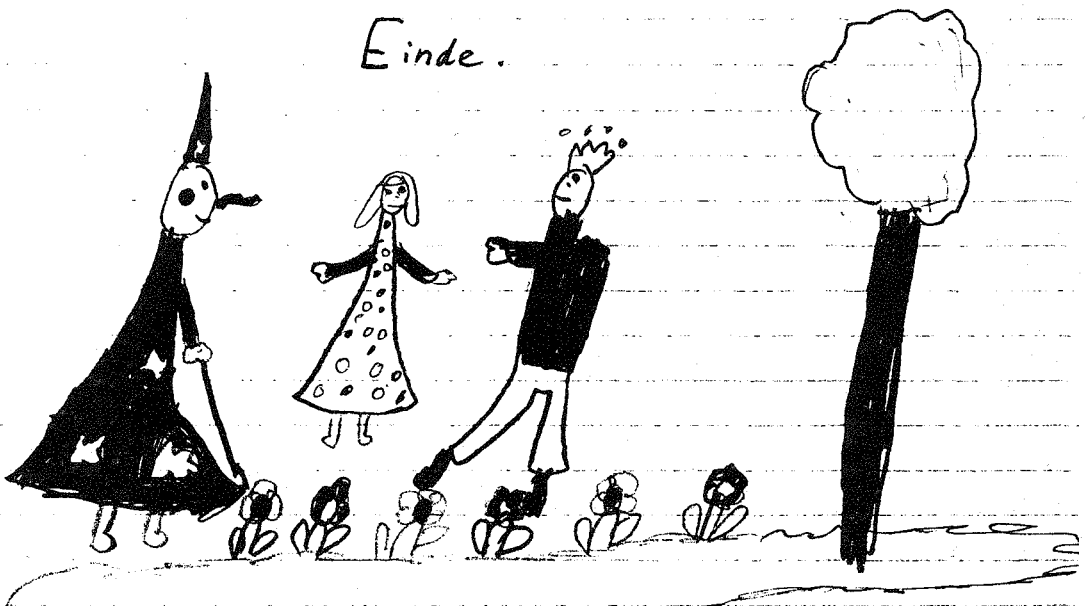
juist heel aardig van die prins! Ze besloot

om de prins heel gauw terug te veranderen!

Toen de prins terug veranderd was zei de

heks: het spijt me heel erg dat ik je
veranderd heb! Eens was ik heel
dom! Het geeft niet zei de prins.
Wand ik ben ook wel eens dom!
Het meisje kwam ook langs en zei
tegen de prins: bedanke dat je me
geholpen hebt! Toen zei de prins:
Het is Toch nog goed afgelopen!

Einde.



Arjen,

Je laat veel opera door je proefschrift lopen, begrijpelijk.
Maar hoe zou het zijn, als er eens een opera kwam over
priemgetallen?

Misschien werd het ongeveer zo...

Oom Gerben.

Molto vivace.



Tenor. ff
Wat is hier op aar-de ge-lijk aan een

Bass I. ff
Was gleicht wohl auf Er-den dem Jü-ger-ver-

Bass II. ff
The joy of the hunt-er on earth all sur-



priem-ge-tal? Niets is van meer waarde in't gan-se heel-al. Wie

gü- gen, wem spru- delt der- Be- cher das Le- bens so reich? Heim

pass- es, The foun- tain of- plea- sure for him doth a- bound, Thro'



zal mij be- let-ten er- steeds naar op- acht te gaan. Ik hoor de trom-

Klan- ge der Hör- ner im Grü- nen zu lie- - gen, den Hirsch zu ver-

wood and thro' flood, where the stag flits and pass- es, He flies in pur-



pet-ten geef mij maar ruim baan. Wat geeft het een vreugde, dit
 fol - gen durch Di - ckicht und Telch, ist fürst - li - che Freu - do, ist
 suit while the horns gai - ly sound. Oh this is a plea - sure that

man- lijk ver- lan-gen; Naakt goed wat niet deugde, het zout in de
 mün- lich Ver - lan - gen, er - stür - ket die Gie - der und wür - zet das
 princ - es might en - vy, For health and for man - hood the chief of de -

pap. Het staat als een rots en is niet te ver- van-gen, een
 Mahl. Wenn Wäl - der und Fel - sen uns hal - lend um - fan - gen, lät
 lights, 'Mid e - choes re - ply - ing, when day - light is dy - ing, To

bzui-sen-de bron, waar ik steeds weer uit tap. Jo ho, tra la la, la la
 frei - er und freud'-ger der vol - le Po - kal. Jo ho, tra la la, la la
 rest and the wine - cup our la - bor in - vites. Then hark, fol-low hark, fol-low

4 or 8 SOLO VOICES.

la, la la la, la la
hark, follow hark, fol-low

la, la la la, la la
hark, fol-low hark, fol-low, fol-low, fol-low,

la, la la la, la la
hark, follow hark, follow

CHORUS in unison.

la, la la la, la la la, la la la, la la la, la la
hark, follow hark, follow hark, follow hark, follow hark, follow hark, follow hark, follow

la la, la la la, la la
fol-low, fol-low hark, fol-low

la, la la la, la la
hark, fol-low hark, fol-low, fol-low, fol-low,

la, la la la, la la
hark, follow hark, follow

la, la la la, la la
hark, follow hark, follow hark, follow hark, follow hark, follow hark, follow hark, follow

la la, la la la, la la
fol-low, fol-low hark, follow hark,

la, la la la, la la
hark, follow hark, hark, follow hark, fol-low, fol-low

la, la la la, la la la, la la la, la la la, la la la, la la la
hark, follow hark, follow hark, follow hark, follow hark, follow hark, fol-low, fol-low

la, la, la la la, la la
hark, hark, fol-low hark, fol-low, fol-low, fol-low,

la, la la la la, la la la, la la la, la la la, la la la, la la
hark, hark, fol-low hark, fol-low hark, fol-low hark, fol-low hark, fol-low hark, fol-low

[illegible][illegible]

lal hark!

lal hark!

Tutti

ff

[illegible]

Tenor.
Laat slegfried zijn Zwaard Par-si-fal nu de Graal, Ik priem mij ge-
maar, gun

Bass I.
Di - a - na ist - kun - dig die Nacht su er - hel - len, wie la - bend an
Di - a - na by - night doth li - lu - mine her bow - er, Where oft we are

Bass II.

tal - len en ga aan de haal, Ik breng ze on - deelbaar te -

Ta - ge thr Dun - kel uns kühlit, Den blu - ti - gen Wolf and den
shel - terd from day's an - gry glare, We know in what cav - erns the

rug naar mijn ch fer-slot het zijn er wel veel, maar het kan niet ka -

E - ber zu fäl - len, dor gie - rig die grü - nen - den Saa - ten durch
wolf flies to caw - er, We fol - low the boar to his dark, wood - ed

pot. Wat geeft het een vreug - de, dit manlijk ver - lan gen? Maakt

wüht, ist fürst - li - che Freu - de, ist männ - lich Ver - lan - gen, er -
laß. Oh this is a plea - sure that princ - es might on - vy, For

[illegible]

la, la la la,
hark, fol-low hark,
la, la la la,
hark, fol-low hark,
la, la la la la
hark, fol-low, fol - low
la, hark,

la, la la la, la la la, la la la, la la la, la la la la la, la,
hark, fol-low hark, fol-low hark, fol-low hark, fol-low hark, fol-low, fol - low hark,

[illegible]

The musical score is written for a vocal soloist and a piano accompaniment. The key signature is one sharp (F#), and the time signature is 4/4. The vocal part begins with a melodic line in the treble clef, starting on a G4 and moving through various intervals to reach a high G5. The lyrics are: "la, hark, la la fol - low hark, la la, fol - low, la la, fol - low, la la, fol - low, la la, fol - low". The piano accompaniment consists of two staves. The right hand plays a steady eighth-note pattern in the treble clef, while the left hand plays a similar pattern in the bass clef. The overall mood is solemn and reverent.

KRACHTIGE MEETKUNDE

H.W. Lenstra sr., Oosterhout N.-B.

Het wiskunde-programma dat in het voortgezet onderwijs wordt aangeboden is in de loop van de tijd vaak en aanzienlijk veranderd. Het blijft een moeilijke zaak bij de vaststelling hiervan recht te doen aan alle ter zake doende argumenten, b.v. berustende op latere toepassing bij studie of werk, op „vormende” waarde (wat het dan ook vormt), beschikbare tijd, enz., enz.

Vrijwel verdwenen uit het onderwijs zijn de vroeger belangrijk gevonden puzzel-achtige vraagstukken uit de vlakke meetkunde. Voor de meeste leerlingen hadden deze weinig nut, maar vooral de in wiskunde betere leerlingen beleefden aan het oplossen er van vaak veel genoeg. Dikwijls werd geprobeerd regels te leveren, die moesten helpen op het goede idee te komen; hier zijn hele leerboeken aan gewijd.

Zo werden voor het type vraagstuk: bewijs dat die en die drie rechte lijnen door één punt gaan, verschillende manieren aanbevolen om te proberen. Het kan natuurlijk - en dat is er van overgebleven - „analytisch” en dan in de moderne uitvoering met behulp van de lineaire algebra. Maar andere methoden waren b.v.:

1. Vastgesteld werd dat de rechten a , b en c achtereenvolgens puntverzamelingen zijn met de eigenschappen A , B en C (vroeger heetten dat „meetkundige plaatsen”). Wanneer dan kon worden bewezen dat een punt met eigenschappen A en B ook de eigenschap C heeft, was de zaak rond. B.v. een deellijn van een hoek van een driehoek is de verzameling van punten binnen de driehoek die gelijke afstanden tot de benen van die hoek hebben. De preciese uitwerking van deze gedachte laten we graag aan de geïnteresseerde lezer over, gelijk wij ook zonder nader excuus in het volgende nog wel zullen doen, wetende dat het ware genoeg bij de beoefening van de wiskunde zit in het „zelf vinden”, althans in de illusie daarvan.

2. Men zoekt een eigenschap van het punt op a , waar deze door b wordt gesneden en ook één van het punt, waar a door c wordt gesneden. Dit is b.v. de verhouding waarin een lijnstuk op die lijn door dat punt wordt verdeeld. Zo verdelen de zwaartelijnen van een driehoek elkaar in de verhouding $1 : 2$. Dus (zie boven) enz.

3. Men laat zien dat de lijnen in kwestie op te vatten zijn als lijnen waarvoor het verlangde al is bewezen. B.v. men kan bewijzen dat de hoogtelijnen van een driehoek door één punt gaan door een andere driehoek aan te geven, waarvan deze hoogtelijnen de middelloodlijnen zijn.

De bedoeling van dit stukje is de aandacht te vestigen op een wel grappige manier om het door één punt gaan van drie rechten te bewijzen met behulp van de mechanica. Wanneer namelijk drie krachten elkaar opheffen, dan liggen hun werklijnen in één vlak en gaan door één punt (of ze zijn evenwijdig!).

In plaatje 1 b.v. zijn 6 krachten getekend, die elkaar 2 aan 2 opheffen. Wanneer de twee in hetzelfde punt aangrijpende krachten telkens worden samengesteld, komen er 3, elkaar dus opheffende, krachten te voorschijn met de deellijnen van de hoeken van de driehoek als werklijnen, zodat deze door één punt gaan.

Zie in plaatje 2 hoe het door één punt gaan van de drie zwaartelijnen van een driehoek kan worden bewezen.

In plaatje 3 zijn op de zijden van de driehoek AKL buitenwaarts de vierkanten $AKCB$, $KLED$ en $LAGF$ getekend. H , J , Q , M , N en P zijn de middens van de zijden van de zeshoek $BCDEFG$. Te bewijzen is, dat de rechten HM , QP en NJ door één punt gaan.

Aan de lezer het plezier, dit met behulp van de 4de aangegeven methode uit te werken. Ietwat ongeduldige oplossters die „op de kop” kunnen lezen, maken gebruik van de onderstaande aanwijzingen.

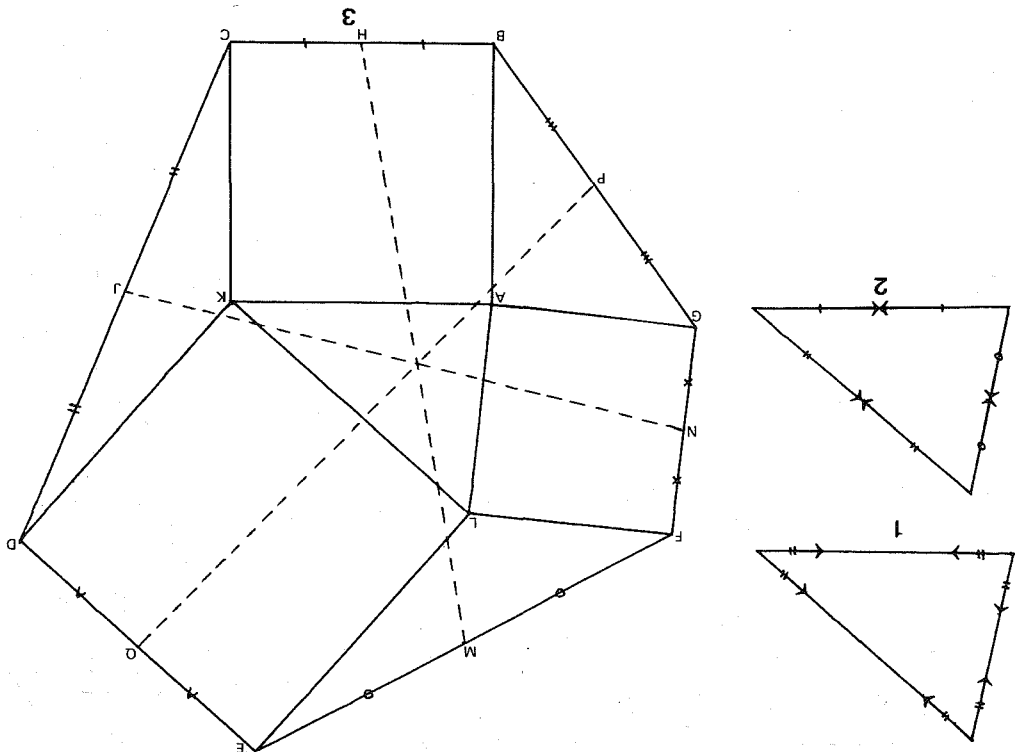
Wordt daardoor snel om hals gebracht;

Een vraagstuk aangepakt met kracht

Zij u gewijfd met deze leer:

Dit opstel, Zeer Geleerde Heer,

Aanwijzing: Neem 9 krachten als uitgangspunt: 3 met het zwaartepunt als aangrijppingspunt en in grootte door de lengten van de zwaartelijnen gegeven, 3 met het middelpunt van de omgeschreven cirkel als aangrijppingspunt, de middelloodlijnen als werklijnen en in grootte door de halve lengten van de zijden gegeven, en 3 met het hoogtepunt als aangrijppingspunt, de hoogtelijnen als werklijnen en in grootte door de lengten van de zijden gegeven. Veel genoeg!



BIOLOGISCHE INFORMATICA

J.A. Lenstra & B.A. Huitema.

Erfelijke eigenschappen worden bepaald door lineaire volgordes van basen in DNA, het erfelijk materiaal in (haast) alle vormen van leven. Door de technische vooruitgang in de moleculaire biologie kan men DNA-volgordes zo snel bepalen, dat de elektronische verwerking van deze informatie steeds belangrijker wordt. Er is behoefte aan een nieuwe discipline, de biologische informatica.

Moleculaire informatie

In de biochemie wil men levensverschijnselen verklaren vanuit de structuur, functie en interactie van moleculen. Wij bestaan uit de volgende chemische componenten: heel veel water, wat anorganische zouten, een groot aantal verschillende kleine organische moleculen (b.v. suiker, melkzuur), koolhydraatketens, vetten en tenslotte heel veel verschillende eiwitten en nucleïnezuren. De laatste twee groepen zijn verreweg het meest interessant. Eiwitten zijn actief betrokken bij haast alle moleculaire levensprocessen, zoals de katalyse van metabolische reacties (enzymen) en het transport van zuurstof door het bloed (hemoglobine). De beide soorten nucleïnezuren DNA en RNA zijn minder betrokken bij de stofwisseling, maar fungeren als dragers van erfelijke informatie. We kunnen de manier waarop deze informatie is opgeslagen en door het organisme wordt gebruikt als volgt samenvatten:

1. Het erfelijk materiaal bestaat uit DNA (met uitzondering van RNA-virussen), opgebouwd uit twee strengen die om elkaar heen zijn gewikkeld, de zg. dubbele helix. Beide strengen zijn lineaire polymeren van basen. Er zijn vier verschillende basen, afgekort met A, C, G en T. De erfelijke informatie wordt gespecificeerd door de volgorde van basen. De volgordes in beide strengen zijn complementair: tegenover elke A in de ene streng zit een T in de andere, tegenover elke G een C. De totale hoeveelheid informatie varieert per organisme, b.v. 4 miljoen basenparen (bp) voor een bacterie en 3 miljard bp voor een haploïd menselijk genoom (verdeeld over 23 chromosomen).

2. Vóór de celdeling wordt het DNA gerepliceerd: beide ketens laten elkaar los en worden ieder voorzien van een nieuwe complementaire streng. Elke dochtercel krijgt een halfnieuw, dubbelstrengs DNA-molecuul. Op deze manier wordt de volledige erfelijke informatie aan elke nieuwe cel en generatie doorgegeven.

3. Eiwitten bestaan uit lineaire ketens van aminozuren. Er zijn 20 verschillende aminozuren. Door zich op een zeer specifieke manier op te vouwen vormt de keten een compacte structuur. De lineaire aminozuurvolgorde bevat de informatie voor deze manier van opvouwen, die op zijn beurt weer essentieel is voor de (b.v. structurele of katalytische) functie van het eiwit.

4. De aminozuurvolgorde van een eiwit wordt bepaald door de basenvolgorde in een bepaald stuk uit het DNA, het gen. Drie opeenvolgende basen vormen een codon. Met 4 verschillende basen zijn er 64 verschillende codons, die ieder bij één bepaald aminozuur horen of het einde van de eiwitketen aangeven (de genetische code; de meeste aminozuren hebben dus meer dan één codon).

5. RNA speelt een centrale rol bij de overdracht van informatie van DNA naar eiwit. Het bestaat uit een enkele lineaire keten van basen, die slechts weinig verschillen van de basen in DNA: A, C, G en U (i.p.v. T). Tijdens de synthese van RNA dient DNA als zg. 'template': Eerst worden ter plaatse van de genen de beide DNA-strengen van elkaar gescheiden. Vervolgens worden de RNA-basen de één na de ander met elkaar worden verbonden, waarbij tegenover elke base in één van de DNA-strengen de complementaire RNA-base komt. Dit proces, transcriptie, zorgt er dus voor dat de informatie van bepaalde delen uit het DNA in RNA terecht komt.

6. RNA waarin de aminozuurvolgorde van een eiwit is gecodeerd heet boodschapper-RNA, mRNA. Daarnaast zijn er verschillende andere soorten RNA. De meeste hiervan zijn vrij klein, hebben net als eiwitten een compacte opvouwing en vervullen, samen met eiwitten, een katalytische functie bij de overdracht van informatie. De belangrijkste zijn de transfer-RNA's, tRNA's.

7. In 1976 deed men de belangwekkende ontdekking, dat bij eukaryoten (organismen met een celkern, dus alle soorten behalve bacteriën) de transcriptie vaak wordt gevolgd door splicing: het RNA wordt ingekort door bepaalde delen, de introns, eruit te knippen en de uiteinden van

de overblijvende exons aan elkaar te koppelen. In het gen kan de rij van codons dus een aantal malen worden onderbroken: 'split genes'. Het hoe en waarom hiervan is nog onduidelijk, behalve dat het tijdens de evolutie heeft geholpen bij het ontstaan van nieuwe eiwitten.

8. Eiwitten worden gesynthetiseerd door translatie van mRNA. Eerst worden de losse aminozuren elk gekoppeld aan een bijbehorend tRNA. tRNA bevat een anticodon, dat kan binden aan het complementaire codon op het mRNA. Vervolgens wordt in een cyclisch proces de aminozuren door het tRNA overgedragen aan de keten van aminozuren die door de vorige tRNA's werden afgeleverd.

Het ontcijferen van eiwit en RNA

Voordat kan worden begonnen met het achterhalen van de informatie die in een bepaald molecuul is opgeslagen, moet dat molecuul eerst zuiver en in voldoende hoeveelheden voorhanden zijn. Eiwitten zijn heel vaak op grond van specifieke eigenschappen (b.v. hun grootte, lading of hydrofobiciteit) met redelijk gemak te zuiveren. Met behulp van de zg. Edman-degradatie kan men dan vanaf één uiteinde de aminozuurresiduen stuk voor stuk verwijderen om vervolgens te identificeren. In gunstige gevallen kan men de volgorde van de eerste 50 aminozuren bepalen. De meeste eiwitten zijn groter; de volledige volgorde kan men (proberen te) achterhalen door het eiwit in discrete brokstukken, peptiden, te splitsen, deze te zuiveren en ze te onderwerpen aan de Edman-degradatie. De volgorde van de fragmenten volgt dan uit een tweede, verschillende manier van splitsen. De procedures zijn moeizaam en tijdrovend; 10 manjaar voor 400 aminozuren is heel gewoon.

Bij de zuivering van RNA en DNA zijn er veel minder mogelijkheden. Nucleïnezuren hebben allemaal ongeveer dezelfde chemische en fysische eigenschappen en verschillen onderling alleen in lengte. Een tweede probleem is, dat er te weinig van de meeste nucleïnezuren aanwezig is om ze te kunnen zuiveren: ca. 2 genen per diploide cel en ca. 15 kopieën van de meeste mRNA's. Ten derde zijn de meeste DNA moleculen veel te lang om ze te kunnen hanteren en analyseren.

Om deze redenen was tot in de jaren '70 de informatie over nucleïnezuurvolgordes beperkt tot de kleine RNA-moleculen waarvan veel aanwezig is, de vrij kleine DNA's of RNA's uit virussen en een enkele

mRNA. De moeizame volgordetechnieken die hierbij werden gebruikt zijn goeddeels verouderd.

Het lezen van DNA

De eerste stap naar betere tijden was het ontdekken van een hele serie verschillende restrictie-enzymen, voor bacteriën een wapen tegen vreemd (viraal) DNA, voor ons een hulpmiddel om DNA in discrete brokstukken te knippen. Restrictie-enzymen herkennen een palindromische volgorde van vier, vijf of zes basen en leveren dus brokstukken van gemiddeld 256 tot 4096 basenparen. Hierdoor konden hanteerbare en manipuleerbare DNA-moleculen worden geschapen: dankzij restrictie-enzymen deed DNA zijn intrede in de moleculaire biologie (sensu stricto).

De twee overgebleven problemen, de kleine hoeveelheden waarin één bepaald nucleïnezuurmolecuul aanwezig is en de grote hoeveelheden ander DNA en RNA, werden uit de wereld geholpen door een tweede doorbraak, de ontwikkeling van recombinant-DNA-technieken. Hierbij wordt gebruik gemaakt van plasmiden, kort circulair DNA in bacteriecellen, dat samen met het grote bacteriële DNA-molecuul wordt gerepliceerd. Plasmiden zijn heel eenvoudig te zuiveren en kunnen weer in de bacteriecel naar binnen worden gebracht; dit laatste heet transformatie. Men kan ook een plasmide openknippen met een restrictie-enzym, de beide uiteinden koppelen aan de uiteinden van een vreemd DNA-fragment en met het nieuwe molecuul cellen transformeren. Het vreemde DNA wordt dan samen met het plasmide door de bacterie gerepliceerd. Doet men dit met een heterogeen mengsel van DNA en verdeelt men na de transformatie de bacteriën over een agarplaat, dan zal de volgende morgen elke kolonie afstammen van één individuele cel en één bepaald vreemd DNA-fragment bevatten; dat DNA is dan gekloneerd. Na het opsporen van de juiste kolonie -dit kan nog heel lastig zijn- is het groeien van de kloon in grote hoeveelheden, het isoleren van het plasmide en het zuiveren van het ingebrachte DNA geen probleem meer.

In plaats van plasmiden worden ook heel vaak fagen gebruikt. Fagen zijn bacteriële virussen, subcellulaire vormen van leven die cellen binnendringen en zich daar laten vermenigvuldigen. Hierdoor wordt de

bacteriecel gelyseerd of in zijn groei geremd, zodat men na transformatie niet moet zoeken naar kolonies, maar naar plaques (negatieve kolonies).

Om RNA-volgordes te weten te komen kan RNA worden overgeschreven naar zg. kopie-DNA (cDNA) via 'reverse transcription'.

Na wat verdere manipulaties kan de bacterie er toe worden gebracht met het ingebrachte DNA mRNA te maken, gevolgd door de productie van een -technologisch mogelijk interessant- eiwit.

Intussen was de tijd rijp voor twee zeer snelle methoden om DNA-volgordes te bepalen, methoden die al het vorige in de schaduw stelden. Beide methoden maken gebruik van de mogelijkheid om met elektroforese (migratie ten gevolge van een elektrisch veld) in een gel enkelstrengs DNA moleculen met een lengte van 1 tot ca. 500 basen van elkaar te scheiden. De posities van al die fragmenten na elektroforese worden aangeduid met banden, het geheel van banden een ladder. Banden worden gedetecteerd door de DNA-moleculen van te voren van een radioactieve label te voorzien en door na de elektroforese een röntgenfilm op de gel te leggen.

In de ene methode, de chemische degradatie van Maxam & Gilbert, wordt eerst een DNA fragment aan één uiteinde voorzien van een radioactief atoom. Dit fragment wordt dan onderworpen aan een behandeling die willekeurig achter een klein deel van alle G's splitst, dus b.v. in het ene molecuul achter de G op de vierde positie, in een ander achter de G op nummer tien en in een derde wellicht achter allebei (let wel, het dan ontstane fragment 5 - 10 is niet radioactief). Na elektroforese is band nummer vier alléén radioactief als zich op positie vier inderdaad een G bevindt, met andere woorden, de radioactieve ladder geeft de posities van alle G's aan. De posities van de andere basen krijgt men op vergelijkbare wijze door partieel achter de andere basen te splitsen.

In de tweede methode (van Sanger) wordt tegen een enkelstrengs DNA-fragment een klein stukje complementair DNA, de primer, geplakt. Voegt men het DNA-replicatie enzym, DNA-polymerase, toe samen met de bouwstenen dATP, dCTP, dGTP en dTTP, dan wordt de primer complementair aan de langere strand verlengd. Met een beetje radioactief dATP wordt de nieuw gesynthetiseerde streng ook radioactief (de radioactiviteit is bij deze methode niet essentieel, maar louter praktisch om de

fragmenten in de gel te kunnen detecteren). Voegt men behalve dATP ook een klein beetje van het analogon ddATP toe, dan wordt op elke A-plaats (d.w.z. tegenover elke complementaire T in het lange fragment) in een deel van de moleculen dit analogon ingebouwd. Dit heeft tot gevolg dat de synthese ter plekke wordt gestopt, dus in het ene molecuul op A op plaats 4, in het ander pas op nummer 24. Na de elektroforese zullen dan banden nummer 4 en 24 radioactief zijn. Behalve ddATP hebben we ook ddCTP, ddGTP en ddTTP, zodat vier ladders de hele basenvolgorde opleveren (zie Fig. 1).

Deze methode geeft de mooiste resultaten, maar had tot voor kort het praktische nadeel dat het DNA enkelstrengs moest zijn en dat ook een primer moest worden geïsoleerd. De chemische degradaties werken net zo goed op dubbelstrengs DNA, zolang maar één uiteinde een radioactief atoom draagt. Met een nieuwe sprong voorwaarts werden deze nadelen van de methode van Sanger opgeheven. Dubbelstrengs DNA wordt gekloneerd in een bepaalde faag, M13, die zo vriendelijk is het DNA enkelstrengs op te leveren; weer laten we de natuur het werk doen. Dat DNA bestaat dan uit het voor ons interessante deel gekoppeld aan het M13-DNA, zodat we elke keer dezelfde primer kunnen gebruiken, en wel een fragment complementair aan de M13-volgorde.

Behalve elegant is het zg. M13-sequenzen zo eenvoudig geworden, dat het evenwicht moest worden hersteld met een allermint elegante, tijdrovende maar wel effectieve procedure: 'shotgun sequencing'. Een groot DNA-fragment, b.v. 10.000 bp, wordt in verschillende porties met verschillende restrictie-enzymen in kleine stukjes geknipt, waarna de mengsels van fragmenten in M13 worden gezet en over een bacterieplaat worden verdeeld. De recombinant-virussen, die ieder een bepaald fragment bevatten, worden blind opgegroeid en onderworpen aan de volgorde procedures. Dit gaat zo snel, dat de meeste tijd gaat zitten in het lezen en verwerken van de gels, soms wel 30 per week. De volgordegegevens worden elektronisch opgeslagen en verwerkt tot een zoveel mogelijk aaneensluitende volgorde. Hiermee gaat men door tot men er genoeg van heeft alleen nog maar bekende gegevens nog een keer te bevestigen, waarna men wat meer gericht de gaatjes gaat vullen. Reken toch maar op een manjaar voor 10.000 basen.

Gelukkig wordt er gewerkt aan meer intelligente procedures om een groot stuk DNA gericht over een aantal M13-fagen te verdelen. Men zou

dan een tempo van minstens duizend basen per week kunnen halen.

Volgordes in de computer

De molecuulair-biologische technieken zijn in korte tijd zo effectief geworden, dat ze eigenlijk meer informatie opleveren dan we aankunnen. We hebben net al genoemd hoe computers werden ingeschakeld om een totale volgorde uit de volgordes van overlappende fragmenten af te leiden. Uiteraard blijft het daar niet bij. Veel toepassingen van computers zijn heel simpel, zoals het voorspellen van de aminozuurvolgorde en het localiseren van herkenningsplaatsen van restrictie-enzymen. Ook kan men op zoek gaan naar bepaalde volgordes die een rol spelen bij de transcriptie en de translatie of naar stukken repeterende volgorde met de zg. Z-conformatie (een links-i.p.v. rechtsdraaiende dubbele helix). Men schrikt echter zeker niet terug voor meer ambitieuze analyses. Helaas leveren deze in de regel wat minder duidelijke resultaten op. Zo wordt er van alles geprobeerd om in eukaryotisch DNA te voorspellen waar introns in exons overgaan. Hoewel deze plaatsen in vivo heel snel en nauwkeurig worden gevonden door de moleculen die zich met splicing bezig houden, is er nog geen algoritme voor. Een tweede nog niet opgelost probleem is het voorspellen van de intramoleculaire complementaire basenparing in de kleine compacte RNA-moleculen. En dan zwijgen we nog maar over de onuitroeibare pogingen om met slecht werkende algoritmen de ruimtelijke structuur van eiwitten af te leiden uit hun aminozuurvolgorde.

Wat veel beter schijnt te lukken is de localisatie van nucleosomen. Nucleosomen bestaan uit een kern van eiwitten omwikkeld door 146 bp eukaryotisch DNA. Volgens sterke aanwijzingen bevat de DNA-volgorde de signalen die de exacte plaats van de nucleosomen langs de DNA-keten aangeven. Deze structurele boodschap in het DNA heeft tot nu toe echter nauwelijks aandacht gekregen.

Twee toepassingen van computers hebben het meest bijgedragen tot een beter begrip van biologische processen. Nieuwe volgordes kunnen elektronisch worden vergeleken met de snel in aantal toenemende bekende volgordes. Een paar keer werden onverwachte overeenkomsten - met verstrekkende consequenties- aan het licht gebracht. Verder kan

men de evolutie van een bepaald molecuul reconstrueren door homologe volgordes te vergelijken, iets wat met eiwitten al veel langer gebeurt.

Computers kunnen meer

Uit het laboratorium komen steeds mooiere gels, computers kunnen er steeds meer mee doen, maar nog onveranderd worden de gels met het oog gelezen en met de hand in de computer ingevoerd. Dit is tijdrovend (in feite: snelheidsbeperkend), onnauwkeurig en zeer vermoeiend. Kan dat niet automatisch? Zeker niet, volgens deskundige biochemici, er zijn teveel artefacten en problemen met de achtergrond die om een deskundig oog vragen. Zeker niet eenvoudig, net zo min als b.v. het automatisch lezen van handgeschreven cijfers, maar toch vast niet onoplosbaar? Het zou de moleculair-biologen veel hoofdpijn besparen.

Als met de nodige investering van tijd en geld een volgorde volledig is bepaald, is het natuurlijk de moeite waard alle informatie die erin ligt opgesloten te achterhalen. De vertaling van DNA- naar eiwitvolgorde is natuurlijk niet zo moeilijk, maar we willen meer. We noemden al de pogingen om de opvouwing van kleine RNA-moleculen, intron-exon-overgangen en de localisatie van Z-DNA en nucleosomen te weten te komen. Met het probleem om de ruimtelijke structuur van eiwitten te voorspellen wordt al zo lang vruchteloos geworsteld, dat we voorlopig veel plezier zouden kunnen hebben van een minder ambitieuze benadering, het gebruik van homologieën.

Van een aantal eiwitten heeft men met röntgendiffractie de ruimtelijke structuur kunnen bepalen. Heel vaak blijkt een nieuwe aminozuurvolgorde een aantal overeenkomsten te hebben met de volgorde van één van die eiwitten, hetgeen meestal betekent dat hun ruimtelijke structuren geheel of gedeeltelijk ook overeenkomen. Bij het opsporen van volgorde-overeenkomsten, die lang niet altijd in het oog springen, kunnen computers zich al nuttig maken. In principe moet dan een ruimtelijke structuur met wat elektronisch passen en meten met de nieuwe volgorde en de oude structuur kunnen worden bepaald. Met name immunologen zouden met zoiets heel blij (moeten) zijn.

Computers, een apart vak

Mogen we verwachten dat alle mogelijkheden zullen worden benut om de informatie die is opgesloten in de basenvolgorde van DNA eruit te halen? Helaas, de tijd lijkt er nog niet rijp voor. Natuurlijk, er wordt van alles gedaan. Tenslotte loopt er op elke afdeling wel een computerfanaat rond.

Waarschijnlijk geeft deze laatste zin de problemen al voor een groot deel weer. Het gebruik van computers is een randgebeuren in de moleculaire biologie. De computerspecialisten werken teveel geïsoleerd, zonder de stimulerende interactie die de experimentele moleculaire biologie kenmerkt, variërend van uitwisseling van gegevens tot meedogenloze kritiek en harde competitie. Zo krijgen de problemen die een betere informatieverwerking in de weg staan, als ze al worden onderkend en als ze al behoorlijk worden gedefinieerd, niet de aandacht die ze verdienen.

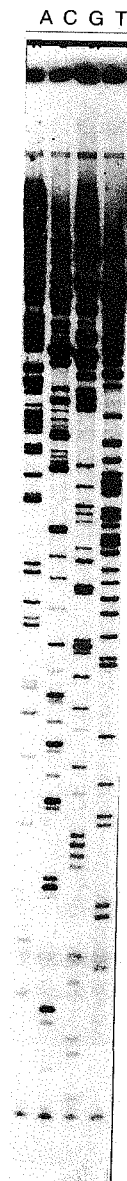
Laten we echter één ding vooropstellen: de molecuulair-biologen treft geen blaam. Zij hebben hun aandeel ruimschoots geleverd en zetten nog steeds vol ijver en inventiviteit hun beste beentje voor. Het zou onredelijk zijn ook nog eens van hun te verlangen dat ze kunnen beoordelen wat er achter de terminal gebeurt. Mocht daar een vooruitgang worden geboekt, dan is voor de computerman een eenzaam tevreden moment de beloning, misschien gevolgd door een weinig gelezen publicatie. Het is ook onvermijdelijk dat de experimentele collega's nogal eens de neiging hebben computers, hoe slecht ook geprogrammeerd, te beschouwen als orakels, hetgeen de ontwikkeling van betere programma's ook niet ten goede komt.

De problemen roepen om de aandacht van de kant van de wetenschap die zich op professioneel niveau met de verwerking van informatie bezighoudt: de informatica. Er zou al veel zijn gewonnen als de problemen in exacte termen werden gedefinieerd of als eens duidelijk werd, wat de kwaliteit is van de diverse in gebruik zijnde algoritmen. Het zou mij niet verbazen als zou blijken dat sommige problemen, indien juist geformuleerd, in feite al waren opgelost. Het zou ook zeker niet de eerste keer zijn dat mensen met een andersoortige opleiding zich op originele en vruchtbare wijze met de biochemie gingen bezighouden.

Gezien de hoeveelheid werk dat er ligt te wachten is er ruimte voor aparte werkgroepen, misschien niet aan elke universiteit maar zeker één in Nederland. Een stel ambitieuze promovendi en studenten, gerecruteerd uit de informatica en uit de biochemie -pas op, anders gaan ze voor je het weet hun eigen doelen najagen, kijk maar naar de theoretische biologie- en het schatgraven in de moleculair-biologische databanken kan beginnen.

Literatuur

Nucl. Acids Res. 12 (1984), 1-856.



Figuur 1. Weergave van een autoradiogram van een DNA-volgordegel. De kleinste fragmenten zijn tijdens de elektroforese het verst gemigreerd en vormen banden onderin de gel. Zie de text voor nadere uitleg.

De figurant

"Eusam, eusam, gentlefree homasjefiboy!" De lezer zal zich onmiddellijk afvragen waar dit over gaat. Wel, dit behelst een soort bezwering die Arjen lang, lang geleden bezigde om in verschillende situaties zijn gemoedstoestand uit te drukken. Toen onze oudere broers hun kennis van de Engelse taal begonnen op te doen, deden wij, Arjen en zijn drie jaar oudere zuster, dapper mee. Hij zal vijf en ik acht jaar geweest zijn toen wij onder het uitstoten van bovenstaande kreten de buurt rond de Kraneweg in Groningen onveilig maakten. Dan speelden we "Hang Kang", een soort diefje met verlos, waarbij Arjen heftig zwaaiend met zijn grijze, plastic zwaard mij op de hielen zat. Ik zou trouwens nu nog best te porren zijn voor een spelletje Hang Kang, al weet ik niet zeker of het bij Arjen nog van harte zou gaan.

Over mijn jongere broer kan ik een boekwerk vol herinneringen schrijven. We trokken, als de twee jongsten, veel met elkaar op. Zijn geboorte herinner ik me nog goed. Staande op mijn tenen kon ik net in de wieg kijken en daar ontwaarde ik een zeer klein rood hoofdje, een zwaaiend handje en een beginnend puntneusje. Ik beschouw Arjen nog steeds als "mijn kleine broertje", behalve als hij in levende lijve voor me staat; dan is de overgang tussen verbeelding en realiteit erg groot.

Ik zal mij in deze ontboezemingen trachten te beperken tot enkele voorvallen uit onze gezamenlijke jeugd; voorvallen waaruit ook zijn subtiële gevoel voor humor zal blijken. Nu al weer enige tijd geleden, ik meen in 1975, gingen wij met vakantie. Wij, dat zijn Arjen, mijn echtgenoot en ik. De fietsen werden in de trein geladen om een halve dag later, samen met ons in Limoges te worden uitgeladen. En vanaf dat punt ging het heuvel op, heuvel af. Tenminste dat was de bedoeling. Slechts 300 meter vanaf het station had Arjen te kampen met bandenpech. Geen probleem. Vijf minuten later stooft hij alweer, met wapperende manen, de eerste serieuze heuvel op. Aangeland op de top hield hij in om zijn reisgezelschap te aanschouwen. Helaas, zijn zwager zwoegde halverwege, en zijn zuster stond schreiend aan de voet van de heuvel, want dat fietsen in Frankrijk afzien betekent, dat wist ze niet. Het echte afzien heeft zij overigens de rest van die vakantie niet geheel onder de knie gekregen, tot grote ergernis van haar broer. Waarschijnlijk heeft hij het hevig betreurd op pad te zijn gegaan met twee bejaarden. Toch bracht deze vakantie vele hoogtepunten op een ander vlak.

Na een fietstocht van twintig kilometer in de regen belandden wij laat in de ochtend in de stad Aurillac. Aldaar betraden wij, als drie verzopen katten, een hotel dat een sterke gelijkenis vertoonde met het Kurhaus. Het personeelslid achter de balie gaf door middel van zijn gelaatsuitdrukking te kennen ons niet kredietwaardig te achten, maar overhandigde toch een sleutel. Op onze kamer werd uit de plunjezakken de nette kleding opgediept. Na een warm bad schreden wij, op en top keurige lieden, de gigantische eetzaal binnen, nagestaard door een verbaasde balieklerk. Het menu van de heren omvatte vijf gangen maar na de tweede gang, genaamd "pounti" (geconcentreerd varkensvet, dat trouwens naar recept van Arjen met cacao en beschuutkruim héél smakelijk tot Arretje Nof is om te toveren) deed hen al de das om. De verdere attracties van Aurillac zijn voor ons verborgen gebleven.

Daags erna gingen wij uitgerust verder, om uiteindelijk terecht te komen in Lyon. Wij streken daar neer op een zonnig terras en Arjen en ik begonnen spoorlags aan ons geliefde spelletje: stilzwijgend namen wij aan dat het figurantenbureau weer zijn uiterste best had gedaan en bussen vol gewilligen voorbij liet paraderen. Aan ons de taak daar bekenden uit

op te pikken. Op die manier flaneerde onze hele kennissenkring voorbij. Mijn gade ergerde zich immer in stilte aan dit platvloerse vermaak. Totdat we hem uitdaagden. De stoïcijnse gelatenheid die van alle voor ons langs drentelende figuranten uitstraalde zou hij niet kunnen evenaren. Top! Dat zou hij wel even doen. Wij zaten met de rug naar het etablissement en rechts van het terras liep de rivier. Mijn gade zou links opkomen en als argeloze wandelaar voorbij lopen. Arjen en ik bestelden gezellig nog een whisky (vreemd genoeg was het in Frankrijk dat whisky zijn lijfdrank werd), en mijn levensgezel verwijderde zich. Omdat hij ongeveer dertig centimeter langer is dan de gemiddelde Fransman, zou hij trachten ietsje door de knieën te zakken.

Terwijl wij reikhalzend zaten uit te kijken naar een blonde batavier kwamen herinneringen boven over onze Franse bovenbuurman in Amsterdam. Deze man, mijnheer Duchêne, had de gewoonte zijn vrouw het leven zuur te maken; hun ruzies beëindigde hij steevast met een gillend "lâmstrááááál", waarna hij de trap afstootte, zijn vouwfiets voor onze gevel wegrukte en hoog op de wielen wegsputte. Zijn vrouw keek hem dan vanaf het balkon weemoedig na. Op een middag was het weer raak. Arjen en ik keken elkaar aan, liepen naar buiten en maakten de vouwfiets onklaar door alle moeren los te draaien. Zo op het oog leek het nog een respectabel rijwiel, maar toen de heer Duchêne met rode konen zijn pand verliet en het stuur naar zich toe rukte, bleef de rest van het vehikel staan. Scheldend monteerde hij het stuur, waagde opnieuw een poging en verloor na twee meter de trappers en nog wat andere onderdelen. Intussen waren wij slap van het lachen aan het badmintonnen (ons record is geloof ik 4086 slagen) maar het laatste "lâmstrááááál" gold ongetwijfeld ons. Vrolijkheid alom, daar in Lyon. Maar waar bleef onze reisgenoot? Het duurde toch wel erg lang. Misschien had hij de kans aangegrepen er op deze manier tussen uit te knippen (mijn suggestie), of was hij een pruikenwinkel gaan bezoeken om ons op een dwaalspoor te brengen (Arjen's suggestie).

