TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

DISCRETE WISKUNDE

Prof. Dr. J.J. Seidel

1971

TECHNISCHE HOGESCHOOL EINDHOVEN

ONDERAFDELING DER WISKUNDE

discrete wiskunde

prof. dr. j. j. seidel

1971

Inhoudsbeschrijving

DISCRETE WISKUNDE

J.J. Seidel

1971

Bijlage voor niet-wiskundestudenten

JdG, 29 Juli 2005

DISCRETE WISKUNDE

1971

J.J. SEIDEL

Seidel
retour !!

College Discrete Wiskunde 1971

door

J.J. Seidel

1. Inleiding

1.1. Hadamard matrices

Uit de 8 hoekpunten van een kubus kan men er vier kiezen die de hoekpunten zijn van een regelmatig viervlak. Inderdaad, neem de oorsprong van een coördinatenstelsel in het middelpunt van een kubus met ribbe 2, neem de assen evenwijdig aan de ribben, dan voldoen de punten

$$\begin{matrix}(\ 1,\ 1,\ 1)\\ (\ 1,-1,-1)\\ (-1,\ 1,-1)\\ (-1,-1,\ 1)\end{matrix}\ .\qquad \text{De matrix}\qquad \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

bevat slechts de getallen 1 en -1 en is orthogonaal. Zo'n matrix heet een Hadamard matrix van de orde 4.

Definitie. Een Hadamard matrix H_r is een vierkante matrix van de orde r, waarvan alle elementen 1 of -1 zijn, die voldoet aan

$$H_r H_r^T = r I_r .$$

Nodige voorwaarden voor het bestaan van Hadamard matrices H_r zijn

$$r = 2, \quad r \equiv 0 \pmod 4.$$

Men vermoedt dat deze voorwaarden ook voldoende zijn. Dit vermoeden is bevestigd voor alle $r < 188$ en voor oneindig veel andere waarden van r.

Opgave 1. Bewijs de nodige voorwaarden. Maak daartoe van één rij alle elementen 1, en bekijk nog twee rijen.

Een Latijns vierkant van de orde 4 bestaat uit 16 geordende drietallen uit 4 symbolen, zodat voor elk paar coördinaten elk paar symbolen precies eenmaal voorkomt.
Er zijn twee (niet-isomorfe) Latijnse vierkanten van de orde 4, namelijk de hiervoren gegeven vierkanten.

Opgave 3. Maak twee (niet-isomorfe) Latijnse vierkanten van de orde 5.

1.4. Error correcting codes

Zij V(4,3) de vectorruimte van dimensie 4 over GF(3). Het Galois lichaam GF(3) is de verzameling {0, 1,-1} met als afwijkende rekenregels 1 + 1 = -1, -1-1 = 1. De vectoren

(0, +, +, +) en (+, 0, +, -)

spannen een vlak op, dat 9 vectoren bevat:

(0, +, +, +)	(0, -, -, -)	(0, 0, 0, 0).
(+, 0, +, -)	(-, 0, -, +)	
(+, +, -, 0)	(-, -, +, 0)	
(-, +, 0, -)	(+, -, 0, +)	

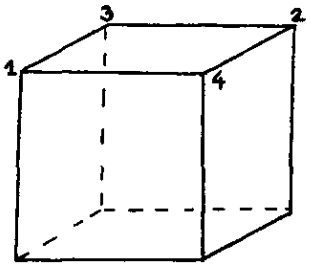
Deze 9 vectoren hebben de eigenschap dat elk paar de afstand 3 heeft. Daarbij wordt onder de afstand van twee vectoren verstaan het aantal coördinaten waarin de vectoren verschillen.
V(4,3) heeft 81 vectoren, genaamd woorden. Het vlak heet een lineaire code, en zijn 9 vectoren heten codewoorden.Onze code heeft de eigenschap dat hij één fout kan corrigeren, single-error-correcting is.
Onze code is perfect, omdat de bollen met straal 1 om de 9 codewoorden disjunct zijn en de gehele V(4,3) uitputten.

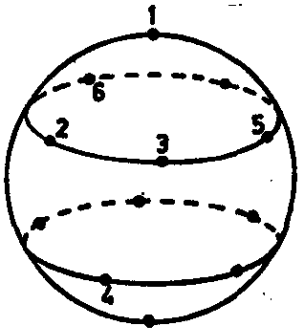
Opgave 4. Construeer 16 vectoren in V(8,2), waarvan elk paar afstand ≥ 4 heeft, uitgaande van de Hadamard matrix H_8 van opgave 2.

1.5. Gelijkhoekige rechten en grafen

Een stelsel rechten heet gelijkhoekig als de hoek tussen elk paar rechten dezelfde is. De vier diagonalen van een kubus vormen een gelijk-

hoekig stelsel met hoek arccos $\frac{1}{3}$. De zes diagonalen van een icosaëder vormen een gelijkhoekig stelsel met hoek arccos $1/\sqrt{5}$.





Neem eenheidsvectoren p_i langs de rechten en beschouw de matrix der inproducten $P = [(p_i,p_j)]$. Voor

$$A = \frac{1}{\cos \varphi}\,[P-I]$$

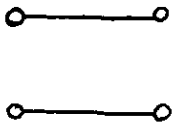
hebben wij in de voorbeelden:

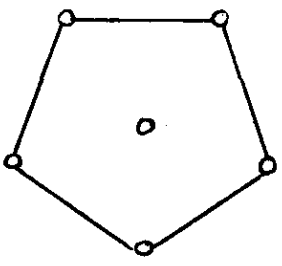
$$A_4 = \begin{bmatrix} 0 & - & + & + \\ - & 0 & + & + \\ + & + & 0 & - \\ + & + & - & 0 \end{bmatrix}; \qquad A_6 = \begin{bmatrix} 0 & + & + & + & + & + \\ + & 0 & - & + & + & - \\ + & - & 0 & - & + & + \\ + & + & - & 0 & - & + \\ + & + & + & - & 0 & - \\ + & - & + & + & - & 0 \end{bmatrix}.$$

Voor deze matrices geldt:

$(A_4-I)(A_4+3I) = 0$, $A_4J = J$; $A_6^2 = 5I$.

De matrices A_4 en A_6 zijn verbindingsmatrix van de grafen





Opgave 5. Bepaal de eigenwaarden van A_4 en A_6.

Opgave 6. Construeer 28 gelijkhoekige rechten in de 7-dimensionale ruimte. Gebruik hiertoe de matrix N van 1.2 en de vier punten van 1.1.

Opgave 7. Construeer een Hadamard matrix H_{12}, door gebruik te maken van de matrix A_6.

Bijlage Discrete Wiskunde

3. Ringen en lichamen

3.1. Definities (A en A 137)

Beschouw een verzameling V met twee productoperaties. Schrijf $(V;+,\cdot)$ en noem de operatie + de opteloperatie, de operatie $\cdot$ de vermenigvuldigoperatie. Beschouw de volgende eigenschappen:

O_1 : $\forall_{a,b\in V}\ (a+b=b+a)$, commutatieve eig.,

O_2 : $\forall_{a,b,c\in V}((a+b)+c=a+(b+c))$, associatieve eig.,

O_3 : $\forall_{a,b\in V}\ \exists!_{x\in V}\ (a+x=b)$, eig.v.eenduidige opl.

Opm. $\exists!$ betekent: er is precies één.

Opm. Als O_1, O_2, O_3 gelden, dan is er in V precies één element, schrijf 0, zodat $\forall_{a\in V}\ (a+0=0+a=a)$.

V_1 : $\forall_{a,b\in V}(a\cdot b=b\cdot a)$, commutatieve eig.,

V_2 : $\forall_{a,b,c\in V}\ ((a\cdot b)\cdot c=a\cdot(b\cdot c))$, associatieve eig.,

V_3 : $\forall_{a\neq 0,b\in V}\ \exists!_{x\in V}(a\cdot x=b)$, eig.v.eenduidige opl.

Opm. Als V_1, V_2, V_3 gelden, dan is er in V precies één element, schrijf 1, zodat $\forall_{a\in V}\ (a\cdot 1=1\cdot a=a)$.

D : $\forall_{a,b,c\in V}(a\cdot(b+c)=a\cdot b+a\cdot c)$, distributieve eig.

Def. Een lichaam is een $(V;+,\cdot)$ waarin de eigenschappen $O_{1,2,3}$, $V_{1,2,3}$, D gelden.

Def. Een ring is een $(V;+,\cdot)$ waarin de eigenschappen $O_{1,2,3}$, $V_{1,2}$, D gelden.

3.2. Voorbeelden

Vb. 1. R, Q, C, met de gewone optelling en vermenigvuldiging, zijn lichamen.

Vb. 2. Z is een ring, maar geen lichaam, omdat V_3 niet altijd geldt: $2x = 3$ heeft geen oplossing in Z.

Vb. 3. De verzameling der 2×2 matrices, met de gewone optelling en vermenigvuldiging, is een (niet-commutatieve) ring, maar geen lichaam:

$$\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & y\\ z & u\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\ \text{heeft}\ \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix},\ \begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix},\ \begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}$$

als (niet eenduidige) oplossing.

Vb. 4. De equivalentieklassen mod 6 vormen een ring, maar geen lichaam. Immers $2x \equiv 3 \pmod 6$ heeft geen, en $2x \equiv 4 \pmod 6$ heeft twee oplossingen.

Stelling. De equivalentieklassen mod p, p priem, met de optelling en vermenigvuldiging van 1.5, vormen een lichaam.

Dit is GF(p), het Galois lichaam van de orde p, p priem.

3.3. Polynoomringen (A en A 146)

Zij F een lichaam, bijvoorbeeld R, Q, C, GF(p).
Beschouw de verzameling F[x] der veeltermen

$a(x) := a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, $a_i \in F$, $a_n \neq 0$,

$b(x) := b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$, $b_i \in F$, $b_m \neq 0$.

Neem $n \geq m$ en definieer als volgt:

$a(x) = b(x)$ als $a_i = b_i$, $i = 1,\ldots,n$,

$$a(x) + b(x) := \sum_{i=0}^{n} (a_i+b_i)x^i ,$$

$$a(x) \cdot b(x) := \sum_{k=1}^{m+n} c_k x^k \text{ met } c_k = \sum_{i=0}^{k} a_i\, b_{k-i} ,$$

$0(x) := 0$,

$1(x) := 1$.

Onder deze definities is $(F[x];+,\cdot)$ een ring, maar niet een lichaam.
Inderdaad, er behoeft niet een veelterm y(x) te bestaan zodat

$a(x) = y(x)\, b(x)$, bijv. $(x+2) = y(x)\,(x+3)$.

De ring F[x] heeft wel de eigenschap dat uit

$a(x) \cdot b(x) = 0$ volgt $a(x) = 0$ of $b(x) = 0$.

Van de middelbare school kennen wij de

Deelalgorithme: Bij veeltermen a(x) van graad n, en b(x) van graad m, $n \geq m$, bestaan eenduidig veeltermen q(x) van graad n-m, en r(x) van graad $\leq m-1$, zodat $a(x) = b(x) \cdot q(x) + r(x)$.

3.4. Het Galois lichaam $GF(p^k)$, p priem

Zij $F = GF(p)$. Zij $f(x)$ een veelterm van de graad k over F, dus een veelterm met als coëfficiënten gehele getallen modulo p. Zij $f(x)$ irreducibel, dat is, niet het produkt van twee veeltermen van graad $< k$. Definieer nu:

$a(x) \equiv b(x) \pmod{f(x)}$ door $a(x) - b(x) = f(x)\, v(x)$

voor zekere veelterm $v(x)$. Wij gaan dus rekenen modulo $f(x)$ van graad k. Dit betekent dat de veeltermen kunnen worden teruggebracht tot veeltermen van de vorm

$$c_0 + c_1 x + \ldots + c_{k-1}\, x^{k-1} .$$

Bovenstaande relatie is een equivalentie relatie.

Stelling. De equivalentieklassen mod $f(x)$ vormen een lichaam van de orde p^k, het Galois lichaam $GF(p^k)$.

Bewijs. Elke coëfficiënt c_i doorloopt de p elementen van GF(p). Totaal zijn er dus p^k veeltermen

$$c_0 + c_1 x + \ldots + c_{k-1}\, x^{k-1} .$$

Om te bewijzen dat de equivalentieklassen niet slechts een ring, doch zelfs een lichaam vormen, moeten wij de eigenschap V_3 der eenduidige oplossing bewijzen.
Laat $a(x)$ een gegeven equivalentieklasse $\neq 0(x)$ voorstellen. Laat $c(x)$ alle equivalentieklassen mod $f(x)$ doorlopen. Dan doorloopt ook $a(x)\, c(x)$ alle equivalentieklassen mod $f(x)$. Inderdaad, stel

$$a(x) \cdot c(x) \equiv a(x) \cdot d(x) \pmod{f(x)},$$

$$a(x)\,[c(x) - d(x)] = f(x) \cdot v(x) .$$

$a(x)$ heeft graad $< k$, en $c(x) - d(x)$ heeft graad $< k$. Omdat $f(x)$ irreducibel van graad k is, moet $c(x) = d(x)$. De conclusie is dat er een $c(x)$ is zodat

$$a(x) \cdot c(x) = b(x) ,$$

dus dat de equivalentieklassen een lichaam vormen.
Voor voorbeelden zij verwezen naar D.W. 17.

College Discrete Wiskunde 1971

Hoofdstuk 4. Orthogonale matrices.

4.1. Het Legendre symbool

Het Galois lichaam GF(q), $q = p^k$, $p \neq 2$ priem, bevat, behalve het nul-element 0, nog $\frac{1}{2}(q-1)$ kwadraten en $\frac{1}{2}(q-1)$ niet-kwadraten. Dit is op twee manieren in te zien:

(i) $GF(q) \setminus \{0\} = \{w, w^2, w^3, \ldots, w^{q-1} = 1\}$, w primitief.

(ii) $x^2 = y^2$ ddan als $x = \pm y$ in GF(q).

Def. Het Legendre symbool $\chi(a)$ van $a \in GF(q)$ is

$$\chi(a) := \begin{cases} 0 & \text{als } a = 0, \\ 1 & \text{als a is kwadraat,} \\ -1 & \text{als a is niet-kwadraat.} \end{cases}$$

Eigenschap 1. $\chi(ab) = \chi(a)\ \chi(b)$.

Bewijs: verifieer, voor $a \neq 0$, $b \neq 0$ met de primitieve w.

Eigenschap 2. Voor $q \equiv 1 \pmod 4$ is $\chi(-1) = 1$,
voor $q \equiv -1 \pmod 4$ is $\chi(-1) = -1$.

Bewijs: zij w primitief in GF(q), dan $w^{\frac{1}{2}(q-1)} = -1$.

Eigenschap 3. $\sum_{a \in GF(q)} \chi(a) = 0$.

Bewijs: er zijn evenveel kwadraten als niet-kwadraten.

Eigenschap 4. $\sum_{a \in GF(q)} \chi(a)\ \chi(a+b) = -1$, voor $b \neq 0$.

Bewijs: Stel a+b=ca. Als a doorloopt $GF(q) \setminus \{0\}$, dan c doorloopt $GF(q) \setminus \{1\}$. Inderdaad,

$a_1 + b = ca$, $a_2 + b = ca_2$, dan $(a_1 - a_2)(1-c) = 0$,

dus $a_1 = a_2$, omdat $c \neq 1$ wegens $b \neq 0$. Nu is

$$\sum_{a \neq 0} \chi(a)\ \chi(a+b) = \sum_{a \neq 0} \chi(a^2 c) = \sum_{c \neq 1} \chi(c) = \sum_{c} \chi(c) - \chi(1) = 0 - 1 = -1.$$

4.2. Paley-matrices [4], p.29.

Stelling. De $q \times q$ matrix $S = [\chi(a_r - a_k)]$, waar a_r en a_k de elementen van GF(q) doorlopen, voldoet aan

$SS^T = q\,I - J$, $Sj = j\,S = 0$.

Bewijs. Elke rij van S bevat eén 0 en q-1 elementen ± 1.
Het inproduct van de rijen r en s is wegens eig.4 $\sum_k \chi(a_r - a_k)\,\chi(a_s - a_k) = -1$ voor $r \neq s$ en q-1 voor r = s. Voorts is de som van elementen van elke rij nul, wegens eig.3. Dit bewijst de bewering, als we noemen:
J = de matrix waarvan alle elementen 1 zijn,
j = de kolomvector waarvan alle elementen 1 zijn.

Stelling. De $(q+1) \times (q+1)$ matrix

$$C = \begin{bmatrix} 0 & j^T \\ j & \chi(-1) \\ & \chi(a_r - a_k) \end{bmatrix}, \quad a_r,\ a_k \in GF(q),$$

is symmetrisch voor $q \equiv 1 \pmod 4$, scheef voor $q \equiv -1 \pmod 4$ en voldoet aan

$$CC^T = q\,I\ .$$

Bewijs. Met eigenschap 2 en de vorige stelling.

Voorbeeld. GF(5) = {0, 1, 2, 3, 4}
met $\chi(a) = 0, 1, -1, -1, 1$.

GF(7) = {0, 1, 2, 3, 4, 5, 6}
met $\chi(a) = 0, 1, 1, -1, 1, -1, -1$.

Daarom zijn de volgende matrices orthogonaal:

$$C_6 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}, \quad C_8 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 0 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 0 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 0 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{bmatrix}$$

4.3. Conferentie-matrices

Een conferentie-matrix C van orde v is een vierkante matrix van orde v met diagonaal elementen 0 en overige elementen $\pm$ 1, die voldoet aan

$$C\,C^T = (v-1)\,I.$$

Stelling. Nodige voorwaarde voor het bestaan van een symmetrische [scheve] C-matrix van de orde v is dat
$v \equiv 2 \pmod 4$ [$v = 2$ en $v \equiv 0 \pmod 4$] .

Bewijs. Voor $v = 2$ triviaal. Neem $v > 3$, normaliseer en permuteer rijen en kolommen zodat de eerste drie rijen zijn

0	+	+	—+—	—+—	—+—	—+—
	0	+	—+—	—+—	———	———
		0	—+—	———	—+—	———

met 1, 1, 1, x, y, z, u kolommen. Uit de inproducten concluderen wij in het symmetrische en het scheve geval respectievelijk:

$1 + x + y + z + u = v - 1$	$1 + x + y + z + u = v - 2$
$1 + x + y - z - u = 0$	$1 + x + y - z - u = 0$
$1 + x - y + z - u = 0$	$-1 + x - y + z - u = 0$
$1 + x - y - z + u = 0$	$1 + x - y - z + u = 0$

$4(x+1) = 4y = 4z = 4u = v - 2$, $\quad 4(x+1) = 4(y+1) = 4z = 4(u+1) = v$.

Stelling. Nodige voorwaarde voor het bestaan van een symmetrische C-matrix van de orde v is

$$v - 1 = a^2 + b^2 \text{ , a en b geheel.}$$

Bewijs: zie [1] en [5] .

In 4.2 werden speciale C-matrices van de orde $v = 1 + p^k$, $p \neq 2$ priem, geconstrueerd. Zij heten Paley-matrices, naar R.E.A.C. Paley (1933).
Er bestaan ook andere C-matrices, bijv. van de orde v = 226, zie [2].
Het kleinste onopgeloste geval is v = 46.

4.4. Hadamard matrices

Def. Een Hadamard matrix van de orde n is een vierkante matrix H, waarvan alle elementen $\pm$ 1 zijn en waarvoor geldt $H\,H^T = n\,I$.

Stelling. Als H_n bestaat, dan is $n = 1$, $n = 2$, $n \equiv 0 \pmod 4$.

Bewijs: zie [4], p. 28.

Stelling. Als C_n een scheve conferentie matrix is, dan is $H_n = C_n + I_n$ een Hadamard matrix.

Bewijs. $C^T = -C$, dus

$$(C+I)(C^T+I) = CC^T + C + C^T + I = (n-1)\, I + 0 + I = n\, I.$$

Stelling. Als C_n een symmetrische conferentie matrix is, dan is

$$H_{2n} = \begin{bmatrix} C_n + I_n & C_n - I_n \\ C_n - I_n & -C_n - I_n \end{bmatrix}$$

een Hadamard matrix van de orde 2n.

Bewijs.

$$\begin{bmatrix} C+I & C-I \\ C-I & -C-I \end{bmatrix}^2 = \begin{bmatrix} (C+I)^2 + (C-I)^2 & (C+I)(C-I) - (C-I)(C+I) \\ (C-I)(C+I) - (C+I)(C-I) & (C-I)^2 + (C+I)^2 \end{bmatrix} =$$

$$\begin{bmatrix} 2C^2 + 2I & 0 \\ 0 & 2C^2 + 2I \end{bmatrix} = \begin{bmatrix} 2nI & 0 \\ 0 & 2nI \end{bmatrix}.$$

4.5. Kronecker product

Het Kronecker product $A \times B$ van de vierkante matrices $A = [a_{ij}]$ van orde m, en $B = [b_{kl}]$ van orde n, is de matrix van orde mn gedefinieerd door:

$$A \times B = \begin{bmatrix} a_{11} B & \cdots & a_{1m} B \\ \vdots & & \vdots \\ a_{m1} B & \cdots & a_{mm} B \end{bmatrix}.$$

Eigenschappen:

$(A \times B) \times C = A \times (B \times C)$,

$(A \times B)^T = A^T \times B^T$,

$(A \times B)(C \times D) = (AC) \times (BD)$,

$(\alpha A+\beta B) \times (\gamma C+\delta D) = \alpha\gamma A \times C + \alpha\delta A \times D + \beta\gamma B \times C + \beta\delta B \times D$.

Stelling. Als H_m en H_n Hadamard matrices zijn, dan is $H_m \times H_n$ Hadamard matrix van de orde mn.

Bewijs.

$(H_m \times H_n)(H_m \times H_n)^T = (H_m \times H_n)(H_m^T \times H_n^T) =$

$= (H_m H_m^T) \times (H_n H_n^T) = mn\, I_m \times I_n = mn\, I_{mn}$.

Opm. Voor een algemene definitie van Kronecker producten, zie [4], p. 27.

4.6. Toepassingen

A. Zij $M = [m_{ij}]$ een vierkante matrix van orde n met elementen $-1 \leq m_{ij} \leq 1$, dan geldt

$$\det M \leq n^{\frac{1}{2}n},$$ ongelijkheid van Hadamard,

met gelijkheid ddan als M een Hadamard matrix is (zie [3] en [7]).

B. De n directeuren van een concern wensen hun conferenties per telefoon te houden, zodanig dat elke directeur met elke collega kan spreken en dat de anderen hun discussies kunnen horen. De constructie van een daarvoor geschikt conferentie-netwerk (een lineaire, verliesvrije, frequentie-onafhankelijke, reciproke n-poort, met uniforme verdeling en zonder reflectie) is gelijkwaardig met de constructie van een symmetrische conferentie matrix. Zie Belevitch [1].

C. Een tournooi is een halve competitie tussen n spelers, waarbij slechts winst en verlies, geen remise, is toegestaan. Een tournooi kan worden beschreven door een gerichte graaf, en ook door een scheve (+,-) matrix met nuldiagonaal. Een S-matrix van orde q volgens Paley is een bijzonder tournooi, waarin elke speler even vaak wint als verliest, en elk paar spelers in $\frac{1}{4}(q-3)$ spelers hun gezamenlijke meerdere erkennen.

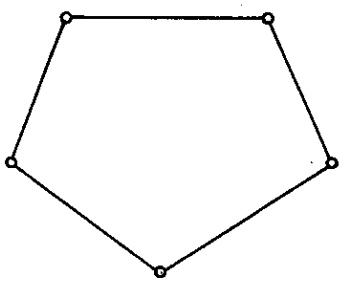
D. Wat is de "beste" strategie, teneinde n objecten te wegen in n wegingen, onder zekere voorwaarden en met een definitie van "beste"? Beschrijf de strategie door een matrix $C = [c_{ij}]$ met

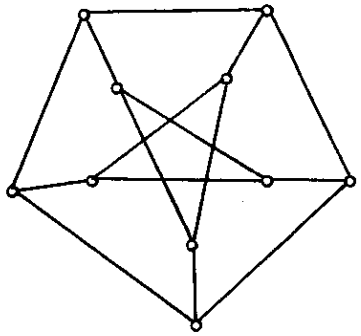
$c_{ij} = 1$, als object j tijdens weging i op de linker schaal,
$c_{ij} = -1$, als object j tijdens weging i op de rechter schaal,
$c_{ij} = 0$, als object j tijdens weging i niet voorkomt.

Voor $n \equiv 0 \pmod 4$ is de beste weging volgens een Hadamard matrix, voor $n \equiv 2 \pmod 4$ volgens een conferentie matrix. Zie Raghavarao [6].

E. Voor toepassingen op coding theory zie het betreffende hoofdstuk.

F. Gewone grafen laten zich beschrijven door vierkante symmetrische matrices met nul-diagonaal en overige elementen ± 1. Wij geven twee voorbeelden. Zie verder [8].





$$A = \begin{bmatrix} 0 & - & + & + & - \\ - & 0 & - & + & + \\ + & - & 0 & - & + \\ + & + & - & 0 & - \\ - & + & + & - & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} A & J-2I \\ J-2I & -A \end{bmatrix}$$

$A^2 = 5\ I-J,\ Aj = 0\ ,$

$B^2 = 9\ I,\ Bj = 3j\ .$

4.7. Literatuur

[1] V. Belevitch, Conference networks and Hadamard matrices, Ann.Soc.Scient. Bruxelles 82 (1968), 13-32.

[2] J.M. Goethals-J.J.Seidel, Orhtogonal matrices with zero diagonal, Canad. Journ. Math. 19 (1967), 1001-1010.

[3] M. Hall, Combinatorial theory (Blaisdell 1967).

[4] J.H. van Lint, Discrete wiskunde, THE syllabus (1970).

[5] J.H. van Lint-J.J. Seidel, Equilateral point sets in elliptic geometry, Kon.Ned. Akad. Wetensch.Amst.Proc.A 69 (= Indag.Math.28)(1966), 335-348.

[6] D. Raghavarao, Some aspects of weighing designs, Ann.Math.Statist. 31 (1960), 878-884.

[7] H.J. Ryser, Combinatorial mathematics, Carus monograph (1963).

[8] J.J. Seidel, Strongly regular graphs, in W.T. Tutte, Recent progress in combinatorics, New York (1969), 185-198.

[9] J.H.van Lint, J.J. Seidel, P.C. Baayen, Colloquium Discrete Wiskunde, Math.Centrum Syllabus 5 (1968).

A.1. Find the three numbers n less than 10,000 with $\varphi(n) \geq 60$.
Note $n = 7! \Rightarrow \varphi(7!) = 60$, but there are two numbers with $\varphi(n) > 60$, $n < 10{,}000$.

A.2. 125 dieren van drie soorten, mussen, eenden en ganzen kosten in totaal ƒ125,--.
Mussen kosten ƒ0,05, eenden kosten ