CWI Syllabi

Managing Editors

J.W. de Bakker (CWI, Amsterdam)
M. Hazewinkel (CWI, Amsterdam)
J.K. Lenstra (CWI, Amsterdam)

Editorial Board

W. Albers (Maastricht)
P.C. Baayen (Amsterdam)
R.J. Boute (Nijmegen)
E.M. de Jager (Amsterdam)
M.A. Kaashoek (Amsterdam)
M.S. Keane (Delft)
J.P.C. Kleijnen (Tilburg)
H. Kwakernaak (Enschede)
J. van Leeuwen (Utrecht)
P.W.H. Lemmens (Utrecht)
M. van der Put (Groningen)
M. Rem (Eindhoven)
A.H.G. Rinnooy Kan (Rotterdam)
M.N. Spijker (Leiden)

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

The CWI is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

CWI Syllabus 11

Discrete wiskunde: tellen, grafen, spelen en codes

P.W.H. Lemmens

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

ISBN 90 6196 307 9

Copyright © 1986, Mathematisch Centrum, Amsterdam
Printed in the Netherlands

Voorwoord

In de loop der jaren is er via de vacantiecursussen van het CWI (voorheen MC) en ook uit andere bronnen heel wat materiaal ter beschikking geweest over nieuwe ontwikkelingen in de wiskunde, nieuwe deelgebieden of klassiek materiaal opnieuw bekeken van een overwegend inleidend karakter. Veel hiervan, inclusief de oudere vacantiecursussen, is moeilijk bereikbaar en soms zelfs alleen nog in archieven of een enkele bibliotheek te vinden. Aan de andere kant is er regelmatig vraag naar zulk materiaal, b.v. van de kant van leraren en wetenschappers uit nabuurgebieden van de wiskunde.

Het CWI heeft nu enerzijds het initiatief genomen de vacantiecursussen vanaf 1984 op te nemen in de CWI-syllabus serie en anderzijds in dezelfde serie bundels geselecteerde, samenhangende bijdragen uit oudere cursussen en ander materiaal uit te geven.

In deze publikatie treft U een herdruk (waar mogelijk gecorrigeerd) aan van een aantal voordrachten over discrete wiskunde en grafentheorie uit de serie vacantiecursussen in de periode 1963-1980. Zij belichten interessante aspecten van de theorie en haar toepassingen zonder volledigheid na te streven. Vaak zijn referenties aangegeven voor een diepgaande studie.

Om het karakter van de oorspronkelijke voordrachten te behouden, is geen poging gedaan de teksten te integreren. Wel zijn zeer incidentele, volledige overlappingen vermeden.

Helaas zijn de docenten S.C. van Veen en J.C. Boland overleden; hun bijdragen zijn nagenoeg ongewijzigd gereproduceerd. Aan de overige docenten gaat de dank van de samensteller uit voor hun toestemming tot herpublikatie en voor hun bereidheid de nodige correcties en aanvullingen te verzorgen. Voor zijn nimmer aflatende steun en advies is hier ook zeker een woord van dank op zijn plaats aan prof. dr. F. van der Blij. Het typewerk is verzorgd door de dames W. van Nieuwamerongen en E. Goeree (Mathematisch Instituut RU Utrecht), waarvoor dank.

P.W.H. LEMMENS

Inleiding in de discrete wiskunde (1975) 1
H.J.A. Duparc

Het tellen van vroeger tot nu (1980) 13
H.J.A. Duparc

Teltechnieken (1980) 25
F. Göbel

Woorden tellen (1980) 39
H.C.A. van Tilborg

De stelling van Polya (1980) 47
N.G. de Bruijn

Theorie der grafen (1963) 61
J.C. Boland

Wat zijn grafen (1972) 69
G. Laman

Spelen op een graaf (1975) 83
N.G. de Bruijn

Reizen op een graaf (1975) 95
J.K. Lenstra en A.H.G. Rinnooy Kan

Speltheorie (1975) 111
S.H. Tijs

Discrete wiskunde in de Shannon theorie (1975) 125
J.P.M. Schalkwijk

Het vierkleurenprobleem (1963) 137
J.M. Aarts

De roosterpunten in het platte vlak (1965) 147
S.C. van Veen

INLEIDING IN DE DISCRETE WISKUNDE

H.J.A. Duparc

0. De laatste jaren wordt het steeds duidelijker dat in de wiskunde modeverschijnselen een rol spelen. Nu kon men bij de wiskunde wat haar conventies, notaties en preferenties betreft door de eeuwen heen wel iets als een mode signaleren, maar het modeverschijnsel waar het hier over willen hebben is van een geheel andere aard: het betreft enerzijds het onder een nieuwe naam (en wel de naam *Discrete Wiskunde*) brengen van een aantal deelgebieden der wiskunde, anderzijds de nadruk waarmee dit nieuwbenaamde gebied wordt geïntroduceerd. Dit laatste mede in verband met ontwikkelingen in de informatica, die hieraan meer behoefte heeft dan aan analyse.

Wij willen hier twee aspecten van de discrete wiskunde behandelen. Allereerst de ontwikkeling en later afbakening van dit deel der wiskunde in relatie tot de ontwikkeling van de wiskunde in het algemeen en verder aan de hand van een zeer globale inventarisatie van wat men thans onder discrete wiskunde verstaat, een uitwerking van enkele onderdelen (met indicatie over hun toepassingen).

1.1. Bij het beschouwen van de geschiedenis der wiskunde onderkent men van oudsher de meetkunde als hoofddiscipline, eerst experimenteel-practisch ontwikkeld, later - in de griekse tijd - geaxiomatiseerd tot een redelijk streng deductief systeem. Daarnaast kwam het rekenen op; aanvankelijk evenzeer als practische vak, zij het dat dit - vooral in de Oudheid - op uiterst

onpractische manier werd bedreven.

Wel vindt men in de elementen van Euclides reeds een kiem van de theorie van het rekenen, ja zelfs van die van het irrationele getal, een grotere rekenvaardigheid werd echter pas later door Arabieren ontwikkeld en bereikte (West-)Europa vele eeuwen nadien. Het gebruik maken van het positiestelsel om (natuurlijke) getallen aan te duiden was de grote vondst die het rekenen voor op den duur ieder toegankelijk en uitvoerbaar maakte. Verdere al dan niet Arabische vaardigheden als het oplossen van vergelijkingen droegen het hunne ertoe bij dat in het onderwijs naast het vak meetkunde een vakkencomplex als rekenen en algebra algemeen doordrong.

De westerse ontwikkeling der natuurwetenschappen en techniek werd mogelijk dank zij de ontdekking der infinitesimaalrekening, die zo'n vier eeuwen geleden in de universitaire programma's en zo'n vier*jaar geleden definitief in de programma's van secundair onderwijs werd opgenomen (een trend die met het rekenen zonder meer al eerder had plaats gevonden: eerst op de universiteiten, later in het secundair onderwijs en nu nog in het lager onderwijs - volgens sommigen daarin ook al niet meer in voldoende mate).

Tezamen met verdere vakken als beschrijvende, projectieve en analytische meetkunde en lineaire algebra heeft men hier een basisopsomming van de kernelementen in de eerste helft van deze eeuw van de aan universiteiten of technische hogeschool gedoceerde pre-candidaats wiskunde. De analyse begon - mede in het licht van het eerder genoemde gebruik in andere disciplines - een steeds overheersender positie in te nemen. Ongetwijfeld was daaraan mede het feit debet dat in de negentiende eeuw voor dit vak door mensen als Cauchy een fundering was gelegd, die een Euclides niet zou hebben misstaan. Men kon nu gerust zijn, in de analyse wist men heel precies wat wel en niet toelaatbaar was. Had Euler nog genoeg intuïtieve feeling om een eeuw vóór Cauchy te weten wat wel en niet toelaatbaar was, thans behoeft men slechts netjes de theorie te volgen om als gewoon mens (of nu al als scholier) volgens de regels der kunst analyse te kunnen bedrijven.

*) Deze voordracht dateert uit 1975.

1.2. In deze eeuw - en daarbij moeten wij wat uitgebreider stilstaan - trad de algebra op de voorgrond. Misschien hebben de wiskundigen zich wel eens afgevraagd waarom in de meetkunde (en later in de analyse) wél de behoefte bestond om deze te beoefenen vanuit een streng axiomatisch systeem, maar waarom dat niet het geval was met de algebra. Op de lagere school leerde je rekenen volgens bepaalde - veelal niet of nauwelijks beargumenteerde - regels en in het verdere onderwijs ging het in de algebra niet zo erg veel anders toe. Het leek wel of pas nu de tijd ervoor rijp was dat ook de algebra een axiomatisering zou ondergaan. Een belangrijke bijdrage hieraan bracht het verschijnen van VAN DER WAERDENs "*Moderne Algebra*".

Men is zich er sindsdien van bewust dat de bestaande rekentechnieken op enkele grondregels berusten en dat bij het invoeren van een ander systeem van grondregels een andere algebra te voorschijn kan komen. Hier signaleren wij een analoge ontwikkeling als bij de meetkunde, waar de vorige eeuw ons naast de euclidische meetkunde andere evenzeer axiomatisch sluitende meetkunden bracht.

Allengs werd de rol van de algebra belangrijker. Men onderkende dat de meetkunde van een algebraïsch uitgangspunt is op te bouwen en men zag later in dat een ander algebraïsch systeem voerde tot een andere meetkunde (een enkel voorbeeld hiervan vindt men in de huidige MOB-stof, zodat wij er hier niet verder op in behoeven te gaan). Maar daar bleef het niet bij. De andere algebraïsche systemen begonnen elders aftrek te vinden. Wij noemen de algebra van Boole, die voor electrotechnici de poorten der schakeltechniek en netwerktheorie opent, waarin het wel of niet gaan van electrische stromen in een netwerk beschreven wordt.

Anderzijds waren er andere gebieden waar ook elementen in optraden, die nauw verwant waren aan de algebra van Boole. Wij denken daarbij enerzijds aan de mathematische logica, die zich na haar beoefening in de Oudheid en de Middeleeuwen in de laatste eeuw tot een algebra-achtig geheel ontwikkelde. Ook hier geldt weer dat wijziging in de axioma's of uitgangspunten kan voeren tot alternatieve systemen. Daarbij kan men denken aan meer-waardige logica's, logica's dan waarbij van een bewering niet langer geldt dat die òf juist òf onjuist is, maar waarbij meer (waarheids-) gradaties mogelijk zijn.

Nauw verwant hiermee is in eerste aanleg de opbouw der waarschijnlijkheidsrekening.

Voorts ontmoet men als verwant systeem aan de algebra van Boole de verzamelingsleer, een theorie waarin de in het secundair onderwijs binnengedrongen Venn-diagrammen een belangrijke beginrol vervullen.

De wiskunde zou de wiskunde niet zijn, als de behoefte niet was gevoeld om de diverse hier geschetste algebraïsche of algebra-achtige ontwikkelingen onder één noemer te vatten. Dat is dan ook gebeurd en het bijbehorend etiket heet *Discrete Wiskunde*. De opsomming der deelgebieden, die men hieronder kan rekenen, is niet volledig geweest. Slechts die werden genoemd die in de hier naar voren gehaalde historische ontwikkeling aan bod kwamen. Straks komen er meer onderdelen aan de orde. Maar voordat dat gebeurt iets over de naam.

1.3. De naam *Discrete Wiskunde* (liever in eerste instantie discrete wiskunde in ruimere zin te noemen) suggereert reeds dat het hier gaat om een onderscheid tussen continue en niet-continue (d.w.z. discrete) wiskunde. In dit verband speelt wellicht in eerste instantie de analyse een rol en wel de plaats van de jonge numerieke wiskunde erin, waar een aantal moeilijke analytische problemen door discretisering wordt aangepakt. Dan komt men terecht in het gebied der discrete wiskunde in engere zin, liever discrete analyse (voor sommigen wellicht een contradictio in terminis) te noemen. Van dit gezichtspunt uit past voor discrete wiskunde in het algemeen wellicht ook wel de naam limiet-vrije wiskunde. Het is dan ook wel duidelijk dat dit soort wiskunde, behalve van theoretische kant uit, ook een rol speelt bij het beschrijven van allerlei zaken, die zich slechts in een eindig aantal toestanden kunnen bevinden: de stroom die wel of niet in een netwerk loopt, de gediscretiseerde waarschijnlijkheid van een gebeurtenis, de kunst van het rekenen met behulp van een eindig aantal symbolen (al dan niet met apparatuur), om nog eens de eerder aangeduide onderwerpen van dit gezichtspunt uit te noemen.

2.0. Na deze gedeeltelijk-historische introductie, willen wij ons thans wagen aan een - reeds aangekondigde - iets meer systematische opsomming van

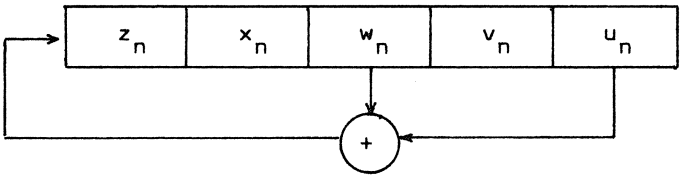
de onderwerpen, die tot de discrete wiskunde (in ruimere zin) te rekenen zijn en aan een simpele aanduiding van hun werkwijze en toepassingsgebied.

2.1. Men behoort, dat is uit het bovenstaande wel duidelijk, natuurlijk te beginnen met de *Algebra* en wel de algebra zoals die zich deze eeuw in abstract-axiomatische zin heeft ontwikkeld. Naast de algebra van Boole, zijn er talloze andere onderdelen van de algebra te noemen. Wij denken bijvoorbeeld aan de theorie van de eindige lichamen, die diverse informatie-theoretische toepassingen vindt. Wij willen er hier twee van noemen.

2.1.1. De theorie der schuifregisters, die voor het genereren van allerlei getallenrijen (of soms zelfs imiteren van bepaalde verschijnselen) van belang is. Een schuifregister bestaat uit een aantal (zeg k) informatie-elementen ("hokjes"), die elk in een eindig aantal (zeg N) toestanden kunnen verkeren. Een momentopname van een schuifregister levert dus een vector $(u,v,w,\ldots,z)$ met k componenten; elk der componenten kan N waarden aannemen. In totaal kan zo'n register zich in N^k toestanden bevinden. Vervolgens wordt afgesproken dat een toestandsverandering zich op discrete momenten zal voltrekken. Wij zullen eenvoudigheidshalve deze momenten aequidistant nemen en kunnen dan spreken over de toestandsvector $(u_n,v_n,w_n,\ldots,z_n)$ op het "moment" n. Bij een schuifregister is het veelal zo dat de toestandsvector op het moment n + 1 grotendeels volgt uit die op het vorige moment door een "opschuiven", d.w.z. $u_{n+1} = v_n$, $v_{n+1} = w_n$, enz., terwijl z_{n+1} een voorgeschreven functie is van de k grootheden $u_n,v_n,w_n,\ldots,z_n$. Wij nemen als voorbeeld k = 5 en N = 2 (d.w.z. elke component kan slechts twee waarden aannemen; wij nemen er voor de getallen 0 en 1) zodat er in totaal 2^5 = 32 verschillende toestanden van het register (u_n,v_n,w_n,x_n,z_n) mogelijk zijn. Tenslotte moeten wij z_{n+1} nog definiëren en daarvoor een dusdanige functie nemen van u_n,v_n,w_n,x_n, en z_n dat het antwoord onder alle 32 omstandigheden weer 0 of 1 wordt.

We kiezen daartoe bijvoorbeeld $z_{n+1} \equiv u_n + w_n \pmod 2$, een relatie waarmee deze eis te verwezenlijken valt.

Schematisch is het gebeuren met onderstaand plaatje weergegeven.



Uit het bovenstaande volgt dat men de toestandsvector op het moment n ook kan aanduiden met $\underline{u}_n = (u_n, u_{n+1}, u_{n+2}, u_{n+3}, u_{n+4})$ en dat verder geldt $u_n+5 \equiv u_n + u_{n+2}$ (mod 2). Na invoeren van de verschuivingsoperator E (die bij elke grootheid u_n de index met 1 verhoogt) krijgt men de formule

$$E^5 u_n \equiv u_n + E^2 u_n \pmod 2$$

ofwel na "herleiden op nul"

$$(E^5+E^2+1)u_n \equiv 0 \pmod 2.$$

Hierbij speelt de veelterm $f(E) = E^5 + E^2 + 1$, ook wel de karakteristieke veelterm van dit proces genoemd, een belangrijke rol. Uit de algebra is bekend dat deze veelterm irreducibel is mod 2, waaruit met behulp van de theorie der eindige lichamen volgt dat f(E) deelbaar is op $E^{31} - 1$. Dit betekent dat onze op nul herleidde formule na (toelaatbare!) vermenigvuldiging met het quotient $(E^{31}-1) : f(E)$ voert tot $(E^{31}-1)u_n \equiv 0$ (mod 2) en dat dat tenslotte leidt tot $u_{n+31} = u_n$. De door het register gegenereerde rij getallen u_n (n=0,1,...) is dus periodiek; hij herhaalt zich na 31 stappen (of in het enige bijzonder uitzonderingsgeval dat men met de nulvector zou beginnen, reeds na 1 stap).

Nog twee opmerkingen over dit resultaat. Als men een proces had beschouwd alweer met k = 5 en N = 2, waarbij de karakteristieke veelterm reducibel is, dan was, zoals zich laat aantonen, de periode van het proces kleiner geworden. Wil men dus processen met lange periode dan verdienen die, waarbij de karakteristieke veelterm irreducibel is, de voorkeur. In een geval als k = 6 en N = 2 blijkt evenzo dat de periode van het proces bij een irreducibele karakteristieke veelterm gelijk is aan $2^6 - 1 = 63$ (of een deler

ervan). Slechts bij die keuzen van k waarbij $2^k - 1$ priem is, is in zulke gevallen de periode op zijn grootst (d.w.z. $2^k - 1$). Zo voert onze schuifregistertheorie dan tevens tot een getallentheoretische vraag, namelijk de vraag voor welke k het getal $M_k = 2^k - 1$ (getal van Mersenne) ondeelbaar is. De grootste thans (1975) bekende k is het getal 19937; een schuifregister met zoveel secties is echter technisch niet construeerbaar. Hier heeft de sport naar records het royaal gewonnen van de techniek.

Ook nog een voorbeeld met een kleine waarde van k en wel k = 3. Kiest men andermaal N = 2 en kiest men $f(E) = E^3 + E + 1$ (een irreducibele derde graads vorm dus), dan vindt men voor de periode van de u-rij (mits $\underline{u}_0 \neq 0$) de waarde $2^3 - 1 = 7$. Bij $\underline{u}_0 = (0,0,1)$ heeft men dan voor de eerste 7 elementen van de rij de waarden 0,0,1,0,1,1,1, een rij waarop wij straks nog terugkomen.

2.1.2. Een ander gebied, evenzeer uit de informatica, waarbij de algebra een belangrijke rol speelt, is de *coderingstheorie*. Ook hier gaat het om een stukje discrete wiskunde. Wij gaan uit van het coderen van de letters a,...,z door middel van het Morse systeem, waarbij wij gemakshalve de punten en streepjes door de cijfers 0 en 1 weergeven. Voor de 26 letters van ons alphabet zijn 5 dergelijke cijfers voldoende, want zij bieden 2^5 mogelijkheden en $2^5 > 26$ (dat in Morseschrift niet alle letters door evenveel symbolen worden gecodeerd laten wij hier buiten beschouwing). Nu komt het in de praktijk voor dat wel eens een symbool bij doorseinen verminkt overkomt, zodat de ontvanger in bepaalde gevallen een dergelijke boodschap zonder meer niet zal begrijpen. Om dit euvel te verhelpen zou men kunnen afspreken dat geen twee coderingen mogen voorkomen, die slechts in één symbool verschillend zijn. Sterker nog, in de praktijk richt men het wel zo in dat alle gebruikte coderingen onderling twee aan twee in b.v. tenminste 3 plaatsen een verschil vertonen, anders gezegd alle coderingen hebben een onderlinge "afstand" 3 of meer. Wordt nu een symbool op één plek verminkt doorgezonden dan heeft het verminkte symbool tot de overige een afstand 2 of meer en alleen tot het oorspronkelijk bedoelde symbool een afstand 1. De ontvanger kan het dus ondanks de verminking reconstrueren.

Wij geven hier een voorbeeld waarbij 7 symbolen in het spel zijn, alle met afstand 4. Dit wordt ontleend aan de zoeven ontmoete vector $\underline{u}$ = (0010111) en alle 6 cyclische permutaties ervan. Het is niet moeilijk na te gaan dat deze 7 vectoren de gewenste eigenschap bezitten. Dat kan men ook aldus inzien. Het verschil tussen $\underline{u}$ en de cyclisch één keer verschoven vector $E\underline{u}$ = = $\underline{v}$ = (1001011) wordt bepaald door het aantal keren dat een component van $\underline{u}$ (cyclisch gezien) verschilt van zijn opvolger, in casu dus vier keer. Maar ook het verschil tussen $\underline{u}$ en $E^2\underline{u}$ moet nu vier zijn, d.w.z. ook moet het vier keer voorkomen dat een component verschilt van de twee plaatsen verder gelegen component. Zo kan men doorgaan: eveneens moet het op vier plaatsen gebeuren dat twee componenten van $\underline{u}$ met plaatsverschil 3 verschillende componenten hebben, enz. Dit laatste laat zich ook anders verifiëren. Onder de rangnummers van de componenten 0 in $\underline{u}$ treden alle verschillen even vaak op. Dan blijkt dat ook zo te zijn met de rangnummers van de componenten 1 in $\underline{u}$.

De rangnummers 1, 2 en 4 van de componenten 0 in $\underline{u}$ hebben (mod 7) dus de eigenschap dat hun verschillen alle waarden 1,2,...,6 even vaak (in casu één maal) opleveren. Zo'n verzameling noemt men een verschilverzameling. Deze soort verzamelingen kan ons helpen om geschikte coderingen te vinden. De vraag is op welke plekken men de cijfers 0 dan wel moet plaatsen. Ook hier blijkt de getallentheorie te helpen: het zijn de plekken met die rangnummers die kwadraatresten mod 7 zijn. Iets dergelijks geldt ook al algemener bij codes van p (waarbij p een ondeelbaar 4-voud + 3 is) symbolen, met $\frac{1}{2}(p-1)$ nullen en $\frac{1}{2}(p+1)$ enen. Men kan voor de plaatsen der nullen de kwadraatresten mod p nemen.

2.2. Een ander belangrijk onderdeel van de discrete wiskunde, is de *combinatoriek* of - wat daarmee verwant is - de leer van het tellen van aantallen. Het is een problematiek die zo oud is als de wereld, zou men wat overdreven kunnen zeggen. De daarbij gebruikte methoden zijn veelal al lang geleden ontwikkeld. Hier, en niet alleen hier, is een stuk discrete wiskunde in het spel dat vroeger onder een andere naam incidenteel werd beoefend, een verschijnsel dat men ook op andere plaatsen in de discrete wiskunde ontdekt.

Natuurlijk zijn er ook wel nieuwe methoden aan de oudere toegevoegd. Een ervan willen wij hier wat nader bespreken. Het is de theorie der voortbrengende functies. Bij een rij $u_n (n=0,1,\ldots)$ definieert men de voortbrengende functie $V(u)$ door middel van de reeks

$$V(u) = \sum_{n=0}^{\infty} u_n x^n .$$

Wij laten voor een aantal voorbeelden het nut van deze theorie zien. Allereerst nemen wij voor u_n het aantal partities $p(n)$ van het getal n, dat is het aantal manieren waarop n als een som van natuurlijke getallen te schrijven is. Hierbij is het toegelaten dat onder die natuurlijke getallen onderling gelijke voorkomen. Verder worden partities waarin slechts de volgorde der termen verschilt als dezelfde gerekend. Onder deze afspraken vindt men

$$p(1) = 1,\ p(2) = 2,\ p(3) = 3,\ p(4) = 5,\ p(5) = 7,\ \ldots$$

Definieert men nog $p(0) = 1$ (zoiets blijkt vaker in de wiskunde nuttig) dan valt gemakkelijk af te leiden dat

$$V(p) = \sum_{n=0}^{\infty} p(n)x^n = 1 : \prod_{k=1}^{\infty} (1-x^k).$$

$$\prod_{k=1}^{\infty} \sum_{m=0}^{\infty} x^{mk}.$$

Formeel hoort hier (trouwens steeds in de theorie van de voortbrengende functies) de convergentie van de reeks te worden bekeken. Als wij ons beperken tot $|x| < 1$ kan men daarover gerust zijn.

Beschouwt men voorts partities $q(n)$ van een getal n, waaronder geen gelijke elementen voorkomen, dan vindt men als voortbrengende functie

$$V(q) = \sum_{n=0}^{\infty} q(n)x^n = \prod_{k=1}^{\infty} (1+x^k).$$

Verder voldoet de voortbrengende functie V(r) van het aantal verdelingen r(n) in oneven delen aan

$$V(r) = \sum_{n=0}^{\infty} r(n)x^n = 1 : \prod_{k=0}^{\infty} (1-x^{2k+1}).$$

Nu leert de relatie

$$V(r) = \frac{1}{(1-x)(1-x^3)(1-x^5)\ldots} = \frac{(1-x^2)(1-x^4)(1-x^6)\ldots}{(1-x)(1-x^2)(1-x^3)\ldots} =$$

$$= (1+x)(1+x^2)(1+x^3)\ \ldots = V(q)$$

dat het aantal partities van een natuurlijk getal in oneven delen even groot is als het aantal partities van dat getal in ongelijke delen. Natuurlijk is voor dit resultaat ook wel direct (maar wel wat subtiel) bewijs mogelijk; de voortbrengende functies maken het bewijs echter wel erg eenvoudig.

2.3. Als laatste gebied van de summiere opsomming van een aantal onderwerpen uit de discrete wiskunde noemen wij de differentierekening, die eigenlijk als een soort discrete analyse te beschouwen is. Hier gaat het om grootheden u_n, die voor discrete n (vaak $n \in \mathbb{N}$ of $n \in \mathbb{Z}$) gedefinieerd zijn, maar waarvan de waarden willekeurig reëel of imaginair kunnen zijn. Dit vak kwam in relatie met de numerieke wiskunde tot ontplooiïng. Vaak werden problemen over functies u(x) (x willekeurig reëel) waarin ook de afgeleide u'(x) mee deed door discretisering aangepakt, waarbij in principe de grootheid u'(x) door de differentie $\Delta u(x) = u(x+1) - u(x)$ werd vervangen. Numerici en analytici doorgronden gaarne hoe groot de daarbij optredende fout wel is. Wij laten die hier voor wat hij is en beperken ons tot de analoga van de differentiaalvergelijkingen, die men differentievergelijkingen noemt. Zo heeft een homogene lineaire differentievergelijking van de tweede orde met constante coëfficiënten de gedaante.

$$a\Delta^2 u_n + b\Delta u_n + cu_n = 0.$$

Zo'n relatie is ook anders te schrijven, immers $\Delta u_n = u_{n+1} - u_n = Eu_n - u_n =$

$= (E-1)u_n$, dus $\Delta^2 u_n = (E-1)^2 u_n$. Onze differentievergelijking is dus ook te schrijven als een homogene lineaire relatie $Au_{n+2} + Bu_{n+1} + Cu_n = 0$ tussen u_n, u_{n+1} en u_{n+2}, ook wel een recurrente relatie (van de tweede orde) genoemd.

Naast diverse oplossingstactieken is hier ook die met behulp van voortbrengende functies van nut. Immers men heeft bij

$$V(u_n) = \sum_{n=0}^{\infty} u_n x^n$$

de betrekking

$$V(Eu_n) = V(u_{n+1}) = \frac{1}{x} \sum_{x=0}^{\infty} u_{n+1} x^{n+1} = \frac{1}{x} (V(u_n) - u_0) = \frac{1}{x} V(u_n) - \frac{u_0}{x}$$

en evenzo

$$V(E^2 u_n) = \frac{1}{x} V(Eu_n) - \frac{u_1}{x} = \frac{1}{x^2} V(u_n) - \frac{u_0}{x^2} - \frac{u_1}{x} .$$

Dan gaat onze recurrente relatie over in

$$AV(E^2 u_n) + BV(Eu_n) + CV(u_n) = 0,$$

dus in

$$\left(\frac{A}{x^2} + \frac{B}{x} + C\right) V(u_n) = \frac{Au_0 + Au_1 x + Bu_0 x}{x^2} ,$$

dus

$$V(u_n) = \frac{Au_0 + Au_1 x + Bu_0 x}{A + Bx + Cx^2} .$$

Als men de laatste uitdrukking in een Taylorreeks ontwikkelt vindt men een formule voor u_n, de coëfficiënt van x^n in die Taylorreeks.

De methode loopt nog iets fraaier als men in plaats van de voortbrengende functies gebruik maakt van de in de techniek welbekende z-transformatie. Bij een rij u_n $(n=0,1,\ldots)$ definiëert men deze als volgt

$$Z(u_n) = \sum_{n=0}^{\infty} u_n z^{-n-1} .$$

Men vindt dan gemakkelijk

$$Z(Eu_n) = zZ(u_n) - u_0,$$

een formule die sterk herinnert aan de formule

$$L(y') = sL(y) - y(0)$$

uit de theorie van de Laplace-transformaties. Deze kunnen van nut zijn bij het oplossen van zekere differentiaalvergelijkingen, de z-transformaties presteren hetzelfde bij de differentievergelijkingen.

3. Hoewel nog heel wat verdere gebieden uit de discrete wiskunde te vermelden zijn willen wij het hierbij laten. Een zekere afsluiting en samenvatting kan wel liggen in de uitspraak dat de rol die de analyse vervult bij de klassieke toegepaste wiskunde, machanica en physica thans wordt gespeeld door de discrete wiskunde ten behoeve van de informatica. Daarbij wordt een sterk beroep gedaan op diverse stukken algebra, getallentheorie, combinatoriek en dat heus niet op grond van het feit dat veel rekentuig zijn rekenen zelf in het tweetallig stelsel verricht (hoe interessant dat feit op zichzelf ook mag zijn).

HET TELLEN VAN VROEGER TOT NU

H.J.A. Duparc

§0. INLEIDING

Er ligt een lange weg van de oerintuïtie van het tellen tot de huidige geraffineerde wiskundige taktieken van tellen. Laten we ter inleiding enkele aspecten over het tellen zelf vermelden, waarbij tevens de verwevenheid van taal en tal (tellen) naar voren komt.

Reeds in een primitief stadium van de ontwikkeling van een gemeenschap ontstaat een behoefte tot tellen. In eerste instantie is dit een registrerende aangelegenheid, men ziet een bepaald object, men ziet nog een dergelijk object en men begint zich te realiseren dat men deze indrukken korter kan weergeven door de mededeling dat men (twee) objecten heeft gezien; het meervoud van een substantief is dan geboren. In nogal wat niet al te primitieve talen kent men bij een zelfstandig naamwoord dan ook aparte vormen voor enkelvoud resp. meervoud. In het Maleis (bahasa Indonesia) wordt het meervoud vaak gegeven door een herhaling van het substantief; zo betekent orang orang (veelal geschreven als orang^2) mensen; in tal van talen heeft men aparte achtervoegsels voor het meervoud.

Ontwikkelt een en ander zich verder dan is er de trits: een, twee, veel. Sporen daarvan zijn VWO-ers, die Grieks hebben geleerd, bekend, in welke taal men enkelvoud, tweevoud (dualis) en meervoud onderscheidt.

Om zijn bezit aan gelijksoortige objecten te kunnen vaststellen kreeg de mens behoefte aan afzonderlijke telwoorden, waarbij een verregaande nuancering van het zoeven genoemde begrip "veel" plaatsvond.

Interessant is een soort intelligentietoets waarbij men kan vaststellen welk aantal gelijksoortige objecten men nog met één oogopslag kan vaststellen en welke niet meer. Veelal ligt de grens - vooral wanneer het om ordeloos bewegende objecten als koeien of vogels gaat - ergens tussen de tien en twintig.

Het moet een hele ontdekking zijn geweest toen men tot het besef kwam dat dezelfde telwoorden dienst konden doen voor het aangeven van aantallen van allerlei onderling totaal verschillende dingen. Zo kent het Japans nog aparte telwoorden voor aantallen mensen, vogels, voorwerpen enz., zij het dat die telwoorden onderling wel enige etymologische verwantschappen vertonen.

Voor een wiskundige wordt het tellen al een beetje interessant als men aantallen ook op schrift kan stellen, met andere woorden als hij methoden kent om aantallen in cijfers weer te geven. In de loop der tijden zijn daarvoor geheel verschillende systemen ontwikkeld.

Uiterst primitief is de kerfstok, elk streepje geeft een eenheid aan en het bedoelde aantal is af te lezen uit wat men op zijn kerfstok heeft.
De Chinees-Japanse cijfers 一, 二, 三 (die wij hier zonder uitleg durven geven) en de Romeinse cijfers voor dezelfde getallen herinneren ons daar nog aan.
Al gauw onstonden slimme notatiesystemen voor grotere aantallen. Kende men in het oud-Latijnse schrift nog het symbool IIII, later toen voor het getal vijf al lang het symbool V was ingevoerd, werd via een subtractief systeem voor het getal 4 de welbekende schrijfwijze IV ingevoerd. Subtractief worden in het Latijn ook getallen als 9 geschreven en getallen als 18 (duo-de-viginti) en 19 uitgesproken.

Wil men naar hogere aantallen toe dan is men meer gediend met additieve dan met subtractieve methoden, waarbij men een aantal basissymbolen voor hogere aantallen invoert en zo komt tot het systeem I,V,X,L,C,D,M. In het oud-Griekse systeem gold ook iets dergelijks, maar later benutte men de Griekse letters, voorzien van een extra accent voor de telwoorden 1,2,...,9; 10,20,...,

90; 100,200,...,900. Omdat het Griekse alfabet slechts 24 letters telde, gebruikte men er 3 Phoenicische leensymbolen bij. Door een andere plaatsing van het accent bracht men het tot de basiseenheden 1000,2000,...,900.000.

In een en andere onderkent men zowel in naamgeving als in schrijfwijze de speciale rol van de getallen 5 en 10, welke samenhangen met de aantallen vingers per menselijk hand ("je kunt het op je vingers natellen").

Wat de taal betreft kende men in het Griekse aparte woorden voor tien, honderd, duizend en tienduizend. Ook in het Japans is voor tienduizend een apart woord en waar wij (zonder speciaal woord voor 10^4) aparte benamingen kennen voor de aantallen $10^3, 10^6, 10^9, \ldots$ heeft men die in het Japans heel consequent voor $10^4, 10^8, 10^{12}, \ldots$.

Het Frans herinnert ons aan nog andere elementen in het tellen door hun woorden voor getallen als 70,...,79 en vooral 80,...,99. Ook andere getallen speelden wel een - zij het wat meer summiere- rol in het tellen; men denke aan uitdrukkingen als een paar, een stel, een dozijn, enz.

Het is duidelijk dat al dit soort systemen weinig noodt tot aantrekkelijke rekenpraktijken. Toch zag een man als Archimedes kans het getal π met vrij grote nauwkeurigheid te berekenen. Ja ook doorbrak hij bewust de grens van $10^6 - 1$ in zijn zandrekening, waarin hij het aantal zandkorrels berekende dat het heelal (in de toenmalige visie erover) zou kunnen vullen.

Pas de invoering van het positiestelsel, mede mogelijk geworden door de bewustwording over en het in symbool invoeren van het getal nul, bracht ons zo'n viertal eeuwen terug een essentiële verbetering in het schrijven van en rekenen met getallen. Heel geleidelijk verhuisde het vak rekenen van de universiteit naar middelbaar en lager onderwijs. Dat kan met een vak dat zich heeft ontwikkeld tot een welhaast mechanische routine-bezigheid. De ontwikkeling van moderne mechanische tel- en rekenapparatuur zal dit proces verder beïnvloeden en wellicht het bijbrengen van vaardigheid in het zonder hulpmiddelen rekenen ook in het basisonderwijs minder belangrijk maken.

§1. TELLEN IN DE INFORMATICA

Wij stappen nu af van de primaire aspecten van het tellen en gaan kijken hoe men met telresultaten werkt. Daarbij is er onderscheid te maken tussen het ordenen, opbergen en weer tevoorschijn halen van telresultaten enerzijds en het toepassen van (rekenkundige) operaties op getallen anderzijds. Het eerste type activiteiten ondervindt thans grote aandacht in de informatica, het tweede type in diverse (verdere) takken van wiskunde.

Bij het eerste type gaat het vaak niet alleen om achter elkaar opslaan van telgegevens, maar ook om dit soort zaken op een enigszins logische wijze te doen plaatsvinden. Vaak brengt men de plaats u van opslaan van het (n^e) gegeven in een of andere vorm in relatie tot n, kortweg er is een afbeelding van n naar u_n, die ook handig zo kan worden gebruikt dat uit het getal u_n het oorspronkelijke getal n weer is terug te vinden. Voorbeelden hiervan in min of meer zuivere vorm zijn onder meer onze telefoonnummers. Aanvankelijk was het nummersysteem van de kengetallen in relatie tot een geografische ordening van onze gemeenten, terwijl bij de abonneenummers dit principe ook in een of andere mate locaal werd gebruikt: bij dicht bij elkaar wonende abonnees verschillen de telefoonnummers veelal slechts in de eindcijfers. Men zou hier kunnen spreken van een verzwakte vorm van continuïteit. In onze moderne maatschappij is het reeds zover gekomen dat men meer dan één nummer aan een individu toevoegt; naast telefoonnummers denkt men aan banknummers, paspoortnummers, salarisadministratienummers, enz. Niet bij elk systeem is de systematiek even essentieël. Er zijn stellig informatici die liever zouden zien dat iedereen één nummer kreeg toegewezen dat voor alle doeleinden bruikbaar zou zijn. Daarbij komt men natuurlijk in conflict met andere organisatorische eisen die de gebruiker (de bank, de werkgever) in zijn systeem wil aanbrengen. Eén ding is wel duidelijk: de naam van een mens is ondeugdelijk als ondubbelzinnige codering van de betrokkene; men denke alleen al aan de traditie in vele families om kinderen naar hun (groot)ouders te vernoemen.

§2. TELLEN IN DE (KLASSIEKE) WISKUNDE

Richten wij ons thans tot de klassieke wiskunde dan liggen de telproblemen voor het grijpen. Eigenlijk kwamen die geleidelijk naar voren als gevolg van het doordringen van wiskundige aspecten op steeds meer plekken in het dagelijks leven. Dat bij allerlei physisch/technische problemen de rij der natuurlijke getallen diverse verfijningen nodig had, laten wij hier buiten beschouwing, het is niet het doel van deze voordracht. Er zijn voldoende andere problemen waar de natuurlijke getallen een antwoord op kunnen brengen of hulp kunnen bieden.

2.1. Tellen in de meetkunde

Eerst behandelen wij wat problemen uit de meetkunde. Wij noemen hierbij het aantal regelmatige lichamen in de driedimensionale Euclidische ruimte met generalisatie naar meer dimensies. Ook kunnen wij ons afvragen in hoeveel gedeelten de R_2 wordt verdeeld door n (n = 1,2,3,...) algemeen gelegen rechten, waarna een analoge vraag opkomt voor de $R_3, R_4, \ldots$. Genoeg zij het hier het antwoord te geven, maar wij laten het expres weg ten behoeve van hen die het liever zelf willen uitzoeken.

In een apart onderdeel der meetkunde, de door H. Schubert ontwikkelde en door B.L. van der Waerden op (algebraïsche) poten gezette Meetkunde van het Aantal (Abzählende Geometrie) beantwoordt men de vraag naar het aantal oplossingen van bepaalde meetkundige problemen. Het daarbij gebruikte beginsel van het behoud van het aantal (dat zou overigens ook wel aardig motto zijn geweest voor deze vacantiecursus) helpt essentieel mee om tot antwoorden te komen. Wij illustreren dat aan de vraag naar het aantal overlijnen van 4 willekeurig gelegen gegeven rechten in R_3 (dat is het aantal rechten dat ze alle 4 snijdt). Volgens genoemd beginsel kan men dit antwoord ook krijgen als van de vier rechten er twee zijn die elkaar snijden en ook de andere twee elkaar snijden. Dan ziet men snel in dat er twee oplossingen zijn voor dit probleem en "dus" zijn er in het algemeen ook twee (en de theorie van de hyperboloïde die bij een "klassieke" behandeling van dit probleem hoort heeft men aldus niet nodig).

In ditzelfde vak wordt ook op eenvoudige wijze antwoord gegeven op de vraag naar de klasse van een vlakke kromme van de graad n, dat is het aantal raaklijnen uit een willekeurig punt aan die kromme. Men vindt er voor het bekende aantal $n(n-1)$ bij krommen zonder dubbelpunten en keerpunten ofwel $n(n-1) - 2d - 3k$ voor een kromme met d dubbelpunten en k keerpunten (formules van Plücker).

Ook via dit vak kan men een eenvoudig bewijs geven van de stelling van Bezout, die inhoudt dat het aantal snijpunten van een vlakke kromme van de graad n en een vlakke kromme van de graad m gelijk is aan m n.

2.2. Tellen in de discrete wiskunde

Met name in de discrete wiskunde speelt het tellen een belangrijke rol. Daarbij komen al gauw aanrakingsgebieden met de waarschijnlijkheidsrekening en operationele analyse naar voren.

2.2.1. Waarschijnlijkheidsrekening

Laten wij beginnen met de waarschijnlijkheidsrekening waar in het kader van de klassieke definitie van kans aantallen gunstige en mogelijke gevallen moeten worden berekend. Wij herinneren eraan dat daarbij vaak combinatorische problemen op de voorgrond treden. Zo ziet men dat een dominospel bestaat uit $\binom{7}{2}$ (aantal stenen met onderling verschillende aantallen ogen) + $\binom{7}{1}$ (aantal stenen met onderling gelijke aantallen ogen) = 28 stenen en de keus dat men er blindelings een steen uit trekt met ogensom 7 is dus $\frac{3}{28}$, waarbij de teller gevonden wordt door tellen zonder meer. In hoeverre kaartspelers zich bij hun spel laten leiden door bliksemsnel kansberekeningen dan wel routine of intuïtie laat ik hier liever in het midden.