Hoe het ook zij, wij konden in de verste verte niemand ontdekken die ook maar enigszins op het origineel leek. Wij waren dus al heftig bezig zijn inventiviteit en acteertalent te prijzen. Het figurantenbureau staat voor niets! Nog een whisky besteld en we werden steeds vrolijker. Wederom gingen onze gedachten terug in de tijd. Toen Arjen eind-examen deed aan het Vossius Gymnasium waren mevrouw Tuin (mijn moeder) en ik aanwezig bij de diploma-uitreiking. Terwijl Arjen zijn papieren in de hand kreeg gedrukt van de 206 cm lange rector Van der Raa, mijn vroegere conrector van de HBS, zei ik tegen mijn moeder: "Wat is Van der Raa toch lang, hè?", waarop zij tot mijn stomme verbazing antwoordde: "Ja, maar er zitten dooie puntjes aan!" Dat Arjen zijn diploma kreeg terwijl zijn familie luidkeels stond te schateren had dus niets te maken met de waardering voor zijn intellectuele prestaties, doch met het feit dat mijn moeder verstond: "Wat is Arjen's haar toch lang, hè?"

Opeens verscheen in onze rechter ooghoek een hijgend, puffend en roodaangelopen manspersoon, die moeilijk door de knieën lopend en opzij spiedend voor het café langs spurtte. Alles viel op aan hem, het meeste nog zijn snelheid, alsof hij door een winkeldetective op de hielen werd gezeten. Test mislukt. Achteraf bleek dat hij, om ons te misleiden, niet links had willen opkomen, maar door gauw even het blokje achter het café om te lopen rechts het toneel had willen betreden. Echter, het blokje bleek een totale omtrek van anderhalve kilometer te hebben. Arjen zelf slaagde daarna met vlag en wimpel. Met een uitgestreken smoel, zich aanpassend aan zijn omgeving, niet op- of onkijkend, gleed hij langs ons heen. Zo was er geen lol aan te beleven. Ik riep nog in de hoop hem enige emotie te ontlokken, "Eusam, eusam, gentlefreet homasjefiboy", maar helaas.....

Willemien Lenstra

PAS DE PROBLÈMES

"Kleine tutzorgjes van Mevrouw Tuin? Leg de boot maar in het dok."
Geen probleem.

Dat waren de eerste opmerkingen toen mevrouw Slagschip en Arjen samen in de auto een vacantietje gingen houden. Ieder ander lid van het gezin had bezigheden elders en zo kwam het dat het plan was geboren dat zij met zijn tweeën iets zouden ondernemen. Geen probleem.

"Jongen, kijk uit, hier moet je vijftig rijden. Wil je misschien wat lekkers?"

De zon scheen aangenaam, de auto ronkte goedmoedig, legde zich al van te voren neer bij al het onwaarschijnlijke dat van hem gevraagd zou worden. Hij herinnerde zich nog heel goed de "coup spécial" in Lille, die in zijn binnenste wel wat gerommel en pijn teweeg had gebracht; de bestuurder en de inzittenden zaten echter te gieren van de pret en dat deed de narigheid weer vergeten. Ook stond hem nog duidelijk voor de geest het vingervlugge nemen van de Corniches, op weg naar Monte Carlo. Dat was een kolfje naar zijn hand, al was hij op dat moment wel liever een sportmodel geweest. Pas de problème.

Beide inzittenden genoten van het "er even uit zijn". Het was ook druk geweest. Het kolenhok kuisen: een groots karwei uitgevoerd in het ochtendgloren; vroeg gewekt door de wekker, enkele kopjes thee, vooral niet te veel kleren aan en dan maar schrobben. Samen hadden ze het werk uitgevoerd; tevreden dat het geklaard was, spraken ze er nog even samen over. "En weet je nog van die stoelen? Dat was ook niet zo maar klaar." "Nee, mevrouw Kaashoofdje, maar het resultaat mag er zijn; gelukkig dat jij er niet te veel met je onhandige knopvingers aan gezeten hebt, want dan zouden we ze nu niet kunnen gebruiken." Ook de stoelen hadden na het kraaien van de haan stuk voor stuk een beurt ondergaan: nieuwe zittingen, vullingen, bespijkingen + sierknopjes. Geen probleem.

Al rijdend had een ieder zo zijn gedachten. Mevrouw Du Jardin zat de bestuurder eens even op te nemen: haar jongste, natuurlijk gruwelijk geplaaide, anderzijds misschien ietwat in de watten gelegde zoon, zat daar. Wat een tijd geleden dat hij, 's morgens om een uur of elf, op zijn stoeltje klom, het schemerlampje aanknipte, een blad klaar zette met één kopje, één beker en twee stukken koek en vervolgens aan de tafel ging zitten, afwachting wat er ging gebeuren. Dat was zijn ogenblik, alle groten naar school, alle aandacht was even voor hem alleen. De kleuterschool, die hij allerm minst vervelend vond, had een eind gemaakt aan dit ritueel. Ze zag hem nog voor zich hoe hij, helemaal ontdaan, naar huis kwam hollen; had zijn pantoffeltjes aangehouden en de risee van de klas zijn, leek geen prettig vooruitzicht.

Al voortsnorrend, zo nu en dan pauzerend, schoten ze lekker op. Een goede wandeling op de plaats van bestemming zou de stijfheid zeker doen verdwijnen. Geen probleem.

En dat werd een wandeling. Steil was het in het bos, glad waren de bladeren. Mevrouw Worstjes zag het soms niet meer zitten, maar aangemoedigd en geholpen kwam ook zij boven. Daar woei de wind met grote kracht. De uitkijktoren zou ongetwijfeld veel moois laten zien. Alleen Arjen waagde zich er op, zijn moeder durfde nauwelijks omhoog te kijken, met de toren mee zwiepte Arjen lustig in de harde wind. De terugtocht bood alleen maar gemak, "als je valt, ga je zitten." Helaas vergat hij zijn hoofd in de juiste positie te houden, zodat een flinke klap, bij even uitglijden, op zijn achterhoofd zijn deel werd.

De avondmaaltijd had natuurlijk weer een verrassing. Lopend door het dorpje was Arjen bij de slager een heerlijk gerecht, kalfskop, opgevallen. Laat dat nu net op het menu staan. Dat trof. Bij het diner kreeg mevrouw Knopvinger het ene smakelijke schaalkje na het andere; waar bleef de kalfskop? Het wachten werd beloond. En hoe! Onder een deksel, in een onduidelijke saus, lagen vellen, botten, ogen en drillerige vetmassa's Arjen toe te lachen. Eén hap werd gewaagd; beviel niet. Kom, niet direct denken dat het echt niet smakelijk is. De aanhouder won echter niet en Arjen kreeg van de andere schaalpjes een flinke portie. Maar hoe zich te ontdoen van de kalfskop? Vol de schaal terug naar de keuken, zou een belediging zijn. Geen nood. Vele lagen papieren zakdoekjes werden op schoot gevleid, steeds verdween een oog, vel of bot in de diepte; zacht warm voelde het opgerolde pakje aan, lekker lauw kwam het in de vuilnisbak op straat terecht. Geen probleem.

De volgende dag waren er geen bijzondere gebeurtenissen of het moest zijn dat de beklimming van de Mont d'Eutrope in Orange, laat op de avond, een aparte aanblik bood. Beiden waren moe, echter toch nog van plan wat te ondernemen. En wat is mooier dan in donker een onbekend pad te nemen dat naar de top leidt van een berg, die je alleen maar bij licht kent? De lange benen snelden voort, de hand hield een ceintuur vast, die aan de andere kant werd beetgepakt door Mevrouw Gordijntjesstijver, vallend over iedere oneffenheid. „Gaaf het wel?” Natuurlijk was het antwoord niet: „Eigenlijk niet.” Het gaat namelijk altijd, het moet altijd gaan. Boven aangekomen nog even een paar goede momenten met het fluiten van enkele operafragmenten, hiertoe geïnspireerd door de aanblik van het amfitheater aan de voet van de berg. Op die plaats dachten ze nog even aan een ander muziekgebeuren: om een, clandestiene, opname van een belangrijke opera-opvoering in Parijs te verkrijgen, had Arjen zijn mouw volgepropt met een microfoon, achter zijn benen stond apparatuur en zo was er het een en ander meer. Een eenvoudige opgave was het niet, maar tot volle tevredenheid kwam de opname tot stand. Geen probleem.

„Och mevrouw, dat kun je best.” Een aanmoediging, die met liefde werd aangehoord, als je wel eens niet precies wist, of iets wel in je macht lag. Hoe die opmerking onderweg opeens in de geest kwam van mevrouw Knopvingertje, is niet meer te achterhalen. Misschien zag ze voor zich het samen duwen, trekken, wringen, wurgen van de grote stoel door de te kleine deuropening aan de Eikenweg. Een enkel bemoedigend woord was nog meer op zijn plaats voor Arjen; half ziek voerde hij een verhuizing uit. „Ga jij nu maar even die kleedjes recht leggen, dan haal ik wel wat.” En hoe? Op het hoofd, een zwaar meubelstuk, vele trappen op. Geen probleem.

Onderweg werd natuurlijk steeds heerlijk gegeten. Maar: brood met geel overhemd, dat stond nergens op tafel. Is ook zeer af te raden; de presentatie kan goed zijn, de plaagzin kan tot zijn recht komen, de consument ergert zich zeer, de smaak evenwel is zeer, zeer slecht. Het leed, veroorzaakt door dit recept, aangedaan door het ene lid van het reisgezelschap aan het andere, in een ver verleden, was groot. Om een oordeel te vellen over dit volstrekt niet alledaags gebeuren is het echter nodig alle gegevens in een goede context te plaatsen, de historische bepaaldheid spreekt hier een woordje mee. Aangezien dit allemaal het zeer bescheiden karakter van dit werkje te buiten gaat, wordt er verder geen aandacht besteed aan dit ongewone gebeuren.

Aangezien Hein Mammerie Hoischap ook wel eens het stuur hanteerde, arriveerde het tweetal „sain et sauf” tijdig in het vaderland, blij weer thuis te zijn. Natuurlijk werd de avond gebruikt om in het bos nog een mooie wandeling te maken. Dat waren steeds uitgezochte gelegenheden om, al stappend door kuilen of over takken heen, mevrouw Zeurtje de pyramiden

van Egypte of de koningsgraven voor ogen te toveren. Deze reisdoelen waren eerder door Arjen bezocht en in beeldende taal zag mevrouw Boontjes de mooiste dingen voor het geestesoog. De Massada in Israël was volgens de beschrijving nog indrukwekkender dan in werkelijkheid. Doch hier bleef het niet bij op de wandelingen. Ging er een bejaarde, omvangrijke vriendin mee in het pikkedonker: geen probleem; onder luid protest werd deze door Arjen over een balk gehesen, een ware krachttoer. (De vriendin in kwestie is er nog niet over uitgepraat.)

De tochten in het bos leverden nog veel meer op. „Kent mevrouw Kneutertje de inhoud van die opera niet?" Zeer gedetailleerd volgde dan het hele libretto, afgewisseld met het fluiten van aria's. Soms was het wel eens zo donker dat een pad nauwelijks viel te onderscheiden. Een goed richtinggevoel hielp hen steeds weer op de juiste weg; eenmaal kon Arjen zijn beweringen omtrent de te volgen weg staven door de aanwezigheid van een van ijs voorziene kuil, op de heenweg gepasseerd. Sindsdien heet die plek: het plasje van Arjen. Misschien is het beter niet te memoreren de slee-experimenten in het Amsterdamse Bos, van de berg af. In hun ogen toen ware excursies. Eenmaal aangekomen op de top van de heuvel was een tochtje naar beneden een feest. Een bank kan dan lelijk in de weg staan. Gelukkig legde Arjen tijdig zijn hoofd plat, een groot geluk. Pas de problème.

Zoals gezegd was het tweetal gelukkig, weer op het uitgangspunt teruggekeerd te zijn. Pas de problèmes.

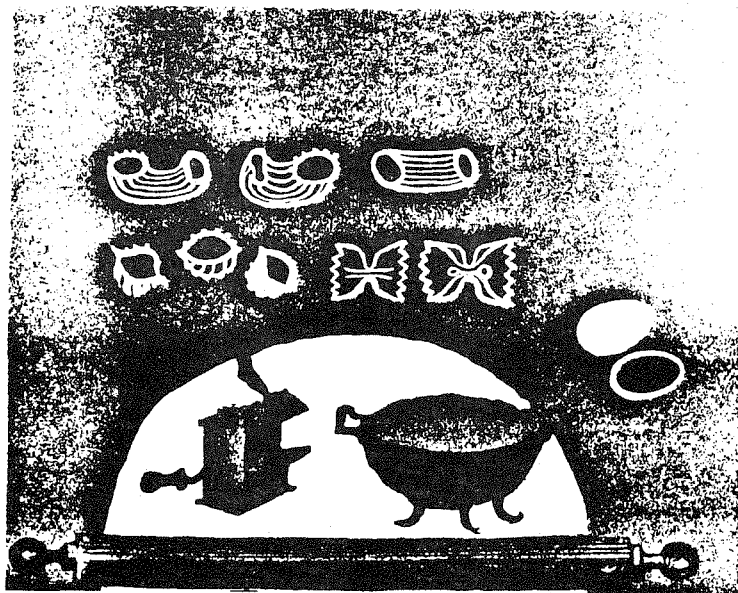
Mam pakt de bagage uit, zit nog alles eens te overpeinzen en denkt: Dat is geweest, dat was goed. Dank je voor alles.

Mam denkt aan de toekomst van Arjen, die nu „samen" is en vat dat wat komen gaat in het volgende citaat samen:

O Seligkeit, dich fass ich kaum!
Ihr Auge wird mir strahlen,
Ihr Himmelreis mir blühn.

Mam

Paste alimentari



Cottura delle paste alimentari

Saranno date istruzioni dettagliate anche nella stesura di buona parte delle ricette.

La cottura delle paste alimentari, di estrema facilità, richiede qualche attenzione. L'acqua deve essere anzitutto abbondante; c'è chi calcola $\frac{1}{2}$ litro per 100 gr., chi 1 litro. Noi consigliamo di avvicinarsi al litro, in quanto la pasta deve bollire in molta acqua per evitare sia il sapore colloso, sia il suo agglomerarsi. Per la stessa ragione sarà bene adottare recipienti di vaste proporzioni, naturalmente secondo la quantità della pasta in cottura. In linea di massima, salare l'acqua fredda in ragione di 10 gr. per ogni litro d'acqua.

La pasta verrà immersa quando l'acqua avrà raggiunto una piena ebollizione, non in un colpo solo, ma aggiungendola, poca alla volta, sparpagliandola con cura e mescolandola con continuità per evitare che spaghetti, fettuccine, ecc., s'incollino l'un l'altro. Far riprendere l'ebollizione, abbassare la fiamma e continuare la cottura a coperto, pur mescolando ogni poco.

Non è possibile dare il tempo di cottura in quanto, oltre che dalla qualità delle farine usate e dal tipo della pasta, occorre tener conto del gusto dei commensali. Il nostro consiglio è di cuocerle sempre al dente. A cottura ritirare dal fuoco (aggiungendo un poco d'acqua fredda per arrestarla) e far scolare la pasta, il più rapidamente possibile, in uno scolapasta. Servirla immediatamente.

Per paste cotte al burro e parmigiano è consigliabile tenere da parte qualche cucchiaiata di acqua di cottura da aggiungere, nell'eventualità che si attacchino tra loro, prima di servirle.

È abitudine condire le paste alimentari prima con la salsa e poi col formaggio (se serviti a parte); è un evidente errore tecnico. Prima cospargere il formaggio grattugiato, che al contatto con la pasta calda inizia a rapprendersi, poi la salsa a sua volta ben calda, quindi mescolare bene.

Paste all'uovo

PREPARAZIONE DELLA PASTA ALL'UOVO

Mettere a fontana sulla spianatoia 500 gr. di farina setacciata; rompere 5 uova in una fondina, sbatterle con una cucchiata d'olio e un pizzico di sale, rovesciarle nel centro della fontana. Lavorando con le dita, portare progressivamente la farina nel centro, poi, con ambedue le mani, lavorare la pasta sino ad ottenerne un impasto piuttosto sostenuto. Bagnare in acqua tiepida un panno bianco ben pulito, strizzarlo bene, avvolgerci l'impasto e farlo riposare per circa mezz'ora. Col matterello, tirarne sfoglie, più o meno sottili, secondo la loro destinazione. Per determinate preparazioni è preferibile impiegare un impasto « poroso » che si ottiene aumentando la quantità della farina e lasciando le sfoglie piuttosto spesse.

I diversi tipi

La pasta all'uovo, tirata in sfoglie più o meno fini, si presta per la preparazione di una larghissima gamma di tipi, a loro volta caratterizzati dalla forma e dal taglio. Ne citeremo qui alcuni, che si ritroveranno poi nelle relative ricette.

Tortellini, agnolotti, cappelletti, ravioli, cannelloni, tortelli, tortelloni, ecc. sono caratterizzati da un ripieno, la pasta è generalmente quella sopra descritta, può variare il numero delle uova e le sfoglie possono essere preparate più o meno sostenute. I cappelletti si differenziano dai tortellini per la maggiore grandezza.

L'impasto dei tortellini sia liscio e omogeneo, dopo un breve riposo sia steso in sfoglie ritraendone, col tagliapasta rotondo, dischetti di 4 cm. scarsi di diametro.

La sfoglia dei tortelli e dei tortelloni sia stesa sottilissima, sia lasciata riposare un'oretta, se ne ritraggano, col tagliapasta rotondo, dischi di 6-8 cm. di diametro. Verranno farciti e ripiegati in mezzelune.

A Genova si confeziona la pasta per ravioli, preparata generalmente come sopra descritto, adoperando per ogni chilo di farina solo tre uova, l'acqua necessaria e un pizzico di sale. La sfoglia dei ravioli si stende molto fine, si farcisce col ripieno messo a pallottoline o a mucchietti, con l'apposita rotella dentellata se ne ricavano dei quadrucci (v'è chi li prepara con altra forma) di circa 4 cm. per lato.

Gli agnolotti si confezionano e si farciscono come i ravioli, ma devono essere più grossi e di forma rotonda.

La pasta per cannelloni è generalmente quella sopra descritta; dalle sfoglie si ricavano pezzi di 10 cm. di lunghezza per 8 di larghezza; si cuociono in acqua bollente, abbondante e leggermente salata, si sgocciolano, si allineano sopra un panno bagnato ben strizzato e, prima dell'impiego, si fanno raffreddare.

Tagliatelle, dette anche fettuccine, lasagne, taglierini, ecc. si ricavano dalle sfoglie e vanno usati senza ripieno; si trovano anche in vendita già confezionati.

Tutti questi tipi differiscono tra di loro per la grandezza o la forma, raramente per l'impasto. Si troveranno le eventuali precisazioni nelle ricette.

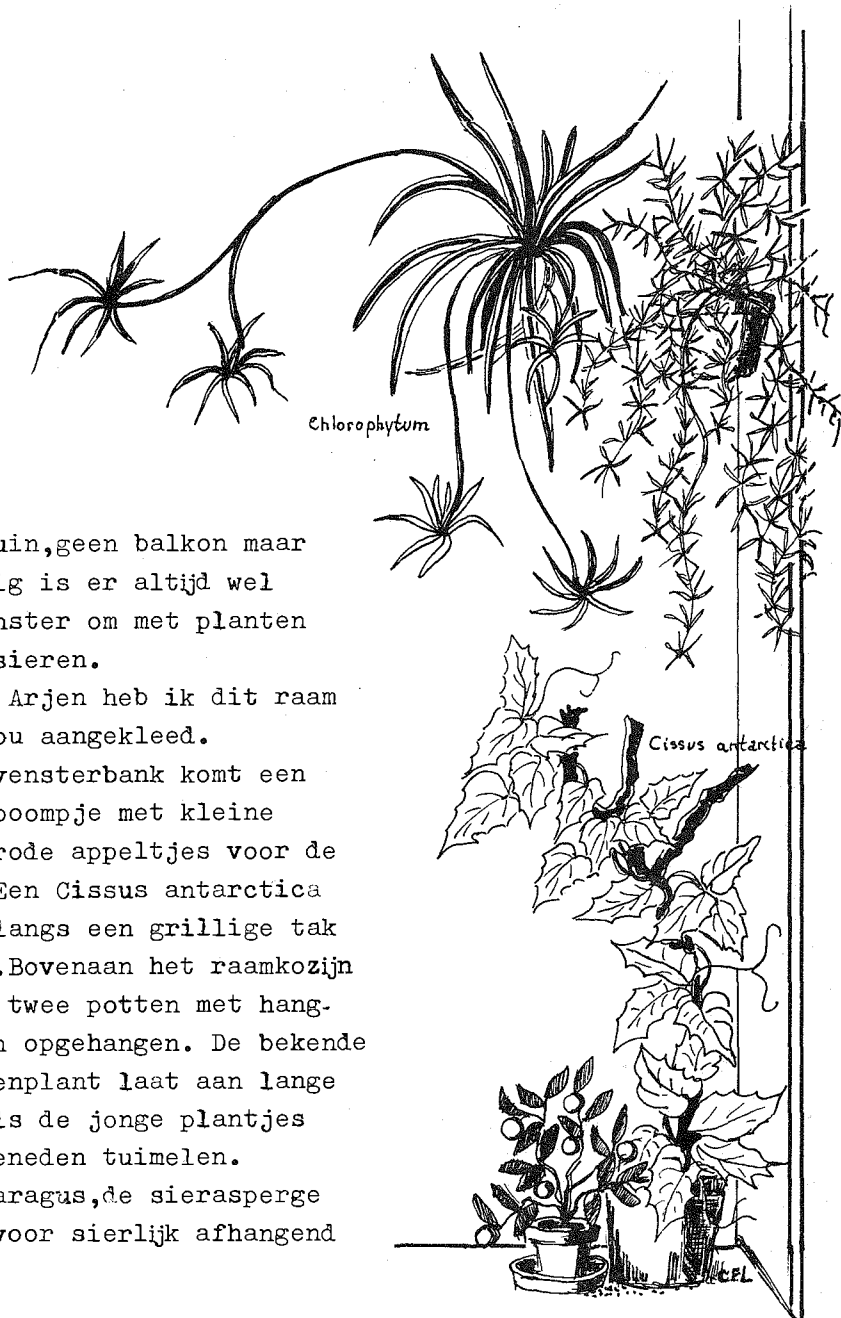
Le fettuccine o tagliatelle hanno scarsa larghezza, le lasagne medie 3 cm. circa; le lasagne grandi 8 cm. e servono per la preparazione delle varie ricette di « lasagna pasticcata ».

Abbiamo qui dato scarse e frammentarie delucidazioni, sia perchè le stesse denominazioni variano da paese a paese, sia perchè ad ogni ricetta si daranno dettagliate spiegazioni.

*Veel Succes Gewenst
op alle fronten
tant Martha*

EEN VENSTERBANK VOOR ARJEN

Geen tuin, geen balkon maar gelukkig is er altijd wel een venster om met planten te versieren. Daarom Arjen heb ik dit raam voor jou aangekleed. Op de vensterbank komt een oranjeboompje met kleine orangerode appeltjes voor de kleur. Een *Cissus antarctica* klimt langs een grillige tak omhoog. Bovenaan het raamkozijn worden twee potten met hangplanten opgehangen. De bekende sprietenplant laat aan lange stengels de jonge plantjes naar beneden tuimelen. De *Asparagus*, de sierasperge zorgt voor sierlijk afhangend groen.





Aan de andere kant van het raam gaan we net zo te werk. Op de vensterbank zorgt een klimplant, een Philodendron, voor het groen van onder naar boven. Bovenaan hangen een bonte klimop en een kleinbladige Ficus pumila voor het groen van boven naar beneden.

tante Toos

Het BELIAL project.

Opgedragen aan mijn geachte collega Arjen K. Lenstra ter gelegenheid van zijn bevordering tot doctorale waardigheid, door
Balthasar Elias Lub, Univ. of Umbar, Harad.

Tijdens een recent bezoek aan Nederland wees mijn collega Peter van Emde Boas mij op de aanstaande promotie van Arjen. Gezien de belangrijke bijdrage die Arjen, geheel buiten zijn weten om, heeft geleverd aan een minder bekend project dat voor de toekomst van Harad van doorslaggevend belang is wil ik gaarne van deze gelegenheid gebruik maken om Arjen iets te laten weten over dit project. Dat het project minder bekend is in het buitenland hangt samen met de oorsprong ervan. Tot enkele maanden terug was alle informatie over het BELIAL project volstrekt geheim, maar inmiddels zijn de ontwikkelingen in de wereld zodanig dat wij deze informatie rustig bekend kunnen maken omdat geen enkele vijand deze kennis tegen ons zal kunnen gebruiken.

Het zal U ongetwijfeld bekend zijn dat Harad een klein land is gelegen in een turbulent deel van deze wereld. Tot voor twintig jaar terug beruste de nationale veiligheid van Harad op de wetenschap dat niemand in dit gebied geïnteresseerd was - in een later stadium kende het land gedurende een korte periode een grote rijkdom waarmee regionale vijanden konden worden afgekocht, maar ook deze periode is afgesloten. Harad is op dit moment, zoals zovele staten gewoon aangewezen op de kracht van het onoverwinnelijke Haraanse leger. Omdat deze kracht niet kan berusten op numerieke sterkte is Harad gedwongen deze kracht te zoeken in slimheid en wel in het bijzonder in de automatisering via de computer.

Uiteraard heeft de Haraanse regering toen zij het einde van de periode van voorspoed zag aankomen, en zich de problematiek van de landsverdediging bewust werd in de wereld rondgekeken, om te zien hoe de interactie tussen het militaire systeem en de informatica elders verloopt. De ervaringen waren bepaald niet bemoedigend. Bij militaire toepassingen waren alom de gevolgen van de Software crisis zichtbaar, en als Harad zich een ding niet kon permitteren dan is het wel het verlies van mankracht en hulpmiddelen aan het produceren van niet werkende programmatuur. De om. in de VS gezochte oplossing die er op neer kwam hiertoe een nieuwe programmeertaal te ontwikkelen kwam als ongeloofwaardig over. Bij nader analyse slaagde Hosia W. Labbers er ook in om aan te tonen dat de taal ADA slachts gezien kan worden als een neocolonialistisch instrument dat erop is gericht het programmeren te maken

tot een privilege van de geïndustrialiseerde wereld. Dit doel wordt bereikt door de taal zodanig gecompliceerd te maken dat volkeren die dichter bij de natuur leven zich wel in walging van deze taal moeten afwenden, waarmee ze de toegang tot de op ADA gerichte computersystemen dreigen te verliezen.

In zijn analyse stelde Labbers bovendien vast dat de aanpak van groot-schalige softwareontwikkelingsprojecten via taal- en of systeemontwikkeling allemaal leiden aan een fundamentele misvatting - de misvatting dat de taal waarin de "hogere" uitdrukkingsmiddelen zijn opgenomen die het de ontwerper van algoritmen makkelijk moeten maken zich uit te drukken, tevens executeerbaar moet zijn. Dit terwijl iedere informaticus doordrongen zou moeten zijn van de simpele waarheid die leert dat software die moet werken geschreven wordt in FORTRAN.

Op grond van deze overwegingen kwam Labbers tot een radicaal andere aanpak van de software crisis, gebaseerd op de absolute scheiding tussen ontwerp en codering. Deze scheiding kwam tot stand door de ontwerper te dwingen zijn ideeën neer te schrijven in een taal waarvan bij wet zou worden verboden ooit een vertaler of interpretator te ontwikkelen. In samenwerking met de heer Ismael B. Merodak en ondergetekende werden in enkele maanden tijd de eerste ideeën over de taal BELIAL (Balthasar Elias Lub's Informal Algorithmic Language) ontwikkeld en uitgewerkt.

De filosofie van het BELIAL project is dat algoritmen worden ontworpen door specialisten in deze niet implementeerbare taal. De feitelijke programmering geschiedt naderhand in FORTRAN door dommekrachten. Op dit moment is nog niet geheel duidelijk hoe deze lieden dienen te worden geselecteerd; een probleem bij deze selectie is de ingewortelde neiging bij programmeurs slimmer te willen zijn dan de opdrachtgever voor wenselijk houdt. Volgens I.B. Merodak is dit echter een geslachtsgebonden eigenschap (en hij kan het weten want hij heeft ooit sociologie gestudeerd). De remedie die hij voorstelt bestaat uit het inhuren van dames voor deze taak, waarbij niet wordt uitgesloten dat voor echt gevoelig werk gebruik zal worden gemaakt van eunuchen.

De taal BELIAL zelf berust in haar syntactische structuur op ALGOL 68 . De redenen die tot deze keuze hebben geleid zijn deels historisch (ik gebruikte 10 jaar geleden in mijn eigen proefschrift een dergelijk ALGOL 68 derivaat, in navolging van P. van Emde Boas). Bovendien leert de ervaring dat dit een goed hulpmiddel is om de schapen van de bokken te scheiden. De doorslag gaf echter een aantal programmapakketten geschreven door Arjen K. Lenstra die de heer Labbers ooit van een bezoek aan Amsterdam meebracht. In het bijzonder de

elegante wijze om in een willekeurig grote expressie de gehele betekenis van de optredende operatoren te reduceren modulo p , eenvoudig door de expressie te termineren met de symbolen `....//p` vormde een overtuigend argument om een dergelijke taal als uitgangspunt te kiezen voor ons project.

Omdat de taal niet geïmplementeerd kan en mag worden is het geen probleem de taal volledig uitbreidbaar te maken. Allerlei standaard gegevensstructuren zijn op te nemen zonder dat de bedoelde types en operaties dienen te worden gedeclareerd - een simpele verwijzing naar de literatuur waar de structuur beschreven staat opgenomen in een stukje commentaar is voldoende. In dit opzicht zijn in BELIAL de nodige ideeën uit het PIDGIN ALGOL van Aho, Hopcroft & Ullman uit 1974 terecht gekomen. Het is opmerkelijk dat deze auteurs inmiddels zelf dit zo gangbare pad hebben verlaten en zich hebben geëncanaaleerd met een misbaksel als "Super PASCAL" hetgeen ertoe leidt dat een inleidend boek over algoritmen en gegevensstructuren tegenwoordig ontaard tot een domme programmeurscursus.

Een ander project waarmee BELIAL kan worden vergeleken is het voormalige ABSTRACTO project, thans het B-project geheten. Hierbij is duidelijk weer de fout gemaakt de taal executeerbaar te willen maken, hetgeen tot vele beperkingen heeft geleid. Dit feit, in combinatie met de bedoeling de taal en bijbehorende omgeving te willen richten op het "programmeren achter de terminal" geeft wel aan hoezeer dit project afwijkt van de door ons gehuldigde opvattingen.

Het is ook aannemelijk te maken dat BELIAL een ideaal uitdrukkingsmiddel is voor algoritmen in de wiskunde en andere rechtschapen wetenschappen. Omdat elementen uit andere talen naar willekeur kunnen worden geïncorporeerd hoeft de wiskundige zich nooit zorgen te maken over triviale syntax puzzeltjes, want alles wat hij ooit ergens heeft mogen schrijven is correct BELIAL. De enige conditie is dat de notaties consistent worden gebruikt, en dat de resultaten door een dommekracht met de hand kunnen worden geconverteerd naar werkend FORTRAN.

Ook voor onderwijsdoeleinden is het ideaal als je als docent je kunt beperken tot het essentiële van algoritmen zonder je zorgen te hoeven maken over syntactische trivia; voor de studenten is het prettig te weten dat ze vrij zijn in de formulering van hun tentamenantwoorden mits ze maar consistent zijn.

Keren wij aan het einde van deze beschouwing terug tot het oorspronkelijke doel van het project: de landsverdediging. Op dit moment hebben wij nog geen ervaringen kunnen opdoen met de werkzaamheid van de via BELIAL geprogrammeerde wapensystemen, aangezien onze vijanden op dit moment bezig zijn elkander af te slachten. De export van de door onze vooruitstrevende industrie ontwikkelde wapensystemen verloopt echter voorspoedig. Wellicht zult U ooit nog eens met een van onze kwaliteitsproducten worden geconfronteerd. U weet dan op basis van welke wetenschappelijke resultaten de goede werking kan worden gegarandeerd.

Voor belangstellenden zou op deze plaats een verwijzing naar een definitie van de taal BELIAL en haar semantiek niet misstaan, maar gelijk de goede lezer begrijpen zal zou een Revised Report voor BELIAL het de vijand veel te makkelijk maken om toch een implementatie van de taal te ontwikkelen. Om deze reden is dit Revised Report geheim gehouden. Ik zal U deze referentie derhalve moeten onthouden. Wij zijn echter wel geïnteresseerd in niet triviale toepassingen van de taal. Programmateksten kunnen worden opgestuurd naar het onderstaande adres:

Project BELIAL
c/o Balthasar E. Lub
Dept. Theodynamics, Univ. of Umbar
UMBAR 14853
HARAD

Indien vergezeld van een magneetband zal de resulterende FORTRAN versie worden geretourneerd, gesteld dat de voorgedragen teksten waardig worden geoordeeld. Over deze evaluatie is geen correspondentie mogelijk.

Over een jonge doctor, zijn bagage, en twee ringen

Beste Arjen,

Het is mij een groot voorrecht ter gelegenheid van je promotie enige woorden tot je te mogen richten. Allereerst mijn gelukwensen met het geslaagde proefschrift, waarin je ons uitgebreid uit de doeken doet hoe het factorizeren van polynomen efficiënt gedaan kan worden. Het is een genoegen te zien dat je je geestelijke bagage in ruime mate en op kundige wijze hebt weten uit te pakken. Dat je in staat bent je wereldlijke bagage krap en kundig in te pakken is mij reeds lang bekend. Zo herinner ik mij, dat aan het begin van onze studententijd jij reeds aan een kleine bruine hoekige tas voldoende had, terwijl ik nog met de riante boekentas van de middelbare school rondliep. Deze tas gaf jou tevens een bepaalde uitstraling. Zo kon het gebeuren, dat toen je op zekere zondagmorgen bij mij in Uithoorn op bezoek kwam, een niet nader te noemen dorpsbewoner meende dat het hier iemand der Jehova's getuigen betrof, die maar beter op de stoep kon blijven staan. Gelukkig heb je enige volharding bij het aanbellen getoond.

Later, toen de moderne student, en wij dus ook, er niet meer onderuit kon zich met een koffertje door het leven te reppen, koos jij wederom voor het platste model dat te verkrijgen was. Dat het wereldlijk voer, gegoten in een etensblik, hierin minder goed paste vond je niet erg. Belangrijk was wel dat het geestelijk voer, en hier doel ik uiteraard op de vele klassieke langspeelplaten, hierin ongeschonden door het drukke Amsterdamse verkeer geloodst kon worden. Kennelijk ben ik niet de enige geweest, die zich over de omvang en de inhoud van dit koffertje verbaasd heeft. Ook anderen hebben moeilijk kunnen geloven dat het omvangrijk genoeg was om alle benodigdheden voor een werkbezoek aan Israel gevolgd door een vakantie in Egypte in mee te nemen.

Verder staat mij nog onze kampeervakantie naar Griekenland bij. Je hebt mij bij die gelegenheid overtuigend aangetoond dat alle benodigdheden voor zo'n reis, waaronder een tent, gereedschap, kleding en niet te vergeten een uitgebreide collectie lijvige reisgidsen, gemakkelijk in twee kleine schoudertassen kunnen. Alhoewel? Dat ik tenslotte degene was bij wie de slaapzak er echt niet meer bij

kon zal niemand verbazen. Zo vlogen wij met louter handbagage, de stewardess verzwijgend dat elk der tassen ruim 10 kg. te zwaar was, naar zonnig Griekenland.

Zoals reeds opgemerkt vormt de klassieke muziek een belangrijk facet van jouw leven. Ik zou je dan ook graag een serenade willen brengen. Helaas, het medium is papier, en het notenschrift beheers ik niet. Het treft daarom bijzonder, dat mij recentelijk een compositie ter ore kwam, die weliswaar niet de muziekliefhebber, maar hopelijk wel de informaticus in jou zal aanspreken. Voordat ik tot weergave van de opname die ik bij die gelegenheid gemaakt heb overga, volgen eerst enkele saillante details om het bijzondere karakter van zowel de compositie als de opname te illustreren.

- de componist heet Yossi Shiloach, en de oeruitvoering van het werk vond plaats in de "Information Processing Letters", Vol. 8, Nmb. 5, juni 1979.
- de compositie vergt slechts zes strofen, behoort reeds tot de klassieken, en ... bevat een ringmotief.
- de opname is gemaakt op 6 december 1983; het betrof hier een uitvoering ter afsluiting van 17 jaar "Inleiding tot de Kunst van het Programmeren".
- de orchestratie droeg een duidelijke Eindhovense signatuur, en de solist bij deze gelegenheid was maestro E.W. Dijkstra.

Shiloach's Algoritme

Gegeven zijn twee ringen (cyclische lijsten, zoals de componist ze noemt) met $N \geq 0$ objecten ieder. Deze objecten zijn afkomstig uit een totaal geordende verzameling, waarvoor we hier gemakshalve de gehele getallen zullen kiezen. Gevraagd wordt na te gaan of deze ringen equivalent zijn, d.w.z. of ze op een cyclische permutatie na gelijk zijn. Een formele specificatie van dit probleem luidt :

Bepaal een statement list S die voldoet aan

```
[ [ N : int { N ≥ 0 }  
; A(i : 0 ≤ i < N) , B(i : 0 ≤ i < N) : array of int
```

```

; [[ b : bool
; S
{ b ≡ (E h, k : 0 ≤ h < N ∧ 0 ≤ k < N :
    (A i : 0 ≤ i < N : A(h+i) = B(k+i))
    )
}
]]
]]

```

In de postconditie, en in het vervolg, is verondersteld dat alle referenties naar ring elementen modulo N geschieden.

Indien A en B equivalent zijn dan kunnen we dit constateren door voor zekere h en k vast te stellen dat

$$(0) \quad (A i : 0 \leq i < N : A(h+i) = B(k+i)).$$

Dit is eenvoudig na te gaan met een repetitie. De bijbehorende invariant P wordt verkregen door in (0) constante N door variabele n te vervangen. Dit levert

$$P : \quad (A i : 0 \leq i < n : A(h+i) = B(k+i)) \wedge 0 \leq n$$

met de volgende eigenschappen

- (1) $P_0^n \equiv \text{true}$,
- (2) $P \wedge A(h+n) = B(k+n) \Rightarrow P_{n+1}^n$,
- (3) $P \wedge n \geq N \Rightarrow (E h, k : 0 \leq h < N \wedge 0 \leq k < N : (A i : 0 \leq i < N : A(h+i) = B(k+i)))$.

Stel nu dat het antecedent van (3) niet bewerkstelligd kan worden, omdat er een n bestaat zodanig dat $A(h+n) \neq B(k+n)$. Dan moeten we allereerst nagaan of er inmiddels voldoende paren h, k onderzocht zijn om te kunnen concluderen dat A en B niet equivalent zijn. Indien dat niet het geval is, dan moeten we een volgend paar h, k bepalen waarvoor (0) geverifieerd dient te worden.

De vondst van Shiloach is nu, dat hij de lexicografische ordening op de cyclische permutaties van A en B in beschouwing neemt. In zijn voetspoor definiëren we A_n (B_k) als de ring die uit A (B) ontstaat door deze over h (k) posities te draaien, d.w.z.

$$(4) \quad A_h = A(h+i : 0 \leq i < N), \text{ voor } 0 \leq h,$$

$$(5) \quad B_k = B(k+i : 0 \leq i < N), \text{ voor } 0 \leq k.$$

In het vervolg noteren we (0) als $A_h = B_k$ en gebruiken we het symbool "<" niet alleen voor de ordening tussen ring elementen, maar ook voor de geïnduceerde lexicografische ordening tussen de permutaties van A en B.

Tenslotte definiëren we nog de lexicografische minima

$$(6) \quad AA = (\text{MIN } h : 0 \leq h < N : A_h),$$

$$(7) \quad BB = (\text{MIN } k : 0 \leq k < N : B_k).$$

De cruciale observatie is

$$(8) \quad (AA = BB) \equiv (\exists h, k : 0 \leq h < N \wedge 0 \leq k < N : A_h = B_k)$$

Met deze kennis gewapend gaan we de situatie

$P \wedge A(h+n) \neq B(k+n)$ te lijf. Op grond van de symmetrie in A en B (en in h en k respectievelijk) is het voldoende alleen het geval $P \wedge A(h+n) < B(k+n)$ te beschouwen. We merken op dat

$$(9) \quad P \wedge A(h+n) < B(k+n) \Rightarrow (\exists i : 0 \leq i < n+1 : A_{h+i} < B_{k+i})$$

en dus op grond van (6) en enig henummeren

$$(10) \quad P \wedge A(h+n) < B(k+n) \Rightarrow (\exists j : k \leq j < k+n+1 : AA < B_j)$$

Formule (10) brengt ons er toe een tweede invariant PA te introduceren

$$PA : (\exists j : 0 \leq j < k : AA < B_j) \wedge 0 \leq k$$

met de volgende eigenschappen

$$(11) \quad PA_0^k \equiv \text{true},$$

$$(12) \quad PA \wedge P \wedge A(h+n) < B(k+n) \Rightarrow PA_{k+n+1}^k,$$

$$(13) \quad PA \wedge k \geq N \Rightarrow AA < BB.$$

Aldus komen we tot de statement list

S : $\llbracket h, k, n : \text{int}$

; $h, k, n := 0, 0, 0$

{Invariant : $P \wedge PA \wedge PB$

met $P : (\exists i : 0 \leq i < n : A(h+i) = B(k+i)) \wedge 0 \leq n,$

en $PA : (\exists j : 0 \leq j < k : AA < B_j) \wedge 0 \leq k,$

en $PB : (\exists j : 0 \leq j < h : BB < A_j) \wedge 0 \leq h.$

```

    Variante functie vf :  $3 \cdot (N-1) - (n+h+k)$ 
  }
; do  $n < N \wedge h < N \wedge k < N$ 
  → if  $A(h+n) < B(k+n) \rightarrow k, n := k+n+1, 0$ 
    □  $A(h+n) \neq B(k+n) \rightarrow n := n+1$ 
    □  $A(h+n) > B(k+n) \rightarrow h, n := h+n+1, 0$ 
  fi
od
{  $P \wedge PA \wedge PB \wedge (n \geq N \vee h \geq N \vee k \geq N)$  }
;  $b := (n \geq N)$ 
{  $b \equiv (AA = BB)$  }
]

```

Om aan te tonen dat deze algoritme slechts aanleiding geeft tot eindige berekeningen is aan de preconditione van de repetitie een variante functie toegevoegd. Met betrekking tot dit eenvoudige polymorfisme in meerdere variabelen merken we het volgende op

- uit de guard van de repetitie volgt $vf \geq 0$
- bij iedere slag van de repetitie neemt de waarde van vf met precies 1 af

Hieruit maken we op dat de algoritme termineert en ten hoogste $3 \cdot (N-1)$ vergelijkingen tussen ring elementen vergt.

(Einde Shiloach's algoritme)

Opmerking.

Wellicht zul je zo af en toe onaangenaam getroffen zijn door enkele dissonanten. Hoewel het met de hedendaagse registratietechnieken zeer wel mogelijk is deze te onderdrukken, heb ik gemeend dit omwille van de authenticiteit niet te moeten doen.
(einde opmerking.)

Er rest mij slechts de wens uit te spreken dat je in je verdere wetenschappelijke loopbaan nog vaak zult uitpakken.

Nogmaals, gefeliciteerd

Rudolf Mak

A T T I
del
2° CONGRESSO NAZIONALE DELL' A. I. C. A.
(Napoli, 26 - 29 Settembre 1968)

ALGORITHMS FOR SYMBOLIC DETERMINATION
OF LAPLACE TRANSFORM

A. MIOLA

Istituto Matematico « Guido Castelnuovo » dell'Università di Roma

1. INTRODUCTION

This paper describes a recursive method for the symbolic determination of the Laplace transform, direct or inverse, of a function belonging to a well defined class.

During the IFIP working conference on symbol manipulation languages, held in Pisa in September 1966, Prof. Carl Engleman and other research workers from the MITRE-Corporation of Bedford presented a very interesting paper which, among other things, considers the problem of the Laplace transform [3] [4].

Taking into consideration some of the results obtained by Engleman we present a method which enlarges remarkably the family of functions to be manipulated thus allowing to meet numerous applications of the analysis.

2. DESCRIPTION OF THE ALGORITHM

2.1 *Family of transformable functions.*

The family $\mathcal{F}$ of transformable functions $F(t)$ has been recursively defined as follows: the following functions, (called base or elementary functions) belong to $\mathcal{F}$

- 1) k
- 2) $(at + b)^k$
- 3) e^{kt}
- 4) e^{kt^2}
- 5) $\log (at + b)$
- 6) $1(at + b) = \begin{cases} 1 & \text{if } at + b \geq 0 \\ 0 & \text{if } at + b < 0 \end{cases}$
- 7) $\text{Erf}(at + b) = \frac{2}{\sqrt{\pi}} \int_0^{at+b} e^{-\tau^2} d\tau$
- 8) $J_k(at + b) = \left(\frac{at + b}{2} \right)^k \sum_{h=0}^{\infty} (-1)^h \frac{\left(\frac{at + b}{2} \right)^{2h}}{h! \Gamma(k + h + 1)}$

where k is a complex constant while a and b are real constants with $b \leq 0$; moreover there belong to $\mathcal{F}$ all the functions obtainable by applying to functions of the family $\mathcal{F}$ one of the following operators:

$$D_1(F_1(t), F_2(t), \dots, F_n(t)) = c_1 F_1(t) + c_2 F_2(t) + \dots + c_n F_n(t)$$

where $c_1, c_2, \dots, c_n$ are complex constants

$$D_2(F(t)) = t^n F(t)$$

$$D_3(F(t)) = e^{kt} F(t)$$

$$D_4(F(t), h) = \sum_{h=0}^{\infty} F_h(t)$$

$$D_5(F(t), G(t)) = F(t) \star G(t) = \int_0^1 F(t-\tau) G(\tau) d\tau$$

$$D_6(F(t)) = F'(t)$$

where k is a complex constant and n an integer.

The family $\mathcal{F}^{-1}$ of the antitransformable functions $f(s)$ is analogously determined and includes as elementary functions:

1) Functions rational in s .

2) Functions $f(s)$ such as: $L^{-1}[f(s)] = J_0(at+b)$.

Moreover it comprises all the functions obtainable by applying to functions of the same family $\mathcal{F}^{-1}$ one of the following operators:

D_1, D_4, D_6 (already dealt)

$$D_7(f(s), g(s)) = f(s)g(s)$$

2.2 Transformation method.

The procedure for determining the transform (antitransform) of a $F(t)$ ($f(s)$) takes place in three stages. In the first stage some substitutions are made on the mentioned function, possibly reducing functions sine and cosine trigonometric or hyperbolic, exponentials on whatever basis into exponentials on basis 'e', Bessel functions of the second kind into Bessel functions of the first kind.

Therefore if the considered function comes out from the application of one of the operators $D_1, D_2, D_3, D_4, D_5, D_6$ (D_1, D_4, D_6, D_7) to other functions, the problem reduces to the transformations of the latter, making use of one of the known properties of the operator L (L^{-1}) (see [1]).

If on the contrary the considered function is not of the type described, we pass to the third stage in which if it comes out to be an elementary function its transform is given; otherwise it is explained why the transform has not been done.

Remarks:

1) The antitransforms of the rational functions are determined by the following formula:

$$L^{-1} \left[\frac{f(s)}{g(s)} \right] = \sum_{k=1}^n \sum_{h=1}^{m_k} \frac{\Phi_{kh}(\alpha_k)}{(m_k - h)! (h-1)!} t^{m_k - h} e^{\alpha_k t}$$

$$\text{where } g(s) = \prod_{r=1}^n (s - \alpha_k)^{m_k}$$

$f(s)$ of order $< m_1 + m_2 + \dots + m_n$

$$\Phi_{kh}(s) = \frac{d^{h-1}}{ds^{h-1}} \left[\frac{f(s) (s - \alpha_k)^{m_k}}{g(s)} \right]$$

2) The shown method does not keep into account the existence of the transform, of which one must be sure beforehand.

3. DESCRIPTION OF THE PROGRAMS

3.1 LAPTR and INLT

The method presented in the preceding paragraphs was programmed in LISP, in a first version for the IBM 7090 of the C.N.U.C.E. of Pisa, and in the present one for the CINAC of the INAC of Rome.

The LISP-functions LAPTR and INLT operating respectively the direct and inverse transform, have three arguments: the expression to be transformed, its principal variable and the principal variable (which can be therefore chosen at will) of the expression obtained as result.

The three stages of the procedure (see 2.2) for determining the transform (antitransform) requested to LAPTR (INLT) are carried out: the first one from the LISP-functions FUNTRA and COMM, the second one from LAP1 (INL1), and the third one from LAP2 (INL2). These above mentioned LISP-functions have only one argument: the expression on which they operate.

Note that INL2 antitransforms the rational functions according to the algorithm shown (see 2.2).

The LISP-function SINAC with zero arguments, initiates the transformation procedure, calling for the operation to be carried out (LAPTR or INLT); then, after receiving the information, calls for the arguments on which to operate: the expression to be transformed (which is translated from its external infix form to its internal prefixed form, from the input LISP-function LISPIN), and the principal variables; finally after the transformation it prints the result already reported in the external form with the LISPOUT function.

The internal representation of the expressions is the one in prefixed notation with all the brackets necessary to LISP; the external one is determined as follows in Backus normal form:

```

<figure> ::= 0|1|2|3|4|5|6|7|8|9
<character> ::= A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z
<*op> ::= *|/
<+op> ::= +|-
<number> ::= <figure> | <number> <figure>
<atom> ::= <character> | <atom> <character> | <atom> <number>
<expression> ::= <number> | <atom> | (<sum>) | (<function>)
<power> ::= <expression> | <power> ^ <expression>
<product> ::= <power> | <product> <*op> <power>
<sum> ::= <product> | <sum> <+op> <product> | - <product>
<function> ::= <atom> <list args>
<list args> ::= <expression> | <list args> <expression>

```

The input language just defined, however, must be restricted compatibly with the expressions of the functions recognized by LAPTR and INLT.

Some particular constants have an atom fixed for their representations, that is: E for the basis « e » of the exponentials, PI for π , EC for the Euler's constant γ ; the recognized functions are on the contrary SQRT, SIN, COS, SINH, COSH, TANG, LN, ERFC, ONEF, GAMMA, JBES; moreover SERIES K means $\sum_{k=0}^{\infty}$ and FALTUNG denotes the integral product.

3.2 Subprograms.

Among the subprograms used by LAPTR and INLT, some ones have particular importance.

The program D/D which carries out the symbolic derivation of algebraic functions, trigonometric direct and inverse functions, exponential and logarithmic functions and of the function of the errors Erf.

The programs S+, S-, S*, S/, S $\uparrow$ are called in by any other program which builds up algebraic expressions, they reduce the expressions themselves consolidating the numerical terms and carrying out symbolically the operations shown in the expressions according to the rules of the literal calculus.

4. CONCLUSIONS

Keeping into account the functions which may belong to the family $\mathcal{F}(\mathcal{F}^{-1})$, note that the given method allows to meet numerous problems of the numerical analysis and calculus; this is in contraposition with the Engleman's work which, operating on rational, exponential and trigonometric functions was particularly apt for dealing with algebraic problems.

It must also be noted that the enlargement of the family $\mathcal{F}(\mathcal{F}^{-1})$ implied the modification of the algorithm and therefore a different idea of the programs, for a wider generality. It is in fact possible to enlarge further on the family $\mathcal{F}(\mathcal{F}^{-1})$ of transformable functions introducing other elementary functions, or other operators, without modifying the algorithm.

5. ONE APPLICATION

Now we see how some examples of those carried out by means of LAPTR and INLT, can be used for a problem referring to the heat transmission in solid bodies (see [5]).

Let us consider two bars concurring in a node, and assume that in the node be located a source of heat; moreover let us assume that the loss of heat in the medium be negligible.

If the bars are exactly alike, the heat emitted by the source will be shared equally between the two bars. If on the contrary the thermic properties of the bars are different, the distribution law will vary according to the time, even if it is conditioned by the equality of temperature in the sections converging to the node.

Then having assigned the law $q(t)$ of the heat emitted by the source, we have to compute the laws $q_1(t)$ and $q_2(t)$ of the heat received by the two bars.

Moreover the temperatures of the two bars in the node must be equal. We recall here the law expressing the temperature with respect to the flux in the nodal section:

$$\theta(t) = \frac{1}{\sqrt{\pi}} \frac{a}{\lambda F} \int_0^t q(\tau) \frac{e^{-b^2(t-\tau)}}{\sqrt{t-\tau}} d\tau$$

where λ is the coefficient of thermic conductivity of the medium, F is the section in which temperature is measured, a is the thermic diffusibility, b is the heat loss.

Then we have

$$q(t) = q_1(t) + q_2(t)$$

$$\frac{a_1}{\lambda_1 F_1} \int_0^t q_1(\tau) \frac{e^{-b_1^2(t-\tau)}}{\sqrt{t-\tau}} d\tau = \frac{a_2}{\lambda_2 F_2} \int_0^t q_2(\tau) \frac{e^{-b_2^2(t-\tau)}}{\sqrt{t-\tau}} d\tau$$

These equations form a system of functional equations in $q_1(t)$ e $q_2(t)$, having preassigned $q(t)$.

Let be $L[q(t)] = q_0$ we apply the L -transform assuming

$$L[q_1(t)] = \bar{q}_1(p)$$

$$L[q_2(t)] = \bar{q}_2(p)$$

Then we have

$$\bar{q}_1(p) + \bar{q}_2(p) = L[q_0]$$

$$\frac{a_1}{\lambda_1 F_1} \bar{q}_1(p) L\left[\frac{e^{-b_1^2 t}}{\sqrt{t}}\right] = \frac{a_2}{\lambda_1 F_1} \bar{q}_2(p) L\left[\frac{e^{-b_2^2 t}}{\sqrt{t}}\right]$$

If we carry out L -transformations by means of LAPTR, (see examples).

We then obtain

$$\frac{\bar{q}_1(p)}{q_0} = \frac{1}{p} \cdot \frac{F_1 \sqrt{p+b_1^2}}{F_1 \sqrt{p+b_1^2} + F_2 \sqrt{p+b_2^2}}$$

$$\frac{\bar{q}_2(p)}{q_0} = \frac{1}{p} \cdot \frac{F_2 \sqrt{p+b_2^2}}{F_1 \sqrt{p+b_1^2} + F_2 \sqrt{p+b_2^2}}$$

having put

$$K = \frac{F_1^2 b_1^2 - F_2^2 b_2^2}{F_1^2 - F_2^2}$$

with $F_1 b_1 \neq F_2 b_2$ and $F_1 \neq F_2$ we obtain

$$\frac{\bar{q}_1(p)}{q_0} = \frac{F_1^2}{F_1^2 - F_2^2} \cdot \frac{p + b_1^2}{p(p+K)} - \frac{F_1 F_2}{F_1^2 - F_2^2} \frac{(p+b_1^2)(p+b_2^2)}{p(p+K)} \cdot \frac{1}{\sqrt{(p+b_1^2)(p+b_2^2)}}$$

and analogously for $\frac{\bar{q}_2(p)}{q_0}$.

We consider the only $q_1(t)$, $q_2(t)$ and we shall obtain by difference.

Having put

$$\begin{aligned}
A_1 &= \frac{F_1^2}{F_1^2 - F_2^2} \cdot \frac{b_1^2}{K} \\
A_2 &= \frac{F_1^2}{F_1^2 - F_2^2} \cdot \frac{K - b_1^2}{K} \\
B_1 &= \frac{F_1 F_2}{F_1^2 - F_2^2} \\
B_2 &= \frac{F_1 F_2}{F_1^2 - F_2^2} \cdot \frac{b_1^2 b_2^2}{K} \\
B_3 &= \frac{F_1 F_2}{F_1^2 - F_2^2} \cdot \frac{(K - b_1^2)(K - b_2^2)}{K}
\end{aligned}$$

we have:

$$\frac{\bar{q}_1(p)}{q_0} = \frac{A_1}{p} + \frac{A_2}{p+K} \left(B_1 + \frac{B_2}{p} + \frac{B_3}{p+K} \right) \frac{1}{\sqrt{(p+b_1^2)(p+b_2^2)}}$$

Antitransforming this last expression using INLT, (see examples), we get:

$$\begin{aligned}
\frac{q_1(t)}{q_0} &= A_1 + A_2 e^{-kt} - B_1 f(t) - B_2 \int_0^t f(\tau) d\tau - \\
&\quad - B_3 e^{-kt} \int_0^t e^{k\tau} f(\tau) d\tau
\end{aligned}$$

where

$$f(t) = e^{-\frac{b_1^2 + b_2^2}{2} t} \cdot I_0 \left(\frac{(b_1^2 - b_2^2)}{2} t \right) \cdot \frac{q_2(t)}{q_0} = 1 - \frac{q_1(t)}{q_0}.$$

6. APPENDIX

In order to obtain a transform (antitransform) it suffices to initialize the procedure by means of SINAC and to supply on request: LAPTR (INLT) and their arguments (see examples).

The causes of a non-execution of the requested transform, pointed out by an error with progressive numeration can be:

- 1) Derivation of a function non recognized by D/D.
- 2) Transformation of the type $L[t^k(F(t))]$ with k non integer.
- 3) Transformation of the type $F_1(t)F_2(t)$.
- 4) Transformation of the type $e^{ant} \cdot F(t)$ with $n > 1$.
- 5) Transformation of a function non recognized by LAPTR.
- 6) Transformation of a function non recognized by INLT.

Examples:

(SINAC)

LAPTR

((ONEF T) - 2 * (ONEF (T - A)) + (ONEF (T - 2 * A)))

T

S

(1 / S - 2 * E ↑ (-A * S) / S + E ↑ (-2 * A * S) / S)

LAPTR

$$\begin{aligned}
& (E \uparrow (-B \uparrow 2 * T) / (\text{SQRT } T)) \\
& T \\
& S \\
& (\text{SQRT } (P I / (S + B \uparrow 2))) \\
& \text{INLT} \\
& (1 / (S * (S - A) \uparrow 2)) \\
& S \\
& T \\
& (1 / A \uparrow 2 + T * E \uparrow (A * T) / A - E \uparrow (A * T) / A \uparrow 2) \\
& \text{INLT} \\
& (1 / (\text{SQRT } ((S + A) * (S + B)))) \\
& S \\
& T \\
& (E \uparrow (- (A + B) * T / 2) * (\text{IBES } ((A - B) * T / 2) 0))
\end{aligned}$$

REFERENCES

- [1] GHIZZETTI, A.: *Calcolo simbolico*. Zanichelli, Bologna 1943.
- [2] DOETSCH, G.: *Introduction à l'utilisation pratique de la transformation de Laplace*. Gauthier-Villars, Paris 1959.
- [3] ENGLEMAN, C.: *MATHLAB: a program for on-line machine assistance in symbolic computations*. MITRE-Corporation MTP 18, ottobre 1965.
- [4] ENGLEMAN, C.: *Rational functions in MATHLAB*. MITRE-Corporation MTP 35, agosto 1966.
- [5] TURRA, M.: *Stato termico e dilatazione degli elementi prismatici*. I.P.S.I. - Pompei 1965.

Discussioni

A. ASCARI: Chiedo al presentatore conferma del carattere di « matematica non numerica » del suo contributo, osservando che, in una certa classe di applicazioni, è particolarmente interessante la possibilità di ottenere trasformate inverse in forma analitica, specie con l'uso dell'operatore « serie ».

A. MIOLA: Ho confermato la natura « non numerica » del lavoro presentato, esponendo anche il desiderio di conoscere le esigenze di eventuali utilizzatori del metodo per adeguare la famiglia delle funzioni trattabili alle esigenze stesse.

Capability Management in Distributed Operating Systems

Sape J. Mullender

*Centre for Mathematics and Computer Science
Amsterdam*

Introduction

Soon, most office buildings will have a cable snaking through the cable ducts, with an outlet in each room into which users can plug their personal computers. The traditional approach to protection, a secure operating system in every machine to check permissions before carrying out a command, is not suitable for such an environment. It is too easy for a malicious user to replace the operating system in one of the network machines, or to replace a machine altogether by one without a secure operating system, to obtain confidential information illicitly.

New methods for protection must be devised, methods that do not require secure, trustworthy operating systems. This paper presents mechanisms, based on *encryption*. We shall show that they are equally powerful, and, in some cases, more versatile than existing protection schemes, implemented by a secure operating system.

We assume that every object is managed and controled by a *service*. A service is an abstract entity, defined as a "set of commands and responses" that operate on the *objects* managed by it. It is implemented by one or more server processes, that receive requests to carry out operations, carry them out and return a reply. The design of those servers and the design of the protocols they use form an important part of the system software of fifth generation computers.

The object model is well-known in in the programming languages community under the name of "abstract data type." This model is especially suited to distributed systems because in many cases an abstract data type can be implemented on one of the network machines, its clients communicating with it via the exchange of messages.

A major advantage of the object or abstract data type model is that the semantics are inherently location independent. The concept of performing operations on an object does not require the user to be aware of where the object is located or how the communication is actually implemented. This property gives the system the possibility of moving objects around, to position them close to where they are frequently used.

Authentication and Ports

Every object is managed by a service. A request to carry out an operation on an object must be sent to the managing service, which checks whether the requested operation is allowed, and if it is, carries out the request and returns a reply.

We assume the client that requests the operation and the service are on different machines, connected by the cable that forms the network. We assume neither machine has a secure operating system, so the client is faced with the problem of making sure it sends its requests to one of the server processes and not to an imposter, while the server must have the means to find out if the client actually has the right to access the requested object.

Every service has one or more **ports** [Mullender82] to which client processes can send packets to contact the service. Ports consist of large numbers, typically 48 bits, which are known only to the server processes that comprise the service, and to the service's clients. For a public service, such as the system file service, the port will be generally made known to all users. The ports used by an ordinary user process will, in general, be kept secret. Knowledge of a port is taken by the system as *prima facie* evidence that the sender has a right to communicate with the service. Of course the service is not required to carry out work for clients just because they know the port, for example, the public file service may refuse to read or write files for clients lacking account numbers, appropriate authorization, etc.

Although the port mechanism provides a convenient way to provide partial authentication of clients ("if you know the port, you may at least talk to the service"), it does not deal with the authentication of servers. The basic primitive operations offered by the system are `PUT(PORT, MESSAGE)` and `GET(PORT, MESSAGE)`. Since everyone knows the port of the file server, as an example, how does one insure that malicious users do not execute `GETS` on the file server's port, in effect impersonating the file server to the rest of the system?

One approach is to have all ports manipulated by kernels that are presumed trustworthy and are supposed to know who may `GET` from which port. We reject this strategy because some machines, e.g., personal computers connected to larger multimodule systems may not be trustworthy, and also because we believe that by making the kernel as small as possible, we can enhance the reliability of the system as a whole. Instead, we have chosen a different solution that can be implemented in either hardware or software. First we will describe the hardware solution; later we will describe the software solution.

In the hardware solution, we need to place a small interface box, which we call an F-box (Function-box) between each processor module and the network. The most logical place to put it is on the VLSI chip that is used to interface to the network. Alternatively, it can be put on a small printed circuit board inside the wall socket through which personal computers attach to the network. In those cases where the processors have user mode and kernel mode and a trusted operating system running in kernel mode, it can also be put into operating system software. In any event, we assume that somehow or other all packets entering and leaving every processor undergo a simple transformation that users cannot bypass.

The transformation works like this. Each port is really a pair of ports, P , and G , related by: $P = F(G)$, where F is a (publicly-known) one-way function [Wilkes68, Purdy74, Evans74] performed by the F-box. The one-way function has the property that given G it is a straightforward computation to find P , but that given P , finding G is so difficult that the only approach is to try every possible G to see which one produces P . If P and G contain sufficient bits, this approach can be made to take millions of years on the world's largest supercomputer, thus making it effectively impossible to find G given only P . Note that a one-way function differs from a cryptographic transformation in the sense that the latter must have an inverse to be useful, but the former has been carefully chosen so that no inverse can be found.

Using the one-way F-box, the server authentication can be handled in a simple way. Each server chooses a get-port, G , and computes the corresponding put-port, P . The get-port is kept secret; the put-port is distributed to potential clients or in the case of public servers, is published. When the server is ready to accept client requests, it does a `GET(G)`. The F-box then computes $P = F(G)$ and waits for packets containing P to arrive. When one arrives, it is given to the process that did `GET(G)`. To send a packet to the server, the client merely does `PUT(P)`, which sends a packet containing P in a header field to the server. The F-box on the sender's side does not perform any transformation on the P field of the outgoing packet.

Now let us consider the system from an intruder's point of view. To impersonate a server, the intruder must do $\text{GET}(G)$. However, G is a well-kept secret, and is never transmitted on the network. Since we have assumed that G cannot be deduced from P (the one-way property of F) and that the intruder cannot circumvent the F-box, he cannot intercept packets not intended for him. Replies from the server to the client are protected the same way, only with the client picking a get-port for the reply, say, G' , and including $P' = F(G')$ in the request packet.

The presence of the F-box makes it easy to implement digital signatures for still further authentication, if that is desired. To do so, each client chooses a random signature, S , and publishes $F(S)$. The F-box must be designed to work as follows. Each packet presented to the F-box contains three special header fields: destination (P), reply (G'), and signature (S). The F-box applies the one-way function to the second and third of these, transmitting the three ports as: P , $F(G')$, and $F(S)$, respectively. The first is used by the receiver's F-box to admit only packets for which the corresponding GET has been done, the second is used as the put-port for the reply, and the third can be used to authenticate the sender, since only the true owner of the signature will know what number to put in the third field to insure that the publicly-known $F(S)$ comes out.

It is important to note that the F-box arrangement merely provides a simple *mechanism* for implementing security and protection, but gives operating system designers considerable latitude for choosing various *policies*. The mechanism is sufficiently flexible and general that it should be possible to put it into hardware with precluding many as-yet-unthought-of operating systems to be designed in the future.

One-Way Ciphers

One-way ciphers have been studied by a number of people who have used them for password protection in operating systems. Basically there are two different approaches to designing a secure one-way cipher; the first is finding a function that is mathematically hard to invert, the second is to find a function that is computationally hard to invert. The two methods are different. In the first method we try to find a function about which we can prove certain properties, one of the properties being the amount of work involved in computing the inverse function. In the second approach, we try to find functions of which we do not know the mathematical properties, but can be confident that the computational difficulties involved in finding the inverse are immense.

The **degeneracy** of a one-way cipher is the maximum number of x s mapped onto any one $F(x)$. The degeneracy of one-way ciphers is important, because the greater the degeneracy, the greater the chance of breaking a one-way cipher. Suppose a one-way cipher maps the numbers $\{1 \cdots N\}$ onto $\{1 \cdots N\}$, with degeneracy d . For any one $y \in \{1 \cdots N\}$ there can be as many as d numbers x , such that $F(x) = y$. The probability of breaking a one-way cipher by searching for a plaintext that produces the desired ciphertext is d/N per probe, that is, the chance of breaking a one-way cipher by brute force is directly proportional to the degeneracy.

Most one-way ciphers of mathematical origin are based on properties of natural numbers, derived from number theory. One possibility is to use a polynomial to a prime modulus, as described in [Purdy74]:

We choose our one-way cipher $F(x)$ by choosing a polynomial

$$p(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

where $n, a_1, \dots, a_n$ are integers. Let P be a large prime number, and define $F(x)$ by

$$F(x) \equiv p(x) \pmod{P}$$

Then $F(x)$ can be used as a one-way cipher that maps the numbers $0 \cdots P-1$ onto

$0 \dots P-1$. Polynomials of degree n to a prime modulus have n roots or less [LeVeque56, theorem 3.15, p.42]. Consequently the degeneracy of F , which is the maximum number of x s mapped by F into any one y , or the number of solutions to the congruence

$$F(x) - y \equiv 0 \pmod{P}$$

does not exceed n .

Given that $y = F(x)$, breaking the cipher amounts to finding roots of the congruence $F(x) - y \equiv 0 \pmod{P}$. This can be done by brute force, that is, by trying random ports, applying F to them and checking if they produce one of the desired cipher-ports, or it can be done by finding the inverse function of F using a *polynomial root finding algorithm*. The best root finding algorithms to date require $cn^2(\log P)^2$ operations to find the roots of a polynomial of degree n , modulus a prime P ; c is a constant [Knuth69, Berlekamp70]. The brute force approach (trial and error method) requires an expected number of P/nm tries to find an inverse of one of a set of m ports. Suppose, for example that $P = 2^{64} - 179$ (which is prime), $n = 2^{19} - 1$, and the number of ports in the network $m = 10,000$. Then the number of operations required to break the cipher by the root finding method is on the order of $n^2(\log N)^2$, or 5×10^9 . At a rate of a million operations a second, it would take about 17 years to break the cipher using this approach.

The expected number of tries needed to break one port of a set of m cipher-ports is P/nm , or 3×10^9 when $m = 10,000$. Assuming it takes 1 msec to compute $F(x)$, it would take 40 days of CPU time to break just one port out of a set of 10,000, and even then, chances are that the port thus obtained would be no use whatsoever to the cracker.

As an example of a computationally hard to invert one-way cipher we can look at the work of Evans et al. [Evans74], who, in their proposed one-way cipher, use a small set of one-to-one mappings, which eventually produce a ciphertext. In a nutshell, their scheme works as follows: Assume the one-way cipher must map n -bit plaintext-ports onto n -bit ciphertext-ports. Let $f_1, f_2, \dots, f_k$ be k different scrambling functions. Each of the f_i must be one-to-one, to keep the degeneracy within bounds. The scrambling functions take an intermediate result X of the calculation into a new value of X . Some of the functions may be parameterised by the original plain-port P , or a small integer, m , derived from P or X . Possible scrambling functions can be:

- rotate m bits
- permute bits, fixed or calculated (from P or m)
- compute the non-carrying binary sum or the XOR of P and X .
- add a constant, or a quantity calculated from P to each byte of X .
- choose some of the machine instructions that can be used to perform some one-to-one transformation of X , parameterised by P or m . Use a subset of these, calculated from P .

Fig. 1 shows how these functions are then used to transform P into a cipher-port V , via a succession of X s. K is the number of different scrambling functions, J is the number of cycles, and the function $next$ computes new values of X from old. The function q_k derives small integers from P and X .

The result of the one-way cipher thus obtained, is very hard to analyse, and the degeneracy is probably very small [Evans74]. Each of the f_k is one-to-one. The composition of one-to-one functions is also one-to-one, but Evans' algorithm is not an ordinary composition of the f_k , but one depending on the value of P , which makes it possible that it is no longer one-to-one. This type of one-way ciphers is most suitable for our needs: the degeneracy is small, so a trial and error approach will take a very long time to yield results, and other approaches to cracking the cipher are not known. The cipher can be chosen such that it takes, for instance, 20 msec to compute, limiting the number of tries in

```

const J = NumberOfCycles; {e.g., 5}
      K = NumberOfDifferentScramblingFunctions;
function F(P: port): port;
var X,V      : port
    j,k,m,M  : integer;
begin
  X := P; V := P;
  for j := 1 to J do
  begin
    for k := 1 to K do
    begin
      M := qk(P,X);
      for m := 1 to M do
        V := fk(V,P,X)
      end;
      X := next(X)
    end;
  end;
  F := V
end;

```

Fig. 1. Calculation of Evans et al.'s one-way cipher

an attempt to break it to 50 per second. At this rate, with a degeneracy of say three, it will take 6 years on average to get just one plaintext-port of a set of 10,000 48-bit ciphertext-ports, not counting the time needed to look up the result of the encryption to see if a port has been cracked. With a 64-bit port, the time is at least 256 times longer.

Another well known approach to finding computationally hard to invert one-way ciphers, is to use a cryptosystem as a basis. Good results can often be obtained by using the number to be enciphered as the key to encrypt a known constant. Consider as an example the *Data Encryption Standard*, DES [Standards77]. The key for this cipher is 56 bits, and it is used to encrypt or decrypt 64 bit quantities at a time. DES can be turned into a one-way cipher by encrypting a known 64-bit constant, using the plaintext as the key.

Protection without F-Boxes

Earlier we said that protection could also be achieved without F-boxes. It is slightly more complicated, since it uses both conventional and public-key encryption, but it is still quite usable. The basic idea underlying the method is the fact that in nearly all networks an intruder can forge nearly all parts of a packet being sent except the source address, which is supplied by the network interface hardware. To take advantage of this property, imagine a (possibly symmetric) conceptual matrix of conventional (e.g., DES) encryption keys, with the rows being labeled by source machine and the columns by destination machine. Thus the matrix selects a unique key for encrypting the *capabilities* in any packet. The data need not be encrypted, although that is also possible if needed.

Each machine is assumed to know its row and column of the matrix, and nothing else (how this will be achieved will be discussed shortly). With this arrangement, intruder *I* can easily capture packets from client *C* to server *S*, but attempts to "play them back" to the server will fail because the server will see the source machine as *I* (assumed unforgeable) and use element M_{IS} as the decryption key instead of the correct M_{CS} . No matter what the intruder does, he cannot trick the server into using a decryption key that decrypts the capabilities to make sense, that is, to contain random numbers that agree with those stored in

the file tables.

To avoid having to run the encryption/decryption algorithm frequently, all machines can maintain a hashed cache of capabilities that they have been using frequently. Clients will hash their caches on the unencrypted capabilities in the form of triples: (unencrypted capability, destination, encrypted capability), whereas servers will hash theirs in the form of triples: (encrypted capability, source, unencrypted capability).

To set up the matrix initially, the following procedure can be used. A public server, such as a file server, makes its put-port and a public encryption key known to the whole world. When a new machine joins the network (e.g., after a crash or upon initial system boot), it sends a broadcast message announcing its presence. Suppose, for example, the file server has just come up, and must (1) prove that it is the file server to other processes, and (2) establish the conventional keys used for encrypting capabilities in both directions.

A client machine, C , which receives the broadcast from the alleged file server, F , picks a new conventional encryption key, K , for use in subsequent C to F traffic and sends it to F encrypted with F 's public key. F then decrypts K and replies to C by sending a packet containing both K and a newly chosen conventional key to be used for reverse traffic. This packet is encrypted both with K itself and with the inverse of F 's public key, so C can use K and F 's public key to decrypt it. If the decrypted packet contains K , C can be sure that the other conventional key was indeed generated by owner of F 's public key, thus convincing C that he is indeed talking to the file server. Both of the above-mentioned conditions have now been fulfilled, so normal communication can now take place. Note that the use of different conventional keys after each reboot make it impossible for an intruder to fool anyone by playing back old packets.

Capabilities

To control access to objects, *capabilities* are used [Dennis66]. A capability works like a ticket: if the holder can show possession of a capability for an operation on an object, he is allowed to carry out that operation on that object. In traditional capability systems, capabilities are managed by the operating system kernel [Wulf74]. The operating system controls handing out capabilities, copying them, giving them away, destroying them. Each capability holds a number of *rights*, each right protecting one or more operations on the object it is for. The more rights a capability holds, the more powerful it is.

Clearly, in our model of a distributed system, capabilities cannot be handled by the operating system kernel. Instead, capabilities are given directly to the clients, who keep them in their own address space. There is nothing to prevent a user in this method to prevent him from giving away the bit-pattern that represents his capability to another user, or to attempt to construct a bit-pattern that functions as a capability.

Giving away capabilities need not be prevented. A client who gives away a capability for an operation on an object, gives away the right he already has to carry out that operation on that object. He could have given away that right in a conventional capability system by carrying out operations (using his capability that he cannot give away) on behalf of other users (that he would like to give his capability to). The prevention of forgery of capabilities is a much more serious problem. If this problem can be solved, a service need not check the identity of its clients, nor need it know whether its client can be trusted; the presented capability is sufficient proof of the right to carry out the requested operation.

An capability for object O managed by service S is defined as a bit string, made up of two parts, a *port-part*, for service S , and a *private part*, interpreted by service S as a capability for object O . This is illustrated in Fig. 2. The semantics of the *port-part* will be explained in a later section, suffice it to mention here that it is a capability, allowing a client to talk to service S .

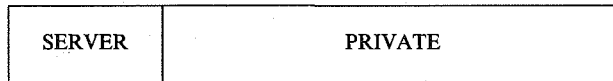


Fig. 2. Layout of a capability with a port-part and a private part

The designer of the service is free to determine both the length and the semantics of the private part. Most services up to date use an 80-bit private part for a 128-bit capability. Often, the private part will contain an *object* field which is used as an index into a table of objects, a *rights* field, indicating what rights the capability holds for the object, and a *check* field which makes the capability sparse (see Fig. 3). Sparseness is essential for protection; capabilities are kept in user space, so a malicious user may try to forge capabilities by creating bit strings and passing them off as capabilities. By making capabilities sparse enough, the probability of a user succeeding in coming up with a bit string that is a legal capability can be made arbitrarily small.

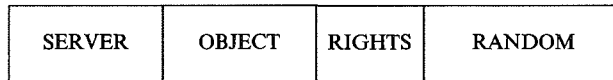


Fig. 3. Lay out of a typical capability

The *check* field of a capability must depend on the *object* field and the *rights* field. If this were not the case it would be trivial, knowing a capability for one object, to create capabilities with different rights for that object, or to construct capabilities for other objects as well. Typically a server will encrypt the object number, the rights field and possibly a random number, using a one-way cipher and use the result as the *check* part of the capability.

There is no compulsion to adhere to the capability structure of Fig. 3, but it is a general form, and it will be used to illustrate how operations on capabilities can be implemented. Some services, for instance, may not distinguish different rights on their objects, so they will not have a *rights* field. Other services may not use objects (e.g., compiler service), but have different rights (e.g., for debugging options); such services will not use an *object* field.

Operations on Capabilities

The operations on capabilities are not just limited to presenting it to a service for inspection so access is granted to an operation on an object. It is possible to give capabilities away to other clients, giving them permission to perform the same operations on the object. New capabilities can be derived from old with a subset of the rights of the original one, or capabilities can be made invalid. In this section the operations on capabilities are discussed: *capability passing*, *restrict*, and *retract*.

Capability passing is trivial in a system where capabilities are kept in user space; users have direct control over them. A user with a capability for an object can give another user the same rights to the object by just giving away a copy of the capability. In fact, there is no way to prevent users from giving away capabilities. By some, this is viewed as a defect of our capability system. Others hold the opposite viewpoint [Donnelley81]. Suppose user

A holds a capability for some object, and *A* is not allowed to give that capability to user *B*. However, *A* can give a *capability for that capability* to *B*. All *A* needs to do is forward requests for operations using that capability from *B* to the server. *A* has then effectively given away the capability to *B*. It is because of this that we have decided it is useless to restrict capability passing.

Although we believe it is useless to restrict capability passing, it is not difficult to implement. There is a simple mechanism which makes a capability that works in the hands of one user useless in the hands of another. In order to make this work, users must provide an authenticating *signature* with each request (discussed in a following section). A service that wants to hand out a capability that works in the hands of just one user, encrypts the original capability with the signature before giving it to that user. When the capability is subsequently presented to the service, the original is encrypted with the signature and compared to the presented capability. If there is a match, the capability was valid. If not, either the capability or the signature was wrong; in the latter case, it was a capability that was given away.

In this scheme it is still possible to give capabilities away to other users, but this requires giving away the authenticating signature as well. We do not know any systems, however, where this is not possible: Every operating system that claims to be secure uses passwords for user authentication; giving away one's signature in amounts to the same thing as giving away one's password in another operating system.

Before giving away a capability to another user, it is often necessary to *restrict* that capability; that is, take away some of the rights in the capability. Again we consider the example of a file server. When a client requests the file server to create a file, the server returns an *owner* capability, a capability with all the rights on. Often the client will allow others to read the file, and perhaps allow some to write it or append to it as well. It will be seldom, however, that a client will give the *owner* right away, the right to remove the file altogether, and the right to retract the existing capabilities (make the existing capabilities illegal). First these rights have to be removed from the capability.

In conventional capability systems, where the capabilities are managed by the operating system this is easy: when a "pass capability" system call is made, the client specifies which rights should be passed, and the operating system will strip some rights bits before copying the capability. In our system this is more difficult, since capabilities are in user space. If the client would just strip some rights bits and then give the capability away, there is nothing to prevent the recipient to add these bits on again.

The usual way to do *restrict* is to ask the server to create a restricted capability. The capability of Fig. 3, for instance, can be constructed by making the *check* field depend on the *object* and *rights* fields. To make a restricted capability, the server would clear selected *rights* bits and recompute the check field. This is a straightforward mechanism, but it requires an extra transaction with the server, each time a (new) restricted capability is required. In practise, the message traffic need not increase at all, however, if servers allow their clients to ask for a number of capabilities with different rights the moment an object is created. Apart from the *owner* capability, a user would then receive a few other capabilities "for giving away."

An alternative scheme exists that allows clients to construct capabilities with restricted rights themselves. Naturally, this mechanism can only be used to remove rights, not add them. The method is based on *one-way ciphers*, which, as it turns out, find many applications. The mechanism works as follows.

We start with the familiar capability lay out of Fig. 3. We assume there are *k* rights, numbered from 1 to *k*. Each right is represented by one bit in the *rights* field, a one when the right is present, a zero when it is absent. Initially, the server constructs a capability

with all the rights on, the *rights* field is set to all ones, and the *check* field is set to some random number. One random number is chosen per object, and stored along with the object.

Let us now assume there are k one-way ciphers, $G_1, \dots, G_k$, one for each right, that are *commutative*, that is,

$$G_i G_j(R) = G_j G_i(R) \quad \text{for all functions } G_i \text{ and } G_j.$$

The functions G_i form a mapping of the *check* field onto itself. The server makes the functions G_i public, and clients can restrict capabilities by proceeding as follows: Given a capability with right i on, a new capability with right i off is created by clearing the i 'th *rights* bit, and applying G_i to the *check* field. The capability thus constructed can be further restricting by repeating the procedure over and over. The commutativity of the one-way ciphers ensures that the order in which the rights are removed is irrelevant.

When presented with a capability, the server can easily check the validity by applying the one-way ciphers associated with the absent rights (indicated by the rights bits in the *rights* field of the presented capability) to the original random number (which was stored along with the object itself). If this yields the same *check* field as the one in the presented capability, the capability is genuine.

It is an interesting exercise to find a set of commutative one-way ciphers. We have succeeded in creating such a set, based on the RSA public key algorithm [Rivest78]. It is not always practical, however, due to the enormous size of the *check* field, necessary for this method. This is how it works.

Choose a number n of sufficient size that it cannot be factored (this may be done by taking the product of two or more large primes, as in the RSA algorithm). Also choose k numbers $e_1, \dots, e_k$. These numbers must be chosen in a special way, which will be explained later. Define $G_i(R)$ ($i = 1, \dots, k$) as follows:

$$G_i(R) \equiv R^{e_i} \pmod{n}$$

Then the functions G_i are commutative:

$$G_i G_j(R) \equiv R^{e_i e_j} \pmod{n} \equiv R^{e_j e_i} \pmod{n} \equiv G_j G_i(R) \pmod{n}$$

The G_i commute, but are they one-way ciphers? They are, if the e_i are chosen to be relatively prime to $\phi(n)$. In order to see this, note that each of the G_i can be viewed as an RSA public-key encryption function with the decryption function thrown away. The arguments for the robustness of the RSA algorithm also apply to our one-way ciphers. In Rivest, Shamir and Adleman's paper a discussion can be found on the security of the algorithm [Rivest78].

The e_i must be chosen carefully. Suppose e_i is a multiple of e_j . Then, having a capability without right j , it is possible to change it into a capability without right i , by raising the *check* field to the power $\frac{i}{j}$, thus giving a capability without right i , but *with* right j . But if all the e_i are co-prime such constructions are not possible. In fact, another interesting construction becomes possible if the e_i are co-prime. Suppose a client holds two capabilities that differ in one aspect: one has right j but does not have right i and the other has right i but does not have right j . The client that holds these capabilities can combine the two to make one capability that has both right i and right j by choosing two numbers d_i and d_j , such that $e_i d_i - e_j d_j = 1$. Note that such numbers exist since e_i and e_j are co-prime. The capability that contains right i , but not right j contains some random number R , raised to the power e_j , while the other capability contains the same number R , raised to the power e_i . What is needed for the combined capability is the number R itself. This number can easily be found by computing

$$R \equiv \frac{R^{e_i d_i}}{R^{e_j d_j}} \pmod{n}$$

This computation is feasible if $R^{e_i d_i}$ is co-prime with n . This is the case with a high probability, since n is the product of two very large primes.

Sometimes, the combination of two capabilities with two different rights into one with both rights is undesirable, because, for instance, the combined capability allows an operation that cannot be realised with the two capabilities separate. This can be done, using the following mechanism: Let $p_1, \dots, p_k$ be k different primes, and let P denote the product of these primes. Define the e_i as P / p_i . If the p_i are co-prime with $\phi(n)$, this yields commutative one-way ciphers that do not allow combination of capabilities.

The two above methods can be combined to yield a set of rights, some of which may be combined, while others may not. All this is based on the property that, if all the capabilities a client has, have a common factor in the exponent, that factor cannot be removed. If a subset of the e_i of size s have a common factor p in them, and a client has no capabilities with more than s' rights, a client cannot combine more than s' rights into one capability, because of a common factor $p^{s-s'}$ in the exponents. Other factors can be used to prevent other combinations of capabilities.

The last useful property of the commutative one-way ciphers, based on RSA, is the possibility to make *verifiable* capabilities; that is, by a simple computation a client can verify the authenticity of a received capability without having to consult the server. This method uses public signatures: When the server sets up the commutative one-way ciphers, it chooses k (e_i, d_i) pairs. The e_i must be chosen co-prime, or not co-prime, or a combination thereof to realise or prevent the possibility of combining capabilities. Let the product of the d_i be D . When the server generates random numbers R , to be associated with the different objects, some publicly known redundancy is added. Thus, the numbers R can be recognised. When the server gives away a first capability with full rights, R^D is put in the check field. Clients then strip rights in the normal fashion, by raising the random number to the various e_i . To verify a capability, all remaining rights are stripped off. The check field then contains $R^{D \cdot e_1 \cdot e_2 \cdot \dots \cdot e_k} = R$ and the known redundancy can be recognised. Note that it does no harm that clients know R , since only R^D can be used to form capabilities with all rights on, and D is not known outside the service.

It is unfortunate that this method for restricting capabilities is not yet practical, because of the large *check* fields needed, caused by the large moduli required for sufficient security. But we deemed the method interesting enough to mention anyway. The method might be applied in environments where capabilities must be made very secure and their size is not too large a price to pay for that security.

A compromise between *restrict* implemented inside the server, and *restrict* by the client using commutative one-way ciphers, is to use one-way ciphers that do not commute. These can be used in two ways: the simplest way is to allow rights to be stripped only in a predefined order. The commutative property is not necessary then. In many cases this restriction on the order in which rights can be stripped is not so severe as it seems. On a file, for instance, a typical order of the rights could be *owner*, *write*, *append*, and *read*. Only in few applications the rights will have to be taken off in any different order. In these cases, a request could be sent to the server to create a special capability.

When rights can only be taken off in one predefined order, there is no need for a different one-way cipher for each right. One cipher will do, the number of times it is applied then serves as the indication of what rights are still present. In fact, the *rights* field can be totally dispensed with. When the size of the *check* field is taken to be the same size as that of a *port*, the standard one-way cipher C can be used.

A method that does not require commutative one-way ciphers, but allows taking away rights in any order, requires that capabilities contain the order in which rights were taken away. The server can then perform the same computations as the client in order to check the validity of a capability. This method does need k different one-way ciphers for k different rights. The number of orders in which k rights can be taken away is $k!$, so the number of bits needed to store this information is $\log_2 k!$. For example, for 4 rights, 8 bits are needed, for 8 rights, 20 bits and for 16 rights, 50 bits.

The third operation on capabilities is *retract*. This operation invalidates all extant capabilities for an object, and gives the owner a new one. In conventional capability systems *retract* is a complicated operation, requiring indirect objects, back pointers and other complicated machinery (see, for example, [Jones75]); here, *retract* is childishly simple: the server need only change the object's random number, and give the owner the new capability derived from it. All extant capabilities automatically become void. The *retract* right is, of course, a powerful right, which should not lightly be given away. Possession of this right allows the holder to make the object inaccessible to everyone else. In practise, *retract* will be protected by the *owner* right, or by a separate rights bit.

