Onderafdeling der Wiskunde

Discrete Wiskunde

NAAR HET COLLEGE VAN PROF. DR. J.H. VAN LINT

VOORJAARSSEMESTER 1971

TECHNISCHE HOGESCHOOL EINDHOVEN

TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

DISCRETE WISKUNDE

Naar het college van

Prof. Dr. J.H. van Lint

Voorjaarssemester 1971

Inhoudsbeschrijving

DISCRETE WISKUNDE

J.H. van Lint

voorjaarssemester 1971

Hoofdstuk I.	Getaltheorie	1
Hoofdstuk II.	Algebra	12
Hoofdstuk III.	Coding Theory	18
	Lineaire codes (groep-codes)	22
	Hamming codes	25
	Reed-Muller codes	26
	Product codes (Slepian)	27
	Hadamard matrices en codes	28
	Hadamard code	31
	Cyclische codes	32
	BCH-codes	34
Hoofdstuk IV.	Block designs	37
	Eindige meetkunde	38
	Latijnse vierkanten	41
	Difference sets	42
	Toepassingen	44
	Opgaven 1-35 Discrete Wiskunde	47

JdG, 29 Juli 2005

College Discrete Wiskunde 1969

Hoofdstuk I. Getaltheorie

De natuurlijke getallen worden bekend verondersteld, evenals deelbaarheidseigenschappen enz. We gebruiken de notatie $n \mid m$ om aan te geven dat n een deler van m is. De eigenschappen (1.1) t/m (1.4) nemen we als bekend aan.

(1.1) Het getal $p > 1$ heet priemgetal als p geen andere delers heeft dan 1 en p zelf. (Het getal 1 is niet een priemgetal.)

(1.2) Ieder getal groter dan 1 is éénduidig te ontbinden in priemfactoren (op volgorde na).

(1.3) Bij ieder paar getallen a, b is er een éénduidig bepaald getal d met de eigenschappen

(i) $d \mid a$ en $d \mid b$,

(ii) uit $d_1 \mid a$ en $d_1 \mid b$ volgt $d_1 \mid d$.

We noemen d de grootste gemene deler van a en b en geven deze in het vervolg aan met (a,b).

(1.4) Bij ieder paar getallen a, b is er een éénduidig bepaald getal m met de eigenschappen

(i) $a \mid m$ en $b \mid m$,

(ii) uit $a \mid n$ en $b \mid n$ volgt $m \mid n$.

We noemen m het kleinste gemene veelvoud van a en b en geven dit in het vervolg aan met [a,b].

De priemgetallen kunnen we nummeren naar toenemende grootte:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots \quad .$$

(1.5) Stelling: Er zijn oneindig veel priemgetallen.

Bewijs: Beschouw het getal $n = p_1 p_2 p_3 \ldots p_r + 1$. Daar voor $i \leq r$ duidelijk is dat $p_i \nmid n$ moet op grond van (1.2) n deelbaar zijn door een priemgetal $p > p_r$. Dit geldt voor iedere r.

We kunnen volgens (1.2) ieder getal n als volgt schrijven:

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i} \quad .$$

In dit "oneindige product" zijn slechts eindig veel van de factoren van 1 verschillend.
Het is nu onmiddellijk duidelijk dat uit

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i} \quad \text{en} \quad m = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

volgt

$$(n,m) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\beta_i)} \quad \text{en} \quad [n,m] = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i,\beta_i)} .$$

Hieruit volgt:

(1.6) Stelling: $(n,m)[n,m] = nm$.

Een lijst van priemgetallen kan men maken met behulp van de zgn. zeef van Eratosthenes (276 - 194 v.C.): In iedere stap gaat men uit van alle priemgetallen tot zekere grens N en construeert de priemgetallen $\leq N^2$ door voor iedere $p_i \leq N$ alle veelvouden die $\leq N^2$ zijn uit de rij $1,2,\ldots,N^2$ te schrappen. De getallen die overblijven tussen N en N^2 zijn de priemgetallen in dit interval.

Congruenties

We houden ons nu bezig met alle gehele getallen (ook de negatieve).

(1.7) Definitie: We noemen a en b congruent modulo m en schrijven dit als:
$a \equiv b \pmod m$ als $b - a$ door m deelbaar is.

De relatie $\equiv$ is een equivalentie. We kunnen de gehele getallen indelen in klassen equivalente getallen; iedere klasse bestaat uit getallen die onderling congruent modulo m zijn, d.w.z. iedere klasse bestaat uit getallen die bij deling door m dezelfde rest geven. Een stelsel $a_1,a_2,\ldots,a_m$ heet volledig stelsel representanten of volledig restsysteem modulo m als uit $a_i \equiv a_j \pmod m$ volgt dat $i = j$. Er is dan voor ieder getal n precies één a_i in het stelsel met $a_i \equiv n \pmod m$. Een voorbeeld is $(0,1,2,\ldots,m-1)$.

(1.8) Stelling: Als $a \equiv b \pmod m$ en $c \equiv d \pmod m$ dan is $a+c \equiv b+d \pmod m$, $ac \equiv bd \pmod m$ en $ka \equiv kb \pmod m$ voor iedere k.

Bewijs: a) Uit $m \mid (b-a)$ en $m \mid (d-c)$ volgt $m \mid (b+d-a-c)$.

b) $bd - ac = (b-a)d + a(d-c)$.

c) $kb - ka = k(b-a)$.

(1.9) Stelling: Als $ka \equiv kb \pmod m$ en $(k,m) = d$ dan is

$$a \equiv b \pmod{\frac{m}{d}} .$$

Bewijs: Schrijf $k = dk_1$, $m = dm_1$ met $(k_1,m_1) = 1$. Dan volgt uit $m \mid (kb - ka)$ dat $m_1 \mid k_1(b-a)$ en daar $(k_1,m_1) = 1$ moet $m_1 \mid (b-a)$.

(1.10) Stelling: Als $a_1,a_2,\ldots,a_m$ een volledig restsysteem mod m is en $(k,m) = 1$ dan is ook $ka_1,ka_2,\ldots,ka_m$ een volledig restsysteem mod m.

Bewijs: Uit $ka_i \equiv ka_j \pmod m$ volgt m.b.v. (1.9), dat $a_i \equiv a_j \pmod m$ en dus $i = j$. De getallen $ka_1,\ldots,ka_m$ representeren dus m verschillende restklassen, dat zijn alle restklassen.

Het bijvoeglijk naamwoord "volledig" hebben we gebruikt omdat we vaak in restsystemen geïnteresseerd zijn die niet uit representanten van alle klassen bestaan maar alleen de representanten bevatten van restklassen mod m waarvan de elementen n de eigenschap $(n,m) = 1$ hebben. Zo'n systeem is in het geval $m = 12$ bijvoorbeeld 1,5,7,11. We noemen dit een gereduceerd restsysteem.

(1.11) Definitie: Het aantal elementen in een gereduceerd restsysteem mod m, d.w.z. het aantal natuurlijke getallen $n \leq m$ waarvoor $(n,m) = 1$ wordt aangegeven met $\varphi(m)$ (functie van Euler).

(1.12) Stelling: Als $a_1,a_2,\ldots,a_{\varphi(m)}$ een gereduceerd restsysteem mod m is en $(k,m) = 1$ dan is ook $ka_1,ka_2,\ldots,ka_{\varphi(m)}$ een gereduceerd restsysteem.

Bewijs: Merk op dat het tweede systeem voldoende elementen bevat. Verder is volgens (1.9) $ka_i \equiv ka_j \pmod m$ alleen als $i = j$. Daar voor iedere i geldt $(ka_i,m) = 1$ volgt het gestelde.

(1.13) Definitie: Een functie f gedefinieerd op de natuurlijke getallen heet multiplicatief als $f(mn) = f(m)f(n)$ voor alle paren m, n waarvoor $(m,n) = 1$ geldt.

(1.14) Stelling: φ is multiplicatief.

Bewijs: Zij $(m,n) = 1$. Laat $x_1,x_2,\ldots,x_{\varphi(n)}$ een gereduceerd restsysteem mod n zijn en $y_1,y_2,\ldots,y_{\varphi(m)}$ een gereduceerd restsysteem mod m. Beschouw de getallen

$mx_i + ny_j \quad (i = 1,\ldots,\varphi(n);\ j = 1,\ldots,\varphi(m))$.

Dit zijn $\varphi(n)\varphi(m)$ getallen. Uit

$mx_i + ny_j \equiv mx_k + ny_\ell \pmod{mn}$

volgt

$mx_i \equiv mx_k \pmod{n}$ en $ny_j \equiv ny_\ell \pmod{m}$,

dus volgens (1.9):

$x_i \equiv x_k \pmod{n}$ en $y_j \equiv y_\ell \pmod{m}$,

en dit kan alleen als $i = k$ en $j = \ell$. Daar

$(mx_i + ny_j, mn) = 1$ voor iedere i en j

hebben we hier $\varphi(m)\varphi(n)$ verschillende elementen van een gereduceerd restsysteem mod mn. Als we nog laten zien dat er voor iedere a met $(a,mn) = 1$ een i is en een j zó dat

$mx_i + ny_j \equiv a \pmod{mn}$

is het gestelde bewezen. Nu is volgens (1.12) het stelsel mx_i $(i = 1,\ldots,\varphi(n))$ een gereduceerd restsysteem (mod n), d.w.z. er is een i zo dat $mx_i \equiv a \pmod{n}$ daar $(a,n) = 1$. Evenzo is er een j zo dat $ny_j \equiv a \pmod{m}$. Dus geldt

$m \mid (mx_i + ny_j - a)$,

$n \mid (mx_i + ny_j - a)$

d.w.z. volgens (1.4): $[m,n] \mid (mx_i + ny_j - a)$.

Daar echter uit (1.6) volgt dat $[m,n] = mn$ hebben we bewezen dat $mx_i + ny_j \equiv a \pmod{mn}$.

(1.15) Stelling: $\varphi(m) = m\prod_{p \mid m}(1 - \frac{1}{p})$.

Bewijs: Als $m = p^\alpha$ dan is uit het volledige restsysteem mod m : $1, 2, 3, \ldots, p^\alpha$ van ieder opeenvolgend p-tal steeds de laatste door p deelbaar. D.w.z. $p^{\alpha-1}$ van deze getallen zijn door p deelbaar. Dus is $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Zij nu

$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

de ontbinding van m in priemfactoren. Volgens (1,14) is dan

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\dots p_k^{\alpha_k - 1}(p_k - 1) =$$

$$= m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = m \Pi_{p|m} \left(1 - \frac{1}{p}\right) \quad .$$

Opmerking: Pas op dat de notatie hier geen verwarring veroorzaakt. In dit bewijs zijn $p_1, p_2, \dots, p_k$ de verschillende priemfactoren die deler zijn van m, dus $\alpha_1 > 0$, $\alpha_2 > 0$, ..., $\alpha_k > 0$. Hier is dus niet p_1 het eerste priemgetal te weten 2, enz. zoals in (1.5) etc. het geval was.

(1.16) Stelling: $\Sigma_{d|n} \varphi(d) = n$.

Bewijs: Laat $d_1, d_2, \dots, d_k$ de delers van n zijn. Verdeel de getallen $1, 2, \dots, n$ in k klassen $C_1, \dots, C_k$ waarbij C_i bestaat uit die getallen $m \leq n$ waarvoor $(m,n) = d_i$. Het aantal getallen in C_i is

$$\Sigma_{m \leq n, (m,n) = d_i} 1 = \Sigma_{m' \leq n/d_i, (m', n/d_i) = 1} 1 = \varphi\left(\frac{n}{d_i}\right) \quad .$$

Daar

$$\Sigma_{d|n} \varphi\left(\frac{n}{d}\right) = \Sigma_{d|n} \varphi(d)$$

volgt het gestelde.

De zeef van Eratosthenes is een methode om van de getallen $\leq N$ alle niet-priemgetallen te elimineren. We geven nog een voorbeeld van een zeef. Deze methode heet principe van Sylvester (ook: principle of inclusion and exclusion).

(1.17) Stelling: Als S een verzameling is met n elementen, $S_1, S_2, \dots, S_N$ deelverzamelingen van S zijn en $E_{i_1, i_2, \dots, i_k}$ het aantal elementen van $S_{i_1} \cap S_{i_2} \cap \dots \cap S_{i_k}$ voorstelt dan is

$$n - \Sigma_i E_i + \Sigma_{i<j} E_{i,j} - \Sigma_{i<j<k} E_{i,j,k} + \dots + (-1)^N E_{1,2,\dots,N}$$

het aantal elementen van $S \setminus (S_1 \cup S_2 \cup \dots \cup S_N)$.

Bewijs: Een element van S dat in géén der S_i ligt draagt in bovenstaande telling 1 bij tot de eerste term en verder niet. Een element van S dat in precies k ($k \geq 1$) deelverzamelingen S_i ligt geeft als bijdrage

$$1 - k + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^k \binom{k}{k} = (1-1)^k = 0 \quad .$$

Nemen we als voorbeeld $S = \{1,2,\ldots,n\}$ waarin $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ en kiezen we voor S_i de deelverzameling van S bestaande uit alle door p_i deelbare getallen dan is volgens (1.11) en (1.17)

$$\varphi(n) = n - \sum_{i=1}^{k} \frac{n}{p_i} + \Sigma_{1 \leq i < j \leq k} \frac{n}{p_i p_j} + \ldots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k}$$

$$= n \Pi_{p|n} \left(1 - \frac{1}{p}\right)$$

hetgeen in (1.15) langs andere weg is aangetoond. We kunnen de hierboven gevonden uitdrukking voor $\varphi(n)$ ook schrijven als

$$\varphi(n) = n \Sigma_{d|n} \frac{\mu(d)}{d}$$

als we definiëren

(1.18) Definitie: De functie van Möbius, aangegeven met μ, is voor natuurlijke n gedefinieerd door

$$\mu(n) := \begin{cases} 1 & \text{als } n = 1, \\ (-1)^i & \text{als n het product is van i verschillende priemfactoren,} \\ 0 & \text{anders (dus als n door het kwadraat van een priemgetal deelbaar is).} \end{cases}$$

Evenals in (1.16) gaan we na wat de som van $\mu(d)$ over alle delers d van n is. Het resultaat is verrassend:

(1.19) Stelling: $$\Sigma_{d|n} \mu(d) = \begin{cases} 1 \text{ als } n = 1, \\ 0 \text{ als } n > 1. \end{cases}$$

Bewijs: Voor $n = 1$ is het triviaal. Als $n > 1$ dan $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Dan heeft n precies $\binom{k}{i}$ delers die product zijn van i verschillende priemfactoren. Dus is

$$\Sigma_{d|n} \mu(d) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0 \quad .$$

De stellingen (1.16) en (1.19) zijn speciale gevallen van een situatie die zich vaker voordoet. Het gaat daarbij om de bepaling van een functie f zo dat $\Sigma_{d|n} f(d)$ gelijk is aan een voorgeschreven functie. Dit probleem is dankzij (1.19) eenvoudig op te lossen:

(1.20) Stelling: Zij f een functie gedefinieerd op de natuurlijke getallen en zij

$$F(n) := \Sigma_{d|n} f(d) \quad .$$

Dan is

$$f(n) = \Sigma_{d|n} \mu(d) F\left(\frac{n}{d}\right) \quad . \qquad \text{(Omkeerformule van Möbius.)}$$

Bewijs: $\Sigma_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \Sigma_{d|n} \left(\mu(d) \Sigma_{m|\frac{n}{d}} f(m) \right) =$

$$= \Sigma_{m|n} \left(f(m) \Sigma_{d|\frac{n}{m}} \mu(d) \right) = f(n)$$

volgens (1.19).

We keren terug naar de bestudering van congruenties. Van de vergelijkingen van het type "bepaal x (mod m) zó dat $f(x) \equiv 0 \pmod m$" is de lineaire congruentie $ax \equiv b \pmod m$ de eenvoudigste. Deze komt neer op het bepalen van gehele x en y zó dat $ax - my = b$. Het is duidelijk dat dit niet kan als (a,m) niet een deler van b is. Is dit wel het geval dan delen we door (a,m). We hebben dan een vergelijking $px - qy = r$ op te lossen met $(p,q) = 1$, anders geschreven $px \equiv r \pmod q$. Volgens (1.10) heeft deze congruentie precies één oplossing mod q. Daarmee is aangetoond:

(1.21) Stelling: De congruentie $ax \equiv b \pmod m$ heeft een oplossing dan en slechts dan als $(a,m) \mid b$. Het aantal oplossingen mod m is dan (a,m).