2.2.2. Taalkunde en cryptografie

Zelfs in de moderne taalkunde dringt het kansbegrip door. Door de frequenties van gebruikte woorden in bijvoorbeeld de Ilias of Odyssee te bepalen (tellen!) komt men tot beschouwingen over de kans dat deze beide werken van eenzelfde of van twee verschillende auteurs afkomstig zijn. Ook in de cryptografie speelde het door tellen bepaalde frequentiepatroon van de letters in een taal een rol om aldus bij "versleutelde" berichten (onder zekere

voorwaarden over het versleutelingssysteem) de code te kunnen "breken".

Bij de klassieke coderingsmethoden worden bijvoorbeeld de letters a,...,z door getallen 00,...,25 gerepresenteerd en dan mod 26 beschouwd. Door nu verder een getallenrij γ_0,γ_1 te genereren en de k^e letter uit een bericht β, in symbool het getal β_k, (mod 26) met γ_k te vermeerderen ontstaat dus - in vectornotatie - een bericht $B = \beta + \gamma$ (mod 26). Zodra de rij periodiek is, laten geraffineerde telmethoden het toe uit de letterverdeling in B in relatie tot de letterverdeling in de taal waarin β is gesteld conclusies over die periode te trekken, hetgeen de eerste stap oplevert voor het decoderen van B. De sport richt zich dan bij voorkeur op het maken van rijen γ met een zeer lange periode, waarbij door wat verdere verfijningen in het systeem niet a priori mod 26 behoeft te worden gerekend.

2.2.3. Genereren van getallenrijen

De elementaire getallentheorie levert vele mogelijkheden van genereren van bepaalde getallenrijen op. Zo kan men het gedrag van de rij γ_n met

$$\gamma_{n+1} \equiv 3\gamma_n \pmod{31}$$

bestuderen of algemener van een eerste orde recurrente rij

$$\gamma_{n+1} \equiv k\gamma_n \pmod{m}$$

bij voorkeur voor ondeelbare m. Een volgende gedachte, om te komen tot een langere periode, voerde tot de overbekende rij van Fibonacci (een tweede orde recurrente rij) mod m genomen

$$\gamma_{n+2} \equiv \gamma_{n+1} + \gamma_n \pmod{m}$$

met $\gamma_0 = 0, \gamma_1 = 1$. Is bij m = 37 de periode van de eerste orde rij een deler van 36, bij m = 37 levert de rij van Fibonacci een periode die een veelvoud is van 38.

Het gedrag van de modulus m speelt bij vele van deze methoden een rol. De bedoelde perioden zijn in het algemeen het grootste bij ondeelbaar m, zo-

dat hier een motivering ligt van de jacht naar grote priemgetallen. Er is ongeveer een eeuw geleden door Lucas een stelling gegeven waarmee ook nu nog de recordhouders worden gevonden. In de uitvoering speelt daarbij de rekenmachine een belangrijke rol. Al die recordhouders zijn van de gedaante 2^s-1 (is uiteraard priem). Op de overige getallen heeft men nauwelijks vat. Voorzover bekend geldt voor de huidige (1980) recordhouder s = 44497.

Wij noemen nog enige andere typen rijen $\gamma_n = u_n + 2v_n$ (met $u_n \in Z_2$), waarbij in de recurrente definitie niet alleen elementen γ met lagere index maar ook dergelijke elementen u en v worden betrokken. Als een eerste voorbeeld noemen wij de rij met definitie

$$\gamma_{n+2} = u_n + u_{n+1} + v_n + v_{n+1},$$

waarbij het dus de bedoeling is dat de som in het rechterlid niet alleen het nieuwe getal γ_{n+2} oplevert, maar ook via de Euclidische algorithme de beide nieuwe getallen u_{n+2} en v_{n+2} (met $v_{n+2} \in \mathbb{N}$ en $u_{n+2} \in Z_2$). Een iets geraffineerdere rij is die welke op analoge wijze wordt bepaald door de relatie:

$$2v_{n+1} + u_{n+27} = u_n + v_n + u_{n+10} + 1.$$

Neemt men niet elk van de vereiste beginvoorwaarden gelijk aan nul, dan heeft de rij de periode 67174400, welke voor menig (cryptografisch) doel groot genoeg is. Hierbij speelt een rol het feit dat het getal $2^{27} + 2^{17} + 1$ priem is.

In deze sector zijn nog genoeg open problemen. Wij noemen - ter aanmoediging of afschrikking - de rij γ_n, die als volgt wordt gedefinieerd:

$$\gamma_{n+1} = \tfrac{1}{2}\gamma_n \quad \text{als } \gamma_n \text{ even is;}$$

$$\gamma_{n+1} = 3\gamma_n + 1 \quad \text{als } \gamma_n \text{ oneven is.}$$

De rij is ook met de hierboven gegeven u-v-notatie weer te geven.
Vraag: is voor elke keuze van γ_0 de rij begrensd (en dus op den duur periodiek)?

2.2.4. Tellen in de grafentheorie

Vervolgens nemen wij nog de grafentheorie waarbij een netwerk van punten en al dan niet georiënteerde verbindingswegen (denk aan éénrichtingsverkeer) is gegeven en de vraag kan rijzen op hoeveel wijzen het mogelijk is van een punt A in dit netwerk langs die wegen naar een punt B ervan te gaan. De hier letterlijk te nemen uitspraak dat er vele wegen naar Rome leiden leerde de mensheid al eerder. Niet zodra is dit probleem opgelost of er dient zich een ingewikkelder variant aan. Daarbij is voor het afleggen van elke verbindingsweg de tijdsduur of de prijs bekend en men kan een vraag stellen over de in tijdsduur kortste of over de goedkoopste weg. Zo'n vraagstuk hoort thuis in de operationele analyse en wordt aangepakt met methoden die in dat vak zijn ontwikkeld, vaak met behulp van rekentuig. Een iets ingewikkelder probleem is dat van de handelsreiziger (travelling Salesman problem), die de kortste weg moet opsporen die langs een aantal voorgeschreven punten van het netwerk voert.

2.2.5. Voortbrengende functies

Een vrij practische probleem is het schrijven van een gegeven natuurlijk getal als niet-negatieve lineaire combinatie van een aantal gegeven natuurlijke getallen. In de praktijk treedt dit op bij de vraag welke munten men moet slaan om in het handelsverkeer practisch te kunnen werken. Interessant is daarbij de vraag naar het minimum aantal munten waarmee men een bepaald bedrag kan betalen. In ons muntsysteem vindt men dat door eerst die munt te gebruiken met de hoogste muntwaarde, die kleiner dan m is en deze procedure te herhalen op het nog te betalen restbedrag. Het is niet moeilijk in te zien dat bij een ander systeem van basismunten deze procedure niet meer op gaat.

Niet verder van deze problematiek verwijderd ligt de vraag op hoeveel manieren u_n een natuurlijk getal n te schrijven is als niet-negatieve lineaire combinatie van twee gegeven onderling ondeelbare natuurlijke getallen a en b. Dit probleem pakken wij aan met behulp van de theorie van de voortbrengende functies (soms deftig genererende functies genoemd). Daarbij voegt men aan een rij getallen u_n $(n \in \mathbb{N})$ de functie

$$U(z) = \sum_{n=0}^{\infty} u_n z^n$$

toe. Het is duidelijk dat voor het zoeven genoemde probleem de functie:

$$\frac{1}{(1-z^a)(1-z^b)}$$

na ontwikkeling in een machtreeks (wat - laten wij dit ter ere van de analytisch bezorgden even vaststellen - voor $|z| < 1$ toelaatbaar is) voldoet. Hieruit leest men direct af dat $u_0 = 1$, iets dat men natuurlijk ook rechtstreeks kan begrijpen. Uit de elementaire schoolalgebra weet men dat de uitdrukking

$$V(z) = \frac{(1-z)(1-z^{ab})}{(1-z^a)(1-z^b)} = (1-z-z^{ab}+z^{ab+1})U(z)$$

een veelterm is van de graad $N = ab - a - b + 1$ in z. Op practische gronden nemen we nog

$$u_k = 0 \text{ voor } k < 0.$$

Dus voor $n > N$ moet gelden

$$u_n - u_{n-1} - u_{n-ab} + u_{n-ab-1} = 0$$

(waarmee men hogere u's kan vinden uit lagere), terwijl u_N, zoals men gemakkelijk inziet, gelijk is aan 1. Nu geldt voor de getallen u_n met $n < N$ dat $n - ab < 0$, $n - ab - 1 < 0$, dus $u_{n-ab} = u_{n-ab-1} = 0$, zodat onze veelterm $V(z)$ ook te schrijven is als

$$\sum_{n=0}^{N} u_n z^n - \sum_{n=0}^{N-1} u_n z^{n+1} = (1-z) \sum_{n=0}^{N-1} u_n z^n + u_N z^N.$$

Dus
$$\frac{1-z^{ab}}{(1-z^a)(1-z^b)} = \sum_{n=0}^{N-1} u_n z^n + \frac{z^N}{1-z}.$$

Vervanging van z door $\frac{1}{z}$ en vermenigvuldiging met z^{ab-a-b} levert

$$(1) \qquad \frac{z^{ab}-1}{(z^a-1)(z^b-1)} = \sum_{n=0}^{N-1} u_n z^{ab-a-b-n} + \frac{1}{z-1}$$

en optelling der formules leert

$$\sum_{n=0}^{N-1} u_n z^n + \sum_{n=0}^{N-1} u_n z^{ab-a-b-n} = \sum_{n=0}^{N-1} (u_n+u_{N-n-1}) z^n = \frac{1-z^N}{1-z} = \sum_{n=0}^{N-1} z^n.$$

Dus $u_{N-n-1} + u_n = 1$, dus van de grootheden u_n en u_{N-n-1} met $0 \leqq n \leqq N-1$ is de ene 0 en de andere 1.

Dus als een getal n splitsbaar is, is het getal N-n-1 = ab-a-b-n het niet.

Verder geldt nog

$$\sum_{n=0}^{\infty} u_n z^n = \frac{1-z^{ab}+z^{ab}}{(1-z^a)(1-z^b)} = \frac{z^{ab}}{(1-z^a)(1-z^b)} + \sum_{n=0}^{N-1} u_n z^n + \sum_{n=0}^{\infty} z^{n+N}$$

$$= \sum_{n=0}^{\infty} u_n z^{ab+n} + \sum_{n=0}^{N-1} u_n z^n + \sum_{n=0}^{\infty} z^{n+N},$$

waaruit voor $n > N$ volgt

$$u_n = u_{n-ab} + 1 \geqslant 1,$$

dus elk getal > N is splitsbaar.

Neemt men in formule (1) nog z = 2, dan komt er

$$\frac{2^{ab}-1}{(2^a-1)(2^b-1)} = 1 + \sum_{n=0}^{N-1} u_n 2^{ab-a-b-n},$$

d.w.z. in de binaire ontwikkeling van het getal

$$\frac{2^{ab}-1}{(2^a-1)(2^b-1)} - 1$$

staat op de n^e plaats een cijfer 0 of 1 alnaar gelang het getal ab-a-b-n splitsbaar is of niet.

TELTECHNIEKEN

F. Göbel

§1. INCIDENTIESTRUKTUREN

Een incidentiestruktuur kan men definiëren als een collectie van twee of meer typen objecten waarbij een binaire relatie (de incidentierelatie) is gegeven tussen objecten van het ene en objecten van het andere type. Bijvoorbeeld, in een collectie van punten en lijnen kan een punt wel of niet op een lijn liggen. Of, in een collectie van elementen en verzamelingen kan een element wel of niet tot een verzameling behoren.

In een incidentiestruktuur valt van alles te tellen. Men kan bijvoorbeeld geïnteresseerd zijn in het aantal objecten van het ene type dat incident is met een gegeven object van het andere type. In het algemeen zal dat aantal afhangen van het gegeven object (en natuurlijk ook van de onderhavige incidentiestruktuur). Wij beschouwen echter gevallen met een zekere regelmaat, waardoor het tellen eenvoudiger en zinvoller wordt.

Een bekend voorbeeld van zo'n regelmatige incidentiestruktuur is de *kubus*. We onderscheiden hier drie typen objecten: hoekpunten, ribben, en zijvlakken. De kubus heeft 6 zijvlakken en ieder zijvlak is incident met 4 punten. Het aantal hoekpunten van de kubus is echter niet 6 x 4, maar 8.
De faktor 3 is te verklaren uit het feit dat ieder hoekpunt incident is met 3 zijvlakken, zodat ieder hoekpunt drie maal geteld werd.

Op analoge wijze kunnen we het aantal ribben van de kubus bepalen: $6 \times 4/2$, immers er zijn 6 zijvlakken, ieder is incident met 4 ribben, en we delen door 2 omdat iedere ribbe incident is met 2 zijvlakken.

OPGAVE 1. Een polyeder wordt begrensd door 20 driehoeken waarvan er 5 in elk hoekpunt samenkomen. Bepaal het aantal hoekpunten en het aantal ribben.

Een schijnbaar geheel ander voorbeeld betreft een groep van 24 mensen. Ieder kent 5 anderen uit de groep, terwijl ieder tweetal kennissen precies 2 gemeenschappelijke kennissen heeft. Hoeveel drietallen van mensen zijn er die elkaar alle drie kennen? Om deze situatie als een incidentiestruktuur te zien, kunnen we de volgende typen objecten onderscheiden: mensen, mensenparen en drietallen. Het gevraagde aantal is $24 \times 5 \times 2/6 = 40$, immers uitgaande van een vaste persoon (24 mogelijkheden) zijn er 5 paren waarmee hij incident is, en daarna zijn er 2 drietallen waarmee het paar incident is. We moeten door 6 delen omdat ieder drietal 6 maal is geteld.

OPGAVE 2. Maak een overzicht van alle drietallen (n,k,r) met $0 \leqslant r < k < n \leqslant 6$ waarvoor geldt: er is een groep van n personen denkbaar waarin iedereen k andere groepsleden kent, terwijl ieder tweetal kennissen precies r gemeenschappelijke kennissen heeft.

In het dorpje Symetria is een bloeiend verenigingsleven. Er zijn 361 inwoners, die allen lid zijn van verscheidene clubs (verenigingen, groeperingen, etc.). Iedere club telt toevallig precies 19 leden. En, zeer toevallig, voor ieder tweetal dorpelingen is er precies 1 club waar beiden lid van zijn. Hoeveel clubs zijn er en van hoeveel clubs is de heer X lid?

Stel r_X is het aantal clubs waarvan X lid is. Iedere club waarvan X lid is, heeft 18 andere leden. Uit het gegeven over de tweetallen dorpelingen volgt dat de $18r_X$ clubgenoten van X precies de hele populatie omvatten (behalve X zelf), dus $18r_X = 360$.
Hieruit volgt $r_X = 20$, onafhankelijk van X.

Stel b is het totale aantal clubs. Iedereen is lid van 20 clubs, zodat het aantal "lidmaatschappen" gelijk is aan 20×361. Omdat iedere club 19 leden heeft, is b gelijk aan $20 \times 161/19 = 380$.

OPGAVE 3. Vervang in het Symetria-voorbeeld de getallen 361, 19, 1 door v,k,λ en bepaal opnieuw b en r_X.

§2. INCLUSIE EN EXCLUSIE

In Symetria vinden we 81 personen die erelid zijn van een of andere vereniging. Verder zijn er 40 honoraire leden. Hoeveel dorpelingen moeten beide titels ontberen? Als we deze vraag beantwoorden met: 361 - 81 - 40 = 240, hebben we geen rekening gehouden met mensen die beide titels dragen. Inderdaad zijn er 10 Symetrianen die zowel erelid als honorair lid zijn, zodat 250 het juiste antwoord is.

Het gevraagde aantal wordt dus bepaald door uit te gaan van het aantal elementen in de hele verzameling, hiervan af te trekken wat niet aan de eis voldoet (exclusie), en daar weer bij op te tellen wat dubbel is afgetrokken (inclusie).

We geven nu een wat algemener voorbeeld. A, B, C zijn deelverzamelingen van een verzameling V. De aantallen $|V|$, $|A|$, $|B|$, $|C|$ zijn bekend, evenals de aantallen in de doorsneden $|AB|$, $|AC|$, $|BC|$, $|ABC|$. Hoeveel elementen van V liggen buiten $A \cup B \cup C$? Het antwoord luidt:

$$|V| - (|A| + |B| + |C|) + (|AB| + |AC| + |BC|) - |ABC|.$$

BEWIJS. Een element dat tot A behoort wordt netto 0 maal geteld, immers voor iedere term waar A in voorkomt bestaat een corresponderende term, met tegengesteld teken, waar A niet in voorkomt. Iets dergelijks geldt voor de elementen die tot B of C behoren. Een element dat niet tot A, B, of C behoort, wordt precies 1 maal geteld, zoals ook de bedoeling is. □

We generaliseren nu naar een verzameling V met n deelverzamelingen $A_1,\ldots,A_n$. Voor iedere groep van r indices $i_1,\ldots,i_r$ is het aantal $N_{i_1,\ldots,i_r} = |A_{i_1}\ldots A_{i_r}|$ gegeven. Laat S_r de som zijn van alle N's met r indices en Q_r het aantal elementen van V dat tot precies r der verzamelingen $A_1,\ldots,A_n$ behoort. Dan geldt:

(1) $$S_r = \sum_{j \geqslant r} \binom{i}{r} Q_i ,$$

(2) $$Q_r = \sum_{j \geqslant r} (-1)^{j+r} \binom{j}{r} S_j .$$

BEWIJS. Een element van V dat tot precies i der verzamelingen $A_1,\ldots,A_n$ behoort, zal alleen dan een bijdrage aan S_r leveren als $i \geqslant r$. De grootte van deze bijdrage is $\binom{i}{r}$, immers er zijn $\binom{i}{r}$ r-tallen waarin zo'n element meetelt. Hiermee is (1) bewezen.

Om (2) te bewijzen, vatten we (1) op als een stelsel van n + 1 lineaire vergelijkingen met de onbekenden $Q_0,Q_1,\ldots,Q_n$. Het stelsel is driehoekig en heeft dus hoogstens 1 oplossing. Het is nu voldoende om te laten zien dat (2) voldoet aan (1). Welnu:

$$\sum_{i \geqslant r} \binom{i}{r} Q_i = \sum_{i \geqslant r} \binom{i}{r} \sum_{j \geqslant i} (-1)^{j+i} \binom{j}{i} S_j =$$

$$\sum_{j \geqslant r} (-1)^j S_j \sum_{i=r}^{j} (-1)^i \binom{i}{r} \binom{j}{i} =$$

$$\sum_{j \geqslant r} (-1)^j \binom{j}{r} S_j \sum_{i=r}^{j} (-1)^1 \binom{j-r}{i-r} .$$

De binnenste som is 0 als $j > r$ en gelijk aan $(-1)^r$ als $j = r$. De hele uitdrukking is dus gelijk aan S_r, waarmee ook (2) bewezen is. □

Een interessant speciaal geval van (2) is r = 0:

(3) $$Q_0 = S_0 - S_1 + S_2 - \ldots \pm S_n .$$

Als toepassing hiervan bepalen we het aantal permutaties $(a_1,a_2,\ldots,a_n)$ van $\{1,2,\ldots,n\}$ met de eigenschap: $a_i \neq i$ voor $i = 1,2,\ldots,n$. Nu is V de verzameling van alle permutaties van $\{1,2,\ldots,n\}$, en A_i de verzameling van de permutaties met $a_i = i$. We kunnen het gevraagde aantal dan bepalen m.b.v. (3) als we de getallen S_r $(r = 0,\ldots,n)$ kennen. Eerst bepalen we

$|A_{i_1} \ldots A_{i_r}|$ voor een willekeurige rij $i_1,\ldots,i_r$ van r indices. Dit aantal is gelijk $(n-r)!$ Dus $S_r = \binom{n}{r}(n-r)! = \frac{n!}{r!}$, en het gevraagde aantal is

$$(4) \qquad D_n = n! \sum_0^n (-1)^r \frac{1}{r!} .$$

OPGAVE 4. Bereken $D_0, D_1, \ldots, D_7$.

OPGAVE 5. Formuleer een kans-theoretische versie van (1) en (2).

§3. RECURRENTE BETREKKINGEN

De grootheid D_n uit §2 kan ook op een geheel andere manier worden bepaald. Stel $n \geqslant 3$ en beschouw een permutatie $(a_1, a_2, \ldots, a_n)$ van $\{1,2,\ldots,n\}$ met $a_i \neq i$ voor $i = 1,2,\ldots,n$. Aangezien $a_n \neq n$, zijn voor de waarde van a_n precies $n-1$ mogelijkheden. Stel $a_n = i$. Beschouw nu a_i. We weten dat $a_i \neq i$; de resterende $n-1$ mogelijkheden verdelen we in twee klassen:

A) $a_i = n$. Nu staan de elementen i en n op elkaars plaats. Bij de overige $n-2$ elementen hebben we slechts te letten op de eis $a_j \neq j$ voor $n-2$ waarden van j. In deze klasse vinden we dus D_{n-2} permutaties (voor iedere i).

B) $a_i \neq n$. We hebben nu te maken met de *plaatsen* $1,2,\ldots,n-1$ en de *elementen* $1,\ldots,i-1, n, i+1,\ldots,n-1$. De restricties zijn: $a_j \neq j$ voor $j=1,\ldots,n-1$ en bovendien $a_i \neq n$. De laatste eis kunnen we in de plaats van $a_i \neq i$ zetten, immers $a_n = i$, zodat $a_i \neq i$ vanzelf geldt. Het aantal permutaties in deze klasse is dus D_{n-1} (voor iedere i).

Samenvattend zien we dat de rij D voldoet aan de volgende betrekking (die overigens al voor $n \geqslant 2$ geldt):

$$(5) \qquad D_n = (n-1)\,(D_{n-1}+D_{n-2}).$$

Met deze *recurrente betrekking* kan D_n blijkbaar worden bepaald zodra D_{n-1} en D_{n-2} bekend zijn. Men kan de betrekking samen met de waarden van D_0 en D_1 opvatten als een manier om de rij te geven, te definiëren. De overgang van de vorm (5) naar de vorm (4) noemt men het *oplossen* van de recurrente betrekking.

<u>OPGAVE 6</u>. Laat zien dat D voldoet aan $D_n = n\,D_{n-1} + (-1)^n$.

Een bekend voorbeeld van een rij die gewoonlijk d.m.v. een recurrente betrekking wordt gedefinieerd, is de rij van Fibonacci: $f_0 = 0$, $f_1 = 1$,

(6) $$f_n = f_{n-1} + f_{n-2} \qquad (n \geq 2).$$

Deze formule is bij uitstek geschikt om bijv. $f_2,\ldots,f_{20}$ te bepalen. Voor het beantwoorden van bepaalde andere vragen over de rij van Fibonacci is een expliciete formule beter geschikt. Het is dus wenselijk een methode te hebben voor het oplossen van recurrente betrekkingen. In de volgende paragraaf wordt zo'n methode geschetst.

§4. GENERERENDE FUNKTIES

Stel $a_0,a_1,\ldots$ is een rij, t is een reëel getal en stel de reeks

(7) $$A(t) = \sum_0^\infty a_i t^i$$

is convergent. Dan heet A de *genererende funktie* van de rij $a_0,a_1,\ldots$. Het is niet onze bedoeling diep op het convergentie-aspekt in te gaan, we merken slechts op: als de reeks (7) convergeert voor $|t| = t_0$, dan convergeert hij voor alle t met $|t| < t_0$.

Als voorbeeld van het gebruik van genererende funkties lossen we de recurrente betrekking (6) op. We vermenigvuldigen beide leden met t^n en sommeren van n = 2 af:

(8) $$\sum_{n=2}^\infty f_n t^n = \sum_{n=2}^\infty f_{n-1}\, t^n + \sum_{n=2}^\infty f_{n-2}\, t^n.$$

We voeren nu $F(t) := \sum_{n=0}^\infty f_n t^n$ in en we schrijven (8) als een betrekking in F:

(9) $$F(t) - f_0 - f_1 t = t\{F(t)-f_0\} + t^2 F(t).$$

Dit is een lineaire vergelijking in F(t) met als oplossing (bedenk dat $f_0 = 0$, $f_1 = 1$):

(10) $$F(t) = \frac{1}{1-t-t^2} .$$

De overgang van genererende funktie naar een expliciete formule noemt men *ontwikkelen*. Het principe hierbij is: omzetten van de genererende funktie in bekende funkties, d.w.z. funkties waarvan we al weten welke rij erbij hoort. In dit voorbeeld lukt die omzetting met behulp van *breuksplitsen*; het resultaat is:

$$F(t) = \frac{1}{\sqrt{5}} \left(\frac{1}{1-\alpha t} - \frac{1}{1-\beta t} \right)$$

met

$$\alpha = \frac{1+\sqrt{5}}{2} , \quad \beta = \frac{1-\sqrt{5}}{2} .$$

Aangezien $\sum_0^\infty c^n t^n = \frac{1}{1-ct}$, herkennen we $\frac{1}{1-\alpha t}$ als de genererende funktie van de rij $1,\alpha,\alpha^2,\ldots$ en omdat de som van twee genererende funkties de genererende funktie van de somrij is (termsgewijs), vinden we

$$f_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right\} .$$

Voor grote waarden van n is

$$\left(\frac{1-\sqrt{5}}{2}\right)^n$$

te verwaarlozen, en we vinden

(11) $$f_n \sim \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n .$$

Bijvoorbeeld, $f_{20} = 6765$ en (11) geeft $f_{20} \approx 6765{,}000029$.

In bovenstaand voorbeeld hadden we aan breuksplitsen en een somregel genoeg om de genererende funktie tot berekenbare vormen terug te brengen.
In de volgende opgave maken we kennis met enkele andere operaties.

OPGAVE 7. Als we weten welke reeks bij f(t) behoort, welke reeks behoort dan bij

a) $t^2 f(t)$,

b) $f(t^2)$,

c) $f(ct)$,

d) $\frac{f(t)}{1-t}$.

Het Fibonacci-voorbeeld diende voornamelijk om het oplossen van een recurrente betrekking m.b.v. genererende funkties te illustreren. Als bijprodukt vonden we het asymptotisch gedrag van de rij (formule 11). Als we echter alleen in het asymptotisch gedrag zijn geïnteresseerd, is er wel een kortere weg. We illustreren de methode, zonder bewijs, aan de hand van het volgende voorbeeld.

Beschouw de rijen a, c, c*, f gedefinieerd door $a_2 = c_2 = 1$, $c_2^* = f_2 = 0$ en

$$
\begin{aligned}
a_{m+1} &= c_m + 2c_m^* + f_m , \\
c_{m+1} &= c_m + 2c_m^* , \\
c_{m+1}^* &= a_m + c_m^* \\
f_{m+1} &= a_m .
\end{aligned}
\tag{12}
$$

OPMERKING. $a_m + c_m^*$ is het aantal Hamilton-cykels in $P_4 \times P_m$

Men kan nu in (12) substitueren $a_m = \alpha\lambda^m$, $c_m = \gamma\lambda^m$, $c_m^* = \gamma^*\lambda^m$ en $f_m = \phi\lambda^m$. Het resultaat is, na deling door λ^m:

$$
\begin{aligned}
\alpha\lambda &= \gamma + 2\gamma^* + \phi, \\
\gamma\lambda &= \gamma + 2\gamma^* , \\
\gamma^*\lambda &= \alpha + \gamma^* , \\
\phi\lambda &= \alpha.
\end{aligned}
\tag{13}
$$

Dit is een stelsel van 4 lineaire homogene vergelijkingen met 4 onbekenden $(\alpha,\gamma,\gamma^*,\phi)$. Het stelsel heeft een oplossing (ongelijk aan de nuloplossing) als de determinant 0 is. Na uitschrijven leidt dit tot

$$\lambda^4 - 2\lambda^3 - 2\lambda^2 + 2\lambda - 1 = 0,$$

de zgn. karakteristieke vergelijking van het stelsel (12). De wortel die in absolute waarde het grootst is, geeft aan hoe de rijen a,c,c^*, f zich asymptotisch gedragen. In het bijzonder geldt

$$a_m + c_m^* \sim b.\lambda_0^m$$

waarin b en λ_0 constanten zijn met $\lambda_0 \doteq 2{,}53865$.

Genererende funkties kunnen ook met vrucht worden gebruikt bij het bewijzen van bepaalde identiteiten. Bijvoorbeeld, de identiteit

$$\sum_i \binom{a}{i}\binom{b}{k-i} = \binom{a+b}{k}$$

volgt direkt uit de relatie $(1+t)^a(1+t)^b = (1+t)^{a+b}$ en het binomium van Newton. Immers, de coëfficiënt van t^k in het rechterlid is $\binom{a+b}{k}$ en in het linkerlid

$$\sum_{i+j=k} \binom{a}{i}\binom{b}{j}$$

§5. CATALAN-GETALLEN

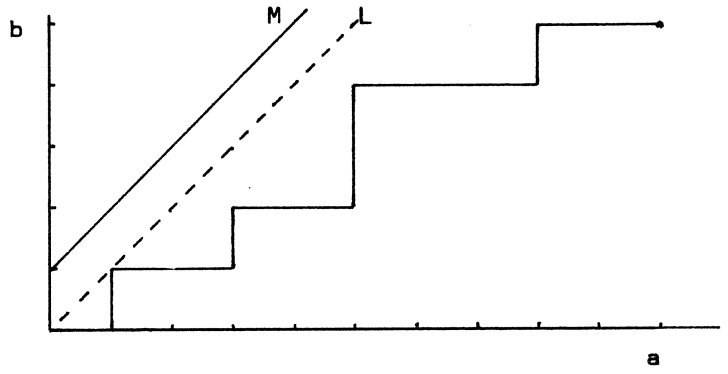
Bij een stemming over twee kandidaten A en B krijgt A in totaal a stemmen en B b stemmen, waarbij $a > b$. Wat is de kans dat A gedurende het tellen van de stemmen steeds een minstens even groot aantal stemmen heeft als B?

Als we de aantallen stemmen op A en B na n getelde stemmen aanduiden met a_n resp. b_n, dan kunnen we de gevraagde kans schrijven als

$$P\{a_n \geqslant b_n \ (n = 1,\ldots,a+b)\}.$$

We nemen aan dat alle (a+b)! volgorden van de stembriefjes even waarschijnlijk zijn.

Het probleem kan worden opgelost m.b.v. een *spiegelingsprincipe*. In onderstaande figuur zijn de punten (a_n,b_n) steeds door lijnstukken van de lengte 1 verbonden. Op deze wijze ontstaat een pad van (0,0) naar (a,b).



De gebeurtenis "$a_n \geqslant b_n$ voor $n = 1,\ldots,a+b$" treedt dan en slechts dan op als het pad niet boven de gestreepte lijn L uit komt. Een pad dat niet aan deze eis voldoet zal ergens de lijn M (zie figuur) raken of snijden. Stel dit gebeurt voor het eerst in het punt S. Dan kunnen we het pad van S tot aan het eindpunt spiegelen t.o.v. de lijn M. We krijgen dan een pad van (0,0) naar (b-1,a+1). Sterker nog: er is een 1-1-verband tussen de paden van (0,0) naar (a,b) die de lijn M snijden of raken enerzijds en de paden van (0,0) naar (b-1,a+1) anderzijds. Het aantal in ieder van deze klassen is dus gelijk aan $\binom{b-1+a+1}{a+1} = \binom{a+b}{a+1}$. Het aantal paden dat niet boven L uitkomt is dus

$$\binom{a+b}{a} - \binom{a+b}{a+1} .$$

Wat kan worden herleid tot

$$\frac{a+1-b}{a+1}\binom{a+b}{a} \tag{14}$$

De gevraagde kans is dus $\frac{a+1-b}{a+1}$.

In het speciale geval a = b gaat (14) over in

$$\frac{1}{a+1}\binom{2a}{a} ,$$

het a-de getal van Catalan.

<u>OPGAVE 8</u>. Bepaal het aantal manieren waarop we n haakjes-openen en n haakjes-sluiten zo kunnen ordenen dat een zinvolle rij van haakjes ontstaat.

We bepalen nu het aantal paden van (0,0) naar (a,b) dat niet boven de lijn L uitkomt, met behulp van een recurrente betrekking. We beperken ons tot het geval a = b = n.

Het totale aantal paden waarin de eerste stap horizontaal is, is $\binom{2n-1}{n}$.
Deze paden kunnen we verdelen in twee klassen:
a) paden die niet boven L uit komen,
b) paden die na k+1 stappen voor het eerst boven L uit komen, voor zekere k.
Het aantal paden in klasse a) is gelijk aan het "onbekende" aantal, dat we c_n noemen. Het aantal paden in klasse b) is gelijk aan

$$\sum_{k=1}^{n-1} c_k \binom{2n-2k-1}{n-k},$$

immers het aantal paden tot en met de k^e stap is c_k, en het aantal paden na de $(k+1)^e$ stap is $\binom{2n-2k-1}{n-k}$.
Zo vinden we de recurrente betrekking

$$\binom{2n-1}{n} = c_n + \sum_{k=1}^{n-1} c_k \binom{2n-2k-1}{n-k}.$$

Dus is (voor $|t| < \frac{1}{4}$):

$$\sum_{n=1}^{\infty} \binom{2n-1}{n} t^n = \sum_{n=1}^{\infty} c_n t^n + \sum_{n=2}^{\infty} \sum_{k=1}^{n-1} c_k \binom{2n-2k-1}{n-k} t^n \tag{15}$$

We voeren nu in $f(t) = \sum_{1}^{\infty} \binom{2n-1}{n} t^n$ en $c(t) = \sum_{1}^{\infty} c_n t^n$.

Na omkering van de sommatie-volgorde in de laatste som van (15) vinden we:

$$f(t) = c(t) + c(t).f(t),$$

zodat we c(t) in f(t) kunnen uitdrukken: $c(t) = \frac{f(t)}{1+f(t)}$.

OPGAVE 9. Bewijs dat $f(t) = \frac{1}{2}(1-4t)^{-\frac{1}{2}} - \frac{1}{2}$ met behulp van het gegeneraliseerde binomium van Newton:

$$(1+t)^{\alpha} = \sum_{n=0}^{\infty} \binom{\alpha}{n} t^n \text{ voor reële } \alpha.$$

Met het resultaat van opgave 9 vinden we dan

$$c(t) = \frac{1-2t-\sqrt{1-4t}}{2t} = \sum_{n=2}^{\infty} \binom{\frac{1}{2}}{n} (-1)^{n-1}\, 2^{2n-1}\, t^{n-1}$$

waarmee we tenslotte vinden

$$c_n = (-1)^n \binom{\frac{1}{2}}{n+1} 2^{2n+1}.$$

§6. PERMANENTEN

Als A een n x n-matrix is met elementen a_{ij}, dan is de permanent van A, notatie per(A), per definitie het getal

$$\Sigma^* a_{1i_1} a_{2i_2} \cdots a_{ni_n}, \tag{16}$$

waarbij wordt gesommeerd over alle permutaties $i_1, i_2, \ldots, i_n$ van $\{1,2,\ldots,n\}$. Bijvoorbeeld, als n = 2 en $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dan is per(A) = ad + bc. Of, als n willekeurig is en $a_{ij} = 1$ voor alle i en j, dan is per(A) = n!, immers in (16) zijn alle termen gelijk aan 1 en het aantal termen is n!

OPGAVE 10. Neem $a_{ij} = 1$ en $a_{ii} = 0$. Bepaal per(A).

Een n x n-matrix A waarvan alle elementen 0 of 1 zijn, kan worden opgevat als een representatie van een bipartiete graaf. De rijen corresponderen met de punten $\{p_1,\ldots,p_n\}$, de kolommen met de andere punten $\{q_1,\ldots,q_n\}$; als het matrixelement a_{ij} gelijk is aan 1, dan is p_i buur van q_j en omgekeerd. De permanent van zo'n matrix is het aantal *perfecte matchings* van de graaf. We beschouwen nu het speciale geval van een 0-1-matrix A waarin iedere rijsom en iedere kolomsom gelijk is aan 3. Voor de bijbehorende bipartiete graaf G betekent dit dat hij 3-regulier is. Uit de huwelijksstelling van

Hall volgt dat zo'n graaf minstens 1 perfecte matching heeft, dus per(A) $\geqslant 1$. Men vermoedde al jarenlang dat per(A) minstens een exponentiële funktie van n is. Uit het vermoeden van van der Waerden (van iedere dubbel-stochastische $n \times n$-matrix is de permanent $\geqslant n!\, n^{-n}$) zou dit direkt volgen. In 1971 bewezen Hartfiel en Crosby dat per(A) $\geqslant 3n-3$. Pas in 1978 gelukte het aan M. Voorhoeve de exponentiële ondergrens te bewijzen. Met elementaire methoden vond hij

$$\mathrm{per}(A) \geqslant 6\left(\tfrac{4}{3}\right)^{n-3}.$$

LITERATUUR

Raghavarao, D., Constructions and Combinatorial Problems in Design of Experiments, Wiley, Toronto, 1971.

Feller, W., An Introduction to Probability Theory and Its Applications, Wiley, Toronto, 1950.

Voorhoeve, M., A Lower Bound for the Permanents of Certain (0,1)-Matrices, Proc. of the Kon.Ned.Akad.Wetenschap., Series A, 82 (1979) 83-86.

WOORDEN TELLEN
(toepassingen in de coderingstheorie)

H.C.A. van Tilborg

Aangezien codes gedefinieerd zijn in vectorruimtes over een eindig lichaam, zullen we ons eerst even met eindige lichamen gaan bezighouden.

DEFINITIE 1. Een *lichaam* (R,+,) bestaat uit een niet lege verzameling R met daarop twee operaties (optelling en vermenigvuldiging genoemd) gedefinieerd, die voldoen aan de volgende eigenschappen:

i) (R,+) is een abelse groep (waarvan we het eenheidselement met 0 aanduiden,

ii) (R\{0},) is een groep (waarvan we het eenheidselement met 1 aanduiden).

VOORBEELDEN: $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{C}$; $\mathbb{F}_p = \mathbb{Z}$ (mod p), p priem.

DEFINITIE 2. Een *eindig lichaam* is een lichaam met eindig veel elementen. Als het lichaam q elementen heeft duiden we het aan met $\mathbb{F}_q$.

De belangrijkste eigenschappen van eindige lichamen vermelden we hier zonder bewijs (zie [1])

- $q = p^r$ met p priem. Het getal p heet de karakteristiek van het lichaam $\mathbb{F}_q$. Het lichaam $\mathbb{F}_q$ bevat $\mathbb{F}_p$ als een deellichaam.
- $(\mathbb{F}_q\backslash\{0\},)$ is een cyclische groep.
- $\mathbb{F}_q$ is op isomorfie na eenduidig bepaald.
- $\mathbb{F}_q$ bestaat voor alle $q = p^r$, $r \geq 1$, p priem.

Zij $V_n(q)$ een n-dimensionale vectorruimte over $\mathbb{F}_q$, $q = p^r$, p priem.

DEFINITIE 3. Het *gewicht* w(x) van een vector $\underline{x}$ in $V_n(q)$ en de *afstand* $d(\underline{x},\underline{y})$ van twee vectoren $\underline{x}$ en $\underline{y}$ in $V_n(q)$ worden als volgt gedefinieerd:

$$w(\underline{x}) \quad := |\{1 \leqslant i \leqslant n | x_i \neq 0\}|,$$
$$d(\underline{x},\underline{y}) \quad := |\{1 \leqslant i \leqslant n | x_i \neq y_i\}|.$$

VOORBEELD. Zij $\underline{x} = (1,0,6,3)$ en $\underline{y} = (2,3,6,4)$ in $V_4(7)$. Dan geldt: $d(\underline{x},\underline{y})=3$, $w(\underline{x}) = 3$ en $w(\underline{y}) = 4$.

DEFINITIE 4. Een (n,M,d)-*code* C over $\mathbb{F}_q$ is een deelverzameling van grootte M in $V_n(q)$ met daarbij een *minimum afstand* d gedefinieerd door

$$d = \min\{d(\underline{c}_1,c_2) | \underline{c}_1 \in C,\ \underline{c}_2 \in C,\ \underline{c}_1 \neq \underline{c}_2\}.$$

Als C een lineaire deelruimte van $V_n(q)$ is met $M = q^k$ dan heet C een *lineaire code* en zeggen we dat C een [n,k,d]-code is.
De minimum afstand geeft aan hoe weinig verschillende codewoorden op elkaar lijken.

DEFINITIE 5. De *weight-enumerator* $\Sigma_{i=0}^{n} A_i z^i$ van een code C is gedefinieerd door:

$$A_i = |\{\underline{c} \in C | w(\underline{c}) = i\}|$$

We zullen verderop zien hoe de weight-enumerator behulpzaam kan zijn bij de bestudering van codes.

DEFINITIE 6. De *duale code* $C^{\perp}$ van een [n,k,d]-code C is de code

$$\{\underline{x} \in V_n(q) | \forall \underline{c} \in C\ [\sum_{i=1}^{n} c_i x_i = 0]\}.$$

Gemakkelijk is na te gaan dat $C^{\perp}$ een lineaire code van dimensie n-k. is en dat $(C^{\perp})^{\perp} = C$.

DEFINITIE 7. De *voortbrenger matrix* G van een [n,k,d]-code C is een $k \times n$ matrix waarvan de rijen C opspannen.

VOORBEELD. Zij C de [n,n-1,2]-code over $\mathbb{F}_2$ voortgebracht door:

$$G = \begin{pmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & \ddots & \vdots \\ & & 1 & 1 \end{pmatrix}$$

(de open posities zijn allemaal 0).

C heeft weight-enumerator

$$A_{2i+1} = 0, \qquad 0 \leqslant i \leqslant [\tfrac{n-1}{2}] ,$$

$$A_{2i} = \binom{n-1}{2i-1} + \binom{n-1}{2i} = \binom{n}{2i}, \quad 0 \leqslant i \leqslant [\tfrac{n-1}{2}]$$

en wordt de *evenweight code* genoemd.
De duale code $C^{\perp}$ wordt voortgebracht door

$$H = (1\ 1\ \ldots\ 1\ ).$$

Hij bevat slechts 2 codewoorden nl. (0,0,...,0) en (1,1,...,1) en wordt derhalve de *repetitie code* genoemd.
Een gemakkelijk af te leiden bovengrens aan de grootte van een (n,M,d) code wordt gegeven door de volgende stelling.