Conclusions

This paper shows that it is possible and practical to build capability-based distributed operating systems, with capability management outside of the operating system kernel. Since the operating system itself is particularly vulnerable to attack in an office environment as we have described, our method is more secure than traditional protection schemes that must rely on the security of the operating system kernel.

Two methods have been presented for the implementation of authenticated communication between client and server processes, one using F-boxes, the other using a combination of public key encryption and conventional encryption techniques. Currently public key encryption is still expensive, both in terms of computational effort (it is slow) and storage requirements (PKE keys are large). The F-box mechanism is a good alternative until fast public key algorithms arrive. F-boxes can be put in the cable ducts, on the network interface cards, in integrated circuits that carry out the network protocol, or, if necessary, in the operating system kernel.

Capability management need not be carried out by a secure operating system: all operations on capabilities that are currently implemented in secure operating system kernels can also be carried out by choosing appropriate encryption techniques, with which client processes can be allowed to handle capabilities and carry out certain (restricted) sets of operations on them.

References

- [Berlekamp70]
Berlekamp, E. R., "Factoring polynomials over large finite fields," *Mathematics of Computation*, vol. 24, no. 111, pp.713-735, July 1970.
- [Dennis66]
Dennis, J. B. and Horn, E. C. van, "Programming Semantics for Multiprogrammed Computations," *Comm. ACM*, vol. 9, no. 3, pp.143-155, March 1966.
- [Donnelley81]
Donnelley, J. E., "Managing Domains in a Network Operating System," *Proc. of the On-Line Conf. on Local Networks & Distributed Office Systems*, pp.345-361, May 1981.
- [Evans74]
Evans, A., Kantrowitz, W., and Weiss, E., "A User Authentication Scheme Not Requiring Secrecy in the Computer," *Comm. ACM*, vol. 17, no. 8, pp.437-442, August 1974.
- [Jones75]
Jones, A. and Wulf, W. A., "Towards the Design of Secure Systems," *Software P & E*, vol. 5, pp.321-326, 1975.
- [Knuth69]
Knuth, D. E., *The Art of Computer Programming, Vol. II*. Reading, Mass: Addison Wesley, 1969.
- [LeVeque56]
LeVeque, W. J., *Topics in Number Theory*. Reading, Mass.: Addison Wesley, 1956.
- [Mullender82]
Mullender, S.J. and Tanenbaum, A.S., "Protection and Resource Control in Distributed Operating Systems", IR-79, Vrije Universiteit, Amsterdam, August 1982.
- [Purdy74]
Purdy, G. B., "A High Security Log-in Procedure," *Comm. ACM*, vol. 17, no. 8, pp.442-445, August 1974.
- [Rivest78]
Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Comm. ACM*, vol. 21, no. 2, pp.120-126, Februari 1978.
- [Standards77]
Standards, National Bureau of, "Data Encryption Standard," *Fed. Inf. Process. Stand. Publ. 46*, January 1977.
- [Wilkes68]
Wilkes, M. V., *Time-Sharing Computer Systems*. New York: American Elsevier, 1968.
- [Wulf74]
Wulf, W., Cohen, E., Corwin, W., Jones, A., Levin, R., Pierson, C., and Pollack, F., "HYDRA: The Kernel of a Multiprocessor Operating System," *Comm. ACM*, vol. 17, no. 6, pp.337-345, June 1974.

HET MUNTEN-WEEG-PROBLEEM.

De vraag van dit probleem luidt in zijn eenvoudigste vorm:

Gegeven is een verzameling van $(3+w-1)/2$ munten waarvan precies één munt vals is, hetgeen zich uit in een afwijkend gewicht. Daarnaast staat één echte munt ter beschikking, alsmede een weegschaal waarmee gewichten kunnen worden vergeleken. Gevraagd wordt om met w wegingen de afwijkende munt te vinden en ook te weten te komen of hij te licht dan wel te zwaar is.

Hoewel dit probleem voor bijv. $w=5$ wel ingewikkeld, maar niet echt moeilijk is, is bij mijn weten een ordelijke oplossing niet beschreven, zodat dat nu maar eens moet gebeuren.

De uitkomst van een weging is: rechts lichter, gelijk of rechts zwaarder. Met w wegingen kunnen dus in principe $3+w$ mogelijkheden worden onderscheiden, dat is dus één meer dan vereist.

Het is duidelijk welke uitkomst over is: als alle wegingen in evenwicht zijn moet de bewering "er is precies één valse munt" onjuist zijn. Aangezien de vraag "te licht of te zwaar?" gesteld wordt moeten alle munten op de weegschaal hebben gelegen, het evenwicht moet dus minstens één keer verstoord zijn.

Het resultaat van w wegingen wordt een code van w 3-waardige digits. In het geval dat we deze digits als volgt kiezen: rechts lichter: 0 ; gelijk: 1 ; rechts zwaarder: 2 stelt de code een getal in het 3-tallig stelsel voor. We moeten nu dus proberen deze getallen zó aan de mogelijke conclusies toe te voegen dat uitvoerbare wegingen tot de gewenste code leiden.

Het is duidelijk dat complementaire mogelijkheden (dezelfde munt is te licht of is te zwaar) aanleiding geven tot complementaire getallen ($\{0,1,2\} \rightarrow \{2,1,0\}$). Als we de munten nummeren kunnen we ze dus toevoegen aan het betreffende getal, dit vult de codes tot de verboden code van uitsluitend énen en daar voorbij komen dan de complementen.

Open blijft nog de vraag: te licht of te zwaar. Zouden we voor alle munten dezelfde keus maken dan schrijft de code van de meest significante digit voor dat $3+(w-1)$ munten aan één kant van de weegschaal komen en geen (te onderzoeken) munten aan de andere kant. Voor $w>1$ komen we dan dus goede munten tekort om zinvolle wegingen te kunnen uitvoeren.

De voor de hand liggende oplossing is nu de omschrijving "te licht" en "te zwaar" steeds af te wisselen, dus bijv. voor de even genummerde munten "munt te licht" en voor de oneven genummerde "munt te zwaar" toe te voegen aan de code van de wegingen. Op deze wijze blijkt dat het aantal munten dat bij een weging links moet liggen altijd één verschilt van het aantal dat rechts moet liggen, de bijgevoegde echte munt maakt de weging dan uitvoerbaar.

Op deze manier is dus het probleem in zijn eenvoudigste vorm opgelost. Er blijven nog een aantal varianten over die nu niet moeilijk meer zijn. Zij berusten erop dat de verboden code kan worden toegevoegd aan het vals zijn van een extra munt, die dus niet bij de wegingen wordt betrokken, en op de eigenschap dat de munt met code afwisselend 0 en 2 altijd aan de overbevolkte kant ligt, als we deze munt weglaten hebben we geen echte munt nodig.

TOEKOMST-VISIOEN.

Na enkele honderden publikaties en een aantal wereldrecords, mag Arjen van zijn pensioen genieten. Om het luisteren naar opera's met iets anders aangenaams af te wisselen start hij een ambitieus projekt:

De simulatie van een Cray-1 super-computer.

Dit door nostalgie ingegeven projekt moet bekroond worden door het laten lopen van een oud (jaren '80) priemgetal programma. Zelf ziet Arjen de Fortran compiler als de finishing touch van het projekt, tenslotte is programmeren in Fortran een excellent voorbeeld van zelfkastijding.

De Zesde generatie computers waarop de simulatie moet lopen wordt geprogrammeerd in Algol'007. Deze verre nazaat van Algol'68 kent 37 vormen van nul. Daar kunnen zelfs de Japanners, met 19 woorden voor "nee" niet tegenop! De wiskundige achtergrond van Algol'007 blijkt verder uit de eindeloze variatie van oneindigheden. Interessant is dat de religie en de wiskunde elkaar vinden in deze wereld van nirwana tot infinity. Arjen verfoeit deze nieuwe hang naar het religieuze:

Wiskundigen die het nirwana prediken, moeten hun mond met zeep spoelen!

Als afsluiting van het projekt wil Arjen de laatste stelling van zijn proefschrift herberekenen, met een inflatie korrektie voor de bedragen.

Gabbit.

ETRE OU NE PAS ETRE UN CARRE

On peut se demander si Hamlet possédait un bon algorithme pour résoudre son problème existentiel. J'espère que, docteur, Arjen saura construire pour lui-même un tel algorithme qui marche en temps réel. A défaut de lui proposer une solution, je vais parler d'un problème similaire, mais un peu moins profond.

Pour déterminer si un entier N est un carré parfait, on peut utiliser la racine carrée réelle de l'ordinateur en testant si N est égal à :

$$\text{INT} (\text{SQRT} (\text{FLOAT} (N) + .5)) ** 2$$

On peut aussi écrire un sous-programme de calcul de la racine carrée en nombres entiers par la méthode de Newton :

$$X_{k+1} = \frac{1}{2} (X_k + N/X_k)$$

On peut, pour gagner du temps, tester d'abord si N est un carré modulo M où M est un nombre que l'on se fixe. Si oui, on applique l'une des méthodes précédentes, sinon c'est terminé.

Comment choisir M ? Dans son article : " Factoring large integers " R. SHERMAN LEHMAN (Math. of comp. 28, 1974, p. 637-646) utilise $M = 729$. Ce n'est pas le meilleur choix.

Appelons $q(n)$ le nombre de carrés mod n . La fonction q est multiplicative : si m et n sont premiers entre eux, on a :

$$q(mn) = q(m) q(n)$$

et l'on a :

$$q(2^\alpha) = [2^{\alpha/6}] + 2$$

et pour $p \neq 2$:

$$q(p^\alpha) = \left[\frac{p^{\alpha+1}}{2(p+1)} \right] + 1$$

où $[x]$ désigne la partie entière de x . On dira que n est un nombre " de petit q " si la probabilité d'être un carré modulo n est plus faible que pour les nombres précédents, autrement dit si :

$$m < n \Rightarrow q(m)/m > q(n)/n$$

Les méthodes des nombres hautement composés s'appliquent à ce problème et l'on a la table où figure entre parenthèse la valeur $n/q(n)$:

Table des nombres " de petit q "

2	(1.)	3	(1.5)	*4	(2.)	8	(2. 67)
12	(3.)	*16	(4.)	32	(4.57)	*48	(6.)
80	(6.67)	96	(6.86)	112	(7.)	*144	(9.)
240	(10.)	288	(10.29)	336	(10.5)	480	(11.43)
560	(11.67)	576	(12.)	*720	(15.)	1008	(15.75)
1440	(17.14)	1680	(17.5)	2016	(18.)	2640	(18.33)
2880	(20.)	3600	(20.45)	4032	(21.)	*5040	(26.25)

Avec l'accord du guide Michelin, nous avons signalé par une étoile les nombres analogues aux nombres hautement composés supérieurs et qui sont particulièrement recommandés.

Il arrive dans certains cas que les nombres à tester ne sont pas distribués de façon aléatoire modulo 2 et que l'on préfère prendre M impair. Sont alors conseillés :

45	(3.75)	315	(6.56)	3465	(12.03)
----	--------	-----	--------	------	---------

Le choix de M dans ces tables dépend du nombre de mémoires dont on dispose. On construit alors un tableau $T(1) \dots T(M)$, où $T(I)$ vaut 1 si I est un carré modulo M, et 0 sinon. Le nombre N ne sera pas un carré si $T(\text{MOD}(N, M)) = 0$.

J.L. NICOLAS

Département de Mathématiques
Université de Limoges
123, Avenue Albert Thomas
F-87060 LIMOGES CEDEX

A DISPROOF OF THE REIMANN HYPOTHESIS

M.A. Odlyzko

Bell Laboratories, Murray Hill, NJ 07974, USA

The lattice basis reduction algorithm of Arjen Klaas Lenstra, Hendrik Willem Lenstra, Jr., and Laszlo Lovász [1] has led to immense progress in factorization of polynomials, public key cryptography, and analytic number theory. At about the same time, the English "cyberneticist and educationist" [2] Arnold Arnold has evolved a "general systems analytic computer program generator" [2] of "immense analytical potential" [2], which has enabled him to prove Fermat's Last Theorem and demonstrate that the Mersenne number $M(p) = 2^p - 1$ for $p = 2,143,138,339$ is prime (the existence of the divisor $2 \cdot 69 \cdot p + 1$ being only an illusion due to unreasonable adherence to the "contemporary mathematical and semantic dogma" [2]). What appears not to have been noticed before, though, is that it is possible to combine "the multi-dimensional vector techniques" [2] of Arnold Arnold with the Lenstra-Lenstra-Lovász lattice basis reduction algorithm. What results from such a combination is a plethora of stunning mathematical discoveries, one of which is that the zeta function has zeros at

$$\frac{1}{2} \pm u^{-1} \pm iu,$$

where

$$u = 782,367,441,744,522,748,794,340,361,500, \\ 121,107,356,850,262,876,798,925.232643559.$$

This, of course, disproves the notorious Reimann hypothesis! Further results of the new theories will be announced in due course.

References

1. A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982), 515-534.
2. *The Manchester Guardian*, Dec. 1983 and Jan. 1984.

SOME NP-HARD PROBLEMS CONNECTED WITH THE
EXTENDED EUCLIDEAN-ALGORITHM FOR
n-INTEGERS

by

Azaria Paz

October 1983

I would like to offer this survey and paper to Arjen K. Lenstra,
who introduced me to beautiful operas and whose hospitality I enjoyed
for several days in Amsterdam.

Azaria Paz

1. Introduction

The greatest common divisors (gcd) of $n > 2$ positive integers $a_1, \dots, a_n$ can be calculated by successively calculating $\gcd(a_1, a_2)$ then $\gcd(\gcd(a_1, a_2), a_3)$ etc. The steps of this algorithm can be traced back so as to determine integers x_i satisfying

$$\sum_{i=1}^n x_i a_i = \gcd(a_1, \dots, a_n) \quad (1)$$

Blankinship [1] proposed a different algorithm for calculating $\gcd(a_1, \dots, a_n)$ together with the x_i 's as defined above (1). Blankinship's algorithm eliminates the need for backtracking and produces the coefficients $x_1, \dots, x_n$ in (1) on line. Bradley [3] modified Blankinship's algorithm showing that the calculation of $\gcd(a_1, \dots, a_n)$ can be done in $n-2 + d(a_1, a_2)$ division steps where $d(a_1, a_2)$ is the number of division steps needed for calculating $\gcd(a_1, a_2)$, using the ordinary Euclidean algorithm, and $a_1 < a_2 \dots < a_n$. Lamé [8] showed that $d(a_1, a_2)$ is bounded by $\log_g a_1$ where $g = (1 + \sqrt{5})/2$ and showed also that this bound is sharp in a certain sense. It follows that the number of division steps needed for calculating $\gcd(a_1, \dots, a_n)$ is bounded by $n-2 + \log_g a_1$.

It is obvious that the equation (1) has infinitely many solutions with integral x_i 's. Bradley [loc cit] has shown that a solution which is "minimal" in a sense defined in his paper, can be constructed at some extra cost (linear in n). The minimal solution defined by Bradley has the property that the product of the nonzero coefficients x_i is bounded by $|a_n|^{k/2} \cdot \gcd(a_1, \dots, a_n)$ where $a_n = \max(a_1, \dots, a_n)$, and k is the number of nonzero coefficients in the solution.

Another modification of Blankinship's algorithm was suggested by Morito and Salkin [9]. Their algorithm produces, together with a solution of the equation (1) a set of generators for the set of all integral solutions of the equation

$$\sum_{i=1}^n x_i a_i = 0 \quad (2)$$

Moreover based on heuristic considerations and on computational experience, they claim that the coefficients x_i generated by their algorithm are relatively small, a desired property from a computational point of view (for some practical applications, see Morito, Salkin and Mathews [10]).

Given an equation as in (1), let $s(a_1, \dots, a_n)$ be defined as follows: Let X be the set of all solutions of (1). For $x = (x_1, \dots, x_n) \in X$ set

$$x_* = \max_i |x_i|$$

Then,

$$s(a_1, \dots, a_n) = \min\{x_* : x \in X\}$$

Let $\hat{x} = (\hat{x}_1, \dots, \hat{x}_n)$ be a vector in X such that $x_* = s(a_1, \dots, a_n)$. It would be nice to have an algorithm for finding such a solution $\hat{x}$, which is "minimal" in a strong sense. Unfortunately, as will be shown in the next section, finding such a solution is NP-hard. In the third section of the paper a new algorithm of Blankinship type will be presented. The algorithm is subtractive (uses no divisions) and tends to keep the coefficients of the solution small.

The 4th section of the paper discusses the complexity of the new algorithm. The last section of the paper considers the case where the a_i 's are Gaussian integers.

2. Finding a "Minimal" Solution is NP-Hard

For the sake of simplicity we assume in the sequel that $\gcd(a_1, \dots, a_n) = 1$; the general case is similar. Consider the following problem:

AES (almost equal subsets):

Given n integers $a_1, \dots, a_n$, set $I_n = \langle 1, 2, \dots, n \rangle$.

Question: Are there two disjoint subsets of I_n , I'_n and I''_n , such that

$$\sum_{i \in I'_n} a_i - \sum_{j \in I''_n} a_j = 1$$

where $I'_n \cap I''_n = \emptyset$ but $I'_n \cup I''_n$ may be a proper subset of I_n .

Lemma 1. If $s(a_1, \dots, a_n)$ can be calculated in polynomial time, then AES is in P.

Proof: Two almost equal sets exist if and only if the equation

$$\sum_{i=1}^n a_i x_i = 1 \quad (3)$$

has a solution such that for all i , $x_i = 0$ or $|x_i| = 1$. But the equation (3) has such a solution if and only if $s(a_1, \dots, a_n) = 1$. Thus, to solve a given AES problem calculate $s(a_1, \dots, a_n)$ and answer 'yes' if and only if $s(a_1, \dots, a_n) = 1$.

Consider now the problem AEP (almost equal partition): This problem is the same as AES but we require that $I'_n \cup I''_n = I_n$.

Lemma 2. If AES is in P then AEP is in P.

Proof: The proof is by polynomial reduction and is similar to a proof given by A. Shamir [11]. For the sake of completeness we reproduce here a proof of M. Blum [2, private communication] which is somewhat simpler than Shamir's proof.

Assume that the integers $a_1 < a_2 \dots < a_n$ are given in decimal notation (this assumption is not restrictive). Set $k = \log_{10} a_n$ and define $2n$ integers b_i as follows:

If a_i has $d(\leq k)$ digits then a_i is the sequence of k digits with zeros in the left $k-d$ positions, and a_i in the right d positions. The b_i 's are the integers represented in the rows of the table below, where the leftmost zeros in each row are ignored.

	n	$\log_{10} n$	k
b_1	1 1 0 0	0 0	$\leftarrow a'_1 \rightarrow$
b_2	0 1 1 0	0 0	$\leftarrow a'_2 \rightarrow$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_{n-1}	0 0 1 1		
b_n	1 0 1 0 0	$\leftarrow a'_n \rightarrow$	
b_{n+1}	2 0 0 0 0	0 0	
b_{n+2}	0 2 0 0 0	0 0 0	
$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_{2n}	0 2 0 0	0 0	

It is easily verified that the above construction is polynomial in the length of the input (the sequence of a's). We will show now that an almost equal partition over the a's exists if and only if two almost equal subsets exist over the b's.

Assume first that an almost equal partition exists over the a's, determined by the sets of indices I'_n and I''_n . Two almost equal sets over the b's can be constructed as follows:

Include the b's corresponding to I'_n in one set and the b's corresponding to I''_n in the second set. The sum of the b's in the first set differs by 1 from the sum of the b's in the second set in their last $\log_{10} n + k$ positions (no addition overflow can use more than $\log_{10} n$ positions). Every column in the table 1 has exactly 2 ones. This implies that if the above sums differ in some position $t > k + \log_2 n$ then the difference in that position is equal to 2. If this is the case then we can add to the proper set an additional b_j , $j > n$, to reduce the difference in that position to zero. The construction is completed when the sums of the b's in the two sets are equal in all the positions t , with $t > \log_{10} n + k$.

Assume now that two almost equal sets over the b's are given. Then, by the definition of the b's, at least one of the two sets I' say, must include some b_j , $j \leq n$. It is easy to see that the sum of any proper subset of the b_j which does not include all the b_j , $j \leq n$ has some odd entry which cannot be split into two equal parts. It follows that all the b_j , $j \leq n$ belong to either I' or I'' . Partitioning the a_j 's corresponding to the partition of the b_j 's; $j \leq n$ results therefore in an almost equal partition over the a's (the b_j 's with $j > n$ contribute nothing to the positions t with $t \leq \log_{10} n + k$). This concludes the proof of Lemma 2.

We relate now the well known problem Partition to the problem AEP, where Partition is the same as AEP except that the two subsets are required to be equal.

Lemma 3. IF AEP is in P then so is Partition.

Proof: Given a set of integers $\langle a_1, \dots, a_n \rangle$ construct the set of integers $\langle 3a_1, \dots, 3a_n, 1 \rangle = \langle b_1, \dots, b_{n+1} \rangle$. It is easy to show that the first set can be partitioned into two equal sets if and only if the second set can be partitioned into two almost equal sets. We are now ready to prove the following:

Theorem 1. Let $\langle a_1, \dots, a_n \rangle$ be a set of integers. Calculating a solution $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)$ to (1) such that $\bar{x}_n = s(a_1, \dots, a_n)$ is NP-hard.

Proof: If a solution as above can be calculated in polynomial time then $s(a_1, \dots, a_n)$ can be calculated in polynomial time, which implies, by lemma 1 that AEP is in P. This implies by lemma 2 that AEP is in P and by lemma 3 this implies that Partition is in P. But partition is known to be NP complete [4]. Our theorem is thus proved.

Remark: Two related results have been published in the literature. Van Emde Boas [12] showed that calculating a solution to equation (2) which is "minimal" (i.e. with $\bar{x}_n = s(a_1, \dots, a_n)$), where $s(a_1, \dots, a_n)$ is defined over the set of solutions of (2) is NP-hard. Our proof here, can be modified easily so as to cover the case where the right hand side of (1) is equal to any value (including zero) which is a multiple of the g.c.d. of the a's.

The second result is due to Kannan [5] who showed that calculating a solution to (1) such that $\sum_{i=1}^n |x_i|$ is minimal over the set of all solutions of (1) is also NP-hard.

3. A Subtractive Algorithm for $\gcd(a_1, \dots, a_n)$

The algorithm we want to present here is a Blankinship type algorithm. We explain first the general principle on which it is based.

Given n integers $a_n > a_{n-1} > \dots > a_1$ (we assume that there are no duplicates - as those can be removed - and we assume the integers ordered according to magnitude although this assumption is not essential).

Let I be the $n \times n$ unit matrix and let a be the vector $a = (a_1, \dots, a_n)$ then

$$Ia^T = a^T$$

and, if I_j is the j -th row of I then $I_j a^T = a_j$. We want to find a vector of integers ξ such that $\xi a^T = \gcd(a_1, \dots, a_n)$. Obviously, such a vector ξ is an integral combination of the rows of I . A Blankinship-type algorithm starts with the equality $Ia^T = a^T$ denoted as $A_0 b_0^T = b_0^T$ and generates from it a sequence of equalities $A_1 b_1^T = b_1^T$, $A_2 b_2^T = b_2^T$, $A_k b_k^T = b_k^T$ such that

- (i) Some row of A_i and the corresponding entry in b_i^T are replaced by a linear integral combination of the rows of A_i and the entries of b_i^T , resulting in A_{i+1} and b_{i+1}^T correspondingly, $1 \leq i \leq k-1$.
- (ii) The entry of b_{i+1}^T corresponding to the replaced row is smaller in absolute value than the entry, in the same position, in b_i^T .
- (iii) The gcd of the entries of b_{i+1}^T is equal to the gcd of the entries of b_i^T .
- (iv) The algorithm stops after generating A_k, b_k^T when some entry of b_k, b_{kj} , is either equal to 1 or divides all the other entries of b_k .

It is clear that, because of (ii), there is a k satisfying (iv) so that the algorithm stops. Let ξ_j be the j -th row in A_k corresponding to the entry $b_{kj} = a$ in (iv). Then by (i)

$$\xi_j b_0^T = b_{kj} = \gcd(a_1, a_2, \dots, a_n)$$

(by (iii) and (iv)), so that the vector ξ_j is the required solution of the equation (1). The different versions of the Blankinship-type algorithms differ in the implementation of step (i). Thus the Morito-Salkin algorithm mentioned in the Introduction uses the following substitution rule: Let b_{ip} and b_{iq} be the largest and second largest elements in b_i . Let ξ_p and ξ_q be the corresponding rows in A_i , and let $r = \lfloor b_{ip}/b_{iq} \rfloor$. Then A_{i+1} and b_{i+1} are derived from A_i and b_i by substituting $\xi_p - r \cdot \xi_q$ for ξ_p and $b_{ip} - r \cdot b_{iq}$ for b_{ip} in A_i and b_i respectively. They have not analyzed the complexity (rate of convergence) of their algorithm but it can be shown that the number of iterations of their algorithm is $O(\log a_1)$ where $1 < \alpha < 1.466$ and $\alpha + 1$ when $n \rightarrow \infty$.

The following is a generalization of the classical subtractive (with no divisions) extended Euclidean algorithm for n integers. It is intended to produce a solution to (1) with relatively small coefficients and is inspired by a recent work of N. Karmarkar and R.M. Karp [6]. Karmarkar and Karp considered the following problem (and a more general and related problem): Given a finite set of real numbers $S \subseteq [0,1]$ partition S into two subsets A_1 and A_2 so as to minimize

$$D = D(A_1, A_2) = \left| \sum_{x \in A_1} x - \sum_{x \in A_2} x \right|.$$

While this problem is NP-complete, the authors presented an $O(n)$ -algorithm which, under very general assumptions on the distribution of the inputs will, with probability $\rightarrow 1$ as $n \rightarrow \infty$, produce a partition with $D = O(n^{-c \log n})$ for some $c > 0$.

Any solution as above, is equivalent to the construction of a vector ξ whose entries are equal to ± 1 such that $\xi a^T = D$ where $a = (a_1, \dots, a_n)$ is the vector of inputs. Our algorithm is described below.

4. SGCD(n) (Subtraction GCD for n Integers)

1. Initialization

Given n integers $(a_1, \dots, a_n)$ in the range $[0, M]$, assume that they are all different (otherwise discard duplicates - they will have the coefficient 0 in the final solution of (1)). Define $A_0 = I$ the unit $n \times n$ matrix and $b_0^T = a^T$ where a is the vector $a = (a_1, \dots, a_n)$.

2. Recursive Step

For $0 \leq j$, given that an $m \times n$ matrix A_j ($m \leq n$) and a vector b_j^T of dimension m have been constructed such that $A_j b_0^T = b_j^T$, and the condition for termination is not true, construct A_{j+1} and b_{j+1} as defined below:

Apply algorithm K-K (Karmarkar and Karp [6]) or a similar algorithm (e.g. algorithm A in that paper) to the entries of b_j^T , normalized to fit into the $[0, 1]$ interval. The result can be represented by a vector ξ whose entries are ± 1 and such that $\xi b_j^T = D_j \geq 0$. Let b_{ji} be the maximal entry in b_j and let $A_j[i]$ be the corresponding i -th row in A_j . If $D_j > 0$, then b_{j+1} is derived from b_j by substituting D_j for b_{ji} and leaving all the other entries of b_j unchanged; and A_{j+1} is the matrix derived from A_j by substituting $\xi A_j[i]$ for the row $A_j[i]$ and leaving all the other rows of A_j unchanged. Given that $A_j b_0^T = b_j$, we have that $\xi A_j b_0^T = \xi b_j^T = D_j$. Therefore $A_{j+1} b_0^T = b_{j+1}^T$ as follows from our construction. If $D_j = 0$ eliminate $A_j[i]$ from A_j , eliminate b_{ji} from b_j , reset $m = m-1$ and redo step 2, ($D_j = 0$ means that b_{ji} is an integral combination of the other entries of b_j and therefore its deletion will not affect the gcd we are looking for).

3. Termination

If $m > 1$ and (for the current j) there is an i such that $b_{ji} = 1$ then the vector $A_j[i]$ is a solution of the equation (1) with $\gcd(a_1, \dots, a_n) = 1$. If $m = 1$ then A_j is a vector and b_j is an integer. In this case b_j is the gcd of $(a_1, \dots, a_n)$ and A_j satisfies $A_j a^T = b_j$ thus solving equation (1). The following termination rule completes therefore the algorithm:

If ($m > 1$ and $b_{ji} = 1$) or $m = 1$ then stop and output $A_j[i]$ as the vector of coefficients solving (1) with right hand side (gcd) equal to 1 ($m > 1$) or output the vector A_j solving (1) with right hand side (gcd) equal to b_j ($m = 1$). If the above conditions are false, go back to step 2.

Example

The table below shows the different steps of the above algorithm when applied to the input $a = (a_1, a_2, a_3, a_4, a_5) = (630, 1050, 3000, 7224, 19089)$.

The vector ξ is the vector with ± 1 coefficients in Step 2 of the algorithm. The active rows are the rows whose combination by ξ should replace the active row with maximal coefficients in the sixth (labelled 'b') column. The active row to be replaced is underlined.

Row #	Matrix A	b	Active Rows	ξ
-4	1 0 0 0 0	630	-	-
-3	0 1 0 0 0	1050	-	-
-2	0 0 1 0 0	3000	-	-
-1	0 0 0 1 0	7224	-	-
0	0 0 0 0 1	19089	(-4, -3, -2, -1, 0)	(-1, -1, -1, -1, 1)
1	-1 -1 -1 -1 1	7185	(-4, -3, -2, -1, 1)	(-1, -1, -1, -1, +1)
2	-2 -2 0 -2 1	1281	(-4, -3, -2, 1, 2)	(-1, -1, -1, +1, -1)
3	0 0 -2 1 0	1224	(-4, -3, -2, 2, 3)	(1, -1, +1, -1, -1)
4	3 1 3 1 -1	75	(-4, -3, 2, 3, 4)	(-1, +1, -1, +1, -1)
5	-2 2 -5 2 0	288	(-4, -3, 3, 4, 5)	(+1, +1, -1, -1, -1)
6	0 -2 4 -4 1	93	(-4, -3, 4, 5, 6)	(+1, -1, +1, +1, +1)
7	2 0 2 -1 0	36	(-4, 4, 5, 6, 7)	(+1, -1, -1, -1, -1)
8	-2 -1 -4 2 0	138	(4, 5, 6, 7, 8)	(-1, +1, -1, +1, -1)
9	-1 4 -6 2 0	18	(4, 6, 7, 8, 9)	(+1, +1, -1, -1, +1)
10	2 4 3 -2 0	12	(4, 6, 7, 9, 10)	remove row 6
11	-	-	(4, 7, 9, 10)	(+1, -1, -1, -1)
12	0 -7 4 2 -1	9	(7, 9, 10, 12)	(-1, +1, +1, +1)
13	-1 1 -1 3 -1	3	(9, 10, 12, 13)	remove row 9
14	-	-	(10, 12, 13)	remove row 10
15	-	-	(12, 13)	(+1, -1)
16	1 -8 5 -1 0	6	(13, 16)	(-1, +1)
17	2 -9 6 -4 1	3	(13, 17)	remove row 17
18	-	-	(13)	output

Output: $-1 \cdot 630 + 1 \cdot 1050 - 1 \cdot 3000 + 3 \cdot 7224 - 1 \cdot 19089 = 3$.
gcd(630, 1050, 3000, 7224, 19089) = 3.

Notice the following features:

- The algorithm needed 17 iterations, with 4 iterations of row-removal type (iterations number 10, 13, 14, 17).
- The entries in the consecutive rows grow quite slowly, with the coefficients of the output smaller in absolute value than 3.
- By way of contrast, if the ordinary gcd algorithm (with divisions) is applied to the same data, the output, after 11 iterations, is:
 $65950132 \cdot 630 - 32975066 \cdot 1050 - 2300586 \cdot 3000 - 3182 \cdot 7224 - 19089 = 3$.

We would like to mention that while this example has been constructed with the purpose of stressing the difference between our algorithm and the ordinary one, with regard to the magnitude of the coefficients, still computing experience shows that the same difference is apparent for random inputs in general even if it is not always as striking. It is also worth mentioning that the Morito-Salkin algorithm provides the same output as our output for this example, and needs 25 iterations.

Analysis and Discussion

With every iteration either a row is eliminated - and this can happen at most $n-1$ times, or a row is replaced by another row with a smaller coefficient in the b-column, therefore the algorithm terminates. At the initialization stage we have that $A_0 a^T = A_0 b_0^T = b_0^T$ and by induction

$A_j a^T = A_j b_0^T = b_j^T$ after the j -th iteration. If the j -th iteration is a row-elimination then the row eliminated is an integral combination of the other rows, implying that $\gcd(b_{j-1}) = \gcd(b_j)$. If the j -th iteration replaces the i -th row of A_{j-1} and the corresponding entry of b_{j-1} then

$$b_j = (b_{j-1,1}, \dots, b_{j-1,i-1}, \sum_{k=1}^n e_k b_{j-1,k}, \dots, b_{j-1,n})$$

where $e_k \in \langle \pm 1, -1 \rangle$, and $b_{j-1} = (b_{j-1,1}, b_{j-1,2}, \dots, b_{j-1,i}, \dots, b_{j-1,n})$. Thus $\gcd(b_{j-1}) = \gcd(b_j)$ in this case too. It is clear therefore that, when termination occurs, the algorithm outputs a solution to the equation (1) as required. The algorithm is thus shown to be correct. Unfortunately we cannot apply the analysis of Karmarkar and Karp in order to estimate the rate of convergence (complexity) of our algorithm, as after a few substitutions the entries of b_j may not be randomly distributed anymore. Experience shows that our algorithm converges quite fast but we have no way of estimating how fast, and will leave this as an open problem. We conjecture that the rate of convergence is $O(\log_{a_1}^2)$ where $1 < a \leq 2$. We encounter the same problem when trying to estimate the magnitude of the coefficients of the solution provided by our algorithm. If the j -th iteration eliminates a row of A_{j-1} then it does not affect the entries of A_{j-1} . If the j -th iteration substituted ξA_{j-1} for the i -th row of A_{j-1} to form A_j then, as the entries of ξ are equal to ± 1 , one would expect that the coefficients of the new row would be only moderately bigger than the entries of A_{j-1} . On the other hand, if the number of iterations is big then even a moderate increase may accumulate into relatively big coefficients. In practice, the results we got showed both a fast convergence and outputs with small coefficients.

5. Subtractive Euclidean Algorithm for Gaussian Integers

It is well known that the Euclidean algorithm can be applied to other domains such as Gaussian integers, integral Quaternions polynomials, etc. We would like to consider here the domain of Gaussian integers $G = \{(a+bi) : a \text{ and } b \text{ integers}\}$ and investigate the question whether the Euclidean algorithm can be applied to this domain, but without using divisions.

We want to show first that this can be done. We shall need to perform multiplications though, but multiplication is an operation which is simpler than division, especially for this domain $((a,b)/(c,d) = (a,b) \cdot (c,-d)/(c^2+d^2))$.

Let z_1 and z_2 be two Gaussian integers with $\rho(z_1) \geq \rho(z_2)$. (If $z = a+bi$ then $\rho(z) = a^2+b^2$). Denote by $|z|$ the length of z or $|z| = \rho^{1/2}(z)$. We prove first the following:

Lemma 4. $|z_1 - \epsilon z_2| \leq |z_1| - (1 - \sqrt{2 - \sqrt{2}})|z_2|$ for some unit ϵ of the domain.

Proof: The domain G has four units $1+0i, -1+0i, 0+i, 0-i$ to be denoted by $\epsilon_1, \epsilon_{-1}, \epsilon_i$ and ϵ_{-i} respectively. Let ϵ be a unit such that the angle between ϵz_2 and z_1 to be denoted by α is less or equal than $\pi/4$ in absolute value (such an ϵ clearly exists). Consider the complex number $u_\alpha = \cos \alpha + i \sin \alpha$ (this number does not have to belong to G). By the definition of α we have that $u_\alpha \epsilon z_2$ is collinear with z_1 and oriented in the same direction. As $\alpha \leq \pi/4$ we have that

$$\rho(\epsilon_1 - u_\alpha) = (1 - \cos \alpha)^2 + (\sin \alpha)^2 = 2(1 - \cos \alpha) \leq 2 \left(1 - \frac{\sqrt{2}}{2}\right) = 2 - \sqrt{2}$$

and

$$|\epsilon_1 - u_\alpha| \leq \sqrt{2 - \sqrt{2}}.$$

Thus

$$\begin{aligned} |z_1 - \epsilon z_2| &= |z_1 - \epsilon_1 \epsilon z_2| = \\ &= |z_1 - u_\alpha \epsilon z_2 - (\epsilon_1 - u_\alpha) \epsilon z_2| \leq |z_1 - u_\alpha \epsilon z_2| + |\epsilon_1 - u_\alpha| |z_2| = \\ &= |z_1| - |z_2| + (\sqrt{2 - \sqrt{2}}) |z_2| = \\ &= |z_1| - (1 - \sqrt{2 - \sqrt{2}}) |z_2|. \end{aligned}$$

q.e.d.

We will show now how to find a unit ϵ such that the angle between ϵz_2 and z_1 is less or equal than $\pi/4$ for given $z_1, z_2 \in G, |z_1| \geq |z_2| > 0$. Let $z_1 = a+bi$ and $z_2 = c+di$; a, b, c, d integers. Define the transformation $T: G \rightarrow G$ as follows

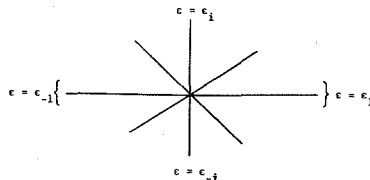
$$(x+iy)T = (x+iy)(c-id).$$

The above transformation rotates the complex plane by a fixed angle, dilates it, and carries $z_2 = c+id$ into the number c^2+d^2+0i . The angle between $z_1T = w_1$ and $z_2T = w_2$ is the same as the angle between z_1 and z_2 . Let $w_1 = u+iv$. We have the following procedure for finding the required ϵ (see figure below).

Procedure: Find $\epsilon(z_1, z_2)$: Find $w_1 = u+vi$ and

- (i) if $|u| \geq |v|$ and $u > 0$ set $\epsilon = \epsilon_1$
- (ii) if $|u| \geq |v|$ and $u < 0$ set $\epsilon = \epsilon_{-1}$
- (iii) if $|u| < |v|$ and $v > 0$ set $\epsilon = \epsilon_i$
- (iv) if $|u| < |v|$ and $v < 0$ set $\epsilon = \epsilon_{-i}$

Choosing ϵ as above will ensure that the angle between ϵw_2 and w_1 is not bigger than $\pi/4$ and the same will be true for ϵz_2 and z_1 .



The above considerations provide a means for defining a subtractive (extended) Euclidean algorithm for two Gaussian integers and can be generalized to any number of such integers, based on our algorithm in the previous section as follows:

1. For two integers: To solve $w_1 z_1 + w_2 z_2 = \gcd(z_1, z_2)$.
- 1.1 Start with the matrix (assume $|z_1| \geq |z_2|$)

$$\begin{pmatrix} \epsilon_1 & 0 & z_1 \\ 0 & \epsilon_1 & z_2 \end{pmatrix}$$

- 1.2 Assume that the current matrix is

$$\begin{pmatrix} w_{11} & w_{12} & v_1 \\ w_{21} & w_{22} & v_2 \end{pmatrix}$$

and that $|v_1| \geq |v_2|$.

- 1.2.1 If $v_2 = 0$ output the coefficients $w_1 = w_{11}, w_2 = w_{12}$ with $\gcd = v_1$.
- 1.2.2 If v_2 is a unit output $w_1 = w_{21}, w_2 = w_{22}$ with $\gcd = v_2$.
- 1.2.3 Subtract the second row multiplied by ϵ from the first row, where ϵ is chosen by the procedure Find $\epsilon(v_1, v_2)$.

It is clear that $\gcd(v_1, v_2) = \gcd(v_1 - \epsilon v_2, v_2)$ so that the algorithm is correct. By lemma 4 it also terminates.

2. When more than two Gaussian integers are involved, every phase of the algorithm will consist of either an elimination of a row from the current matrix or a substitution of a row, by a combination of the other rows, with units of G as the coefficients of combination. One will have to develop a heuristic algorithm for getting such a combination whose length is relatively small to increase the rate of convergence, but this is out of the scope of this paper.

Example (input: $75 + 67i$, $61 + 71i$, $37 + 41$, $31 + 44i$)

Row #	Matrix A	b	p	Active Rows	g
-3	(1, 0), (0, 0), (0, 0), (0, 0)	(75, 67)	10114		
-2	(0, 0), (1, 0), (0, 0), (0, 0)	(61, 71)	8762		
-1	(0, 0), (0, 0), (1, 0), (0, 0)	(37, 41)	3050		
0	(0, 0), (0, 0), (0, 0), (1, 0)	(31, 44)	2897	(-3, -2, -1, 0) (1, -1, -1, 1)	
1	(1, 0), (-1, 0), (-1, 0), (1, 0)	(8, -1)	65	(-2, -1, 0, 1) (-1, 1, 1, -1)	
2	(0, -1), (-1, 1), (1, 1), (1, -1)	(6, 6)	72	(-1, 0, 1, 2) (1, -1, 1, -1)	
3	(0, 2), (1, -2), (0, -2), (-2, 2)	(1, -1)	2	(0, 1, 2, 3) (1, -1, -1, -1)	
4	(2, 0), (-1, -1), (-3, 0), (2, 2)	(23, 29)	1370	(1, 2, 3, 4) (-1, -1, -1, 1)	
5	(4, 0), (-2, -2), (-6, 0), (3, 4)	(15, 14)	421	(1, 2, 3, 5) (-1, -1, -1, 1)	
6	(4, -2), (-2, 0), (-7, 2), (4, 2)	(7, 1)	49	(1, 2, 3, 6) (1, -1, -1, 1)	
7	(6, 0), (-3, -3), (-10, 0), (5, 6)	(1, 2)	5	(1, 3, 6, 7) (1, -1, 1, 1)	
8	(-3, 10), (5, -5), (6, -14), (-11, 15)	(0, -2)	4	(3, 6, 7, 8) (1, 1, 1, -1)	
9	(16, 7), (-6, -9), (-23, -14), (5, 20)	(2, 1)	5	(3, 7, 8, 9) remove row 7	
10		(0, 0)	0	(3, 8, 9) (1, -1, 1)	
11	(26, 12), (-10, -16), (-37, -22), (8, 33)	(1, 0)	1	output	

$$\begin{aligned}
 & \cdot (26 + 12i) + (75 + 67i) - (10 + 16i) + (61 + 71i) - (37 + 22i) + (37 + 41i) + \\
 & + (8 + 33i) = (31 + 44i) = 1 + 0i; \quad 1 + 0i \text{ is the gcd.}
 \end{aligned}$$

The matrix A and b have all their entries in G represented by their coordinates; $p = a^2 + b^2$ is the modulus of the complex number $z = a + bi$; the other notations are similar to the ones used in our previous example.

An interesting open problem is the following:

Does there exist a subtractive g.c.d. algorithm for Gaussian Integers which uses additions and subtractions only (does not use multiplications nor divisions)?