Voorbeeld: Los op: $34x \equiv 60 \pmod{98}$.

Oplossing: Daar $(34,98) = 2$ en $2 \mid 60$ heeft de congruentie 2 oplossingen mod 98. We vinden die door $17x \equiv 30 \pmod{49}$ op te lossen. We moeten een gehele y vinden en een gehele x zo dat

$$17x - 49y = 30 \quad \text{of} \quad x = 3y + 2 - \frac{2y+4}{17} \quad .$$

We zien onmiddellijk dat $y = -2$ een oplossing geeft nl. $x = -4$.

De gevraagde oplossingen zijn $\begin{cases} x \equiv -4 \pmod{98}, \\ x \equiv 45 \pmod{98}. \end{cases}$

Ons volgende probleem is de bepaling van een x die aan verschillende congruenties tegelijk voldoet. Een noodzakelijke en voldoende voorwaarde voor de oplosbaarheid van een dergelijk stelsel congruenties is bekend onder de naam Chinese reststelling (voor het eerst vermeld in een boek van Sun-Tsŭ, omstreeks het begin van onze jaartelling):

(1.22) Stelling: Het stelsel $x \equiv c_i \pmod{m_i}$ $(i = 1,2,\ldots,n)$ heeft een oplossing dan en slechts dan als voor ieder paar i,j geldt $(m_i,m_j) \mid (c_i - c_j)$. De oplossing is dan éénduidig $\bmod[m_1,m_2,\ldots,m_n]$.

Bewijs: a) Dat de voorwaarde noodzakelijk is is triviaal daar uit $x \equiv c_i \pmod{m_i}$ en $x \equiv c_j \pmod{m_j}$ volgt dat $c_i - c_j \equiv 0 \pmod{(m_i,m_j)}$.

b) Dat de voorwaarde voldoende is bewijzen we voor $n = 2$. Met volledige inductie is dan de stelling voor grotere n te bewijzen. Schrijf $x = c_1 + m_1 t$. Dan is $x \equiv c_1 \pmod{m_1}$. De vraag is of t zó gekozen kan worden dat

$$c_1 + m_1 t \equiv c_2 \pmod{m_2},$$

d.w.z.

$$m_1 t \equiv c_2 - c_1 \pmod{m_2}.$$

Volgens (1.21) is er precies één t $\bmod \frac{m_2}{(m_1,m_2)}$ die de gevraagde eigenschap heeft. Dus is het gegeven stelsel op te lossen en x is éénduidig bepaald $\bmod \frac{m_1 m_2}{(m_1,m_2)}$ d.w.z. $\bmod[m_1,m_2]$.

Als voorbeeld behandelen we een speciaal geval nl. een stelsel congruenties $x \equiv c_i \pmod{m_i}$ $(i = 1,2,\ldots,n)$ waarvoor $(m_i,m_j) = 1$ voor alle paren i,j met $i \neq j$. Ongeacht de keuze van de getallen c_i is dan aan de voorwaarde van (1.22) voldaan. Het stelsel heeft volgens (1.22) precies één oplossing $\bmod m_1 m_2 \ldots m_n$. Daar $\left(m_i, \frac{m_1 m_2 \ldots m_n}{m_i}\right) = 1$ is er een getal a_i zó dat

$\frac{m_1 m_2 \ldots m_n}{m_i} a_i \equiv 1 \pmod{m_i}$. Definieer $r_i = \frac{m_1 m_2 \ldots m_n}{m_i} a_i$. Dan is $x = \sum_{i=1}^{n} c_i r_i$ de oplossing van het gegeven stelsel. Dit is onmiddellijk duidelijk als we bedenken dat $r_i \equiv 0 \pmod{m_j}$ als $j \neq i$ en $r_i \equiv 1 \pmod{m_i}$.

Voorbeeld: Los op het stelsel $\begin{cases} x \equiv \alpha \pmod 2, \\ x \equiv \beta \pmod 3, \\ x \equiv \gamma \pmod 5. \end{cases}$

Oplossing: We lossen eerst de volgende drie congruenties op

$$15a_1 \equiv 1 \pmod 2 ,$$
$$10a_2 \equiv 1 \pmod 3 ,$$
$$6a_3 \equiv 1 \pmod 5 .$$

De oplossing is $a_1 = a_2 = a_3 = 1$. Dan is

$$x = 15\alpha + 10\beta + 6\gamma$$

de oplossing van het gegeven stelsel.

De nu volgende niet lineaire congruenties zijn zeer bekend. We zullen vele toepassingen van deze stellingen tegenkomen.

(1.23) Stelling: Als p een priemgetal is, $p \nmid a$, dan is $a^{p-1} \equiv 1 \pmod p$. (Stelling van Fermat.)

(1.24) Stelling. Als $(a,m) = 1$ dan is $a^{\varphi(m)} \equiv 1 \pmod m$. (Stelling van Euler.)

Bewijs: We merken op dat (1.23) een speciaal geval is van (1.24). Laat $c_1, c_2, \ldots, c_{\varphi(m)}$ een gereduceerd restsysteem mod m zijn. Dan is $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ ook een gereduceerd restsysteem (1.12). Volgens (1.8) is dan

$$\prod_{i=1}^{\varphi(m)} (ac_i) \equiv \prod_{i=1}^{\varphi(m)} c_i \pmod m$$

en daar $(m, \prod_{i=1}^{\varphi(m)} c_i) = 1$ volgt het gestelde m.b.v. (1.9).

Men noemt (1.24) wel de stelling van Euler-Fermat. Deze stelling zegt dat als $(a,m) = 1$ de resten van $1, a, a^2, a^3, \ldots$ bij deling door m een rij vormen die periodiek is met periode $\varphi(m)$. De kleinste periode t van deze rij is

dus een deler van $\varphi(m)$. Dit getal t heet orde van a (mod m) en we schrijven dit als $t = \text{ord}_m a$. Als voor a geldt $\text{ord}_m a = \varphi(m)$ dan heet a een primitieve wortel van m. Primitieve wortels zijn nuttig omdat uit $\text{ord}_m a = \varphi(m)$ volgt dat $1, a, a^2, \ldots, a^{\varphi(m)-1}$ een gereduceerd restsysteem vormen. Deze eenvoudige representatie van een gereduceerd restsysteem maakt vermenigvuldigen binnen het restsysteem gemakkelijk.

Voorbeeld: $\varphi(12) = 4$. Een gerduceerd restsysteem is 1,5,7,11. Nu is $1^1 \equiv 1 \pmod{12}$ en $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$. Dus heeft 12 géén primitieve wortel. Het getal 10 heeft wel een primitieve wortel, bv. 3, d.w.z. 1,3,9,27 is een gereduceerd restsysteem mod 10.

Als laatste congruentie beschouwen we $x^2 \equiv a \pmod{p}$ waarbij $p \nmid a$. Heeft deze een oplossing dan noemen we a een kwadraatrest mod p. We zien dat van de getallen $1, 2, \ldots, p-1$ (een gereduceerd restsysteem) de helft kwadraatresten zijn. Als c een primitieve wortel van p is dan zijn de even machten van c (mod p) de kwadraatresten, de oneven machten zijn de niet-resten. De congruentie $x^2 \equiv a \pmod{p}$ heeft één oplossing als $a \equiv 0$, twee als a een kwadraatrest is en anders geen oplossing.

Als afsluiting van dit hoofdstuk over getaltheorie beschouwen we een aantal representaties van natuurlijke getallen.

a) De gebruikelijke voorstelling is die in het 10-tallig stelsel. Daarin schrijven we $n = a_1 a_2 a_3 \ldots a_k$ als afkorting voor $n = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \ldots + a_k$. Hierin is $0 \leq a_i \leq 9$ voor iedere i.

b) Analoog aan de vorige voorstelling is de binaire representatie waarbij het getal 2 de rol speelt die 10 had. Ieder natuurlijk getal is éénduidig de schrijven als $\Sigma\, \varepsilon_i \cdot 2^i$ waarbij iedere $\varepsilon_i = 0$ of 1. Dit is de gebruikelijke voorstelling in rekenmachines.

c) In het begin van dit hoofdstuk hebben we de voorstelling $n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ leren kennen. Deze kunnen we afkorten door alleen de exponenten te geven t/m de laatste die niet 0 is. Zo stelt dan (0,1,1,2) het getal $735 = 3.5.7^2$ voor.

d) Uit (1.22) zien we dat alle getallen $< m_1 m_2 \ldots m_n$ eenduidig worden gerepresenteerd door hun resten mod $m_1, \ldots,$ mod m_n. Kiezen we bijvoorbeeld 2,3,5,7,11,13 en 17 als moduli dan is

$$375 = (1,0,0,4,1,11,1) \quad \text{en} \quad 243 = (1,0,3,5,1,9,5) \quad .$$

Met deze voorstelling zijn bewerkingen als optelling en vermenigvuldiging zeer eenvoudig omdat iedere plaats afzonderlijk wordt behandeld (d.w.z. er is géén "onthouden" nodig). Zo is $375 \times 243 = (1,0,0,6,1,8,5)$. Van dit principe is gebruik gemaakt door A. Svoboda om een rekenmachine te construeren met snelle vermenigvuldiging. Als de getallen binair zijn gerepresenteerd kan men voor de m_i getallen $2^n \pm 1$ nemen. De bepaling van de resten mod m_i is dan eenvoudig. Om later van de voorstelling door resten naar de binaire terug te keren gaat men te werk als in het voorbeeld na (1.22)

e) In combinatorische problemen is de volgende voorstelling soms nuttig:

$$n = a_1 \cdot 1! + a_2 \cdot 2! + a_3 \cdot 3! + \ldots \quad (0 \leq a_i \leq i,\ i = 1,2,\ldots) .$$

Ook deze voorstelling is eenduidig. We korten weer af tot $n = (a_1,a_2,\ldots)$. Zo is $1000 = (0,2,2,1,2,1)$. Om een voorbeeld te geven van deze voorstelling beschouwen we een lijst van alle permutaties van de symbolen 1,2,3, 4,5,6,7 opgeschreven in lexicografische volgorde. We nummeren deze permutaties van 0 tot en met $7! - 1$. De permutatie met nummer 1000 (dat is de 1001-ste van de lijst) is met bovenstaande voorstelling direct aan te geven. Daar het laatste cijfer in de voorstelling van 1000 een 1 is en de lijst begint met 6! permutaties die met een 1 beginnen, dan 6! permutaties die met een 2 beginnen enz., zien we dat de gezochte met een 2 begint. Zo verder gaande vinden we de permutatie 2,4,3,6,7,1,5. Deze methode wordt gebruikt voor het genereren van random-permutaties.

Hoofdstuk II. Algebra

We beschouwen verzamelingen V waarop een bewerking is gedefinieerd, dat is een voorschrift dat aan ieder geordend paar elementen (a,b) van V een element van V toevoegt. We schrijven het aan (a,b) toegevoegde element vaak als ab of a+b en spreken van product resp. som van a en b.

(2.1) Definitie: Een verzameling met productoperatie (G,) heet een groep als:

$$G1: \forall_{a\in G}\,\forall_{b\in G}\,\forall_{c\in G}\,[(ab)c = a(bc)] \quad ,$$

$$G2: \exists_{e\in G}\,\forall_{a\in G}\,[ae = ea = a] \quad ,$$

$$G3: \forall_{a\in G}\,\exists_{b\in G}\,[ab = ba = e] \quad .$$

Het element e heet de eenheid. Als we de bewerking aanduiden met + spreken we van een additieve groep. We schrijven dan i.p.v. e meestal 0 en noemen dit het nulelement. Het is eenvoudig in te zien dat er bij iedere a precies één b is met ab = e. We schrijven vaak $b = a^{-1}$. Als de groep additief geschreven wordt dan noemen we dit element b de tegengestelde en schrijven (-a).

(2.2) Definitie: Een groep (G,) heet abels of commutatief als

$$\forall_{a\in G}\,\forall_{b\in G}\,[ab = ba] \quad .$$

(2.3) Definitie: Is (G,) een groep en H ⊂ G en (H,) een groep dan noemen we (H,) een ondergroep van (G,).

(2.4) Definitie: Is (G,) een groep en het aantal elementen van G eindig dan noemen we dit aantal de orde van de groep.

Voorbeelden: a) $(R\ell,+)$ is een (additieve) groep.

b) $(R\ell\setminus\{0\},\ )$ is een (multiplicatieve) groep.

c) $(Gh,+)$ is een groep. Deze groep is een ondergroep van $(R\ell,+)$.

d) De matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ met $ad - bc \neq 0$ en vermenigvuldiging als bewerking vormen een groep. Hierin is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ de eenheid. Deze groep is niet abels.

e) De gehele getallen mod m met optelling als bewerking vormen een groep. De orde van deze groep is m.

f) De vectorruimte R_n met optelling als bewerking is een groep. In R_3 is iedere R_2 een ondergroep.

g) Het gereduceerde restklassensysteem mod 10, bestaande uit 1, 3, 7 en 9, met vermenigvuldiging mod 10 als bewerking is een groep. De orde van de groep is 4. De vermenigvuldigingsregels kunnen in een tabel worden aangegeven:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

h) Zij (G,) een groep. De eenheid schrijven we als 1. Als $a \in G$ dan ook $a^2, a^3, \ldots$. Als in deze rij een element meer dan één keer voorkomt is er een kleinste n waarvoor $a^n = 1$ (de rij is periodiek). Dan vormen $1, a, a^2, \ldots, a^{n-1}$ een ondergroep van (G,). Is dit (G,) zelf dan noemen we (G,) een cyclische groep van de orde n.
Het in f) genoemde voorbeeld is een cyclische groep van de orde 4. We noemen a (in het voorbeeld f) kunnen we hiervoor 3 nemen) een voortbrenger van de groep.

(2.5) Definitie: Als (G,) een groep is, $a \in G$, dan heet de kleinste positieve n waarvoor $a^n = 1$ (1 is de eenheid van de groep) de orde van het element a.

Voorbeeld: 1,2,4,7,8,11,13,14 is een gereduceerd restklassensysteem mod 15. Als we vermenigvuldiging mod 15 als bewerking nemen dan is dit een groep (van de orde 8). Deze groep is niet cyclisch omdat voor alle elementen a geldt $a^4 = 1$ (d.w.z. 15 heeft geen primitieve wortel). De groep heeft een aantal cyclische ondergroepen zoals bv. $(1, 7, 7^2 = 4, 7^3 = 13)$ en $(1, 11)$.

(2.6) Definitie: Een verzameling met twee bewerkingen (R, +,) heet een ring als

R1: (R, +) is een abelse groep ,

R2: $\forall_{a \in R} \forall_{b \in R} \forall_{c \in R} [a(bc) = (ab)c]$,

$$R3: \ \forall_{a\in R}\ \forall_{b\in R}\ \forall_{c\in R}\ [a(b+c) = ab+ac] \quad \text{en}$$

$$\forall_{a\in R}\ \forall_{b\in R}\ \forall_{c\in R}\ [(a+b)c = ac+bc] \quad .$$

(2.7) Definitie: $(R,+,\ )$ heet commutatieve ring als

$$\forall_{a\in R}\ \forall_{b\in R}\ [ab = ba] \quad .$$

We noemen $(R,+)$ de additieve groep van de ring.

(2.8) Definitie: Is $(R,+,\ )$ een ring en $S \subset R$, dan heet S een ideaal in de ring als

$$\forall_{a\in S}\ \forall_{b\in S}\ [a-b \in S] \quad \text{en}$$

$$\forall_{a\in S}\ \forall_{b\in R}\ [ab \in S \ \&\ ba \in S] \quad .$$

Het ideaal heet echt als S een echte deelverzameling van R is.

(2.9) Definitie: Een lichaam is een ring $(R,+,\ )$ waarvoor $(R\setminus\{0\},\ )$ een abelse groep is. (Als we "abels" weglaten dan spreken we van een scheef lichaam.) (In engelse literatuur: field.)

Voorbeelden: a) $(R\ell,+,\ )$ is een lichaam.

b) $(Gh,+,\ )$ is een (commutatieve) ring.

c) De 3-vouden vormen een ideaal in $(Gh,+,\ )$.

d) De verzameling van alle polynomen met gehele coëfficiënten met optelling en vermenigvuldiging als bewerkingen is een ring.

e) $(Gh \bmod m,+,\ )$ is een ring. Als m een priemgetal is dan is het een lichaam. Voor $m = 2$ hebben we een lichaam met 2 elementen (het kleinste lichaam).