STELLING 8 (Singleton). *Zij* C een (n,M,d)-code over $\mathbb{F}_q$ dan geldt:

$$M \leqslant q^{n-d+1}$$

i.h.b. geldt voor lineaire codes dat $d \leqslant n-k+1$.

BEWIJS. Als 2 codewoorden op een gegeven (n-d+1)-tal posities overeenstemmen is hun afstand kleiner dan d. Derhalve zijn alle codewoorden op dit (n-d+1)-tal posities verschillend. □

DEFINITIE 9. Een [n,k,d]-code heet *optimaal* als d = n-k+1

STELLING 10. *Een* [n,k,d]-*code C is optimaal d.e.s.d. als elk* (n-k)-*tal kolommen van de voortbrenger matrix* H *van* $C^{\perp}$ *onafhankelijk is.*

BEWIJS. Dit volgt uit

$$\underline{c} \in C \Longleftrightarrow H\underline{c} = \underline{0}. \quad \square$$

STELLING 11. *Als een* [n,k,d]-*code C optimaal is dan is ook zijn duale code* $C^{\perp}$ *optimaal met parameters* $[n,n-k,d^{\perp}]$, $d^{\perp} = k+1$.

BEWIJS. Op grond van stelling 8 geldt $d^{\perp} \leqq k+1$. Stel nu dat $C^{\perp}$ een codewoord $\underline{c}$ bevat van gewicht $\leqq k$, i.e. met $\geqq (n-k)$ coördinaten gelijk aan 0. Dan heeft de voortbrenger matrix H van $C^{\perp}$ n-k kolommen (corresponderend met (n-k) coördinaten waar $\underline{c}$ nul is) die afhankelijk zijn. Dit is in tegenspraak met stelling 10. $\square$

STELLING 12. *Zij* C *een* [n,k,d]-*code. Dan zijn de volgende uitspraken equivalent.*

i) C *is optimaal,*

ii) $C^{\perp}$ *is optimaal,*

iii) *elk* k-*tal kolommen van de voortbrenger matrix van* C *is onafhankelijk*

iv) *elk* (n-k)-*tal kolommen van de voortbrenger matrix van* $C^{\perp}$ *is onafhankelijk.*

BEWIJS. Dit is een rechtstreeks gevolg van stellingen 10 en 11. $\square$

STELLING 13. *Zij* C *een optimale* [n,k,d]-*code met weight-enumerator* A_i, $0 \leqq i \leqq n$. *Dan geldt*

i) $A_d = \binom{n}{k-1}(q-1)$,

ii) $A_{d+1} = \binom{n}{k-2}(q-1)(q-n+k-1)$.

BEWIJS. i) Het aantal codewoorden ongelijk aan $\underline{0}$ die een 0 hebben op een gegeven (k-1)-tal coördinaten is op grond van de minimum afstand van C hooguit q-1 nl. een codewoord met al zijn veelvouden, en op grond van stelling 12 iv) minimaal q-1 nl. een codewoord met al zijn veelvouden. Derhalve geldt i).

ii) Het aantal codewoorden ongelijk aan $\underline{0}$ in C die een 0 hebben op een gegeven (k-2)-tal coördinaten is evenzo $(q-1)^2$. Sommatie over alle (k-2)-tallen coördinaten levert dus

$$\binom{n}{k-2}(q-1)^2.$$

Anderzijds levert dit elk codewoord van gewicht d precies $\binom{k-1}{k-2}$ keer en elk woord van gewicht d+1 precies 1 keer. Derhalve geldt

$$\binom{k-1}{k-2} A_d + A_{d+1} = \binom{n}{k-2}(q-1)^2.$$

Substitutie van i) levert nu ii). □

STELLING 14. *Zij C een optimale* [n,k,d]-*code over* $\mathbb{F}_q$, *dan geldt:*

i) $k \geqslant 2 \Rightarrow q \geqslant n-k+1$,

ii) $k \leqslant n-2 \Rightarrow q \geqslant k+1$.

BEWIJS. Dit volgt uit stelling 13 ii) toegepast op C en $C^{\perp}$. □

Bovenstaande stelling illustreert het belang van de weight-enumerator bij de bestudering van codes. We geven nog een ander voorbeeld van het bepalen van de weight-enumerator van een code.

STELLING 15. (Hamming). *Zij* C *een* (n,M,d)-*code over* $\mathbb{F}_q$ *en zij* $e = [\frac{d-2}{2}]$ *dan geldt*

$$M \cdot \sum_{i=0}^{e} \binom{n}{i}(q-i)^i \leq q^n.$$

BEWIJS. Bollen met straal e rond de codewoorden snijden elkaar niet. Hun volume is

$$\sum_{i=0}^{e} \binom{n}{i}(q-1)^i. \quad \square$$

DEFINITIE 16. Een (n,M,d)-code C heet *perfect* als

$$|C| \cdot \sum_{i=0}^{e} \binom{n}{i}(q-1)^i = q^n,$$

m.a.w. als elke vector $\underline{x}$ in $V_n(q)$ in een unieke bol van straal e rond een codewoord ligt.

STELLING. *Zij C een perfecte binaire code met* d = 3 *en met weight-enumerator* $\Sigma_{i-0}^{n} A_i z^i$. *Zij* $\underline{0} \in C$, *dan geldt*

$$A(z) = \frac{1}{n+1}\{(1+z)^n + n(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}\}.$$

BEWIJS. Daar elk woord van gewicht w op afstand $\leqq 1$ van een uniek codewoord ligt, is het zelf een codewoord of ligt het op afstand 1 van een codewoord van gewicht w-1 of w+1. Derhalve geldt:

$$\binom{n}{w} = A_w + (n-w+1)A_{w-1} + (w+1)A_{w+1}$$

Als we nu definiëren $A_{-\ell} = A_{n+\ell} = 0$, $\ell \geqq 1$, dan geldt (*) voor alle $w \in N$. Vermenigvuldiging van (*) met z^w, gevolgd door een sommatie over alle waarden van w levert

$$(1+z)^n = \Sigma_w A_w z^w + nz \sum_w A_{w-1} z^{w-1} - z^2 \sum_w (w-1) A_{w-1} z^{w-2} +$$

$$\sum_w (w+1) A_{w+1} z^w$$

i.e.

$$(1+z)^n = A(z) + nzA(z) - z^2A'(z) + A'(z).$$

Dit levert de eerste orde differentiaal vergelijking

$$(1-z^2)A'(z) = (1+z)^n - (1+nz)A(z),$$

waarvan de algemene oplossing is

$$A(z) = \frac{(1+z)^n}{n+1} + \alpha(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}.$$

Daar $A(0) = A_0 = 1$ geldt $\alpha = \frac{n}{n+1}$. Dit bewijst de stelling. □

LITERATUUR

[1] *Berlekamp,E.R.*, Algebraic coding theory, McGraw-Hill, New York 1968.

[2] *Cameron,P.J. & J.H. van Lint*, Graph theory, coding theory and block designs, London Math. Soc. Lecture Note Series, No.19, Cambridge University Press, London, 1975.

[3] *Van Lint, J.H.*, Coding theory, Lecture Notes in Mathematics 201, Springer Verlag, Berlin etc., 1971.

[4] *Van Lint, J.H.*, Inleiding in de coderingstheorie, MC syllabus 31, Mathematisch Centrum, Amsterdam, 1976.

[5] *Van Lint, J.H.*, Introduction to coding theory, Graduate Texts in Mathematics 86, Springer Verlag, New York etc., 1982.

DE STELLING VAN POLYA, MET TOEPASSING OP HET TELLEN VAN BOMEN EN BOOMVORMIGE MOLEKULEN

N.G. de Bruijn

§1. Inleiding.

Het overgrote deel van deze voordracht is afkomstig uit Polya's beroemde artikel [7] uit 1937. Wij behandelen hier de hoofdstelling (stelling 5.1) en in §7 de toepassing op het tellen van molekulen. Voor een uitvoerige presentatie van de hoofdstelling en uitbreidingen zij verwezen naar [1]. De in §6 beschouwde uitbreiding is daar niet te vinden, wel in [2] en [5]. Een gemakkelijk leesbare formele behandeling van de molekuultellingen is nooit gegeven. Men zie (ook voor uitbreiding) [3], en voor informele behandeling [4] en [7].

§2. Permutaties.

Laat V een niet-lege eindige verzameling zijn. Het aantal elementen wordt door $|V|$ voorgesteld. Een *permutatie* van V is niets anders dan een bijectie $V \to V$. De verzameling van de permutaties heet S_V. Dus $|S_V| = |V|!$.

Als $p_1 \in S_V$, $p_2 \in S_V$ dan is het *product* p_1p_2 gedefinieerd als de samengestelde afbeelding: $(p_1p_2)(v) = p_1(p_2(v))$ voor alle $v \in V$. Met deze productdefinitie is S_V een *groep*.

Als $p \in S_V$ dan is V daardoor in cyclen gesplitst. Een *cyclus* is een stel verschillende elementen $v_1,\ldots,v_k$ met

$$p(v_1) = v_2, \quad p(v_2) = v_3,\ldots,p(v_k) = v_1.$$

Het getal k heet de *lengte* van de cyclus. Laat $b_k(p)$ het aantal cyclen voorstellen met lengte k. Dus $\sum_{k=1}^{\infty} kb_k(p) = |V|$. De vector $(b_1(p), b_2(p), b_3(p), \ldots)$ wordt het *type* van V genoemd.

Terzijde vermelden we dat p_1 en p_2 d.e.s.d. hetzelfde type hebben als er een $q \in S_V$ bestaat met $qp_1q^{-1} = p_2$. Een ook dat het aantal $p \in S_V$ waarvan het type gelijk is aan de gegeven vector $(b_1,b_2,\ldots)$ (met b_k geheel, $b_k \geqq 0$, $\Sigma kb_k = |V|$) bedraagt

$$\frac{|V|!}{b_1!\ 1^{b_1}\ b_2!\ 2^{b_2}\ b_3!\ 3^{b_3}\ldots}$$

§3. Representaties van een groep d.m.v. permutaties.

Laat G een eindige groep zijn, V een niet-lege eindige verzameling en ρ een *representatie* van G d.m.v. permutaties van V. Dit betekent dat ρ een homomorfe afbeelding is van G in S_V:

$$\rho(g_1g_2^{-1}) = \rho(g_1).(\rho(g_2))^{-1} \qquad (g_1 \in G,\ g_2 \in G)$$

(in het bijzonder gaat het eenheidselement van G in de identieke permutatie over).

<u>VOORBEELD 3.1</u>. G is de groep van alle 24-ruimte-draaiingen die de eenheidskubus invariant laten. Als $g \in G$, dan wordt door g de verzameling V der 12 ribben gepermuteerd; deze permutatie noemen we $\rho(g)$.

Ten bate van allerlei combinatorische vragen zijn we geïnteresseerd in een inventaris van de typen $(b_1(\rho(g)), b_2(\rho(g)),\ldots)$. We beschrijven die met een voortbrengende functie door variabelen $x_1, x_2, x_3, \ldots$ te kiezen en een type $(b_1, b_2, \ldots)$ te associëren met een term $x_1^{b_1}x_2^{b_2}\ldots$ (we nemen niet de moeite om de slotfactor van

zo'n product te noteren, en schrijven het hier als een oneindig product). Het gemiddelde ervan, genomen over de groep, heet de *cyclenindex*:

$$P_{G,\rho}(x_1,x_2,\ldots) = \frac{1}{|G|} \sum_{g \in G} x_1^{b_1(\rho(g))} x_2^{b_2(\rho(g))} \ldots$$

VOORBEELD 3.2. Bij de zoëven genoemde kubusdraaiingen met representatie d.m.v. de *ribben* is

$$P_{G,\rho} = \frac{1}{24}(x_1^{12} + 3x_2^6 + 6x_4^3 + 6x_1^2x_2^5 + 8x_3^4).$$

Doen we het t.a.v. de *hoekpunten* dan is

$$P_{G,\rho} = \frac{1}{24}(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2);$$

Doen we het t.a.v. de *zijvlakken* dan komt er

$$P_{G,\rho} = \frac{1}{24}(x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2).$$

VOORBEELD 3.3. Laat $G = S_V$, en ρ de triviale afbeelding ($\rho(g) = g$). Als $|V| = n$, dan is $P_{G,\rho}$ de coëfficiënt van z^n in de ontwikkeling van

$$\exp(zx_1 + \frac{z^2x_2}{2} + \frac{z^3x_3}{3} + \ldots).$$

OPMERKING 3.4. Voor elke G en ρ is

$$P_{G,\rho}(x, x^2, x^3, \ldots) = x^{|V|}.$$

§4. Lemma van Cauchy-Frobenius.

Laat G een eindige groep zijn, V een eindige verzameling, ρ een representatie van G d.m.v. permutaties van V.

De elementen v_1, v_2 van V heten *equivalent* (notatie $v_1 \sim v_2$) als er een $g \in G$ is met $\rho(g)v_1 = v_2$. Het *aantal* equivalentieklassen wordt uitgedrukt in het volgende lemma.

LEMMA 4.1 (Cauchy-Frobenius). (Ten onrechte vaak naar Burnside genoemd). *Laat (voor elke* $g \in G$*)* $\psi(g)$ *het aantal* $v \in V$ *voorstellen dat aan* $\rho(g)v = v$ *voldoet (dus* $\psi(g) = b_1(\rho(g))$*). Dan is het aantal equivalentieklassen*

$$\frac{1}{|G|} \sum_{g \in G} \psi(g).$$

BEWIJS. Als $v \in V$, $w \in V$ dan stelt $Z(v,w)$ voor: het aantal $g \in G$ met $\rho(g)v = w$.

De som $\sum_g \psi(g)$ is het aantal paren (g,v) met $\rho(g)v = v$, zodat

$$\sum_{g \in G} \psi(g) = \sum_{v \in V} Z(v,v).$$

Als v en w equivalent zijn dan is $Z(v,w) = Z(v,v)$, en anders $Z(v,w) = 0$. Bij elke v is $\sum_{w \in V} Z(v,w) = |G|$. Derhalve is $Z(v,v)$ gelijk aan $|G|/k(v)$, waarin $k(v)$ het aantal elementen is in de equivalentieklasse van v.

Het bewijs wordt nu beëindigd door de opmerking dat $\sum_{v \in V} (k(v))^{-1}$ gelijk is aan het aantal klassen.

Met een beetje meer moeite bewijst men de volgende uitbreiding ([6]).

LEMMA 4.2. *Laat* p *een permutatie van* V *zijn met de eigenschap dat uit* $v_1 \sim v_2$ *steeds* $pv_1 \sim pv_2$ *volgt. Een equivalentieklasse* K *heet* p*-invariant als er een* $v \in K$ *is met* $pv \in K$ *(in dit geval geldt het voor alle* $v \in K$*). Het aantal* p*-invariante equivalentieklassen bedraagt*

$$\frac{1}{|G|} \sum_{g \in G} \quad (\textit{aantal der } v \in V \textit{ met } \rho(g)v = pv).$$

BEWIJS. Fixeer een $w \in V$. Definieer $f(w) = 1$ als w in een p-invariante klasse ligt, en anders $f(w) = 0$. We berekenen

$$\sum_g \sum_{v \in V \mid v \sim w, \rho(g)v = pv} 1 =$$

$$= \sum_{v \in V \mid v \sim w} (\text{aantal } g \in G \text{ met } \rho(g)v = pv) =$$

$$= \sum_{v \in V \mid v \sim w} (\text{aantal } g \in G \text{ met } \rho(g)\rho(k)w = pv) =$$

$$= \sum_{v \in V \mid v \sim w} (\text{aantal } g \in G \text{ met } \rho(g)w = pv) =$$

$$= \sum_{g \in G} (\text{aantal } v \in V \text{ met } v \sim w \text{ en } \rho(g)w = pv) =$$

$$= f(w) \cdot \sum_{g \in G} (\text{aantal } v \in V \text{ met } \rho(g)w = pv) = f(w) \cdot |G|.$$

(De hierboven ingevoerde k is een element van G dat aan $\rho(k)w = v$ voldoet. En bij het voorlaatste gelijkteken is gebruikt dat uit $pv_1 \sim pv_2$ weer $v_1 \sim v_2$ volgt, op grond van het feit dat een macht van p de identiteit is).

Laat $V_1,\ldots,V_h$ de equivalentieklassen zijn. Kies in elke V_j een w_j. Het aantal p-invariante klassen is $f(w_1) + \ldots + f(w_h)$. Door de bovenbereikte gelijkheid voor $w = w_1,\ldots,w_h$ op te stellen en te sommeren, volgt het lemma na de opmerking dat elke v met precies één w_j equivalent is.

§5. De stelling van Polya.

Laat D en R eindige verzamelingen zijn. De elementen van R zullen we *kleuren* noemen, de afbeeldingen f van D in R heten *kleuringen*. Verder is G een eindige groep, en ρ een representatie van G d.m.v. permutaties van D.

Twee kleuringen f_1, f_2 heten *equivalent* als er een $g \in G$ is met $f_1 = f_2 \cdot \rho(g)$. Een equivalentieklasse heet een *kleurpatroon*.

We kennen aan elke kleur r een *gewicht* w_r toe. De w_r's zijn gekozen uit een commutatieve algebra A over de rationele getallen. De w_r's zouden dus ook *variabelen* kunnen zijn.

Aan kleuring f kennen we als gewicht toe

$$W(f) = \prod_{d \in D} w_{f(d)}.$$

Equivalente kleuringen hebben hetzelfde gewicht. We kennen dit gewicht ook aan de patronen toe: als F een patroon, en $f \in F$ dan

stellen we $W(F) = W(f)$.

STELLING 5.1 (Polya). *De som van de gewichten van de kleurpatronen bedraagt*

$$P_{G,\rho}(\sum_{z\in R} w_r, \sum_{z\in R} w_r^2, \sum_{z\in R} w_r^3, \ldots).$$

BEWIJS. De verzameling van alle kleuringen stellen we door R^D voor. We definiëren een representatie τ van G d.m.v. permutaties van R^D door

$$\tau(g)f = f.(\rho(g))^{-1}.$$

De kleuringen f_1 en f_2 zijn d.e.s.d. equivalent als er een $g \in G$ bestaat met $\tau(g)f_1 = f_2$.

Laat q een element van de algebra A zijn, en V_q de verzameling der $f \in R^D$ met $W(f) = q$. V_q is de vereniging van een stel patronen. Het aantal dezer patronen wordt gevonden met behulp van de stelling van Cauchy-Frobenius

$$\frac{1}{|G|} \sum_{g\in G} \psi_q(g),$$

waarin $\psi_q(g)$ het aantal $f \in V_q$ is met $\tau(g)f = f$. Sommeren we dit over alle mogelijke $q \in A$ dan vinden we dat de som der gewichten van de patronen bedraagt

$$\frac{1}{|G|} \sum_{g\in G} \Psi(g),$$

waarin $\Psi(g)$ gewichtsom is der $f \in R^D$ met $\tau(g)f = f$, d.w.z. met $f = f.\rho(g)$.

Een $f \in R^D$ voldoet aan $f = f.\rho(g)$ d.e.s.d. als f constant is op elke cyclus die $\rho(g)$ in D genereert. Geven we het type van $\rho(g)$ aan met $(b_1,b_2,\ldots)$ dan zien we dat

$$\Psi(g) = (\Sigma\, w_r)^{b_1}(\Sigma\, w_r^2)^{b_2}(\Sigma\, w_r^3)^{b_3}\ldots,$$

d.i. het resultaat van de substituties $x_1 = \Sigma w_r$, $x_2 = \Sigma w_r^2$ ... in de

term $x_1^{b_1(\rho(g))}x_2^{b_2(\rho(g))}\ldots$ van de cyclenindex $P_{G,\rho}$. Sommatie over g levert nu de stelling van Polya.

VOORBEELD 5.2. We kleuren de zijvlakken van een kubus. Er zijn drie kleuren, rood, wit en blauw, beschikbaar. We eisen dat 3 zijvlakken rood, 2 wit en 1 blauw wordt. Twee kleuringen worden tot hetzelfde kleurpatroon gerekend als de ene door een draaiing van de kubus in de andere overgaat. Hoeveel van zulke patronen zijn er? We hechten aan de kleuren als gewichten de variabelen r, w, b. De som der gewichten van alle patronen is een veelterm waarvan we alleen de coëfficiënt van r^3w^2b willen hebben. Het antwoord is dus: de coëfficient van r^3w^2b uit

$$\frac{1}{24}\left((r + w + b)^6 + 3(r + w + b)^2(r^2 + w^2 + b^2)^2\right)$$

(want de termen $x_1^2x_4$, x_2^3 en x_3^2 uit de cyclenindex geven hier geen bijdrage). De uitkomst is 3. Deze drie patronen zijn hier nog gemakkelijk door inspectie te verkrijgen:

1° kleuringen met 3 rode zijvlakken die in één punt samenkomen.

2° grondvlak rood, bovenvlak wit, opstaande zijvlakken rondgaande rood, blauw, rood, wit.

3° grondvlak rood, bovenvlak blauw, opstaande zijvlakken rondgaande rood, wit, rood, wit.

§6. Een uitbreiding van de stelling van Polya.

We noemen een uitbreiding, waarbij we ons terwille van de eenvoud beperken tot het geval dat alle gewichten 1 zijn.

Laat q een vaste permutatie van R zijn. Een patroon F heet q-invariant als voor alle $f \in F$ geldt dat $q.f \in F$.

STELLING 6.1. *Het aantal* q*-invariante patronen bedraagt*

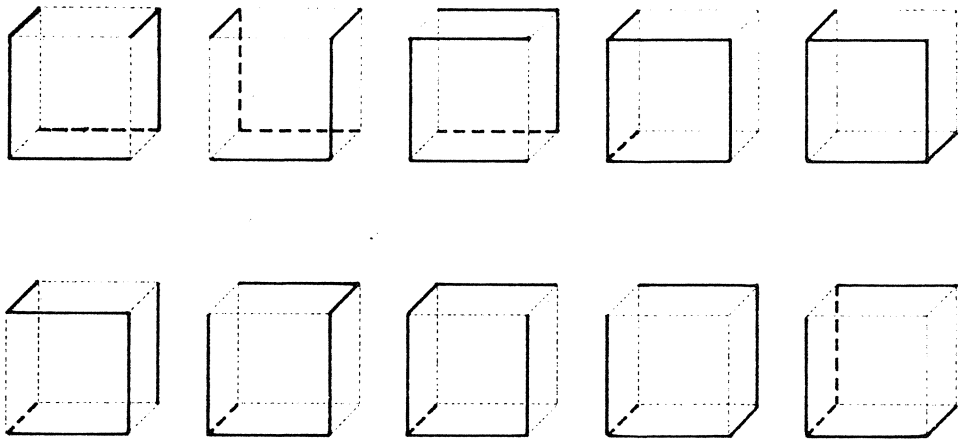
$$P_{G,\rho}(\lambda_1,\lambda_2,\lambda_3,\ldots).$$

Hierin is (voor $j = 1,2,\ldots$) λ_j *het aantal* $r \in R$ *dat invariant is bij*

de j-*de macht van* q.

Het bewijs is analoog aan dat van de stelling van Polya, maar berust op de uitbreiding (lemma 4.2) van de stelling van Caucy-Frobenius.

VOORBEELD 6.2. Sommige deelverzamelingen van de verzameling der 12 ribben van een kubus gaan door draaiing in hun complement over. Hoeveel "deelverzamelingspatronen" hebben deze eigenschap? Voor R nemen we {ja,nee} , voor q de verwisseling van ja en nee. Nu is $\lambda_1 = \lambda_3 = \lambda_5 = \ldots = 0$, $\lambda_2 = \lambda_4 = \lambda_6 = \ldots = 2$. Door substitutie van 0,2,0,2,... in de betreffende cyclenindex komt er $\frac{1}{24}(3.2^6 + 6.2^3) = 10$. Met enige moeite zijn deze patronen door inspectie te vinden (zie figuur).

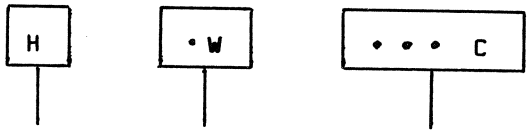


Figuur 1.

§7. Boomvormige molekulen.

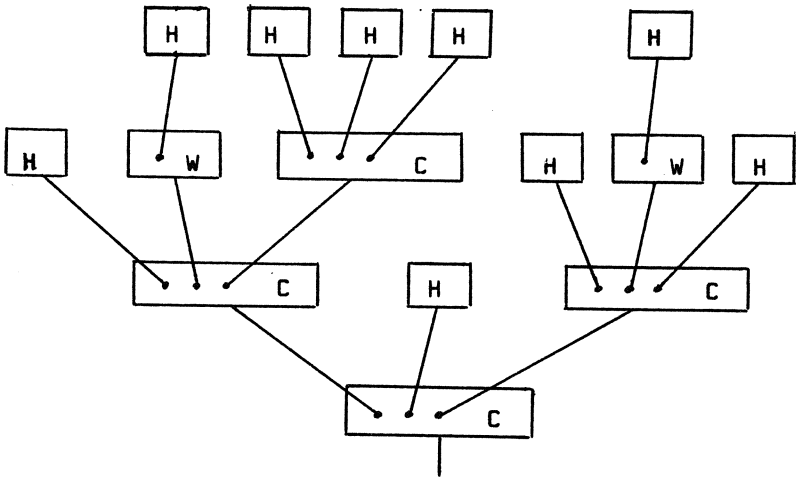
De molekulen die we beschrijven hebben allemaal een duidelijk onderkenbaar punt dat als *wortel* wordt aangeduid; ze kunen beschouwd worden als van dat punt uit gegroeid te zijn. De atomen die als bouwstenen dienen, hebben dan ook steeds één duidelijke binding naar beneden (naar de wortel) en nul of meer bindingen naar boven. Een atoom is dan ook beschreven door een bordje op een stok (de stok stelt de binding naar beneden voor). Op het bordje staat aangetekend (i) de naam van het atoom (zoals H,C,O), (ii) een rijtje punten die dienen als aanhechtingsplaats voor k ($k \geqq 0$) bindingen (k heet de *uitvalentie*; de gewone valentie van het atoom is dan $k + 1$), (iii) een groep van permutaties van deze aanhechtingspunten.

We gaan uit van een collectie bouwstenen (met onderling verschillende namen), bijv.



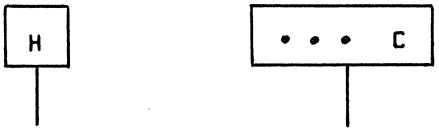
en bij C wordt de alternerende groep A_3 gekozen. Het begrip "boom" wordt nu als volgt recursief gedefinieerd: (i) een atoom met uitvalentie 0, (ii) een atoom (het zgn. grondatoom) met uitvalentie $k > 0$, waarbij op elk der k punten een boom is geplant. In figuur 2 zien we een voorbeeld.

Een *radikaal* is een equivalentieklasse van bomen, weer recursief gedefinieerd. (i) Twee atomen met uitvalentie 0 zijn d.e.s.d. equivalent als ze gelijk zijn. (ii) Twee niet-atomaire bomen zijn d.e.s.d. equivalent wanneer ze hetzelfde grondatoom hebben en de op het grondatoom van de eerste boom geplante bomen, na toepassing van een permutatie volgens de groep van het grondatoom, overgaan in een stel bomen en stuk voor stuk equivalent zijn met de op het grondatoom van de tweede boom geplante bomen.



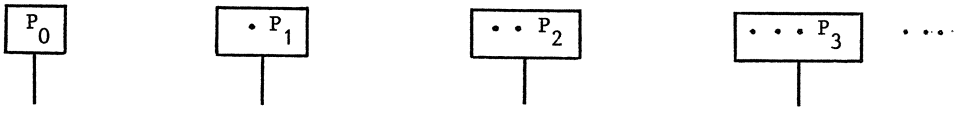
Figuur 2.

VOORBEELD 7.1. Bij de atoomvoorraad



met bij C de symmetrische groep, krijgen we radikalen die, wanneer ze op een OH-groep geplant worden, *alkoholen* heten. Nemen we bij C de alternerende groep dan worden het *stereoalkoholen*; daarbij worden alkoholen met verschillende optische activiteit als verschillend beschouwd.

VOORBEELD 7.2. Neem de atoomvoorraad



en bij P_n de triviale groep (alleen de identiteit). De radikalen zijn

nu *planaire stambomen*. Nemen we daarentegen bij P_n de symmetrische groep dan krijgen we de *topologische wortelbomen*.

We kennen aan elk atoom van de atoomvoorraad ook een *gewicht* toe. Het gewicht van een radikaal is het *produkt* (dus niet zoals in de chemie de som) van de daarin gebruikte atomen (elk zo vaak geteld als de frequentie bedraagt). We beperken ons tot het geval dat het gewicht van een atoom een aan de naam van het atoom toegevoegde *variabele* is (bijv. y_H, y_c).

We beschrijven de atoomvoorraad (eindig of aftelbaar veel atomen) als volgt. I is een indexverzameling (eindig of aftelbaar); als $i \in I$ is i een atoomnaam. Bij i is een eindige verzameling E_i gegeven (de verzameling der aanhechtingspunten) en een groep H_i van permutaties van E_i. Aan i is toegevoegd de variabele y_i; daarnaast hebben we de variabelen x_1, x_2, x_3, ... die in de cyclenindices voorkomen. Bij H_i beschouwen we de triviale representatie: $\rho(h) = h$ voor alle $h \in H_i$. We schrijven dan ook P_{H_i} i.p.v. $P_{H_i,\rho}$.

Aan de atoomvoorraad voegen we toe de machtreeks (eventueel polynoom)

$$Q(x_1,x_2,\ldots) = \sum_{i\in I} y_i \, P_{h_i}(x_1,x_2,\ldots).$$

De door de atoomvoorraad voortgebrachte radikalen geven aanleiding tot de reeks

$$f(y_1,y_2,\ldots) = \sum_{t\in T} (\text{gewicht van } t),$$

waarin T de verzameling van radikalen is.

De coëfficiënten van f kunnen worden gevonden uit de volgende in wezen van Polya [7] afkomstige functionaalbetrekking:

STELLING 7.3.

$$f(y_1,y_2,\ldots) = Q(fy_1,y_2,y_3,\ldots),\ f(y_1^2,y_2^2,y_3^2,\ldots),\ f(y_1^3,y_2^3,\ldots),\ldots).$$

Het bewijs van deze stelling kan met handgewuif worden gegeven. Een formeel bewijs is moeilijker (bijv. [3], waar tegelijk een uitbreiding gegeven is).

VOORBEELD 7.4. Alkoholen. Geef aan H het gewicht 1, aan C het gewicht y. Is a_n het aantal alkoholen met n C-atomen, dan voldoet $f(y) = \sum_0^\infty a_n y^n$ aan

$$f(y) = 1 + \frac{1}{6}\left((f(y))^3 + 2f(y^3) + 3f(y)f(y^2)\right).$$

VOORBEELD 7.5. Stereoalkoholen. Met dezelfde notatie als in het vorige voorbeeld is nu

$$f(y) = 1 + \frac{1}{3}\left((f(y))^3 + 2f(y^3)\right).$$

VOORBEELD 7.6. Plenaire stambomen. Is a_n het aantal ervan met n punten dan is

$$f(x) = x(1 + f(x) + (f(x))^2 + \ldots).$$

Deze vergelijking kan worden opgelost, en geeft

$$f(x) = \tfrac{1}{2} - \tfrac{1}{2}(1 - 4x)^{\frac{1}{2}} = \sum_1^\infty \frac{(2n)!}{n!(n+1)!}\, x^n.$$

VOORBEELD 7.7. Topologische wortelbomen. Met behulp van voorbeeld 3.3 vinden we Cayley's formule

$$f(x) = x \exp(f(x) + \tfrac{1}{2}f(x^2) + \tfrac{1}{3} f(x^3) + \ldots).$$

Literatuur.

[1] *N.G. de Bruijn*, Polya's theory of counting, in: Applied Combinatorial Mathematics, ed. E.F. Beckenbach, pp. 144-148. Wiley 1964.

[2] *N.G. de Bruijn*, Colour patterns that are invariant under a given permutation of the colours, Journal of Combinatorial Theory 2 (1967), 418-421.

[3] *N.G. de Bruijn*, Enumberation of tree-shaped molecules, in: Recent Progress in Combinatorics, ed. W.T. Tutte, pp. 59-68. Academic Press 1969.

[4] *N.G. de Bruijn*, Polya's Abzähltheorie: Muster für Graphen und chemische Verbindungen, in: Selecta Mathematica III, ed. K. Jacobs. Heidelberger Taschenbücher Bd. 86., pp. 1-26. Springer 1971.

[5] *N.G. de Bruijn*, A survey of generalizations of Polya's enumeration theorem, Nieuw Archief v. Wiskunde (2) 19, 89-112 (1971).

[6] *N.G. de Bruijn*, A note on the Cauchy-Frobenius Lemma, Proc. Kon. Nederl. Akad. v. Wetensch. A 82 (= Indag. Math. 41) 225-228 (1979).

[7] *G. Polya*, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, Acta Math. 68, 145-254 (1937).

THEORIE DER GRAPHEN

J.C. Boland

We beginnen onze beschouwingen met het volgende vraagstuk. In een studentenvereniging is ieder lid bevriend met een aantal (minstens één) van de andere leden. Is het nu mogelijk de leden van deze vereniging zo in twee groepen te splitsen, dat twee vrienden nooit tot dezelfde groep behoren.

Een dergelijk vraagstuk is duidelijk een kombinatorische kwestie.
We hebben nu in de graphentheorie een taal, die vaak bijzonder geschikt is voor het bespreken en zo mogelijk oplossen van dergelijke kombinatorische problemen.

In ons vraagstuk hebben we te maken met:
1) een verzameling A van studenten
2) een binaire relatie R(x,y), die als volgt gedefinieerd is: voor $x \in A$ en $y \in A$ geldt dan en slechts dan de relatie R, als $x \neq y$ en x bevriend is met y.

We nemen hierbij aan dat de relatie R symmetrisch is, d.w.z. zodra x bevriend is met y, is ook omgekeerd y bevriend met x.

Onder een graph verstaan we nu een verzameling A tezamen met een op A gedefinieerde binaire symmetrische relatie.

In principe mag de verzameling A een willekeurige machtigheid hebben. De machtigheid van A noemen we ook wel de machtigheid van de graph [A,R].
We zullen ons beperken tot de beschouwing van eindige graphen. Van deze graphen kunnen we nu op de volgende manier een eenvoudige geometrische representatie geven.

Aan ieder element x van A voegen we een punt toe, dat we eveneens x noemen.

Geldt voor twee elementen x en y van A de relatie R(x,y), dan verbinden we de punten x en y door een boog L(x,y), die x en y tot eindpunten heeft. Geldt R(x,y) niet, dan worden x en y niet door een boog verbonden. De punten van A noemen we de hoekpunten van de graph en de bogen L(x,y) de kanten. De vereniging van alle kanten van een graph G is een puntverzameling, die we als representatie van G kunnen beschouwen. Daar we doorgaans niet onderscheiden tussen een graph en zijn representatie zullen we de representatie van G eveneens G noemen. De graph G is dus éénduidig bepaald door zijn hoekpunten en zijn kanten. Onder een deelgraph van G zullen we verstaan een deelverzameling van de kantenverzameling van G.

Tot dusver hebben we de representatie van G beschouwd als een puntverzameling. De vraag rijst of we deze puntverzameling mogen opvatten als deelverzameling van een R^n. We kunnen nu op een natuurlijke wijze in G een metriek invoeren, waardoor G een 1-dimensionale metrisch separabele ruimte wordt. Op grond van de inbeddingsstelling van Hurewicz kan G dan altijd in de R^3 worden ingebed.

Om dit in te zien voeren we nog enige begrippen in. Laat gegeven zijn een rij hoekpunten a_i (i=1...N) zodanig dat a_i en a_{i+1} (i=1...N-1) eindpunten van een kant zijn. De verzameling van kanten $[a_i,a_{i+1}]$ noemen we dan een kantentrek. a_1 en a_N noemen we het begin- resp. het eindpunt van de kantentrek. Zijn begin- en eindpunt van een kantentrek hetzelfde hoekpunt, dan noemen we de kantentrek een cyclus. Zijn alle hoekpunten van een kantentrek twee aan twee verschillend, dan noemen we de kantentrek een weg.

Men ziet gemakkelijk dat twee hoekpunten die door een kantentrek kunnen worden verbonden, ook door een weg verbonden kunnen worden. We kunnen onze graph nu als volgt metriseren.

In iedere kant kunnen we een natuurlijke metriek kiezen, waardoor de kant de totale lengte 1 krijgt. Onder de lengte van een weg verstaan we dan het totale aantal kanten dat in de weg voorkomt. Zijn nu a en b twee verschillende hoekpunten van G, dan verstaan we onder de afstand $\rho(a,b)$ de lengte van de kortste weg, die a en b verbindt. Kunnen a en b niet door een weg verbonden worden, dan stellen we $\rho(a,b)=1$.

Is p een punt van een kant $[x_1,x_2]$ en q een punt van $[y_1,y_2]$ dan definiëren we $\rho(p,g) = \inf(\rho(p,x_i) + \rho(x_i,y_j) + \rho(y_j,q))$ met $i,j = 1,2$.

Tenslotte stellen we nog $\rho(x,x) = 0$ voor $x \in G$. Het is nu gemakkelijk te zien dat de aldus gedefiniëerde functie $\rho(x,y)$ aan de metrische axioma's voldoet. We zien onmiddellijk dat G ook separabel is.
Immers we kunnen op iedere kant een aftelbare overal dichte deelverzameling kiezen. Daar G slechts eindig veel kanten heeft, is de vereniging van deze aftelbare verzamelingen weer aftelbaar. Bovendien is hij overal dicht in G. G is dus een metrische separabele ruimte. Daar iedere kant een gesloten deelverzameling van G is met dimensie 1, volgt uit de somstelling van de dimensietheorie, dat ook $\dim(G) = 1$.
Hieruit zien we dus dat iedere eindige graph in R^3 ingebed kan worden.
We merken nog op, dat hetzelfde redenering ook nog voor aftelbaar oneindige graphen geldt.

Als we nu terugkeren tot het vraagstuk waar we vanuit gegaan zijn, dan kunnen we ons probleem nu ook als volgt stellen: is het mogelijk met behulp van twee verschillende kleuren, de hoekpunten van een graph zo te kleuren, dat iedere kant twee verschillend gekleurde uiteinden krijgt.
Als voorbeeld bekijken we eens de graphen K_1 en K_2 uit figuur 1.

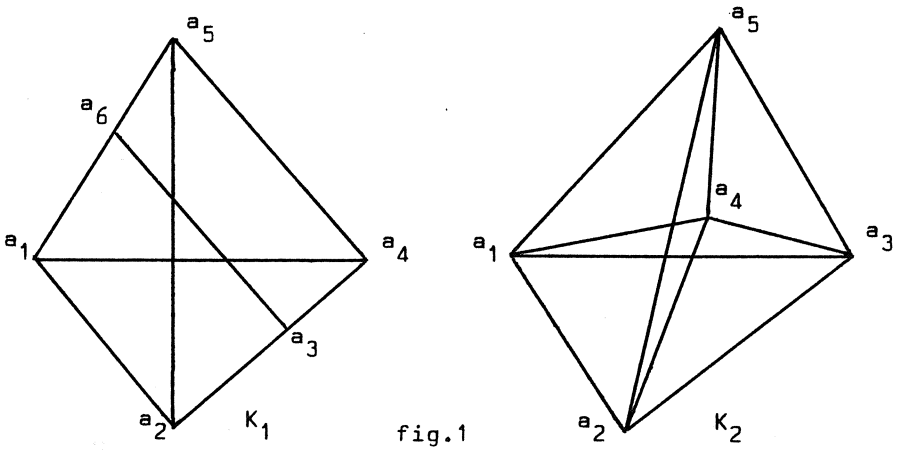


fig.1

We zien dat we in de graph K_1 ons doel kunnen bereiken, door bijv. de punten a_1, a_3 en a_5 blauw te kleuren en a_2, a_4 en a_6 rood. In de graph K_2

zal het ons echter niet lukken. Immers als a_1 bijv. blauw gemaakt wordt, dan moet a_2 rood worden, maar kunnen a_3, a_4 en a_5 noch blauw noch rood gemaakt worden.

Het is nu gemakkelijk in te zien, dat ons probleem dan en slechts dan een oplossing bezit als de bijbehorende graph de eigenschap heeft, dat iedere cyclus een even aantal kanten bezit.

Ons voorbeeld toont aan hoe de graphentheorie een makkelijk hulpmiddel kan zijn voor het oplossen van sommige kombinatorische problemen. Daar in de laatste decennia in verschillende wetenschappen dergelijke problemen naar voren zijn gekomen, is ook de belangstelling voor de graphentheorie snel toegenomen. We willen nog enkele belangrijke punten hiervan bespreken.

Laat de graph G = [A,R] gegeven zijn, en kies een hoekpunt a van G. Laat A(a) de verzameling van alle hoekpunten x van G zijn, die voldoen aan de volgende voorwaarde: x = a of x kan door een weg met a verbonden worden.

Dan geldt dat iedere kant ofwel beide eindpunten in A(a) heeft, ofwel niets met A(a) gemeen heeft. De deelgraph van G, die gevormd wordt door alle kanten, die beide eindpunten in A(a) hebben, noemen we de komponent van a. Men ziet gemakkelijk, dat G op éénduidige wijze in komponenten gesplitst wordt. Heeft G slechts 1 komponent, dan heet hij samenhangend. We zullen ons in het vervolg beperken tot samenhangende graphen.

Men kan nu in iedere kant van G een richting vastleggen. In dat geval spreekt men wel van een gerichte graph. Een gerichte graph is nu een georiënteerd komplex in de zin van de homologietheorie. De homologiegroepen van G vormen dus belangrijke topologische invarianten. Als G samenhangend is, weten we uit de homologietheorie, dat de 0-de homologiegroep een oneindig cyclische groep is. De rang p^0 hiervan is dus 1. De eerste homologiegroep is te schrijven als directe som van een eindig aantal p^1, van oneindig cyclische groepen en eventueel een aantal eindige cyclische groepen. Deze laatsten ontbreken hier echter. Immers als z een 1-dimensionale cyclus en m een heel getal is, zodanig dat $mz \sim 0$ is, dan volgt hieruit dat $mz = 0$ is, daar dim G = 1. Uit $mz = 0$ volgt echter $m = 0$ of $z = 0$.

Het getal p^1 geeft ons het maximale aantal lineair onafhankelijke cyclen, terwijl we weten dat een graph nooit torsie bezit. Het getal p^1 laat zich nu gemakkelijk berekenen als we het aantal hoekpunten en het aantal kanten van de graph kennen. We beschouwen daartoe eerst een samenhangende graph, die geen topologische cirkel bevat. Een dergelijke graph noemt men een boom. Als een boom α^0 hoekpunten en α^1 kanten heeft, dan is $\alpha^1 = \alpha^0 - 1$. Deze formule is juist als de boom slechts uit één kant bestaat. Als de formule juist is voor een boom B en we voegen aan B een kant k toe, die met B slechts één eindpunt gemeen heeft, dan geldt de formule ook voor de boom $B' = B \cup k$. Immers door toevoeging van k neemt het aantal kanten en hoekpunten beide met 1 toe. Bovendien is B' zeker weer een boom. Daar nu iedere boom verkregen kan worden door van één van zijn kanten uit te gaan en stap voor stap kanten toe te voegen, die met de reeds verkregen boom 1 eindpunt gemeen hebben, geldt de formule algemeen. Daar voor een boom $p^1 = 0$ is, geldt voor bomen de formule $p^1 = \alpha^1 - \alpha^0 + 1$. Deze formule geldt echter ook voor iedere eindige samenhangende graph. Zij n.l. G een graph en B_0 een deelboom van G. Als iedere kant van G, die niet tot B_0 behoort de beide eindpunten in B_0 heeft, dan heet B_0 maximaal. Is B_0 niet maximaal, dan kunnen we hem uitbreiden tot een boom B_1 die ontstaat door aan B_0 een kant toe te voegen, die met B_0 slechts 1 eindpunt gemeen heeft. Daar G slechts eindig veel kanten heeft, moeten we op deze manier voortgaand, na eindig veel stappen een maximale boom bereiken. Iedere boom van G is dus altijd bevat in een maximale boom. Deze stelling geldt ook nog voor oneindige graphen. Bij het bewijs moet dan echter gebruik gemaakt worden van het lemma van Zorn.

Men ziet gemakkelijk dat een maximale boom B in G, alle hoekpunten van G moet bevatten. Immers zouden er hoekpunten in G zijn, die niet in B bevat zijn, dan zou er op grond van de samenhang van G zeker een kant moeten zijn, die slechts 1 eindpunt met B gemeen heeft. Dit is uitgesloten, omdat B maximaal is.

Om nu onze formule te bewijzen, kiezen we een maximale boom B in G. De kanten van B zullen we aangeven met de letter k, en de niet tot B behorende kanten met de letter l. Iedere kant l heeft beide eindpunten in B liggen.

Daar B een boom is kunnen de eindpunten van l door één en slechts één weg w in B verbonden worden. Dan is echter w U l een cyclus, die we als z(l) aangeven. Daar iedere cyclus z(l) slechts 1 kant l bevat zijn de cyclen z(l) lineair onafhankelijk.

Bovendien vormen zij een basis voor de cyclen in G. Is n.l. z een willekeurige cyclus in G, dan bevat z zeker kanten l. Laat $l_1 \ldots l_N$ de in z bevatte kanten l zijn, en laat l_i in z voorkomen met de coëfficient t_i. Dan bevat de cyclus $z - \sum_{i=1}^{N} t_i\, z(l_i)$ geen kanten l. Derhalve is $z - \sum_{i=1}^{N} t_i\, z(l_i) = 0$ of $z = \sum_{i=1}^{N} t_i\, z(l_i)$. We kunnen hieruit de conclusie trekken dat er juist p^1 cyclen z(l) zijn, en dus ook dat er p^1 kanten l zijn. Daar B een boom is, die alle hoekpunten van G bevat, zijn er α^0-1 kanten k. We hebben dus $\alpha^1 = p^1 + \alpha^0 - 1$ of $p^1 = \alpha^1 - \alpha^0 + 1$. Bezit de graph G n verschillende komponenten, dan ziet men gemakkelijk dat $p^1 = \alpha^1 - \alpha^0 + n$. Het getal p^1 noemt men ook wel de rang van de graph. Het blijkt, dat twee graphen, die eenzelfde aantal komponenten hebben en ook dezelfde rang, in alle homologie en homotopie eigenschappen overeenstemmen.

Een belangrijke reeks vragen hangt samen met de zogenaamde inbeddingsproblemen van graphen. We weten reeds, dat iedere graph in R^3 kan worden ingebed. Men kan zich afvragen of dit misschien ook reeds in R^2 mogelijk is. Nu is gemakkelijk te zien, dat de graphen K_1 en K_2 uit fig.1 geen van beide in het platte vlak kunnen worden ingebed. Kuratowski heeft bewezen dat een eindige graph G dan en slechts dan in R^2 kan worden ingebed, als G geen topologisch beeld van één der beide graphen K_1 en K_2 bevat. Deze stelling kan vrij eenvoudig bewezen worden door inductie naar het aantal kanten van de graph. Het resultaat van Kuratowski kan ook uitgebreid worden tot aftelbaar oneindige graphen. (zie ook de bijdrage van Laman).

Eevenzo kan men zich afvragen onder welke omstandigheden een graph bijv. in het projectieve vlak of in het ringoppervlak kan worden ingebed. Bekend is, dat de volledige 6-graph in het projectieve vlak en de volledige 7-graph in het ringoppervlak kan worden ingebed. Daarbij verstaan we onder de volledige n-graph, de graph met n hoekpunten, waarbij ieder tweetal

hoekpunten door een kant verbonden is. Een karakterisering van de in het projectieve vlak inbedbare graphen door middel van verboden figuren wordt minder geschikt door het grote aantal verboden figuren, dat optreedt. Het is bekend, dat iedere graph in een oriënteerbaar oppervlak van voldoend hoog geslacht kan worden ingebed. Onder de genus van een graph verstaan we nu het kleinste natuurlijke getal g, zodanig dat de graph in een oriënteerbaar oppervlak van geslacht g kan worden ingebed. Er zijn echter nog geen methoden bekend om de genus van een graph te berekenen.

LITERATUUR

N.L.Biggs, *E.K.Lloyd*, *R.J.Wilson*, Graph theory 1736 - 1936. Oxford etc. 1977.

WAT ZIJN GRAFEN?

G. Laman

In grafentheorie is "graaf" een verzamelwoord voor een aantal verwante begrippen waarin het gemeenschappelijke hierin bestaat dat het telkens gaat om verbindingen tussen discrete objecten.

Voorbeelden:

I. Objecten: hoekpunten van een kubus;
Verbindingen: ribben van de kubus.

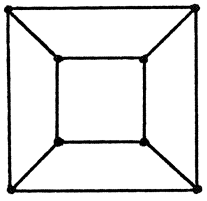


fig.1

II. Hiërarchie.
Objecten: personen;
Verbinding: onderschikking.

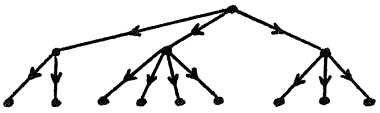


fig.2

III. Stangenconstructie (bijv. voor bouwsteiger).
Objecten: plaatsen waar twee of meer stangen aan elkaar bevestigd zijn;
Verbindingen: delen van stangen tussen twee bevestigingen.

IV. Schaakbord.

Objecten: de 64 velden;

Verbinding: 2 velden zijn verbonden als een toren op een overigens leeg bord in één zet van het ene het andere veld kan bereiken.

Opm.: Andere stukken leveren andere grafen.

V. Schaakspel.

Objecten: posities (inclusief wie aan zet is);

Verbinding: een positie is met een andere verbonden als de één in de ander overgaat door een reglementaire zet.

DEFINITIE: Een <u>graaf</u> (X,R) bestaat uit een niet-lege eindige verzameling X van <u>punten</u> en een eindige verzameling R van <u>kanten</u>; elke kant $r \in R$ verbindt twee verschillende punten x_1 en x_2, de <u>uiteinden</u> van r, x_1 en x_2 heten <u>buren</u>; er is ten hoogste één kant in R die twee gegeven punten verbindt.

DEFINITIE: Een <u>gerichte graaf</u> $(X, \vec{R})$ bestaat uit een niet-lege eindige verzameling X van <u>punten</u> en een eindige verzameling $\vec{R}$ van <u>gerichte kanten</u>; elke gerichte kant $\vec{r} \in \vec{R}$ verbindt een <u>beginpunt</u> x_1 met een <u>eindpunt</u> $x_2 \neq x_1$, x_1 en x_2 heten dan <u>buren</u>; er is ten hoogste één gerichte kant in $\vec{R}$ die x_1 als beginpunt en x_2 als eindpunt heeft.

VI. Een beroemd voorbeeld (Euler) is dat van de bruggen van Königsberg. Daar waren één rivier, twee oevers, twee eilanden en zeven bruggen, zoals aangegeven in fig. 3.

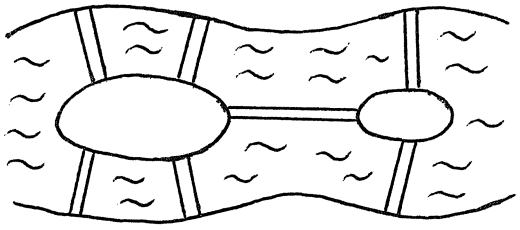


fig.3

De vraagstelling was: Bestaat er een wandeling waarbij men elke brug precies éénmaal passeert?
Een aan deze vraagstelling aangepast model is:
Objecten: oevers en eilanden;
Verbindingen: bruggen.
Maar fig. 4 levert geen graaf in de boven gedefinieerde zin!

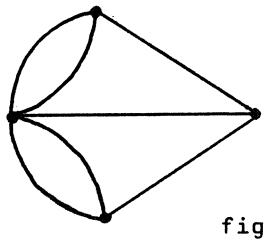


fig.4

VII. Verzameling van deelverzamelingen van $\{1,2,3\}$.
Objecten: deelverzamelingen;
Verbinding: inclusie.

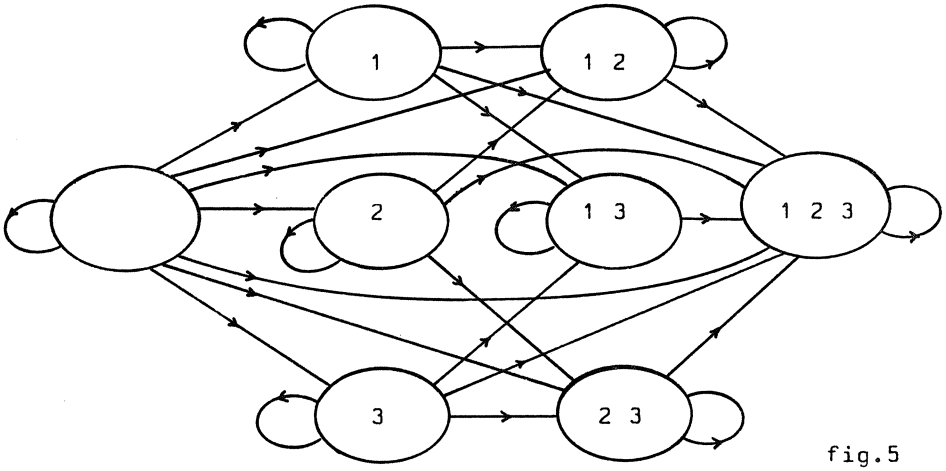


fig.5

DEFINITIE: Een <u>multi-graaf</u> (X,R) bestaat uit een niet-lege eindige verzameling X van <u>punten</u> en een eindige verzameling R van <u>kanten</u>; elke kant $r \in R$ verbindt twee punten (die kunnen samenvallen).

DEFINITIE: Een <u>gerichte multi-graaf</u> $(X,\vec{R})$ bestaat uit een niet-lege eindige verzameling X van <u>punten</u> en een eindige verzameling $\vec{R}$ van <u>gerichte kanten</u>; elke gerichte kant $\vec{r} \in \vec{R}$ verbindt een <u>beginpunt</u> x_1 met een <u>eindpunt</u> x_2 (die kunnen samenvallen).

DEFINITIE: Een <u>lus</u> is een (gerichte) kant, waarvan de uiteinden (begin- en eindpunt) samenvallen.
<u>Meervoudige</u> (gerichte) <u>kanten</u> zijn kanten die dezelfde uiteinden (begin- en eindpunten) hebben.

De terminologie in de grafentheorie is verre van genormaliseerd, ja zelfs nogal chaotisch. Het is dus zaak in de literatuur over grafen goed te lezen wat <u>deze</u> auteur met <u>dit</u> woord bedoelt. Welke definities en welke woorden gekozen worden is sterk afhankelijk van de probleemstelling. Er zijn ook situaties waarin lussen wél, meervoudige kanten niét toegelaten worden of omgekeerd. Ook grafen met oneindige verzamelingen punten en kanten komen vaak voor. Er is nogal wat te definiëren, voordat er wat valt te beginnen. *)

DEFINITIE: In een multi-graaf is $d(x)$ - de <u>graad</u> van $x \in X$ - het aantal kanten waarvan x uiteinde is (lussen dubbel geteld).
In een gerichte multigraaf is
$id(x)$ - de <u>in-graad</u> van $x \in X$ - het aantal gerichte kanten waarvan x eindpunt is,
$od(x)$ - de <u>uit-graad</u> van $x \in X$ - het aantal gerichte kanten waarvan x beginpunt is,
$d(x) = id(x) + od(x)$ - de <u>graad</u> van $x \in X$.

Opmerking: Wat voor multi-graaf gedefinieerd is, geldt ook voor graaf; wat voor gerichte multigraaf gedefinieerd is, geldt ook voor gerichte graaf.

*) Red.:
Ter illustratie van deze opmerking vergelijke men de verschillende bijdragen over grafentheorie in deze syllabus.

DEFINITIE: Een <u>partiële graaf</u> van een multi-graaf (X,R) is een multigraaf (X,S) met $S \subset R$.
Een <u>deelgraaf</u> van een multi-graaf (X,R) is een multi-graaf (Y,T) waarin $Y \subset X$ en T alle kanten van R bevat die beide uiteinden in Y hebben.
Partiële graaf en deelgraaf van een gerichte multi-graaf worden analoog gedefinieerd.

DEFINITIE: Twee grafen (X,R) en $(\tilde{X},\tilde{R})$ zijn <u>isomorf</u> als er één-éénduidige afbeeldingen $\xi: X \to \tilde{X}$, $\rho: R \to \tilde{R}$ bestaan zodat voor elke $r \in R$ met uiteinden x_1 en x_2, $\xi(x_1)$ en $\xi(x_2)$ de uiteinden van $\rho(r)$ zijn. Analoog voor (gerichte) multi-grafen.

Het is niet moeilijk voor kleine grafen na te gaan of ze isomorf zijn of niet:

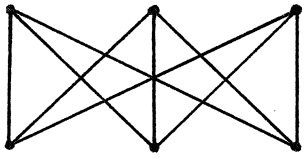


fig.6a

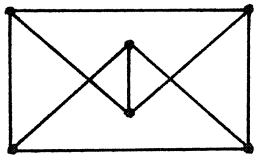


fig.6b

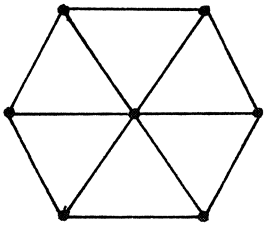


fig.6c

Voor grotere grafen neemt de moeilijkheid zo snel toe met het aantal punten, dat men van het isomorfie-probleem spreekt.

DEFINITIE: Een graaf waarin R (bij gegeven X) zo groot mogelijk is heet <u>volledig</u>; i.h.b. heet de graaf met n punten en $\frac{1}{2}n(n-1)$ kanten de <u>volledige n-graaf</u> K_n.

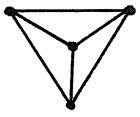
Voorbeelden: K_2: K_3: K_4: 

fig.7a fig.7b fig.7c

K_n: halve competitie van n teams.

DEFINITIE: In een <u>volledige tweedelige graaf</u> is de puntenverzameling X disjuncte vereniging van X_1 en X_2 en bestaat R uit alle kanten met één uiteinde in X_1 en één in X_2; als $|X_1| = p$ en $|X_2| = q$ wordt deze graaf aangeduid met $K_{p,q}$.

Voorbeelden:

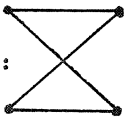
$K_{2,2}$: 

fig.8a

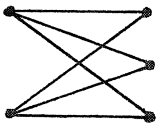
$K_{2,3}$: 

fig.8b

$K_{3,3}$: fig.6a

DEFINITIE: De <u>complementaire graaf</u> van een graaf (X,R) is de graaf (X,R'), waarin R' het complement is van R, d.w.z. precies alle kanten bevat die niet in R voorkomen.

Voorbeeld: De complementaire graaf van $K_{p,q}$ bestaat uit een K_p en een K_q.

DEFINITIE: Een <u>keten</u> van <u>lengte</u> q in een multi-graaf (X,R) is een rij van q kanten $(r_1, r_2, \ldots, r_q)$ zodat elke kant r_α $(1<\alpha<q)$ één uiteinde met $r_{\alpha-1}$ en het andere met $r_{\alpha+1}$ gemeen heeft. De "vrije" uiteinden van r_1 resp. r_q heten <u>beginpunt</u> resp. <u>eindpunt</u> van de keten. Als begin- en eindpunt samenvallen heet de keten een <u>cykel</u>. Een keten is <u>elementair</u> als geen element (van X of van R) meer dan éénmaal in de rij optreedt.

DEFINITIE: Een multi-graaf is <u>samenhangend</u>, als er een keten is van elk punt naar elk ander punt. Een <u>samenhangende component</u> van een multi-graaf is een maximale samenhangende deelgraaf. De <u>afstand</u> van twee punten x_1 en x_2 van een multi-graaf is gedefinieerd als x_1 en x_2 tot dezelfde samenhangende component behoren en wel als de lengte van de kortste keten die x_1 en x_2 als begin- en eindpunt heeft. Een <u>isthmus</u> is een kant bij verwijdering waarvan het aantal samenhangende componenten met één toeneemt. Een <u>boom</u> is een samenhangende graaf zonder cykels.

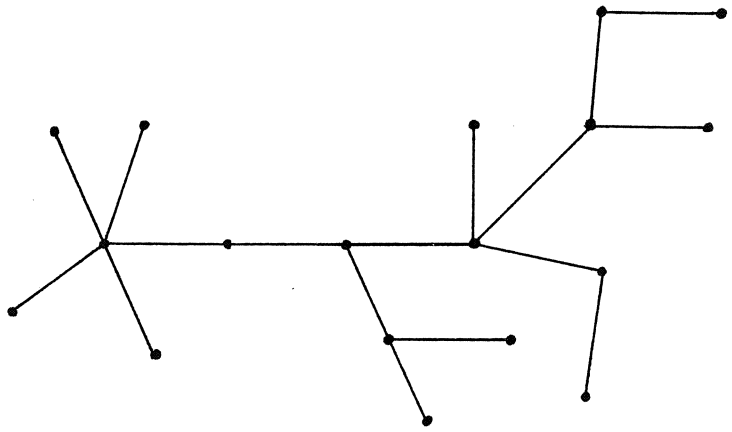


fig.9

STELLING 1: Een boom met meer dan één punt heeft tenminste twee punten van graad 1.

Bewijs: Wegens samenhang is er tenminste één kant. Neem een kant en maak een steeds grotere keten door in elk begin- of eindpunt van graad $\geqslant 2$ telkens een niet gebruikte kant toe te voegen. Wegens eindigheid loopt dit af hetzij doordat begin- en eindpunt samenvallen hetzij doordat begin en eindpunt beide graad 1 hebben. Het eerste alternatief vervalt want een boom heeft geen cykels.

STELLING 2: Een graaf (X,R) met $|R| \geqslant |X|$ heeft een cykel.

Bewijs: Als er punten van graad 0 en graad 1 zijn vindt men door weglating daarvan en van de kanten die de punten van graad 1 als uiteinde hebben eventueel na herhaling een graaf (Y,T) met $|T| \geqslant |Y|$ en waarin alle punten graad $\geqslant 2$ hebben. Van de beide alternatieven uit het bewijs van st. 1 treedt nu het eerste op.

STELLING 3: Voor een graaf (X,R) zijn equivalent de beweringen:

I (X,R) is een boom.

II Er is tussen elk paar punten precies één elementaire keten.

III (X,R) heeft geen cykles en toevoeging van een willekeurige kant vormt een cykel.

IV (X,R) is samenhangend en verliest deze eigenschap bij verwijdering van een willekeurige kant.

V $|R| = |X| - 1$ en (X,R) heeft geen cykels.

VI $|R| = |X| - 1$ en (X,R) is samenhangend.

Bewijs: Het bestaan van twee verschillende elementaire ketens tussen twee punten impliceert het bestaan van een cykel en omgekeerd.
Daarop berust de equivalentie van I, II, III en IV.
I ⇒ V wordt bewezen met volledige inductie: Voor $|X| = 2$ is het juist dat $|R| = |X| - 1$. Neem aan dat dat ook juist is voor bomen met $|X| \leqslant n$ en laat (X,R) een boom zijn met $|X| = n+1$.
Verwijder dan een punt van graad 1 met de kant die dat punt als uiteinde heeft - dat kan wegens st. 1 -. De nieuwe graaf is weer een boom dus $|R| - 1 = (|X| - 1) - 1$.
V ⇒ VI, want als (X,R) niet samenhangend is zijn er tenminste twee samenhangende componenten (X_i,R_i) en dan volgt uit $|R| = |X| - 1$ voor tenminste één component $|R_i| \geqslant |X_i|$ en dan is er dus een cykel volgens st. 2.
VI ⇒ I, want als (X,R) een cykel van lengte m bevat, dan heeft elk van de $|X| - m$ punten die niet op de cykel liggen een kortste keten die dat punt met de cykel verbindt (wegens de samenhang).
De eerste kanten van deze $|X| - m$ ketens zijn alle verschillend.
Er zijn dus tenminste $m + |X| - m = |X|$ kanten in tegenspraak met $|R| = |X| - 1$.

We komen nu terug op voorbeeld VI.

DEFINITIE: Een <u>Euler-keten</u> (<u>Euler-cykel</u>) in een multi-graph is een keten (cykel) die elke kant precies éénmaal bevat.

STELLING 4: Een samenhangende multi-graaf heeft een Euler-cykel desda elk punt even graad heeft, een Euler-keten met uiteinden y en $z \neq y$ desda y en z de enige punten met oneven graad zijn.

Bewijs: A. Nodig. Elke "doorgang" door een punt levert een bijdrage van 2 aan de graad.

B. Voldoende.

Het gestelde is vanzelfsprekend voor de (enige samenhangende) multi-graaf zonder kanten.

Neem aan dat de bewering bewezen is voor multi-grafen met ten hoogste m kanten en dat (X,R) een multi-graaf is met $|R| = m+1$. Als er geen punten van oneven graad zijn wordt een willekeurige kant verwijderd: $r = (x_1,x_2)$. r kan geen isthmus zijn, want dan ligt x_1 in de ene en x_2 in de andere samenhangende component na verwijdering van r en dan is in elke samenhangende component de som van de graden oneven, terwijl voor elke graaf de som van de graden even moet zijn. De graaf $(X,\tilde{R})$ die bij verwijdering van r ontstaat heeft dus $|\tilde{R}| = m$ en x_1 en x_2 als enige punten van oneven graad. De Euler-keten die in $(X,\tilde{R})$ bestaat wordt door r tot Euler-cykel in (X,R) gesloten.

Als y en $z \neq y$ oneven graad hebben verwijdert men een kant $r = (x,z)$. Er zijn twee mogelijkheden:

1) r is een isthmus. Dan behoren x en y tot dezelfde samenhangende component (zie boven!). In die component bestaat een Euler-keten van y naar x en in de andere een Euler-cykel van z naar z. "Zet" die twee met r "aan elkaar".
2) r is geen isthmus. Dan is er een Euler-keten in (X,R) van y naar x, die met r verlengd kan worden tot een Euler-keten van y naar z in (X,R).

Gevolgen: De inwoner van Königsberg krijgt zijn wandeling niet want alle 4 de punten hebben oneven orde.

De bekende "tekeningen zonder de pen van het papier te nemen" slagen alleen als in ten hoogste 2 punten de graad oneven is.

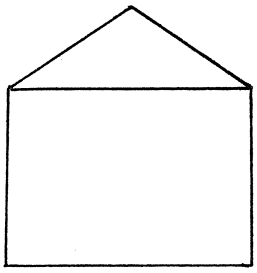


fig.10a

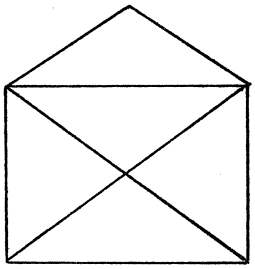


fig.10b

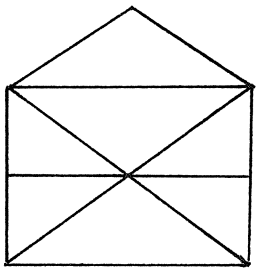


fig.10c

Analoog met de definities van keten, cykel, samenhang enz. heeft men:

DEFINITIE: Een <u>weg</u> van lengte <u>q</u> in een gerichte multi-graaf is een rij van q gerichte kanten $(\vec{r}_1,\vec{r}_2,\ldots,\vec{r}_q)$ zodat voor elke $\alpha \in \{1,2,\ldots,q-1\}$ het eindpunt van $\vec{r}_\alpha$ samenvalt met het beginpunt van $\vec{r}_{\alpha+1}$. Als vroeger definieert men <u>beginpunt</u> en <u>eindpunt</u> van de weg, <u>circuit</u> (analoog met cykel) en <u>elementaire</u> weg.

DEFINITIE: In een gerichte multi-graaf is het punt x_2 <u>bereikbaar vanuit</u> het punt x_1 als er een weg met beginpunt x_1 en eindpunt x_2 (een <u>weg van</u> x_1 <u>naar</u> x_2) is. De <u>afstand van</u> x_1 <u>naar</u> x_2 is gedefinieerd als x_2 bereikbaar is vanuit x_1 en wel als de lengte van de kortste weg van x_1 naar x_2. (Dit afstandsbegrip is dus niet symmetrisch!) Een gerichte multi-graaf heet <u>sterk samenhangend</u> als elk punt vanuit elk ander punt bereikbaar is. Een <u>sterke component</u> van een gerichte multi-graaf is een maximale sterk samenhangende deelgraaf. Aan elke gerichte multi-graaf is toegevoegd een ongerichte multi-graaf verkregen door van elke gerichte kant de richting te "vergeten". Een <u>zwakke component</u> van een gerichte multi-graaf G is een deelgraaf die onder deze toevoeging correspondeert met een samenhangende component van de aan G toegevoegde multi-graaf.

DEFINITIE: Een <u>Euler-weg</u> (<u>Euler-circuit</u>) in een gerichte multi-graaf is een weg (circuit) die (dat) elke gerichte kant precies één maal bevat.

Ook stelling 4 heeft een analogon; stelling 5 volgt hier zonder bewijs:

STELLING 5: Een zwak samenhangende gerichte multi-graaf heeft een Eulercircuit desda voor elk punt de ingraad gelijk is aan de uitgraad.

Toepassingen: Elk figuur (bestaande uit lijnstukken en samenhangend) kan zonder de pen van het papier te nemen getekend worden als elk lijnstuk in elke richting precies éénmaal doorlopen moet worden.
Het is mogelijk op 2^k cyclisch geordende plaatsen nullen en enen zo in te vullen dat elk k-tal opeenvolgende symbolen verschilt van elk ander k-tal.

DEFINITIE: Een graaf heet <u>planair</u> als hij in het platte vlak kan worden ingebed.

Opmerkingen:
1) Planariteit van een graaf komt er dus op neer dat hij zo in het platte vlak kan worden getekend dat elk gemeenschappelijk punt van de getekende kanten ook tot de puntenverzameling van de graaf behoort. Een voorbeeld van een niet-planaire graaf is $K_{3,3}$ zoals verderop wordt bewezen.
2) Een graaf die in het platte vlak kan worden ingebed kan ook in de bol worden ingebed en omgekeerd. Zulke inbeddingen kunnen uit elkaar worden verkregen door stereografische projectie.
3) Inbedden is een topologisch begrip. We ontlenen nog enige begrippen en resultaten zonder bewijzen aan de topologie. Een deel van het vlak dat door kanten van een ingebedde graaf wordt begrensd heet een gebied van de ingebedde graaf. Als bij een ingebedde graaf een kant wordt verwijderd neemt óf het aantal gebieden met 1 af, óf het aantal samenhangende componenten met 1 toe.

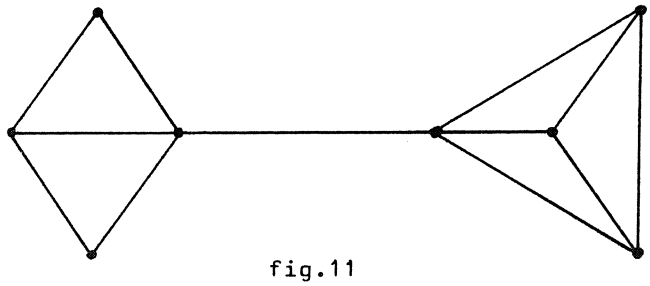


fig.11

STELLING 6: Voor elke graaf ingebed in het platte vlak met n punten, m kanten, l gebieden en c samenhangende componenten geldt: $-m+n = c+1$.

Bewijs: De bewering is juist voor elke graaf zonder kanten:
$l = 1,\ m = 0,\ n = c$.
Neem aan dat het gestelde juist is voor elke graaf met $m = k \geqslant 0$ en laat (X,R) een ingebedde graaf met $|R| = m = k+1$ zijn.
Verwijder een willekeurige kant dan ontstaat een graaf (X,R') met n punten, $m' = k$ kanten, l' gebieden en c' samenhangende componenten.
Als het aantal gebieden met één is afgenomen geldt $l-m+n-c-1 = l-1-(m-1)+n-c-1 = l'-m'+n-c'-1 = 0$.
Als het aantal samenhangende componenten met één is toegenomen geldt $l-m+n-c-1 = l-(m-1)+n-(c+1)-1 = l'-m'+n-c'-1 = 0$.

STELLING 7: Als voor een samenhangende graaf ingebed in het platte vlak met n punten en m kanten de lengte van elke cykel $\geqslant q$ is, dan geldt $m \leqslant \frac{q(n-2)}{q-2}$.

Bewijs: Elke kant behoort tot de randcykel van 2 gebieden, elke randcykel heeft $\geqslant q$ kanten en er zijn l randcykels dus $2m \geqslant l\,q$; $c=1$;
dus $\quad 2 = l-m+n \leqslant \frac{2}{q}\,m-m+n = n-\frac{q-2}{q}\,m$.

STELLING 8: K_5 en $K_{3,3}$ zijn niet planair.

Bewijs:

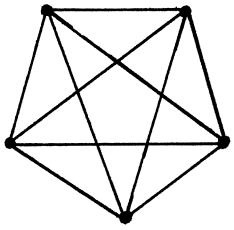


fig.12

In K_5 hebben alle cykels lengte $\geqslant 3$, $n = 5$.
Als er een inbedding bestond dan moest $m \leqslant \frac{3(n-2)}{1} = 9$ zijn.
Het aantal kanten van K_5 is evenwel $\frac{1}{2}n(n-1) = 10$.

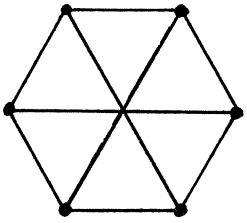


fig.13

In $K_{3,3}$ hebben alle cykels lengte $\geqslant 4$, $n = 6$.
Als er een inbedding bestond dan moest $m \leqslant \frac{4(n-2)}{2} = 8$ zijn.
Het aantal kanten van $K_{3,3}$ is evenwel $3.3 = 9$.

K_5 en $K_{3,3}$ zijn voor de klasse der planaire grafen van bijzondere betekenis
Om die betekenis toe te lichten hebben we nog een definitie nodig.

DEFINITIE: Een <u>onderverdeling</u> van een graaf wordt verkregen door kanten te vervangen door ketens. Twee grafen heten <u>homeomorf</u> als ze beide onderverdelingen zijn van isomorfe grafen.

Voorbeeld:

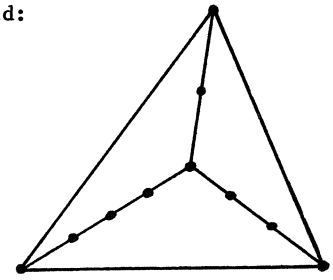


fig.14a

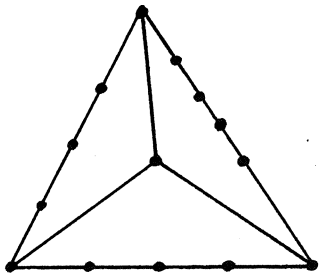


fig.14b

STELLING 10: (Stelling van Kuratowski; zonder bewijs)
Als een graaf niet planair is heeft hij
óf een partiële deelgraaf die homeomorf is met K_5,
óf een partiële deelgraaf die homeomorf is met $K_{3,3}$.

Opmerking: Het is niet aan te bevelen deze stelling te gebruiken om na te gaan of een gegeven graaf planair is; daarvoor zijn in de literatuur goede algorithmen te vinden.

SPELEN OP EEN GRAAF

N.G. de Bruijn

§1. Vele tweepersoonsspelen laten zich formuleren als spel op een georienteerde graaf. Er wordt dan gespeeld met één fiche dat op elk ogenblik in een punt van de graaf staat. Er zijn twee spelers, Jan en Piet, die om de beurt een zet doen. Een zet is het schuiven van het fiche naar een ander punt langs een lijn van de graaf, in overeenstemming met de richting die op die lijn is aangegeven. Er kunnen punten zijn waar geen enkele lijn van uitgaat; bij zulke punten staat een bedrag aangegeven. De speler die het fiche naar een dergelijk punt toe schuift, beëindigt het spel, en krijgt het bij dat punt genoemde bedrag door de tegenstander uitgekeerd. (Dit bedrag kan ook wel negatief zijn.)

VOORBEELD 1.1. Jan begint met het getal 0 op te schrijven. Piet's zet bestaat uit het daarbij optellen van 1, 2 of 3; vervolgens telt Jan daar 1, 2 of 3 bij op, dan Piet weer, enz. Wie het eerst 25 opschrijft krijgt *f* 1,-- van de ander. Getallen boven de 25 mogen niet worden opgeschreven. We kunnen dit spel met een graaf beschrijven die als punten de getallen 0,1,...,25 heeft. Van elk punt i met $i < 25$ gaan pijlen naar $i + 1$, $i + 2$, $i + 3$ (voor zover die ≤ 25 zijn). Bij het uitgangsloze punt 25 staat de uitkering *f* 1,--.

Dit bekende kinderspel heeft een eenvoudige strategie: wie aan zet is, zorgt ervoor een 4-voud + 1 te bereiken als daartoe de kans bestaat (die kans is er niet als er al een 4-voud + 1 staat). Als een

speler eenmaal een 4-voud + 1 heeft bereikt, kan hij het bij elke volgende beurt wéér doen.

§2. We geven nu eerst wat definities en een beetje theorie, die in wezen van E. Zermelo afkomstig is (zie het in §12 vermelde boek van D. König).

Een gerichte graaf is een paar (G,Δ) waarin G een verzameling is en Δ een deelverzameling van $G\times G$. We sluiten de mogelijkheid dat G oneindig is niet uit.

Als x en y punten van G zijn met $(x,y) \in \Delta$ dan zeggen we dat er een pijl van x naar y loopt. Onder $\Gamma(x)$ verstaan we de verzameling van alle y met $(x,y) \in \Delta$. Het kan zijn dat $(x,x) \in \Delta$: dan heet (x,x) een *lus*.

Als $\Gamma(x)$ leeg is, heet x *uitgangsloos* of *dood*.

Het aantal elementen van $\Gamma(x)$ heet de *uitgraad* van x (de *ingraad* is het aantal y's met $(y,x) \in \Delta$).

Een *van* x *uitgaand pad* is een eindige rij punten $x_0,x_1,\ldots,x_n$ resp. oneindige rij punten $x_0,x_1,\ldots$ met $x_0 = x$, $x_i \in G$ voor alle i, $(x_{i-1},x_i) \in \Delta$ voor $i = 1,\ldots,n$ resp. $1,2,\ldots$. Het getal n resp. het symbool ∞ heet de *lengte* van het pad. Men eist niet dat het pad vrij is van herhalingen. Er kunnen ook *kringen* zijn (paden met $x_n = x_0$).

De *uitloop* van een punt x is het supremum van de lengte van de van x uitgaande paden. (Opmerking: als de uitloop van x oneindig is, hoeft er nog geen oneindig pad van x uit te gaan. Voorbeeld: $G = \{0,1,2,\ldots\}$, Δ bestaat uit alle $(i-1,i)$ met $i \in G\setminus\{0,1,4,9,16,\ldots\}$ en alle $(0,i)$ met $i \in \{1,4,9,16,\ldots\}$. Het punt 0 heeft uitloop ∞, maar er gaat geen oneindig pad van 0 uit. Ook de uitgraad van 0 is oneindig. In dit verband vermelden we het zgn. *oneindigheidslemma* van König dat uitspreekt dat in een graaf waar elk punt een eindige uitgraad heeft, de punten met oneindige uitloop wèl steeds uitgangspunt van een oneindig pad zijn.)

We kunnen G disjunct opsplitsen als

$$G = G_\infty \cup G_0 \cup G_1 \cup \ldots$$

naar punten met uitloop $\infty,0,1,\ldots$. Hier nemen we waar:

(i) Elk punt van G_0 is uitgangsloos.

(ii) Voor $i = 1,2,3,\ldots$ gaat van elk punt van G_i een pijl naar tenminste één punt van G_{i-1}, en geen enkele pijl naar een punt van G_j met $j \geq i$ of naar een punt van G_∞.

(iii) Uit een punt van G_∞ waaruit geen pijlen gaan die binnen G_∞ blijven, gaan pijlen naar G_i's met willekeurig grote i.

Merk op dat G_∞ alle kringen van de graaf bevat.

Vaak nemen we aan dat elk punt van G eindige uitloop heeft. In dat geval is G_∞ leeg.

§3. Bij een tweepersoonsspel wordt de vraag naar de *beste strategie* gesteld. Wat is in een gegeven stelling de beste zet voor Jan wanneer wordt aangenomen dat zijn tegenspeler zo goed mogelijk speelt? Het is niet gemakkelijk deze vraag goed te stellen. Pas nadat de vraag beantwoord is, kan men zien hoe ze gesteld moet worden! Want om te zeggen wat men verstaat onder "het beste voor Jan" zegt men dat Piet doet wat "het beste voor Piet" is, en om dat te kunnen zeggen moet men weer zeggen dat Jan doet wat "het beste voor Jan" is. Men zou deze knoop alleen maar kunnen ontwarren door een soort recursieve definitie te geven, met een beroep op de eindige speelduur. Eenvoudiger is het echter om alleen het antwoord te geven en de vraag achterwege te laten.

Gemakshalve zullen we ons beperken tot het geval dat elk punt eindige uitgraad zowel als eindige uitloop heeft.

STELLING 3.1. *Laat* (G,Γ) *een georiënteerde graaf zijn waarin elk punt eindige uitgraad en eindige uitloop heeft. Laat* u *een afbeelding zijn van de verzameling* G_0 *der uitgangsloze punten in de verzameling der reële getallen. Dan is er precies één afbeelding* ϕ *van* G *in de reële getallen met de eigenschap dat*

(i) $\phi(x) = u(x) \qquad (x \in G_0)$,

(ii) $\phi(x) = -\max\limits_{y\in\Gamma(x)} \phi(y) \qquad (x \in G\backslash G_0)$.

BEWIJS. Definieer ϕ op G_0 door (i). Nu kan ϕ op G_1 op precies één manier gekozen worden zó dat aan (ii) is voldaan; daarna kan ϕ op G_2 op precies één goede manier worden gekozen, enz. □

INTERPRETATIE. Bij elk uitgangsloos punt x is u(x) de *uitkering* die beloofd wordt aan de speler die het fiche er heen schuift; die uitkering wordt door de tegenstander betaald. Voor elke speler, en op elk moment van het spel, is (wanneer x de positie van het fiche is) de *waarde* van het spel gelijk aan $\phi(x)$ als hij niet aan zet is, en $-\phi(x)$ als hij wèl aan zet is (als $x \in G_0$ is komt dit laatste niet voor). De waarde die het spel voor een speler heeft kan dalen als hij bij zijn zet nalaat een uitgang y te kiezen met $\phi(y) = -\phi(x)$, en zijn waarde zal stijgen wanneer zijn tegenspeler een dergelijke keus verzaakt. Wanneer Jan op een zeker ogenblik als spelwaarde het bedrag c heeft, en verder steeds een y met $\phi(y) = -\phi(x)$ kiest, is hij zeker van een uitkering $\geqq$ c.

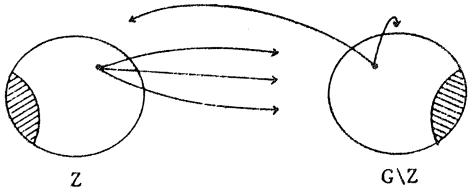
§4. Gevallen met uitkeringen ±1.