References

- [1] Blankinship, W.A., A new version of the Euclidean algorithm. Amer. Math. Mon. 70 (1963) 742-745.
- [2] Blum, M. Private communication.
- [3] Bradley, G.H., Algorithm and bound for the greatest common division of n integers, Numerical Math., Vol. 13, No. 7 (1970) 433-436.
- [4] Garey, M.R. and Johnson, D.S. Computers and Intractability, Freeman & Co., 1979.
- [5] Kannan, R., Polynomial-time aggregation of integer programming problems. U.C. Berkeley Report, 1978.
- [6] Karmarkar, N. and Karp, R.M., The differencing method of set partitioning. U.C. Berkeley Report, 1982.
- [7] Knuth, D.E. The art of computer programming, Vol. 2, Addison Wesley, second edition, 1981.
- [8] Lamé, G., Note sur la limite de nombre des divisions dans le recherche du plus grand commun diviseur entre deux nombres entiers. C.R. Acad. Sci. Paris, 19 (1944) 867-870.
- [9] Morito, S. & Salkin, H.M., Using the Blankinship algorithm to find the general solution of a linear Diophantine equation, Acta Informatica 13 (1980) 379-382.
- [10] Morito, S., Salkin, H.M. & Williams, D.E., Two backtrack algorithms for the radio frequency intermodulation problem, Appl. Math. Optim. 6 (1980) 221-240.
- [11] Shamir, A., On the cryptocomplexity of Knapsack systems, 11-th STOC (1979), pp. 118-119.
- [12] Van Emde Boas, Another NP-complete problem and the complexity of computing short vectors in a lattice. Report 81-04, University of Amsterdam, Mathematisch Instituut, 1981.

Are there counter-examples to the Baillie - PSW primality test?

Carl Pomerance

to Arjen K. Lenstra on the defense of his doctoral thesis

In [2] the following procedure is suggested for deciding whether a positive integer n is prime or composite:

- (1) Perform a base 2 strong pseudoprime test on n . If this test fails, declare n composite and halt. If this test succeeds, n is probably prime. Go on to step (2).
- (2) In the sequence $5, -7, 9, -11, 13, \dots$ find the first number D for which $(D/n) = -1$. Then perform a Lucas pseudoprime test with discriminant D on n (a specific one of these tests as described in [2]). If this test fails, declare n composite. If this test succeeds, n is "very probably" prime.

Although it first appeared in [2], the idea of trying such a combined test originated with Baillie.

In an exhaustive search up to $25 \cdot 10^9$ in [2], no composite number was found that passed both (1) and (2). In fact, if (1) is weakened to just an ordinary base 2 pseudoprime test, every composite $n \leq 25 \cdot 10^9$ fails either (1) or (2).

The authors of [2] have offered a prize of \$30 (U.S.) for a composite number n (with its prime factorization) that passes (1) and (2) or a proof that no such n exists. Since the publication of [2], the second author has increased his \$10 share of the prize money ten-fold, so now the award stands at

\$120. (The cheap first and third authors have not increased their shares as yet, although the third author has contemplated offering a "bit" more.)

In the interests of helping Arjen start his post-doctoral career on a sound financial footing, I will give here some hint on how a counter-example to this Baillie-PSW "primality test" may be constructed. In fact, I will give a heuristic argument that will show that the number of counter-examples up to x is $\gg x^{1-\epsilon}$ for any $\epsilon > 0$. This argument is based on one by Erdős [1] that suggested there are many Carmichael numbers.

Let $k > 4$ be arbitrary but fixed and let T be large. Let $P_k(T)$ denote the set of primes p in the interval $[T, T^k]$ such that

- (a) $p \equiv 3 \pmod{8}$, $(5/p) = -1$,
- (b) $(p-1)/2$ is square free and composed solely of primes $q < T$ with $q \equiv 1 \pmod{4}$,
- (c) $(p+1)/4$ is square free and composed solely of primes $q < T$ with $q \equiv 3 \pmod{4}$.

Of course, $1/8$ of all primes (asymptotically) in $[T, T^k]$ satisfy condition (a), and it can be shown that the conditions that $(p-1)/2$ and $(p+1)/4$ also be square free still leaves a positive fraction of all primes in $[T, T^k]$. Heuristically, the conditions that $p-1$ and $p+1$ are composed solely of primes below T , allow us to keep still a positive proportion of all primes in $[T, T^k]$ (using k fixed). Finally, the event that every prime in $(p-1)/2$ is $1 \pmod{4}$ should occur with probability $c(\log T)^{-1/2}$ and similarly for the event that every prime in $(p+1)/4$ is $3 \pmod{4}$. Thus the cardinality of $P_k(T)$ should be asymptotically as $T \rightarrow \infty$

$$\frac{cT^k}{\log^2 T}$$

where c is positive constant that depends on the choice of k .

We now form square free numbers n composed of k primes of $P_k(T)$, where k is odd and just below $T^2/\log(T^k)$. The number of choices for n is thus about

$$\binom{[cT^k/\log^2 T]}{k} > e^{T^2(1-3/k)}$$

for large T (and k fixed). Also, each such n is less than e^{T^2} .

Let Q_1 denote the product of the primes $q < T$ with $q \equiv 1 \pmod{4}$ and let Q_3 denote the product of the primes $q < T$ with $q \equiv 3 \pmod{4}$. Then $(Q_1, Q_3) = 1$ and $Q_1 Q_3 \approx e^T$. Thus the number of choices for n formed that in addition satisfy

$$n \equiv 1 \pmod{Q_1}, n \equiv -1 \pmod{Q_3}$$

should, heuristically, be at least

$$e^{T^2(1-3/k)/e^{2T}} > e^{T^2(1-4/k)}$$

for large T .

But any such n is a counter-example to the Baillie-PSW primality test. Indeed, n will be a Carmichael number so it will automatically be a base 2 pseudoprime. Since $n \equiv 3 \pmod{8}$ and each $p|n$ is also $\equiv 3 \pmod{8}$, it is easy to see that n will also be a strong base 2 pseudoprime. Since $(5/n) = -1$, since every prime $p|n$ satisfies $(5/p) = -1$, and since $p+1|n+1$ for every prime $p|n$, it follows that n is a Lucas pseudoprime for any Lucas test with discriminant 5.

We thus see that for any fixed k and all large T , there should be at least $e^{T^2(1-4/k)}$ counter-examples to Baillie-PSW below e^{T^2} . That is, if we let $x = e^{T^2}$, then there are at least $x^{1-4/k}$

counter-examples below x , so long as x is large. Since k is arbitrary, our argument implies that the number of counter-examples below x is $\gg x^{1-\epsilon}$ for any $\epsilon > 0$.

Remark. Both in the APR primality test and in the Cohen-Lenstra variation there is a part where many kinds of pseudo-primality tests are performed followed by a step where a limited amount of trial division is performed. No one has ever encountered an example of a number where the trial division was really needed - that is, every number that has made it through the pseudo-primality tests actually was prime. Perhaps an argument similar to the one here can show that in fact there are composite numbers that pass all the pseudo-primality tests and for which the trial division step is really needed to distinguish them from the primes.

References

1. P. Erdős, On pseudoprimes and Carmichael numbers, Publ. Math. Debrecen 4(1956), 201-206.
2. C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr., The pseudoprimes to $25 \cdot 10^9$, Math. Comp. 35(1980), 1003-1026.

Department of Mathematics
University of Georgia
Athens, Georgia 30602 U.S.A.

HET BROUWER INSTITUUT

*"To know
That which before us lies in daily life
Is the prime wisdom".*

John Milton

*"Ieder priemgetal is te schrijven als
som of als verschil van twee kwadraten
van natuurlijke getallen".*

Martin Rem

Op mijn vrijdagse bezoeken aan het Centrum voor Wiskunde en Informatica (C.W.I., ook wel: C.M.C.S. of C.M.I. of Z.M.I.) versmaad ik bij de lunch nooit de zoute haring. Ik bevind mij dan doorgaans in het gezelschap van een deel van de Afdeling Informatica, een deel waarin Arjen K. Lenstra nooit ontbreekt. Op een goede dag gaat het gesprek eens niet over opera's, eethuizen of oude genever — ik ben Arjen vooral dankbaar voor zijn tip hoe je Corenwijn in de diepvries moet bewaren — maar over de huidige naam van het Centrum. Wij bespreken bij die gelegenheid hoe slecht de afkorting C.W.I. klinkt in het Engels en hoe ongelukkig het is dat het Centrum net zoveel namen heeft als er talen worden gesproken in de wereld.

Het Centrum is een instituut dat de beoefening, verbreiding en toepassing van de wiskunde bevordert. Ter vermindering van misverstanden moet ik in plaats van "de wiskunde" wellicht "de wiskundige wetenschappen" zeggen, want het omvat bijvoorbeeld ook de statistiek, de numerieke wiskunde en de informatica, gebieden die aan Amerikaanse universiteiten vaak gescheiden van de (rest van de) wiskunde worden beoefend en onderwezen. In Nederland is dat nog niet het geval, maar met de stichting van studierichtingen informatica is de naam Mathematisch Centrum toch als te beperkend ervaren. Zodra er studierichtingen statistiek ontstaan moet er waarschijnlijk weer een naamsverandering komen.

Tijdens die betreffende lunch nu, herinneren wij ons dat Amsterdam een wiskundige van wereldfaam heeft gekend die trachtte, in zijn werk aan het intuitionisme, de wiskunde op zuiver-constructieve methoden te baseren. Wij kunnen er thans over twisten hoe succesvol deze pogingen zijn gebleken, maar feit is dat na zijn dood in 1966, er een wiskundige discipline is ontstaan die een wel zeer constructieve vorm van wiskundig redeneren behelst. Ik bedoel natuurlijk de informatica. Zo pratende is tijdens deze lunch het idee ontstaan om deze "informaticus avant la lettre" te eren door het Centrum de naam te geven die ik deze notitie als titel heb meegegeven.

Ik verwacht eerlijk gezegd niet dat dit voorstel zal worden uitgevoerd, maar er zijn naderhand zoveel mensen geweest die het een goed idee vonden, dat ik het niet heb kunnen nalaten deze lunchgedachte op te tekenen.

Martin Rem
Eindhoven, 8 april 1984

DE MATHEMATISCHE ACHTERGROND VAN DE RHINOCEROS

Het is drie uur in de morgen. Zojuist ben ik aangekomen op het vliegveld van de Indiase hoofdstad New Delhi, na een korte maar wel zeer nachtelijke vlucht uit het warmere Bombay. Een paar mensen staan me op te wachten met de mededeling dat ze net de vorige dag kans hadden gezien om een vergunning voor me te krijgen om Manipur te bezoeken. Dat is zeer onverwacht. Manipur is een staat van India, gelegen in het uiterste noordoosten tegen de grens met Burma aan. Vanwege deze militair kritische ligging hebben buitenlanders een speciale vergunning van de Indiase regering nodig om toegelaten te worden, en die vergunning wordt eigenlijk zonder uitzondering geweigerd. Mijn huidige werkgever, de Stichting Redt een Kind, steunt hier al geruime tijd een kindertehuis, maar het was ons nog nooit gelukt dit persoonlijk te zien. Nu was het dus voor het eerst mogelijk om een bezoek te brengen aan Manipur. Ik stapte derhalve direkt de volgende morgen in het vliegtuig en arriveerde vijf uur later in de grootste stad van Manipur, Imphal. Eigenlijk viel het me op het eerste gezicht nogal tegen, want behalve de gelaatstrekken van de mensen, leek het allemaal erg op de elders in India voorkomende toestanden. Gelukkig was die indruk niet helemaal juist. De leiding van het kindertehuis en de daarin opgenomen kinderen behoren allen tot de Hmar, een bergstam die pas vrij recent met enige beschaving in aanraking is gekomen. Aan het begin van deze eeuw waren het Koppesnellers, scholen kwamen daar pas na de laatste oorlog die ook in Manipur in alle hevigheid uitgevochten werd, en ook nu is een groot deel van de stam door de grote afstand van de ontwikkeling afgesloten. Hun gewoonten zijn daarom nog vrij primitief. Op hun vraag wat ik wilde eten, heb ik mij moeten verstimmen om mee te delen dat ik niet bereid was het vlees van apen of honden te verorberen, iets wat door deze mensen met name aan gasten als lekkernij aangeboden wordt. Dit had tot gevolg dat ik de ingewanden van een kip voorgezet kreeg, hetgeen dus ook niet in grote hoeveelheden in mijn maag verdween. Manipur was een interessante, en bijna unieke ervaring.

Mijn eerste interesse in Manipur is al van veel vroeger datum en op een geheel ander vlak. Hierover moet ik hier wel verhalen, anders zou ik onze vriend Arjen wel zeer teleurstellen. Gedurende mijn bibliografische onderzoeken van de neushoorn kwam ik al vrij vroeg een vraagstuk tegen, dat in de literatuur haast een eigen leven is gaan leiden. Aan het einde van de jaren zestig van de vorige eeuw werd er, jawel, in Manipur een neushoorn gevangen, overigens praktisch het enige exemplaar dat daar ooit gevangen of waargenomen is. Het dier werd getransporteerd naar Calcutta en enige tijd later naar Londen. Daar werd het in 1872 enige tijd gehouden in de stallen van de eigenaar, een dierenhandelaar genaamd Jamrach. Ook al bezat de Londense dierentuin in die tijd een mooie verzameling neushoorns, waarop men vandaag zeer jaloers zou zijn, was elke nieuwe aanwinst nog steeds speciale aandacht waard. Dit was een periode in de geschiedenis waarin veel voor de wetenschap nieuwe of praktisch nieuwe diersoorten voor het eerst in Europa tentoongesteld werden. De systematici van de 19e eeuw zijn deels berucht geworden vanwege hun neiging om nieuwe soorten te beschrijven aan de hand van zeer beperkt materiaal. Het leek belangrijker om de auteur te zijn van een nieuwe naam, dan te wachten totdat er een wetenschappelijk gefundeerd oordeel gegeven kon worden. Er was juist in 1872 door de secretaris van de Zoological Society of London, P.L. Sclater, een nieuwe neushoornsoort (*Rhinoceros lasiotis*) beschreven omdat de haren langs de oorranden van een dier in de Londense dierentuin langer schenen dan bij andere exemplaren. In dat taxonomische klimaat dus kwam de neushoorn uit Manipur. Natuurlijk gingen de Londense biologen er met belangstelling naar kijken. Volgens hen was dit eenhoornige dier in de meeste opzichten hetzelfde als een ander exemplaar in de dierentuin van Londen en behoorde het niet tot een nog niet beschreven soort.

Voor goed begrip, moet hier iets gezegd worden over de huidige inzichten betreffende de systematiek van de Aziatische neushoorns. Er zijn drie soorten in Azië, elk met een althans gedeeltelijk verschillend verspreidingsgebied, dat echter vroeger juist in het noordoostelijk deel van India elkander raakte of overlapte. Er is een relatief kleine, langharige soort met twee horens op de neus, bekend als de Sumatraanse neushoorn of *Dicerorhinus sumatrensis*. Dit dier

verschilt duidelijk van de twee andere soorten, maar is toch nogal eens verward omdat het in de jungle vaak moeilijk is om neushoorns lang gade te slaan. De andere twee soorten lijken erg op elkaar, zijn beide gepantserd en éénhoornig. De Javaanse neushoorn (*Rhinoceros sondaicus*) is echter iets kleiner en heeft een verspreidingsgebied dat veel overeenkomsten vertoont met dat van de Sumatraanse neushoorn; beide leven in de zuidoost-aziatische landen en op enkele Indonesische eilanden. De derde soort, de Indische neushoorn (*Rhinoceros unicornis*) is de grootste en leeft langs de zuidrand van de Himalaya.

De neushoorn uit Manipur werd door Jamrach in 1872 verkocht aan de dieren-tuin in Berlijn. Daar leefde het waarschijnlijk een jaar of tien. Het is bijzonder ongelukkig dat juist van dit dier onbekend is wanneer het is overleden en of de huid en het skelet ergens bewaard zijn gebleven. Dat is de voornaamste reden van de huidige literaire controverse. In Londen had men het als een Javaanse neushoorn beschouwd. Toen echter P.L. Sclater het dier enkele jaren later in Berlijn terugzag - en het was in de tussentijd wat gegroeid - veranderde hij van gedachte en verklaarde hij het tot Indische neushoorn. In Berlijn bleef men het echter lange tijd als javaans beschouwen en hield men het dier apart van een paar Indische neushoorns, dat daar in dezelfde tijd aanwezig was. Maar de verwarring was nog niet compleet. De importeur Jamrach geloofde niets van al deze taxonomische tegenstrijdigheden. Hij meende de Javaanse en Indische, en alle andere in die tijd erkende soorten, goed te kennen en vond dat het door hem geïmporteerde dier daarvan verschilde. Nadat de stafleden van de Londense dierentuin geweigerd hadden om het Manipurse dier als nieuw te beschrijven, was Jamrach daarover weinig te spreken. Toen hij zijn vriend in 1875 in Berlijn terugzag, wist hij ineens zeker dat de biologen een verkeerd oordeel hadden gegeven. Hij schreef een pamflet van drie pagina's, waarin hij wat achtergrond-informatie gaf en hij noemde het dier, zonder valse schaamte, naar zichzelf, als *Rhinoceros jamrachi*. Het bestaan van dit pamflet werd door Sclater in 1876 in een voetnoot vermeld, maar sindsdien was het nooit meer boven water gekomen. Dit is niet iets waar je gauw bewust naar gaat zoeken, want de kans van slagen is bijna miniem. Toen ik enkele jaren geleden de oude onderwerpcatalogus van de Parijse dierentuin doorkeek, was ik verbaasd en verheugd daar het pamflet van William Jamrach in vermeld te zien. Het was nog steeds in goede staat aanwezig. Het probleem van de neushoorn uit Manipur blijft onopgelost. Het is nog steeds niet met zekerheid bekend tot welke soort het behoorde. Er kunnen met goede fantasie nog veel geleerde artikelen aan gewijd worden, maar het zal wel weinig goed resultaat opleveren zolang niet de resten van het dier tevoorschijn komen of er een goede afbeelding bekend wordt.

De bovenstaande verhandeling in dit Album Amicorum zal u misschien verbazen en men zal mij wel de onjuistheid van de titel ten laste leggen. Dat laatste zou terecht zijn, want dit was alleen bedoeld om de interesse te wekken van het merendeel van Arjen's vrienden en om de fantasie te stimuleren. Arjen echter kent mij al langer en verwacht zeker een rhinocerologisch opstel van mijn hand. Vandaar. Ik ken Arjen al sinds onze gezamenlijke jaren op het Vossius Gymnasium. Hij was toen, zover ik het kon beoordelen, een wiskundig wonder. Het was jammer dat hij nooit had geleerd om duidelijk te schrijven, zodat de eenvoud waarmee hij de meest waanzinnige wiskundige problemen oploste voor de rest van de klas onbekend bleef. Met het vermeerdere gebruik van typemachines en computers is dit nadeel voor Arjen's collega's grotendeels weggenomen, wat hopelijk zal leiden tot een algemene erkenning van zijn talenten.

Arjen, het ga je goed!

Kees Rookmaaker

Een laatste stelling ter verdediging

Lang geleden, in de zestiger jaren, was Huize Lenstra in de Frans Mierisstraat te Amsterdam een geliefde en gevreesde badgelegenheid voor vervuilde studenten. Als arme, wat verweesde student in een nederig vak als de medicijnen begaf ik mij eens in de veertien dagen en soms zelfs vaker, wanneer de walm niet langer te harden was en ik dringend korsten bier uit mijn kruin moest spoelen, naar het huis van de roemruchte Lenstra's om me daar heerlijk veilig in het douchehok op te sluiten. Eenmaal schoon geschrobd was er geen ontkomen meer aan. De familiekring van elfdegraadsneven - net als bij de homeopathie: hoe sterker de verdunning, hoe krachtiger het effect - sloot zich met ongekend felle apeliëfde om het domme neefje, dat ik nu eenmaal was en ben. Een spervuur van spitsvondigheden perforeerde mijn trommelvliesen. Het rood, niet langer van het boenen maar van schaamte stond op mijn kaken. Het was eenvoudig te veel voor een simpele ziel. Zo veel lange linke Lenstra's die lorrig Lotje wilden leren lopen lans de lange Lindenlaan, het was om van door de grond te gaan. Soms was er nog even redding onder Ma-Lenstra's rokken, maar snel daar onder uit getrokken, begonnen de heren je te mitrilleren met hun genadeloze strikvragen: "Er zitten tien muggen op tafel; één sla ik er dood: hoeveel zitten er nog op tafel?"

Tegen dat geweld faalde elke verdediging. Je mompelde: muggenzifterij. Je kwam, naar je dacht, met een ijzersterke medische diagnose: cerebrale hypertrophie en pernicieuze overcompensatie, maar neerbuigend hoongelach was je deel. Je siste in je zelf: snuggere, gisse jongens, maar niet wijs! Het mocht niet baten. Wie kon immers de vergelijking doorstaan met de geniale Andries: zelfgebouwde kano, virtuoos bespeelde piano en van de Alliance een aardig mondje Frans - gelukkig deed Ma dat laatste later nog veel beter - ; of met de schrandere Jan Karel die mijn studentendispuutje van een bankroet redde door alle honoraire leden aan te slaan voor het bedrag dat ze ooit al te veel hadden betaald; of de knappe Hendrik die mijn vluchtweg op het schaakbord afsneed - ik beheerste in die dagen het herdersmat volledig - door me composities voor te schotelen waarop mijn brein simpel brak en zelfs met Hans, de jongste van de oudere lichter, die slechts meewarig hoefde te kijken om mij te doen beseffen een gans te zijn?

Voor het hele stel gold en geldt: markant, important, een berg verstand en perfect gebakken tulband.

Heel groot was daarom mijn bewondering voor Willemien, die zich minzaam staande hield. Dat gold ook ene zo nu en dan in Huize Lenstra toevende Van Ende Boas, die met beperkt postuur zo maar overeind bleef tussen al die lange leperikken.

Voor mij was er geen hoop, totdat ik op goede dag ter hoogte van mijn kuit een borelingske, Arjen genaamd, ontwaarde, dat nog vriendelijk uit zijn oogjes keek. Het was mijn laatste kans. Het knaapje was nog speels en mild gestemd. Het wilde zelfs buiten op straat, daar waar de familiedruk wat minder aanwezig was, met mij badmintonnen. Daarbij maakten wij steeds langere slagenseries: 3, 5, 7, 11, 13, 17, 19, 23 en zelfs 29 keer voordat de shuttle neerstortte. Het viel mij toen al wel op, dat het ventje bij het bereiken van die oplopende aantallen de shuttle opzettelijk liet vallen of zo aanspeelde dat ik er onmogelijk bij kon, maar dat het iets met de getallenleer van zijn broer Hendrik junior te maken kon hebben ontging mij geheel.

Thans, zo'n kleine twintig jaar later, besef ik pijnlijk dat ook mijn laatste hoop, het vriendelijke kereltje, me tuk had.

Het is genoegzaam bekend dat van een dissertatie in feite de bijbehorende laatste stelling het belangrijkste is. In die stelling culmineert het hele werk, dat abusievelijk proefschrift heet. Zo'n werk is niet te proeven. Wat zijn nou polynomen? Volgens mij zijn dat kwaad-aardige tumoren die veel bij Polynesiërs voorkomen.

Die stelling, inhoudende een kolossaal priemgetal, is mijn laatste hoop, mijn laatste verdedigingslinie. Het zal me één keer lukken één van de gebroeders Lenstra te slim af te zijn. Dat getal kan niet kloppen, want het is onmogelijk zo'n getal zonder tikfout te reproduceren.

Beste Arjen, ik moet nu stoppen, want de rest van de avond en zo nodig de rest van mijn leven zal ik zoeken naar een deler.

E. W. Roscam Abbing

A REMARK ON THE CONSTRUCTION OF SHORT LATTICE ELEMENTS

On the occasion of Arjen K. Lenstra's promotion.

by C. P. Schnorr

April 1984

The ingenious basis reduction method of A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász¹ leads to a polynomial time algorithm which constructs short, non zero elements of a given lattice $L \subset \mathbb{Z}^n$. For fixed $\sigma > \sqrt{4/3}$ the algorithm finds some $\underline{y} \in L \setminus \{0\}$, $|\underline{y}| \leq \sigma^{n-1} \lambda(L)$ with $\lambda(L) := \min \{|\underline{x}| : \underline{x} \in L \setminus \{0\}\}$. We show that the $\sqrt{4/3}$ -bound can be improved to $(3/2)^{1/4}$ by a variant of the LLL-algorithm and we discuss the prospects of tighter approximations of $\lambda(L)$ by polynomial time algorithms.

We introduce a hierarchy of polynomial time reduction algorithms. There is a constant σ_k corresponding to the k -th algorithm of the hierarchy. For fixed $\sigma > \sigma_k$ the k -th algorithm finds in polynomial time some $\underline{y} \in L \setminus \{0\}$, $|\underline{y}| \leq \sigma^{n-1} \lambda(L)$. The hierarchy starts with the LLL-reduction algorithm, $\sigma_1 = \sqrt{4/3}$, $\sigma_2 = (3/2)^{1/4}$. We do not know whether $\lim_k \sigma_k = 1$. *see appendix!*

For a fixed basis $\underline{b}_1, \dots, \underline{b}_n$ of some lattice $L = \sum_{i=1}^n \underline{b}_i \mathbb{Z} \subset \mathbb{R}^d$ and for $\underline{a} \in \sum_{i=1}^n \underline{b}_i \mathbb{R}$ we let $\underline{a}(j)$, $\langle L_j$, resp.) be the projection of $\underline{a}$ (L , resp.) on $(\sum_{i < j} \underline{b}_i \mathbb{R})^\perp$. The projections $\underline{b}_i(i)$ $i = 1, \dots, n$ form an orthogonal system.

Let a basis $\underline{b}_1, \dots, \underline{b}_n$ of the lattice L be Kannan-reduced, see Kannan², if

- (1) for $i = 1, \dots, n$: $|\underline{b}_i(i)| = \lambda(L_i)$
- (2) for $i \leq j < i \leq n$: $|\langle \underline{b}_i(j), \underline{b}_j(j) \rangle / \langle \underline{b}_j(j), \underline{b}_j(j) \rangle| \leq 1/2$.

There is a polynomial time algorithm² which for fixed dimension n transforms a given basis $\underline{b}_1, \dots, \underline{b}_n \in \mathbb{Z}^n$ of any lattice $L \subset \mathbb{Z}^n$ into a Kannan reduced basis of L .

We consider bases that are "locally" Kannan reduced and which can be constructed in polynomial time for arbitrary dimension n . For $k = 1, 2, \dots$

and $\epsilon \geq 0$ call a basis $\underline{b}_1, \dots, \underline{b}_n$ (k, ϵ) -reduced if

- (1) for $i = 1, \dots, n-k$: $|\underline{b}_i(i)| \leq (1+\epsilon) \lambda \left(\sum_{v=0}^k \underline{b}_{i+v}(i) \mathbb{Z} \right)$
- (2) for $1 \leq j < i \leq n$: $|\langle \underline{b}_i(j), \underline{b}_j(j) \rangle| / |\langle \underline{b}_j(j), \underline{b}_j(j) \rangle| \leq 1/2$.

For $k = 1$, $\epsilon = 1/3$ the condition

$$(1) \quad |\underline{b}_i(i)| \leq 4/3 \lambda \left(\underline{b}_i(i) \mathbb{Z} + \underline{b}_{i+1}(i) \mathbb{Z} \right)$$

implies the LLL-condition (1.5)¹:

$$|\underline{b}_i(i)| \leq 4/3 |\underline{b}_{i+1}(i)|.$$

The LLL-algorithm can easily be modified as to satisfy the stronger condition (1) : instead of interchanging $\underline{b}_i(i)$ and $\underline{b}_{i+1}(i)$ replace $\underline{b}_i$ by the shortest element of $\underline{b}_i(i) \mathbb{Z} + \underline{b}_{i+1}(i) \mathbb{Z} \setminus \{0\}$.

Theorem 1: For fixed (k, ϵ) there is a polynomial time algorithm which transforms a given basis $\underline{b}_1, \dots, \underline{b}_n \in \mathbb{Z}^n$ (of arbitrary dimension n) into some (k, ϵ) -reduced basis.

Proof. A (k, ϵ) -reduced basis can be constructed as follows.

1. transform $\underline{b}_1, \dots, \underline{b}_n$ so that condition (1) is satisfied and $\underline{b}_i(i)$ $i = 1, \dots, n$ are preserved. (This can easily be done in polynomial time.)
2. if $\underline{b}_1, \dots, \underline{b}_n$ is not yet (k, ϵ) -reduced proceed as follows
 - 2.1 choose the minimal $i \leq n-k$ such that

$$|\underline{b}_i(i)| > (1+\epsilon) \lambda \left(\sum_{v=0}^k \underline{b}_{i+v}(i) \mathbb{Z} \right)$$
 - 2.2 construct $\underline{b}'_1, \dots, \underline{b}'_{i+k} \in \sum_{v=0}^k \underline{b}_{i+v} \mathbb{Z}$ such that $\underline{b}'_1(i), \dots, \underline{b}'_{i+k}(i)$ is a Kannan-reduced basis of $\sum_{v=0}^k \underline{b}_{i+v}(i) \mathbb{Z}$
 - 2.3 replace $\underline{b}_1, \dots, \underline{b}_{i+k}$ by $\underline{b}'_1, \dots, \underline{b}'_{i+k}$ and go to 1.

According to Kannan's algorithm the transformation step 2 does not

change the $b_j(j)$ for $(j < i \text{ or } j > i+k)$, and the $|b_j(j)|$ with $i \leq j \leq i+k$ do not increase during the transformation.

The transformation step 2 only takes polynomial time since (for fixed dimension $k+1$) a Kannan reduced basis can be constructed in polynomial time. So it remains to bound the number of transformation steps 2. We borrow the argument from the analysis of the LLL-algorithm. Suppose that the input basis consists of integer vectors $b_1, \dots, b_n$ and let $B := \max_{i=1, \dots, n} |b_i|^2$. Let

$$d_\mu := \det(\langle b_j, b_\nu \rangle)_{1 \leq j, \nu \leq \mu}, \quad D = \prod_{\mu=1}^n d_\mu$$

Then
$$d_\mu = \prod_{j=1}^n |b_j(j)| \leq B^j.$$

Each transformation step 2 reduces d_i by at least a factor $(1+\epsilon)$ and does not increase the d_μ with $\mu \neq i$. The d_μ remain integer and are not changed by step 1. Hence the number of transformation steps 2 is not larger than

$$\log D / \log (1+\epsilon) \leq n^2 \log B / \log (1+\epsilon).$$

A detailed analysis, similar to the analysis of the LLL-algorithms and of Kannan's algorithm, shows that the initial value d_n is a common denominator for all the rational numbers occurring in the algorithm. Moreover all numbers occurring in the algorithm are bounded as $O(n \log B)$. This finally proves the polynomial time bound.

Q.E.D.

For small ϵ the worst case performance of a (k, ϵ) -reduced lattice basis depends on the lattice constant

$$\delta_k := \max \left\{ |b_1| / |b_{k+1}(k+1)| \right\}.$$

where the maximum is taken over all Kannan reduced bases $b_1, \dots, b_{k+1} \in \mathbb{R}^{k+1}$.

We have $\delta_1 = \sqrt{4/3}$ since $\sqrt{3}/4$ is the height of the regular triangle with side length 1, $\delta_2 = \sqrt{3/2}$ since $\sqrt{2}/3$ is the height of the tetraeder with side length 1.

Fact 2: $\delta_{i+j} \leq \delta_i \cdot \delta_j$

Proof. If $b_1, \dots, b_{i+j+1}$ is Kannan reduced then so are

$$b_1, \dots, b_i, b_{i+1} \quad \text{and}$$

$$b_{i+1}^{(i+1)}, \dots, b_{i+j}^{(i+1)}, b_{i+j+1}^{(i+1)}.$$

Hence $|b_1| / |b_{i+1}^{(i+1)}| \leq \delta_i$ and

$$|b_{i+1}^{(i+1)}| / |b_{i+j+1}^{(i+1)}| \leq \delta_j.$$

Therefore $|b_1| / |b_{i+j+1}^{(i+1)}| \leq \delta_i \cdot \delta_j$.

Q.E.D.

Proposition 3: The following holds for every $(k,0)$ -reduced basis of any lattice $L \subset \mathbb{R}^n$:

- (1) $|b_i(i)| \leq \delta_k |b_{i+k}(i+k)|$.
- (2) $|b_i(i)| \leq \delta_k^v |b_j(j)|$ for $i < j \leq i+vk$.
- (3) $|b_1| \leq \delta_k^{\lceil (n-1)/k \rceil} \lambda(L)$.

Proof. (1) holds since $b_i(i), \dots, b_{i+k}(i+k)$ is a Kannan reduced basis of a lattice with dimension $k+1$.

(2) follows from (1) and $\delta_{\bar{k}} \leq \delta_k$ for $\bar{k} \leq k$ by induction on v .

(3) Let $x \in L$ with $|x| = \lambda(L)$, $x = \sum_{i=1}^n r_i b_i = \sum_{i=1}^n r'_i b_i(i)$,

$$r_i \in \mathbb{Z}, r'_i \in \mathbb{R} \text{ for } i = 1, \dots, n.$$

Let i be the largest index with $r_i \neq 0$, then $r_i = r'_i$.

So $|x| \geq r_i |b_i(i)| \geq |b_i(i)|$. Hence $|b_1| \leq \delta_k^{\lceil (n-1)/k \rceil} |b_i(i)| \leq \delta_k^{\lceil (n-1)/k \rceil} |x|$

Q.E.D.

Conclusion: Let $\sigma_k := \delta_k^{1/k}$. It follows from our considerations that for each $\sigma > \sigma_k$ there is a polynomial time algorithm which given a basis of some integer lattice $L \subset \mathbb{Z}^n$ finds some non zero lattice element y with $|y| \leq \sigma^{n-1} \lambda(L)$. One finds y by constructing a (k, ϵ) -reduced basis of L for a sufficiently small ϵ . We pose it as an open problem whether $\lim_k \sigma_k = 1$.

see appendix!

Acknowledgement: This remark has been inspired by the LLL-paper¹ and by various discussions with A.K. Lenstra and H.W. Lenstra, Jr.

References:

1. A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász:
Factoring Polynomials with Rational Coefficients.
Math. Ann. 261 (1982), 515-534
2. R. Kannan: Improved Algorithms for Integer Programming and Related Problems.
24th IEEE Symposium on Foundations of Computer Science (1983)

Appendix: solution of the open problem

Recall that a basis $\underline{b}_1, \dots, \underline{b}_n$ is Kannan reduced if

$$(1) \text{ for } i=1, \dots, n \quad |\underline{b}_i(i)| = \lambda(L_i)$$

where λ gives the length of the minimal non zero lattice element.

$$(2) \text{ for } 1 \leq i < k \leq n$$

$$|\langle \underline{b}_i(i), \underline{b}_k(i) \rangle| / |\langle \underline{b}_i(i), \underline{b}_i(i) \rangle| \leq 1/2.$$

Theorem 4: Let $\underline{b}_1, \dots, \underline{b}_n$ be a Kannan reduced base of a lattice $L \subset \mathbb{R}^n$. Then $\prod_{i=1}^n |\underline{b}_i| \leq n^n \det L$.

Proof. Let $M_1, \dots, M_n$ be the sequence of minima of L , i.e.
 $M_k = \min \{c \in \mathbb{R} \mid \dim \{ \underline{b} \in L \mid |\underline{b}| \leq c \} \geq k \}$. We know from Minkowski's theorem (γ_n is the Hermite constant):

$$(3) \quad \prod_{i=1}^n M_i \leq \gamma_n^{n/2} \det L.$$

Let $\underline{y}_1, \dots, \underline{y}_n$ be linearly independent lattice elements with $|\underline{y}_i| = M_i$ for $i = 1, \dots, n$. There exists $i \leq k$ such that $\underline{y}_i \notin \sum_{v < k} \mathbb{Z} \underline{b}_v$.

Since $|\underline{b}_k(k)| = \lambda(L_k)$ we have

$$(4) \quad |\underline{b}_k(k)| \leq |\underline{y}_i(k)| \leq |\underline{y}_i| \leq M_k$$

On the other hand the triangular inequality and (2), (4) imply

$$(5) \quad |\underline{b}_k - \underline{b}_k(k)|^2 \stackrel{(2)}{\leq} \frac{1}{4} \sum_{i < k} |\underline{b}_i(i)|^2 \stackrel{(4)}{\leq} \frac{1}{4} \sum_{i < k} M_i^2.$$

Hence

$$|b_k|^2 \stackrel{(4,5)}{\leq} M_k^2 + \frac{1}{4} \sum_{i < k} M_i^2 \leq k M_k^2.$$

So we obtain

$$\prod_{i=1}^n |b_i| \leq \prod_{k=1}^n \sqrt{k} M_k \stackrel{(3)}{\leq} \sqrt{n!} \gamma_n^{n/2} \det L \leq n^n \det L.$$

Q.E.D.

Theorem 5: Let $\delta_k := \max \left\{ \frac{|b_k|}{|b_k(k)|} : b_1, \dots, b_k \text{ Kannan-reduced} \right\}$

then $\delta_k \leq \min_{m \in \mathbb{N}} ((m+1)k)^{(1+1/m)} = O(k(\log k)^2)$

Proof. The following Fact should be obvious.

Fact: Let $b_1, \dots, b_k$ be Kannan reduced and let $\underline{c} \in (\sum_{i=1}^{k-1} b_i \mathbb{R})^\perp$ satisfy $\langle b_k(k), \underline{c} \rangle = 0$, $|b_k(k)| = |\underline{c}|$. Then $b_1, \dots, b_k, b_{k+1}$ with $b_{k+1} := b_k - b_k(k) + \underline{c}$ is Kannan reduced. (Note that $|b_k| / |b_k(k)| = |b_{k+1}(k+1)| / |b_{k+1}(k+1)|$.)

It can easily be seen from this fact that there exists a Kannan reduced basis $b_1, \dots, b_{(m+1)k}$ of some lattice L such that

$$(6) \quad |b_j| / |b_j(j)| = \delta_k \quad \text{for } j = k+1, \dots, (m+1)k.$$

Hence

$$\begin{aligned} ((m+1)k)^{(m+1)k} &\stackrel{\text{Th. 4}}{\geq} (\prod_{i=1}^{(m+1)k} |b_i|) / \det L \\ &= \prod_{i=1}^{(m+1)k} |b_i| / |b_i(i)| \stackrel{(6)}{\geq} \delta_k^{m \cdot k} \end{aligned}$$

and therefore $\delta_k \leq ((m+1)k)^{1+1/m}$. Choose $m = \lfloor \log k \rfloor$ then it can easily

be seen that $((m+1)k)^{1/m} = O(\log k)$.

Q.E.D.

Corollary 6: $\sigma_k := \delta_k^{1/k}$ satisfies $\lim_k \sigma_k = 1$.

Root finding in polynomial time

A. Schönhage, Tübingen

By the end of 1983, A.K. Lenstra sent me a preprint "Polynomial factorization by root approximation", in which he has carried out the idea of combining the basis reduction algorithm with numerical root approximation, already mentioned on page 37 of his Thesis, i.e. in the Annalen paper [2]. Thereby he has independently established part of my own research on the same subject (see [4]). Moreover, he virtually seems to be the first mathematician (except for myself) who has applied my result on root finding given in [3] - though I dare to doubt whether he really has checked all the details of that rather sketchy preliminary report. (Sometimes I myself was not sure about that, by the way.) In order to obtain good time bounds on factorization we certainly should combine the best methods available. But if we are mainly interested in just giving some (generous) polynomial time bound, then a much simpler approach is possible. My present contribution is inspired by Lehmer's method [1], but I can avoid the difficulties arising from instabilities with the Schur-Cohn test.

For simplicity I consider $f(z) = c_0 + c_1 z + \dots + c_n z^n$ with $c_j \in \mathbb{Z} + i\mathbb{Z}$. Let h measure the size of f such that $|f| \leq 2^h$ (and $n \leq 2^h$). I want to show how to compute a

t -bit approximation to one of the roots $z_1, \dots, z_n$ of f within a time bound polynomial in n, h, t . Thus the goal is to find some v for which the distance

$$d(v) = \min_j |v - z_j|$$

becomes small. More precisely, my algorithm will generate numbers v_t, r_t (for $t = 0, 1, 2, \dots$) such that

$$(1) \quad v_t \in (\mathbb{Z} + i\mathbb{Z})2^{-t} \quad \text{and} \quad d(v_t) \leq r_t \leq 4n \cdot 2^{-t}.$$

Let $|c_0| \leq |c_n|$ (otherwise $f^*(z) = c_n + \dots + c_0 z^n$ with

its zeros $1/z_j$ could be treated). Then initialization is simply by $v_0 = 0, r_0 = 1$. Now I describe how to proceed from v_{t-1}, r_{t-1} (subject to (1) for $t-1$) to v_t, r_t . For any (reasonably bounded) $v \in (\mathbb{Z} + i\mathbb{Z})2^{-t}$ the coefficients in $f(v+z) = a_0 + a_1 z + \dots + a_n z^n$ can be found by Horner's scheme. Even with exact computation and by using classical integer multiplication this requires not more than $O(n^2(nt+nh)(t+h))$ bit operations.

Next I invoke an elementary root bound, namely

$$(2) \quad R(v) = n \cdot \min_{k \geq 1} |a_0/a_k|^{1/k} \quad \text{satisfies} \quad d(v) \leq R(v) \leq 2n \cdot d(v).$$

Practically, $R(v)$ is to be replaced by some feasible approximation, say $r(v)$, where $R(v) \leq r(v) \leq 2R(v)$ is quite sufficient, and such an $r(v)$ can be computed very fast from the a 's.

Now I can explain how v_t, r_t are determined. The algorithm computes the a 's and then $r(v)$ for all numbers

$v \in (\mathbb{Z} + i\mathbb{Z})2^{-t}$ satisfying $|v - v_{t-1}| \leq r_{t-1} + 2^{-t}$ and chooses v_t among these such that $r_t = r(v_t)$ becomes minimal. For at least one of those v 's one must have $d(v) < 2^{-t}$, whence $r_t \leq r(v) \leq 2R(v) < 4n \cdot 2^{-t}$ by (2). Due to $r_{t-1} \leq 4n \cdot 2^{-t+1}$ the number of points to be tested is $O(n^2)$, and hereby a one bit improvement of the approximation is achieved. A global time analysis therefore amounts to the time bound

$$O(n^5(t+h)^3)$$

for computing a t -bit approximation to some root of f .

References

- [1] D.H. Lehmer, A machine method for solving polynomial equations. JACM 8, 151-162 (1961).
- [2] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients. Math. Ann. 261, 515-534 (1982).
- [3] A. Schönhage, The fundamental theorem of algebra in terms of computational complexity. Preliminary report, Math. Inst. Univ. Tübingen, 1982.
- [4] A. Schönhage, Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. To appear in Proc. ICALP 1984 (Antwerpen).

Let p be the prime 158209 and let E be the elliptic curve over $\mathbb{F}_p$ with the following equation:

$$Y^2 = X^3 + 3X - 31846.$$

We dedicate this curve to

ARJEN K. LENSTRA

on the occasion of his thesis defense at the University of Amsterdam, 16-5-1984.

The abelian group $E(\mathbb{F}_p)$ is isomorphic to

$$C(16) \times C(5) \times C(1984).$$

We would like to thank Arjen for not delaying by a month.

René Schoof
Larry Washington

ERVARINGEN MET L , L^2 EN L^3

Lex Schrijver

Van de drie mij bekende Lenstra's, Hendrik, Jan Karel en Arjen, ken ik de laatste het minst. Jaren geleden heb ik al wel eens met Arjen en Hendrik gedineerd in C73, het bekende MC-restaurant uit het Tweede Boerhaave-tijdperk (een broeinest voor homoseksuelen, waarschuwden sommige MC-ers), maar toen werd Arjen nog slechts als "mijn broer Arjen" door Hendrik geïntroduceerd, en ik herinner me verder alleen nog dat Arjen het bestek op dezelfde manier hanteerde als zijn grotere broers. Een tweede gelegenheid Arjen te leren kennen kwam zo omstreeks 1981, toen hij dus al bijna beroemd was. Laci ("Lotsie") Lovász bracht een bezoek aan het Institut für Operations Research in Bonn, en we besloten af te reizen om Laci te spreken, Arjen en Hendrik over het L^3 -artikel, ikzelf over een te schrijven boek. (Overigens: L^2 is de Hongaarse afkorting voor Lovász László, in zijn eentje dus al.) Maar toen bleek Arjen een trein eerder genomen te hebben, om pas vanaf Keulen onze trein te nemen, vanwege een of andere platenwinkel of iets dergelijks. Ruim voor Köln Hauptbahnhof manoeuvreerden Hendrik en Peter van Emde Boas (die ook mee wilde) hun hoofden door de nauwelijks te openen raamspleet, om de op het perron wachtende Arjen niet te missen, maar die leek niets te zien. Op de vraag van Peter aan de even later toch de coupé binnenstappende Arjen of hij de twee hoofden niet had gezien en gehoord, en waarom hij dan niets had laten merken, antwoordde Arjen dat dit volstrekt overbodig was, omdat het toch overduidelijk was dat iedereen die twee hoofden had gezien. (In zijn toon dacht ik te horen dat hij al had gevreesd dat de twee hoofden zouden worden uitgestoken.) Verder is mij weinig van ons bezoek aan Bonn bijgebleven - vaag staat me bij dat het net Carnaval was, waarbij Duitse secretaresses plotseling met scharen mogen rondlopen om stropdassen af te knippen, waarna gezoen volgt, en dat, naast de Direktor van het Institut, alleen Hendrik zich van een stropdas had voorzien, maar het precieze verloop ben ik vergeten, en 't kan ook een andere keer zijn geweest dat ik die rare Duitse folklore heb meegemaakt in Bonn. Op de terugreis nam Arjen weer een trein eerder, ik geloof omdat hij voor 't donker thuis wilde zijn.

Een derde kennismaking deed zich voor toen ik Arjen aanzocht als interessante spreker voor een groep Hongaarse wiskunde-studenten, die uitgenodigd waren door hun Nederlandse collega's, en Amsterdam bezochten, en daarmee uiteraard het Mathematisch Centrum. In Boedapest had Laci Lovász verteld over de L^3 -algoritme, en nu leek het hen wel een goed idee ook die andere L eens aan te horen. Tijdens Arjen's briljante voordracht bleek de groep echter voornamelijk vanwege de te verkrijgen subsidie een wetenschappelijk gedeelte in hun programma te hebben ingelast. De groep had zich al in koppels ingedeeld, aanvankelijk met het idee elkaar al dat moeilijkjes uit te leggen, maar om zich na een paar minuten, toen het echt moeilijk werd, over te geven aan het sociale gedeelte.

Dit waren mijn spaarzame contacten met Arjen. Aan de overige leden van het L^3 -genootschap heb ik meer herinneringen, zoals toen Hendrik door Laci thuis was uitgenodigd, ergens achterin Hongarije, en Laci zijn Texas Instruments-calculator liet zien, toendertijd een trots bezit in Hongarije. Hendrik begon direct omstandig uit te leggen hoe inferieur een Texas Instruments is aan zijn eigen Hewlett-Packard (de T.I. had geloof ik geen *entierknop*), en dat hij de T.I. het liefst door de muur zou smijten, ware het niet dat hij de burens niet met een T.I. wilde opscheppen. Maar toen was

Arjen er weer niet bij (die me overigens wel de meest vriendelijke, menselijke als het ware, van de drie mij bekende Lenstra's lijkt).

Beter ken ik Arjen indirect, en wel door de mede door hem ontwikkelde, in zo korte tijd zo beroemd geworden L^3 -basis-reductie algoritme. Deze algoritme vormt o.a. een belangrijke basis voor de binnenkort te verschijnen standaardwerken *The Ellipsoid Method and Combinatorial Optimization* (Springer-Verlag) en *Theory of Linear and Integer Programming* (John Wiley & Sons). Opvallend in de algoritme is de historische factor $\frac{4}{3}$. Al in 1773 komt deze factor voor in Lagrange's *Recherches d'Arithmétique*, waarin een methode wordt gegeven om in een 2-dimensionaal rooster Λ een basis b_1, b_2 te vinden met

$$(1) \quad |b_1| \cdot |b_2| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}} \cdot \det \Lambda.$$

(waarbij het niet moeilijk is in te zien dat de factor $\left(\frac{4}{3}\right)^{\frac{1}{2}}$ de laagst mogelijke is). Een direct gevolg is dat Λ een element $x \neq 0$ bevat waarvoor

$$(2) \quad |x| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}} \sqrt{\det \Lambda}.$$

Vervolgens bewees Gauss in Artt. 266-285 van zijn *Disquisitiones Arithmeticae* (1801) dat een 3-dimensionaal rooster Λ steeds een element $x \neq 0$ bevat met

$$(3) \quad |x| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}} \sqrt[3]{\det \Lambda}.$$

Als vervolg hierop schreef Gauss' student L.A. Seeber in 1831 een proefschrift waarin op zeer ingewikkelde wijze wordt bewezen dat ieder 3-dimensionaal rooster Λ een basis b_1, b_2, b_3 heeft waarvoor

$$(4) \quad |b_1| \cdot |b_2| \cdot |b_3| \leq 3 \cdot \det \Lambda.$$

Op 9 juli 1831 verscheen in de *Göttingische gelehrte Anzeigen* een anonieme bespreking van Seeber's werk, waarin een eenvoudig bewijs van Seeber's resultaat wordt gegeven. [De recensent merkt echter op: "Wenn ein schwieriges Problem oder Theorem aufzulösen oder zu beweisen vorliegt, so ist allezeit der erste und mit gebührendem Danke zu erkennende Schritt, dass überhaupt eine Auflösung oder ein Beweis gefunden werde, und die Frage, ob dies nicht auf eine leichtere und einfachere Art hätte geschehen können, bleibt so lange eine müßige, als die Möglichkeit nicht zugleich durch die That entschieden wird. Wir halten es daher für unzeitig, hier bei dieser Frage zu verweilen."] Achteraf bleek Gauss de auteur van de bespreking te zijn. Hij verbeterde in de recensie Seeber's factor 3 tot 2.

In een reeks aan Jacobi gerichte brieven, welke in 1850 werden gepubliceerd in Crelle's Journal, beschreef Hermite een aantal resultaten waarin weer regelmatig de factor $\frac{4}{3}$ voorkomt. In zijn eerste brief bewees Hermite dat elk n -dimensionaal rooster Λ een vector $x \neq 0$ bevat met

$$(5) \quad |x| \leq \left(\frac{4}{3}\right)^{\frac{1}{4}(n-1)} (\det \Lambda)^{1/n}.$$

Hermite bewees deze grens met behulp van het volgende inductie-argument. Laat x_0 in Λ gegeven zijn. Zij Ω het rooster

$$(6) \quad \Omega := \{y \in \mathbb{R}^n \mid y^T x \in \mathbb{Z} \text{ voor elke } x \in \Lambda; y^T x_0 = 0\}.$$

Ω is een rooster in $n-1$ dimensies, en dus bestaat er volgens inductie-hypothese een $y_0 \in \Omega$ met $y_0 \neq 0$ en

$$(7) \quad |y_0| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}(n-2)} (\det \Omega)^{1/(n-1)}.$$

Evenzo bestaat er een $x_1 \in \Gamma := \Lambda \cap \{x \mid y_0^T x = 0\}$ met $x_1 \neq 0$ en

$$(8) \quad |x_1| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}(n-2)} (\det \Gamma)^{1/(n-1)}.$$

Aangezien $\det \Omega = |x_0| \cdot (\det \Lambda)^{-1}$ en $\det \Gamma = |y_0| \cdot \det \Lambda$, volgt nu:

$$(9) \quad |x_1| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}n(n-2)/(n-1)} (\det \Lambda)^{(n-2)/(n-1)^2} |x_0|^{1/(n-1)^2}.$$

Vervang nu x_0 door x_1 , en begin opnieuw. Als we dit vaak genoeg herhalen vinden we ten slotte een vector x die voldoet aan (5).

In feite geeft Hermite's algoritme een vector x in Λ met

$$(10) \quad 0 < |x| \leq \left(\frac{4}{3} + \varepsilon\right)^{\frac{1}{2}n(n-1)} (\det \Lambda)^{1/n}$$

binnen tijd welke, voor iedere vaste n , wordt begrensd door een polynoom in de afmeting van de gegeven voortbrengers van Λ en in $1/\varepsilon$.

In Hermite's tweede brief wordt aangetoond dat ieder n -dimensionaal rooster een basis $b_1, \dots, b_n$ bevat met

$$(11) \quad |b_1| \cdot \dots \cdot |b_n| \leq \left(\frac{4}{3}\right)^{\frac{1}{2}n(n-1)} \det \Lambda.$$

Dit impliceert (5), en generaliseert het eerdere werk van Lagrange, Gauss en Seeber. Overigens werd in 1896 in Minkowski's *Geometrie der Zahlen* bewezen dat de factor in (11) niet de best mogelijke is, maar dat ook een factor lineair in $\sqrt{n}$ mogelijk is. Het bewijs van Minkowski is niet-algoritmisch, gebaseerd op een extensie van Dirichlet's *Schubfachprinzip* ("pigeon-hole principle"): de som van de volumina der goederen die in een kist met inhoud $1 m^n$ passen, is niet groter dan $1 m^n$. (Minkowski's stelling impliceert natuurlijk wel een enumeratieve algoritme.)

Ook in de L^3 -basis-reductie algoritme speelt $\frac{4}{3}$ een belangrijke rol. In feite wordt een polynomiale benadering van Hermite's grenzen (10) en (11) gegeven: voor een gegeven rooster Λ en $\varepsilon > 0$ wordt een basis $b_1, \dots, b_n$ voor Λ bepaald met

$$(12) \quad |b_1| \cdot \dots \cdot |b_n| \leq \left(\frac{4}{3} + \varepsilon\right)^{\frac{1}{2}n(n-1)} \det \Lambda,$$

in tijd begrensd door een polynoom in de afmeting der voortbrengers en in $1/\varepsilon$ (zelfs lineair in $1/\varepsilon$). Dit verbetert dus Hermite's algoritme voor (10).

De L^3 -basis-reductie algoritme heeft zeer veel toepassingen, o.a. in de algebra, getaltheorie, cryptografie, lineaire programmering en geheel-tallige lineaire programmering. Ieder die over deze laatste twee toepassingen iets meer wil weten wordt ten sterkste aangeraden de binnenkort te verschijnen boeken *The Ellipsoid Method and Combinatorial Optimization* en *Theory of Linear and Integer Programming* aan te schaffen.

Two conjectures about a_n

Daniel Shanks, College Park, Md., USA

There is a sequence a_n , beginning with $a_1 = 1$, $a_2 = 47$, $a_3 = 2488$, that has many remarkable properties [1]. I will assume that the reader has [1] before him and that he has seen the (complex) definition of a_n given there in (12). A simpler (but less interesting) definition given in (13) is this:

$$a_n = \frac{1}{24} \text{ of the coefficient of } x^n \text{ in } \prod_{k=1}^{\infty} (1 + x^{2k-1})^{24n}.$$

In [1] the following were proved *inter alia*:

(A) All a_n are positive integers.

(B) a_n is odd if and only if $n = 2^k$.

(C) $a_{mpk} \equiv a_{mpk-1} \pmod{p^k}$

is valid for all primes p and all positive integers m and k .

It is a psychological law of creativity that when one (and this "one" includes at least me if it is not a universal law), discovers something *astonishing*, one is somewhat inclined to *gaze at it in admiration* and not attempt to improve it further. The design of a splendid algorithm encounters a similar pitfall; even when its author is *ecstatic* he should not cease. It is my experience that even the most brilliant algorithm can always be improved by 30%. Having indulged in these philosophical considerations for your benefit, a_k , as you go forth into the world, let me illustrate it with (B). Newman and I were both delighted with it.

But it is not the correct question to ask! That is: What is the largest power of 2 that divides a_k ; i.e., what is s in

$$2^s \parallel a_k ?$$

Write k in binary and let $b(k)$ be the number of "one bits" in this representation. Then

Conjecture 1. $s = 3(b(k) - 1)$.

This is more astonishing, more delightful, and it clearly implies (B)!

Now consider (C) for m odd and $p = 2$. We have

$$2^k \mid a_{m2k} - a_{m2k-1},$$

but what is s in

$$2^s \parallel a_{m2k} - a_{m2k-1} ?$$

Conjecture 2. Let $b = b(m)$. Then

$$(D) \quad \begin{aligned} s &= 3b - 2 & (k = 1) \\ s &= 5k + 3b - 4 & (k > 1). \end{aligned}$$

Astonishing! Why 5? Why 3? Why b ?

In [1, p. 202] we ask the identity of a certain 2-adic number. From the known a_{64} , and (D) for $m = 1$, $k = 7$, we can now write this number to 35 bits (reading from right to left) as follows:

$$\dots 00 \ 010 \ 101 \ 010 \ 111 \ 001 \ 000 \ 101 \ 111 \ 000 \ 101 \ 111. = x.$$

What is x ?

[1] Newman & Shanks, "On a sequence arising in series for π ," *Math. Comp.*, 1984, pp. 199-217.

Note added one week later: I have now proved Conjecture 1.

09.50
16460 facwn nl
44000 asdtg nl

goede morgen
hebben hier een telegram voorhanden uit albuquerque new mexico u.s.a. met
adressering
int h.w. lenstra, jr.
magxxxxx mathematisch inst. universiteit v amsterdam
roetersstr. 15 1018 wb amsterddam

het tgm is afkomstig van g.j. simmons manager applies math dept. 1640 sandia
natkional laboratories albuquerque nm 87185 usa

is dit bericht misschien voor u bestemd +???

jaukunt hetbericht op deze telex zettten bedantk en prettige feesrdagen bibi
x dkuwel mom aub +?
nnnn

zczc atx070 wam913 1-0201xxxx 1-020719a108
n am cn uwnx 428
middltown va 428/403 17 2241p est page 1/052

quote
1-011753a108
0025 intl tdlx albuquerque new mexico april 17, 1984
int h. w. lenstra, jr.
mathematisch instituut, universiteit van
amsterdam, roetersstraat 15, 1018 wb amsterdam,
(netherlands via wui)
i am both embarassed and sorry that an intensive

travel and lecture
schedule has prevented me from submitting an appropriate contribution to the
album amicorum for arjen. as you may not know, he left a continuing reminder
of his visit to the sandia national labortories last year in the form of a
suite of codes that we use almost daily.

one of the more important research efforts in our department is the
development of general purpose algorithms and codes for the factoring of
large composite numbers. as an indication of the success of this effort, we
have advanced the state of the art from nominally 50 digits to over

70 digits in the past two years. the impetus for this work is the
relationship between the difficulty of factoring 'hard' composite numbers
and the cryptosecurity of the rsa asymmetric cryptoalgorithm that sandia
uses in many applications. jim davis and diane holdridge,
with whom arjen spent a very profitable visit,

have achieved roughly
three orders of magnitude improvement in factoring efficiency (as measured
by the time required to calculate a factorization), largely through
exploiting the architecture of the cray family of computers (1s and x-mp)
in an intimate matching of the machine with various refinements of the
quadratic sieve algorithm.

arjen was a visitor
to our department during a critical period of this advance. we were all

greatly impressed by the way he "rolled his sleeves" and worked long hours like a regular member of the staff to implement his primality test on the cray 1s -- a notrivial

problem incidentally because of a slightly different operating system in our machine from what he was familiar with. now, each time a newer and larger number is factored, arjen's code pronounces the final verdict for the factors as prime or composite.
for jim davis, diane holdridge, myself and all the

other memeber os
our department who met and got to know arjen, i extend our congratulations on this occasion and our best wishes for the future to a valued colleague.
g. j. simmons, manager, applies mathematics dept. 1640
sandia national laboratories
albuquerque, new mexico 87185 usa
twx 910-989-1600
tlx 169012

end/mk

Op feesten en verjaardagen,
had je meestal wel wat vragen,
hoe toch die treinen konden vertragen,
waarom de tarieven niet te verlagen,
aldus de mensen niet uit bus of tram te jagen.

In Israël of Egypte aangeland,
had je de ansichten zo bij de hand,
railvoertuigen stonden dan garant,
voor een smeug verhaal, klein doch pikant.

In de kantine van de Roetersstraat,
werd heel wat wiskunde doorgepraat,
en vervolgens lagen dan de kaarten paraat.

Toepen was dan het spel,
ja, de tijden gaan snel.

Arjen, het ga je goed, met een grap en wat kol,

Wouter Simonis, alias Pol.

ONWETENSCHAPPELIJKE OBSERVATIES

Naamloos, maar onmiskenbaar een Lenstra, kwam hij aan op het MC, en wij noemden hem de eerste weken vanwege zijn jeugdige uiterlijk Babytje Lenstra. Zijn lengte en zijn ongekend bekakte spraak gaven hem echter overwicht (trouwe Hendrik Lenstra-aanhangers verdedigen die spraak als "Gronings", maar Arjen behoeft deze verdediging niet: het is zo rondborstig bekakt dat het weer innemend is). Zijn vriendelijke glimlach maakte hem toegankelijk. Weldra noemden wij hem dan ook Arjen. Die glimlach en zijn hoge zwarte herenfiets onderscheidde hem van zijn MC-broer.

Broers en zusters moeten niet met elkaar vergeleken worden. Leraren op school hebben die gewoonte, en ik heb vrienden die daar zeer ondergeleden hebben. Bij de Lenstra's echter is vergelijken welhaast onvermijdelijk. Het gerucht gaat dat voor een van hen vrouwen volstrekt verwisselbaar zijn. Hij zou ze slechts door de kleur van hun truitje uit elkaar kunnen houden. Wij vinden dit, komend van een Lenstra, een got-spe, want zijn deze broers niet vrijwel identieke copieën van elkaar? Ikzelf heb Arjen voor het eerst gezien, ver voor zijn MC tijd, in het Concertgebouw, waar wij een abonnement op dezelfde serie hadden. Hij zat drie stoelen voor mij en een bibliotheekcollega. Bij het derde concert zei mijn collega, die niet over één nacht ijs gaat: "Die jongen heeft net zo'n achterhoofd als Jan Karel." Aan de telefoon is het, zelfs voor henzelf zoals eentje mij opbiechtte, volstrekt onmogelijk om uit te maken wie je aan de lijn hebt, zeker daar ze allemaal opnemen met een licht geprikkeld "Lèn-stra".

Doordat Arjen niet voortdurend glimlachte en doordat het drie jaar geleden nog geen gewoonte was om binnen het MC met je fiets rond te lopen, kwam het toch nog wel eens voor dat hij met Jan Karel verward werd. In dat geval bood de vrouwentruc van hun slimme broer uitkomst: die met de grijze trui was Arjen. Tegenwoordig is het veel makkelijker en zowel visueel als acoustisch eenvoudig vast te stellen: die met de hinderlijke pieper is Jan Karel.

Spoedig werd Arjen ingeschakeld bij het toekennen van classificatiecodes aan de bibliotheekboeken. Al zegt hij van zichzelf "Ik ben een aartsluiaard", het was juist zijn werklust die ons voor hem innam. Met een angstwekkend élan voorzag hij een hele boekenkast vol achterstallige

boeken met zijn hanepootje van een MSC-code. Zuchtend en steunend nam hij altijd zgn. SPOED-boeken van mij in ontvangst, om ze een kwartier later verwerkt en al blijmoedig op mijn bureau te deponeren. Hij was het die het duurste boek dat de bibliotheek ooit op zicht heeft gehad (veertienhonderdvierennegentig gulden en zevenenzestig cent) aan de boekhandel durfde te retourneren met de dodelijke kritiek: "Het is net een Time-Life boek!" Enigszins verdrietig dat zulke lelijke, inhoudsloze boeken geproduceerd konden worden, schudde hij daarbij het hoofd.

Met oog voor detail haalde hij, net als zijn broer Jan Karel, geregeld punten van mijn hoofdletters i. Ik heb die punten pas afgeleerd toen ik de programmeertaal B leerde, waarvoor ik veel in hoofdletters moest schrijven, met name de woorden IN en IF. Die taal is overigens het enige wrijvingspunt geweest tussen Arjen en mij. Hij heeft zich uitsluitend met diepe minachting over het ontwikkelen van B uitgelaten en volgde gemeen gniffelend aan een belendende terminal mijn lessen. De frequentie en langdurigheid waarmee B-mensen de photo-typesetter plegen te bezetten en ook de gewoonte die zij hebben om van het ene uiteinde van de terminalruimte naar het andere luidkeels met elkaar te converseren over het onderwerp van hun wetenschappelijke interesse, hebben ons kort geleden een andere Arjen doen leren kennen: de boze variant, die ons in niets meer herinnerde aan het verlegen Babytje Lenstra van weleer. Arjen is zichtbaar ouder geworden in zijn jaren op het MC.

Het is algemeen bekend dat Lenstra's zich van hun waarde en kwaliteiten bewust zijn en daar zonder deemoedigheid mee weten te leven. In Arjen werd dit onlangs geïllustreerd toen ik met hem sprak over zijn naderende afscheid van het MC ("het zinkende schip verlaten" noemde hij het zelf). Terugkijkend op ons contact zei ik: "Ik zal je missen." - "Dat weet ik," zei hij eenvoudig.

Joke Sterringa

OVER DE LAATSTE STELLING

door

Herman J.J. te Riele
CWI, Amsterdam

De laatste stelling (nummer 9) bij het proefschrift van Arjen Klaas Lenstra luidt (om het tellen van de cijfers van het in deze stelling voorkomende getal voor de lezer iets te vereenvoudigen heb ik twee " telregels " toegevoegd):

1	2	3	4	5	6
1234567890	1234567890	1234567890	1234567890	1234567890	1234567890

1920151820	2706126283	5271516270	1021427180	5110514091	4071421131
3051827548	2423212722	0114270128	1128271205	1419201801	2720052701
1319200518	0401132705	1427040914	0727130505	2714010118	2704052706
1244284527	0605051920	1618090513	1618091019	is	priem.

Vaak hebben laatste stellingen een dubbele bodem. In deze bijdrage aan het album amicorum zal ik proberen een dubbele bodem op te sporen.

Om het album niet te dik maken, neem ik de vrijheid om het onderwerp van de laatste stelling af te korten met N. Ik werk steeds, zoals naar ik aanneem ook de promovendus in zijn laatste stelling, in het tientallig stelsel.

Het eerste wat me opvalt is dat het aantal cijfers van N 220 is. Het getal 220 is het kleinste element van het kleinste bevriende getallenpaar (220,284). Voorwaar een opmerkelijke (Freudiaanse?) coincidentie bij het verschijnen van dit album amicorum!

Voor hen die niet weten wat een bevriend getallenpaar is: dat zijn twee verschillende getallen met de eigenschap dat de som van alle delers van het ene getal die kleiner zijn dan dat getal, gelijk is aan het andere, en omgekeerd. Bevriende getallenparen zijn mij persoonlijk zeer dierbaar en eenieder die geïnteresseerd is kan van mij een flinke lijst van deze getallenparen krijgen.

Het tweede wat me te doen viel, was te verifiëren of N inderdaad priem is. Dit niet om Arjen te beledigen, maar om te kijken of ik zijn programma uit de elektronische ingewanden van SARA zou kunnen opduiken. Dit lukte, na enig zoeken, en inderdaad verklaarde het gevonden programma, na 651339 milliseconden rekenen, dat N priem is. Dit is uiteraard geen onafhankelijke controle, maar ik kan niet uitsluiten dat de versie die Arjen gebruikte een andere is dan die welke ik heb gebruikt. Het getal dat ik kreeg door de cijfers van N in omgekeerde volgorde op te schrijven is samengesteld, met kleinste priemdelers 557. Derhalve is N wel een gewoon, maar geen palindromisch priemgetal.

Vervolgens vroeg ik me af of Arjen N zo had gekozen dat ik zou kunnen bewijzen dat er bij het reproductieproces niet twee verschillende opeenvolgende cijfers van N waren verwisseld. Dit bewijs zou ondubbelzinnig geleverd kunnen worden als alle getallen, die men kan vormen door in N twee opeenvolgende verschillende cijfers te verwisselen, samengesteld zijn. Aangezien N een getal van 220 cijfers is en het i - de en $(i+1)$ - ste cijfer slechts aan elkaar gelijk zijn voor $i = 42, 57, 79, 82, 91, 114, 120, 126, 134, 168$ en 183 (namelijk, respectievelijk, $1, 1, 2, 1, 1, 0, 1, 0, 1, 1$, en 4), zijn er $219 - 11 = 208$ getallen, waarvan ik moest onderzoeken of ze samengesteld zijn, teneinde het bovenbedoelde bewijs te kunnen leveren. Dat was nogal wat werk, en mijn moeite werd niet beloond: helaas is een van die 208 getallen priem, namelijk het getal dat men krijgt door in N het 130 - ste en het 131 - ste cijfer (8 en 0) te verwisselen. Noem dit getal M. Het bovengenoemde programma verklaarde M priem na 470769 milliseconden rekenen. Alle andere 207 getallen bleken samengesteld te zijn. De vraag lijkt daarom gerechtvaardigd: heeft Arjen in zijn laatste stelling misschien bedoeld: " M is priem ", in plaats van: " N is priem " ?

Een andere vraag die men naar aanleiding van het bovenstaande zou kunnen stellen is de volgende: bestaan er priemgetallen met de eigenschap dat je, als je daarin twee opeenvolgende verschillende cijfers verwisselt, in alle mogelijke gevallen weer een priemgetal krijgt ? Het antwoord is eenvoudig: ja, bv. 11. Met de computer vond ik dat er tussen 10 en 1000000 precies 381 van dergelijke priemgetallen liggen. Veel van die getallen hebben op een of meerdere plaatsen gelijke opeenvolgende cijfers. Als we die getallen uitsluiten, dan blijven er 78 over:

TABEL
=====

VAN ALLE PRIEMGETALLEN VAN 2, 3, 4, 5 EN 6 CIJFERS DIE DE VOLGENDE TWEE EIGENSCHAPPEN HEBBEN:

1. GEEN TWEE OPEENVOLGENDE CIJFERS ZIJN AAN ELKAAR GELIJK;
2. ALS MEN TWEE OPEENVOLGENDE CIJFERS ONDERLING VERWISSELT KRIJGT MEN WEER EEN PRIEMGETAL.

aantal cijfers	priemgetallen
=====	
2	13 17 31 37 71 73 79 97
3	131 137 179 373 379 397 419 491 613 919
4	1013 1031 1091 1213 1231 1579 2131 2719 3617 4217 4519 4937 4973 5417 5897 6073 6373 6791 9431 9473 9697 9871
5	15193 17597 24373 26497 26731 30391 35419 36793 42473 54139 60217 60373 63097 63131 65731 74717 76213 82031 86171 89017 89213 95971
6	102539 105373 196837 210193 235439 258673 262313 265831 463231 505691 567493 582391 594379 617971 648191 918139
=====	

Als we nu ook nog de restricties opleggen dat het eerste en laatste cijfer verschillend moeten zijn en dat we na verwisseling hiervan ook nog een priemgetal moeten krijgen, dan wordt de spoeling erg dun: afgezien van de getallen van twee cijfers in bovenstaande tabel, blijven er dan nog slechts zeven over: 179, 9431, 9697, 9871, 17597, 35419 en 76213.

Ik ben me ervan bewust dat ik wat ben afgedwaald van mijn speurtocht naar een mogelijke dubbele bodem in Arjen's laatste stelling, maar dat mag ook best, lijkt me, met zo'n stelling. Of ik er in geslaagd ben een al of niet bewust door Arjen aangebrachte dubbele bodem op te sporen, laat ik aan het oordeel van de lezer over.

Hoe zit het trouwens met Stelling 10? Is het ontbreken daarvan soms een dubbele bodem in Stelling 9?

LA MUSICA E LE PAROLE

door R. Tijdeman

Prima la musica, dopo le parole, zo luidt de achtste van A.K. Lenstra. Muziek, de kunstvorm bij uitstek om uiting te geven aan gemeenschappelijke gevoelens. Het woord, het communicatiemiddel bij uitstek om gedachten aan een ander kenbaar te maken. Eerst de muziek, dan het woord? Ik geloof dat deze stelling een dissonant in het proefschrift van de heer Lenstra is.

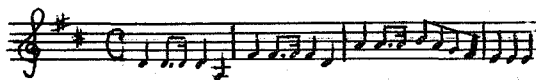
Al voor een baby kan praten, komt hij met muziek in aanraking. Ik herinner me verschillende nachten "Slaap kindje, slaap", gezongen te hebben, als onze kinderen de slaap niet konden vatten, verder "Draai het wieletje nog er eens rond" en "Schuitje varen, theetje drinken" om op een plezierige wijze bepaalde bewegingen te oefenen, "Poesje mauw, kom eens gauw" om dierennamen met hun geluiden te associëren, enz. Afgezien van de vraag of je mijn zingen met muziek wil aanduiden, betrof dit woord èn muziek, met een enkele uitzondering. Het is een dierbare herinnering hoe onze dochter Katinka, toen net een jaar oud, elke avond spontaan een rondedansje maakte op de muziek van een commercial die op een vaste tijd werd uitgezonden. We zetten de televisie aan om van het dansje te genieten. Toch kende ze toen al verscheidene woorden. Ik geloof niet dat de heer Lenstra zijn stelling zal verdedigen door te betogen dat kinderen eerst met muziek vertrouwd gemaakt moeten worden voordat ze door de ouders toegesproken mogen worden, of dat ze muziek moeten kunnen maken voor ze mogen praten.

Het is mogelijk dat de a.s. doctor wil propageren dat ook in andere proefschriften elk hoofdstuk wordt voorafgegaan door een notenbalk. Maar dit zou een ernstige misvatting zijn. Een notenbalk is geen muziek. Het suggereert muziek, zoals de daarop volgende woorden en formules aan de ingewijden een wiskundige gedachtengang suggereren. Het zijn beide reeksen codewoorden. Het zou wellicht ongebruikelijk, maar niet moeilijk zijn om een stuk wiskunde te presenteren door noten op een notenbalk, en niet onmogelijk om een stuk muziek te presenteren in de vorm van een computerprogramma. De kenner zou met het resultaat vermoedelijk geen vrede hebben, maar functioneel gezien is een notenbalk met noten meer woord dan muziek. zo bezien heb ik een boekwerk vol woorden ontvangen, al zit er zeker muziek in. Maar misschien zoek ik het te ver en heeft de heer Lenstra met zijn stelling er alleen op willen duiden dat we in de Aula van de Universiteit vóór de uitwisseling van gedachten vergast zullen worden op muziek.

Dit leidt me tot een derde mogelijke verdediging van de stelling. Zou het zin hebben dat mensen voor er gesproken wordt eerst tezamen naar muziek zouden luisteren of samen musiceren? Onder bepaalde omstandigheden zeker wel. Denk aan orgelspel in een kerkdienst of, in ander verband, aan een muziekkorps dat poogt mensen in carnavalsstemming te brengen. Maar het "eerst de muziek" heeft alleen betrekking op een korte tijdsspanne, want de toehoorders moeten een zekere ervaring gemeen hebben, wil er nog van een daaropvolgend woord sprake zijn. Zet honderd willekeurige mensen in een kerkgebouw waar iemand orgel speelt of in een feestzaal waar carnavals-schlaggers gespeeld worden en voor het muziekstuk voltooid is, zal een aanzienlijk deel van de bezoekers de zaal verlaten hebben.

Pas dan als de aanwezigen weten wat ze kunnen verwachten en zich daarbij betrokken voelen, zal er gelegenheid zijn om ongestoord van de muziek te genieten. De enige andere mogelijkheid om de aanwezigen er toe te brengen naar muziek te luisteren is om hen eerst zodanig toe te spreken dat ze nieuwsgierig of geïnteresseerd raken en pas als er zo een sfeer ontstaan is, zal er ongestoord naar de muziek geluisterd worden. Ook in deze gevallen is het dus niet zo dat muziek het werkelijke begin vormt.

Het is natuurlijk niet zeker dat het "prima...dopo..." op tijd betrekking heeft. Wellicht wil de promovendus staande houden dat "muziek" belangrijker is dan woord. Maar in dat geval is de stelling, ongetwijfeld gewild, onvolledig. Belangrijker waarvoor? Het belang van de muziek als middel om aan gevoelens uiting te geven is niet te meten. Het is een voor velen onmisbaar communicatiemiddel. Denk aan de liefdesliederen, vaak geschreven als de geliefde niet aanwezig is en ook niet geneigd is om terug te keren, om over requiems nog maar te zwijgen. Maar ook het woord vervult soms die functie. Een aanzienlijk deel van de poëzie is onder dezelfde omstandigheden geschapen. Als het woord uit de wereld gebannen zou worden, zou er van een samenleving geen sprake kunnen zijn! Drs. A.K. Lenstra zou ook nooit Dr. A.K. Lenstra kunnen worden en dat zou toch te betreuren zijn. Ik hoop en verwacht dat velen door het lezen van het proefschrift zo geraakt worden, dat ze miodels muziek uiting zullen geven aan hun vreugde over zoveel moois. In dit geval dus: Prima le parole, dopo la musica.



DE FYSICA VAN HET OPENEN VAN EEN DEUR

door G.M.Tuynman

1. Inleiding

Er bestaan verschijnselen die doorgaans niet opvallen, doch die, wanneer men er eenmaal op attent gemaakt is, veelvuldig blijken voor te komen. Het openen van een dubbele deur is zo'n verschijnsel. Prof.dr.S.A.Wouthuysen wees mij eens op het feit dat de grootte van de opening die ontstaat bij het openen van een dubbele deur slechts een tweede orde effect is (in de openingshoek), terwijl de opening bij een enkele deur een eerste orde effect is.

Deze correcte observatie heeft enkele soms lachwekkende gevolgen waaronder het volgende : bij een warenhuis (die hebben vaak dubbele deuren) kan men regelmatig waarnemen dat een klant via één van de twee deuren naar binnen wil gaan, en dat een tweede klant, die door de tweede deur naar binnen wil gaan, effectief de doorgang van de eerst genoemde belemmert, juist door het openen van de tweede deur.

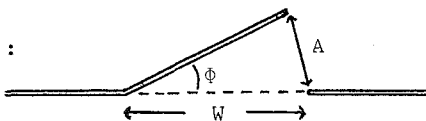
Dit regelmatig voorkomende verschijnsel, waar schrijver dezes soms ook de dupe van wordt, geeft aanleiding tot de vraag : waarom gebruikt men dubbele deuren ? Een poging tot beantwoording van deze vraag heeft geleid tot onderstaande studie.

2. Het probleem

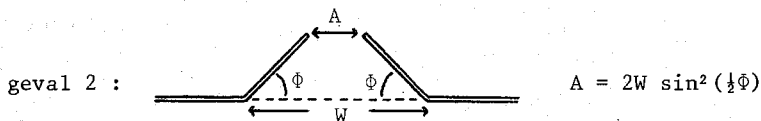
Wanneer men dubbele deuren wil vergelijken met een enkele deur (van dubbele breedte), dan is de eerst te beantwoorden vraag : welk aspect moet vergeleken worden ? In deze studie is gekozen voor het aspect tijd : de tijd die nodig is om de gewenste opening voor doorgang te verkrijgen, gegeven dat men een eenmalige duw tegen het uiteinde van de deur (deuren) geeft. Die configuratie die in de kortste tijd de gewenste opening geeft wordt dan gezien als de voorkeursconfiguratie.

Zij nu W de breedte van het deurgat (dat wil zeggen de breedte van de deur in het geval van een enkele deur en tweemaal die breedte in het geval van een dubbele deur), zij A de gewenste opening en Φ de hoek die de deur (deuren) maakt (maken) met de muur (= dichte stand van de deur) wanneer de gewenste opening A is bereikt. In de twee situaties die we zullen beschouwen (genummerd 1 en 2) wordt het verband tussen de grootheden W , A en Φ gegeven door de volgende vergelijkingen :

geval 1 :



$$A = 2W \sin(\frac{1}{2}\Phi)$$



Aan deze formules is direct de oorspronkelijke observatie te verifiëren, namelijk dat de opening van een dubbele deur een tweede orde effect is, in tegenstelling tot een enkele deur waar het een eerste orde effect is. Er dient nu echter opgemerkt te worden dat de twee geschetste situaties niet de enig mogelijke zijn, en dat de te verkrijgen resultaten niet toegepast kunnen worden indien de deur (deuren) toegang geeft (geven) tot een smalle gang waarvan de lengte-richting loodrecht op de deur staat, omdat in geval 1 de opening A zoals geschetst in de figuur dan niet de reële opening van de deur is.

3. De fysica

De bewegingsvergelijking van een voorwerp dat roteert om een vaste as wordt gegeven door :

$$(1) \quad \tau = I \frac{d^2\phi}{dt^2}$$

waarbij ϕ de hoek is die de positie van het voorwerp beschrijft, τ het moment van de uitgeoefende kracht (dat wil zeggen $\tau = F \cdot r$ waar F de uitgeoefende kracht is en r de afstand van de as van draaiing tot de werklijn van de kracht) en I het traagheidsmoment van het voorwerp ten opzichte van de gegeven as :

$$I = \sum_j m_j r_j^2$$

waarin de sommatie loopt over alle constituerende deeltjes van het voorwerp, waarin m_j de massa van het j-de deeltje is en r_j de afstand van dit deeltje tot de as van rotatie. Wanneer het voorwerp gezien wordt als hebbende een semi-continue massaverdeling, dan mag men de sommatie vervangen door integratie (men raadplege voor preciezere beschouwingen omtrent roterende voorwerpen het boek "Mechanics and properties of matter" van R.J. Stephenson).

Wanneer we veronderstellen dat een deur een te verwaarlozen dikte heeft en dat de massa per breedte m bedraagt, dan wordt het traagheidsmoment van een deur met breedte R gegeven door :

$$I = \int_0^R m r^2 dr = \frac{1}{3} m R^3$$

We veronderstellen nu dat men, om een deur te openen, gedurende een korte tijd Δt een constante kracht F loodrecht op het uiteinde van de deur uitoefent en de deur vervolgens op eigen kracht laat verder draaien (wrijvingsloos!?). Voorts veronderstellen we dat de tijd Δt dermate kort is dat we de verandering van de hoek ϕ gedurende die tijd mogen verwaarlozen (de deur krijgt een korte stoot). Gaan we uit van de beginsituatie :

$$\phi(0) = 0, \quad \frac{d\phi}{dt}(0) = 0$$

(dit is de toestand van een dichte deur in rust) dan volgt uit vergelijking (1) :

$$\phi(\Delta t) \approx 0, \quad I \frac{d\phi}{dt}(\Delta t) = \tau \cdot \Delta t$$

$$\frac{d\phi}{dt}(\Delta t) = 3 \frac{F \cdot \Delta t}{mR^2}$$

of, wanneer we het tijdstip $t = \Delta t$ weer als beginpunt van de tijd zien :

$$\phi(0) = 0, \quad \frac{d\phi}{dt}(0) = 3 \frac{F \cdot \Delta t}{mR^2}$$

waarna de deur (weer volgens vergelijking (1)) met een eenparige hoeksnelheid verder opengaat :

$$\phi(t) = \frac{d\phi}{dt}(0) \cdot t = 3 \frac{F \cdot \Delta t}{mR^2} \cdot t$$

$$(2) \quad T = \frac{1}{3} \frac{mR^2}{F \cdot \Delta t} \phi$$

4. De analyse

We passen nu de resultaten van §3 toe op de twee situaties zoals geschetst in §2. In geval 1 komt de kracht F geheel ten goede aan de deur met breedte $R = W$ en wordt de gewenste openingshoek gegeven door $\phi_1 = 2 \arcsin(\frac{1}{2}A/W)$, zodat de tijd die nodig is om deze opening te bereiken gegeven wordt door :

$$(3) \quad T_1 = \frac{2}{3} \frac{mW^2}{F \cdot \Delta t} \arcsin(\frac{1}{2}A/W)$$

In geval 2 komt slechts de halve kracht ten goede aan een deur met breedte $R = \frac{1}{2}W$ en wordt de gewenste openingshoek gegeven door :

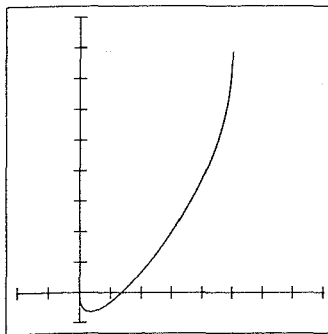
$$\phi_2 = 2 \arcsin(\sqrt{\frac{1}{2}A/W})$$

zodat de tijd die nodig is om in deze situatie de gewenste opening te krijgen gegeven wordt door :

$$T_2 = \frac{2}{3} \frac{m(\frac{1}{2}W)^2}{\frac{1}{2}F \cdot \Delta t} \arcsin(\sqrt{\frac{1}{2}A/W})$$

$$(4) \quad T_2 = \frac{1}{3} \frac{mW^2}{F \cdot \Delta t} \arcsin(\sqrt{\frac{1}{2}A/W})$$

Wanneer we het verschil $T_1 - T_2$ uitzetten als functie van $\frac{1}{2}A/W$, dan krijgen we (in zekere eenheden) figuur 1, waarin $\frac{1}{2}A/W$ loopt van 0 tot 1; het nulpunt van deze functie ligt bij $\frac{1}{2}A/W = 0.2696$ ofwel bij $A = 0.5392 \cdot W$.



figuur 1

5. Conclusies

Stelt men de vraag wanneer men (met name in warenhuizen) enkele deuren, dan wel dubbele deuren moet gebruiken, waarbij men als beslissingscriterium neemt de snelheid waarmee de deur (deuren) geopend kan (kunnen) worden, dan zal het antwoord afhangen van de verhouding $A : W$ waarbij we A kunnen zien als de gewenste gemiddelde opening (gemiddeld over vele malen openen) en W als de gewenste maximale opening (het deurgat). Voor $A : W \leq .5392$ verdient een enkele deur de voorkeur, voor $A : W \geq .5392$ de dubbele deur, uitgaande van de veronderstelling dat de deur (deuren) met een korte stoot wordt (worden) open geduwd en aannemende dat men bij een dubbele deur beide deuren opent en er midden tussen door gaat.

Tot slot dient opgemerkt te worden dat bovenstaande studie slechts betrekking heeft op het openen van deuren, met name wanneer deze toegang geven tot grote ruimten; het probleem van het daarna wederom sluiten van de deuren valt buiten het kader van deze studie. Eveneens buiten het kader van deze studie vallen deuren die voorzien zijn van een dranger systeem.

! ? TRUE .OR. FALSE ? !

by

J. van de LUNE

Our theme (con variationi in words and formulas) will be a tentative reconsideration of some of the oldest mathematical objects, to wit: the natural numbers 1, 2, 3,

Hitherto we have considered these numbers as *constants*, having unique decompositions into *constant (natural) "atoms"* which, in a short-hand notation, are usually denoted as

$$(1) \quad n = \prod_p p^{e_p(n)}.$$

A good deal of the regularities as well as the irregularities of these decompositions are reflected in the corresponding so-called zeta function of Riemann

$$(2) \quad \zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad (s = \sigma + it; \sigma > 1).$$

It is well known that this function is in fact a meromorphic function with only one simple pole at $s = 1$. Furthermore, the non-real zeros of $\zeta(s)$ have attracted much attention during the last 100 years.

Riemann stated (without the slightest hint of proof) that all these (non-trivial) zeros lie on the vertical $\sigma = \frac{1}{2}$. This statement is the famous Riemann Hypothesis which has never been proved nor disproved, although we know, since the 11-th of April 1984, that the first 1 000 000 000 non-trivial zeros of $\zeta(s)$ are all simple and lie on the critical line $\sigma = \frac{1}{2}$.

Although it is known for quite a long time that all zeros of $\zeta(s)$ have real part < 1 , one of the most striking things is that nobody has ever succeeded in showing that there exists a number $\alpha < 1$ such that $\zeta(s) \neq 0$ for all $\sigma > \alpha$. In spite of even the best results concerning the zero-free region of $\zeta(s)$ we are still faced with the "possibility" that $\zeta(s)$ has zeros arbitrarily close to $\sigma = 1$.

However, there seem to be only a few mathematicians considering this

possibility as realistic. Nevertheless, it should not be forgotten that some of the main experts in this field had serious doubts with respect to the truth of the Riemann Hypothesis. Through the grapevine I have heard that, for example, Littlewood and Turán were amongst them. I think that they were and are right in the sense that especially in mathematics one should not too readily believe in things which have not been proved. Just recall Hardy versus Eddington in relation to Skewes' number.