Zij $(G,\ )$ een abelse groep, $(H,\ )$ een ondergroep. De verzamelingen $\{ah \mid h \in H\}$ heten nevenklassen van H. Twee nevenklassen van H zijn disjunct of identiek. Alle producten van elementen uit de nevenklasse aH met elementen uit bH behoren tot éénzelfde nevenklasse, namelijk de nevenklasse abH. We kunnen dus een vermenigvuldiging van nevenklassen definiëren door abH het product van aH en bH te noemen. De nevenklassen vormen dan een groep met H, de nevenklasse van e, als eenheid. Deze groep wordt met G/H aangegeven en heet factorgroep van G naar H.

Voorbeelden: a) $(Gh,+)$ met ondergroep H bestaande uit alle 5-vouden. Er zijn 5 nevenklassen namelijk $0+H$, $1+H$, $2+H$, $3+H$, $4+H$. De factorgroep is de groep $(Gh \bmod 5,+)$.

b) In het eerder gegeven voorbeeld van het gereduceerde restklassensysteem mod 15 met $H = (1,4,7,13)$ als ondergroep, is er naast H nog één nevenklasse, bestaande uit 2, 8, 11 en 14. De factorgroep is de cyclische groep van de orde 2.

Is S een ideaal in de ring $(R,+,\ )$ dan is $(S,+)$ een ondergroep van de additieve groep $(R,+)$. We kunnen hier weer de factorgroep beschouwen. De nevenklassen noemen we restklassen mod S. Voor deze restklassen kunnen we naast de optelling ook vermenigvuldiging definiëren op analoge wijze. Het is eenvoudig na te gaan dat $(R/S,+,\ )$ een ring is. We noemen dit de quotiëntring of restklassenring mod S. Van deze methode hebben we al voorbeelden gezien waaraan ook de gebruikte namen ontleend zijn.

(2.10) Stelling: Als p een priemgetal is dan is $(Gh \bmod p,+,\ )$ een lichaam.

Bewijs: We weten reeds dat we met een commutatieve ring te maken hebben. Is $a \not\equiv 0$ een element van deze ring, dan is $(a,p) = 1$ en dus is er een x met $ax \equiv 1 \pmod p$ volgens (1.21). Dit wil zeggen dat $(Gh \bmod p\setminus\{0\},\ )$ een abelse groep is, hetgeen we moesten bewijzen.

We noemen deze lichamen priemlichamen. Als n niet een priemgetal is dan is de ring $(Gh \bmod n,+,\ )$ geen lichaam.

Eindige lichamen, d.w.z. lichamen met eindig veel elementen, zijn het eerst bestudeerd door Galois en worden daarom ook Galois lichamen genoemd (engels: Galois fields) en aangegeven als GF(n) (Galois lichaam met n elementen). Laat $(K,+,\ )$ een eindig lichaam zijn. De eenheid noemen we 1. Het element $1+1$ noemen we 2, $2+1$ noemen we 3, enz. Daar het lichaam eindig is vormen deze veelvouden van 1 een eindige cyclische ondergroep van $(K,+,\ )$. Dit is zelfs een lichaam en wel een priemlichaam. Het lichaam K bevat dus een priemlichaam GF(p) als deellichaam. We beschouwen nu in K een maximaal stelsel lineair onafhankelijke elementen (t.o.v. GF(p)) d.w.z. elementen $x_1, x_2, \ldots, x_m$ uit K zó dat $c_1x_1 + c_2x_2 + \ldots + c_mx_m$ $(0 \leq c_i < p)$ alleen 0 is als alle $c_i = 0$ zijn. Ieder element van K is eenduidig te schrijven als lineaire combinatie van x_1 t/m x_m met coëfficiënten uit GF(p). Met $x_1, x_2, \ldots, x_m$ als basisvectoren is K een vectorruimte van dimensie m over het lichaam GF(p). We hebben hiermee bewezen:

(2.11) Stelling: Het aantal elementen van een eindig lichaam is een macht van een priemgetal.

We delen hier zonder bewijs mee dat er slechts één lichaam is met p elementen. We geven het zoals eerder reeds gezegd is aan met $GF(p^m)$. (Iets beter gezegd: twee lichamen met evenveel elementen zijn isomorf.) Voor een grondige behandeling van Galois lichamen verwijzen we naar: B.L. van der Waerden, Algebra. We volstaan hier met het vermelden van enige stellingen (zonder bewijs) en enige voorbeelden.

(2.12) Stelling. Alle elementen $\neq 0$ van $GF(q)$ zijn machten van één zelfde element (primitief element), d.w.z. de multiplicatieve groep van $GF(q)$ is cyclisch (van de orde $q-1$).

We geven nu een methode om $GF(p^m)$ te construeren. Laat f een polynoom zijn van de graad m met coëfficiënten in GF(p) en laat f irreducibel zijn (f is niet het product van 2 polynomen van lagere graad met coëfficiënten in GF(p)). Alle polynomen met coëfficiënten in GF(p) vormen een ring $(R,+,\ )$. De veelvouden van f vormen een ideaal S in R. De restklassenring R/S is op te vatten als de verzameling polynomen $c_0 + c_1x + \ldots + c_{m-1}x^{m-1}$ $(0 \leq c_i < p)$ met optelling en vermenigvuldiging mod p èn mod f(x). Als g(x) een element van R/S is en c(x) doorloopt R/S dan doorloopt ook g(x)c(x) de hele restklassenring daar $g(x)c_1(x) \equiv g(x)c_2(x)$ zou impliceren dat $g(x)\{c_1(x) - c_2(x)\} = r(x)f(x)$ en dit kan niet als f irreducibel is. Uit bovenstaande volgt dat er bij iedere g(x) in R/S een c(x) is zó dat $g(x)c(x) = 1$, m.a.w. R/S is een lichaam. Dit is het lichaam $GF(p^m)$.

Het volgende voorbeeld illustreert deze methode en tevens stelling (2.12). We construeren $GF(2^4)$ door uit te gaan van een primitief element x dat voldoet aan $x^4 + x + 1 = 0$ (dan is $x^{15} = 1$):

$$
\begin{aligned}
0 &= (0\ 0\ 0\ 0)\\
x^0 &= 1 = (1\ 0\ 0\ 0)\\
x^1 &= x = (0\ 1\ 0\ 0)\\
x^2 &= x^2 = (0\ 0\ 1\ 0)\\
x^3 &= x^3 = (0\ 0\ 0\ 1)\\
x^4 &= 1 + x = (1\ 1\ 0\ 0)\\
x^5 &= x + x^2 = (0\ 1\ 1\ 0)\\
x^6 &= x^2 + x^3 = (0\ 0\ 1\ 1)\\
x^7 &= 1 + x + x^3 = (1\ 1\ 0\ 1)\\
x^8 &= 1 + x^2 = (1\ 0\ 1\ 0)\\
x^9 &= x + x^3 = (0\ 1\ 0\ 1)\\
x^{10} &= 1 + x + x^2 = (1\ 1\ 1\ 0)\\
x^{11} &= x + x^2 + x^3 = (0\ 1\ 1\ 1)\\
x^{12} &= 1 + x + x^2 + x^3 = (1\ 1\ 1\ 1)\\
x^{13} &= 1 + x^2 + x^3 = (1\ 0\ 1\ 1)\\
x^{14} &= 1 + x^3 = (1\ 0\ 0\ 1)
\end{aligned}
$$

De representatie als machten van x geeft de structuur van de multiplicatieve groep van $GF(2^4)$ en de representatie als vectoren (4-dimensionale vectorruimte over $GF(2)$) geeft de structuur van de additieve groep.

We merken nog op dat we analoog aan het bovenstaande een vectorruimte kunnen maken van de n-tallen $(a_1, a_2, \ldots, a_n)$ waarbij alle a_i uit een lichaam K gekozen zijn. Dit heet een n-dimensionale vectorruimte over het lichaam K.

Als oefening kan men $GF(3^3)$ construeren door bovenstaande constructie uit te voeren m.b.v. een polynoom $x^3 + ax^2 + bx + c$ dat deler is van $x^{13} + 1$. Als we dan de machten van x schrijven als lineaire combinatie van 1, x en x^2 met coëfficiënten uit $GF(3)$, dan is x^{26} de kleinste macht die = 1 is, d.w.z. we vinden voor de multiplicatieve groep x als voortbrenger (x is primitief element).

Hoofdstuk II. Coding Theory

In dit hoofdstuk zijn we geïnteresseerd in vergroting van de nauwkeurigheid bij transport van informatie over diverse kanalen. Men denke bijvoorbeeld aan een gesprek over een telefoonlijn, communicatie met rekenmachines, opdrachten voor apparatuur in satellieten, informatie afkomstig van magneetbanden etc.

Er zijn 2 mogelijke manieren van aanpak. De eerste is technisch, nl. verbetering van de apparatuur waardoor de kans op fouten geringer wordt. Dit is vaak duur en helpt niets voor bepaalde soorten fouten zoals vergissingen. Een andere manier is "coding" het onderwerp van dit hoofdstuk. Een idee van het principe krijgen we door aan een telefoongesprek te denken. De uitgezonden informatie komt gestoord aan (ruis (= noise) op de lijn etc.). Toch kan men in het algemeen wel verstaan wat gezegd is. De oorzaak hiervan is wat in informatie-theorie "redundancy" wordt genoemd, d.i. de overbodige informatie die door het kanaal loopt. Een goed verstaander heeft maar een half woord nodig! We kunnen het anders zeggen: als een woord niet al te verminkt aankomt, kan de ontvanger met grote kans op succes raden wat in werkelijkheid is uitgezonden. Moeilijkheden bij het verstaan treden op bij woorden die op elkaar lijken. In een goede "taal" moet men dit dus vermijden. Het probleem in coding theory is bij een gegeven aantal mogelijke mededelingen een code te bedenken die aan elk van deze een signaal toevoegt en een decodeermethode (+ apparatuur) die fouten in de ontvangen berichten ontdekt en verbetert en daarna de code terugvertaalt. We zijn voornamelijk geïnteresseerd in kanalen waarbij verzoek om herhaling niet mogelijk is (= one-way channels) hetgeen bij telefoongesprekken wel kan. Het gaat om "error-correcting codes" en niet "error-detecting codes". Hier moeten we nog onderscheid maken tussen incidentele toevallige fouten waarbij de kans op veel fouten vlak bij elkaar dus klein is en ophopingen van fouten zoals dat bijvoorbeeld voorkomt bij blikseminslag tijdens een telefoongesprek. Fouten in magneetbanden komen ook in series voor. Men spreekt in dat geval van "burst-error correction".

Laten we ons eerst beperken tot zgn. binaire kanalen. In dat geval zijn 2 signalen mogelijk die we door 0 en 1 representeren. We spreken van een binair symmetrisch kanaal als voor elk der signalen de kans p is dat het andere signaal ontvangen wordt. Een ander veel bestudeerd voorbeeld is het zogenaamde "binary erasure channel" waarbij voor elk der signalen de kans p is dat géén signaal ontvangen wordt terwijl de kans 1 - p is dat het goede signaal ontvangen wordt.

Een eerste voorbeeld van een code is het volgende. Stel dat er 4 mogelijke mededelingen via het kanaal verzonden moeten worden. In principe zijn de series signalen 00, 01, 10 en 11 hiervoor voldoende maar dan mogen geen fouten gemaakt worden. We kunnen nu echter de volgende 4 series signalen kiezen: 11000, 00110, 10011 en 01101. We noemen dit woorden. De ontvanger heeft een woordenboek waar alle codewoorden in staan met voor elk woord een lijst van ontvangen woorden die vertaald moeten worden in dat codewoord. Deze vertaling berust, als we niet met burst errors te maken hebben, op het principe dat de kans op veel fouten kleiner is dan de kans op weinig fouten (maximum likelihood decoding). Wordt dus 11001 ontvangen dan neemt men aan dat het woord 11000 is uitgezonden. Als het woord 01010 ontvangen wordt gaan we na op hoeveel plaatsen het van codewoorden verschilt. Dit aantal noemt men de afstand van de woorden (= Hamming distance; merk op dat alle woorden van gegeven lengte met deze afstandsfunctie een metrische ruimte vormen). Nu blijkt dat 01010 afstand 2 heeft tot de eerste twee codewoorden, afstand 3 tot de laatste 2. Hier moeten we een keuze maken hoe we decoderen. In dit voorbeeld worden alle ontvangen woorden die ten hoogste één fout bevatten goed vertaald. We spreken van een single error-correcting code. Als een code zo geconstrueerd is dat elk tweetal codewoorden afstand ≥ 4 heeft, dan kan men woorden met één fout goed decoderen en tevens van woorden met twee fouten vaststellen dat er meer dan één fout is gemaakt. We spreken van een double error detecting code.

We merken op dat het gegeven voorbeeld behoort tot de codes die block codes heten, dat zijn codes waarin alle woorden n-tupels van signalen zijn. Het is duidelijk dat een goede code uit lange woorden zal bestaan. Dit betekent dat het werken met een woordenboek ondoenlijk is. Het probleem dat we moeten oplossen is het construeren van codes die zó veel regelmaat vertonen dat het decoderen systematisch kan gebeuren. Men moet daarbij in gedachten houden dat een practische realisatie geconstrueerd moet kunnen worden.

De stelling van Shannon (speciaal geval)

We geven nu een idee van de grote mogelijkheden van coding door een voorbeeld (van D. Slepian). We hebben een binair symmetrisch kanaal ter beschikking met kans p dat een symbool verkeerd wordt ontvangen en kans $q = 1 - p$ dat het goed aankomt. Via dit kanaal willen we de resultaten overbrengen van een experiment waarbij met constante snelheid met een munt kruis of munt wordt geworpen. Stel dat we over het kanaal met twee keer zo grote snelheid symbolen kunnen overbrengen. Als we niet aan deze snelheden gebonden

waren zouden we voor een overbrenging met willekeurig grote nauwkeurigheid kunnen zorgen en wel als volgt. Bij de worp kruis zenden we N keer een 1 over het kanaal, bij munt N keer een 0. De ontvanger vertaalt een serie van N signalen in kruis als meer dan de helft van de signalen 1 is. Neem nu als voorbeeld p = 0,001. De kans dat de ontvanger verkeerd decodeert is dan

$$\sum_{k=0}^{N/2} \binom{N}{k} q^k p^{N-k} < (0,07)^N$$

en deze kans heeft limiet 0 voor $N \to \infty$.

Nu we aan de gegeven snelheden gebonden zijn is de zaak veel lastiger. Ieder symbool 2 keer zenden heeft geen zin! De fundamentele stelling van Shannon uit de informatie-theorie zegt dat ondanks deze beperking toch willekeurig grote nauwkeurigheid is te bereiken. Een eerste idee over de methode krijgen we door aan ieder paar worpen een signaal van 4 symbolen te verbinden op de volgende manier:

munt - munt → 0000
kruis - munt → 1001
munt - kruis → 0111
kruis - kruis → 1110 .

Als een ander woord ontvangen wordt nemen we aan dat op één van de eerste drie plaatsen een fout is gemaakt. De kans op verkeerd overkomen van het resultaat van twee worpen is nu ongeveer 0,001 terwijl bij gewoon zenden deze kans 0,002 is. Nog groter nauwkeurigheid bereiken we door aan iedere serie van 3 worpen een signaal van 6 symbolen toe te voegen enz.

We geven nu het bewijs (van E.N. Gilbert) van de stelling van Shannon voor dit speciale voorbeeld. We stellen het probleem eerst precies:

a) Er is een $\varepsilon > 0$ gegeven.

b) We willen aan iedere serie van s worpen een signaal van $n = 2s$ symbolen toevoegen zó dat bij het zenden van elk van deze signalen en geschikte decodeerprocedure de kans op verkeerd decoderen $< \varepsilon$ is.

We construeren de signalen en het decodeervoorschrift zó dat deze kans inderdaad $< \varepsilon$ is. De constructie levert k van die signalen. We moeten dan aantonen dat voor grote n geldt: $k \geq 2^{\frac{1}{2}n} = 2^s$. Als met n symbolen, bij zekere code, k verschillende mededelingen kunnen worden gezonden over het kanaal noemt men $\frac{\log_2 k}{n}$ de <u>transmissiesnelheid</u>. Dit is een maat voor de hoeveelheid informatie per symbool. In ons voorbeeld moet deze snelheid ten-

minste $\frac{1}{2}$ zijn. (In dit bewijs schrijven we log i.p.v. $^2\log$.) Voor het bewijs zijn de volgende voorbereidingen nodig:

(1) We beschouwen woorden van n symbolen, dat zijn vectoren $\underline{x}$ met n componenten 0 of 1. We geven met $P(\underline{x};\underline{y})$ de kans aan dat bij zenden van $\underline{x}$ over het kanaal het woord $\underline{y}$ wordt ontvangen. Deze kans wordt bepaald door het aantal fouten. We merken op dat $P(\underline{x};\underline{y}) = P(\underline{y};\underline{x})$.

(2) De kans dat bij het zenden van een woord precies w fouten optreden bij ontvangst is

$$\binom{n}{w} p^w q^{n-w} \quad .$$

(3) Zij $b = \sqrt{\frac{2np(1-p)}{\varepsilon}}$. Daar voor ieder symbool de kans op verkeerd overkomen p is, is voor woorden van n symbolen het gemiddeld aantal fouten np met variantie $np(1-p)$. Volgens de ongelijkheid van Bienaymé-Chebyshev is

$$P(w > np + b) \leqslant \frac{\varepsilon}{2} \quad .$$

(4) Als $\underline{x}_i$ een woord is verstaan we onder de bol $B_i := B(\underline{x}_i, \rho)$ de verzameling woorden $\underline{y}$ waarvoor de Hamming-distance tot $\underline{x}_i$ niet groter dan ρ is. We nemen nu $\rho = np + b$. Als we dan een woord $\underline{x}_i$ zenden is volgens (3) de kans dat het ontvangen woord $\underline{y}$ buiten B_i ligt ten hoogste $\frac{\varepsilon}{2}$. Voor voldoend grote n geldt $np + b < \frac{1}{2}n$. Het aantal woorden in een bol $B(\underline{x}, \rho)$ is dan

$$\Sigma_{w \leqslant np+b} \binom{n}{w} < \tfrac{1}{2} n \binom{n}{\rho} \quad .$$

(5) $$1 = 1^n = \left[\frac{m}{n} + \left(1 - \frac{m}{n}\right)\right]^n \geqslant \binom{n}{m} \left(\frac{m}{n}\right)^m \left(1 - \frac{m}{n}\right)^{n-m} \quad .$$

Dus:

$$\binom{n}{m} \leqslant \frac{n^n}{m^m (n-m)^{n-m}} \quad .$$

(6) $$\log \frac{\rho}{n} = \log\left(p + \frac{b}{n}\right) = \log p + O(n^{-\frac{1}{2}}) \quad ,$$

dus $$\frac{\rho}{n} \log \frac{\rho}{n} = p \log p + O(n^{-\frac{1}{2}})$$

en analoog

$$\left(1 - \frac{\rho}{n}\right) \log\left(1 - \frac{\rho}{n}\right) = q \log q + O(n^{-\frac{1}{2}}) \quad .$$

Nu geven we de constructie van de codewoorden. We kiezen een eerste woord $\underline{x}_1$. Het decodeergebied R_1 is de bol B_1. De kans op verkeerd decoderen is $\leqslant \frac{\varepsilon}{2}$. Als $\underline{x}_1,\ldots,\underline{x}_{j-1}$ gekozen zijn kiezen we $\underline{x}_j$ buiten $R_1 \cup R_2 \cup \ldots \cup R_{j-1}$ en definiëren $R_j = B_j \setminus (R_1 \cup \ldots \cup R_{j-1})$ en eisen dat de kans op verkeerd decoderen $< \varepsilon$ is. Als we na het kiezen van $\underline{x}_1,\ldots,\underline{x}_k$ niet verder kunnen en $R = R_1 \cup \ldots \cup R_k$ dan is blijkbaar voor iedere $\underline{x} \notin R$ de kans dat we een $\underline{y} \in R$ ontvangen als we $\underline{x}$ zenden groter dan $\frac{\varepsilon}{2}$. (Anders zouden we immers $\underline{x}_{k+1} = \underline{x}$ kunnen kiezen.) Voor een $\underline{x} \in R$ is deze kans ook groter dan $\frac{\varepsilon}{2}$. Dus is $P(\underline{x} \in R) = \Sigma_{\underline{x}\in R,\underline{y}} P(\underline{x};\underline{y}) = \Sigma_{\underline{x}\in R,\underline{y}} P(\underline{y};\underline{x})$, dat is de kans dat het ontvangen signaal in R ligt. Deze is $\geqslant \frac{\varepsilon}{2}$. Is N het aantal woorden in R dan is dus $\frac{N}{2^n} \geqslant \frac{\varepsilon}{2}$. Volgens (4) en (5) is

$$N < k \cdot \tfrac{1}{2} n \binom{n}{\rho} \leqslant \tfrac{1}{2} kn \frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}} \quad .$$

Als we deze ongelijkheden combineren, de logarithme nemen en (6) toepassen vinden we

$$\frac{\log k}{n} \geqslant 1 + p \log p + q \log q + O(n^{-\frac{1}{2}}) \quad .$$

In ons voorbeeld is $p = 0{,}001$ en het rechterlid voor grote n dus $> 0{,}9$ terwijl we slechts moesten aantonen dat de transmissiesnelheid $\geqslant \frac{1}{2}$ bereikt kon worden! Het gestelde is hiermee bewezen.
(Opmerking: $-p \log p - q \log q$ noemt men in de informatietheorie entropie.)

Met dit voorbeeld is aangetoond dat codes bestaan die grote nauwkeurigheid garanderen. De constructie van de codes en de methode van decoderen is een andere zaak! We hebben gezien dat goede codes uit lange woorden bestaan. Het is dus van belang codes te construeren die veel regelmaat vertonen waardoor decoderen eenvoudig wordt en waardoor bewezen kan worden dat bepaalde fouten-verbeterende eigenschappen aanwezig zijn.

Lineaire codes (groep-codes)

Beschouw een kanaal waarvoor het aantal verschillende symbolen gelijk is aan q, waarin q een macht van een priemgetal is. De symbolen kunnen dan worden opgevat als elementen van GF(q). Vaak zullen we ons tot $q = 2$ beperken (symbolen 0 en 1). De verzameling n-tallen van dergelijke symbolen is een vectorruimte R over GF(q). Als een collectie n-tallen een k-dimensionale

lineaire deelruimte V van R vormt noemen we het een lineaire code en wel een (n,k) code. Het gewicht van een vector (= Hamming weight) is het aantal componenten $\neq 0$. Daar het verschil van 2 vectoren uit de code weer een codevector is, is de minimale afstand tussen vectoren van de code gelijk aan het minimale gewicht van de vectoren $\neq (0,0,\ldots,0)$ uit V.

We kunnen de code op de volgende 2 manieren beschrijven:

(a) Voortbrenger: We vormen een matrix G (k rijen, n kolommen) door k basisvectoren van V als rijen van G te nemen. Voor iedere $\underline{\alpha} = (\alpha_1,\alpha_2,\ldots,\alpha_k)$ met $\alpha_i \in GF(q)$ is $\underline{\alpha}G$ een codewoord (d.i. een vector uit V). De code bestaat uit q^k woorden. G heet voortbrenger van de code.

(b) Parity-check matrix: Alle vectoren uit R die loodrecht staan op iedere code vector vormen een lineaire deelruimte van R van dimensie n - k (orthogonale complement V' van V). We vormen een matrix H (n - k rijen, n kolommen) door n - k basisvectoren van V' als rijen van H te nemen. Voor iedere code vector $\underline{v}$ geldt $\underline{v}H^T = \underline{0}$. De code vectoren zijn de oplossingsruimte van n - k lineair onafhankelijke vergelijkingen $\sum_{j=1}^{n} v_j h_{ij} = 0$. In het binaire geval noemt men dit "parity checks" en H de parity-check matrix van de code. De woorden van V' vormen een code die we de duale van V noemen.

De eigenschappen van de code die ons interesseren veranderen niet als we de kolommen van de voortbrenger G permuteren. De codes die zo uit G ontstaan noemen we equivalent met de oorspronkelijke. Het is eenvoudig in te zien dat er bij een gegeven code een equivalente code is waarvan de matrix G de vorm $(I_k\ P)$ heeft waarin I_k de $k \times k$ eenheidsmatrix is en P een $k \times (n-k)$ matrix. De bijbehorende parity-check matrix is $(-P^T\ I_{n-k})$. Een codevector vinden we door $v_1,v_2,\ldots,v_k$ willekeurig te kiezen en $v_{k+j} = \sum_{i=1}^{k} v_i p_{ij}$ (voor $j = 1,2,\ldots,n-k$) te nemen. Het coderen is nu een eenvoudige zaak geworden! Men noemt v_1 t/m v_k information symbols, v_{k+1} t/m v_n parity-check symbols.

Een tabel voor het decoderen maken we als volgt. We merken op dat V een ondergroep is van R. Uit iedere nevenklasse van V kiezen we een representant en wel zo dat de kans op ontvangst van deze representant als $(0,0,\ldots,0)$ het gezonden signaal is maximaal is. Dat wil dus zeggen dat we uit iedere nevenklasse een element met minimaal gewicht kiezen. Schrijf in een rij, achter elkaar, de codewoorden $\underline{v}_1 = \underline{0}, \underline{v}_2,\ldots,\underline{v}_{qk}$. Schrijf onder $\underline{v}_1$ de gekozen representanten van de nevenklassen en achter zo'n representant in een rij

$\underline{v}+\underline{v}_2$, $\underline{v}+\underline{v}_3$, etc. Een ontvangen woord wordt vertaald in het codewoord waar het onder staat in dit schema. Als $\underline{u}$ wordt gezonden en $\underline{v}$ ontvangen dan is deze manier van decoderen goed als $\underline{v}-\underline{u}$ één van de gekozen representanten is.

Voorbeeld: Neem $q=3$, $n=4$, $k=2$. De ruimte R bestaat uit 81 vectoren, de code V uit 9 vectoren. Laat $(0,1,1,1)$ en $(1,0,1,2)$ een basis zijn van de 2-dimensionale deelruimte V. De voortbrenger G is $\begin{pmatrix}1&0&1&2\\0&1&1&1\end{pmatrix}$. Dit is de standaardvorm met I_2 voorop en $P = \begin{pmatrix}1&2\\1&1\end{pmatrix}$ daar achter. De parity-check vergelijkingen zijn

$$v_3 = v_1 + v_2 ,$$
$$v_4 = 2v_1 + v_2 .$$

De code V bestaat uit de woorden: $(0,0,0,0)$, $(0,1,1,1)$, $(0,2,2,2)$, $(1,0,1,2)$, $(2,0,2,1)$, $(1,1,2,0)$, $(2,1,0,2)$, $(1,2,0,1)$ en $(2,2,1,0)$. We zien dat alle woorden behalve $(0,0,0,0)$ gewicht 3 hebben. Dus hebben alle paren afstand 3. Deze code is dus een single-error-correcting code. Met de boven beschreven manier van decoderen zien we dit als volgt: twee verschillende vectoren met gewicht 1 hebben afstand 1 of 2 en liggen dus niet in dezelfde nevenklasse van V. Er zijn 8 zulke vectoren. Deze vormen samen met $(0,0,0,0)$ de 9 representanten van de nevenklasse van V. Ieder ontvangen signaal dat geen of één fout bevat wordt dan goed gedecodeerd. Zo'n code waarin alle woorden van gewicht $\leq m$ het representantensysteem vormen heet perfect.

De geschetste manier van decoderen heeft nog een groot voordeel. We hebben de boven beschreven tabel niet helemaal nodig maar alleen een lijst van alle codewoorden en alle representanten van nevenklassen met voor elk van deze representanten $\underline{v}$ ook de parity-check vector $\underline{v}H^T$. Als 2 vectoren tot dezelfde nevenklasse van V behoren is de parity-check vector van hun verschil $\underline{0}$ en omgekeerd. Als een signaal $\underline{v}$ ontvangen wordt bepalen we de parity-check vector, zoeken deze in de lijst en trekken de bijbehorende representant van $\underline{v}$ af.

Hamming codes

Beschouw een matrix H met m rijen en $2^m - 1$ kolommen waarvan de j-de kolom de binaire representatie van het getal j is. De som van 2 kolommen is niet 0 (mod 2) d.w.z. dat over GF(2) een lineaire combinatie van kolommen die 0 is uit tenminste 3 termen bestaat. Anders gezegd: iedere rijvector die loodrecht staat op elke rij van H heeft gewicht ≥ 3. Dus is H parity check matrix van een lineaire code V waarvan de codewoorden onderlinge afstand ≥ 3 hebben. Dit is dan een single-error-correcting code. Zulke codes heten binaire Hamming codes. Als we weer decoderen met behulp van representanten van nevenklassen van V merken we op dat vectoren met gewicht 1 in verschillende nevenklassen liggen. Er zijn $2^m - 1$ zulke vectoren. Samen met 0 zijn dit 2^m vectoren uit verschillende restklassen en daar er precies 2^m restklassen van V zijn hebben we hier met een perfecte code te maken. In deze code is de lengte van de woorden $n = 2^m - 1$, de dimensie van V is $k = 2^m - 1 - m$, d.w.z. er zijn $2^m - 1 - m$ information symbols en m parity-check symbols.

Het opsporen en verbeteren van één fout met deze code is bijzonder eenvoudig. Als de ontvangen vector $\underline{v}$ op de j-de plaats van de gezonden vector afwijkt is nl. $\underline{v}H^T$ de binaire representatie van het getal j.

We merken op dat de redenering waarmee aangetoond werd dat we een single-error-correcting code hadden geldig blijft als we uit H een aantal kolommen weglaten. We kunnen dus Hamming codes van willekeurige lengte maken.

Een andere modificatie is de volgende. Voeg aan ieder woord van een binaire Hamming code een parity-check symbol toe dat de som is van de voorafgaande symbolen. De nieuwe code heeft dan minimale afstand 4 en is dus een double-error-detecting code. Als we dit extra symbool voor de oude codewoorden zetten ziet de nieuwe parity-check matrix H^* er als volgt uit

$$H^* = \begin{pmatrix} 0 & & \\ \vdots & & \\ 0 & & H \\ 1 & 1 \ldots 1 & \end{pmatrix}$$

Hierin is H de oude parity-check matrix. Merk op dat de kolommen van H^* de binaire representatie van de oneven getallen $\leq 2^{m+1}$ zijn.

Een Hamming code over GF(q) wordt op analoge wijze geconstrueerd. Om er voor te zorgen dat H geen 2 kolommen bevat die lineair afhankelijk zijn, laten we alleen kolomvectoren toe waarvan het eerste symbool $\neq 0$ een 1 is.

Als voorbeeld beschouwen we GF(3) en nemen

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix} .$$

H is de parity-check matrix van een (13,10) code V. Dit is weer een single-error-correcting code. De code bestaat uit 3^{10} woorden. Als we elk van deze woorden als een kolom voorspellingen voor de voetbalpool insturen zijn we er zeker van de tweede prijs of de eerste te winnen. (Men moet dan wel *f* 15.000,- inzetten!)

Reed-Muller codes

Een klasse lineaire codes die de eigenschap hebben eenvoudig te decoderen te zijn is door D.E. Muller ontdekt en door I.S. Reed beschreven. We laten het idee hier aan de hand van een voorbeeld zien:
$\underline{v}_1$, $\underline{v}_2$ en $\underline{v}_3$ zijn de rijen van een matrix waarvan de 8 kolommen de binaire representatie van de getallen 0,1,...,7 zijn; $\underline{v}_0$ is de rijvector bestaande uit 8 elementen 1. We beschouwen nu vermenigvuldiging van vectoren coördinaatsgewijs en vinden dan

$$\begin{aligned} \underline{v}_0 &= (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \\ \underline{v}_1 &= (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \\ \underline{v}_2 &= (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \\ \underline{v}_3 &= (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \\ \underline{v}_1\underline{v}_2 &= (0\ 0\ 0\ 0\ 0\ 0\ 1\ 1) \\ \underline{v}_1\underline{v}_3 &= (0\ 0\ 0\ 0\ 0\ 1\ 0\ 1) \\ \underline{v}_2\underline{v}_3 &= (0\ 0\ 0\ 1\ 0\ 0\ 0\ 1) \\ \underline{v}_1\underline{v}_2\underline{v}_3 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 1) . \end{aligned}$$

Voor $\nu = 0,1,\ldots,7$ is er in dit schema een vector die met ν nullen begint. De vectoren zijn dus lineair onafhankelijk. Merk op dat alle vectoren behalve de laatste een even aantal elementen 1 hebben en dus loodrecht op zichzelf staan. Het product van een vector $\underline{v}$ met zichzelf is weer $\underline{v}$. Als we nu i.p.v. 8 kolommen 2^m kolommen nemen vinden we een schema met vectoren $\underline{v}_0, \underline{v}_1, \ldots, \underline{v}_m$ en dan $\binom{m}{2}$ producten $\underline{v}_i\underline{v}_j$, $\binom{m}{3}$ producten $\underline{v}_i\underline{v}_j\underline{v}_k$ etc. Als we alle producten van ten hoogste r factoren $\underline{v}_i$ als basis van een lineaire deelruimte van de n-dimensionale vectorruimte R over GF(2) nemen hebben we een (n,k) code met

$$n = 2^m \quad \text{en} \quad k = 1 + \binom{m}{1} + \ldots + \binom{m}{r} .$$

Dit is de Reed-Muller code van de orde r.