Hier gaat het alleen om "winst" of "verlies": wie de uitkering 1 toucheert, heeft gewonnen, wie -1 opstrijkt heeft verloren. De functie ϕ heeft nu ook alleen waarden ±1. We kunnen ϕ volledig beschrijven door de verzameling Z aan te geven van alle punten met $\phi(x) = +1$. Deze is gekenmerkt door de volgende eigenschappen:

(i) Er gaan geen pijlen uit Z naar Z,

(ii) Als $x \in G\backslash Z$, en x niet dood is, gaat er uit x tenminste één pijl naar Z.

(iii) De uitgangsloze punten x met $\phi(x) = 1$, liggen in Z, die met $\phi(x) = -1$ in $G\backslash Z$.



(De gearceerde stukken zijn dood).

§5. Voorbeelden.

§5.1. In voorbeeld 1.1 is $Z = \{25,21,17,13,9,5,1\}$.

§5.2. Het Nimspel.

Er zijn drie hoopjes lucifers; een zet bestaat uit het wegnemen van één of meer lucifers van eenzelfde stapel. Wie niet meer zetten kan heeft verloren. Men kan hier G beschrijven als de verzameling van alle tripels (k,l,m) met $k,l,m \in \{0,1,2,\ldots\}$. Het enige dode punt is $(0,0,0)$, met uitkering +1. De verzameling Z is

$$\{(k,l,m) \mid \forall_i \ \varepsilon_i(k) + \varepsilon_i(l) + \varepsilon_i(m) \equiv 0 \pmod 2\};$$

hierin is $\varepsilon_i(n)$ het i-de cijfer in de binaire representatie van n, van voren aangeduid met nullen:

$$n = \sum_{i=0}^{\infty} 2^{i-1} \varepsilon_i(n).$$

Wanner het spel met meer dan drie hoopjes gespeeld word, is de beschrijving analoog.

§5.3. Er is een variant op het nimspel die niet direct als zodanig opvalt (Wiskundige opgaven met de Oplossingen, deel 19(1) 1950, Vraagstuk 25).

			0			0		0			0		0	
1	2	3	4	5	6	7	8	9	.	.	.	.	.	

Er is een genummerde rij vakjes $(1,2,\ldots)$. Op elk vakje kan een fiche liggen; het aantal fiches is eindig. Een zet bestaat uit het naar links schuiven van een fiche, bij die zet mag het niet over een ander fiche heen gaan en ook niet op de plaats van een ander fiche terechtkomen. Als alle fiches aaneengesloten liggen aan het begin, is de positie dood; wie naar deze dode positie toe schuift heeft gewonnen (dus de uitkering van dit dode punt is +1).

Als de fiches liggen op $x_1,\ldots,x_m$ $(1 \leqq x_1 < x_2 < \ldots < x_m)$ hechten we aan deze positie een nim-positie bestaande uit de getallen

$$x_m - x_{m-1} - 1,\ x_{m-2} - x_{m-3} - 1,\ \ldots,\ x_1 - 1$$

als m oneven is, en

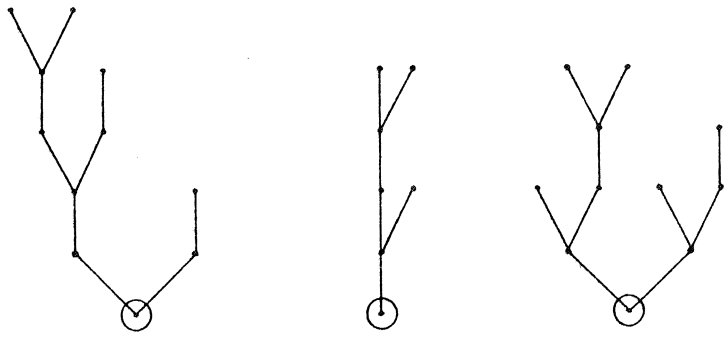
$$x_m - x_{m-1} - 1,\ x_{m-2} - x_{m-3} - 1,\ \ldots,\ x_2 - x_1 - 1$$

als m even is.

Als we de Z vastleggen als bij het nim-spel, voldoet Z weer aan 4(i), 4(ii) en 4(iii). Merk op dat de spelers soms één der nimgetallen ook *groter* kan maken; niettemin loopt het spel in eindig vele zetten af.

§5.4. Nim op boompjes. (R. Sprague)

Men tekent een aantal boompjes, en legt bij elk boompje één fiche in het onderste punt.



Een zet bestaat uit het naar boven schuiven van één der fiches over willekeurige afstand. De positie is dood als alle fiches in eindpunten liggen. De dode positie heeft uitkering 1. Als een fiche ergens in een boom ligt, kan men tellen wat het grootste aantal stapjes is dat het fiche nog naar boven zou kunnen doen, d.i. de uitloop naar boven. Zo

kan men aan een positie met k boompjes ook k getallen hechten, en daarop kan men gewoon nim spelen!

Het voordeel van dit boompjes-nim is, dat men bij elk spelletje nieuwe boompjes tekent, zodat degene die de strategie kent weinig laat merken aan een tegenspeler die de strategie niet kent.

§5.5. Spel van W.A. Wijthoff.

Er zijn twee hoopjes lucifers, maar behalve de nim-zetten is er nog een soort zet: men mag van beide hoopjes tegelijk nemen, mits van beide hetzelfde aantal. De dode positie (0,0) heeft weer waarde 1 en behoort dus tot Z.

Verder bestaat Z uit de paren

$$(0,0),\ (1,2),\ (3,5),\ (4,7),\ (6,10),\ \ldots$$

plus de gespiegelden van deze ((2,1), (5,3), ...). Afgezien van (0,0) zijn dit de paren (a_k,b_k) $(k = 1,2,\ldots)$ met

$$a_k = [k\tau], \quad b_k = [k\tau^2] = a_k + k,$$

wanneer $\tau = \frac{1}{2}(1 + \sqrt{5})$. Om de eigenschappen 4(i), 4(ii) te bewijzen stellen we $\alpha = \tau$, $\beta = \tau + 1$, zodat α en β positieve irrationale getallen zijn met $\alpha^{-1} + \beta^{-1} = 1$. Daaruit volgt dat er tussen n en n+1 $(n = 1,2,\ldots)$ precies één veelvoud van α òf precies één veelvoud van β ligt, want

$$[\tfrac{n}{\alpha}] + [\tfrac{n}{\beta}] = n - 1.$$

Hieruit zien we dat de rij $a_1,b_1,a_2,b_2,\ldots$ alle natuurlijke getallen elk één keer bevat, terwijl $b_k = a_k + k$, $a_1 < a_2 < \ldots$.

§6. Spelen met ongelijke rechten.

Er zijn spelen waarbij voor Jan andere regels gelden dan voor Piet. (Bij schaak mag Piet niet met Jan's stukken zetten!). We kunnen zo'n spel in onze beschouwingen betrekken door van G over te gaan op

$G \times A$, waarin A uit twee elementen a_J en a_P bestaat. De pijlen uit een punt (x,a_J) gaan naar de punten (y,a_P) waarin y de punten doorloopt waarheen Jan vanuit x mag zetten. Evenzo gaan er pijlen van punten (x,a_P) naar punten (y,a_J).

§7. Spelen waarin de beginner kan winnen als hij maar wist hoe.

Er zijn wat spelen bekend waarbij bewezen kan worden dat de beginner een winnende strategie heeft maar waarbij het erg moeilijk schijnt te zijn de winnende strategie aan te wijzen. Een fraai voorbeeld is Hex (zie M. Gardner, *Scientific American Problem Book*, Vol I, p. 77), maar al een simpel voorbeeld is het volgende. Op een blad papier staan de getallen 1,2,...,100. Een zet bestaat uit het schrappen van een getal, maar het is verboden een getal te schrappen waarvan al eerder een of ander veelvoud geschrapt is. Wie niet meer kan zetten, verliest. Jan begint.

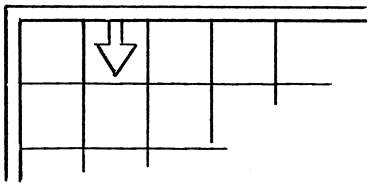
De spelgraaf heeft als puntverzameling G de verzameling van alle deelverzamelingen (de geschrapte getallen) van $\{1,\ldots,100\}$. De pijlen worden volgens de gestelde regels aangebracht. De graaf voldoet aan de eisen van stelling 3.1. We laten zien dat de beginstand, d.i. de lege verzameling, niet tot Z behoort. Neem aan dat de beginstand tot Z behoort. Dan gaat elke zet daaruit naar $Y = G \setminus Z$; in het bijzonder is de stand waarbij slechts het getal 1 is geschrapt in Y gelegen. Er is van daaruit dus een zet naar Z mogelijk. Als die zet bestaat uit het schrappen van het getal k ($k > 1$), dan is de stand waarbij 1 en k geschrapt zijn, in Z gelegen. De stand waarbij slechts k geschrapt is, ligt niet in Z (want die is in één zet uit de beginstelling te halen). Maar de stand waarbij 1 en k geschrapt zijn heeft dezelfde waarde als de stand waarbij alleen k geschrapt is: in beide gevallen zijn de uitbreidingsmogelijkheden dezelfde, en ze leiden weer tot standen die slechts verschillen wat de 1 betreft. Dit geeft een tegenspraak.

Een wat meer intuïtieve redenering is de volgende. Beschouw naast ons spel S het spel S' waarbij men werkt met de getallen 2,3,...,100. In het spel S kan alleen Jan de 1 schrappen en dat alleen bij de eerste zet; besluit hij om bij de eerste zet een ander getal te schrappen, dan

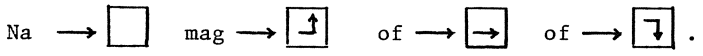
kan later niemand meer de 1 schrappen. We kunnen dus zeggen dat in plaats van het spel S we even goed het spel S' kunnen spelen maar de beginner Jan het recht geven om bij de eerste zet zijn beurt voorbij te laten gaan. Zijn strategie is nu om zijn beurt voorbij te laten gaan als het spel S' voor de beginner verloren is, en anders niet. Deze taktiek (tempozet) is bij schaken welbekend, bijv. wanneer in een pionneneindspel de ene koning een driehoekje kan draaien en de ander niet.

§8. Spel met verrassende strategie.

Op een schaakbord wordt een wandeling gemaakt, waarvan het begin is voorgeschreven, bijv.



Een zet bestaat uit het voortzetten van deze wandeling over één veld en het voorschrijven van de uitgang: die uitgang moet verschillen van de ingang op het veld. Een veld mag niet meer dan één keer gebruikt worden. De zetmogelijkheid geven we in een figuur aan:



Wie niet meer zetten kan heeft gewonnen; het is dus zaak te proberen zó te spelen dat de tegenstander nog kan doorgaan.

De beginner Jan kan dit spel winnen. In gedachten verdeelt hij het bord van 64 velden in 32 dominostenen: bij iedere zet komt hij in een dominosteen terecht. Zij strategie bestaat er nu uit te zorgen dat Piet zijn zet binnen dezelfde dominosteen moet houden; Jan gaat dus de kromme richten op de middenlijn van de steen. Het gevolg is dat Jan elke keer dat hij kan zetten, een nog onaangebroken steen voor zich ziet.

§9. Spelen met remisemogelijkheid.

Laat G een geöriënteerde graaf zijn; de uitgraad van elk punt is eindig; de uitloop mag oneindig zijn. Aan elk dood punt is een der waarden ±1 gehecht. We kunnen nu G opsplitsen in winstposities (Z), verliesposities (Y) en remiseposities (R) (winstpositie betekent winst voor degene die er naartoe zet en verlies voor degene die er van uit moet gaan).

Deze indeling heeft de volgende eigenschappen:

(i) De dode punten met waarde 1 liggen in Z.

(ii) De dode punten met waarde -1 liggen in Y.

(iii) Uit geen punt van $Z \cup R$ gaat een pijl naar Z.

(iv) Uit een punt van Z gaat geen pijl naar R.

(v) Uit een niet-dood punt van Y gaat steeds tenminste één pijl naar Z.

(vi) Uit een punt van R gaat tenminste één pijl naar R.

In paragraaf 4 legde een dergelijk stel eigenschappen de Z en $G\backslash Z$ eenduidig vast; hier is het wat minder eenvoudig, en we zullen ook niet proberen de indeling volledig door eisen als (i) - (vi) te karakteriseren.

We construeren Z en Y als volgt. Eerst verdelen we de dode punten over Z en Y volgens (i) en (ii). Die vormen de verzameling Z_0 en Y_0. Vervolgens zetten we elk punt uit $G\backslash(Z_0 \cup Y_0)$ in Z_1 als al zijn uitgangen in Y_0 liggen, en in Y_1 als tenminste één uitgang in Z_0 ligt. In de volgende ronde zetten we elk punt uit $G\backslash(Z_0 \cup Y_0 \cup Z_1 \cup Y_1)$ in Z_2 als al zijn uitgangen in $Y_0 \cup Y_1$ liggen, en in Y_2 als tenminste één uitgang in $Z_0 \cup Z_1$ ligt. Dit procédé wordt oneindig vaak voortgezet. We nemen nu

$$Z = \bigcup_{i=0}^{\infty} Z_i, \quad Y = \bigcup_{i=0}^{\infty} Y_i, \quad R = G\backslash(Z \cup Y).$$

Wie naar Z schuift en dat in het verdere spelverloop blijft doen, is zeker van de winst. Wie vanuit Y naar Y schuift, verspeelt 2 punten, wie vanuit Y naar R of vanuit R naar Y schuift, verliest 1 punt.

§10. Een spel met remise-strategie.

Jan en Piet zetten om de beurt een witte resp. zwarte schijf op een in 4 richtingen oneindig schaakbord. Geen veld mag dubbel bezet worden. Wie voor het eerst 9 schijven aaneengesloten op een rij heeft (horizontaal, vertikaal of diagonaal), heeft gewonnen. Als Jan begint kan Piet dit spel als volgt remise houden. Hij verdeelt in gedachten het bord in H's; dat zijn figuren van de vorm

1		5
2	4	6
3		7

(Afgezien van translaties en spiegelingen kan dat maar op één manier). Als er ergens 9 witte schijven aaneengesloten staan, komt het ergens voor dat er in een H 3 witte schijven op een rijtje staan, en wel in de linkerpoot als het een vertikale rij betreft. Als Piet er nu voor zorgt dat hij steeds in dezelfde H zet waar Jan het laatste in zette, kan hij het spel in elke H remise houden. Als Jan begint op 4, zet Piet daarna 2; als Jan's eerste zet niet 4 is, doet Piet dit als eerste zet.

Literatuur.

E.R. Berlekamp, J.H. Conway en R.K. Guy , Winning Ways, 2 vols. Academic Press 1982.

D. König, Theorie der Endlichen und Unendlichen Graphen, Leipzig 1936; Chelsea Publ. Comp. 1950

R. Sprague, Recreation in Mathematics. (Transl. T.H. O'Beirne). Black

F. Schuh, Wonderlijke Problemen. W.J. Thieme & Cie. 1943.

REIZEN OP EEN GRAAF

J.K.Lenstra & A.H.G.Rinnooy Kan

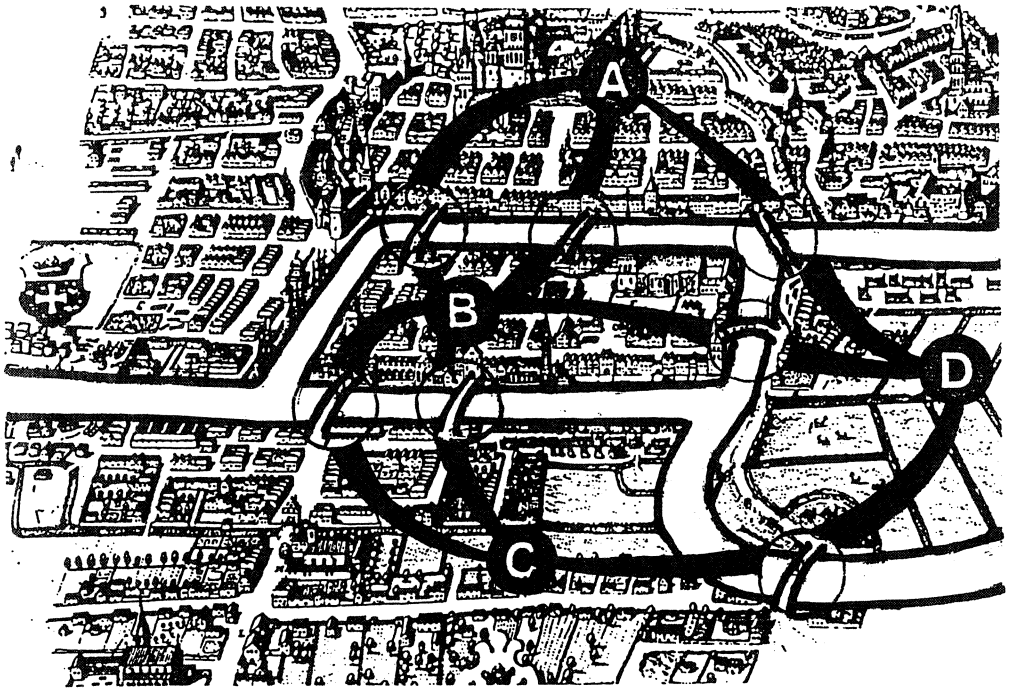
1. EULERPADEN EN HAMILTONCIRCUITS

Een *graaf* G wordt gedefinieerd door een verzameling V van n *punten* en een collectie E van *kanten*. Een kant e = (v,w) is een element van VxV. Als G *gericht* is heeft een kant (v,w) *beginpunt* v en *eindpunt* w; de *ingraad* $\vec{d}(v)$ en *uitgraad* $\overleftarrow{d}(v)$ van v geven het aantal kanten aan met v als eindpunt resp. beginpunt. Als G *ongericht* is identificeren we (w,v) met (w,v); v en w *liggen op* (v,w) en de *graad* d(v) van v is het aantal kanten waarop v ligt. Merk op dat E een *zelfkant* (*lus*)(v,v) en *meervoudige kanten* (v,w),...,(v,w) kan bevatten.

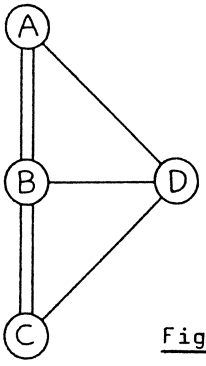
Een reis op een graaf vindt plaats langs een *pad* $(v_1,v_2,\ldots,v_k)$ met $(v_i,v_{i+1}) \in E$ voor i = 1,...,k-1; we spreken van een *circuit* als $v_1 = v_k$. Bij gerichte grafen is dus in elke kant sprake van éénrichtingsverkeer; kanten in een ongerichte graaf mogen in twee richtingen doorlopen worden. We beperken ons tot *samenhangende* grafen waarin met verwaarlozing van eventuele richtingen van de kanten, tussen elk tweetal punten een pad te vinden is.

Een reiziger op een graaf kan zich afhankelijk van zijn doelstellingen voor diverse problemen gesteld zien. Zo is het bijvoorbeeld mogelijk dat hij gaarne *elke kant precies één keer* zou willen doorlopen. Voor deze

opgave zag de Zwitserse wiskundige LEONHARD EULER (1707-1783) zich geplaatst, toen hij wilde nagaan of het mogelijk was tijdens een wandeling in de stad Königsberg de zeven bruggen over de rivier de Pregel elk precies één keer over te steken. Waar zijn zwakke gezichtsvermogen uitgebreide experimenten tot een riskante aangelegenheid maakte, leerde een blik op de plattegrond (Figuur 1.1(a)) hem al spoedig dat een dergelijke wandeling



(a)



(b)

Figuur 1.1 De zeven bruggen van Königsberg

niet te maken was. Een achtste brug zou hiervoor noodzakelijk zijn en volgens niet bevestigde geruchten is die in het huidige Kaliningrad inmiddels ook aangelegd.

Elke brug in Figuur 1.1(a) komt overeen met een kant van de ongerichte graaf in Figuur 1.1(b). In het algemeen kan men zich afvragen of in een gegeven graaf een pad of circuit te vinden is dat elke kant precies één keer doorloopt. Een dergelijke route heet een *Eulerpad* resp. *Eulercircuit*.

Het is duidelijk dat in een ongerichte graaf die een Eulercircuit bevat de graad d(v) van elk punt v even is. Bestaat er een Eulerpad, dan zijn er ten hoogste twee punten van oneven graad. In een gerichte graaf die een Eulercircuit bevat is $\vec{d}(v) = \overleftarrow{d}(v)$ voor elke v. Een analoge eigenschap van gerichte grafen die een Eulerpad bevatten is eenvoudig te formuleren.

Deze *noodzakelijke* voorwaarden voor de existentie van Eulerpaden en Eulercircuits blijken ook *voldoende* te zijn. Men kan eenvoudig aantonen dat de onderstaande algoritme van FLEURY in een ongerichte graaf met d(v) even voor alle v een Eulercircuit construeert:

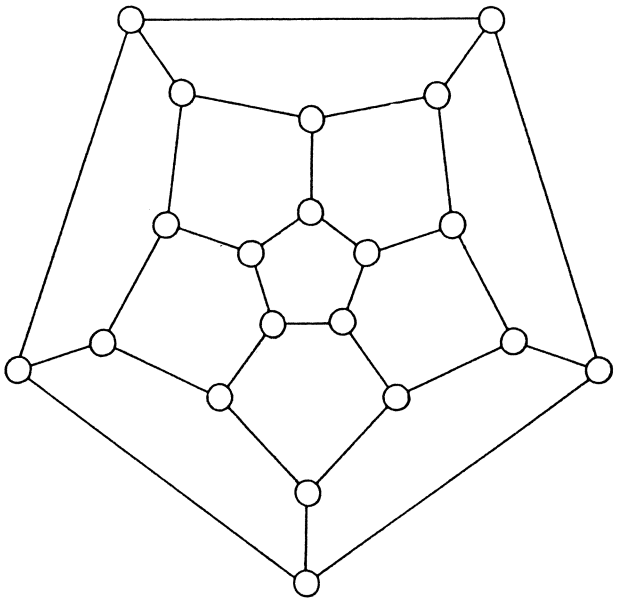
Begin in een willekeurig punt en doorloop de kanten op willekeurige wijze met inachtneming van twee regels:

- verwijder elke doorlopen kant en elk punt dat daardoor graad 0 krijgt;
- gebruik een kant die na verwijdering de graaf in twee samenhangende stukken uiteen zou doen vallen alleen als het niet anders kan.

Deze methode laat zich gemakkelijk uitbreiden tot Eulerpaden en gerichte grafen.

Aangemoedigd door deze resultaten bekommeren wij ons nu om de reziger op een graaf die gaarne *elk punt precies één keer* zou willen bezoeken en zich afvraagt of een dergelijke reis uitvoerbaar is. Hij zou op dit probleem gestuit kunnen zijn doordat hij een exemplaar van het spel "all around the world", ontworpen door de Ierse wiskundige SIR WILLIAM HAMILTON (1805-1865), heeft aangeschaft. De opgave in dit spel bestaat uit het vinden van een gesloten route langs de ribben van het dodecahedron, afgebeeld in Figuur 1.2, waarbij elk hoekpunt precies één keer bezocht moet worden. Het spel was geen commercieel succes, maar de naam van de ontwerper is aan het probleem gekoppeld gebleven; een circuit of pad op een graaf dat elk

punt precies één keer bezoekt heet een *Hamiltoncircuit* resp. *Hamiltonpad*.



Figuur 1.2 "All around the world"

Analoog aan de analyse van Eulerpaden en Eulercircuits zouden wij noodzakelijke en voldoende voorwaarden willen weten voor de existentie van Hamiltoncircuits en Hamiltonpaden. Helaas stuiten wij hier op een berucht en vooralsnog onopgelost probleem. Er zijn slechts enkele *voldoende* voorwaarden bekend, zoals bijvoorbeeld de stelling van ORE:

Een ongerichte graaf bevat een Hamiltoncircuit (Hamiltonpad) als $n \geqslant 3$ en $d(v)+d(w) \geqslant n$ $(d(v)+d(w) \geqslant n-1)$ voor alle $(v,w) \notin E$.

Noodzakelijk zijn deze voorwaarden niet, zoals de bestudering van een regelmatige vijfhoek onmiddellijk aantoont. Een soortgelijk resultaat is:

Een gerichte graaf bevat een Hamiltonpad als voor elk paar $(v,w) \in V \times V$ geldt dat òf $(v,w) \in E$ òf $(w,v) \in E$ (een dergelijke graaf wordt een *tournooi* genoemd).

Voor de bewijzen van bovenstaande en vergelijkbare stellingen verwijzen we naar BERGE [3] en LIU [7].

Tot dusver is de reiziger op de graaf geconfronteerd met *existentieproblemen*. In een *gewogen* graaf, waar aan elke kant een gewicht (lengte) is toegekend, kan hij met *optimaliseringsproblemen* te maken krijgen. Hieraan besteden we aandacht in het volgende hoofdstuk.

VRAAGSTUKKEN

1.1 Formuleer het Königsberger bruggenprobleem als het probleem om in een ongerichte graaf een Hamiltonpad te vinden.

1.2 Kunnen de 28 dominostenen zodanig in een cirkel gelegd worden dat de aangrenzende helften van elk paar opeenvolgende dominostenen gelijk zijn?

1.3 Laat zien dat 2^n nullen en enen zodanig op een cirkel te rangschikken zijn dat de 2^n n-tupels van n opeenvolgende cijfers alle verschillend zijn. (Er zijn $2^{2^{n-1}-n}$ dergelijke *De Bruijn-rijen*.)

1.4 Laat zien dat de 2^n verschillende n-tupels van nullen en enen zodanig op een cirkel te rangschikken zijn dat elke twee opeenvolgende n-tupels slechts op één plaats van elkaar verschillen. (Het is niet bekend hoeveel dergelijke *binaire Gray-codes* er zijn als functie van n.)

1.5 Stel dat er één drukpers en één bindmachine beschikbaar zijn om n boeken te produceren. Laten d_i en b_i de tijden zijn benodigd om boek i te drukken resp. te binden. Als voor elk tweetal boeken (i,j) geldt dat òf $d_i \leqslant b_j$ òf $d_j \leqslant b_i$, laat dan zien dat de boeken in een zodanige volgorde kunnen worden gedrukt dat de bindmachine zonder interrupties in bedrijf is.

1.6 Een paard moet elk veld van een n×n-schaakbord precies één keer bezoeken en weer op zijn startveld terugkeren. Is dit mogelijk voor n = 4, n = 6, n = 8?

2. KORTSTE PADEN, CHINESE POSTBODEN EN HANDELSREIZIGERS

Bevindt een reiziger zich in een punt van een gewogen graaf G, dan is een voor de hand liggende vraag welke van de paden naar een ander punt het kortste is. Laat G een gerichte graaf zijn met $V = \{v_1,\ldots,v_n\}$; aan elke kant $(v_i,v_j) \in E$ is een niet-negatief gewicht c_{ij} toegekend. De lengte van het kortste pad van v_1 naar v_j wordt aangeduid met d_j, waarbij $d_1 = 0$. Onderstel eerst dat G *acyclisch* is, d.w.z. geen circuits bevat. De kortste paden van v_1 naar alle punten v_j die uit v_1 bereikbaar zijn kunnen dan recursief worden bepaald m.b.v. de vergelijking

$$d_j = \min\{d_i+c_{ij} \mid (v_i,v_j) \in E\}.$$

Het is duidelijk dat deze methode hoogstens $\frac{1}{2}n(n-1)$ optellingen en $\frac{1}{2}(n-1)(n-2)$ vergelijkingen vergt: de *orde* van de methode is $O(n^2)$. Een dergelijke algoritme waarbij het aantal berekeningen polynomiaal begrensd is in de probleemparameters noemen we een *goede* of *efficiënte* algoritme. Merk op dat hier geen gebruik gemaakt wordt van de niet-negativiteit van de gewichten.

Indien G wel circuits bevat kunnen wij de volgende methode van G.B.DANTZIG toepassen. Stel dat we na de s-de stap van de algoritme de kortste paden gevonden hebben van v_1 naar alle punten in een verzameling $S \subset V$ met $|S| = s$. We bepalen voor elk punt $v_i \in S$ een punt $v_{i'} \notin S$ zodanig dat $c_{ii'} = \min\{c_{ik} \mid v_k \notin S,\ (v_i,v_k) \in E\}$. We kiezen vervolgens uit de punten $v_{i'}$ een punt $v_{j'}$ waarvoor

$$d_j+c_{jj'} = \min\{d_i+c_{ii'} \mid v_i \in S\}$$

en voegen $v_{j'}$ als (s+1)-ste punt aan S toe. Het is duidelijk dat $d_{j'} = d_j+c_{jj'}$, want elk pad van v_1 naar $v_{j'}$ moet via een punt $v_i \in S$ lopen en heeft dus een lengte tenminste gelijk aan $d_i+c_{ii'} \geqslant d_{j'}$.

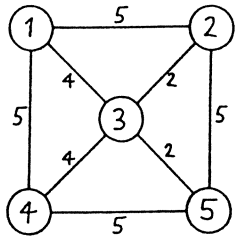
In een handige implementatie van E.W. DIJKSTRA is bovenstaande procedure uit te voeren in $O(n^2)$ stappen. Uitbreiding tot ongerichte grafen vindt plaats door elke ongerichte kant (v_i,v_j) te vervangen door twee gerichte kanten (v_i,v_j) en (v_j,v_i), beide met gewicht c_{ij}.

Staan wij ook negatieve gewichten toe, dan wordt het probleem lastiger maar het blijft efficiënt oplosbaar, tenzij de graaf circuits bevat van negatief totaal gewicht. Voor dit laatste geval is het bestaan van een efficiënte algoritme zeer onwaarschijnlijk (vgl. vraagstuk 2.3).

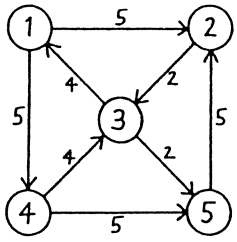
Gewapend met deze kennis wenden wij ons nu tot de reiziger die aan de hand van Eulers inzichten tot de conclusie is gekomen dat een eenmalig bezoek aan elke kant voor hem niet is weggelegd. Ongenoegen over deze situatie bestaat bijvoorbeeld bij een *postbode*, die zich beroepshalve toch verplicht acht een dergelijk bezoek af te leggen. Hij hoopt nu een zodanige gesloten route te kunnen vinden dat de totale lengte van de meer dan eens te doorlopen kanten (en daarmee de lengte van de gehele route) minimaal is. Wij kunnen hem onderstaande efficiënte algoritmen voor het *Chinese postbodeprobleem* (zo genoemd ter ere van de geestelijke vader MEI-KO KWAN) aanbieden.

Wij bekijken eerst het probleem op een *ongerichte* graaf G. De resultaten van hoofdstuk 1 wijzen uit dat wij paden zullen moeten toevoegen tussen punten van oneven graad, zodanig dat hun graad even wordt. In de *eerste stap* van de algoritme construeren wij een ongerichte graaf H op de m punten van G van oneven graad; merk op dat m even is. Tussen elk tweetal punten van H wordt een kant gelegd (een dergelijke graaf heet *volledig*) en elke kant (v,w) krijgt als gewicht de lengte van het kortste pad in G tussen v en w. Al deze gewichten zijn in $O(n^3)$ berekeningen te bepalen m.b.v. de algoritme van Dijkstra. In de *tweede stap* zoeken wij in H naar een deelverzameling van $\frac{1}{2}m$ kanten van minimaal totaal gewicht zodanig dat elk punt op precies één van deze kanten ligt. Een dergelijke minimale *koppeling* is in $O(m^3)$ berekeningen te vinden m.b.v. een ingenieuze algoritme van J. EDMONDS. In de *derde stap* tenslotte breiden wij G uit met de $\frac{1}{2}m$ paden die met de koppeling in H corresponderen. Alle punten van G zijn daardoor van even graad geworden en het kortste Eulercircuit voor de postbode laat zich vinden m.b.v. de algoritme van Fleury. De gehele procedure, daterend uit 1965, is geïllustreerd aan een voorbeeld in Figuur 2.1(a).

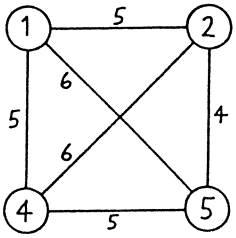
Voor het Chinese postbodeprobleem op een *gerichte* graaf G was al langer een efficiënte algoritme bekend. Uit eerdere overwegingen is het duidelijk dat we alleen paden hoeven toe te voegen van $S = \{v \mid \vec{d}(v) > \overleftarrow{d}(v)\}$ naar $T = \{v \mid \vec{d}(v) < \overleftarrow{d}(v)\}$. In de *eerste stap* van de algoritme vervangen wij elk



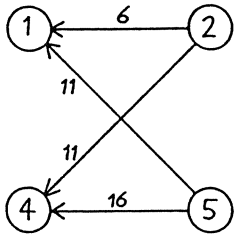
Graaf G



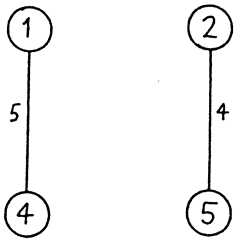
Graaf G



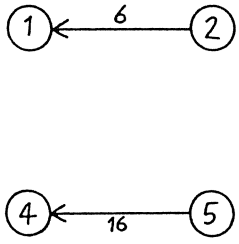
Volledige graaf H



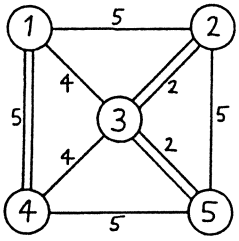
Volledige bipartite graaf H



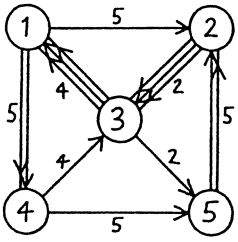
Minimale koppeling in H;
gewicht 9



Minimale toewijzing in H;
gewicht 22



Uitgebreide graaf G;
totaal gewicht 41



Uitgebreide graaf G;
totaal gewicht 54

(a) G is ongericht (b) G is gericht

Figuur 2.1 Chinese postbodeproblemen

punt $v \in S \cup T$ door $|\vec{d}(v)-\overleftarrow{d}(v)|$ kopieën; dit geeft twee verzamelingen S' en T' met $|S'| = |T'| = m$. Wij construeren een graaf H met puntenverzameling $S' \cup T'$ en kantenverzameling $S' \times T'$ (een graaf op twee disjuncte puntenverzamelingen waarin geen enkele kant twee punten uit dezelfde verzameling met elkaar verbindt heet *bipartiet*; H is een volledige bipartite graaf). Elke kant krijgt weer als gewicht de lengte van het overeenkomstige kortste pad in G. In de *tweede stap* zoeken wij in H naar een minimale koppeling van m kanten. Het koppelingsprobleem in een bipartite graaf heet een *toewijzingsprobleem*, omdat aan elk punt in S' precies één punt in T' wordt toegewezen en vice versa. Er bestaan diverse technieken om een minimale toewijzing in $O(m^3)$ berekeningen te bepalen. In de *derde stap* tenslotte levert uitbreiding van G met de m kortste paden die met deze toewijzing corresponderen, de oplossing van het probleem. Een uitgewerkt voorbeeld is te vinden in Figuur 2.1(b).

Slechts wanneer G een *gemengde* graaf is, d.w.z. zowel gerichte als ongerichte kanten bevat, kunnen wij het Chinese postbodeprobleem niet op efficiënte wijze oplossen. Waar het de bepaling van routes betreft wordt een sneeuwruimer voor moeilijker opgaven geplaatst dan een brievenbesteller.

Het is te verwachten dat ook de reiziger die een eenmalig bezoek aan elk punt wenst te brengen deze eis zal afzwakken tot het tenminste één keer bezoeken van elk punt. Definiëren we op de puntenverzameling V van de oorspronkelijke graaf G een volledige graaf G* met als gewicht c_{ij} voor elke kant (v_i,v_j) de lengte van het corresponderende kortste pad in G, dan is hij nu in wezen geïnteresseerd in de vraag welke van de $(n-1)!$ Hamiltoncircuits in G* het kortste is. De oplossing van een dergelijk probleem kan bijvoorbeeld van belang zijn voor een *handelsreiziger* die zijn klanten liefst in een zodanige volgorde bezoekt dat hij zo snel mogelijk weer thuis is. Het zal geen enkele automobilist verbazen dat het handelsreizigersprobleem *asymmetrisch* kan zijn: c_{ij} en c_{ji} zijn dan niet gelijk voor alle (v_i,v_j).

Geven wij elke kant van G een gewicht gelijk aan 1, dan zou een efficiënte methode om het kortste Hamiltoncircuit in G* te bepalen ons tevens op efficiënte wijze duidelijk maken of G een Hamiltoncircuit bevat of niet; in het laatste geval is de optimale route in G* namelijk langer dan n. Gezien de complexiteit van het existentieprobleem op G lijkt het niet waar-

schijnlijk dat een dergelijke efficiënte algoritme bestaat.

Gelukkig zijn er diverse methoden geconstrueerd waarmee de handelsreiziger toch, zij het op niet efficiënte wijze, geholpen kan worden. Een belangrijke plaats nemen de z.g. *branch-and-bound* methoden in, die gebaseerd zijn op *impliciete aftelling* van alle (n-1)! elementen van de oplossingsverzameling F. Elk element van F correspondeert met een bepaald Hamiltoncircuit in G*. F wordt nu successievelijk gesplitst in steeds kleinere deelverzamelingen. Een deelverzameling $F' \subset F$ kan op twee manieren *geëlimineerd* worden:

(1) F' bevat slechts één oplossing;

(2) geen enkele oplossing in F' heeft een lagere waarde dan de beste oplossing die wij tot op dat moment gevonden hebben.

Een branch-and-bound procedure ligt zodoende vast door drie voorschriften:

(A) een *splitsingsvoorschrift* dat aangeeft hoe een bepaalde deelverzameling $F' \subset F$ gesplitst moet worden in (liefst disjuncte) deelverzamelingen;

(B) een *ondergrensberekening* die bij elke gegenereerde deelverzameling F' een getal LB(F') levert dat kleiner dan of gelijk aan de waarde van elke oplossing in F' is;

(C) een *zoekstrategie* die vastlegt welke van de nog niet geëlimineerde deelverzamelingen in aanmerking komt voor verdere splitsing.

Op elk moment levert de waarde van de beste tot dan toe gevonden oplossing een *bovengrens* UB op voor de waarde van de optimale oplossing. Als F' t.g.v. (1) wordt geëlimineerd kan dit een verlaging van UB tot gevolg hebben; eliminatie t.g.v. (2) vindt plaats als $LB(F') \geqslant UB$. We zoeken nu net zo lang verder, voortdurend UB aanpassend, totdat alle gegenereerde deelverzamelingen geëlimineerd zijn. UB is dan gelijk aan de waarde van de optimale oplossing.

Voor het handelsreizigersprobleem zijn verscheidene splitsingsvoorschriften en ondergrensberekeningen bedacht. Een ondergrens LB(F) voor de lengte van het kortste Hamiltoncircuit in G* laat zich bijvoorbeeld berekenen door een bipartite graaf H te construeren op twee kopieën V' en V" van V met kantenverzameling $\{(v_i,v_j) | v_i \in V';\ v_j \in V'',\ i \neq j\}$; het gewicht van (v_i,v_j) is c_{ij}. In H bepalen we een minimale toewijzing. Het is duidelijk dat bij de met deze toewijzing corresponderende reis in G* precies één keer uit elk punt vertrokken wordt en precies één keer in elk punt aange-

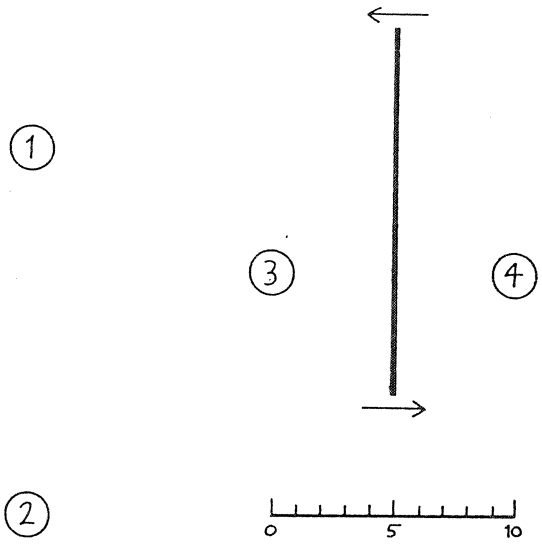
komen wordt. Niets garandeert echter dat de reis *samenhangend* is; hij kan best bestaan uit meer dan één circuit. Waar wij dus t.a.v. een Hamiltoncircuit strengere eisen stellen, is het totale gewicht van een minimale toewijzing in H nooit groter dan (en dus een ondergrens voor) de lengte van het kortste Hamiltoncircuit in G*.

Als de toewijzing in H correspondeert met precies één circuit in G* zijn we natuurlijk klaar. Anders bekijken we één van de circuits $(v_{i_1}, v_{i_2}, \ldots, v_{i_k}, v_{i_1})$ (bijvoorbeeld elk circuit waarvoor k minimaal is). De kanten in dit circuit kunnen nooit alle in één Hamiltoncircuit voorkomen en dit levert ons een splitsingsvoorschrift. We creëren k deelverzamelingen van F die tezamen F overdekken, door achtereenvolgens de kanten $(v_{i_1}, v_{i_2}), \ldots, (v_{i_{k-1}}, v_{i_k}), (v_{i_k}, v_{i_1})$ te verbieden middels het op oneindig stellen van resp. $c_{i_1 i_2}, \ldots, c_{i_{k-1} i_k}, c_{i_k i_1}$. De oplossing van de nieuwe toewijzingsproblemen levert een ondergrens voor elk van deze deelverzamelingen op.

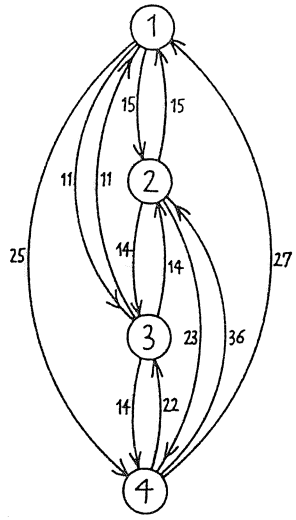
Wij kiezen nu (bijvoorbeeld) de deelverzameling met de laagste ondergrens voor verder onderzoek. Op deze wijze voortgaand tellen wij de gehele verzameling F impliciet af; elke gegenereerde deelverzameling wordt gekarakteriseerd door een aantal kanten die verboden zijn doordat hun gewichten op oneindig zijn gesteld.

Bij wijze van voorbeeld bekijken wij de situatie weergegeven in Figuur 2.2(a). De grafen G* en H zijn afgebeeld in Figuur 2.2(b,c). De minimale toewijzing in H bestaat uit de kantenverzameling {(1,2),(2,1),(3,4),(4,3)}, heeft gewicht LB(F) = 66, en correspondeert met twee circuits (1,2,1) en (3,4,3) in G*. F wordt gesplitst in twee deelverzamelingen F_1 en F_2 door resp. c_{12} en c_{21} op oneindig te stellen. In F_1 heeft de minimale toewijzing {(1,3),(2,4),(3,2),(4,1)} een gewicht $LB(F_1) = 75$; in F_2 heeft de minimale toewijzing {(1,2),(2,3),(3,4),(4,1)} een gewicht $LB(F_2) = 70$. Beide toewijzingen leveren een Hamiltoncircuit in G*; het tweede hiervan is de optimale oplossing (1,2,3,4,1).

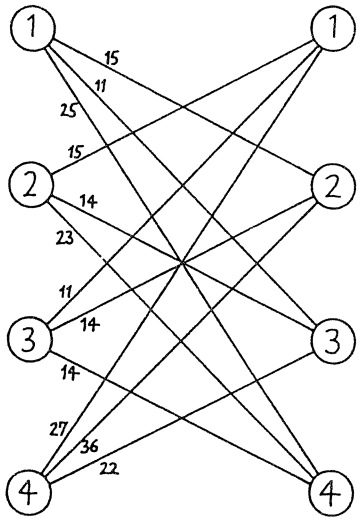
De hierboven geschetste procedure is in 1958 ontwikkeld door W.L. EASTMAN. Zij heeft twee nadelen:



(a) Plattegrond met wegversperring



(b) Volledige graaf G^*



(c) Bipartite graaf H

Figuur 2.2 Een handelsreizigersprobleem

(1) als het probleem symmetrisch is, d.w.z. $c_{ij} = c_{ji}$ voor alle (v_i,v_j), zullen bij de ondergrensberekening relatief veel circuits van twee kanten ontstaan;

(2) het splitsingsvoorschrift leidt niet tot disjuncte deelverzamelingen.

Wij verwijzen naar [1] voor een bespreking van de wijze waarop deze bezwaren ondervangen kunnen worden.

Impliciete aftellingsprocedures als de bovenstaande worden gebruikt voor het oplossen van vele combinatorische optimaliseringsproblemen, indien er tenminste aanwijzingen zijn dat er geen efficiënte algoritme bestaat. De voornaamste uitdaging ligt dan in het construeren van een zodanig scherpe ondergrens dat de eventueel wat langere tijd die nodig is om hem te berekenen ruimschoots gecompenseerd wordt door de vroegtijdige eliminatie van grote deelverzamelingen. Bij elk van deze methoden is de rekentijd echter nogal onvoorspelbaar; vaak neemt zij drastisch (*superpolynomiaal*) toe met de omvang van het probleem. Bij grote problemen zoals die in de praktijk optreden ($n \geqslant 80$) zal men tevreden moeten zijn met het vinden van goede maar mogelijk niet optimale oplossingen. Hierover maken we enige opmerkingen in het laatste hoofdstuk.

VRAAGSTUKKEN

2.1 In een communicatienetwerk is de kans dat een bericht uit v in w aankomt gelijk aan p(v,w). Al deze kansen zijn onafhankelijk van elkaar. Formuleer het probleem van de betrouwbaarste route tussen twee punten als een kortste-padprobleem.

2.2 Als activiteit v vóór activiteit w moet geschieden geven wij dat aan d.m.v. een kant (v,w) in de gerichte graaf G. Aan iedere punt wordt een gewicht toegekend, corresponderend met de tijdsduur van de betreffende activiteit. De lengte van het langste pad tussen de (mogelijk fictieve) eerste en laatste activiteit bepaalt de minimale tijdsduur van het gehele project. Laat zien dat G acyclisch is en dat het zgn. *kritieke pad* op efficiënte wijze gevonden kan worden.

2.3 Vervang in een gewogen volledige graaf de gewichten c_{ij} door $\lambda - c_{ij}$, waarbij λ een groot getal is. Laat zien dat het kortste Hamiltonpad

van v naar w in de oorspronkelijke graaf correspondeert met het langste pad van v naar w in de nieuwe graaf dat elk punt hoogstens één keer bezoekt. Waarom levert dit geen efficiënte algoritme (vgl.vraagstuk 2.2)?

2.4 Laat zien dat algoritmen om in een graaf
- het kortste Hamiltonpad van een gegeven punt v naar een gegeven punt w
- het kortste Hamiltonpad

te vinden gebruikt kunnen worden om het handelsreizigersprobleem op te lossen.

2.5 Op een machine moeten n produkten gefabriceerd worden. De omschakeltijd als produkt i direct gevolgd wordt door produkt j is gelijk aan c_{ij}. Laat zien dat het bepalen van de kortste totale produktietijd een handelsreizigersprobleem is.

2.6 Op een machine moeten n produkten gefabriceerd worden; elk produkt vereist één tijdseenheid. Als produkt i klaar komt op tijdstip t brengt dit kosten $c_i(t)$ met zich mee. De functies c_i zijn monotoon niet-dalend in t. Laat zien dat het vinden van een produktievolgorde die de totale kosten minimaliseert een toewijzingsprobleem is.

3. PRAKTIJKPROBLEMEN

Routeringsproblemen dienen zich in de praktijk niet altijd aan in de gestyleerde vorm van Chinese postbode- of handelsreizigersproblemen. Vaak is er meer dan één reiziger beschikbaar om de klanten te bezoeken; zowel de totale hoeveelheid goederen die een reiziger kan vervoeren als de afstand die hij kan afleggen zijn daarbij begrensd. Daarnaast stellen ook de klanten hun eisen t.a.v. het bezoektijdstip of zelfs t.a.v. de reiziger die zij wensen te ontvangen.

Stel dat m handelsreizigers onder dergelijke nevenvoorwaarden hun weg langs n klanten moeten vinden vanuit een gemeenschappelijk vertrekpunt v.
We bekijken het vertrouwde handelsreizigersprobleem in een graaf op m+n punten, nl. m kopieën van het vertrekpunt en één punt voor elke klant.
Elk hernieuwd bezoek aan v door de eenzame handelsreiziger correspondeert

met het inzetten van een nieuwe reiziger in het oorspronkelijke probleem. Maken we de onderlinge afstand λ tussen de kopieën van v zeer groot, dan zullen inderdaad alle m reizigers op stap gaan; maken we λ zeer klein, dan zullen - met inachtneming van de oorspronkelijke restricties - zo weinig mogelijk reizigers gebruikt worden. In het algemeen kan men zeggen dat $-\lambda$ de kosten van het inzetten van een extra reiziger dient weer te geven.
Op deze wijze is o.m. bij de P.T.T. een aantal praktijkproblemen aangepakt; wij verwijzen naar [5] voor een uitgebreider toelichting.

Gezien de gebruikelijke omvang van praktijkproblemen, de verscheidenheid van de mogelijke nevenvoorwaarden en de fundamentele complexiteit van het handelsreizigersprobleem, zijn wij voor het oplossen van deze problemen aangewezen op *suboptimale* methoden (z.g. *heuristieken*) die relatief snel een goede maar wellicht niet optimale oplossing leveren.
Vaak kan bij het ontwikkelen van een dergelijke heuristiek met vrucht een beroep worden gedaan op ideeën ontwikkeld in de context van een gestyleerde. de vorm van het probleem. Zo heeft het vorige hoofdstuk ons bijvoorbeeld geleerd dat het Chinese postbodeprobleem aanzienlijk eenvoudiger is dan het handelsreizigersprobleem. Het ligt dan ook voor de hand om zoveel mogelijk punten die bezocht moeten worden te vervangen door kanten die doorlopen moeten worden en het resulterende probleem op te lossen, met een impliciete aftellingsprocedure die gebruik maakt van verkregen inzichten in het Chinese postbodeprobleem. Een dergelijke omzetting van verplichte punten in verplichte kanten kan leiden tot een niet-optimale oplossing, maar deze methode geeft in de praktijk heel acceptabele resultaten (vgl. [8;9;6]).

Concluderend kan men zeggen dat het vele werk om de klassieke problemen van postbode en handelsreiziger op te lossen het nodige rendement oplevert voor hen die onder ingewikkelder voorwaarden willen reizen op een graaf.

LITERATUUR

1. *M. Bellmore, J.C. Malone*, Pathology of traveling-salesman subtour elimination algoritms. Oper. Res. 19 (1971), 278-307, 1766.
2. *C. Berge*, The theory of Graphs and Its Applications. Methuen, London (1962).
3. *C. Berge*, Graphes et Hypergraphes. Dunod, Paris (1970).
4. *E.L. Lawler*, Combinatorial Optimization: Networks and Matroids. Holt, Rinehart, and Winston, New York (1976).
5. *J.K. Lenstra, A.H.G. Rinnooy Kan*, Some simple applications of the travelling salesman problem. Oper. Res. Quart. 26 (1975), 717-733.
6. *J.K. Lenstra, A.H.G. Rinnooy Kan*, On general routing problems. Networks 6 (1976), 273-280.
7. *C.L. Liu*, Topics in Combinatorial Mathematics. Mathematical Association of America (1972).
8. *C.S. Orloff*, A fundamental problem in vehicle routing. Networks 4 (1974), 35-64.
9. *C.S. Orloff*, Routing a fleet of M vehicles to/from a central facility. Networks 4 (1974), 147-162.
10. *R.J. Wilson*, Introduction to Graph Theory. Oliver & Boyd, Edinburgh (^{2}972).

Dit artikel, zonder de vraagstukken, is eerder verschenen in het *Nieuw Tijdschrift voor Wiskunde* 63 (1976), 221-229.

SPELTHEORIE

S.H. Tijs

1. INLEIDING

Speltheorie zou men kunnen omschrijven als een tak van de wiskunde welke zich bezighoudt met het ontwerpen en bestuderen van mathematische modellen van conflictsituaties. Oorspronkelijk geïnspireerd door strategische spelen (zoals pokeren, schaak, nim) is daarna haar inspiratiebron en werkterrein uitgebreid tot o.a. economie, statistiek en psychologie.

Vrijwel algemeen wordt aanvaard dat JOHN VON NEUMANN (1903-1957) de grondslag van deze theorie heeft gelegd met zijn artikel:
"Zur Theorie der Gesellschaftsspiele", Math. Ann. 100, 1928, 295-320. Vele van de ideëen hierin neergelegd zal ik tijdens deze voordracht opgraven. Overigens is de ontwikkeling van het vak pas goed doorgezet na het verschijnen van het boek:
"Theory of Games and Economic Behaviour" door J. VON NEUMANN & O.MORGENSTERN in 1944.

Niet alle conflictsituaties zijn in één model te vangen.

Een onderverdeling in klassen van spelen krijgt men door te kijken naar de volgende facetten welke bij elke conflictsituatie relevant zijn:

(1) het aantal spelers (deelnemers),
(2) de invloed van de spelers,
(3) de doelstellingen van de spelers.

Men onderscheidt tweepersoonsspelen van spelen met meer dan twee personen, eenzetsspelen van meerzetsspelen; spelen waarbij uitbetalingen reële getallen zijn van spelen waarbij om bijv. goederenpakketten gestreden wordt.

In deze voordracht zullen we ons beperken tot tweepersoonsspelen (waarbij de spelers aangegeven worden met I en II) en we veronderstellen dat de uitbetalingen in reële getallen kunnen worden uitgedrukt. Vragen als:
Wat is optimaal handelen?
Wat is het voor een speler waard aan een spel deel te nemen?
Hoe moeten optimale strategieën berekend worden?
liggen voor de hand.

2. TWEEPERSOONSSPELEN IN NORMALE VORM

We kijken eerst naar tweepersoonsspelen waarbij partijtjes als volgt verlopen: onafhankelijk van elkaar kiezen speler I en speler II elementen x en y uit voorgeschreven verzamelingen X en Y, waarna er uitbetalingen volgen aan speler I en speler II die afhankelijk zijn van het paar (x,y) en welke we zullen aangeven met $K_1(x,y)$ en $K_2(x,y)$. Laten we dit even formaliseren in

DEFINITIE 1. Een *tweepersoonsspel* (*in normale vorm*) is een geordend viertal $\langle X,Y,K_1,K_2\rangle$ waarbij X en Y niet-lege verzamelingen en $K_1: X \times Y \to \mathbb{R}$ en $K_2: X \times Y \to \mathbb{R}$ reëelwaardige funkties op $X \times Y$ zijn.

De elementen van X zullen we (*zuivere*) *strategieën van speler* I en de elementen van Y (*zuivere*) *strategieën van speler* II noemen. X, Y en $X \times Y$ heten achtereenvolgens: *strategieënruimte van speler* I, *strategieënruimte van speler* II en *uitkomstenruimte van het spel*. De funktie K_1 (resp. K_2) op de uitkomstenruimte noemen we de *uitbetalingsfunktie van speler* I (resp. speler II).

Op het eerste gezicht zijn in dit model weinig conflictsituaties te vangen maar de situatie is bij nadere beschouwing veel gunstiger zoals we in §3 zullen zien. Laten we eerst enkele voorbeelden geven welke rechtstreeks in dit model passen.

VOORBEELD 1. (DUOPOLYMODEL VAN A. WALD) Veronderstel dat een bepaald product geproduceerd wordt door twee producenten I en II welke achtereenvolgens productiecapaciteit $c_1 > 0$ en $c_2 > 0$ hebben. Als I besluit per tijdseenheid een hoeveelheid $x \in [0,c_1]$ te produceren en op de markt te brengen en als II besluit een hoeveelheid $y \in [0,c_2]$ per tijdseenheid aan te bieden, dan brengt het product een prijs $p(x+y) \geqslant 0$ per eenheid product op. Veronderstel dat bij een productie x (resp. y) door I (resp. II) de productiekosten $k(x) \geqslant 0$ (resp. $k(y) \geqslant 0$) bedragen. Dan is deze marktsituatie om te zetten in het tweepersoonsspel $\langle X,Y,K_1,K_2\rangle$ waarbij $X = [0,c_1]$, $Y = [0,c_2]$, en voor elke $x \in X$, $y \in Y$ geldt:

$$K_1(x,y) = xp(x+y)-k(x), \quad K_2(x,y) = yp(x+y)-k(y).$$

VOORBEELD 2. (GAME OF TIMING) In een duel tussen "spelers" I en II met van geluiddempers voorziene pistolen zijn de spelregels als volgt: alleen in het tijdsinterval $[0,T]$ $(T>0)$ mag er gevuurd worden. Elke speler mag hoogstens éénmaal schieten. Als één van de spelers de tegenstander treft dan moet de getroffene één eenheid aan de schutter betalen en mag zelf niet meer vuren. Laten we voor beide spelers de trefkans van de tegenstander ten tijde t stellen op $p(t)$ $(p(t) \in [0,1])$. [We veronderstellen dus gelijke duelcapaciteit]. We kunnen deze situatie herleiden tot het tweepersoonsspel $\langle X,Y,K_1,K_2\rangle$ waarbij $X = Y = [0,T]$ en

$$K_1(x,y) = \begin{cases} p(x) - (1-p(x))p(y) & \text{als } x < y \\ 0 & \text{als } x = y \\ -p(y) + (1-p(y))p(x) & \text{als } x > y \end{cases}$$

$$K_2(x,y) = -K_1(x,y) \text{ voor elke } (x,y) \in [0,T] \times [0,T].$$

DEFINITIE 2. Een tweepersoonsspel $\langle X,Y,K_1,K_2\rangle$ zullen we een *nulsomspel* noemen als

$$K_1(x,y) + K_2(x,y) = 0 \text{ voor elke } (x,y) \in X \times Y.$$

Het spel in voorbeeld 2 is een nulsomspel; het spel in voorbeeld 1 i.h.a. niet. In een nulsomspel vindt de verrekening na een partij tussen de spelers onderling plaats.

DEFINITIE 3. Een tweepersoonsspel $\langle X,Y,K_1,K_2\rangle$ zullen we een *eindig spel* noemen als de strategieënruimten X en Y eindig veel elementen bevatten. Laat

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

een $m \times n$-matrix zijn waarbij in de cellen reële getallen staan. Dan kunnen we hierbij een eindig tweepersoonsnulsomspel maken en wel als volgt: in een partijtje wijst speler I een rij $i \in \{1,2,\ldots,m\}$ en (onafhankelijk daarvan) speler II een kolom $j \in \{1,2,\ldots,n\}$ aan, waarna een uitbetaling a_{ij} volgt aan speler I door speler II.

Zo'n spel correspondeert dan met het tweepersoonsnulsomspel $\langle X,Y,K\rangle$ waarbij $X = \{1,2,\ldots,m\}$, $Y = \{1,2,\ldots,n\}$ en $K(i,j) = a_{ij}$ voor elke $(i,j) \in X \times Y$.

Zo'n spel heet een *matrixspel* en A noemt men de *uitbetalingsmatrix*. Merk op dat elk eindig tweepersoonsnulsomspel is om te zetten in een matrixspel door de strategieën van de spelers te nummeren.

VOORBEELD 3. (STEEN-PAPIER-SCHAAR-SPEL) Gelijktijdig noemen speler I en II een van de woorden uit de verzameling {S(teen), P(apier), Sc(haar)}. Er is afgesproken dat schaar van papier, papier van steen en steen van schaar wint en dat de partij onbeslist is als beide spelers hetzelfde woord noemen. Op een voor de hand liggende manier correspondeert dit spel met het

3 × 3-matrixspel

$$\begin{array}{cc} & \text{II} \\ & \begin{array}{ccc} S & P & Sc \end{array} \\ \text{I} \begin{array}{c} S \\ P \\ Sc \end{array} & \begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix} \end{array}$$

VOORBEELD 4. (TWO-FINGER MORRA) Reeds door de Romeinen werd dit spel gespeeld (alleen niet met guldens). Partijtjes verlopen als volgt: gelijktijdig steken de spelers I en II 1 of 2 vingers in de lucht en raden hoeveel vingers de tegenstander opsteekt. Als één der spelers goed raadt wint hij evenveel guldens als er door beide spelers vingers in de lucht zijn gestoken; als beiden goed of beiden fout raden volgt er geen uitbetaling. In dit spel hebben beide spelers vier strategieën ter beschikking en wel (1,1), (1,2), (2,1), (2,2) waarbij met (i,j) de strategie wordt bedoeld: "steek i vingers in de lucht en raad j".
Dit spel correspondeert met het 4 × 4-matrixspel

$$\begin{array}{cc} & \text{II} \\ & \begin{array}{cccc} (1,1) & (1,2) & (2,1) & (2,2) \end{array} \\ \text{I} \begin{array}{c} (1,1) \\ (1,2) \\ (2,1) \\ (2,2) \end{array} & \begin{bmatrix} 0 & 2 & -3 & 0 \\ -2 & 0 & 0 & 3 \\ 3 & 0 & 0 & -4 \\ 0 & -3 & 4 & 0 \end{bmatrix} \end{array}$$

3. HET NORMALISEREN VAN SPELEN

In een tweepersoonsspel in normale vorm doen beide spelers één zet en wel gelijktijdig. Gezelschapsspelen zijn meestal meerzetsspelen (ook wel spelen in uitgebreide vorm genoemd). Hierbij zetten de spelers om de beurt en een speler komt vaak meermalen aan zet terwijl soms ook het toeval een rol speelt (verdelen kaarten). John von Neumann merkte op dat in principe de meeste gezelschapsspelen te reduceren zijn tot spelen in normale vorm en zelfs tot matrixspelen. Het idee hierbij is om (grofweg) onder een strategie van een speler te verstaan: een volledig uitgewerkt speelplan

vooraf dat de speler (of een vervanger) precies vertelt wat te doen in elke situatie van elke mogelijke partij waarin de bewuste speler een zet moet doen. Als beide spelers elk zo'n speelplan aan een scheidsrechter opsturen, dan kan deze uitmaken tot welke uitbetalingen de gekozen strategieën leiden. Laten we één en ander aan enkele voorbeelden demonstreren (en een formele behandeling van het "normalisatieprocédé" achterwege laten).

VOORBEELD 5. (BAMZAAIEN, VUISTEN, KNOBBELEN) Laat m en n natuurlijke getallen zijn.
Met $B_{m,n}$ zullen we het volgende eindige tweepersoonsnulsomspel in uitgebreide vorm bedoelen. De spelers I en II hebben resp. m en n lucifers ter beschikking. Een partijtje $B_{m,n}$ verloopt als volgt: speler I neemt onzichtbaar voor II een zeker aantal (eventueel 0) van zijn lucifers in de rechterhand. Vervolgens neemt speler II onzichtbaar voor de tegenstander een aantal van zijn lucifers in zijn rechterhand en noemt daarna hoorbaar voor I één der getallen uit de verzameling $\{0,1,\ldots,m+n\}$. Vervolgens noemt I ook zo'n getal maar niet hetzelfde getal als II. Als één der spelers een getal genoemd heeft dat gelijk is aan het totaal aantal lucifers in beide rechterhanden dan krijgt deze één eenheid uitbetaald van de tegenstander. Raden geen van beide spelers het juiste aantal lucifers in de beide rechterhanden, dan volgt er geen uitbetalingen.

We gaan nu $B_{m,n}$ reduceren tot een spel in normale vorm: (Zuivere) strategieën van speler II kunnen we aangeven met (i.j) waarmee we bedoelen: "neem i lucifers in de rechterhand en noem vervolgens het getal j". Hierbij is $0 \leqslant i \leqslant n$, $0 \leqslant j \leqslant m+n$. Met $(k;\ \ell_0,\ell_1,\ldots,\ell_s,\ldots,\ell_{m+n})$ bedoelen we de volgende (zuivere) strategie voor speler I: "neem k lucifers in de hand en noem het getal ℓ_s als speler II in de partij het getal s genoemd heeft".
Hierbij is $0 \leqslant k \leqslant m$; verder veronderstellen we (zonder bezwaar) dat $k \leqslant \ell_s \leqslant k+n$ voor elke $s \in \{0,1,\ldots,m+n\}$.
Het spel $\langle X_{m,n},Y_{m,n},K_{m,n}\rangle$ waarbij

$$X_{m,n} := \{(k;\ell_0,\ell_1,\ldots,\ell_{m+n})\ ;\ 0 \leqslant k \leqslant m,$$
$$\forall_{s\in\{0,\ldots,m+n\}}[\ell_s \in \{k,k+1,\ldots,k+n\}\setminus\{s\}]\},$$

$Y_{m,n} := \{(i,j)\ ;\ i \in \{0,1,\ldots,n\},\ j \in \{0,1,\ldots,m+n\}\}$

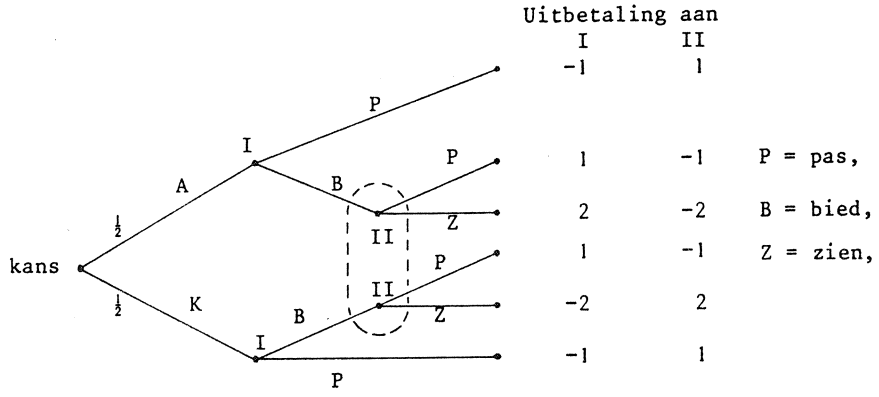
en waarbij $K_{m,n}: X_{m,n} \times Y_{m,n} \to \mathbb{R}$ is vastgelegd door

$$K_{m,n}((k;\ell_0,\ell_1,\ldots,\ell_{m+n}),(i,j)) = \begin{cases} -1 \text{ als } k+i = j \\ 1 \text{ als } k+i = \ell_j \\ 0 \text{ als } k+i \notin \{j,\ell_j\} \end{cases}$$

zullen we de (ge)normal(iseerd)e vorm van $B_{m,n}$ noemen en aangeven met $N_{m,n}$. $N_{1,1}$ is op te vatten als een 4×6-matrixspel met uitbetalingsmatrix

$$\begin{array}{c} \\ (0;1,0,0) \\ (0;1,0,1) \\ (1;1,2,1) \\ (1;2,2,1) \end{array} \begin{array}{c} \begin{array}{cccccc} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \end{array} \\ \begin{bmatrix} -1 & 1 & 1 & 1 & -1 & 0 \\ -1 & 1 & 0 & 1 & -1 & 1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 1 & 1 & -1 \end{bmatrix} \end{array}$$

<u>VOORBEELD 6</u>. (EEN VEREENVOUDIGD POKERMODEL) We bekijken een spel waarin een kanselement een rol speelt. Aan het begin van een partij krijgt (trekt) speler I één van de kaarten uit een stok {K,A} bestaande uit een koning en een aas en wel met kans ½ een K en met kans ½ een A. Speler I bekijkt dan (onzichtbaar voor speler II) de getrokken kaart en zegt vervolgens: pas of bied (naar eigen keuze). Als speler I past, moet hij *f* 1,-- betalen aan speler II. Als speler I biedt komt speler II aan zet. Hij kan dan passen of zien. Past speler II dan moet hij *f* 1,-- betalen aan speler I. Ziet speler II dan betaalt resp. ontvangt hij *f* 2,-- van speler I al naar gelang I een aas resp. een koning getrokken had. We kunnen dit spel als volgt schematisch weergeven.



[In dit tweepersoonsspel is speler II, wanneer hij aan zet (bod) komt niet volledig geïnformeerd over het verloop van de partij tot dan toe. Hij weet wel wat speler I gedaan heeft maar niet wat het toeval (ook wel de kansspeler genoemd) deed aan het begin van de partij. (In bovenstaande figuur is dit met stippeltjes aangegeven).] Bij dit spel zijn er zes mogelijke partijen.

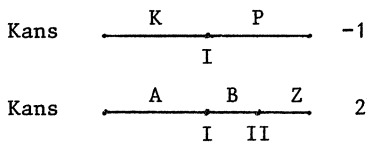
We gaan dit spel nu in normale vorm brengen. De 4 strategieën van speler I geven we aan met

$$x_1 = \binom{A\ K}{P\ P},\ x_2 = \binom{A\ K}{P\ B},\ x_3 = \binom{A\ K}{B\ P},\ x_4 = \binom{A\ K}{B\ B}$$

waarbij bijv. $\binom{A\ K}{B\ P}$ de strategie is: "bied ingeval een aas getrokken is en pas als een koning is getrokken" enz..

Speler II heeft 2 strategieën welke we aangeven met P (pas) en Z (zien).

Veronderstel dat speler I vóór een match besluit tot strategie $\binom{A\ K}{B\ P}$ en speler II tot strategie Z. Dan kan dit, afhankelijk van het kansmechanisme (uitdelen kaart), resulteren in één van de volgende twee partijen en wel beide met kans ½:



Na de eerste partij volgt een uitbetaling -1, na de tweede een uitbetaling $+2$ aan I door II. De verwachte uitbetaling van II aan I bij keuze van bovengenoemde strategieën is dan $\frac{1}{2}(-1) + \frac{1}{2}(2) = \frac{1}{2}$. Op analoge manier kunnen de verwachte uitbetalingen aan speler I door speler II in de 7 andere gevallen berekend worden. Het resultaat van de rekenpartij kan in een 4×2 matrix gezet worden:

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array} \begin{array}{c} \begin{array}{cc} P & Z \end{array} \\ \begin{bmatrix} -1 & -1 \\ 0 & -1\frac{1}{2} \\ 0 & \frac{1}{2} \\ 1 & 0 \end{bmatrix} \end{array}$$

$[K_1(x_2,Z) = -1\frac{1}{2},\ K_2(x_2,Z) = -(-1\frac{1}{2})$ enz.$]$

4. WAARDE EN OPTIMALE STRATEGIEËN

<u>DEFINITIE 4</u>. Een tweepersoonsnulsomspel $\langle X,Y,K\rangle$ zullen we *strikt bepaald* noemen als er een getal v bestaat en strategieën $\hat{x} \in X$ en $\hat{y} \in Y$ zó dat

(1) $K(\hat{x},y) \geqslant v$ voor elke $y \in Y$,

(2) $K(x,\hat{y}) \leqslant v$ voor elke $x \in X$.

Ingeval van strikte bepaaldheid noemen we v de *waarde van het spel* (voor speler I) en $\hat{x}$ (resp. $\hat{y}$) een *optimale strategie van speler* I (resp. speler II).

In een spel met waarde v kan speler I zich d.m.v. zijn optimale strategie $\hat{x}$ een uitbetaling van tenminste v garanderen ongeacht wat speler II doet en speler II kan m.b.v. $\hat{y}$ ervoor zorgen dat hij in een willekeurige partij ten hoogste v hoeft af te dragen aan speler I.

VOORBEELD 7.

Het matrixspel $\begin{bmatrix} 2 & 0 & 0 \\ 2 & 3 & 1 \\ 0 & 5 & 0 \end{bmatrix}$ is strikt bepaald. De waarde is gelijk aan 1, rij 2 is een optimale strategie van speler I en kolom 3 een optimale strategie van speler II.

Men kan gemakkelijk inzien dat de matrixspelen in de voorbeelden 3, 4, 5 en 6 niet strikt bepaald zijn. Zonder bewijs vermelden we dat matrixspelen welke afkomstig zijn van gezelschapsspelen (door normaliseren) waarbij elke speler wanneer hij aan zet is steeds volledig geïnformeerd is over het verloop van de partij tot dan toe, strikt bepaald zijn.
[Voor het schaken werd dit aangetoond door ZERMELO in 1913; de generalisatoe door J.VON NEUMANN en H. KUHN.]

5. GEMENGDE UITBREIDINGEN VAN MATRIXSPELEN

In ons bamzaai- en pokervoorbeeld hebben we geen strikte bepaaldheid.
Nu kan men bij elk matrixspel een nieuw spel maken door het invoeren van z.g. gemengde strategieën en het belangrijkste resultaat van J. von Neumann in bovengenoemd artikel is het bewijs dat we dan een strikt bepaald spel krijgen.

DEFINITIE 4. Zij $A = [a_{ij}]_{i=1,\ j=1}^{m\ \ \ n}$ een $m \times n$-matrix van reële getallen.
Zij

$$S^m := \{(p_1,p_2,\ldots,p_m) \in \mathbb{R}^m;\ \sum_{i=1}^{m} p_i = 1,\ p_i \geqslant 0 \text{ voor elke } i \in \{1,\ldots,m\}\},$$

$$S^n := \{(q_1,q_2,\ldots,q_n) \in \mathbb{R}^n;\ \sum_{j=1}^{n} q_j = 1,\ q_j \geqslant 0 \text{ voor elke } j \in \{1,\ldots,n\}\},$$

$$E_A(p,q) := \sum_{i=1}^{m}\sum_{j=1}^{n} p_i a_{ij} q_j = pAq^t \text{ voor elke } p = (p_1,\ldots,p_m) \in S^m \text{ en}$$

$$\text{elke } q = (q_1,q_2,\ldots,q_n) \in S^n.$$

Dan heet het tweepersoonsnulsomspel $\langle S^m, S^n, E_A\rangle$ de *gemengde uitbreiding van* het *matrixspel* A. We geven dit spel aan met G(A). De elementen van S^m(resp. S^n) heten *gemengde strategieën van speler* I (resp. speler II).

Deze definitie behoeft enige toelichting.

(a) Bij een gemengde strategie $(p_1,p_2,\ldots,p_m) \in S^m$ voor speler I bij een $m \times n$-matrixspel kunnen we aan het volgende denken: (voor) speler I kiest (een kansmechanisme) in een partij de zuivere strategie 1 met kans p_1, de zuivere strategie 2 met kans $p_2,\ldots$, de zuivere strategie m met kans p_m; m.a.w. de zuivere strategieën worden "gemengd" met kansen $p_1,p_2,\ldots,p_m$. In het steen-papier-schaar spel kan speler I bijv. de gemengde strategie $(\frac{1}{2},\frac{1}{4},\frac{1}{4})$ kiezen. [Deze kan bijv. als volgt gerealiseerd worden: op het moment dat speler I een zuivere strategie moet noemen kijkt hij op zijn (niet stilstaand) horloge (onzichtbaar voor speler II) en noemt steen als de secondewijzer tussen 12 en 6, papier als de secondewijzer tussen 6 en 9 en schaar als de secondewijzer tussen 9 en 12 staat.] Bij deze gemengde strategie is de verwachte uitbetaling aan speler I ingeval speler II zuivere strategie 1 (resp. 2,3) kiest gelijk aan $\frac{1}{2}.0+\frac{1}{4}.1+\frac{1}{4}(-1)= 0$ (resp. $\frac{1}{2}(-1)+\frac{1}{2}.0+\frac{1}{4}.1 = -\frac{1}{4}$, $\frac{1}{2}.1+\frac{1}{4}(-1)+\frac{1}{4}.0 = \frac{1}{4}$). Merk op dat

$$(\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{1}{3}) \begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix} \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} = 0 \text{ voor elke } q = (q_1,q_2,q_3) \in S^3$$

$$\text{en}(p_1,p_2,p_3) \begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix} \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \\ \frac{1}{3} \end{pmatrix} = 0 \text{ voor elke } p \in S^3 \text{ zodat de waarde}$$

van de gemengde uitbreiding van het steen-papier-schaar spel 0 is en de gemengde strategie $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$ zowel een optimale gemengde strategie voor speler I als voor speler II is.

Het steen-papier-schaar spel is een voorbeeld van een matrixspel dat zelf geen waarde heeft, maar de gemengde uitbreiding wel.

(b) De term "uitbreiding" slaat op het feit dat we een zuivere strategie (rij) i van I kunnen identificeren met de gemengde strategie $e_i \in S^m$ en een zuivere strategie (kolom) j van speler II in het matrixspel met de strategie $e_j \in S^n$ in G(A) temeer omdat $E_A(e_i,e_j) = a_{ij}$ voor elke $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}$. [Hierbij is e_i de vector met i-de

coördinaat gelijk aan 1 en alle andere coördinaten gelijk aan 0.]

(c) Als in een partijtje de spelers I en II (onafhankelijk van elkaar) de gemengde strategieën $p = (p_1, p_2, \ldots, p_m)$ en $q = (q_1, q_2, \ldots, q_n)$ gebruiken, dan is met kans $p_i q_j$ de cel (i,j) van de matrix, corresponderend met de uitbetaling a_{ij}, de uitkomst van de partij. $E_A(p,q)$ is dus te interpreteren als de verwachte uitbetaling aan speler I bij keuze van de strategieën p en q.

HOOFDSTELLING VAN DE THEORIE VAN MATRIXSPELEN (VON NEUMANN)
De gemengde uitbreiding G(A) *van een matrixspel* A *is strikt bepaald.*

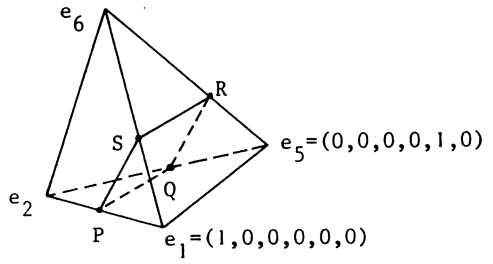
We zullen deze stelling hier niet bewijzen (zie bijv. [7].) Wel zullen we waarde en optimale strategieën proberen op te sporen van gemengde uitbreidingen van enkele reeds geïntroduceerde matrixspelen.

VOORBEELD 8. Laten we de gemengde uitbreiding bekijken van de in voorbeeld 4 geïntroduceerde 4×4-matrix A. Symmetrieoverwegingen leiden tot de conclusie dat de waarde van G(A) gelijk is aan 0 en dat speler I en II dezelfde gemengde optimale strategieën bezitten. $p \in S^4$ is een optimale strategie als $pA \geqslant (0,0,0,0)$ ofwel $p \in \mathbb{R}^4$ is optimaal precies dan als

$$(*) \quad \begin{cases} -2p_2 + 3p_3 \geqslant 0,\ 2p_1 - 3p_4 \geqslant 0,\ -3p_1 + 4p_4 \geqslant 0,\ 3p_2 - 4p_3 \geqslant 0 \\ p_1 \geqslant 0,\ p_2 \geqslant 0,\ p_3 \geqslant 0,\ p_4 \geqslant 0,\ p_1 + p_2 + p_3 + p_4 = 1. \end{cases}$$

Uit (*) volgt: $p_1 = p_4 = 0$, $\frac{2}{5} \leqslant p_3 \leqslant \frac{3}{7}$, $p_2 = 1 - p_3$, zodat de optimale gemengde strategieën van speler I precies de punten zijn liggend op het lijnstuk in $\mathbb{R}^4$ dat eindpunten $(0,\frac{3}{5},\frac{2}{5},0)$ en $(0,\frac{4}{7},\frac{3}{7},0)$ heeft.

VOORBEELD 9. Door enig rekenwerk kunnen we zien dat de gemengde uitbreiding van het 4×6-matrixspel uit voorbeeld 5 waarde nul heeft en dat $(0,\frac{1}{2},\frac{1}{2},0)$ de enige optimale gemengde strategie van speler I is terwijl de optimale strategieënruimte van speler II het hieronder aangegeven vierkant PQRS in $\mathbb{R}^6$ is.



VOORBEELD 10. De gemengde uitbreiding van de 4 × 2-matrix uit voorbeeld 6 heeft waarde $\frac{1}{3}$ en $(0,0,\frac{2}{3},\frac{1}{3})$ is de enige optimale strategie van speler I (waarbij met kans $\frac{2}{3}$ de strategie x_3 en met kans $\frac{1}{3}$ de "blufstrategie" x_4 wordt gekozen) terwijl $(\frac{1}{3},\frac{2}{3})$ de enige optimale strategie voor speler II is.

Tot slot merken we op dat het opsporen van waarde en optimale strategieën van de gemengde uitbreiding van een matrixspel equivalent is met het oplossen van een lineair programmeringsprobleem (en zijn duale) en hiervoor is een stadaardmethode beschikbaar (de z.g. simplexmethode).

OPGAVEN

1. Verwijder vóór het in voorbeeld 2 beschreven duel de geluiddempers van de pistolen. Veronderstel verder dat $p(t) = t$ voor elke $t \in [0,T]$. Herleid deze nieuwe situatie tot een tweepersoonsspel in normale vorm.

2. Bekijk het tweepersoonsspel (in uitgebreide vorm) waarbij een partij als volgt verloopt: speler II verbergt zich in één der n kamers van een hotel welke genummerd zijn van 1 t.e.m. n. Vervolgens moet speler I net zo lang nummers raden totdat het kamernummer waarin speler II verborgen zit genoemd is. Elke keer raden kost speler I *f* 1,--, te betalen aan speler II. Normaliseer dit spel. Ga na dat ingeval n=3 dit *verberg-en-raad-spel* correspondeert met een 6 × 3-matrixspel dat niet strikt bepaald is.

3. Gan na, dat het in voorbeeld 5 geïntroduceerde spel $B_{2,1}$ correspondeert met een 12 × 8-matrixspel.

4. Bepaal de waarde en optimale strategieën voor de gemengde uitbreiding van het matrixspel

$$\begin{bmatrix} -1 & 1 & 2 \\ 1 & -1 & 2 \\ -2 & -2 & -2 \end{bmatrix}$$

[Antwoord: $0,(\frac{1}{2},\frac{1}{2},0),(\frac{1}{2},\frac{1}{2},0)$.]

5. Zij <X,Y,K> een strikt bepaald tweepersoonsnulsomspel. Bewijs dat dan

$$\min_{y\in Y} \sup_{x\in X} K(x,y) = \max_{x\in X} \inf_{y\in Y} K(x,y).$$

LITERATUUR

1. *Williams, J.D.*, Speltheorie (1966). Uitgeverij het Spectrum N.V. Utrecht/Antwerpen (MARKA-reeks).

2. *Davis, M.D.*, Inleiding tot de speltheorie (1970). Uitgeverij het Spectrum. (AULA-pocket 495).

3. *McKinsey, J.C.C.*, Introduction to the theory of games (1952). McGraw-Hill Book Comp. Inc., New York- Toronto- London.

4. *Owen, G.*, Game Theory (1968). W.B., Saunders Comp., Philadelphia.

5. *Karlin, S.*, Matrix games, programming and mathematical economics (1959), Addison-Wesley Publ. Comp., Inc. Reading, Mass.

6. *Parthasarathy, T. & Raghavan, T.E.S.*, Some topics in two-person games (1971), American Elsevier Publ. Comp., Inc., New York.

7. *Tijs, S.H.*, Stelsels lineaire ongelijkheden, Markov ketens en matrixspelen. CWI Syllabus No.1, vacantiecursus 1984 HEWET-PLUS WISKUNDE, (1984), Mathematisch Centrum, Amsterdam.

DISCRETE WISKUNDE IN DE SHANNON THEORIE

J.P.M. Schalkwijk

De Shannon theorie [1] heeft als onderwerp de verwerking en de transmissie van informatie. De twee belangrijkste theorema's uit de Shannon theorie betreffen respectievelijk, 1) de meest efficiënte (kortste) representatie van een hoeveelheid informatie, en 2) de betrouwbare (foutloze) transmissie van informatie over een onbetrouwbaar transmissie kanaal. Deze twee basis aspecten van de Shannon theorie zullen elk aan de hand van een voorbeeld worden toegelicht.

1. DE KORTSTE REPRESENTATIE

Beschouw de in Fig. 1 afgebeelde symmetrische roulette. Een serie uitkomsten AABABA... kan worden gecodeerd volgens A→0, B→1 als 001010... . In het geval van een symmetrische roulette geeft dit inderdaad de meest efficiënte (kortste) beschrijving van het resultaat AABABA..., m.a.w. de symmetrische roulette beschouwd als informatiebron produceert 1 bit per uitkomst.

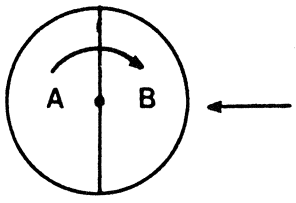


Fig.1. Symmetrische roulette als informatiebron.

Voor een asymmetrische roulette als in Fig. 2 levert een codering volgens A→0, B→1 echter geen efficiënte (korte) beschrijving van het resultaat AABABA... op.

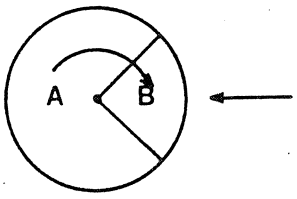


Fig.2. Asymmetrische roulette als informatiebron.

Dit kan als volgt worden ingezien. Als de sector B in Fig. 2 een fractie p van de omtrek van de roulette beslaat, is de kans P(B), dat de informatiebron een B produceert, gelijk aan P(B) = p. Volgens de wet van de grote getallen zal de frequentie van de B's in een rij van N uitkomsten AABABA... met toenemende N tot p naderen. Maar er zijn slechts $\binom{N}{pN}$ rijen ter lengte N met een frequentie van B's gelijk aan p. Om zulk een uitkomst AABABA... ter lengte N te specifieren zijn slechts $\lceil \log_2 \binom{N}{pN} \rceil$ bits nodig, waarbij $\lceil x \rceil$ het kleinste gehele getal groter dan of gelijk aan x voorstelt. M.a.w. de kortste beschrijving van een serie uitkomsten van de roulette vraagt

(1) $$\frac{1}{N} \lceil \log_2 \binom{N}{pN} \rceil \text{ bits per uitkomst.}$$

Asymptotisch voor grote N is (1) gelijk aan

(2) $$H(p) = -p \log_2 p - (1-p)\log_2(1-p); \; 0 \leqq p \leqq 1.$$

De grootheid H(p) wordt de *entropie* van de roulette als informatiebron genoemd. Fig. 3 is een afbeelding van H(p) als functie van p. Uit Fig. 3 blijkt dat voor de symmetrische roulette van Fig.1, m.a.w. $p = \frac{1}{2}$, de directe codering volgens A→0, B→1 efficiënt is. Dit levert precies $H(\frac{1}{2})$ = 1 bit per uitkomst op. Beschouw nu het asymmetrische geval van Fig. 2. Laat de sector B gelijk zijn aan 120^0, m.a.w. $p = \frac{1}{3}$. Een rij van uitkomsten AABABA ... ter lengte N moet dan asymptotisch voor grote N te coderen zijn

in $H(\frac{1}{3})$ = 0,92 bits per uitkomst. Hoe kan een dergelijke codering nu worden gerealiseerd?

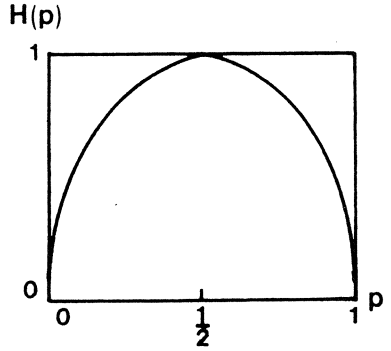


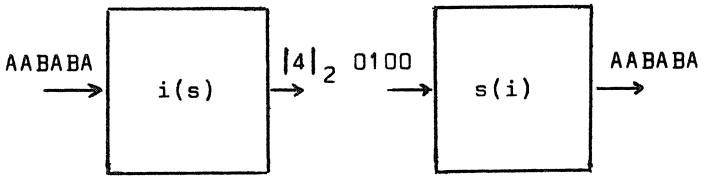
Fig.3. De binaire entropie functie.

Veronderstel eerst dat het aantal B's in een rij uitkomsten AABABA... ter lengte N bekend is. M.a.w. beschouw de verzameling S van alle mogelijke rijtjes van A's en B's ter lengte N, waarbij het aantal B's gelijk is aan fN. De elementen $s \in S$ kunnen nu alphabetisch worden gerangschikt. Tabel 1 is een alphabetische lijst van alle mogelijke rijtjes ter lengte N=6 met de frequentie van de B's gelijk aan $f = \frac{1}{3}$. Codering volgens A→0, B→1 vraagt 6 binaire digits per woord $s \in S$.

$s \in S$	i(s)
A A A A B B	0
A A A B A B	1
A A A B B A	2
A A B A A B	3
A A B A B A	4
A A B B A A	5
A B A A A B	6
A B A A B A	7
A B A B A A	8
A B B A A A	9
B A A A A B	10
B A A A B A	11
B A A B A A	12
B A B A A A	13
B B A A A A	14

Tabel 1. Woordenboek van woorden $s \in S$, waarbij S bestaat uit alle rijen van 4 A's en 2 B's.

De *lexicographische index* i(s), die van i(s) = 0 tot i(s) = 14 loopt, vraagt slechts 4 binaire digits in radix-2 notatie en specificeert s ∈ S eenduidig! M.a.w., als 1) er een eenvoudig algorithme bestaat om de lexicographische index i(s) voor gegeven s te bepalen en 2) er een eenvoudig inverse algorithme bestaat om voor gegeven i(s) het woord s ∈ S te reconstrueren, dan kunnen de woorden s ∈ S efficiënt worden gecodeerd d.m.v. hun lexicographische index i(s) in radix-2 notatie, zie Fig.4.



a. compressie algorithme b. inverse algorithme

Fig.4. Het codeeralgorithme en zijn inverse.

Het *Pascal driehoek algorithme* [2,3,4,5] werkt als volgt. Voor de verzameling S van rijtjes van 4 A's en 2 B's snij een rechthoek uit Pascal's driehoek die 4 stappen in de A-richting en 2 stappen in de B-richting toelaat, zie Fig.5. Begin in de oorsprong en neem voor elke A een stap in de A-richting en voor elke B een stap in de B-richting. Het pad dat met

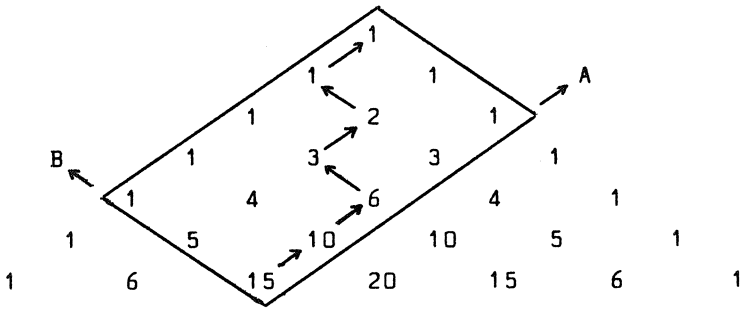


Fig.5. Pascal's driehoek met coderingsrechthoek.

s = AABABA correspondeert is in Fig.5 aangegeven. Voor elke stap in de B-richting accumuleer het getal rechts van het startpunt van deze stap. M.a.w. i(AABABA) = 3 + 1 = 4, zie ook Tabel 1.

Bij het inverse algorithme wordt uitgegaan van de lexicographische index i(s) = 4. Begin wederom in de oorsprong en vergelijk i(s) = 4 en het nummer 10 één stap in de A-richting van 15. Omdat 4 < 10 stappen we naar 10 en noteren een A. Wederom is 4 < 6. Stap naar 6 en noteer weer een A met als resultaat AA. Nu is 4 $\geqslant$ 3, dus stap in de B-richting, noteer een B met als resultaat AAB, en verminder 4 - 3 = 1. Wederom is 1 < 2. Stap naar 2 en noteer weer een A met als resultaat AABA. Nu is 1 $\geqslant$ 1, dus stap in de B-richting, noteer een B met als resultaat AABAB, en verminder 1 - 1 = 0. Wederom is 0 < 1. Stap naar 1 en noteer een A met als uiteindelijk resultaat het gewenste woord AABABA. Het bewijs [2,4,5] van bovenstaande algorithmen wordt aan de lezer overgelaten.

We keren nu terug naar ons oorspronkelijke probleem, nl. het coderen van van een rij uitkomsten AABABA... ter lengte N, gegenereerd m.b.v. een roulette als informatiebron. Aangezien in dit geval fN niet bekend is, zal een prefix van het codewoord het aantal B's moeten aangeven. Aangezien $0 \leqslant fN \leqslant N$ is een prefix van $\lceil \log_2(N+1) \rceil$ binaire digits voldoende. De rest van het codewoord kan nu bestaan uit de lexicographische index i(s) in radix-2 notatie. Omdat $0 \leqslant i(s) < \binom{N}{fn}$ is de totale lengte van het codewoord gelijk aan

$$\lceil \log_2(N+1) \rceil + \lceil \log_2 \binom{N}{fN} \rceil. \tag{3}$$

Het aantal binaire digits per letter krijgen we door (3) door N te delen. Maar $\lceil \log_2(N+1) \rceil / N \to 0$ met toenemende N en volgens (2) is $\lceil \log_2 \binom{N}{fN} \rceil / N$ asymptotisch gelijk aan H(f). Zoals reeds eerder werd opgemerkt zal de frequentie f van de B's met toenemende N tot p naderen en dus realiseert de beschreven coderingstechniek het door Shannon aangegeven minimum aantal van H(p) binaire digits per letter van de informatiebron.

2. FOUTLOZE TRANSMISSIE

In dit tweede gedeelte van de voordracht behandelen we een coderingstechniek voor het foutloos overbrengen van informatie over een onbetrouwbaar transmissiekanaal. Een typisch voorbeeld van zo'n imperfect kanaal is het binair symmetrische kanaal van Fig.6. De kans dat een verzonden 0 als 1 wordt ontvangen, of omgekeerd een verzonden 1 als een 0, is $0 < p < \frac{1}{2}$. Met het kanaal van Fig.6 kan een constante, de *kanaalcapaciteit*

$$C = 1 - H(p) \tag{4}$$

worden geassocieerd, waarbij H(p) in (2) werd gedefinieerd.

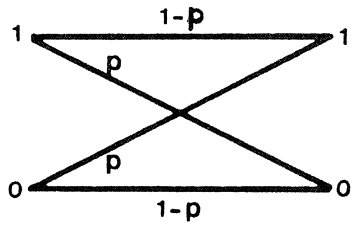


Fig.6. Het binair symmetrische kanaal.

Deze heeft de volgende betekenis. Een *kanaalcode* met *bloklengte* N en *efficiëntie* R is een verzameling van

$$M = 2^{RN}; \quad 0 \leqslant R \leqslant 1 \tag{5}$$

binaire rijtjes ter lengte N. De N binaire digits van een codewoord (rijtje) uit zo'n code worden nu successievelijk aan het kanaal van Fig.6 aangeboden. De ontvanger observeert de N bijbehorende outputs van het kanaal en heeft tot taak te raden welk van de M mogelijke codewoorden (rijtjes) van de code is verzonden. Shannon heeft nu bewezen dar er een klasse van codes bestaat met efficiëntie $R < C$ en zodanig dat de kans op een foute beslissing van de optimale ontvanger met toenemende N tot nul nadert. Voor codes met efficientie $R > C$ kan de foutenkans niet willekeurig klein

zijn. Fig.7 geeft C volgens (4) als een functie van de overgangswaarschijnlijkheid p van het binair symmetrische kanaal.

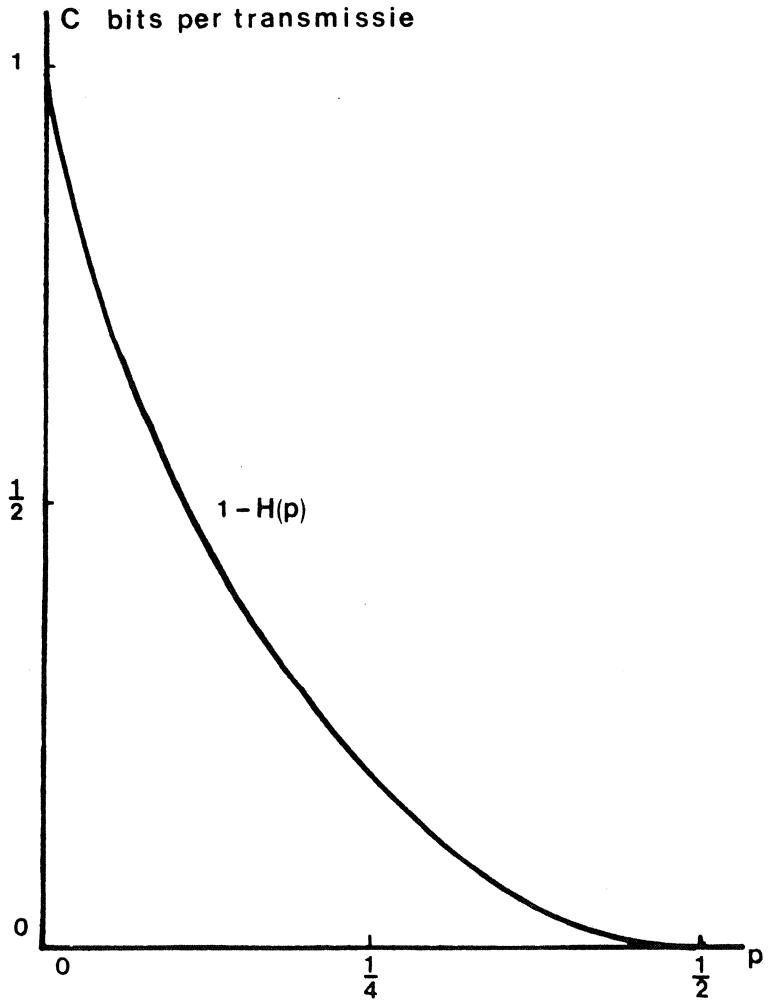


Fig.7. De kanaalcapaciteit als functie van de overgangswaarschijnlijkheid p.

Uit fig.7. blijkt dat een perfect kanaal, d.w.z. p=0, een foutloze informatie-overdracht van 1 bit per transmissie toelaat.

$p=\frac{1}{2}$ is geen foutloze overdracht van informatie meer mogelijk. Hoe kunnen we nu een foutloze informatie-overdracht over een imperfect kanaal, zoals dat van Fig. 6 met $0 < p < \frac{1}{2}$, realiseren?

Als in menselijke communicatie is het eenvoudiger om informatie over te dragen in een dialoog dan in een monoloog. We veronderstellen dus dat er behalve het imperfecte kanaal van Fig. 6 met $0 < p < \frac{1}{2}$ tussen zender en ontvanger nog een perfect terugmeldingskanaal met p=0 tussen ontvanger en zender is. Shannon toont aan dat de aanwezigheid van dit terugmeldingskanaal de informatiecapaciteit C in de richting van zender naar ontvanger niet vergroot. Zoals we direct zullen zien, maakt het terugmeldingskanaal echter een zeer eenvoudige coderingsstrategie [6,7,8] mogelijk. Door de ontvangen binaire digits namelijk over het terugmeldingskanaal naar de zender terug te voeren weet deze direct of een bepaalde verzonden digit goed dan wel fout is overgekomen. Er kan nu direct worden gecorrigeerd. In de volgende alinea beschrijven wij onze coderingsstrategie.

Door in een binaire informatiestroom 01110... na iedere k-2, $k \geqslant 3$, digits een extra digit in te voegen, dat het complement is van het voorafgaande informatie digit, transformeren we de oorspronkelijke informatiestroom in een gemodificeerde binaire stroom, waarin de combinaties 01^k en 10^k niet voorkomen. De oorspronkelijke informatiestroom 01110... wordt.
voor het geval k=3, bijvoorbeeld gemodificeerd in $0\underline{1}1\underline{0}1\underline{0}1\underline{0}0\underline{1}$..., waarbij de ingevoegde digits zijn onderstreept. De combinatie 01^3 = 0111 uit de oorspronkelijke informatiestroom, 01110..., komt in de gemodificeerde informatiestroom niet meer voor.
De gemodificeerde informatiestroom wordt nu aan de ingang van het knaal van Fig. 6 aangeboden, waarbij ieder digit dat fout overkomt k maal wordt herhaald, alvorens de rest van de gemodificeerde informatiestroom met eventuele herhalingen wordt verzonden. De foutencorrectie aan de ontvanger vindt plaats door de ontvangen digits herhaaldelijk van rechts naar links na te lopen, waarbij 01^k door een 1 en 10^k door een 0 wordt vervangen. De gemodificeerde informatiestroom $0\underline{1}1\underline{0}1\underline{0}1\underline{0}0\underline{1}$..., voor k=3 wordt bijvoorbeeld ver-

zonden als de codestroom $0\hat{1}(1\hat{1}(111)1)\underline{1}0\underline{1}0\underline{1}0\underline{0}1\underline{1}$..., waarbij digits die fout zijn overgekomen van een dakje zijn voorzien en herhalingen tussen haakjes zijn geplaatst . We ontvangen dus 0010111110101001.. .
Correctie leidt tot 0010111110101001 → 0011110101001 → 0110101001.
Tenslotte worden de ingevoegde digits in de even posities geelimineerd met als resultaat $0\underline{1}1\underline{0}1\underline{0}1\underline{0}0\underline{1}$ → 01110..., d.w.z. de oorspronkelijke informatiestroom wordt correct gedecodeerd! In de laatste alinea vergelijken we de efficiëntie van dit coderingssysteem met de kanaalcapaciteit volgens Shannon, zie Fig.7.

In een codestroom ter lengte $N \to \infty$ zitten gemiddeld pN fouten of kpN herhalingen. M.a.w. de gemodificeerde bitstroom komt van een informatiestroom ter lengte $K = L(k-2)/(k-1) = N(1-kp)(k-2)/(k-1)$. Met deze informatiestroom ter lengte K corresponderen

$$M = 2^K = 2^{N(1-kp)\ (k-2)/(k-1)} \tag{6}$$

mogelijk berichten. Vergelijking van (5) en (6) levert een efficiëntie van

$$R = (1-kp)\ (k-2)/(k-1); \quad k \geqslant 3. \tag{7}$$

In Fig.8 hebben we efficiëntie R voor deze klasse van coderingsstrategieën geïndexeerd door $k \geqslant 3$, uitgezet tegen de overgangswaarschijnlijkheid p van het binair symmetrische kanaal van Fig.6. Een eenvoudige berekening leert dat de omhullende van het lijnenstelsel (7) de ellips

$$2p = 1 - [R(2-R)]^{\frac{1}{2}} \tag{8}$$

is. De kanaalcapaciteit volgens Shannon, Fig.7, is ter vergelijking nogmaals in Fig.8 gestippeld weergegeven. Merk op dat de efficiëntie van onze coderingsstrategiën de optimale efficiëntie volgens Shannon dicht benadert!

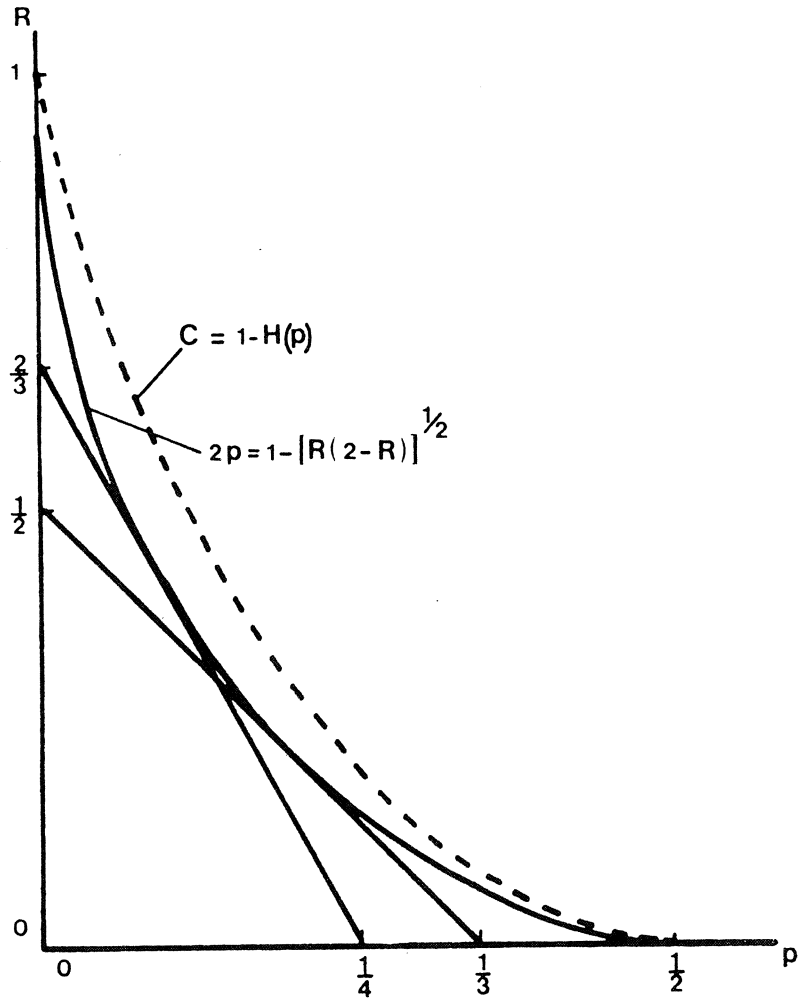


Fig. 8. De efficiëntie als functie van de overgangswaarschijnlijkheid p.

REFERENTIES.

1. *Slepian, D.*, Key papers in the development of information theory. New York: Wiley 1974.

2. *Schalkwijk, J.P.M.*, An algorithm for source coding, IEEE Trans. Inform. Theory, vol. IT-18, May 1972, pp. 395-399.

3. *Schalkwijk, J.P.M., F. Antonio & R. Petry*, An efficient algorithm for data reduction, Proceedings of the Fifth Hawaii International Conference on System Sciences, 1972.

4. *Cover, T.M.*, Enumerative source coding, IEEE Trans. Inform. Theory, vol. IT-19, January 1973, pp. 73-76.

5. *Schalkwijk, J.P.M.*, Coding by lexicographical enumeration, Tijdschrift van het Nederlands Electronica- en Radiogenootschap, deel 39, nr. 5/6, 1974.

6. *Schalkwijk, J.P.M.*, A class of simple and optimal strategies for block coding on the binary symmetric channel with noiseless feedback, IEEE Trans. Inform. Theory, vol. IT-17, May 1971, pp. 283-287.

7. *Schalkwijk, J.P.M. & K.A. Post*, On the error probability for a class of binary recursive feedback strategies, IEEE Trans. Inform. Theory, vol. It-19, July 1973, pp. 498-511.

8. *Schalkwijk, J.P.M.*, A coding scheme for duplex channels, IEEE Trans. Communications, vol. COM-22, September 1974, pp. 1369-1374.

HET VIERKLEURENPROBLEEM

J.M. Aarts

Opmerking van de redactie:

Inmiddels is het vierkleurenprobleem in 1976 opgelost door Kenneth Appel en Wolfgang Haken. Met zeer intensief gebruik van de computer lukte het hun te bewijzen dat vier kleuren inderdaad voldoende zijn om iedere kaart te kleuren. Behalve veel wetenschappelijke publikaties hebben zij hierover een zeer leesbaar artikel (The solution of the Four-Color-Map Problem) geschreven in de SCIENTIFIC AMERICAN, oct. 1977, pp. 108-121.
De hier gepresenteerde tekst blijft echter van waarde omdat de besproken technieken ook in de oplossing van Appel en Haken een essentiële rol vervullen.

1. Inleiding

Voor we het vierkleurenprobleem kunnen formuleren, moeten we eerst nauwkeurig omschrijven, wat we onder een kaart dienen te verstaan.

Laat in het platte vlak een eindig aantal jordan-krommen gegeven zijn. (Een jordankromme is het beeld van een cirkel onder een topologische - d.i. een éénéénduidige in beide richtingen continue - afbeelding.) Het complement van deze jordankrommen valt uiteen in een aantal samenhangende gebieden. Is dit een eindig aantal, dan spreken we van een kaart. Ieder stuk tezamen met zijn rand noemen we land. Landen zullen we aangeven met hoofdletters.

Een kaart in bovengenoemde zin kunnen we ons het beste voorstellen als een "gewone landkaart", waarbij o.a. de zee ook als een land wordt opgevat, ieder eiland als een apart land opgevat wordt, terwijl ook enclaves als aparte landen worden beschouwd.

Twee landen grenzen aan elkaar (zijn buren) als ze een jordanboog (d.i. een topologisch beeld van een segment) gemeenschappelijk hebben. Zo, b.v., grenzen in fig.1^a de landen A en B wel, in fig.1^b niet aan elkaar.

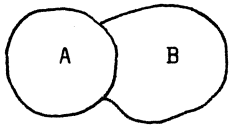


fig.1^a

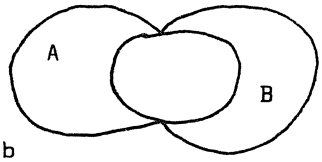


fig.1^b

De gemeenschappelijke boog heet de grens van A en B.

Een kaart kleuren met een gegeven aantal kleuren wil zeggen: ieder land een kleur geven zó, dat buren verschillende kleuren krijgen. Kleuren geven we aan met kleine letters.

We vragen ons nu af: Hoeveel kleuren zijn nodig en voldoende om iedere kaart te kleuren?

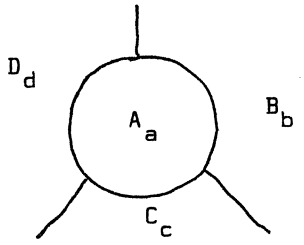


fig.2

De kaart uit fig.2 laat zien dat vier kleuren nodig zijn.
Zijn vier kleuren ook voldoende?
Dit is nu juist het vierkleurenprobleem.

Het werd in 1878 door Cayley [3] als mathematisch probleem geformuleerd. (Het schijnt rond 1850 door De Morgan als "stelling" genoemd te zijn.) Kempe "bewees" in 1879 [9] dat vier kleuren voldoende waren om iedere kaart te kleuren. Heawood (1890) [8] gaf de fout in het "bewijs" van Kempe aan en met een modificatie van dit bewijs toonde hij aan, dat vijf kleuren voldoende zijn om iedere kaart te kleuren. Sindsdien bestaat het vierkleurenprobleem.

2. Ketens

Sinds 1890 is door vele wiskundigen en niet-wiskundigen geprobeerd de vierkleurenhypothese - d.i. de hypothese, dat vier kleuren voldoende zijn om een willekeurige kaart te kleuren - te bewijzen. In deze paragraaf zullen we aan de hand van een stelling een schets geven van de belangrijkste methode, die hierbij gebruikt is. Deze methode maakt gebruik van de Stelling van Jordan: Een jordankromme J in het platte vlak verdeelt het vlak in (precies) twee samenhangende gebieden A en B. Twee punten P en Q uit verschillende gebieden zijn niet te verbinden door een jordanboog (fig.3).

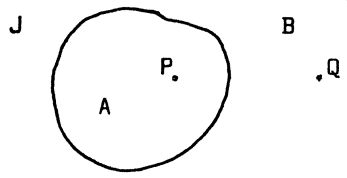


fig.3

Stelling 1: Een kaart waarin ieder land ten hoogste vier buren heeft, is kleurbaar met vier kleuren.

Bewijs: Begin de kaart te kleuren met vier kleuren. We kunnen slechts vastlopen in een situatie zoals geschetst in fig.4: hier hebben we een land E, omgeven door vier landen A,B,C en D, welke reeds gekleurd zijn met vier kleuren. We mogen aannemen dat dit resp. a,b,c en d zijn. We voeren nu het begrip keten in: Als een kaart gedeeltelijk gekleurd is, heten twee landen X en Y verbonden door een (x,y)-keten, indien er een rij landen is, opeenvolgend gekleurd met x en y, zó dat het eerste land uit de rij X is, het laatste Y, terwijl ieder land uit de rij grenst aan zijn opvolger in de rij: Beschouw nu de kaart uit fig.4.

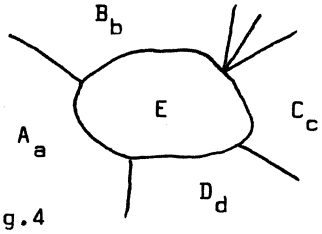


fig.4

We onderscheiden twee gevallen:

(i) Stel A en C zijn niet verbonden door een (a,c)-keten,

(ij) Stel A en C zijn wel verbonden door een (a,c)-keten.

ad (i): Beschouw alle landen welke met A verbonden zijn door een (a,c)-keten. Volgens de veronderstelling behoort C hier niet toe.

We gaan nu bij deze landen de kleuren a en c verwisselen. Hierdoor krijgen we een eveneens geschikte kleuring voor het gedeelte van de kaart dat reeds gekleurd was, waarbij i.h.b. A met c gekleurd is. We kunnen nu E met a kleuren.

ad (ij): Beschouw een (a,c)-keten welke A en C verbindt, tezamen met E. We krijgen dan een ring. Met behulp van de stelling van Jordan vinden we dat de landen B en D niet verbonden kunnen zijn door een (b,d)-keten. We kunnen nu het bewijs bij (i) reproduceren, waarbij we A door B, C door D, a door b, en c door d vervangen. I.h.b. wordt B met d gekleurd en E met b. Nu kunnen we het kleuren van de kaart voortzetten. Hiermede is de stelling bewezen. Bovenstaand bewijs is in feite een bewijs met behulp van volledige inductie naar het aantal gekleurde landen in de kaart. Het in het bewijs gebruikte begrip keten is ingevoerd door Kempe in het hiervoor vermelde artikel. Toch is dit resultaat pas te vinden in een artikel van Dirac uit 1957 [4], waarin een iets algemenere uitspraak bewezen wordt. Verfijning van het bewijs en toevoeging van een truc leidt tot een recent resultaat van Aarts en de Groot [1]:

Stelling 2: Een kaart waarin ieder land ten hoogste vijf buren heeft is kleurbaar met vier kleuren.

3. Reducibele kaarten

Terwille van een eenvoudige beschrijving van de belangrijkste vondsten bij het vierkleurenprobleem, maken we gebruik van het begrip reducibel:

Men noemt een kaart K, bestaande uit n landen, reducibel, indien men een bewijs heeft voor de volgende bewering: als iedere kaart met minder dan n landen gekleurd kan worden met vier kleuren, dan kan K gekleurd worden met vier kleuren.

Met behulp van dit begrip kunnen we gedeelten van een eventueel bewijs van de vierkleurenhypothese eenvoudig formuleren. Men heeft een bewijs m.b.v. volledige inductie voor de vierkleurenhypothese, als men aantoont, dat iedere kaart reducibel is.

Stelling 3: Een kaart welke een meervoudig samenhangend land bevat is reducibel. (Een land heet meervoudig samenhangend als het complement uit meerdere samenhangende stukken bestaat.)

Bewijs: We bewijzen deze stelling voor de kaart K welke geschetst is in fig. 5. (Een bewijs voor het algemene geval is dan gemakkelijk te geven.) A is een meervoudig samenhangend land. Het complement van A bestaat uit twee componenten C_1 en C_2. Stel K heeft n landen en stel dat iedere kaart met minder dan n landen gekleurd kan worden.

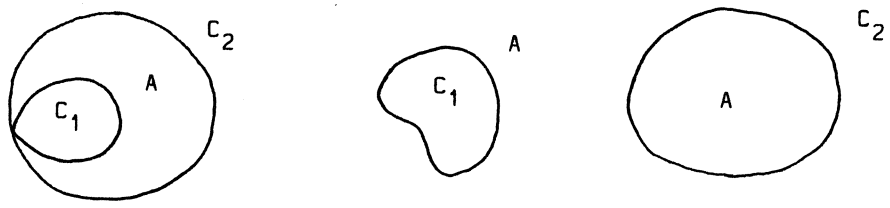


fig.5 : K fig.5^a : K_1 fig.5^b : K_2

We maken twee nieuwe kaarten K_1 resp. K_2, zoals aangegeven in fig.5^a resp. 5^b: K_1 ontstaat uit K door de grenzen van C_2 uit te vegen, K_2 ontstaat uit K door C_1 uit te vegen. De kaarten K_1 en K_2 bezitten ieder minder dan n landen en kunnen dus volgens de bovengemaakte veronderstelling gekleurd worden met vier kleuren. Door een permutatie van de kleuren is te bereiken dat zowel in K_1 als K_2 het land A gekleurd is met a. Door deze kleuring over te brengen naar K verkrijgen we de gezochte kleuring.

Geheel analoog bewijst men:

Stelling 4: Een kaart waarin twee landen tezamen een meervoudig samenhangend deel van het vlak vormen, is reducibel.

Een hoekpunt in de kaart is een punt dat tot drie of meer landen behoort. Het aantal landen waartoe een hoekpunt behoort heet de orde van dat hoekpunt.

Stelling 5: Een kaart waarin een hoekpunt van orde groter dan drie voorkomt, is reducibel.

Bewijs: (fig.6)

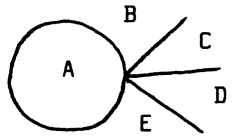


fig.6 : K

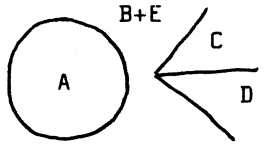


fig.6^a : K^*

Zij K een kaart met n landen, welke een hoekpunt van orde 5 bevat. (Ook hier is het bewijs eenvoudig te generaliseren.) We mogen aannemen dat iedere kaart met minder dan n landen gekleurd kan worden met vier kleuren. Indien K een meervoudig samenhangend land bevat, of indien twee landen in K tezamen een meervoudig samenhangend deel van het vlak vormen, passen we stelling 3 resp. 4 toe. Is dit niet het geval, dan weten we dat de landen B en E verschillend zijn en niet aan elkaar grenzen. We maken nu een nieuwe kaart K* door "het hoekpunt open te breken" (zie fig. 6^a). K* bevat n-1 landen en kan dus gekleurd worden. Breng de kleuren van K* over naar K. In K krijgen B en E dezelfde kleur. Dit kan echter geen kwaad, daar B en E in K niet aan elkaar grenzen.

Uit bovenstaande blijkt dat men zich bij het zoeken naar een bewijs voor de vierkleurenhypothese mag beperken tot een speciale klasse van kaarten, de reguliere kaarten: dit zijn kaarten waarin ieder hoekpunt orde drie heeft en waarin geen één- resp. tweering voorkomt. (Een eenring is een meervoudig samenhangend land, een tweering is een systeem van twee landen die samen een meervoudig stuk van de kaart vormen. Analoog definieert men driering, enz.)

Met weinig moeite kan men nu aantonen, dat een kaart welke een driering bevat reducibel is.

Birkhoff [2] bewees dat een kaart welke een vierring bevat reducibel is. Verder toonde hij aan, dat een kaart welke een vijfring bevat, reducibel is, mits voldaan is aan de voorwaarde, dat iedere component van het complement van de vijfring tenminste twee landen bevat.

In de volgende paragraaf zullen we zien, dat, indien deze laatste voorwaarde gemist kon worden, het vierkleurenprobleem opgelost zou zijn.

Een vijfring welke wel aan deze voorwaarden voldoet, zullen we niet-triviaal noemen.

4. Resultaten

Om enig overzicht te krijgen over de mogelijke kaarten, maken we gebruik van de identiteit van Euler:

Is M een reguliere kaart zonder 1- en 2-ringen en is α_o het aantal hoekpunten van M, α_1 het aantal grenzen, en α_2 het aantal landen, dan is

$$-\alpha_0 + \alpha_1 - \alpha_2 = -2. \qquad (1)$$

Stel eens dat a_i het aantal landen is met i buren, dan is

$$\alpha_o = \sum_{i\geqslant 3} \frac{ia_i}{3} \text{ (in ieder hoekpunt komen 3 landen samen)}$$

$$\alpha_1 = \sum_{i\geqslant 3} \frac{ia_i}{2} \text{ (bij iedere grens komen 2 landen samen)}$$

$$\alpha_2 = \sum_{i\geqslant 3} a_i \ .$$

Gesubstitueerd in (1) levert dit

$$\frac{1}{6} \sum_{i\geqslant 3} ia_i - \sum_{i\geqslant 3} a_i = -2 \ . \qquad (2)$$

Hieruit volgt:

$$3a_3 + 2a_4 + a_5 = 12 + \sum_{i\geqslant 6} (i-6)a_i \qquad (3)$$

Stel nu eens dat we een willekeurige kaart K hebben met n landen. We willen nu proberen te bewijzen dat K gekleurd kan worden met 4 kleuren. We doen dit met volledige inductie naar n. Een kaart bestaande uit 1, 2, 3 of 4 landen kan gekleurd worden met vier kleuren. Stel dat iedere kaart met n-1 landen gekleurd kan worden. In het geval K een hoekpunt van orde groter dan drie bevat, of een 1-, 2-, 3- of 4-ring, óf een niet-triviale 5-ring, is K reducibel volgens §3, en kan dus, door gebruik te maken van de inductieveronderstelling, gekleurd worden met vier kleuren. Is dit niet het geval, dan is K dus regulier en bevat geen 1-, 2-, 3- of 4-ring of niet-triviale

5-ring. K bevat dan i.h.b. geen land met 3 of 4 buren. Uit formule (3) volgt dan ($a_3 = 0$, $a_4 = 0$):

$$a_5 = 12 + \sum_{i \geqslant 6} (i - 6)a_i \ . \qquad (4)$$

Hieruit blijkt dat K ten minste twaalf landen van orde 5 bevat. (De orde van een land is het aantal buren van dat land.) Voor ieder land van orde 7, komt er een land van orde 5 bij, voor ieder land van orde 8, komen er twee landen van orde 5 bij enz. enz. Een land van orde 5 wordt omringd door een vijfring. Dit wil echter nog niet zeggen dat K reducibel is! Zo'n vijfring is triviaal en voldoet niet aan de voorwaarde dat iedere component van het complement tenminste twee landen bevat!

Toch kunnen we enig resultaat bereiken door aan K een royale beperking op te leggen. Laten we eens aannemen, dat K ten hoogste veertien landen bevat, dus $n \leqslant 14$.

Dus $\sum_{i \geqslant 5} a_i \leqslant 14$

of $$a_5 + \sum_{i \geqslant 6} a_i \leqslant 14 \ . \qquad (5)$$

Door (4) in (5) te substitueren, vinden we:

$$\sum_{i \geqslant 6} (i-5)a_i \leqslant 2 \ .$$

Hieraan kan alleen voldaan zijn in de volgende gevallen ($a_8 = 0$, $a_9 = 0$, enz.):

I $a_7 = 1$, $a_6 = 0$, dan is $a_5 = 13$, dus K bevat 14 landen
II $a_7 = 0$, $a_6 = 2$, dan is $a_5 = 12$, dus K bevat 14 landen
III $a_7 = 0$, $a_6 = 1$, dan is $a_5 = 12$, dus K bevat 13 landen
IV $a_7 = 0$, $a_6 = 0$, dan is $a_5 = 12$, dus K bevat 12 landen.

Door uit te tekenen vindt men dat I niet realiseerbaar is (K mag geen vierring of niet-triviale vijfring bevatten!) Evenzo blijkt III niet realiseerbaar.

II is mogelijk in één geval: K bestaat uit een land van orde 6, omringd door een 6-ring met landen van orde 5, wéér omringd door een zesring met landen van orde 5 en tenslotte afgesloten door een land van orde 6. Kleuring voor K: eerste land van orde 6 met a, eerste ring met b en c, tweede ring met a en d, tweede land van orde 6 met b.

IV "K is een dodokaeder". Kleuring zie figuur 7:

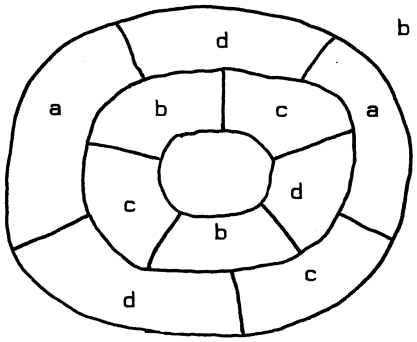


fig.7

Zo blijkt dat K in alle mogelijke gevallen kleurbaar is met vier kleuren. We hebben dus de volgende Stelling:

Een kaart met ten hoogste veertien landen is kleurbaar met vier kleuren.

Het is duidelijk, dat het aantal veertien verhoogd kan worden én door meer reducibele kaarten te vinden, én door beter gebruik te maken van de Euler identiteit.

Zo verhoogde Franklin het in 1922 tot 25 [6], Reynolds in 1927 tot 27 [10], Franklin in 1938 tot 31 [7] en tenslotte Winn in 1940 tot 35 [12]. Reeds eerder had Winn [11], gebruikmakend van het werk van o.a. Errera [5], het volgende nog iets mooiere resultaat bereikt:

Een reguliere kaart waarin ieder land, op ten hoogste één uitzondering na, orde kleiner dan of gelijk aan 6 heeft, is kleurbaar met vier kleuren.

LITERATUUR

[1] *J.M. Aarts* en *J. de Groot*, A case of colouration in the four colour problem, Nieuw Archief voor Wisk. (3), XI (1963), p.10-18.

[2] *G.D. Birkhoff*, The Reducibility of maps, Amer.J.Math. 35 (1913), p.115-128.

[3] *A. Cayley*, On the colouring of maps, Proc. London Math. Soc. 9 (1878), p.148.

[4] *G.A. Dirac*, A theorem of R.L. Brooks and a conjecture of H. Hadwiger, Proc. London Math. Soc. 3, 7 (1957), p.161-195.

[5] *A. Errera*, Une contribution au problème des quatre couleurs, Bull. Soc. Math. France 53 (1925), p.42.

[6] *Ph. Franklin*, The four color problem. Amer.J. Math. 44 (1922), p.225-236.

[7] *Ph. Franklin*, Note on the four color problem, J. Math. and Phys. 16 (1938), p.172-182.

[8] *P.J. Heawood*, Map colour theorem. Qurterly Journal of Pure and Applied Math. 24 (1890), p.332-338.

[9] *A.B. Kempe*, On the geographical problem of the four colours, Amer. J.Math. 2 (1879), p. 193-200.

[10] *C.N. Reynolds*, On the problem of colouring maps in four colours I and II. Ann. of Math. (2) 28 (1927), p.1-15, p.477-492.

[11] *C.E. Winn*, A case of coloration in the four color problem, Amer. J.Math. 59 (1937), p.515-528.

[12] *C.E. Winn*, On the minimum number of polygons in an irreducible map, Amer. J. Math. 62 (1940), p.406-416.

DE ROOSTERPUNTEN IN HET PLATTE VLAK

S.C. van Veen

§0. Inleiding.

In het volgende beknopte overzicht zullen wij ons beperken tot de roosterpunten in het platte vlak. Hier zullen de essentiële moeilijkheden reeds duidelijk naar voren komen. Uitbreiding tot meer dimensies voert zelden tot werkelijk nieuwe gezichtspunten. Wij leggen een rechthoekig coördinatenstelsel ten grondslag.
Roosterpunten zijn punten, waarvan beide coördinaten door gehele getallen worden voorgesteld.
Talrijke problemen uit de getallentheorie hebben gevoerd tot de bepaling van het aantal roosterpunten, gelegen binnen een bepaalde kromme.

§1. Elementaire beschouwingen. Roosterpunten binnen een cirkel (Gauss). Delerprobleem (Dirichlet).

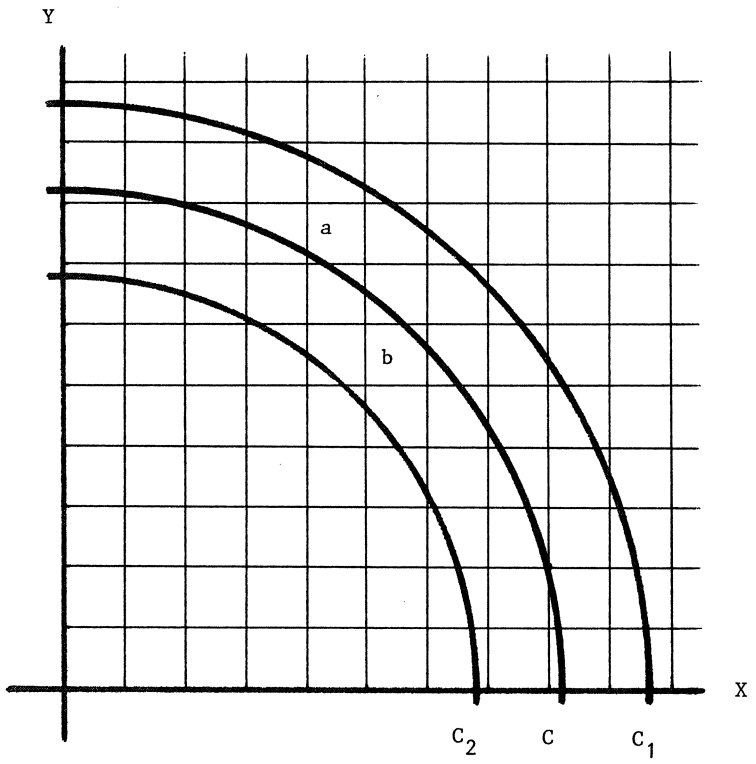
In 1834 en 1837 heeft Gauss zich uitvoerig beziggehouden met de bepaling van het aantal klassen van binaire kwadratische vormen [1].
Hij werd hierbij tot het volgende probleem gevoerd:

Gevraagd het aantal oplossingen in gehele getallen x en y van de ongelijkheid

[1] Gauss (1).

$$x^2 + y^2 \leqq n \quad (n \text{ gegeven}).$$

De meetkundige interpretatie van dit probleem voert onmiddellijk tot de bepaling van het aantal roosterpunten binnen (en op) een cirkel met straal $\sqrt{n}$. (Zie figuur 1).



Figuur 1.

Voegen wij aan ieder roosterpunt het eenheidsvierkant toe, waarvan het roosterpunt de zuid-west-hoek vormt, dan is het ogenblikkelijk duidelijk, dat het aantal roosterpunten op en binnen de cirkel C, met straal $\sqrt{n}$, bij eerste benadering zal worden aangegeven door

(1.1) $A(n) = \pi n.$

Natuurlijk zal het onregelmatige gedrag van de roosterpunten in de omgeving van de cirkelomtrek dit aantal kunnen modificeren. Sommige roosterpunten leveren vierkanten die voor het grootste gedeelte buiten C uitsteken. (Zie vierkant a). Andere roosterpunten leveren vierkanten, die maar voor een zeer klein gedeelte buiten C uitsteken.

Het is echter duidelijk, dat alle binnen of op C gelegen roosterpunten bij vierkanten behoren die ingesloten worden door de concentrische cirkel C_1 met straal $\sqrt{n} + \sqrt{2}$, dus

(1.2) $A(n) \leqq \pi(\sqrt{n} + \sqrt{2})^2 = \pi n + 2\pi\sqrt{2n} + 2\pi.$

Beschouwt men daarnaast de concentrische cirkel C_2 met straal $\sqrt{n} - \sqrt{2}$, dan is het duidelijk dat de vierkanten, behorend bij de roosterpunten gelegen op of binnen C_2, zeker worden ingesloten door C, m.a.w.

(1.3) $A(n) \geqq \pi(\sqrt{n} - \sqrt{2})^2 = \pi n - 2\pi\sqrt{2n} + 2\pi.$

Uit (1.2) en (1.3) volgt

(1.4) $A(n) - \pi n = O(n^{\frac{1}{2}})$ (Gauss).

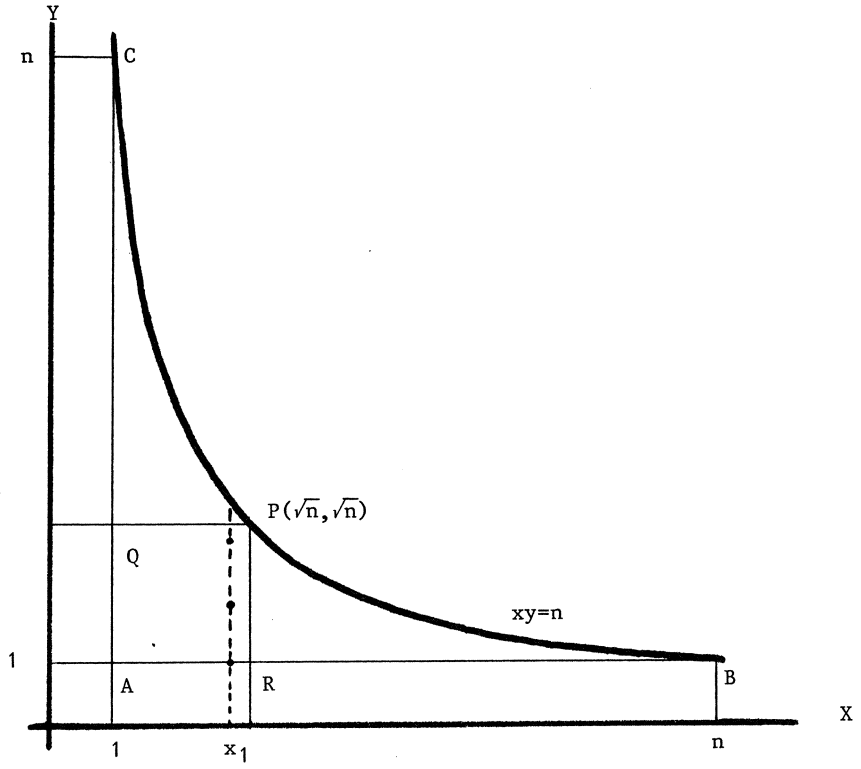
Dit probleem staat bekend als "het cirkel-probleem".
De afleiding van de ongelijkheid (1.4) is volkomen elementair.

In de tussentijd had P.G. Lejeune-Dirichlet zich beziggehouden met een analoog probleem, n.l.:

Gevraagd het aantal delers $\tau(n)$ van alle gehele getallen $\leqq n$, $(n > 0)$[2].

Wanneer men de "positieve" tak van de orthogonale hyperbool $xy = n$ tekent (zie figuur 2), dan is het duidelijk, dat ieder roosterpunt gelegen op of binnen de rand van het gebied $A(1,1)$, $B(n,1)$, $C(1,n)$ een paar gehele positieve getallen oplevert, waarvan het product $\leqq n$ is. Het gevraagde aantal delers $\tau(n)$ is dus gelijk aan het aantal

[2] Lejeune Dirichlet (2).



figuur 2.

roosterpunten op en binnen ABC.

Wanneer wij het grootste gehele getal ≦ a voorstellen door [a], dan is het duielijk, dat het aantal roosterpunten op en binnen ABC, gelegen op de ordinaat van x_1 gelijk is aan $[\frac{n}{x_1}]$.

Dus we vinden de volgende <u>exacte</u> uitkomst

$$(1.5) \qquad \tau(n) = \sum_{x=1}^{n} [\frac{n}{x}].$$

Het vervangen van $[\frac{n}{x}]$ door $\frac{n}{x}$ geeft een eerste benadering, die weer

wordt benaderd door

(1.6) $$n \int_1^n \frac{dx}{x} = n \log n,$$

welke echter te grof is; door Dirichlet werd deze uitkomst op de volgende eenvoudige wijze zeer verfijnd:

P is het punt $(\sqrt{n}, \sqrt{n})$.

ABC = ARPC + AQPB − ARPQ.

Het aantal roosterpunten op en binnen ARPC bedraagt

(1.7) $$\sum_{x=1}^{[\sqrt{n}]} [\frac{n}{x}].$$

Het is verder duidelijk, dat de congruente gebieden ARPC en AQPB evenveel roosterpunten bevatten.

Het aantal roosterpunten op en binnen vierkant ARPQ is

(1.8) $$[\sqrt{n}]^2.$$

Uit (1.7) en (1.8) volgt:

(1.9) $$\tau(n) = 2 \sum_{x=1}^{[\sqrt{n}]} [\frac{n}{x}] - [\sqrt{n}]^2.$$

Deze exacte uitdrukking wordt weer benaderd door in de eerste som $[\frac{n}{x}]$ te vervangen door $\frac{n}{x}$, en de laatste term door $(\sqrt{n})^2$.

Men overtuigt zich gemakkelijk, dat de gemaakte fout in absolute waarde $< 2\sqrt{n} + 2\sqrt{n} + 1$ is, m.a.w.

(1.10) $$\tau(n) = 2n \sum_{x=1}^{[\sqrt{n}]} \frac{1}{x} - n + O(n^{\frac{1}{2}}).$$

Tenslotte maken wij gebruik van het enige <u>niet strict elementaire</u> element uit onze beschouwing, nl. het bekende resultaat

(1.11) $$\sum_{m=1}^{N} \frac{1}{m} = C + \log N + O(N^{-1}),$$

waarin C de constante van Euler voorstelt.

Dit geschiedt alleen om de beschouwing te bekorten. Ook op elementaire manier kan een resultaat als (1.11) worden afgeleid[3].

[3] Vgl. Hardy & Wright. Theory of numbers, third ed., p. 347.

Toepassing van (1.11) op (1.10) geeft:

$$\tau(n) = 2n\{C + \tfrac{1}{2}\log n + O(n^{-\frac{1}{2}})\} - n + O(n^{\frac{1}{2}})$$

of

$$\tau(n) = n\log n + (2C - 1)n + O(n^{\frac{1}{2}}). \tag{1.12}$$

Dit is de uitdrukking die door Lejeune-Dirichlet is opgesteld. Dit probleem staat bekend als "<u>het delerprobleem</u>".

§2. Tweede periode. Verscherping der resultaten door functie-theoretische hulpmiddelen.

Bij de voorafgaande elementaire beschouwingen waren we genoodzaakt, enigszins nonchalant om te springen met de singuliere randvierkantjes, wier invloed niet nauwkeurig te overzien was. Deze beschouwingen hebben ons gevoerd tot de resttermen, die in beide gevallen $O(n^{\frac{1}{2}})$ bleken te zijn. Men kan de wens koesteren de randbeschouwingen nog meer te verfijnen, in de hoop dat daarmede de <u>orde</u> van de resttermen zal worden verlaagd. Men kan zich dus afvragen, of het misschien mogelijk zal zijn de exponent $\frac{1}{2}$ in $O(n^{\frac{1}{2}})$ te <u>verlagen</u>. Bij het cirkelprobleem heeft Gauss zich, voor zover bekend is, nimmer met deze vraag beziggehouden. Bij het delerprobleem heeft Dirichlet deze kwestie <u>wel</u> onder ogen gezien. Hiervan is alleen bekend, dat Dirichlet kort voor zijn dood aan zijn vriend Kronecker heeft geschreven (23.7.1858):

> "Seit unserm neulichem Gespräch ... ist es mir gelungen, die Funktion $\tau(x)$, die ich bisher nur mit einem Fehler der Ordnung $\sqrt{x}$ angeben konnte, <u>bedeutend in die Enge zu treiben</u>."

Dirichlet geeft echter niet aan, welke middelen hem daartoe ten dienste stonden, en welke resultaten hij daarmede kon bereiken. Het is te betwijfelen, of dit wel ooit zal worden opgehelderd. Na de dood van Dirichlet (1859) hebben deze problemen praktisch gerust gedurende de rest van de 19e eeuw. Wel dient even vermeld

te worden dat in 1886, Schuldirektor E. Pfeiffer uit Jena gemeend heeft het probleem verder te kunnen oplossen. Zijn publicatie was echter zeer onduidelijk en vol onnauwkeurigheden, waardoor de bewijskracht van zijn redenering verviel. Tenslotte publiceerde hij zijn onderzoek op een uiterst moeilijk toegankelijke plaats [4], zodat het meer dan 25 jaar heeft geduurd, voordat zijn onderzoek onder ogen van een competente beoordelaar kon komen. Wij hopen hier later op terug te komen.
Eerst in 1903 kon werkelijk vooruitgang worden geboekt. In dat jaar slaagde Voronoi erin, de restterm van het delerprobleem te verscherpen tot $O(n^{1/3} \log n)$ [5]. Het artikel en de behandeling is te lang en te gecompliceerd, om hiervan zelfs een beknopte schets te geven. Deze zelfde opmerking geldt voor de meeste nog te vermelden onderzoekingen. Terecht noemt van der Corput dit "een van de meest verborgen problemen uit de gehele getallenleer".
In 1906 wist W. Sierpinski een analoog resultaat te bereiken bij het cirkelprobleem (restterm $O(n^{1/3})$) [6]. In 1912 begon de grote Edmund Landau zich uitvoerig in de theorie der roosterpunten te verdiepen. In de eerste plaats begon hij kennis te nemen van letterlijk alles wat er vóór die tijd op dit gebied was gepubliceerd, en daarom zag hij zich genoodzaakt de bovengenoemde, reeds lang vergeten verhandeling van E. Pfeiffer uit 1886 uit de vergetelheid op te graven en aan een uitvoerige kritische studie te onderwerpen. Daarbij bleek hem spoedig dat de heuristische methode van Pfeiffer onhoudbaar was. Pfeiffer was bij zijn herhaalde limietovergangen geregeld in conflict gekomen met het begrip gelijkmatige convergentie, en verwarde dit met gewone convergentie. Het bleek Landau echter ook, dat er in de kern van de behandeling Pfeiffer nog enige waardevolle nieuwe ideeën verwerkt waren, die bij strengere opzet wel tot succes zouden kunnen voeren. Dit bracht hem ertoe, het hele onderzoek van Pfeiffer nogmaals te herhalen,

[4] E. Pfeiffer (3).
[5] G. Voronoï (4).
[6] W . Sierpinski (5).

maar nu op volmaakt strenge wijze en met de sedertdien klassiek geworden Landause beknoptheid. Het resultaat werd desondanks toch nog een uiterst omvangrijk, diepzinnig, magistraal artikel van bijna 140 pagina's (d.w.z. 7 x de lengte van het oorspronkelijke artikel) [7].
De tijd ontbreekt mij om uitvoerig stil te staan bij het uiterst waardevolle, omvangrijke onderzoek door Landau op dit gebied verricht. (Hij schreef tussen 1912 en 1926 36 belangrijke artikelen over deze problemen!).
Het wordt tijd, dat wij overgaan tot het werk van onze grote pionier op dit gebied, J.G. van der Corput.

§3. Het eerste werk van Van der Corput. Dissertatie. Gevolgen.

Op 8 juli 1919 promoveerde J.G. van der Corput bij Prof.dr . J.C. Kluyver. De titel van zijn proefschrift was "Over roosterpunten in het platte vlak". (De betekenis van de methoden van Voronoï en Pfeiffer). De inhoud van dit uiterst belangrijke proefschrift geeft nog veel meer dan zijn tamelijk bescheiden titel belooft. Inderdaad geeft het een vergelijkend kritisch onderzoek van de methoden van Voronoï en Pfeiffer, maar de auteur geeft daarbij een volkomen originele opbouw van deze methoden, waarbij hij erin slaagt om op verbluffende wijze eenheid en vereenvoudiging te brengen in de vaak grote diversiteit van de methoden. Ook breidt hij zijn onderzoek uit op talrijke andere roosterpuntproblemen, waarbij uit de aard der zaak veel aandacht wordt geschonken aan het zo belangrijke werk van Landau. Niet zonder belang is de opmerking van Van der Corput bij vergelijking van de methoden van de verschillende auteurs. Ten aanzien van Landau merkt hij op (diss. p. 8): "Wanneer men zich, zoals overal in dit proefschrift geschiedt, tot roosterpunten in het platte vlak en tot benaderingen aan de bovenkant bepaalt, <u>dan staat de methode van Landau op het ogenblik ver achter bij de beide andere (Voronoï en Pfeiffer)</u>".

[7] E. Landau (6).

Het komt mij voor, dat Van der Corput deze bewering enige dagen later niet zou hebben herhaald, zoals ik in de volgende paragraaf nader hoop aan te tonen.
Om alle eventuele misverstand te voorkomen, Landau heeft zijn geweldige waardering voor het meesterwerk van de jonge doctor nimmer onder stoelen of banken gestoken, en deze waardering was wederkerig. Voordat ik dit korte verslag van de dissertatie van Van der Corput beëindig, wil ik er nadrukkelijk op wijzen, dat de verkregen eindresultaten hier nog niet verder gaan dan de bovengenoemde uitkomsten van Sierpinski en Voronoï. Op pagina 11 staat alleen in verband hiermede de opmerking "terwijl het van grote betekenis zou zijn als de exponent $\frac{1}{3}$ verlaagd kon worden". Ook hierin zou Van der Corput vrij spoedig sensationele verandering brengen.

§4. Reactie van Landau? Kort bewijs van de cirkelstelling.

Vóór de verschijning van de dissertatie van Van der Corput had Landau reeds 17 publicaties over de theorie der roosterpunten op zijn naam staan. In meerdere daarvan worden strenge methoden afgeleid, die op geraffineerde wijze voeren tot de resultaten van Voronoï en Sierpinski. Verder heeft Landau deze beschouwingen uitgebreid tot meer dimensies. De meeste resultaten worden verkregen met behulp van verfijnde toepassing van de complexe functietheorie. Ook deze uitwerkingen waren nog tamelijk gecompliceerd en omvangrijk. Maar juist drie dagen vóór de promotie van Van der Corput, op 5 juli 1919, slaagde hij erin, het bewijs van het cirkelprobleem te geven in twee bladzijden. In tegenstelling tot de voorafgaande onderzoekingen wil ik trachten de gang van de gebruikte methode zeer kort (maar onvolledig) te schetsen. Het resultaat wordt gevonden met behulp van algemene eigenschappen van de Besselfuncties, i.h.b. het bekende resultaat

$$(4.1) \qquad \frac{1}{2\pi i}\int_{1-\infty i}^{1+\infty i} \frac{e^{As-\frac{B}{s}}}{s^4}\,ds = \left(\frac{A}{B}\right)^{3/2} J_3(2\sqrt{AB}).\ A > 0,\ B > 0.$$

Het <u>kernpunt</u> vormt de toepassing van de thèta-reeks

$$\theta(s) = \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s},$$

waarvoor de klassieke Jacobi-transformatie geldt

$$(4.2) \qquad \theta(s) = \frac{1}{\sqrt{s}}\,\theta\left(\frac{1}{s}\right).$$

Als r(m) het <u>aantal</u> oplossingen van

$$(4.3) \qquad x^2 + y^2 = m$$

voorstelt, dan is

$$(4.4) \qquad \theta^2(s) = \sum_{m=0}^{\infty} r(m)e^{-\pi ms} = \frac{1}{s} + \frac{1}{s}\sum_{m=1}^{\infty} r(m)e^{-\pi\frac{m}{s}}$$

wegens (4.2).

Het aantal roosterpunten binnen en op de cirkel met straal x bedraagt

$$A(x) = \sum_{m\leq x} r(m) \qquad (x \geqq 0).$$

Het hoofdmoment van het bewijs is het volgende. Men kan gemakkelijk aantonen dat

$$\int_0^x dy \int_0^y A(w)dw = \tfrac{1}{2}\sum_{m\leq x} r(m)(x-m)^2 =$$

$$= \frac{1}{2\pi^3 i}\sum_{m=0}^{\infty} r(m)\int_{1-\infty i}^{1+\infty i} \frac{e^{\pi(x-m)s}}{s^3}\,ds =$$

$$= \frac{1}{2\pi^3 i}\int_{1-\infty i}^{1+\infty i} \frac{e^{\pi xs}}{s^3}\,\theta^2(s)ds =$$

$$= \frac{1}{2\pi^3 i}\int_{1-\infty i}^{1+\infty i} \frac{e^{\pi xs}}{s^4}\,ds + \frac{1}{2\pi^3 1}\int_{1-\infty i}^{1+\infty i}\sum_{m=1}^{\infty} r(m)\,\frac{e^{\pi xs - \pi\frac{m}{s}}}{s^4}ds$$

$$= \frac{\pi}{6}x^3 + \frac{1}{\pi^2}\sum_{m=1}\frac{r(m)}{m^{3/2}}\,x^{3/2}\,J_3(2\pi\sqrt{mx}).$$

Differentiatie naar x geeft

$$(4.5) \qquad \int_0^x A(w)dw = \frac{\pi}{2}x^2 + \frac{1}{\pi}\sum_{m=1}^{\infty}\frac{r(m)}{m}\,xJ_2(2\pi\sqrt{mx}).$$

Voor $z = x + x^{1/3}$ vindt men zonder grote moeite

$$\int_x^z A(w)dw = \pi x^{4/3} + \frac{\pi}{2} x^{2/3} + \frac{1}{\pi} \sum_{m=1}^{\infty} \frac{r(m)}{m}(zJ_2(2\pi\sqrt{mz}) - xJ_2(2\pi\sqrt{mx})) =$$
$$= \pi x^{4/3} + O(x^{2/3}).$$

Tenslotte volgt uit

$$x^{1/3}A(x) \leqq \int_x^z A(w)dw \leqq x^{1/3}A(z)$$

enerzijds

$$A(x) \leqq \pi x + O(x^{1/3}),$$

anderzijds

$$A(z) \geqq \pi x + O(x^{1/3}) = \pi z + O(z^{1/3}),$$

of

$$A(x) - \pi x = O(x^{1/3}).$$

In de volledige uitwerking wordt nog gebruikt gemaakt van bekende recursie-formules voor de Besselfuncties, benevens eenvoudige asymptotische schattingen van $J_1(y)$ en $J_2(y)$. Het bewijs is, zoals bij Landau te verwachten is, in alle opzichten compleet. Alle omkeringen van sommatie- en integratievolgorde worden volledig gemotiveerd.
Gegeven het feit, dat Landau op 5 juli 1919 reeds enige weken in het bezit was van de dissertatie van Van der Corput, waag ik de veronderstelling, in dit bewijs, dat op de dag der promotie (8 juli 1919) bij de redactie van het "Mathematische Zeitschrift" binnenkwam, een reactie te mogen zien op de in paragraaf 3 vermelde opmerking van Van der Corput ten aanzien van de door Landau toegepaste methoden [8]. Landau is terecht steeds trots geweest op dit uiterst korte bewijs.

[8] Landau (7)

§5. De knuppel in het hoenderhok. Sensationele verscherping der resultaten.

Van zeer verschillende zijde waren deze problemen nu met de machtigste middelen der complexe functietheorie aangepakt en al deze diverse methoden hadden uniform geleid tot dezelfde resttermen $O(x^{1/3})$ bij het cirkelprobleem, en $O(x^{1/3}\log x)$, resp. $O(x^{1/3+\varepsilon})$ bij het delerprobleem, zodat in de deskundige kringen met zekere gelatenheid de mening begon post te vatten, dat met deze resultaten de uiterste grens was bereikt.
Er was slechts één argument gevonden, dat althans in afwijkende richting scheen te wijzen. Reeds in 1915 hadden Hardy [9] en Landau [10] onafhankelijk van elkaar bewezen, dat de exponenten van x in beide resttermen zeker $\geq \frac{1}{4}$ moesten zijn.
In 1923 echter deed Van der Corput de wetenschappelijke wereld op haar grondvesten schudden door de publicatie van een uiterst moeilijke verhandeling, waarin hij aantoonde dat de betrokken exponenten kleiner dan $\frac{1}{3}$ moesten zijn [11]. Weliswaar was de aanvankelijk bereikte verscherping niet spectaculair, immers Van der Corput bewees, dat de exponent $\frac{1}{3}$ kon worden vervangen door

$$\frac{33}{100} < \frac{1}{3},$$

maar deze gebeurtenis was van zo groot belang, dat Landau kon spreken van een chaos die Van der Corput door zijn verkleining van de exponent had aangericht. "Die scheinbar prästabilierte Harmonie, dass alle bisherigen, den verschiedenen mathematischen Diziplinen, - Zahlentheorie, reeller Funktionentheorie, komplexer Funktionentheorie, Geometrie, - angehörigen Methoden z.B. beim Kreisproblem zu $\frac{1}{3}$ geführt hatten, ist durchbrochen."
Het artikel van Van der Corput was echter dermate gecompliceerd van opbouw, dat ook de belangrijkste expert met reikhalzen uitzagen naar

9) G.H. Hardy (8).
10) E. Landau (9).
11) J.G. van der Corput (10).

een meer overzichtelijke behandeling van deze moeilijke materie [12].
De nieuwe methode berustte op het volgende beginsel. Van der Corput was er op uiterst geraffineerde wijze in geslaagd om de restschattingen terug te brengen tot de meer overzichtelijke schattingen van exponentiële sommen van het type:

$$(5.1) \qquad S(m,N) = \sum_{n=m}^{n=m+N} e^{\pi i f(n)},$$

waarin f(n) een gegeven reële functie voorstelt, afhankelijk van het gestelde probleem. Triviaal is alleen de schatting

$$(5.2) \qquad |S(m,N)| \leq N.$$

Het is duidelijk dat bij een lineaire functie exacte sommatie mogelijk is. De exacte sommatie voor het geval van een kwadratische functie behoort reeds tot de grootste prestaties van Gauss (sommen van Gauss;. resultaat $O(N^{\frac{1}{2}})$).
Voor meer gecompliceerde functies f(n), bleek het uiterst moeilijk om tot een scherpere schatting dan het triviale resultaat (5.2) te geraken. Dit onderzoek werd met succes ingeleid door H. Weyl (1916), verder met grote intensiteit voortgezet door I.M. Vinogradov, maar bovenal door Van der Corput.
De behoefte aan een meer overzichtelijke behandeling van deze schokkende kwestie werd ook door van der Corput zelf in sterke mate gevoeld. In 1928 verscheen de met ongeduld verwachte verhandeling [13]. Hierin slaagde de auteur om op veel meer overzichtelijke wijze de exponent in het delerprobleem te reduceren tot $\frac{27}{82}$. Tezelfder tijd heeft op instigatie van Van der Corput diens zeer gebaafde leerling L.W. Nieland het cirkelprobleem volgens dezelfde methode uitgewerkt. De exponent van de restterm was dezelfde, nl. $\frac{27}{82}$ [14].

12) Littlewood en Walfisz merken hierbij op: "Van der Corput's method is probably the most formidable argument in the whole of pure mathematics".

13) J.G. van der Corput (11).

14) L.W. Nieland (12). Nieland behoorde tot de in 1945 gevankelijk weggevoerde inwoners van Putten. Hij is helaas tijdens zijn gevangenschap omgekomen.

Na het pionierswerk van Van der Corput en Nieland hebben talrijke auteurs getracht de bovengenoemde records te verbeteren. Al vertonen de uitvoeringen van deze berekeningen op enkele detailpunten geringe vereenvoudigingen, in grote trekken volgen ze dezelfde weg als die van hun voorgangers, al wordt deze weg steeds moeizamer naarmate de exponenten der resttermen kleiner worden. Periodiek wordt het record met een kleinigheidje verbeterd, maar bepaald nieuwe gezichtspunten hebben zich sedertdien niet voorgedaan. Deze verbeteringen hebben zich voortgezet tot in de allerlaatste tijd. Een tamelijk volledig overzicht van deze resultaten is te vinden in het desbetreffende encyclopedie-artikel van L.K. Hua [15]. De scherpste daarin vermelde resultaten zijn:

cirkelprobleem: L.K. Hua; 1942: $\frac{13}{40}$

delerprobleem: Tsung-Too Chih, 1950; H.E. Richert, 1953: $\frac{15}{46}$.

Deze records zijn in de laatste jaren nog verder verbeterd [16]. Tenslotte moet ik hier nog aan toevoegen, dat in 1932 reeds door Vinogradov werd beweerd dat hij een nog lagere grens had bereikt, nl. $\frac{17}{53}$ [17]. Uit de vernietigende bespreking, door Walfisz aan dit artikel gewijd, (Zentralblatt 5, 1933, p. 241), kunnen wij opmaken dat de numerieke resultaten zonder tussenrekening worden aangegeven en daardoor oncontroleerbaar zijn, terwijl er in de theoretische opbouw zulke ontstellende blunders zijn geconstateerd, dat zowel methode als resultaat als waardeloos dienen te worden aangemerkt. Waar zal de grens liggen? Het komt ons voor dat deze grens nog lang niet bereikt is, al is de afstand tot de ondergrens $\frac{1}{4}$ inmiddels al sterk gereduceerd. De tijd zal het misschien leren, maar verdere voortgang langs de tot nog toe bekende wegen worden steeds moeizamer.

15) L.K. Hua (13).

16) In 1963 werd nog door Jing-Zun Chen (Scientia Sinica (Peking) 12, 1963, p. 633-649) bij het cirkelprobleem $\frac{12}{37}$ bereikt.

17) I.M. Vinogradov (14).

Literatuur.

[1] *C.F. Gauss*, De nexu inter multitudinem classicum in quas formae binariae secundi gradus distribuuntur, earumque determinantem. Dit fragmentarisch onderzoek is in de nalatenschap van Gauss ontdekt, en voor het eerst na zijn dood gepubliceerd in zijn Gesammelte Werke, Bd. II (1863), p. 269-291.

[2] *P.G. Lejeune-Dirichlet*, Ueber die Bestimmung der mittleren Werthe in der Zahlentheorie, Abh. der Kön. Akad. d. Wissensch., Berlin, 1849, Math. Abh. p. 69-83, Werke II, p. 49-66.

[3] *E. Pfeiffer*, Ueber die Periodicität in der Teilbarkeit der Zahlen und über die Verteilung der Klassen positiver quadratischer Formen auf ihre Determinanten, Jahresber. der Pfeiffer'schen Lehr- und Erziehungs-Anstalt zu Jena über das Schuljahr von Ostern 1885 bis Ostern 1886, p. 1-21, 1886.

[4] *G. Voronoï*, Sur un problème du calcul des fonctions asymptotiques, J. f. reine u. angew. Math. Bd. 126, p. 241-281, 1903.

[5] *W. Sierpinski*, Prace matematyczno-fizyczni, Bd. 17, p. 77-114, 1906. Resumé in het Frans (3 pag.): Sur un problème du calcul des functions asymptotiques, l.c.p. 115-118.

[6] *E. Landau*, Die Bedeutung der Pfeifferischen Methode für die analytische Zahlentheorie, Sitzungsber. der keiserl. Akad. d. Wissensch. in Wien, Math. naturw. Kl. Bd. 121, Abt. IIa, 1912, p. 2195-2335.

[7] *E. Landau*, Ueber die Gitterpunkte in einem Kreise, Math. Zeitschr. 5, (1919), p. 319-320.

[8] *G.H. Hardy*, On the expression of a number as the sum of two squares, Quarterly Journal of Math., vol. 46, p. 263-283, (1915).

[9] *E. Landau*, Ueber die Gitterpunkte in einem Kreise (II), Göttinger Nachrichten, p. 161-171, (1915).

[10] *J.G. van der Corput*, Neue zahlentheoretische Abschätzungen, Math. Annalen, Bd. LXXXIX, (1923), p. 215-254.

[11] *J.G. van der Corput*, Zum Teilerproblem, Math. Ann. 98, p. 697-716, 1928.

[12] *L.W. Nieland*, Ueber das Kreisproblem, Math. Ann. 98, p. 717-736, 1928.

[13] *Loo Keng Hua*, Peking, Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie, Enzyklopädie der Math. Wissensch. Bd. I 2, Heft 13, Teil I, 121 p., 1959.

[14] *I.M. Vinogradov*, Bull. de l'Ac. des Sciences de l'Urss. VII Série, Classe des sciences mathématiques et naturelles No. 3, p. 313-336, (Russisch), 1932.

MC SYLLABI

1.1 F. Göbel, J. van de Lune. *Leergang besliskunde, deel 1: wiskundige basiskennis.* 1965.

1.2 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 2: kansberekening.* 1965.

1.3 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 3: statistiek.* 1966.

1.4 G. de Leve, W. Molenaar. *Leergang besliskunde, deel 4: Markovketens en wachttijden.* 1966.

1.5 J. Kriens, G. de Leve. *Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde.* 1966.

1.6a B. Dorhout, J. Kriens. *Leergang besliskunde, deel 6a: wiskundige programmering 1.* 1968.

1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. *Leergang besliskunde, deel 6b: wiskundige programmering 2.* 1977.

1.7a G. de Leve. *Leergang besliskunde, deel 7a: dynamische programmering 1.* 1968.

1.7b G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7b: dynamische programmering 2.* 1970.

1.7c G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7c: dynamische programmering 3.* 1971.

1.8 J. Kriens, F. Göbel, W. Molenaar. *Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie.* 1968.

2.1 G.J.R. Förch, P.J. van der Houwen, R.P. van de Riet. *Colloquium stabiliteit van differentieschema's, deel 1.* 1967.

2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. *Colloquium stabiliteit van differentieschema's, deel 2.* 1968.

3.1 H.A. Lauwerier. *Randwaardeproblemen, deel 1.* 1967.

3.2 H.A. Lauwerier. *Randwaardeproblemen, deel 2.* 1968.

3.3 H.A. Lauwerier. *Randwaardeproblemen, deel 3.* 1968.

4 H.A. Lauwerier. *Representaties van groepen.* 1968.

5 J.H. van Lint, J.J. Seidel, P.C. Baayen. *Colloquium discrete wiskunde.* 1968.

6 K.K. Koksma. *Cursus ALGOL 60.* 1969.

7.1 *Colloquium moderne rekenmachines, deel 1.* 1969.

7.2 *Colloquium moderne rekenmachines, deel 2.* 1969.

8 H. Bavinck, J. Grasman. *Relaxatietrillingen.* 1969.

9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. *Colloquium elliptische differentiaalvergelijkingen, deel 1.* 1970.

9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, E.M. de Jager, N.M. Temme, R.J. de Vogelaere. *Colloquium elliptische differentiaalvergelijkingen, deel 2.* 1970.

10 J. Fabius, W.R. van Zwet. *Grondbegrippen van de waarschijnlijkheidsrekening.* 1970.

11 H. Bart, M.A. Kaashoek. H.G.J. Pijls, W.J. de Schipper, J. de Vries. *Colloquium halfalgebra's en positieve operatoren.* 1971.

12 T.J. Dekker. *Numerieke algebra.* 1971.

13 F.E.J. Kruseman Aretz. *Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8.* 1971.

14 H. Bavinck, W. Gautschi, G.M. Willems. *Colloquium approximatietheorie.* 1971.

15.1 T.J. Dekker, P.W. Hemker, P.J. van der Houwen. *Colloquium stijve differentiaalvergelijkingen, deel 1.* 1972.

15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. *Colloquium stijve differentiaalvergelijkingen, deel 2.* 1973.

15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. *Colloquium stijve differentiaalvergelijkingen, deel 3.* 1975.

16.1 L. Geurts. *Cursus programmeren, deel 1: de elementen van het programmeren.* 1973.

16.2 L. Geurts. *Cursus programmeren, deel 2: de programmeertaal ALGOL 60.* 1973.

17.1 P.S. Stobbe. *Lineaire algebra, deel 1.* 1973.

17.2 P.S. Stobbe. *Lineaire algebra, deel 2.* 1973.

17.3 N.M. Temme. *Lineaire algebra, deel 3.* 1976.

18 F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. *Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971.* 1973.

19 A. Hordijk, R. Potharst, J.Th. Runnenburg. *Optimaal stoppen van Markovketens.* 1973.

20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E. Slagt. *ALGOL 60 procedures voor begin- en randwaardeproblemen.* 1976.

21 J.W. de Bakker (red.). *Colloquium programmacorrectheid.* 1975.

22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. *Asymptotische methoden in de toetsingstheorie; toepassingen van naburigheid.* 1976.

23.1 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 1.* 1976.

23.2 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 2.* 1977.

24.1 P.J. van der Houwen. *Numerieke integratie van differentiaalvergelijkingen, deel 1: eenstapsmethoden.* 1974.

25 *Colloquium structuur van programmeertalen.* 1976.

26.1 N.M. Temme (ed.). *Nonlinear analysis, volume 1.* 1976.

26.2 N.M. Temme (ed.). *Nonlinear analysis, volume 2.* 1976.

27 M. Bakker, P.W. Hemker, P.J. van der Houwen, S.J. Polak, M. van Veldhuizen. *Colloquium discretiseringsmethoden.* 1976.

28 O. Diekmann, N.M. Temme (eds.). *Nonlinear diffusion problems.* 1976.

29.1 J.C.P. Bus (red.). *Colloquium numerieke programmatuur, deel 1A, deel 1B.* 1976.

29.2 H.J.J. te Riele (red.). *Colloquium numerieke programmatuur, deel 2.* 1977.

30 J. Heering, P. Klint (red.). *Colloquium programmeeromgevingen.* 1983.

31 J.H. van Lint (red.). *Inleiding in de coderingstheorie.* 1976.

32 L. Geurts (red.). *Colloquium bedrijfsystemen.* 1976.

33 P.J. van der Houwen. *Berekening van waterstanden in zeeën en rivieren.* 1977.

34 J. Hemelrijk. *Oriënterende cursus mathematische statistiek.* 1977.

35 P.J.W. ten Hagen (red.). *Colloquium computer graphics.* 1978.

36 J.M. Aarts, J. de Vries. *Colloquium topologische dynamische systemen.* 1977.

37 J.C. van Vliet (red.). *Colloquium capita datastructuren.* 1978.

38.1 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part I.* 1979.

38.2 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part II.* 1979.

39 O.J. Vrieze, G.L. Wanrooy. *Colloquium stochastische spelen.* 1978.

40 J. van Tiel. *Convexe analyse.* 1979.

41 H.J.J. te Riele (ed.). *Colloquium numerical treatment of integral equations.* 1979.

42 J.C. van Vliet (red.). *Colloquium capita implementatie van programmeertalen.* 1980.

43 A.M. Cohen, H.A. Wilbrink. *Eindige groepen (een inleidende cursus).* 1980.

44 J.G. Verwer (ed.). *Colloquium numerical solution of partial differential equations.* 1980.

45 P. Klint (red.). *Colloquium hogere programmeertalen en computerarchitectuur.* 1980.

46.1 P.M.G. Apers (red.). *Colloquium databankorganisatie, deel 1.* 1981.

46.2 P.G.M. Apers (red.). *Colloquium databankorganisatie, deel 2.* 1981.

47.1 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60: general information and indices.* 1981.

47.2 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 1: elementary procedures; vol. 2: algebraic evaluations.* 1981.

47.3 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra, part I.* 1981.

47.4 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3B: linear algebra, part II.* 1981.

47.5 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems, part I.* 1981.

47.6 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 5B: analytical problems, part II.* 1981.

47.7 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation.* 1981.

48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 1.* 1982.

48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 2.* 1982.

49 T.H. Koornwinder (ed.). *The structure of real semisimple Lie groups.* 1982.

50 H. Nijmeijer. *Inleiding systeemtheorie.* 1982.

51 P.J. Hoogendoorn (red.). *Cursus cryptografie.* 1983.

CWI SYLLABI

1 Vacantiecursus 1984: *Hewet - plus wiskunde.* 1984.

2 E.M. de Jager, H.G.J. Pijls (eds.). *Proceedings Seminar 1981-1982. Mathematical structures in field theories.* 1984.

3 W.C.M. Kallenberg, et al. *Testing statistical hypotheses: worked solutions.* 1984.

4 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 1.* 1984.

5 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 2.* 1984.

6 P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls, J.W. de Roever. *Proceedings Seminar 1982-1983. Mathematical structures in field theories.* 1985.

7 Vacantiecurus 1985: *Variatierekening.* 1985.

8 G.M. Tuynman. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.1 Geometric quantization.* 1985.

9 J. van Leeuwen, J.K. Lenstra (eds.). *Parallel computers and computations.* 1985.

10 Vacantiecursus 1986: *Matrices.* 1986.

11 P.W.H. Lemmens. *Discrete wiskunde: tellen, grafen, spelen en codes.* 1986.