Let us try to reflect somewhat "deeper" upon the zeros of $\zeta(s)$ and which properties of the natural numbers are hidden in them.

First of all let us transform the natural numbers into *polynomials* as follows. For every prime p choose a complex number z_p , write $z := (z_2, z_3, z_5, \dots, z_p, \dots)$ and define for any natural number n the "general natural polynomial" $n(z)$ by

$$(3) \quad n(z) = \prod_p (p+z_p)^{e_p(n)}.$$

It is easily seen that the correspondence $n \leftrightarrow n(z)$ is one-one.

In the sequel we will only deal with the special case $z_p = \tau_p \in \mathbb{R}$.

In order to keep our discussion as simple as possible we subject τ_p to the following constraints. Choose two constants α and K such that $0 \leq \alpha < 1$ and $K > 0$. Let

$$(4) \quad |\tau_p| \leq K \cdot p^\alpha \quad \text{for all sufficiently large } p$$

and

$$(5) \quad p + \tau_p > 1 \quad \text{for all } p.$$

Then we have, similarly as in the classical case,

$$(6) \quad \zeta_\tau(s) := \sum_{n=1}^{\infty} (n(\tau))^{-s} = \prod_p (1 - (p + \tau_p)^{-s})^{-1}, \quad (\sigma > 1)$$

where, as one might have guessed, τ stands for the "vector"

$(\tau_2, \tau_3, \tau_5, \dots)$. It is easily verified that $\zeta_\tau(s)$ is analytic on the halfplane $\sigma > 1$.

Question: Has $\zeta_\tau(s)$ any analytic continuation beyond the line $\sigma = 1$?

At this instance one may feel somewhat baffled since, in the classical case, the analytic continuation of $\zeta(s)$ is most simply achieved by means of the basic observation that the natural numbers are "equally spaced", a property which is *not* shared in general by our "natural polynomials" $n(\tau)$. The situation is even worse than that. In general $m(\tau) - n(\tau)$ isn't even a natural polynomial. Isn't it somewhat remarkable that the analytic continuation of $\zeta(s)$ has never been established by only using properties of its Euler product representation ?

However, something that does not seem to work in the classical case, may work very well in a more weird situation. Indeed, since $\zeta(s) \neq 0$ for $\sigma > 1$ we may consider (for $\sigma > 1$)

$$(7) \quad \frac{\zeta_{\tau}(s)}{\zeta(s)} = \prod_p \frac{1 - \frac{1}{p^s}}{1 - \frac{1}{(p+\tau_p)^s}} = \prod_p \left(1 - \frac{(1 + \frac{\tau_p}{p})^s - 1}{(p + \tau_p)^s - 1} \right) =: P_{\tau}(s).$$

By means of the simple inequality

$$(8) \quad |e^z - 1| \leq |z| e^{|z|}$$

and a theorem of Weierstrass one will have no difficulties in showing that $P_{\tau}(s)$ is analytic for $\sigma > \alpha$.

Hence

$$(9) \quad \zeta_{\tau}(s) = \zeta(s) \cdot P_{\tau}(s)$$

is analytic for $\sigma > \alpha$.

Since $P_{\tau}(s) \neq 0$ for $\sigma > \alpha$ we also find that $\zeta_{\tau}(s)$ and $\zeta(s)$ have the *same zero-pattern* in the halfplane $\sigma > \alpha$. Isn't that something ?

Hence, in order to tackle the Riemann Hypothesis or anything less drastic aiming at a similar goal, we may just as well study the functions $\zeta_{\tau}(s)$ which have the (barely explored) "advantage" of being built up from the *less rigid* "atoms" $p + \tau_p$.

Similarly one may verify that the above generalization of $\zeta(s)$ also applies to all Dirichlet functions $L(s, \chi)$ and that also their zero-pattern is invariant.

So far our discussion was almost free of any genuine speculation.

From now on we will assume that all τ_p are equal to τ where τ satisfies

the conditions stated before ((4) and (5)).

One may verify that $\zeta_\tau(s)$ has a *simple pole* at $s = 1$ with residue

$$(10) \quad \rho_\tau = \prod_p \left(1 - \frac{\tau}{p(p+\tau-1)}\right)$$

which equals 0 if and only if τ assumes the *excluded* value $\tau = -p$ for some prime p . Following Euler we thus find that

$$(11) \quad 0 \equiv \frac{1}{\zeta_\tau(1)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n(\tau)}.$$

Question: For which τ is (11) true indeed? Are there any complex τ -values for which (11) is true?

Now observe that

$$(12) \quad \log n(\tau) = \sum_{p|n} e_p(n) \log(p+\tau)$$

so that

$$(13) \quad \frac{n'(\tau)}{n(\tau)} = \sum_{p|n} \frac{e_p(n)}{p+\tau}.$$

Assuming that (11) is true indeed for all τ close to zero we find by differentiation with respect to τ

$$(14) \quad 0 \equiv \sum_{n=2}^{\infty} \mu(n) \frac{n'(\tau)}{n^2(\tau)} \quad (\text{note that } n(\tau) \cdot n(\tau) = n^2(\tau))$$

which, for $\tau = 0$, using (13), reduces to

$$(15) \quad 0 = \sum_{n=2}^{\infty} \frac{\mu(n)}{n} \sum_{p|n} \frac{1}{p}.$$

By similar means one may derive from (10) and (14) that

$$(16) \quad \sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n} \sum_{p|n} \frac{1}{p} = \sum_p \frac{1}{p(p-1)}.$$

It is worth noting that

$$(17) \quad \sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n} = -1$$

is a well known fact which lies *deeper* than the prime number theorem.

Another remarkable phenomenon is that the right-hand side of (16) is positive whereas that of (17) is negative.

Question: Is (16) true, and if so, what is "its depth" in prime number theory?

Can (15) and/or (16) be proved (if true) by conventional means ?

Another question which arises quite naturally is the following:

For which τ is the set $\{\log(p+\tau) \mid p \text{ prime}\}$ linearly independent over $\mathbb{Q}$? In particular, are there any rational τ 's of this kind ?

We conclude this more or less speculative part by *indicating* some other possible "generalizations" in and around analysis and/or number theory. It is well known that Euler's constant γ may be defined by

$$(18) \quad \gamma = \sum_{n=1}^{\infty} \left(\frac{1}{n} - \log\left(1 + \frac{1}{n}\right) \right).$$

Therefore, let us consider the function

$$(19) \quad \gamma(\tau) := \sum_{n=1}^{\infty} \left(\frac{1}{n(\tau)} - \log\left(1 + \frac{1}{n(\tau)}\right) \right), \quad (\tau \geq 0).$$

It is clear that

$$(20) \quad \gamma'(\tau) = - \sum_{n=2}^{\infty} \frac{n'(\tau)}{n(\tau)} \frac{1}{n(\tau)(n(\tau) + 1)}$$

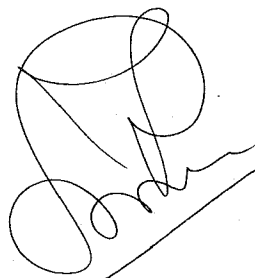
so that by (13)

$$(21) \quad \gamma'(0) = - \sum_{n=2}^{\infty} \frac{1}{n(n+1)} \sum_{p|n} \frac{e_p(n)}{p}.$$

Will FORTRAN live long enough to compute this constant with a precision of at least 220 significant digits ?

Congratulations and good luck for the future,
hoping that you and/or some of your friends
will explore my experimental thoughts further
than I did in the brief sketch above.

Centre for Mathematics and Computer Science
Amsterdam



Dichtwerck ter eere van
den promotie van Arjen Klaes Lenstrae tot
doctor in den wyskunde en zoo meer
XVI Mei MCMLXXXIV

Kort Begryp

Verteller

Hoort wat ick U zeggen gae,
't Is waer gebeurt, gaet het maer nae.
't Treft een Amsterdamschen heer,
Die eens besloot: ick promoveer.
Hy zou dit doen een dagh in Mei
Met paranymphen aen zyn zy.
Van deezen heughelycken dagh
Volgt thans het schriftelyck verslagh.

Den Morgenstont
(aen den Stadthouderskaede XXXII)

Arjen Klaes

"Daer ryst het alverquickent licht
Dat laegh gedaelt beneen de kimmen
De schaduwen en bleecke schimmen
Verdryft van 's aerdtryx aengezicht.
Den speeldoos zich vanzelf ontstoocken
B'gint met quicklent morgenliet,
Deez' dagh nogh verre in 't verschiet,
Ick blyf wat in myn deck gedoocken".
(Langsaem dryft zyn arm opzy
Naer 't bet, hy weet het neven 't syne)
"Ach, is zy daer die 'k noem de myne?"
(Zoeckt en vint haer zeer naby).

"Dagh zoete nyphe, kleine lief,
Heeft U den ooghen oock reets oopen?
Jae toch, magh ick vurigh hoopen,
Waer 's Uw stemme, hartedief?
Zoo U weet is 't nu den dagh:
'k Zal myn proefschrift defendeeren.
Ay! 'k Zal 't mooment wel zeere eeren
Waerop 'k my doctor noemen magh!"

Nyphe

"Myn hart, ick weet het, 't is wel zwaer,
En hulpe kunt U niet verwachten.
'k Ben naest en by U in gedachten,
'k Hoop het allerbeste maer".

Verteller

Zoo hoirden zy den ochtentsangk
En poosden saemen nogh een wyle,
Toen sloen z'opzy het deck en zyle,
Kwaemen langksaem aen op gangk.
Daer klaeterde den waeterstrael,
Lavendel, oly'n, zachte geuren,
Arjen, by het "baedgebeuren"
Galmd' gelyck een nachtegael.
Plots klonk van verre een geschal!
Rommels gingen aen het dond'ren,
Niet van boven, maer van ond'ren:
"Euheup!" broer Hendrick in den hal.
Dat was voor byde "leucke tyd":
Ter morgenstont een zulcker tuitingk
Meend' altoos denzelfden uitingk:
Hendrick's roep tot het ontbyt!
Flucks gedroogt en aengekleet
Om het "priemmael" te gebruicken,
't Was doir 't heele huis te ruicken:
Heerlyck voetsel stont gereet.

(in 't koockgewelf)

Broer Hendrick

"Welckom broeder, zet U toch.

Ick meen 'k en hoef U niet te wyzen

Op deez' overvloed aen spyzen,

Neemt gerust, ^lmeêr is er nogh".

Verteller

Zoo genooten z' alledry,

Genoeghelyck, met caut en coosen.

Arjen, zuchtende met poozen:

't Promotie-uur kwam naederby!

Nymphe

"Wee myn, hoe kyckt U reets bedruckt,

'k Denck, gy vreescht met groote vreezen,

Dat aenstonts er iets mis zal weezen,

Zy toch niet teneer gedruckt".

Arjen Klaes

"Myn lief, ick wort nu ongerust

En moet een wyl alleene weezen

Om 't schrift nogh eenmael doir te leezen.

U wort doir my nu zacht gekust".

Den Middagh

(Arjen Klaes, peinzende, nu gehult in rock)

Arjen Klaes

"Zal 't heemelsche gerecht, zich nu ten langen leste

Ontfermen oover my, in dit benauwde veste,

En oover wat ick zegh, ten goede of ten kwaede.

O, was het maer voirby, het liefste zonder schaede!

Wat zullen zy my vraeghen, den zwarten duivelklicck,

Licht zal ick 't hen niet maeken, ick dien hen van replieck!!

Zy zullen zitten loeren, deez' geesten uit den hel.

Maer 'k zal myn monde roeren, gewis, dat weet ick wel!!!

"Wat voel ick hier van binnen, myn harte dat zo slaet?
Kom, rustigh nu, bezinnen, op wat er koomen gaet.
Myn nymphen staen te wachten, en vraegen waer ick blyf,
'k Zal gaen met hen en trachten te redden 't veege lyf.

- nu voel ick eerst het heil van 't goet
der g'nootschap nu zy byde
zich voeghen aen myn zyde,
wat valt my hun gezelschap goed!-

Wy zullen ons begeeven naer Lutersch' gindsche kerck,
Wat langer hier te kleeven, voiruit nu, aen het werck!

(in den Luterschen Kerck)

Arjen Klaes

"Wat ongheluck zal my in deeze kerck gemoeten?
Gints komt den hellestroom, op schuifelende voeten,
Daer zie ick Lucifer en naest hem Asmodee,
Een somb're satansrey, in zwavelkleet, o Jee!"...

Verteller

Eind'lyck gingh het dan gebeuren:
D'eersten aenval wert gedaen.
Arjen, niet uit 't velt te slaen,
Defendeerd' in geur en kleuren.
Achter sluuwe listverzinsels
Kleedde men den vraegen in.
Gelyck een hongherighen spin
Een aenval doet vanuit haer spinsels
Vingh men aen met zoet'lyck praen
Over 't "hecht doirtimmert" schryven,
Om het daernae te bekyven,
En venynigh toe te slaen.
Maer, noghmaels, 't ging goet, zie booven,
Arjen speelde mee dit spel,
En het ging hem wonderwel,
Daervoir magh men hem wel looven!!

Nae een warme drie kwartieren
Kwam daer, rinckelent, ten lest
Den pedel met "Hora est",
Eind'lyck kon men toen gaen vieren,
Want den schaere hooghe heeren
Hat den uitslagh snel bepraet,
En besloot na kort beraet
Arjen Klaes te promoveeren.
Arjen was zo zeere blyde
Toen hy dit hadde gehoord
En na het verlossent woirt
(Met den nymphen aen zyn zyde)
Mocht hy daer den bul ontvangen.
Zyn promotor gaf die hem,
Verkondigde met luider stem',
Dat men Arjen onbevange
Kussen mocht, feliciteren,
Met omhelzing of een zoen,
Men was daer om dit te doen;
Zoo begon het recipiëren.

Den avontstont

Verteller

Leezer, ziet, wat toen gebeurde,
't Wert een feestelycken dagh,
Met veel dranken, spys en lagh,
Waerby zachte bloemen geurden
In den avont by 't dineren:
Men hat tussen het bancket
Biedermeyers neergezet
Om den gasten te plezeeren.
Feestgenooden aengeschoven
Hieven 't Arjens eer het glas,
(Dat steeds volgeschoncken was)
En waenden zich in eener hooven

Gelyck er is in 't paradyze.
Spyzen der "noevel kwysien"
Hat men nimmer zoo gezien,
Bereit op zoo byzond're wyze.
Zoo bleef men nogh ueren vieren
Menigh spreecker sprack een woirt,
Dat met eerbiet wert gehoirt
En gevolgt doir applaudieren.
Toen tot slot den keersen blusten
Was het ieder bly te moe,
Vielen Arjens ooghen toe,
En ging men voldaan ter ruste.

Naewoirt van den dichter

Arjen hoirt my aen, 't dichtwerck is thans uit,
Maer 'k heb nogh een beright, in 't naewoirt tot besluit.
Of 't wercklyck zoo zal gaen, als booven staet te leezen,
Op dit mooment is 't vaegh, 't kan wel heel anders weezen.
Maer 'k hoop voir U, myn lief, wanneer U dit hier leest,
Dat Uw promotie-dagh een mooie is geweest.
Den toekomst lacht U toe, wat zal het lot U geeven?
't Is onbekent maer 'k hoop: een heel geluckigh leeven.
Dát is wat ick U wens, den slotzin luit aldus:
Den dichter van dit rym stuurt U een kus van

Gus

A.S. van Dobbenburgh
Amsterdam, maart/april 1984

Nu wat luchtigers:

Recept van "Homo polynomo"

Ingrediënten:

- 4 eetlepels mathematische intelligentie
- 2 eetlepels humor
- 3 eetlepels arrogantie
- 1 grote neus
- redelijke scheut rechtsheid
- snufje oranjegezindheid
- 1 pakje liefde voor de hoofdstad
- 3 eetlepels betweterigheid
- 2 pakjes operaliefde
- 1 theelepeltje moeilijke woorden
- 1 liter korenwijn

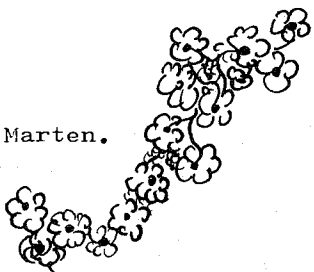
Bereidingswijze:

Neem de grootste beslagkom die u heeft en doe daar alle ingrediënten één voor één in genoemde volgorde in, behalve de korenwijn. Na elke toevoeging goed roeren met een pollepel. Doe nu het mengsel in een braadpan over en breng het aan de kook. Na een kwartier van het vuur nemen en afblussen met de korenwijn. Giet het geheel nu over in een cakevorm. Verwarm de oven voor gedurende tien minuten op stand drie en laat dan het gerecht in vier uur gaar worden. Stort het dan in twee nette, zwarte schoenen. Kneedt het in de door u gewenste vorm en laat het twee uur opstijven in de koelkast.

Let op: Als u er te veel humor bijdoet wordt het nog al meelig; als u er te veel betweterigheid bijdoet wordt het erg zwaar verteerbaar. Maar vergezeld van een goed glas "Appellation A.S. van Dobbenburgh 1955 Controlée" is het 'exquise'.

Proficiat,

Lies en Marten.



Eindelijk vrij!

"Do you speak English?" vroeg hij.

"Yes!" zeiden wij.

"Where are you going?" vroeg hij.

"To Holland!" zeiden wij.

Hij was een Engelse officier, met snor. Hij stak gedeeltelijk bovenuit de koepel van een tank die zachtjes knorrend naast ons was blijven staan. De witte ster op de zijkant was zichtbaar tussen de dennetakken door die het gevaarte aan het oog onttrokken. De loop van het kanon stak er tussenuit in de richting waaruit wij kwamen.

Wij waren drie vrienden, die -toen de tekenen er op wezen dat we dieper landinwaarts zouden worden gebracht- in de ogenblikken van onoplettendheid van de wacht over de omheining waren geklommen. Eind maart 1945.

Sindsdien hadden we twee, het kan ook zijn drie, dagen gelopen, ons zoveel mogelijk schuil houdend om ontmoetingen met het terugvluchtende leger te vermijden.

En daar stonden we nu, oog in oog met het wonder. Eigenlijk geheel perplex, want nog maar even tevoren hadden we een veldspoor verlaten en ons op de grote weg gewaagd, omdat een Franse krijgsgevangene die met dampende paarden een akker omploegde -duidende op een zwak gerommel in de verte- had gezegd: "Ca dure déjà dix jours!"

Daar waren ze dan, op twee kilometer ten Westen van Sulingen op de weg naar Diepholz. Toen we door Sulingen liepen heerste daar een uitgelaten stemming. De Russen, ook dwangarbeiders, hadden de levensmiddelenwinkels nagezien en ook de dranken niet onberoerd gelaten. Aan de rand van de plaats stonden twee Duitse Tigertanks de Engelsen op te wachten. Aan één daarvan mankeerde iets en de beide bemanningen -in de gehate zwarte uniformen- waren daardoor zo in beslag genomen, dat ze ons niet opmerkten. Dat was dom van hen.

De Engelse officier was zeer geïnteresseerd in onze mededelingen over die situatie en sprak: "That was very useful. Thank you very much!" Vervolgens haalde hij een microfoon naar boven en vertelde ons verhaal aan de achter hem komenden.

En dat waren er nog al wat. Toen we een flauwe bocht hadden gepasseerd, waarin een grote boerderij stond, zagen we pas dat de weg -zover we konden zien- vol was met pantserwagens van de meest uiteenlopende aard.

Uit hun boordradio's kwamen met tussenpozen de bevelen van "onze man voorop". Opeens riep iemand: "Take cover you there, we'll get some fire". En hij sloot zijn klep.

Een kort maar hevig kanongebulder weerklonk uit de richting Sulingen.

Toen kwam de stem weer uit de radio: "I want numbers 407 and 512.

Come on, come on!". De opgeroepen monsters maakten zich los uit de file en reden er langs naar voren.

Hij leefde dus nog, en wij ook.

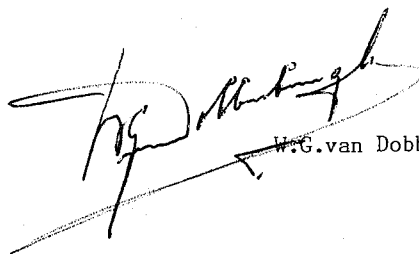
En we waren eindelijk vrij, bijna tastbaar.

Aan dit kleine grote voorval moest ik denken bij de promotie van Arjen. Want hij is dan na vijftien jaar studeren aan het einde van zijn opleiding gekomen. Geen tentamens en examens meer, geen artikelen en geschriften waar iemand het mee eens moet zijn om verder te kunnen. Eindelijk vrij!

Ik wens hem toe, dat hij nooit bevrijd zal behoeven te worden zoals ik toen, en dat hij zich in zijn nieuwe toestand van wetenschappelijke vrijheid zal gevoelen als een vis in het water.

Mogen de vruchten van zijn arbeid steeds blijven voorbehouden aan hen die de vrijheid van anderen ongemoeid laten.

Zwolle, april 1984.

A handwritten signature in dark ink, appearing to read 'W.G. van Dobbenburgh', with a large, sweeping flourish underneath.

W.G. van Dobbenburgh.

Aansluitend aan het hieraan voorafgaande verhaal van mijn man nog dit:

Vrijheid is in vele opzichten een uitermate belangrijk goed.

Toch geven wij op bepaalde gebieden die vrijheid graag prijs. Een duidelijk voorbeeld hiervan is het zoeken naar en het zich verbinden met een partner.

Ik dacht dat jij in dat laatste geslaagd was met onze dochter Gusta.

Verder vind ik, dat je het getroffen hebt met te mogen opgroeien en werken in een land als Nederland. Wat vrijheid betreft zijn er heel wat slechtere plekken te vinden op deze wereld.

Arjen, mijn gelukwensen met je promotie en ik hoop dat je een mooie toekomst tegemoet gaat.

Zwolle, april 1984.

G.M. van Dobbenburgh-Vries.
G.M. van Dobbenburgh-Vries.

Arjen, je kwam, zag, en overwon
de polynomial -time algorithms.
Wis- en Natuurkunde is zijn lust en zijn leven,
Tot hij Gusta zag, en overwon.
Met haar ga je naar de States en Rome
Om je licht op te steken en te verspreiden
En om een plaats te zoeken waar je mee kan zuigen
aan de inventiviteit van de Brave New World.
Het Doctoraat is een eerste opsteek naar
je wetenschappelijke loopbaan en carrière
Die naar het zich laat aan zien krachtig en lang zal zijn .
Van Diergeneeskunde weet je waarschijnlijk net zo veel
als je aanstaande familie van Polynominals.
Wanneer jullie vermoed uit de States of Rome terugkomen,
bedenk dan dat de haard warm en de biest koel is
in de landelijke dreven van Houten.

Badinage.

Als een wervelwind kwam hij binnen. De kust was immers vrij? En bij een vrije kust kan de wind zijn gang gaan, zeker een wervelwind.

Wat de rol van zijn moeder is geweest zal nooit bekend worden, want de wegen ener moeder zijn - evenals de moederschoot - ondoorgronde-lijk.

Hij was er. Op alle mogelijke en onmogelijke tijden. In volle lengte aan de achterdeur, de praktijkdeur. Met of zonder geleende auto. Letterlijk voor halen en brengen. Zorgzaam en attent, maar altijd nadrukkelijk aanwezig. Aanvankelijk met een door onzekerheid ingegeven overcompensatie, die snel afbrokkelde onder de welwillende doch kritische aandacht van de jeugdige inhoud van het huis. In de schok die plaatsvond binnen de natuurwetenschappen tussen de wiskundig en de biologisch georiënteerde denkrichtingen moest er water worden gedaan in de mathematische wijn. Dit was mede noodzakelijk door onbegrip van biologische zijde.

Gelukkig is het mogelijk gebleken persoonlijk tot een synthese te komen.

Deze intelligente jongeman hield weinig rekening met de planning in ons huisgezin. Onze nicht en pleegdochter werd bruusk uit ons gezin weggegrist. Geen rekening werd gehouden met de speciaal in Badhoevedorp geplande vervangende woonruimte, noch met de overeengekomen verblijfsduur van Gusta aldaar tot oktober 1983.

Het zij hem - met moeite - vergeven.

Als we zien naar de zorgzaamheid en de attentie waarmee hij Gusta omringt, kunnen we daar vrede mee hebben.

Weliswaar is een stormachtige periode achter de rug en zijn veel obstakels geslecht, maar om werkelijk tot onze familie te gaan behoren zal er nog het een en ander moeten gebeuren. De tijd is nog te kort geweest voor veelvuldig en intensief contact. Niet alles wat tot de traditie van onze familie behoort is overgedragen.

Doch eens komt de dag.

Daar zullen beide kanten hun best voor doen, daarvan zijn we overtuigd.

Veel succes met je proefschrift en je toekomstige wetenschappelijke carrière.

Veel geluk met Gus. Het ga jullie wel!

Breukelen.

Pauli en Bob Van Dobbenburgh-Rossberg

Een proefschrift:

De manier, waarop het
onvermijdelijke zich
voltrekt, is door
inspanning.

A. en P. van Dobbenburgh.

Ach wee, ik ongelukzalige vrouw
Dat ik kennis en kunst niet heb,
Anders zou ik alles in 't werk stellen
Om U over de jongste Doctor Lenstra te vertellen.
Geen detail zou ik U onthouden,
Noch van zijn escapades met een steeds
 eindelozet getal,
Noch van die lang geleë in de Parijse Salle Garnier.
Mijn pen zou U dan schilderen onze struise Kavalier:
Aan zijn zijde géén Rosenstrauss,
Maar een microfoon in een wollen kous!
Zijn verzameling banden "serieuze" muziek
Werd op deze wijze gans uniek.
Overigens, niet alleen van Richard Strauss,
Ook van die andere Richard heeft hij veel in huis.
Daarvoor timmerde Arjen een levensgrote kast,
Die maar net in zijn fraaie kamer past.
Ik zou nog heel veel meer willen zeggen en wensen,
Doch wee, ik ongelukzalige vrouw
Dat ik kennis en kunst niet heb.

*Een zielige bijdrage, zéér vrij naar Felix Dahn,
zo voldoende duidelijk bepaald van wie.*

PHOTO QUIZ, OPGEDRAGEN AAN ARJEN K. LENSTRA, TER GELEGENHEID VAN ZIJN
BEVORDERING TOT GROOTWAARDIGHEID, door PETER VAN EMDE BOAS.

Beste Arjen. Het is een goede traditie dat het slachtoffer van een dag als deze door de overige erbij betrokkenen wordt overladen met geschenken en andere offeranden. Ik ben uiteraard bij mijzelf te rade gegaan welke van de mij tijdelijk toevertrouwde aardse goederen zich het beste tot dit doel zouden lenen, en na ampele overwegingen heb ik moeten besluiten dat in de gegeven situatie slechts een greep in mijn meest waardevolle bezit, te weten het archief van fotografische prentwerken, als gepast kan worden gezien. Nodeloos te vermelden dat gegeven de slechts chronologische toegankelijkheid van dit bestand, het vele avonden werk heeft gekost om de relevante negatieven te traceren en te doen bewerken.

Onze relatie is uiteraard ouder dan de samenwerking op Wetenschappelijk gebied. Arjen was tenslotte het jongste broertje van Andries, waarvoor op de Frans van Mierisstraat de verzamelde Apedariers zich stille dienden te houden. Arjen mocht ook op mijn huwelijksfeest handtekeningen verzamelen, toen in de eigen familie geen hobol in de geschikte leeftijdscategorie aanwezig bleek te zijn. Wellicht doet het je genoeg te weten dat dit huwelijk dan ook totop de huidige dag stand houdt, hetgeen tegenwoordig een zeldzaamheid schijnt te wezen.

Uit deze periode dateert dan ook de eerste opgave. Op prent 1 zult U ergens uw promotor kunnen herkennen, maar er is nog een object dat U wellicht vertrouwd voorkomt. Welk object wordt hier bedoeld ?

De overige prenten zijn allen van meer recente datum en zijn het resultaat van mijn wetenschappelijk functioneren, dat mij voortdurend door de wereld laat trekken. Bij deze gelegenheden komen diverse collega's in het archief terecht die inmiddels ook hun weg in Uw referenties hebben weten te vinden. Gaarne had ik U een volledige collectie willen aanbieden maar die kan ik U niet bezorgen aangezien ik lang niet iedereen heb gezien.

De opnamen 2, 3 en 4 dateren uit October 1979, en zijn gemaakt te Oberwolfach. Na deze week zal opgave 2 je geen probleem geven; persoon 3 is ongetwijfeld een aanhanger van je 7e stelling, en van de leeuwentemmerskwaliteiten van collega nr. 4 heb je zo vaak gebruik gemaakt dat ook deze opgave je geen problemen zal geven.

Komen we bij onze Italiaanse vriend op 5 , die geheel onschuldig zo'n substantiele bijdrage heeft gegeven tot het gebeuren van vandaag. Wie is echter de tweemaal gefotografeerde pijproker ?

Ter afwisseling een dame als 6e prent. We zaten in het volkswagenbusje van Hal Sudborough die ons vervoerde van Milwaukee naar Evanston. Deze tocht voerde dus niet naar de Puszta waar ik opname 7 vervaardigde. Zoals je ervaren hebt kan de aldaar geknipte collega alles beter, maar dat heb je inmiddels ontmaskerd als pure bluf.

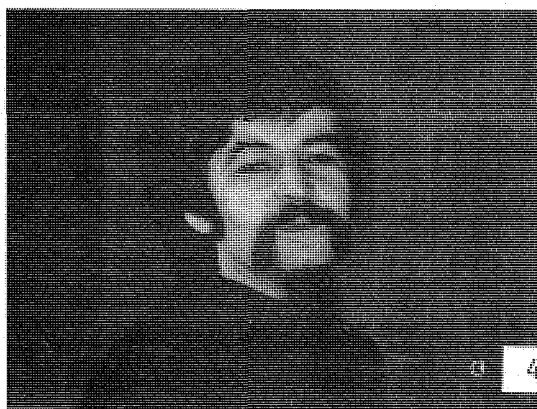
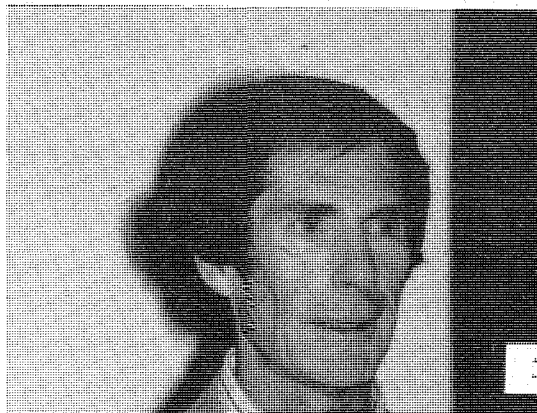
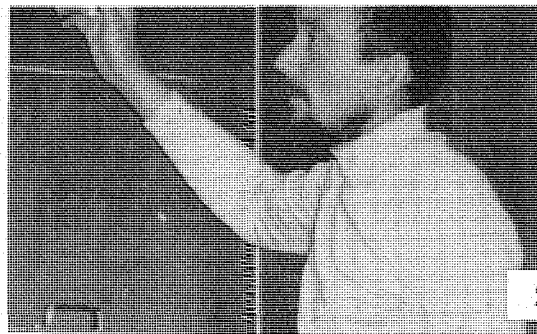
De oude heer op nr. 8 was geïnviteerd spreker bij het afscheid van van Wijngaarden, alwaar hij liet blijken te zijn bekeerd van zijn jeugdzonde uit het verleden die U zo volmondig het eeuwige leven toewenst. Wie o Wie?

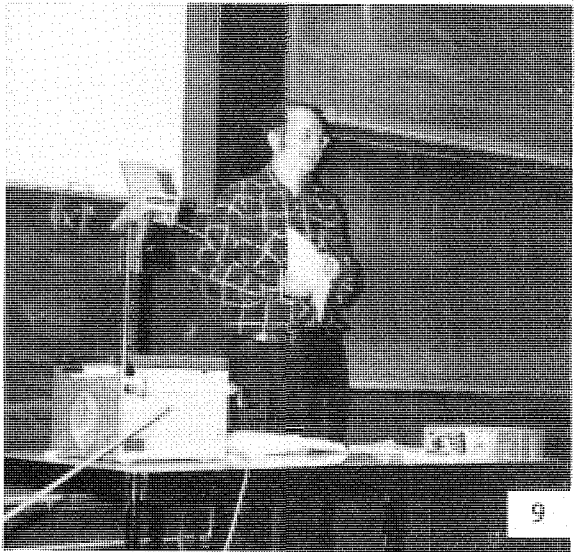
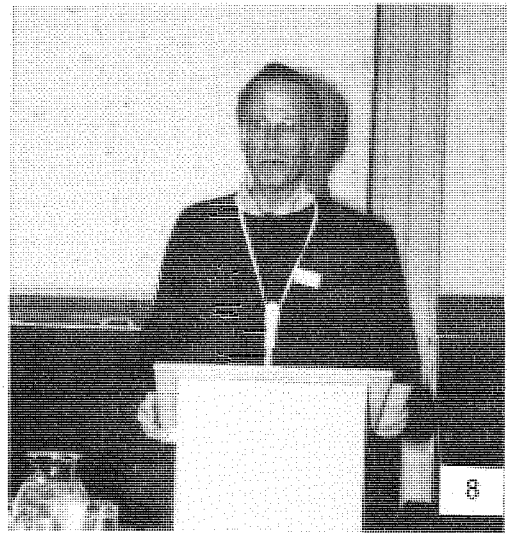
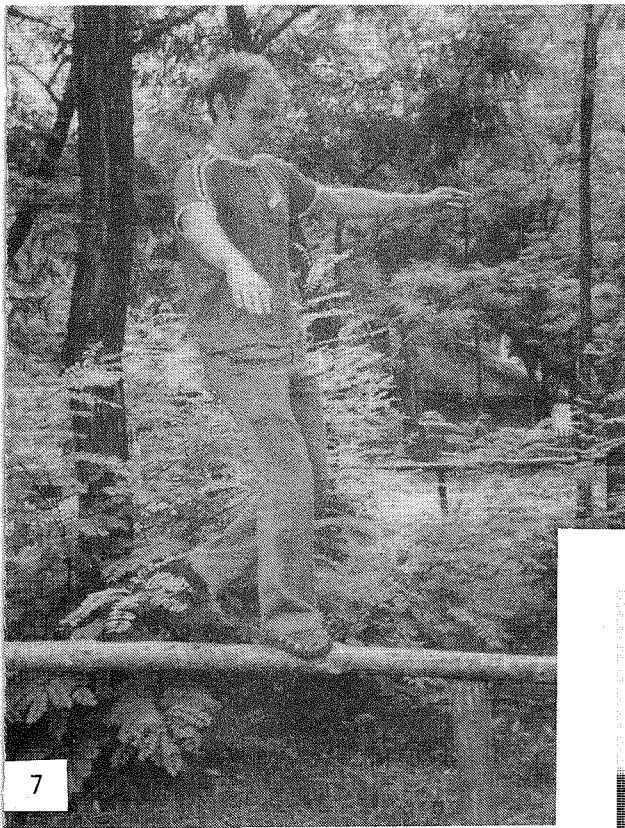
Nummer 9 mag in geen enkele Informatica publicatie als referentie ontbreken, dus hier ook niet. Met de op opname 10 afgebeelde collega hang je inmiddels op een aankondiging op mijn prikbord dus dat kan ook niet missen.

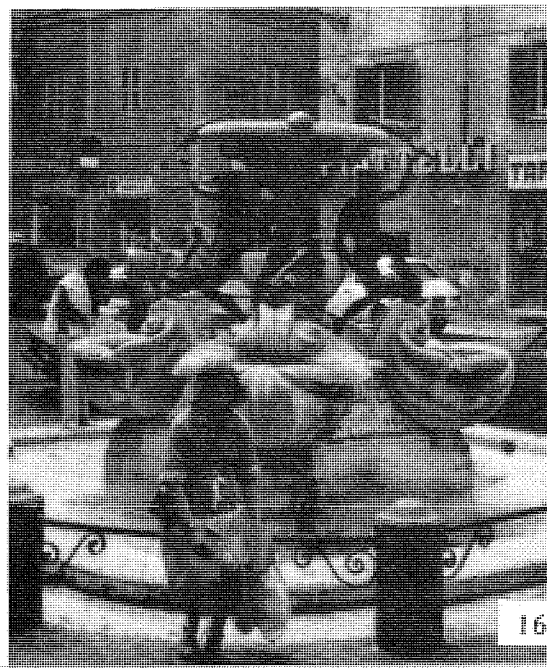
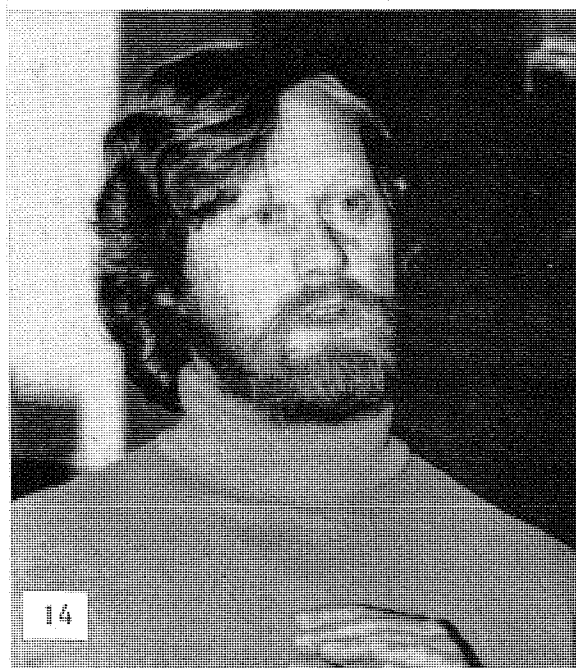
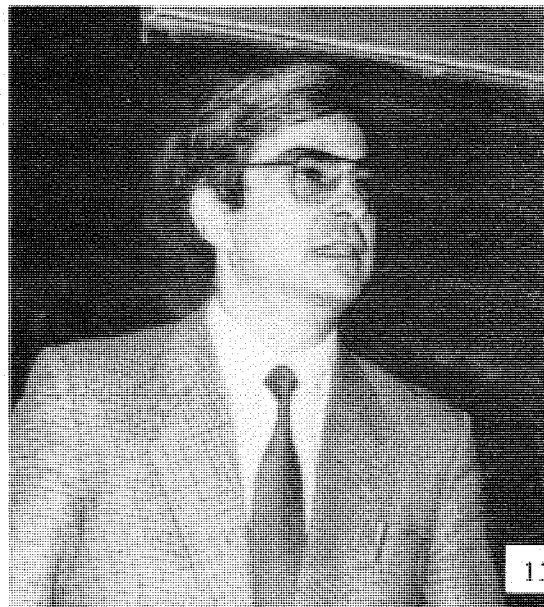
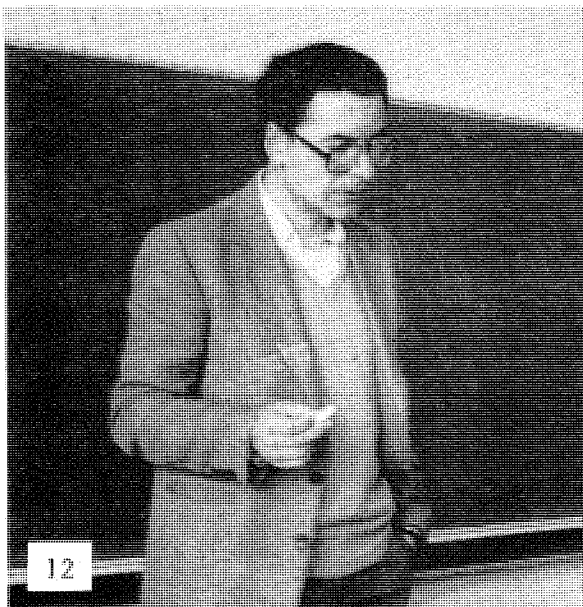
Komen wij bij het unieke en daarom historische groepsportret 11 : de afgebeelde personen zijn genoegzaam bekend en daarom vraag ik naar de identiteit van het bouwsel op de achtergrond. Een drietal schoten voor open doel tot slot (12, 13, en 14): collega's waarmee je samenwerkt of lieden die lastige doch niet steekhoudende vragen stellen.

Dan is er uiteraard de toekomst. Voor een deel heb je deze onder handbereik - zie prent 15 , waarbij ik slechts kan vragen naar de gelegenheid waarbij deze is vervaardigd. Anderzijds weet ik dat de wereld voor je open ligt, dus begin maar eens bij je komende bezoek aan Rome de afgebeelde fontein te traceren van prent 16 , en vergeet vooral niet om me er een briefkaart van te bezorgen, want die hoort weer thuis in een andere collectie van mij.

Arjen, ik twijfel er niet aan of je zult deze vragen allemaal correct beantwoorden, zoals je in het verleden al mijn vragen hebt beantwoord. Voor de arme drommels die dit bundeltje ook mogen ontvangen ben ik echter zo slecht de oplossingen elders te laten afdrukken. Niet spieken derhalve.







DE TOP DER NEDERLANDSE INFORMATICA

K. van Leeuwen
B.S. Mijlpaal
A.D.S. de Schuite

De informatica, zo leest men alom, dient *gestimuleerd* te worden. Zoiets vergt een *nota* en *overlegcircuits*, maar vooral *geld*. Dat laatste is onverwachts in ruime mate ter beschikking gesteld. Bij de verdeling ervan stuit de overheid op het probleem dat het wetenschappelijk *toptalent*, waaraan men de besteding het liefst zou toevertrouwen, uiterst dun gezaaid is - dat is tenslotte de voornaamste reden dat het geld er gekomen is.

Een *kritische evaluatie* van de Nederlandse informatici is daarmee voldoende gemotiveerd. Het zal geen verbazing wekken dat wij hier een taak voor ons zagen weggelegd. Eerder immer lichtte één van ons de Nederlandse *economen* door op wetenschappelijke productiviteit [1,2], en ook op het gebied van de *mathematische beslis-kunde* en *systeemtheorie* hebben wij onze sporen verdiend [3]. Het door de redactie van deze bundel gedane verzoek konden wij dan ook niet negeren.

Een jong vakgebied als de informatica vraagt uiteraard om een andere benadering dan de gevestigde disciplines die hierboven werden genoemd. De *dynamische ontwikkeling* die het vak doormaakt rechtvaardigt een bijzondere belangstelling voor publicaties in de vorm van *technische rapporten*, waarin de nieuwste resultaten worden vastgelegd voor verspreiding op een wijze die jaren vooruitloopt op de internationale tijdschriften. Het aantal publicaties in deze sfeer, zo postuleren wij, is maatgevend voor het wetenschappelijk prestige van de auteur - al zal daarbij aan enige nevenvoorwaarden moeten worden voldaan.

Beperken wij onze exercitie in eerste aanleg tot de *theoretische informatica*, dan verkeren wij in de gelukkige omstandigheid dat de benodigde informatie reeds geruime tijd verzameld wordt in het kader van de *Stichting In Oprichting Nederland* (SION). Bestudering van de nieuwsbrieven van de onder SION ressorterende *Werkgemeenschap Theoretische Informatica* leidt tot de in Tabel 1 weergegeven lijst. Hierin is aan de leden van de werkgemeenschap één punt toegekend voor ieder (co)auteurschap van een technisch rapport. Nulpunts-auteurs zijn piëteitshalve weggelaten.

Welke publicatienorm kan redelijkerwijs worden opgelegd om uit deze lijst de *informatica-elite* te selecteren? Al zijn er nog zo veel informatica-studenten, wij menen dat een rechtgeaard onderzoeker toch geen *semester* voorbij hoort te laten gaan zonder een wetenschappelijke gedachte aan het papier toe te vertrouwen en dat ook de *zomervakantie* niet compleet is wanneer geen nieuwe publicatie op de lijst kan worden bijgeschreven. Dit brengt ons op de *LMS-norm* van drie publicaties per jaar, d.w.z. twaalf in de beschouwde periode. Het stemt tot nadenken dat toepassing van deze bescheiden norm een ware slachting aanricht in Tabel 1. De dertien overlevenden staan in Tabel 2.

Bezien wij deze lijst wat nader, dan valt allereerst het onvoorstelbaar grote aantal publicaties van prof. Rozenberg op, een aantal dat zodanig *medische proporties* aanneemt dat wij tekort zouden schieten in onze kwaliteitsbevorderende taak indien sterke achterdocht jegens het wetenschappelijk niveau van deze publicaties het niet zou winnen van *mechanistisch getalfetisjisme*. Hangende nader onderzoek naar deze kwestie zijn wij genoodzaakt prof. Rozenberg te schrappen uit onze lijst.

In het resterende cijfermateriaal moeten nog drie correcties worden aangebracht. Jonge onderzoekers die slechts een deel van de beschouwde periode actief hebben kunnen zijn verdienen daarvoor compensatie. Deze overweging

TABEL 1. DE TOP-49

naam	score
Aalbersberg	1
Apt	9
Asveld	6
Bakker	10
Bergstra	78
Boas	13
Bra	6
Brock	1
Bruin	5
Chudáček	5
Collard	2
Dekker	4
Dhillon	3
Engelfriet	19
Fokkinga	6
Gaag	1
Gerth	7
Goeman	2
Groenewegen	10
Gyssens	3
Heer	4
Hoenkamp	2
Janssen	3
Janssens	22
Jonkers	4
Kleijn	16
Klop	19
Kuiper	2
Leeuwen	40
Lenstra	18
Lindenmayer	1
Meyer	16
Nijholt	4
Olivié	6
Ollongren	3
Overmars	24
Paredaens	8
Roever	18
Rozenberg	115
Schoone	2
Siero	1
Sommerhalder	1
Torenvliet	2
Verbeek	2
Vitányi	19
Waning	1
Westrhenen	3
Witteveen	2
Wijngaarden	1

beïnvloedt de score van drs. Lenstra, die in aanmerking komt voor een *multiplicatieve correctiefactor* van 2,2. Voorts zou het opgeroepen beeld van de hiërarchie binnen de informatica weinig realistisch zijn als wij voorbij zouden gaan aan het *Socratisch* karakter van de Nederlandse universitaire vorming. Bij dit leerproces is het een natuurgegeven dat de kennis van de leerling nooit meer kan zijn dan de kennis van de leermeester. In onze evaluatie vertaalt deze *volgorderrestrictie* zich in de eis dat, in het bijzonder, een promotor ten minste één punt meer moet hebben dan zijn of haar promovendi. Tenslotte hebben wij de score van dr. Bergstra gesplitst in die van dr. Bergstra (1) en dr. Bergstra (2).

Het doet ons genoegen, na inachtneming van deze nevenvoorwaarden, de *top-5* van de Nederlandse theoretische informatica te kunnen presenteren in Tabel 3. Onderaan vinden wij *ex aequo* de onderzoekers dr. Bergstra (1) en dr. Bergstra (2), op een gedeelde tweede plaats prof. Leeuwen en drs. Lenstra, en op een onbedreigde eerste plaats prof. Boas. Een gelukwens aan al dezen, in het bijzonder aan de lijstaanvoerder, is zeker op zijn plaats. Wij twijfelen er niet aan of de subsidiegever, die blijkens onze informatie worstelt met een overschot aan *geld* en een tekort aan *bestemmingen*, zal zijn weg naar de *top-5* wel weten te vinden.

TABEL 2. DE TOP-13

naam	score
Bergstra	78
Boas	13
Engelfriet	19
Janssens	22
Kleijn	16
Klop	19
Leeuwen	40
Lenstra	18
Meyer	16
Overmars	24
Roever	18
Rozenberg	115
Vitányi	19

Literatuur

1. *Economisch Statistische Berichten* (17 december 1980), 1414-1415.
2. *Intermediair* 18.20 (21 mei 1982), 11-13; 19.13 (1 april 1983), 13-15; 19.50 (16 december 1983), 13-17.
3. *Kwantitatieve Methoden* 11 (1983), 5-11; 12 (1983), 133.
4. *Nieuwsbrief van de Werkgemeenschap Theoretische Informatica* 1 (februari 1980); 2 (oktober 1980); 3 (april 1981); 4 (oktober 1981); 5 (april 1982); 6 (oktober 1982); 7 (april 1983); 8 (oktober 1983); 9 (april 1984).

TABEL 3. DE TOP-5

naam	score
1 Boas	41
2 Leeuwen	40
Lenstra	40
4 Bergstra (1)	39
Bergstra (2)	39

Counting is Easy*
An Essay at the Occasion of Arjen Lenstra's Doctorate
in the Mathematical and Physical Sciences

Paul M.B. Vitányi

Centrum voor Wiskunde en Informatica, Amsterdam†

SUMMARY

An exposition is presented of the recent result that many independent counts with simultaneous zero-check can be maintained in real-time on an oblivious single-head tape unit using the information-theoretical storage minimum. Some extensions of that result are also given. The treatment is informal and aims at making the central ideas more transparent.

1. Introduction

From the earliest times man has developed ever newer methods to count and denote numbers. People knew how to count long before they wrote numerals; simple arithmetic evolved slowly from the operation of counting. It may be observed that denotation for number tends to adapt to the use made thereof. The German student keeps his beer score by chalk marks on the table or nearby wall. In Roman times the familiar variant of this tally system of number representation was used. Increasing use of the arithmetic operations of addition, subtraction, multiplication and division, instead of the use of number representation as just memory aid subject to unit changes, forced the emergence of the more convenient positional notation in general use. This notwithstanding the fact that positional notation is logically considerably more complicated than the tally system. In recent times under the advent of electronic computing devices the use of all sorts of binary representations has flourished. The express purpose of such representations is to alleviate the difficulty of the task at hand. Now consider the task of counting. Tallying is admirably suited for counting, since the addition or subtraction of a unit is always performed by a unit change in the representation. Nonetheless, the already huge size of representation for quite moderate numbers makes the system unwieldy. The common positional system, on the other hand, suffers the drawback that for certain counts a change by a single unit causes more than one digit or even all digits of the representation to change. This means that we have to access unbounded information which takes unbounded time. In less common positional representations, such as Gray codes, only a single bit has to be changed to add or subtract a unit. Unfortunately, the position of this bit depends on the stored number and whether we add or subtract, forcing us to compute that position and therefore to access all of the stored number. Since in computers it is common and feasible to manipulate far larger numbers than without, the question has cropped up in the sixties whether we can combine the ease of tally update with the compactness of positional representation. An additional requirement of the looked-for representation is that the unit time for update should also suffice to check whether the number is zero or not. A device implementing these capabilities is called a *counter*. To make matters more difficult, and to get some insight in the computational complexity of several problems related to counting, the next question asks whether we can so maintain an arbitrary fixed number of such counts, that is, a *multicounter*, on a single-head tape unit [3]. Such a single head tape unit consists of a finite-state control with an input terminal and an output terminal and a single head storage tape. This device is known as a *one-tape on-line Turing machine*.

* This work was supported by the *Stichting Mathematisch Centrum*.

† Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098SJ Amsterdam, The Netherlands.

The result of an investigation [4] was that counting is *easy* in the sense of computational complexity: an arbitrary fixed number of independent counts can be maintained, under unit increments/decrements and simultaneous check for 0, by a real-time oblivious one-head tape unit in logarithmic space. *Oblivious* means that the input data do not influence the storage head movement, that is, the motion of the storage tape head is a function of time alone. The celebrated ARJEN LENSTRA has on several occasions been of the opinion that "the result cannot be true; were I an American university professor, I would tell a student to find the error". Bent on simplifying the solution, JOEL SEIFERAS [2], in a top-down development of the ideas, demonstrated one of the possible alternatives to the original bracketing to control the inherent recursion. This incarnation of the solution takes twice as many bits (4) per tag as the original tagging scheme in [4]. It is most satisfactory however that he improved the details of the radix notation used. Below we follow his appealing exposition and omit all proofs.

2. Counting made easy

We will maintain each counter as a logical sequence of symbols, similar to the familiar radix notation.

Theorem. *There is a data-independent (oblivious) maintenance schedule with the following properties:*

1. *There is a chance to propagate information such as "unit increments" and "unit decrements" at least once in every $O(1)$ steps to the logical 0th position.*
2. *There is a chance to propagate information as "carries" and "borrows" from position i to position $i+1$ at least once every $O(1)$ times there is a chance to propagate such information into position i , for all $i \geq 0$.*
3. *Maintenance of this schedule can be implemented on a single-tape Turing machine with bounded delay* and oblivious head motion.*

The counter contents are denoted in a *redundant symmetric* positional representation. The underlying radix notation used can be base 10, since the constants involved in the $O(1)$ upper bounds turn out to be small (about 3) compared to 10. The representation is symmetric since both positive and negative digits are used. A mark is maintained on the most significant nonzero digit (if any) and on the nonsignificant leading 0's. The representation is redundant since all nonzero integers have infinitely many representations this way, even without nonsignificant leading 0's. The rules for information propagation from position i to position $i+1$ are:

- "Carry" if the digit is greater than 5.
- "Borrow" if the digit is less than -5 .
- Do nothing if the digit is bounded by 5 in absolute value.

By induction, the properties of the maintenance schedule assure that no digit will have to exceed 9 in absolute value. As a consequence, the only digit that might change from zero to nonzero, or vice versa, is at position $i+1$ above, so that only the marks at positions i and $i+1$ might have to change; thus, the marks can be correctly maintained. As another consequence, the most significant nonzero digit (if any) will always correctly indicate the sign of the entire count, so that the count will be 0 if and only if the frequently observed digit at position 0 is a marked 0.

* A Turing machine has *bounded delay* if it performs no more than a fixed constant number of elementary steps in between polling successive input commands from the input terminal. In a *real-time* computation this fixed constant is 1. At the cost of adding states to the finite control and expanding the storage tape alphabet, of the Turing machine concerned, a constant delay computation can always be sped up to a real-time computation.

3. The maintenance schedule

For *random* access we can use the standard Thue sequence of visits, visiting 0 every other step, 1 every other remaining step, 2 every other now remaining step, etc.

0102010301020104010201030102010501020103010201040102...

Equivalently, bracket each visit to $i+1$ by review tours of positions $0, 1, \dots, i$. Thus,

```
tour(i+1):
    tour(i);
    visit i+1;
    tour(i)
```

and

```
tour(0):
    visit 0 .
```

We propagate the carries and borrows from i to $i+1$ on visit to i . Noting that appending 'visit $i+1$; tour(i)' onto the end of 'tour(i)' always gives 'tour($i+1$)' we see that 'tour(∞)' can be defined as the limit of 'tour(i)' for i goes to infinity.

```
tour( $\infty$ ):
    visit 0;
    visit 1; tour(0);
    visit 2; tour(1);
    visit 3; tour(2);
    visit 4; tour(3);
    ...
```

4. Turing machine implementation

The storage tape of our Turing machine shall be semi-infinite to the right. The initial leftmost square is called the start square. In the *instantaneous description* (momentary snapshot) of the tape of the Turing machine we mark the head position by a $>$ or a $<$. The start instantaneous description is

$>12\dots i(i+1)\dots$

Since the head must always be near the logical position 0 we can try:

$\{ >012\dots i(i+1)\dots \}$ tour(i) $\{ i\dots 210>(i+1)\dots \}$,

in preparation for a visit to $i+1$. However, now tour(i) will no longer complete the desired analogous preparation (that is, tour($i+1$)) for a visit to $i+2$. So we construct a revision:

```
tour(i+1):
    tour(i);
    visit i+1;
    tour(i) "transporting" i+1;
    tour(i) "to get back"
```

Denoting 'tour(i) "transporting" $i+1$ ' as 'tour(i)+' , we now obtain:

```

tour( $\infty$ ):
  visit 0;
  visit 1; tour(0)+; tour(0);
  visit 2; tour(1)+; tour(1);
  visit 3; tour(2)+; tour(2);
  ...

```

Roughly speaking therefore:

```

{ ... > 0 1 ... i (i+1) (i+2) ... }
tour(i) { ... i ... 2 1 0 > (i+1) (i+2) ... } visit i+1;
tour(i) "transporting" i+1 { ... (i+1) < 0 1 2 ... i (i+2) ... }
tour(i) "to get back" { ... (i+1) i ... 2 1 0 > (i+2) ... } visit i+2;

```

shows the effect of 'tour($i+1$); visit $i+2$ '.

Remaining worries:

- (1) How to do the "transport"?
- (2) How to keep track of the recursion without a stack?
- (3) When get and recognize the chance to propagate information between logical positions i and $i+1$?

To transport a symbol through a tour we have a second version of each symbol which gets pushed back whenever it gets in the way. Because the second version of $(i+1)$ will be transported, consecutively (but not contiguously) in time, across the sequence $0, 1, 2, \dots, i$ of the original variety, a simple pushback like

$$>_a \text{2nd version } b \text{1st version} \Rightarrow >_b \text{1st version } a \text{2nd version}$$

will always suffice. The recursive formulation is as follows.

```

tour(i+1) "transporting" j2nd version;
  tour(i) "transporting" j2nd version;
  push j2nd version back past (i+1)1st version;
  visit i+1;
  tour(i) "transporting" (i+1)2nd version;
  tour(i) "empty-handed"

```

We have to keep track of the recursion, and to know when to turn. So along with each symbol we maintain the current physical direction (left or right) to its logical successor. Assuming this is done correctly, it is clear when the last pushback of $(i+1)$ occurs, and the symbol can be so marked (the third version). This gives:

$$>_d l_1^{2nd \text{ version}} l_2^{1st \text{ version}} \Rightarrow >_r r_2^{1st \text{ version}} d_1^{3rd \text{ version}},$$

suppressing all but each symbols direction indication (l for 'left' and r for 'right' or d for either). Since only the logically first symbol is not transported nontrivially after it is visited, we maintain a special mark thereon (the fourth version). Again suppressing all but the head representation and direction and each symbol's direction indication of, respectively, "left successor" and "right successor" in the notation: (1) first version $\leftarrow$ and $\rightarrow$; (2) second version

$\in$ and $\ni$; (3) third version $\Leftarrow$ and $\Rightarrow$; (4) fourth version $\Leftrightarrow$ and $\Leftrightarrow$; we finally arrive at the following simple rules for the single-tape Turing machine:

$\triangleright \leftharpoonup$	$\Rightarrow$	$\leftharpoonup \triangleright$	$\triangleright \leftharpoonup$	$\Rightarrow$	$\leftharpoonup \triangleright$	[visit first symbol]
$\triangleright \leftarrow$	$\Rightarrow$	$\in \leftarrow$	$\triangleright \rightarrow$	$\Rightarrow$	$\exists \leftarrow$	[visit and begin transport]
$\triangleright \in_1 \rightarrow_2$	$\Rightarrow$	$\triangleright \rightarrow_2 \in_1$	$\triangleright \exists_1 \rightarrow_2$	$\Rightarrow$	$\triangleright \rightarrow_2 \exists_1$	[pushback]
$\triangleright \in_1 \leftharpoonup_2$	$\Rightarrow$	$\triangleright \leftharpoonup_2 \in_1$	$\triangleright \exists_1 \leftharpoonup_2$	$\Rightarrow$	$\triangleright \leftharpoonup_2 \exists_1$	[pushback past first symbol]
$\triangleright \in_1 \leftarrow_2$	$\Rightarrow$	$\triangleright \rightarrow_2 \leftarrow_1$	$\triangleright \exists_1 \leftarrow_2$	$\Rightarrow$	$\triangleright \rightarrow_2 \exists_1$	[last pushback]
$\triangleright \in_1 \leftharpoonup_2$	$\Rightarrow$	$\triangleright \leftharpoonup_2 \leftarrow_1$	$\triangleright \exists_1 \leftharpoonup_2$	$\Rightarrow$	$\triangleright \leftharpoonup_2 \exists_1$	[first and last pushback]
$\triangleright \leftharpoonup$	$\Rightarrow$	$\leftarrow \leftarrow$	$\triangleright \Rightarrow$	$\Rightarrow$	$\leftarrow \rightarrow$	[begin tour back]

and the symmetrical rules:

$\bar{t} \wedge$	$\Rightarrow$	$\wedge \bar{t}$	$\Rightarrow$	$\wedge \bar{t}$	[visit first symbol]
$\uparrow \wedge$	$\Rightarrow$	$\vee \in$	$\Rightarrow$	$\vee \in$	[visit and begin transport]
$\bar{t}_2 \sqsubset_1 \wedge$	$\Rightarrow$	$\sqsubset_1 \bar{t}_2 \wedge$	$\Rightarrow$	$\sqsubset_1 \bar{t}_2 \wedge$	[pushback]
$\bar{t}_2 \sqsubset_1 \wedge$	$\Rightarrow$	$\sqsubset_1 \bar{t}_2 \wedge$	$\Rightarrow$	$\sqsubset_1 \bar{t}_2 \wedge$	[pushback past first symbol]
$\bar{t}_2 \sqsubset_1 \wedge$	$\Rightarrow$	$\bar{t}_1 \bar{t}_2 \wedge$	$\Rightarrow$	$\bar{t}_1 \bar{t}_2 \wedge$	[last pushback]
$\bar{t}_2 \sqsubset_1 \wedge$	$\Rightarrow$	$\bar{t}_1 \bar{t}_2 \wedge$	$\Rightarrow$	$\bar{t}_1 \bar{t}_2 \wedge$	[first and last pushback]
$\bar{t} \wedge$	$\Rightarrow$	$\bar{t} \wedge$	$\Rightarrow$	$\bar{t} \wedge$	[begin tour back]

At this point it may be instructive to go through part of the simulation, with the logical position numbers but noting that only the successor directions are actually available. As example we display in the Table below an initial segment of the sequence of instantaneous descriptions suppressing all but the head representation and direction and each symbol's direction indication and version. This sequence was computer generated literally using the preceding rules.

[illegible]

Table. The first 81 instantaneous descriptions.

Finally, we must indicate when the information should be propagated, such as carries or

borrows. The rules above maintain the additional information that the symbols to the right or left of the head, not being transported, are in increasing logical order away from the head. So if $> \rightarrow_1 \rightarrow_2$ (or $> \rightarrow_1 \leftarrow_2$, $\leftarrow_2 \leftarrow_1 <$, $\rightarrow_2 \leftarrow_1 <$, $< \rightarrow_1 \rightarrow_2$, and so on) occurs, the symbols being confronted must be the i th and $(i+1)$ st for some i , and the information can be safely propagated. Moreover, the i th and $(i+1)$ st symbols do get confronted this way in every empty-handed tour $(i+1)$, at the end of the prefix empty-handed tour $(i-1)$. Since tour (∞) is a sequence of instances of tour $(i+1)$, every third one of which is empty-handed, interspersed with visits to positions higher than $i+1$ (in the Thue sequence manner), the number of chances to propagate the information into position i without such a confrontation of positions i and $i+1$ is bounded by three times the number of visits to position $i-1$ in tour $(i+1)$, or $3 \times 9 = O(1)$. (Some lookahead for chances to propagate information from position i or a more careful analysis could reduce the number of intervening chances to the promised 3; but we could also simply work in base 56 to get by with the bound 27.)

Multicounter machines. It is not difficult to see that the above Turing machine implementation can be used to maintain any fixed number k of counters. One simply divides each position into k subpositions, one for each count. Since the maintenance schedule is oblivious, the single storage tape head can do the same job to each individual count track subposition as it formerly did to the original single count track position.

Storage complexity. Analysis of the head movement learns that in *each* interval of n steps the head position covers a tape segment of size $\Theta(\log n)$, for *all* $n > 1$. This irrespective of the counter contents. PETER GACS [1] has noticed that the used space can be kept to at most proportional to the logarithm of the largest counter contents. It is obvious that we have to forfeit oblivious operation then. The idea is to *skip* the visit to $i+1$ in tour $(i+1)$ if $i+1$ lies in entirely virgin territory:

```

tour (i+1):
  tour i;
  if necessary then
    begin
      visit i+1;
      tour (i) "transporting" (i+1)2nd version
    end
  end
tour (i)

```

Just one more rule is needed: $> a \Rightarrow < a$ if every counter's track on the symbol a contains a "virgin" marked 0.

Uniform Logspace. Finite Automata have the up till now unique property that any finite collection of them can be replaced by a single one. Thus the regular sets are closed under union and intersection. Since a deterministic device can be modified to accept the complement of the originally accepted set, the regular sets form a Boolean Algebra. In [6] it is noticed that this property also holds for multitape Turing machines of which the heads stay on $O(\log n)$ bounded tape segments for *each* interval of n steps, for *all* $n > 1$. We called such machines *uniform* $O(\log n)$ storage bounded. As noted above, the tagging scheme has the machine access a $\Theta(\log n)$ -length tape segment in each interval of n steps, for all $n > 1$. It can be demonstrated that each uniform $O(\log n)$ storage bounded multitape Turing machine can be real-time simulated by this uniform $\Theta(\log n)$ storage bounded oblivious one-head tape unit. Therefore, in simultaneous real-time and UNIFORM LOGSPACE the amount of heads, tapes, the option of head-to-head jumps, the oblivious restriction, and so on, do not change the computational power.

Augmented Counter Machines. If we can, in a collection of k counters, also replace each counter contents by that of any other counter in the collection in a single step then we have an *Augmented Counter Machine* or ACM. We can formalize such a machine as a multicounter machine with the added instruction of *semipermutation* of the momentary counter contents. A semipermutation is a permutation with repetitions, that is, any total function of a finite set of elements into itself is a semipermutation. The set of semipermutations of k elements forms a semigroup (not group) and has k^k elements. In [5] it is observed that the exhibited mechanism suffices for one-tape real-time oblivious simulation of ACM's. All we need to do is enter a semipermutation in the 0th position, and transport it from a position i to $i+1$ before other information. The semipermutation is like a switch which switches the contents of the logical position it passes; two semipermutations overtaking each other are replaced by the corresponding semipermutation from the semigroup.

REFERENCES

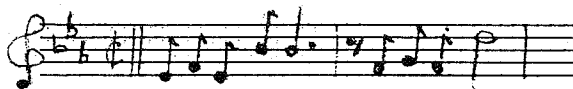
- [1] P. Gacs, as communicated in [2].
- [2] J. Seiferas, Letter of July 13, 1983.
- [3] P.C. Fischer, A.R. Meyer and A.L. Rosenberg, Counter machines and counter languages, *Mathematical Systems Theory* 2 (1968) 265 - 283.
- [4] P.M.B. Vitányi, An optimal simulation of counter machines, *SIAM Journal on Computing*, 1984.
- [5] P.M.B. Vitányi, An optimal simulation of counter machines: the ACM case, *SIAM Journal on Computing*, 1984.
- [6] P.M.B. Vitányi, On the simulation of many storage heads by one, Special issue on ICALP '83, *Theoretical Computer Science*, to appear.

Ontbinding van veeltermen per proefschrift

Motto: Als het maar priem is.

Stellingen: dit leidt tot de volgende adagia:

1. "dat onze beschaafde maatschappij haar ontbinding tegemoet snelt wanneer wij niet beter op de priemen letten"
(vrij naar de N.Gids 1890).
2. Steeds een goed alternatief is het ontbinden met kracht- termen, geschikt voor de diegenen die niet in de termen vallen.
3. Het echte proefgedoe geschiedt bij Dikker en Thijs voor wie er wel in valt.
4. Orobranche minor is priem.
5. Els is priem.
6. Gebed is priem
7. Maar de landloper is priemer.
8. De fuga's en tocata's van Bach, evenals de oudste psalmen zijn te herleiden tot priemgetallen.
9. 19201518201617201716201815201914210141320132013122020124201110
20722217322742375247625772678277928611062926342649465956694679267
92698118821783188416937173826471637364881917151311975311242627282
9313233323435361234567891 is een beetje priem.
10. Het licht van de zon naar Betelgeuze ziet het licht van Betelgeuze richting zon voorbij komen met een snelheid groter dan het licht!



On the Foundations of Computer Science

Part I: What is a Bit?¹

Samuel S. Wagstaff, Jr.²

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

To my friend
Arjen K. Lenstra
at the defense of his doctoral thesis

Computer Science has grown so swiftly in recent years that many students are defending their doctoral theses in computer science before they have learned more than a tiny fraction of the field. Indeed, many such students have only rudimentary knowledge of the most fundamental principles of computer science. This is the first in a series of lectures whose purpose is to remedy this situation by explaining these principles in a clear and complete fashion.

We begin our study of the Foundations of Computer Science with the bedrock upon which these Foundations stand. Of course, this is the data which computers devour and regurgitate. The unit of data is the "binary digit" or "bit", as it is familiarly known. I am surprised by the number of young computer scientists who do not really understand what a bit is.

Every healthy computer has millions of tiny little bits running around inside it all the time. Although they are essential for the proper operation of the computer, it is difficult to see them because they are so small, quick, and elusive. They must be trapped before they can be observed. The most usual trap is a device called an "oscilloscope". It looks like a computer terminal, but has no keyboard, a small screen, and lots of knobs. The way you catch a bit is this: Connect two wires from the oscilloscope to some place inside your computer where you think some interesting bits might be lurking. Turn the knobs until you see something on the little screen. Then you have trapped a bit. It will probably look something like this:



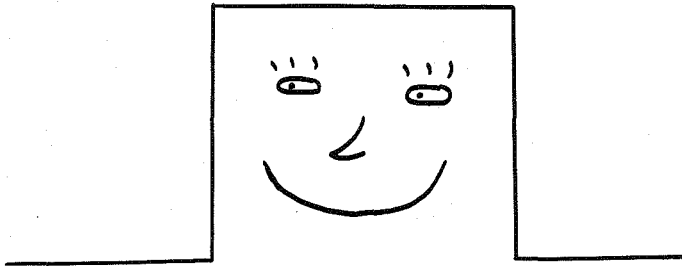
1. This paper was inspired by a delightful lecture given by Dr. John A. Gordon at CRYPTO '83 in Santa Barbara, California on August 23, 1983. Most of the "bits" presented here are his inventions.

2. This research was supported by a grant from the National Science Foundation of the United States of America.

Sometimes you capture a whole bunch of bits at once:



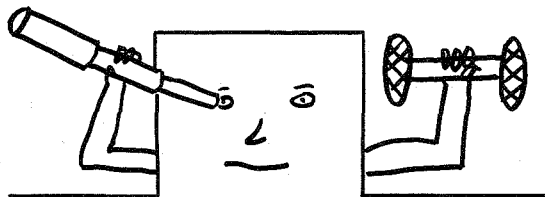
During many years of studying bits, I have observed that, like snowflakes, each one has its own special character. For example, this one is a **happy bit**:



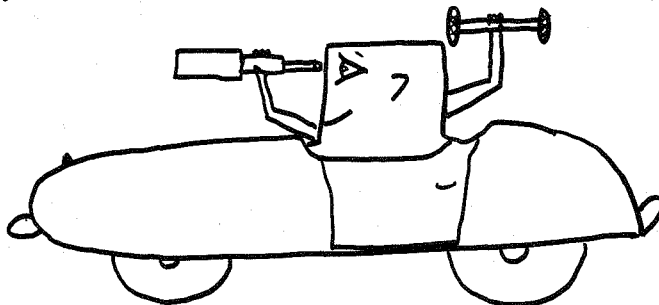
In numerical computations, one has to move big, heavy numbers around from one place in the computer to another place. This labor is accomplished by **carry bits**:



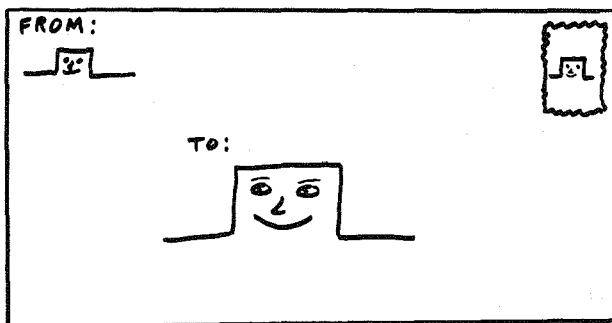
Some computers use **look-ahead carry bits**, which look out where they are going:



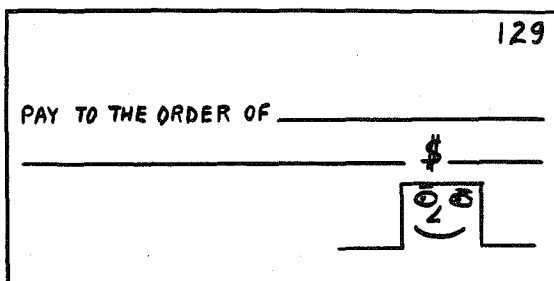
Supercomputers have a special breed of speedy look-ahead carry bits called **fast look-ahead carry bits**:



The next figure shows two address bits. The one in the upper left corner is a return address bit.



The next bit is a valuable one known as a check bit.



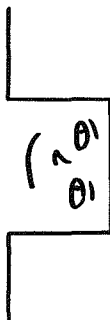
Here we see a little bit:



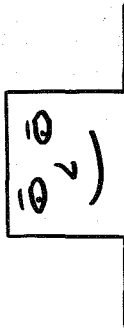
And here is a little bit more:



The next bit is a bit on the side, which is a bit of British terminology,



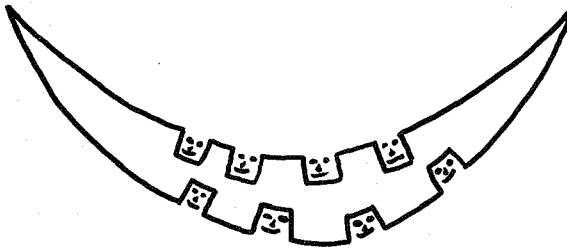
whilst this is a bit on the other side:



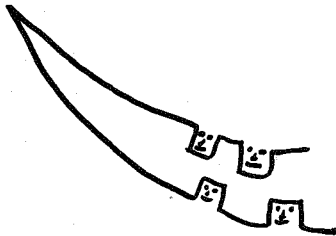
Here is what an **inverted bit** looks like:



Sometimes a certain number of bits together is given a special name. For example, eight bits are called a **byte**:



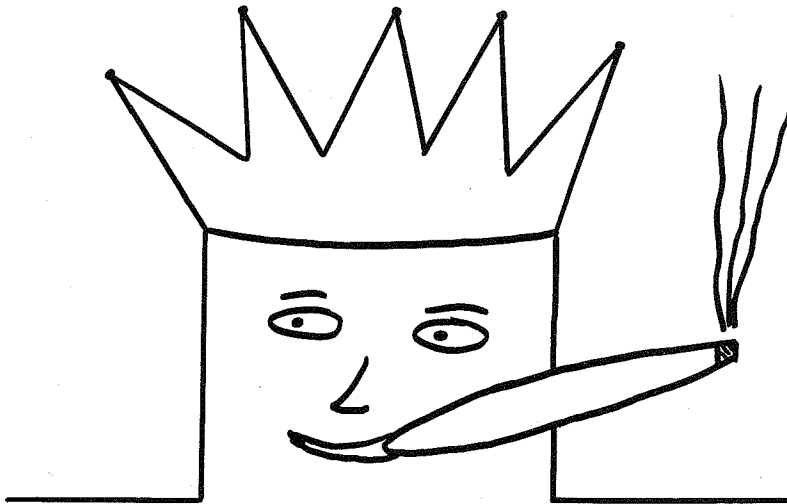
Four bits are called a **nibble**:



The Americans have given a special meaning to **two bits**:

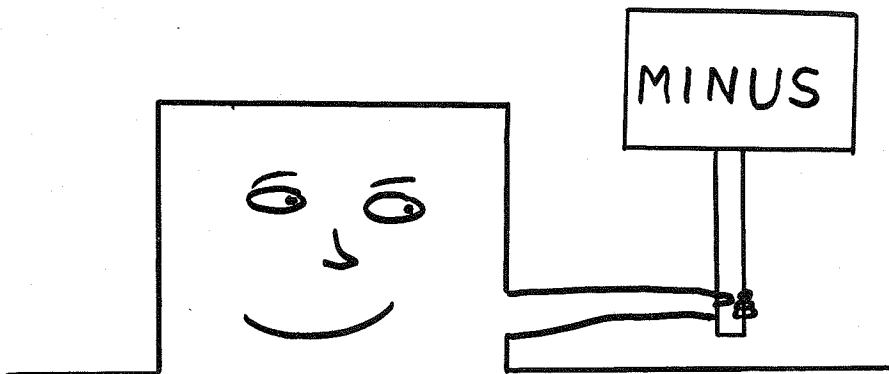


The regal bit which follows is called a **most significant bit**:

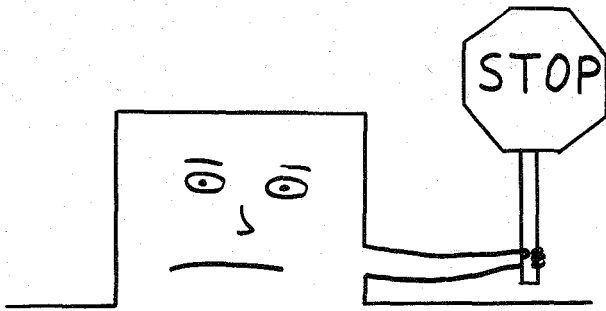


I was going to show you a **least significant bit**, but then I thought, "Why bother?"

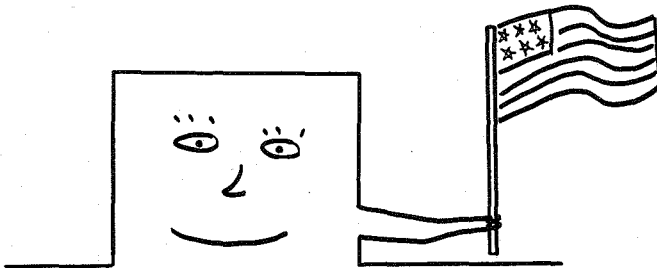
An important class of bits is the class of **sign bits**. Here is a typical example:



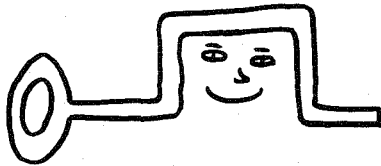
Another sign bit is the **stop bit**:



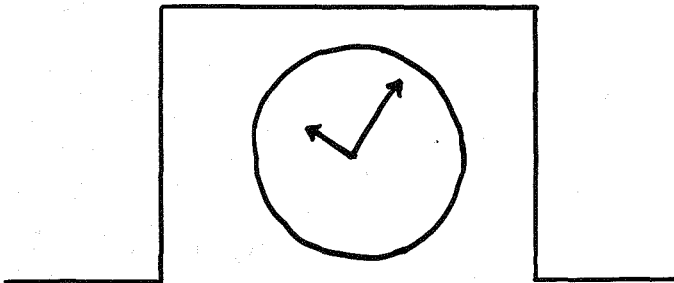
Still another one is the **flag bit**. The particular flag bit shown below is an American flag bit, but they come in all nationalities, of course.



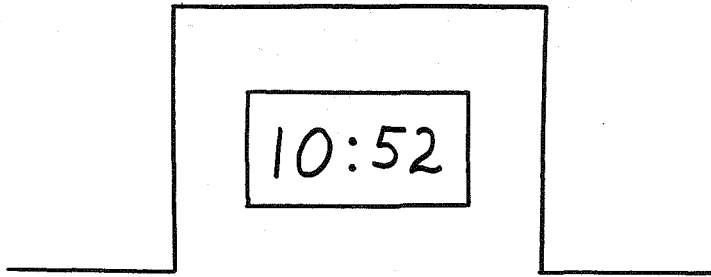
Our next bit is a **key bit**:



Computers can tell what time it is by looking at their **clock bits**:

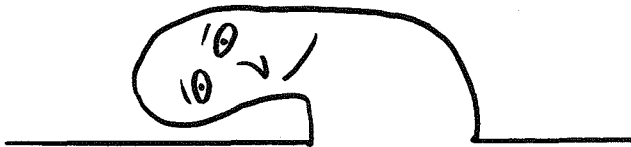


The latest fad in clock bits is the **digital clock bit**:



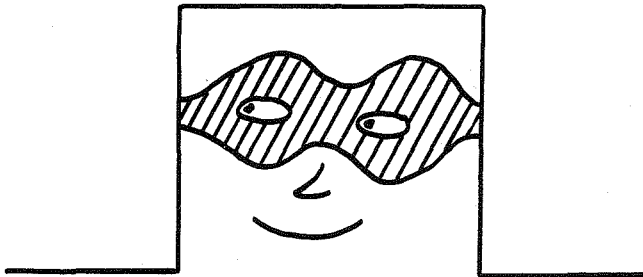
They are used mostly in digital computers.

Graduate students in Computer Science frequently identify the following bit incorrectly.

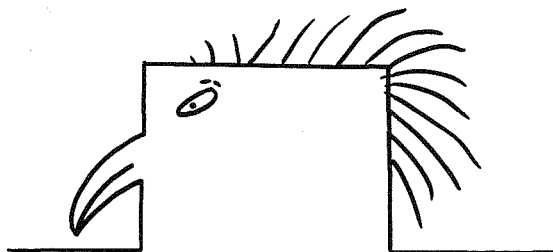


It is an **overflow bit**.

A bit which is often involved in logical operations and computer crime is the **mask bit**:



We conclude today's lecture with another hard-to-identify bit:



It is a **parrot bit**.

We hope you did not think this lecture was a bit too much.

About the author: Samuel S. Wagstaff, Jr. received his B.S. from M.I.T. in 1966 and his Ph.D. from Cornell University in 1970. He now teaches at Purdue University. He is one of the world authorities on bits.

Calculating with Real Numbers

P.J. Weinberger

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

The trouble with computers, as every mathematician knows, is that they are finite state machines. (Computers could make the same complaint about mathematicians.) Computers are fine on small integers, and can be taught about integers of arbitrary size, as long as 'arbitrary' is arbitrarily kept less than about 2^{2^3} . It is on that glory of classical mathematics, the real numbers, that computers fail. What the electrical engineers and computer architects have given us is something called floating-point arithmetic, into which years of effort have gone in a moderately successful effort to make it understandable. Now I can hear you saying, "That's the usual story, blame it on the machine. It is always the programmer's fault," and it is. Programmers managed the fairly-big-integers and the fairly-precise-floating-point a while back, but where are the reals, and why aren't they the same as these big floating point numbers?

What can we expect from the machine? If we think of a real number as a sequence of approximating rationals, then the computer can calculate with the rationals, at least until it runs out of memory or the user out of time. It's clear that equality is not going to be a decidable predicate in any plausible formalization of computing reals. Still, it is possible to do a kind of constructive analysis in which several of the theorems of elementary analysis remain true. From a somewhat more practical point of view it would be nice to do rather better than the following dialogue. Turing asks, "What is the square root of two?" The computer answers, "1.414." Turing asks for more accuracy and the computer responds, "1.414213." Turing asks for more accuracy and the computer responds, "1.4142130000." Turing announces that the computer is a decimal computer and its programmer has failed the Turing test.

My goal is to present a collection of programs that views a constructible real number as a rational approximation together with a function for getting a more precise approximation. The idea is recursive: the new approximation comes with a function which gives an even better approximation. The goal is too ambitious for this note, but I can present some ideas and a few examples. For instance, here is a more desirable conversation

Turing says:	Computer responds:
x = sqrt 2	1.4
x = precision(4, x)	1.4142
x = precision(7, x)	1.4142135
x = precision(25, x)	1.4142135623730950488016887
you are a computer	syntax error near line 5

The point is that after the first line, the number somehow knows about itself, and knows how to make itself more accurate.

After the interesting issues are decided, like how to represent the approximate values, and the like, all that remains is an exercise in functional programming.

The computer is going to implement a domain **Real**, which is a solution to the recursive domain equation

$$\mathbf{Real} = \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times (\mathbf{Z} \rightarrow \mathbf{Real})$$

Such an object exists in a suitable cartesian closed category. In such a quadruple (n, d, p, f) the

approximation is $n/10^d$, while p measures the precision, and the argument of f is the desired precision for the more precise approximation. There are two choices for precision, relative and absolute. Relative precision gives something like floating point, and causes a lot of problems with multiplication, when one of the factors is difficult to distinguish from zero. So the meaning of the **Real** is that its value is known to lie in the interval

$$\left[\frac{n}{10^d} - \frac{1}{10^p}, \frac{n}{10^d} + \frac{1}{10^p} \right]$$

The pervasive use of decimal instead of using arbitrary rationals keeps intermediate expressions from becoming very long (and makes output convenient). Usually $p > 0$, the special value $p = 0$ being reserved to indicate an integer, whose value is known exactly. It would be cleaner to use ∞ , in which case the domain would be defined by

$$\mathbf{Real} = \mathbf{Z} \times \mathbf{Z} \times (\mathbf{Z} + \{\infty\}) \times ((\mathbf{Z} + \{\infty\}) \rightarrow \mathbf{Real}).$$

Here is how it works. The **Real** associated with an integer n should just be $(n, 0, \infty, f_n)$, which is to say that all approximations have numerator n and denominator 1. The function f_n always returns this same real. Here is how the conversion routine would be defined in ML, the language of the implementation.

```
val realofint(n) =
  f(0)
  where val rec f(x) =
    real(n, 0, ∞, f)
  end
```

(This declaration says that the value of the function *realofint* is $f(0)$ where f is recursively defined so that every invocation returns the same thing that the function *realofint* returns.

Unary minus may be defined by

$$-(n, d, p, f) = (-n, d, p, g)$$

where g is defined from f by $g(x) = (-u, v, w, F)$ where $f(x) = (u, v, w, F)$. These are the easiest cases; for an exercise the reader might like to do division.

Note that it is possible to define a not-equals predicate, but the program to compute it need not terminate. Thus the machine can show that $7(1/7) - 1$ (where all are **Real**) is zero to any desired precision, but it cannot prove that it is zero, for the information that $1/7$ is rational has not been kept.

Exercises

What is it good for?

Implement the four rational operations. Did you use FORTRAN?

Compute $1/(1/7)$ to a precision of 1000. How often are f 's evaluated?

Would Turing have known if one of the last digits in the table had been wrong?

Write a computer program that might pass the Turing test. (Hint: denk je in de eigenaar te zijn, die alleen Nederlands spreekt, van een kleine coffee shop in een verlopen deel van Amsterdam. Wat zijn alle mogelijke gesprekken?)

OPLOSSING van CRYPTOGRAM

O P E R A
 N T
 N O Z Z E P O R G Y M P
 R L A A I D A
 M L U L U L M M
 B A L L O J B E L L I N I
 R A O N
 E L V I R A W I S K U N D E A
 U T A O G
 C T F I G A R O R F I
 B I Z E T N S E V I L L A
 A N E C D D
 A R I A D N E E A
 M A N O N R L A L O
 E N M S I
 T O S C A S E N T A O
 N

OPLOSSING PHOTO QUIZ

- 1 19711204 : Peter van Emde Boas als Piet; het klaaspak is familiebezit van de Lenstra's
- 2 19791024 : Arnold Schönhage, Oberwolfach
- 3 19791026 : G.E. Collins, Oberwolfach
- 4 19791026 : M. Mignotte, Oberwolfach
- 5 19800605 : A. Marchetti, Rome; op de afgebeelde photo staat President Pertini
- 6 19810513 : Susan Landau
- 7 19810827 : D. Yu. Grigoryev, FCT'81 excursie, Szeged
- 8 19811029 : J. Backus, van Wijngaardensymposium, Math. Centrum
- 9 19811106 : D.E. Knuth, Oberwolfach
- 10 19811103 : Bruno Buchberger, Oberwolfach
- 11 19820225 : L³ voor het Ernst Moritz Arndt Haus te Bonn.
- 12 19820421 : Henri Cohen, Algemeen Wiskunde Colloquium, UVA
- 13 19831102 : R. Loos, Oberwolfach
- 14 19831102 : Joachim von zur Gathen, Oberwolfach
- 15 19840328 : publiek doctoraal examen Gijs Tuynman
- 16 19800604 : Ghica voor de Fontane dala Tartarughe, Rome