Als we een rij uit dit schema beschouwen die product is van $\leq r$ vectoren $\underline{v}_i$ en een andere rij die product is van $\leq m-r-1$ vectoren dan is het product van deze twee rijen weer een rij uit het schema en bovendien niet de laatste rij. Dit betekent dat deze twee rijen op een even aantal plaatsen beide een 1 hebben; anders gezegd: de rijen staan loodrecht op elkaar. Daar verder de dimensie van de code van de orde r en de dimensie van de code van de orde $m-r-1$ samen 2^m zijn hebben we nu aangetoond dat de code van de orde r en de code van de orde $m-r-1$ duaal zijn.

Merk op dat de reeds eerder genoemde Hamming single-error-correcting, double-error-detecting code blijkbaar een Reed-Muller code van de orde $m-2$ is.

Men kan zich gemakkelijk voorstellen dat de zeer speciale vorm van deze code het decoderen sterk vereenvoudigt. We gaan daar nu niet op in.

Product codes (Slepian)

(3.1) Definitie: Als A een $n \times m$-matrix is met elementen a_{ij} en B een $r \times s$-matrix, dan verstaan we onder het Kronecker-product $A \times B$ de $nr \times ms$-matrix van de vorm

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \dots & \dots & \dots & \dots \\ a_{n1}B & a_{n2}B & \dots & a_{nm}B \end{pmatrix}$$

Voorbeeld:

$$\begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 3 & 1 \\ 2 & 4 & 1 & 2 \\ 0 & 0 & -3 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix} .$$

Door van eenvoudige codes uit te gaan en de voortbrengers te vermenigvuldigen (Kronecker-product) kunnen we goede codes opbouwen. We laten dit weer aan de hand van een voorbeeld zien.

Zij

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

de voortbrenger van een (4,3) code over GF(2). Hier is één parity-check (4e coördinaat is de som van de vorige.) Deze code is single-error-detecting. Analoog voor

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

de voortbrenger van een (5,4) code. De matrix $G = G_1 \times G_2$ is een 12 x 20-matrix. Het is de voortbrenger van een (20,12) code. We kunnen een woord $(a_1, a_2, \ldots, a_{20})$ van deze code ook op de volgende manier opschrijven:

a_1	a_2	a_3	a_4	a_5
a_6	a_7	a_8	a_9	a_{10}
a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
a_{16}	a_{17}	a_{18}	a_{19}	a_{20}

Dan zijn de elementen links boven information symbols. De parity-check vergelijkingen zijn eenvoudig: van iedere rij en van iedere kolom moet de som 0 zijn. Dit betekent dat alle woorden $\neq 0$ gewicht ≥ 4 hebben. Deze code is dus single-error-correcting en double-error-detecting.

Dit soort codes is door de IBM gebruikt om fouten te ontdekken bij gebruik van magneetbanden.

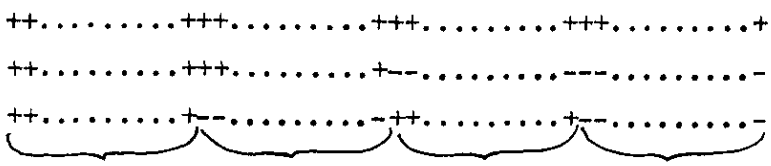
Hadamard matrices en codes

(3.2) Definitie: Een vierkante matrix H waarvan alle elementen ± 1 zijn en waarvoor geldt $HH^T = n\,I$ heet een Hadamard matrix van de orde n.

(3.3) Stelling: Als er een Hadamard matrix van de orde n is, dan is $n = 1$, $n = 2$ of $n \equiv 0 \pmod 4$.

Bewijs: Als we in een Hadamard matrix H de j-de rij of de j-de kolom met -1 vermenigvuldigen ontstaat een andere Hadamard matrix. Als we in H de i-de en j-de rij verwisselen of de i-de en j-de kolom verwisselen ontstaat weer een Hadamard matrix. We mogen dus aannemen dat de eerste rij van H alleen elementen +1 bevat. We zien dus dat de orde n even moet zijn daar de andere rijen van H evenveel elementen +1 als elementen -1 moeten bevatten. Door de boven beschreven ver-

wisselingen kunnen we er voor zorgen dat de eerste drie rijen van H de volgende vorm hebben:



Uit $HH^T = nI$ volgt

$a - b + c - d = 0$,

$a - b - c + d = 0$,

dus $a = b$ en $c = d$, d.w.z. $a = b = c = d = \frac{1}{4}n$ en $n \equiv 0 \pmod 4$.

(3.4) Stelling: Als H_m en H_n Hadamard matrices zijn van de orde m resp. n dan is $H_m \times H_n$ een Hadamard matrix van de orde mn.

Bewijs: Bepaal $(H_m \times H_n)(H_m \times H_n)^T$. Dit is mnI.

Voorbeeld: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is een 2×2 Hadamard matrix, dus is voor iedere Hadamard matrix H_n van de orde n de matrix

$$\begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

een Hadamard matrix van de orde 2n.

Vermoeden: Voor iedere $n \equiv 0 \pmod 4$ bestaat er een Hadamard matrix H van de orde n. (Voor $n < 156$ zijn voorbeelden bekend.)

We beschrijven nu een constructie (van R.E.A.C. Paley) van speciale Hadamard matrices. Zij $q = p^k \equiv 3 \pmod 4$. Op het lichaam GF(q) definiëren we een functie χ door: $\chi(0) = 0$, $\chi(x) = 1$ als $x \neq 0$ een kwadraat is en anders $\chi(x) = -1$. Voor ieder paar x,y uit GF(q) geldt $\chi(xy) = \chi(x)\chi(y)$. Beschouw nu de som

$$\Sigma_{b \in GF(q)} \chi(b)\chi(b+c) \quad .$$

Als $c = 0$ dan is deze som $q - 1$. Als $c \neq 0$ dan is er voor $b \neq 0$ een z zo dat $b + c = bz$ en als b alle elementen $\neq 0$ van GF(q) doorloopt dan doorloopt z alle elementen $\neq 1$ van GF(q). Dus is

$$\Sigma_b\ \chi(b)\chi(b+c) = \Sigma_{b\neq 0}\ \chi(b)\chi(b+c) = \Sigma_{b\neq 0}\{\chi(b)\}^2\chi(z) =$$

$$= \Sigma_{z\neq 1}\ \chi(z) = -1 + \Sigma_z\ \chi(z) = -1 \quad .$$

Als $a_0 = 0, a_1, a_2, \ldots, a_{q-1}$ de elementen van GF(q) zijn definiëren we een matrix S door:

$$S = (s_{ij}) \text{ met } s_{ij} = \chi(a_i - a_j) \qquad (i,j = 0,1,\ldots,q-1) \ .$$

In GF(q) is -1 niet een kwadraat, immers als a alle kwadraten $\neq 0$ doorloopt en -1 is een kwadraat dan doorloopt -a ook alle kwadraten $\neq 0$ en daaruit volgt $(-1)^{\frac{q-1}{2}} = 1$, dus $q \equiv 1 \pmod 4$. We zien dus dat

$$s_{ji} = \chi(a_j - a_i) = \chi(-1)\chi(a_i - a_j) = -s_{ij} \quad .$$

In het vervolg stelt J een matrix voor waarvan alle elementen 1 zijn.
We hebben aangetoond dat

a) $S^T = -S$,

b) $SS^T = qI - J$,

c) $SJ = JS = 0$.

Definieer nu

$$H = \begin{pmatrix} 1 & 1 & 1 & \ldots\ldots & 1 \\ -1 & & & & \\ -1 & & & & \\ \cdot & & & & \\ \cdot & & I_q + S & & \\ \cdot & & & & \\ -1 & & & & \end{pmatrix} \quad .$$

Dan geldt $HH^T = (q+1)I_{q+1}$. Hiermee is aangetoond dat als $n \equiv 0 \pmod 4$ en $n-1$ een macht van een priemgetal is, er een Hadamard matrix van de orde n bestaat.

<u>Voorbeeld</u>: Neem $q = 7$. De kwadraten in GF(7) zijn 1, 2 en 4. Voor S vinden we

$$\begin{pmatrix} 0 & - & - & + & - & + & + \\ + & 0 & - & - & + & - & + \\ + & + & 0 & - & - & + & - \\ - & + & + & 0 & - & - & + \\ + & - & + & + & 0 & - & - \\ - & + & - & + & + & 0 & - \\ - & - & + & - & + & + & 0 \end{pmatrix}$$

We vinden hieruit een scheefsymmetrische Hadamard matrix.

Een symmetrische Hadamard matrix van de orde 8 is ook eenvoudig te vinden. We gaan uit van de matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ en passen twee keer stelling (3.4) toe. In standaardvorm ziet deze matrix er als volgt uit:

$$H_8 = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & + & - & + & - \\ + & - & + & - & - & + & - & + \\ + & - & - & + & + & - & - & + \\ + & - & - & + & - & + & + & - \end{pmatrix}.$$

Hadamard code

We merken op dat uit de definitie (3.2) volgt dat als H een Hadamard matrix van de orde n is, de $2n \times n$-matrix

$$\begin{pmatrix} \frac{1}{2}(H+J) \\ \frac{1}{2}(-H+J) \end{pmatrix}$$

een (0,1) matrix is waarvan elk tweetal verschillende rijen Hamming-distance $\frac{1}{2}n$ of n heeft. Dat betekent dus dat we een code hebben bestaande uit 2n woorden met minimale afstand $\frac{1}{2}n$. In het algemeen is dit niet een lineaire code. Gaan we uit van de symmetrische H_8 in standaardvorm dan vinden we een Hadamard code bestaande uit 16 woorden. Dit is een lineaire code met voortbrenger

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

dat is de al eerder besproken Hamming (8,4) double-error-detecting code.

Cyclische codes

Beschouw de ring R van polynomen met coëfficiënten in GF(q). De veelvouden van $x^n - 1$ vormen een ideaal S. De restklassenring R/S kunnen we representeren door de polynomen $a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ met $a_i \in GF(q)$. Deze schrijven we nu ook als $\underline{a} = (a_0,a_1,\ldots,a_{n-1})$. Dan interpreteren we R/S als vectorruimte over GF(q) met als 2e bewerking de vermenigvuldiging in R/S. Als f(x) een polynoom in x is dan geven we met $\{f(x)\}$ aan de klasse in R/S waartoe f(x) behoort.

(3.5) Definitie: Een k-dimensionale lineaire deelruimte V van de vectorruimte R/S heet cyclische code (= cyclische deelruimte) als voor iedere $\underline{a} = (a_0,a_1,\ldots,a_{n-1}) \in V$ geldt $(a_{n-1},a_0,a_1,\ldots,a_{n-2}) \in V$.

(3.6) Stelling: V is een cyclische code dan en slechts dan als V een ideaal in de ring R/S is.

Bewijs: a) Zij V cyclisch en $\underline{a} \in V$. Dan is

$$\{x\}\{a_0 + a_1x + \ldots + a_{n-1}x^{n-1}\} = \{a_{n-1} + a_0x + \ldots + a_{n-2}x^{n-2}\} \in V .$$

Dus is $\{c_0 + c_1x + \ldots\}\{a_0 + a_1x + \ldots + a_{n-1}x^{n-1}\} \in V$ voor iedere $\underline{c} \in R/S$ d.w.z. V is een ideaal in R/S.

b) Als V een ideaal in R/S is is met $\underline{a} \in V$ ook $\{x\}\{a_0 + \ldots + a_{n-1}x^{n-1}\} \in V$ d.w.z. $(a_{n-1},a_0,\ldots,a_{n-2}) \in V$.

Opmerking: Zonder moeite ziet men in dat een ideaal in R/S bestaat uit alle veelvouden van een polynoom g(x) dat deler is van $x^n - 1$. Dit polynoom heet de voortbrenger van het ideaal.

Voorbeeld: We werken over GF(2). Dan is

$$1 - x^7 = (1 - x)(1 + x + x^3)(1 + x^2 + x^3) .$$

Het polynoom $g(x) = 1 + x^2 + x^3$ is irreducibel over GF(2). We merken op dat volgens de constructie van blz. 16 het lichaam $GF(2^3)$ kan worden voorgesteld door de elementen $0,1,\alpha,\alpha^2,\ldots,\alpha^6$ waarin $1 + \alpha^2 + \alpha^3 = 0$, d.w.z. dat in $GF(2^3)$ het polynoom g(x) is te ontbinden als $g(x) = 1 + x^2 + x^3 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$.
De vectorruimte R/S der polynomen over GF(2) mod $x^7 - 1$ is een 7-dimensionale ruimte over GF(2). Hierin vormen alle veelvouden

van $g(x)$ een ideaal V, te weten de 4-dimensionale lineaire deelruimte van R/S opgespannen door

$\{g(x)\} = (1\ 0\ 1\ 1\ 0\ 0\ 0)$,
$\{xg(x)\} = (0\ 1\ 0\ 1\ 1\ 0\ 0)$,
$\{x^2g(x)\} = (0\ 0\ 1\ 0\ 1\ 1\ 0)$,
$\{x^3g(x)\} = (0\ 0\ 0\ 1\ 0\ 1\ 1)$.

In de terminologie van blz. 23 is de matrix

$$G := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

een voortbrenger van de code. Als parity-check matrix kunnen we nemen

$$H := \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} .$$

We zien dan dat we hier met de (7,4) Hamming code te doen hebben. Nog een andere voorstelling van deze code vinden we door voor $i = 3,4,5$ en 6 te schrijven

$$x^i = (1+x^2+x^3)q_i(x) + r_i(x)$$

waarin r_i een polynoom van graad ≤ 2. Dan zijn de restklassen $\{x^i - r_i(x)\}$ elementen van het ideaal V. Deze 4 elementen vormen een basis van V en de voortbrenger wordt nu

$$G^* := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

Dit is de op blz. 23 besproken standaardvorm, echter met I_4 achteraan. We kunnen de coëfficiënten van x^3 t/m x^6 dan als information symbols nemen en de eerste 3 coëfficiënten als parity-check symbols.

Een cyclische code kan ook gegeven worden door de nulpunten van g (in een geschikt lichaam) te noemen. Alle veeltermen van het ideaal zijn in die punten ook 0. Zo bestaat de in bovenstaand voorbeeld genoemde code uit alle

$(a_0,\ldots,a_6)$ waarvoor $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_6\alpha^6 = 0$ waarin α primitief element van GF(8) is. Zoals boven reeds gezegd is kunnen we a_3 t/m a_6 als information symbols kiezen en dan is $a_0 + a_1\alpha + \ldots + a_6\alpha^6 = 0$ een vergelijking waaruit a_0, a_1 en a_2 zijn op te lossen. De kolommen van de parity-check matrix zijn de voorstellingen van $1,\alpha,\ldots,\alpha^6$ als vectoren over GF(2).

Eén van de nuttige aspecten van cyclische codes waar we hier niet op ingaan is het feit dat de bouw van apparatuur om met de codes te werken eenvoudig is (schuif-registers). Ook het coderen zelf is gemakkelijk. We gaan nog wel enkele eigenschappen op het gebied van fouten-detectie van deze codes bekijken.

(3.7) Definitie: Een "burst" van de lengte d is een vector waarvan de componenten $\neq 0$ zich bevinden onder d opeenvolgende componenten waarvan de eerste en laatste niet 0 zijn. We spreken van een burst-error in een signaal als verschil van gezonden en ontvangen signaal een burst is.

(3.8) Stelling: In een (n,k) cyclische code V is geen enkele codevector een burst van de lengte $d \leq n-k$.

Bewijs: Zij $g(x)$ de voortbrenger van het ideaal V. Dan is $g(x)$ een polynoom van de graad $n-k$. Een burst van de lengte $d \leq n-k$ is op te vatten als restklasse $\{r(x)\}$ met $r(x) = x^a s(x)$ en $s(x)$ een polynoom van graad $< n-k$. Als $\{r(x)\} \in V$ is ook $\{s(x)\}$ een element van V en dit is niet mogelijk daar $s(x)$ niet door $g(x)$ deelbaar is.

Gevolg: De code is in staat een burst-error met lengte $\leq n-k$ te ontdekken. Er zijn ook langere burst-errors die ontdekt worden maar niet alle.

BCH-codes

Als voorbeeld van zeer goede cyclische codes behandelen we nu codes gevonden door Bose, Chaudhuri en Hocquenghem. Deze codes worden gebruikt voor het verbeteren van meerdere fouten en voor burst-error-detection. Het idee is heel eenvoudig.

(3.9) Definitie: Laat α een element van $GF(q^m)$ zijn en m_0 geheel. Een cyclische code over GF(q) heet BCH-code als voor iedere $\{f(x)\}$ uit de code

$\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+d-2}$

nulpunten van f zijn. (We beperken ons verder tot $q = 2$, α primitief element van $GF(2^m)$, $m_0 = 1$.)

We merken eerst op dat uit $f(\alpha) = 0$ volgt $f(\alpha^2) = 0$ daar over GF(2) geldt: $(\Sigma c_i x^i)^2 = \Sigma c_i x^{2i}$. Het is dus voldoende te eisen dat $f(\alpha) = f(\alpha^3) = \ldots = f(\alpha^{2t-1}) = 0$. We tonen nu aan dat ieder codewoord gewicht $\geq 2t+1$ heeft. Schrijf, met $d = 2t+1$

$$H^* := \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \ldots & \end{pmatrix}$$

(Hierin is $n = 2^m - 1$.)

Als er een codewoord met gewicht $< d$ was dan zouden er $d-1$ kolommen van H^* zijn behorend bij $\alpha^{j_1}, \ldots, \alpha^{j_{d-1}}$ zó dat de uit deze kolommen bestaande determinant 0 is. Schrijven we $\xi_i = \alpha^{j_i}$ dan betekent dit

$$\begin{vmatrix} \xi_1 & \xi_2 & \ldots & \xi_{d-1} \\ \xi_1^2 & \xi_2^2 & \ldots & \xi_{d-1}^2 \\ \cdot & \cdot & \cdot & \cdot \\ \xi_1^{d-1} & \ldots & \ldots & \xi_{d-1}^{d-1} \end{vmatrix} = \xi_1 \xi_2 \ldots \xi_{d-1} \prod_{i>k} (\xi_i - \xi_k) = 0 ,$$

d.w.z. $\alpha^{j_i} = \alpha^{j_k}$ voor zekere i en k in strijd met het gegeven dat α een primitief element van $GF(2^m)$ is. Hiermee is aangetoond:

(3.10) Stelling: Is in (3.9) α primitief element van $GF(2^m)$, $m_0 = 1$ en $d = 2t+1$ dan is de afstand van codewoorden tenminste d, d.w.z. de code is t-error-correcting.

Een parity-check matrix voor de code kunnen we nu als volgt beschrijven. We beginnen met $1, \alpha, \ldots, \alpha^{n-1}$ als kolomvectoren van nullen en enen. Onder α^i komen de kolommen $\alpha^{3i}, \alpha^{5i}, \ldots, \alpha^{(2t-1)i}$. We hebben dan een matrix H met mt rijen en $2^m - 1 = n$ kolommen. Voor een codevector $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$ betekent $\underline{c}H^T = \underline{0}$ hetzelfde als $c(\alpha) = c(\alpha^3) = \ldots = c(\alpha^{2t-1}) = 0$ waarin

$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$. We zien hieruit de grote kracht van de code. Van de $2^m - 1$ symbols zijn ten hoogste mt check symbols nodig om tenminste t fouten te kunnen verbeteren.

Nemen we als voorbeeld het binaire symmetrische kanaal van blz. II-3 Kiezen we $m = 10$ en $t = 4$ dan heeft de BCH code een transmissiesnelheid 0,96. We werken met woorden van de lengte 1023. De kans dat een woord onveranderd door het kanaal komt is slechts 36%. Door maximum-likelihood-decoding is de kans dat een gezonden woord verkeerd aankomt kleiner dan 0,4% (voor het kanaal is $p = 0{,}001$).

De methode van decoderen behandelen we nu aan de hand van een voorbeeld. We beschouwen de (15,7) double-error-correcting BCH code waarbij α primitief element van $GF(2^4)$ is en wel $\alpha^4 + \alpha + 1 = 0$. Als een signaal $\underline{s}$ ontvangen wordt vullen we dit in in de parity-check vergelijkingen. Stel dat we vinden $\underline{s}H^T = (1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)$ (mt is nu 8). Nu is $\underline{s} = \underline{c} + \underline{e}$ waarin $\underline{c}$ het gezonden signaal en $\underline{e}$ foutenpatroon is. Daar $\underline{c}H^T = \underline{0}$ moeten we om de fouten te verbeteren $\underline{e}$ bepalen uit $\underline{e}H^T = (1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)$. Als er één fout gemaakt is op de plaats α^i dan is $\alpha^i = (1\ 1\ 1\ 1)$ d.w.z. $i = 12$, dus $\alpha^{3i} = \alpha^6 = (0\ 0\ 1\ 1) \neq (1\ 1\ 0\ 1)$. We zien dat er meer dan één fout is gemaakt. Neem aan dat er twee fouten zijn gemaakt op de plaats α^i en de plaats α^j. Dan moet

$$\alpha^i + \alpha^j = (1\ 1\ 1\ 1) = \alpha^{12},$$
$$\alpha^{3i} + \alpha^{3j} = (1\ 1\ 0\ 1) = \alpha^7 .$$

Hieruit vinden we $\alpha^{i+j} = \alpha^{13}$, d.w.z. α^i en α^j zijn de oplossingen van

$$\xi^2 + \alpha^{12}\xi + \alpha^{13} = 0 .$$

Door voor ξ in te vullen $1, \alpha, \alpha^2$ enz. vinden we oplossingen $\xi = \alpha^3$ en $\xi = \alpha^{10}$. Dit betekent dat op de plaatsen van α^3 en α^{10} (dat is het 4e en het 11e symbool van het woord) fouten zijn gemaakt.

Aan dit voorbeeld zien we hoe belangrijk het is om bij de lichamen die een rol spelen de beschikking te hebben over tabellen als op blz. 17 waaruit men multiplicatieve en additieve structuur van het lichaam tegelijk kan aflezen. De BCH codes zijn ongeveer 10 jaar geleden ontdekt. Er is op dit gebied nog veel werk te doen!

Hoofdstuk IV. Block designs

Beschouw een $v \times b$ matrix A, waarvan alle elementen 0 of 1 zijn (we noemen dit een (0,1) matrix), met de volgende eigenschappen:

B1: in iedere kolom staan evenveel (= k) elementen 1,

B2: van ieder tweetal verschillende rijen is het inproduct hetzelfde (= λ),

B3: $0 < \lambda$ en $k < v - 1$.

Stel dat in de i-de rij r_i elementen 1 voorkomen. Tel nu bij vaste i de paren $(a_{ij}, a_{kj}) = (1,1)$. Volgens B1 is dit aantal $r_i(k-1)$ en volgens B2 is het $\lambda(v-1)$. Dus volgt uit B1 en B2:

B4: in iedere rij van A staan evenveel (= r) elementen 1,

B5: $\lambda(v-1) = r(k-1)$ en $bk = vr$.

(4.1) Stelling: Voor bovengenoemde matrix A geldt

$$AA^T = (r-\lambda)I + \lambda J .$$

Bewijs: B4 + B2.

(4.2) Definitie: Zij V een verzameling met v elementen. De deelverzamelingen van V noemen we blokken. Een stelsel van b blokken heet een balanced incomplete block design (BIBD) als:

BD1: elk blok bevat k elementen,

BD2: elk paar van V ligt in precies λ blokken

BD3: $0 < \lambda$ en $k < v - 1$.

We kunnen een block design beschrijven met behulp van een (0,1) matrix $A = (a_{ij})$ die we incidentiematrix van het block design noemen. We definiëren A door de punten van V te nummeren en de blokken te nummeren en $a_{ij} = 1$ te stellen als punt i in het j-de blok ligt en anders $a_{ij} = 0$. De matrix A heeft dan de eigenschappen B1 t/m B5. Uit (4.1) volgt door eenvoudig vegen:

(4.3) Stelling: $\det(AA^T) = (r-\lambda)^{v-1}\{r + (v-1)\lambda\}$.

Uit B3 en B5 volgt $r > \lambda$ en dus is $\det(AA^T) \neq 0$. Daar verder de rang van AA^T ten hoogste gelijk aan de rang van A is volgt nu dat $b \geq v$ (en dus $r \geq k$). Dit heet de ongelijkheid van Fisher.

(4.4) Definitie: Een BIBD heet symmetrisch als $b = v$ (en dus $r = k$). Men spreekt ook van een (v,k,λ)-configuratie.

Block designs spelen een grote rol in een onderdeel van de statistiek bekend als "design of experiments". We komen hier later op terug.

Zonder bewijs vermelden we hier de stelling:

(4.5) Stelling (Bruck-Ryser): Als een symmetrisch block design bestaat met parameters v,k,λ en als $n = k - \lambda$ dan is

BR1: n een kwadraat als v even is,

BR2: als v oneven is heeft de vergelijking

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$$

een oplossing met gehele $(x,y,z) \neq (0,0,0)$.

Voorbeelden: a) Zij $V := \{1,2,3,4,5,6,7\}$ en kies als blokken de deelverzamelingen $\{1,2,4\}$, $\{2,3,5\}$, $\{3,4,6\}$, $\{4,5,7\}$, $\{5,6,1\}$, $\{6,7,2\}$ en $\{7,1,3\}$. Ieder blok bevat $k = 3$ elementen en ieder paar (a,b), $a \neq b$, komt in $\lambda = 1$ blok voor. Verder is $b = v = 7$ en $r = 3$. Dit is een symmetrisch BIBD.

b) Als H_n een Hadamard matrix is van de orde $n = 4t$ met eerste rij en eerste kolom bestaande uit elementen +1 dan laten we deze eerste rij en kolom weg en vervangen de elementen -1 door 0. De (0,1) matrix die zo ontstaat is incidentiematrix van een symmetrisch BIBD met $v = b = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$. Dit volgt uit de definitie van Hadamard matrix als we nog bedenken dat B1 t/m B3 uit de betrekking van (4.1) volgen.

Eindige meetkunde

(4.6) Definitie: Een projectief vlak π is een verzameling waarvan we de elementen punten noemen en waarvan sommige deelverzamelingen de naam lijn hebben gekregen met de volgende eigenschappen:

P1: door ieder paar verschillende punten gaat één lijn,

P2: ieder paar verschillende lijnen heeft één punt gemeen,

P3: er zijn 4 verschillende punten waarvan géén drietal op één lijn ligt.

We merken op dat uit P1 t/m P3 volgt:

P4: er zijn 4 verschillende rechten waarvan géén drietal door één punt gaat.

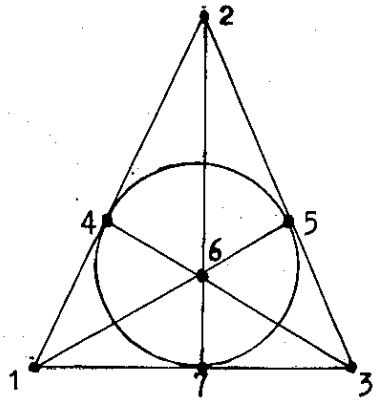
Er is een dualiteit in deze definitie. We kunnen de begrippen punt en lijn verwisselen als we ook "punt ligt op lijn" met "lijn gaat door punt" verwisselen.

Als π slechts eindig veel punten bevat spreken we van een <u>eindig projectief vlak</u>. We zien zonder moeite in dat uit P1 t/m P4 volgt dat in een eindig projectief vlak π alle lijnen precies evenveel punten bevatten. Is dit aantal $n+1$ dan noemen we n de <u>orde</u> van π.

(4.7) <u>Stelling</u>: Als π een projectief vlak is van de orde n dan bevat π n^2+n+1 punten en n^2+n+1 lijnen.

<u>Bewijs</u>: Zij O een punt van π. Er zijn precies $n+1$ lijnen door O. Elke lijn bevat naast O nog n andere punten. Het totale aantal punten is dus $n(n+1)+1$.

<u>Voorbeeld</u>: Het op blz. 38 gegeven voorbeeld a) is een projectief vlak met $7 = 2^2+2+1$ punten. De daar genoemde blokken kunnen we als lijnen nemen. We kunnen deze meetkunde (= meetkunde van Fano) door het volgende plaatje beschrijven:



We beschrijven nu een manier om een projectief vlak te construeren. We beschouwen een 3-dimensionale ruimte R over het lichaam GF(q). Het drietal (0,0,0) laten we buiten beschouwing en verder spreken we af dat als $\lambda \neq 0$ de drietallen (a_1, a_2, a_3) en $(\lambda a_1, \lambda a_2, \lambda a_3)$ geïdentificeerd worden. (We noemen dit ook equivalente drietallen; een klasse equivalente drietallen is een rechte door (0,0,0) in de ruimte R.) De verzameling klassen van drietallen (dus rechten door (0,0,0) in R) nemen we als verzameling <u>punten</u>. Een zelfde verzameling klassen van drietallen nemen we als verzameling <u>lijnen</u>. Een lijn wordt een deelverzameling van de verzameling punten door de volgende afspraak: punt (p_1,p_2,p_3) ligt op lijn (ℓ_1,ℓ_2,ℓ_3) als $p_1\ell_1 + p_2\ell_2 + p_3\ell_3 = 0$.

Zijn de punten (p_1,p_2,p_3) en (q_1,q_2,q_3) verschillend, d.w.z. de drietallen niet evenredig, dan is

$$p_1q_2 - p_2q_1 \neq 0 \quad \text{of} \quad p_1q_3 - p_3q_1 \neq 0 \quad \text{of} \quad p_2q_3 - p_3q_2 \neq 0 .$$

Neem aan dat $p_1q_2 - p_2q_1 \neq 0$. De vergelijkingen

$$p_1x_1 + p_2x_2 = - p_3x_3 ,$$
$$q_1x_1 + q_2x_2 = - q_3x_3$$

hebben als $x_3 = 0$ de oplossing $x_1 = x_2 = 0$ en als $x_3 = 1$ een éénduidig bepaalde oplossing (x_1,x_2). D.w.z. er is precies één lijn (x_1,x_2,x_3) waar (p_1,p_2,p_3) en (q_1,q_2,q_3) op liggen. Analoog is er precies één punt dat op twee verschillende lijnen ligt. Tenslotte liggen van de vier punten $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ en $(1,1,1)$ géén 3 op één lijn. In feite hebben we niets anders gedaan dan de vlakken door $(0,0,0)$ in R de naam lijn geven. We hebben zo een projectief vlak geconstrueerd. De orde van het vlak is q. Dit zien we in door op te merken dat op de rechte $(0,0,1)$ geen andere punten liggen dan $(1,0,0)$ en $(a_i,1,0)$ waarin a_i de elementen van GF(q) doorloopt. Dat zijn $q+1$ punten. Hiermee is aangetoond:

(4.8) Stelling: Als $q = p^k$ (p priem) dan is er een projectief vlak van de orde q.

Opmerking 1: Er zijn tot heden geen andere eindige projectieve vlakken bekend.

Opmerking 2: De boven beschreven constructie kan ook gebruikt worden om een oneindig projectief vlak te construeren. In plaats van GF(q) nemen we de reële getallen.

Een projectief vlak π van de orde n is een voorbeeld van een symmetrisch BIBD met $v = b = n^2 + n + 1$, $k = n + 1$, $\lambda = 1$.

Uit (4.5) en een getaltheoretische stelling volgt:

(4.9) Stelling (Bruck-Ryser): Als een projectief vlak van de orde n bestaat waarbij $n \equiv 1$ of $2 \pmod 4$ dan is

$$n = a^2 + b^2 \quad (a \text{ en } b \text{ geheel}).$$

Uit (4.8) en (4.9) zien we dat $n = 10$ de kleinste orde is waarvoor niet bekend is of er een projectief vlak van die orde is.

Als we uit een projectief vlak met n^2+n+1 punten één lijn ℓ weglaten en in de overgebleven "meetkunde" twee lijnen evenwijdig noemen als ze in het projectieve vlak een snijpunt op ℓ hebben dan hebben we een zgn. affien vlak verkregen. Dit heeft $n(n+1)$ lijnen en n^2 punten. De eigenschappen P1 t/m P3 gaan over in bekende axioma's van de vlakke meetkunde.

Latijnse vierkanten

(4.10) Definitie: Een $n \times n$ matrix A heet latijns vierkant als iedere rij van A en iedere kolom van A een permutatie is van n gegeven symbolen (bijv. de getallen $1,2,\ldots,n$).

(4.11) Definitie: De latijnse vierkanten $A^{(1)} = (a_{ij}^{(1)})$ en $A^{(2)} = (a_{ij}^{(2)})$ heten orthogonaal als de n^2 paren $(a_{ij}^{(1)}, a_{ij}^{(2)})$ allemaal verschillend zijn. Een schema van n rijen en n kolommen met in de i-de rij en j-de kolom het paar $(a_{ij}^{(1)}, a_{ij}^{(2)})$ noemt men dan een grieks-latijns vierkant.

Voorbeeld: De matrices

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

zijn latijnse vierkanten. Ze zijn twee aan twee orthogonaal.

(4.12) Stelling: Als $A^{(1)}, A^{(2)}, \ldots, A^{(t)}$ een stelsel van t twee aan twee orthogonale latijnse vierkanten van de orde $n \geq 3$ is dan is $t \leq n-1$.

Bewijs: In elk der $A^{(i)}$ kunnen we de symbolen 1 t/m n zó permuteren dat de eerste rij van de matrix $1,2,\ldots,n$ wordt. De vierkanten blijven orthogonaal. Nu moeten de t getallen $a_{21}^{(i)}$ verschillend zijn en daar $a_{21}^{(i)} \neq 1$ volgt: $t \leq n-1$.

Als $t = n-1$ heet het stelsel orthogonale latijnse vierkanten volledig. Het is niet moeilijk voor $n = p^k$ (p priem) een volledig stelsel orthogonale latijnse vierkanten aan te geven. We zullen dit niet doen daar het bestaan van zo'n stelsel volgt uit (4.8) en stelling (4.13). We merken nog op dat behalve voor $n = 2$ en $n = 6$ er steeds een paar orthogonale latijnse vierkanten van de orde n is.

(4.13) Stelling: Als een projectief vlak π van de orde n bestaat dan zijn er $n-1$ orthogonale latijnse vierkanten van de orde n en omgekeerd.

Bewijs: Laat π een projectief vlak van de orde n zijn. Kies in π een rechte ℓ en nummer de punten van ℓ: $P_1, P_2, \ldots, P_{n+1}$. De overige punten (affien vlak) nummeren we $Q_1, Q_2, \ldots, Q_{n^2}$. De n lijnen $\neq \ell$ door P_i nummeren we van 1 t/m n (voor iedere i). Nu definiëren we de $n^2 \times (n+1)$ matrix S* door voor s^*_{ij} het nummer van de rechte Q_iP_j te nemen. Kijken we naar twee kolommen van S* dan komen daarin precies alle paren (a,b) met $1 \leq a \leq n$, $1 \leq b \leq n$ voor (elk één keer). We permuteren nu de rijen van S* zó dat een matrix S ontstaat waarin in de laatste twee kolommen de paren (1,1) t/m (n,n) in lexicografische ordening voorkomen. Dan definiëren we $A^{(\nu)}$ voor $\nu = 1, \ldots, n-1$ door

$$A^{(\nu)} = (a^{(\nu)}_{ij}) \quad \text{met} \quad a^{(\nu)}_{ij} = s_{(i-1)n+j,\nu}.$$

Daar $s_{(i-1)n+j,n} = s_{(i-1)n+k,n}$ is $a^{(\nu)}_{ij} \neq a^{(\nu)}_{ik}$ als $j \neq k$ en daar $s_{(i-1)n+j,n+1} = s_{(k-1)n+j,n+1}$ is $a^{(\nu)}_{ij} \neq a^{(\nu)}_{kj}$ als $i \neq k$,

d.w.z. iedere $A^{(\nu)}$ is een latijns vierkant en de orthogonaliteit van deze vierkanten volgt uit het feit dat in de ν-de kolom en μ-de kolom van S alle paren (a,b) voorkomen. Het bewijs van de omkering volgt analoog.

Difference sets

(4.14) Definitie: Een deelverzameling $D = \{d_1, d_2, \ldots, d_k\}$ van de gehele getallen mod v heet een (perfect) difference set met parameters (v,k,λ) als iedere $a \not\equiv 0 \pmod v$ op precies λ manieren is te schrijven als $d_i - d_j \equiv a \pmod v$. Om triviale gevallen uit te sluiten eisen we nog $0 < \lambda < k < v-1$.

Voorbeeld: $\{0,1,3,9\}$ is een (13,4,1) difference set.

Uit de definitie volgt dat als we alle elementen van D met een constante a vermeerderen een difference set D_a ontstaat die precies λ elementen met D gemeen heeft. Dit betekent dat $D, D_1, \ldots, D_{v-1}$ aan de eisen van (4.2) en (4.4) voldoen, d.w.z. een (v,k,λ)-configuratie vormen. Bewezen is hiermee:

(4.15) Stelling: Als een (v,k,λ) difference set bestaat dan is er een (v,k,λ) configuratie waarvan de incidentiematrix cyclisch is. (Ook het omgekeerde is waar.)

De op blz. 30 gedefinieerde matrix S is cyclisch als q een priemgetal is. Daar verder S + J incidentiematrix van een symmetrisch block design is vinden we uit (4.15) de volgende constructie van speciale difference sets:

(4.16) Stelling: Als $p = 4t - 1$ een priemgetal is dan vormen de $\frac{p-1}{2}$ kwadraatresten mod p een verzameling $\{d_1, d_2, \ldots, d_k\}$ die difference set is met parameters $v = p = 4t - 1$, $k = \frac{p-1}{2} = 2t - 1$, $\lambda = t - 1$.

Bewijs: We geven nog een direct bewijs. Er is zeker een oplossing van $d_i - d_j \equiv 1 \pmod p$. Zij c een kwadraatrest dan zijn ook cd_i en cd_j kwadraatresten en $cd_i - cd_j \equiv c \pmod p$. Is omgekeerd $d_k - d_\ell \equiv c \pmod p$ dan is $c^{-1}d_k - c^{-1}d_\ell \equiv 1 \pmod p$ terwijl $c^{-1}d_k$ en $c^{-1}d_\ell$ kwadraatresten zijn. Verder is -1 niet een kwadraatrest. Als we nog opmerken dat uit $d_i - d_j \equiv a \pmod p$ volgt $d_j - d_i \equiv -a \pmod p$ dan is aangetoond dat voor iedere $a \not\equiv 0 \pmod p$ de congruentie $d_i - d_j \equiv a \pmod p$ evenveel oplossingen heeft. Dit aantal is $\frac{k(k-1)}{v-1} = t - 1$.

Voorbeeld: $D := \{1,4,5,6,7,9,11,16,17\}$ is een difference set mod 19; iedere a is op 4 manieren te schrijven als verschil van twee elementen van D (mod 19). Zo is bijv.: $10 \equiv 17 - 7 \equiv 16 - 6 \equiv 11 - 1 \equiv 7 - 16 \pmod{19}$.

Toepassingen

a) Weegschema's. Stel dat v objecten gewogen moeten worden in v wegingen met een balans. We nemen aan dat alle wegingen een zelfde variantie hebben, onafhankelijk van de belasting van de schaal. We verlangen nu dat de wegingen zo worden uitgevoerd dat de gemiddelde variantie van de geschatte gewichten minimaal is.
We geven het schema als volgt aan: als bij de i-de weging het j-de object op de linkerschaal ligt, dan is $a_{ij} = 1$, terwijl voor de rechterschaal $a_{ij} = -1$ en verder nemen we $a_{ij} = 0$ als het j-de object bij de i-de weging niet meedoet. Door Hotelling is bewezen dat als $v \equiv 0 \pmod 4$ de beste weging gevonden wordt door te eisen dat $A = (a_{ij})$ een Hadamard matrix is. De geschatte gewichten hebben dan gelijke varianties en ze zijn niet gecorreleerd.

b) Proefvelden. Op een vierkant stuk bouwland wil men n soorten graan planten en de oogst vergelijken. Hiertoe verdeelt men het stuk land in n^2 subvierkanten. We nemen aan dat (misschien) de grond niet overal even vruchtbaar is maar dat de afhankelijkheid zó is dat $E(y_{ijk})$ = gemiddelde oogst per m^2 voor het k-de soort graan geplant in i-de rij en j-de kolom = $= \rho + \mu_i + \nu_j + \rho_k$ waarbij $\Sigma \mu_i = \Sigma \nu_j = \Sigma \rho_k = 0$. Hierin is ρ de gemiddelde oogst per m^2. Men wil vragen van het type: "zijn de graansoorten verschillend in kwaliteit", "is er werkelijk verschil in vruchtbaarheid voor verschillende rijen resp. kolommen" enz. beantwoorden. Als men de k-de soort graan zó plant dat in iedere rij en iedere kolom één subvierkant met deze soort voorkomt dan is de gemiddelde oogst over deze proefveldjes $\rho + \rho_k$ omdat $\Sigma \mu_i = \Sigma \nu_j = 0$. D.w.z. de invloed van de plaats is geëlimineerd. Om alle soorten zó te planten moet men van het proefveld een latijns vierkant maken.

Statistische analyse van buizenfabricage. Dit voorbeeld is afkomstig van een plaatselijke fabriek waar radiobuizen worden gemaakt. Er zijn vier bewerkingen, te weten a) maken van de wolframdraad, b) maken van de spiraal, c) aanbrengen van de Al_2O_3-laag, d) buizenfabricage. De productie vertoonde een veel te grote spreiding in de gemiddelde gloeistroom. De 4 afdelingen gaven elkaar de schuld en door middel van een experiment moest worden uitgemaakt welke van de 4 factoren oorzaak van het verschijnsel was. I.v.m. tijd en kosten wilde men niet te veel buizen testen.

Voor dit soort experimenten is een grieks-latijns vierkant het hulpmiddel. Beschouw een latijns vierkant van de orde 7 met elementen A, B, C, D, E, F, G en één met elementen a, b, c, d, e, f, g zó dat deze twee orthogonaal zijn. Op 7 verschillende dagen wordt een partij wolframdraad gemaakt en van elke partij maakt men op 7 verschillende dagen spiralen. Een steekproef van 15 spiralen uit elke partij geeft een groep van 49 keer 15 spiralen. Deze plaatst men op het grieks-latijnse vierkant en wel draad van de i-de dag in i-de rij, spiraal van j-de dag in j-de kolom. De 7 partijen op een A-plaats worden op één dag van de Al_2O_3-laag voorzien en teruggeplaatst etc. Daarna worden de 7 partijen op een a-plaats op één dag in buizen gemonteerd etc. Na 28 dagen heeft men 49 keer 15 buizen en aan elke groep worden dan gloeistroommetingen gedaan. Deze opzet heeft bereikt dat voor elke fase de productie van één dag voor iedere andere fase over 7 dagen is verspreid. Het experiment toonde duidelijk aan dat de spreiding (voor verschillende dagen) bij de buizenmontage te groot was.

Kleine experimenten. Het komt vaak voor dat men enkele factoren wil onderzoeken maar dat door tijdgebrek of hoge kosten het niet mogelijk is iedere mogelijkheid voor de eerste factor te koppelen met iedere mogelijkheid voor de tweede.

We nemen als voorbeeld een object dat uit 7 verschillende soorten metaal kan worden gemaakt. Er zijn 7 verschillende processen mogelijk voor de fabricage. Het is te duur alle 49 combinaties te onderzoeken. Hoe nu het experiment op te zetten? Voorbeeld a) op blz. 38 geeft een oplossing. De metalen nummeren we van 1 t/m 7 en aan ieder productieproces kennen we een blok toe. We bereiken dat het eindproduct door elk proces 3 keer is gemaakt, met elk metaal 3 keer is gemaakt en dat er voor ieder tweetal processen één metaal is dat met beide processen is verwerkt. Door middel van variantie-analyse bepaalt men daarna wat de beste keuze is.

Een extra factor. We hebben gezien dat uit de difference-set $\{0,1,3,9\}$ een cyclisch block design gemaakt kan worden. Een voorbeeld van het gebruik hiervan is het volgende:

Men wil 13 soorten tandpasta door proefpersonen laten vergelijken. De soorten zitten in tubes van 4 verschillende kleuren. Iedere proefpersoon krijgt 4 soorten, Ieder soort moet door 4 proefpersonen worden gebruikt en voor ieder tweetal soorten moet er één persoon zijn die ze vergelijkt. Daar we een block design met $v = b = 13$, $r = k = 4$, $\lambda = 1$ hebben kan dit. We kunnen er nu echter ook nog voor zorgen dat ieder soort in één rode, één witte,

één blauwe en één groene tube zit (iedere proefpersoon krijgt 4 tubes van verschillende kleur).

Cyclische codes. Speciale difference sets, nl. die welke verband hebben met projectieve vlakken blijken nuttig te zijn voor het construeren van cyclische codes. Als voorbeeld beschouwen we GF(3). Een projectief vlak van $13 = 3^2 + 3 + 1$ punten bestaat en hiermee staat in verband de op blz. 42 genoemde difference set $\{0,1,3,9\}$. Nu is met $\theta(x) = 1 + x + x^3 + x^9$ op grond van de definitie van difference set

$$\theta(x)\theta(x^{-1}) \equiv 3 + (1 + x + x^2 + \ldots + x^{12}) \bmod (x^{13} - 1)$$

of

$$x^{13} - 1 = (x-1)\theta(x)(1 + x^4 + x^{10} + x^{12}) \bmod 3 .$$

Alle veelvouden van $\theta(x) \bmod (x^{13} - 1)$ (waarbij nu met coëff. uit GF(3) gerekend wordt) vormen een ideaal, d.w.z. ze bepalen een cyclische code (blz. 32). De speciale vorm van $\theta(x)$ maakt dit polynoom zeer geschikt om te gebruiken voor deze code. Het blijkt dat dit een code van dimensie 7 met minimale afstand 4 is! Als oefening kan men dit nagaan m.b.v. de volgende aanwijzingen:

a) $GF(3^3)$ is te construeren m.b.v. het irreducibele polynoom $x^3 + 2x + 1$. Dan is één van de oplossingen van $\alpha^3 + 2\alpha + 1 = 0$ primitief element. Voor iedere β die even macht van α is geldt $\beta^{13} = 1$.

b) $(x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) = x^3 + x^2 + x + 2 = g_1(x)$,

$(x-\alpha^4)(x-\alpha^{10})(x-\alpha^{12}) = x^3 + x^2 + 2 = g_2(x)$,

$(x-\alpha^8)(x-\alpha^{20})(x-\alpha^{24}) = x^3 + 2x^2 + 2x + 2 = g_3(x)$,

$(x-\alpha^{14})(x-\alpha^{16})(x-\alpha^{22}) = x^3 + 2x + 2 = g_4(x)$.

Dus is $x^{13} - 1 = (x-1)g_1(x)g_2(x)g_3(x)g_4(x)$ de ontbinding van $x^{13} - 1$ in irreducibele factoren over GF(3).

c) $g(x) = g_1(x)g_2(x)$ is voortbrenger van een cyclische code van dimensie $13 - 6 = 7$. Daar $\theta(\alpha^2) = \theta(\alpha^4) = 0$ en $\theta(\alpha^8) = -1$, $\theta(\alpha^{14}) = 1$ en verder $\theta(x)(1 + x^4 + x^6) = g_1(x)g_2(x) \bmod (x^{13} - 1)$ is dit de code bestaande uit alle veelvouden van $\theta(x)$.

d) De code is te definiëren door in (3.9) te nemen α^2 i.p.v. α, $q = 3$, $m = 3$, $m_0 = 1$, $d = 4$. Evenals op blz. 35 is gedaan is aan te tonen dat de minimale afstand van de codewoorden d is.

Opgaven Discrete Wiskunde

1. Bewijs dat een getal deelbaar is door 9 als de som van de cijfers (tientallig stelsel) deelbaar is door 9.
   Hoe luidt de overeenkomstige regel voor deelbaarheid door 11 ?

2. Wat is de rest bij deling van 37^{13} door 17 ?

3. Bepaal het kleinste positieve gehele getal dat door 7 deelbaar is en zodat bij deling door 2, 3, 4, 5 of 6 de rest steeds 1 is.

4. Voor welke priemgetallen p is er een geheel getal n zó dat $n^2 + 1$ door p deelbaar is?

5. De kwadraatresten mod 31 zijn de getallen n met $1 \leq n \leq 30$ zó dat er een kwadraat is dat bij deling door 31 de rest n heeft. Als we mod 31 rekenen dan zijn er voor iedere $k \neq 0$ precies 7 paren kwadraatresten n en m zó dat $n - m = k$. Bewijs dit.

6. Hoeveel getallen n zijn er met $0 < n \leq 10^4$, zó dat $2^n + n^2 + 5$ deelbaar is door 7 ?

7. Een natuurlijk getal N heeft $a_1\, a_2\, a_3 \ldots a_n$ als representatie in het 10-tallig stelsel. Het getal met representatie $a_n\, a_1\, a_2 \ldots a_{n-1}$ is 9 keer zo groot. Wat is de kleinste N met deze eigenschap?

8. We schrijven naast elkaar de getallen 87 en 59. Onder 87 schrijven we $[\frac{87}{2}]$, onder 59 het dubbele. Dit zetten we voort tot links een 1 is gekomen. Als in de linkerkolom een getal even is schrappen we de rechterbuur. Dat is:

87	59
43	118
21	236
10	~~472~~
5	944
2	~~1888~~
1	3776 .

   De som van de rechterkolom is het product van 87 en 59. Is dit toeval of een vermenigvuldigingsmethode?

9. Het spel NIM wordt als volgt gespeeld. Er zijn n stapels van respectievelijk $a_1, a_2, \ldots, a_n$ lucifers. Twee spelers mogen om de beurt van een stapel (naar eigen keuze) een aantal (naar eigen keuze) lucifers wegnemen. Wie de laatste lucifer wegneemt heeft gewonnen. Bepaal een winnende strategie.

10. Een spel kaarten (52 kaarten) wordt éénmaal <u>perfect geschud</u> door de onderste 26 van de bovenste 26 weg te nemen en de kaarten om en om neer te leggen (de onderste blijft onder). Hoe vaak kan men dit herhalen voordat alle kaarten op hun oorspronkelijke plaats terug zijn?

11. Er zijn n! permutaties van de getallen 1 t/m n. Er zijn hieronder D_n permutaties $a_1, a_2, \ldots, a_n$ zó dat géén getal op zijn plaats gebleven is, d.w.z. zó dat $a_i \neq i$ voor $i = 1, 2, \ldots, n$.

    Voor n = 4 zijn dit de permutaties (2,1,4,3), (2,3,4,1), (2,4,1,3), (3,1,4,2), (3,4,1,2), (3,4,2,1), (4,1,2,3), (4,3,1,2), (4,3,2,1). Voor D_4 vinden we dus 9. Bepaal $\lim_{n \to \infty} \frac{D_n}{n}$.

12. Probeer permutaties van 1,2,...,n te vinden zó dat alle verschillen mod n verschillend zijn.
    (Voorbeeld: 1,4,2,3 : de verschillen zijn resp. 3,2,1.)

13. Hoeveel onvereenvoudigbare breuken $\frac{a}{b}$ zijn er met $1 \leq a < b$ en b is een deler van 30 ?
    En hoeveel waarvoor b een deler is van 1260 ?

14. Welke gehele getallen zijn te schrijven als $6n_1 + 10n_2 + 15n_3$ met n_1, n_2, n_3 niet-negatief en geheel?

15. Dit probleem gaat over het splitsen van telefoonkabels voor de interlocale dienst.
De draden in zo'n kabel liggen in concentrische lagen. De kabel bestaat uit stukken van enkele honderden meters lengte die aan elkaar zijn gesplitst. Bij dit splitsen moet men de volgorde van de draden veranderen om interferentie en overspraak, waardoor men voor een ander bestemde gesprekken zou horen, zo veel mogelijk te vermijden. In het bijzonder is het gewenst dat 2 naast elkaar lopende draden van een stuk kabel in zo veel mogelijk van de volgende stukken niet naast elkaar lopen. Natuurlijk mag men om praktische redenen de regels voor het splitsen niet te ingewikkeld maken. Het is bijvoorbeeld redelijk, af te spreken dat tussen 2 draden die in een bepaald stuk kabel naast elkaar lopen, in het volgende stuk een vast, van te voren bepaald aantal draden ligt. Als we in elk stuk de draden nummeren van 1 tot en met n en bij het splitsen draad nummer 1 van een stuk vastmaken aan draad nummer 1 van het volgende stuk dan wordt nummer 2 van de eerste vastgemaakt aan nummer $1+s$ van de volgende, 3 aan $1+2s$ enzovoorts. We moeten hierbij getallen groter dan n eerst reduceren, door een veelvoud van n af te trekken. Nummer $n+1$ is dus hetzelfde als nummer 1. Gaan we nu over tot volgende stukken kabel, dan zien we dat een verlenging van de oorspronkelijke draad 1 steeds nummer 1 heeft, de oorspronkelijke nummer 2 achtereenvolgens als rangnummer heeft 2, $1+s$, $1+s^2$, $1+s^3$ enzovoorts. We hadden geëist dat 2 naast elkaar lopende draden van een kabelstuk zo lang mogelijk bij elkaar uit de buurt bleven. Hoe moeten we s kiezen?

16. Een <u>numerieke methode</u> om van een analytische functie

$$f(z) = a_0 + a_1 z + a_2 z^2 + \ldots \qquad (|z| < R,\ R > 1)$$

de afgeleiden in de oorsprong te bepalen, of anders gezegd de coëfficiënten $a_n = \frac{f^{(n)}(0)}{n!}$, berust op het volgende principe. Neem aan dat functiewaarden van f eenvoudig zijn te bepalen. We merken op dat

$$f(0) = a_0 = \frac{1}{2\pi i} \int_{|z|=1} \frac{f(z)}{z}\, dz$$

$$= \int_0^1 f(e^{2\pi i t})\, dt \quad .$$

We gaan deze integraal met de trapeziumregel benaderen.

Schrijf: $g(t) = f(e^{2\pi it})$. Dan vinden we

$$\frac{1}{N}\left[\tfrac{1}{2}g(0) + g(\tfrac{1}{N}) + g(\tfrac{2}{N}) + \ldots + g(\tfrac{N-1}{N}) + \tfrac{1}{2}g(1)\right] = \frac{1}{N}\sum_{k=1}^{N} f\left(e^{2\pi i \frac{k}{N}}\right)$$

$$= \frac{1}{N}\sum_{k=1}^{N}\sum_{m=0}^{\infty} a_m e^{2\pi i \frac{km}{N}} =$$

$$= \sum_{m=0}^{\infty} a_m\left(\frac{1}{N}\sum_{k=1}^{N} e^{2\pi i \frac{km}{N}}\right) = \sum_{\nu=0}^{\infty} a_{\nu N}$$

omdat de uitdrukking tussen haakjes 1 is als m een veelvoud is van N en anders 0 is.

Noemen we de fout die we bij gebruikmaking van de trapeziumregel met N deelintervallen maken b_N dan hebben we dus aangetoond

(1) $$b_N = a_N + a_{2N} + a_{3N} + \ldots \qquad (N = 1,2,\ldots) .$$

Opgave: Uit (1) kan men de getallen a_n bepalen, d.w.z. uitdrukken in de getallen b_N. Bewijs dat het resultaat de volgende vorm heeft:

(2) $$a_n = \sum_{k=1}^{\infty} \mu_k b_{kn} \quad .$$

Geef een formule voor μ_k en bepaal uit (1) en (2) een relatie waaraan μ_k voldoet.

17. Zij $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ met $a_i = 0, 1, 2, 3$ of 4 $(i = 0,\ldots,k)$. We rekenen mod 5. Toon aan dat uit $f(\alpha) = 0$ volgt dat $f(\alpha^5) = 0$.

18. Beschouw de polynomen $x^2 + a_1 x + a_2$ met $a_i = 0, 1$ of 2 $(i = 1,2)$. We rekenen mod 3. Welke van deze polynomen zijn niet in factoren te ontbinden? Geef de ontbinding in irreducibele factoren van $x^8 - 1$.

19. Er zijn 16 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ met elementen 0 of 1. Als we mod 2 rekenen (gewone matrix-optelling en vermenigvuldiging) dan vormen deze matrices een ring (ga na!). Bewijs dat er in deze ring een matrix X is met $X^2 = X + I$ (hierin is I de eenheidsmatrix). Bewijs dat 0, I, X en X + I een lichaam met 4 elementen vormen.

20. (Belangrijke opgave als voorbereiding voor hoofdstuk III). Beschouw alle polynomen $\sum_{i=0}^{7} a_i x^i$ met $a_i = 0, 1$ of 2 $(i = 0,1,\ldots,7)$ en reken daarmee mod 3 èn mod $(x^8 - 1)$ (d.w.z. dat als na vermenigvuldiging een macht x^α voorkomt met $\alpha \geq 8$ de exponent α mod 8 gereduceerd wordt). Ga na dat zo een ring is gedefinieerd. In deze ring vormen alle veelvouden van $x^2 + x + 2$ een ideaal S (ga na!). Beschouw nu de 8-dimensionale vectorruimte R_8 bestaande uit de vectoren $(a_0,a_1,\ldots,a_7)$ met $a_i = 0,1,2$ $(i = 0,\ldots,7)$ en optelling etc. mod 3. Laat V c R gedefinieerd zijn door $(a_0,a_1,\ldots,a_7) \in V :\Leftrightarrow \sum_{i=0}^{7} a_i x^i \in S$. Toon aan dat V een <u>lineaire</u> deelruimte van R_8 is (dimensie?). Toon aan dat uit $(a_0,a_1,\ldots,a_7) \in V$ volgt dat $(a_7,a_0,a_1,\ldots,a_6) \in V$ (dit heet een cyclische deelruimte).

21. Op een voetbalpoolformulier staan 4 wedstrijden. Achter elke wedstrijd kan men invullen 1, 2 of 3 (voorspelling van winst, verlies of gelijkspel voor de thuisclub). Eén kolom is een viertal van dergelijke voorspellingen. Probeer met <u>zo weinig mogelijk</u> verschillende kolommen zekerheid te bereiken dat er een kolom is die 3 of 4 goede voorspellingen bevat.

22. Als we het probleem uit 1 stellen voor 5 wedstrijden is het veel moeilijker. Wat kunt U als schatting geven voor het benodigde <u>aantal</u> kolommen?

23. Via een gestoorde zender wil men een serie van 3 signalen overbrengen waarin elk signaal 0 of 1 is. We nemen aan dat er 10% kans is dat een signaal verkeerd aankomt (dus 1 i.p.v. 0 en omgekeerd). De kans dat het bericht goed overkomt is dan 72,9%. Stel nu dat er voldoende tijd is om 6 i.p.v. 3 signalen uit te zenden. Ga na dat het zinloos is de serie te herhalen. Kan men de kans op goed overkomen van het bericht vergroten? Tot welk percentage?

24. Als in de vorige opgave de storing zodanig is dat in 10% van de gevallen het signaal <u>niet</u> overkomt en in 90% goed, hoe groot is dan de kans te maken op goed overkomen van het bericht? Is herhaling van het bericht hier zinvol?

25. Zij $A = (a_{ij})$ een 8×8 matrix waarvan alle elementen ± 1 zijn. Kunnen de elementen zo gekozen worden dat $A^2 = 8I$? (I is de eenheidsmatrix).

26. Construeer een 3×3 matrix a_{ij} zo dat elke $a_{ij} = 1$, 2 of 3 en bovendien de getallen 1, 2 en 3 in iedere rij en kolom één keer voorkomen. Construeer een tweede matrix b_{ij} met dezelfde eigenschap maar nu zó dat alle 9 paren (a_{ij},b_{ij}) verschillend zijn. Beschouw nu alle 4-tallen (i,j,a_{ij},b_{ij}). Ga na dat deze 9 viertallen de "woorden" vormen van een "taal" waarin een goed verstaander slechts een half woord nodig heeft!

27. Zij H een (0,1) matrix van 4 rijen en 7 kolommen waarvan de kolommen de binaire representatie van de getallen 1 t/m 7 zijn. Beschouw alle (0,1)-rijvectoren die loodrecht staan op iedere rij van H. Hoeveel vectoren zijn dat? Toon aan dat deze vectoren de woorden zijn van een single-error-correcting code.

28. Er zijn 3 kwadraatresten mod 7 namelijk 1, 2 en 4. Beschouw de 7×7 matrix A met $a_{ij} = 1$ als $i - j + 1 \pmod 7$ kwadraatrest is en $a_{ij} = 0$ anders. Een rij van de matrix noemen we lijn, een kolom noemen we punt. Als $a_{ij} = 1$ zeggen we dat punt j ligt op de lijn i. De lijn i snijdt de lijn k in punt j als $a_{ij} = a_{kj} = 1$. Ga na dat met deze definities een meetkunde is gedefinieerd met 7 punten en 7 lijnen waarvoor door twee punten precies één lijn gaat en waarvoor twee lijnen precies één snijpunt hebben. "Evenwijdig" bestaat hier dus niet!

29. De rijen van de matrix A uit de vorige opgave zijn de 7 codewoorden van een code.

a) Als een woord ontvangen wordt met één fout kan men deze fout dan ontdekken en verbeteren?

b) Als een woord ontvangen wordt met twee fouten, wat kan men dan over het uitgezonden signaal concluderen?

c) Als van een woord slechts 4 symbolen ontvangen worden, wat kan men dan over het uitgezonden signaal concluderen?

30. Een Hamming code over GF(2) is perfect en single-error-correcting. Als een (n,k)-code over GF(q) perfect en w-error-correcting is (w > 1) welke betrekking bestaat er dan tussen n, k, q en w? Probeer getallen n, k, q en w > 1 te vinden die aan deze betrekkingen voldoen.

31. Bepaal alle oplossingen van $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = 2^k$ (n en k natuurlijk).

32. Zij α een primitief element van GF(16). Beschouw de verzameling V van alle polynomen $C(x) = c_0 + c_1x + \ldots + c_{14}x^{14}$ met coëfficiënten in GF(2) waarvoor geldt

$$C(\alpha) = C(\alpha^3) = C(\alpha^5) = 0 .$$

Toon aan dat als $c_0 + c_1x + \ldots + c_{14}x^{14} \in V$ ook

$$c_{14} + c_0x + c_1x^2 + \ldots + c_{13}x^{14} \in V .$$

Zij $\bar{V}$ de code bestaande uit de woorden $(c_0,c_1,\ldots,c_{14})$ waarvoor $c_0 + c_1x + \ldots + c_{14}x^{14} \in V$. Toon aan dat $\bar{V}$ een lineaire code is. Hoeveel information symbols bevat elk woord? Bewijs dat dit een 3-error-correcting code is.

33. Zij A een n × n-matrix waarvan alle elementen 0 of 1 zijn. Voor iedere a_{ij} in A die 0 is is de som van de elementen uit de i-de rij + de som van de elementen uit de j-de kolom $\geq$ n. Bewijs dat de som van alle elementen van A tenminste $\frac{1}{2}n^2$ is.

34. Zij A een symmetrische (0,1) matrix (d.w.z. $a_{ij} = a_{ji} = 0$ of 1) van de orde v. Zij

$$A^2 = (k-\lambda)I + \lambda J , \quad 0 < \lambda < k < v-1 \quad \text{en} \quad k-\lambda = k^2 - \lambda v .$$

Als $k-\lambda$ niet kwadraat van een geheel getal is dan heeft A precies k enen op de hoofddiagonaal. Bewijs dit.

35. Bepaal $a_1,a_2,\ldots,a_6$ zó dat de 30 verschillen $a_i - a_j \pmod{31}$ $(i \neq j)$ de getallen 1 t/m 30 zijn!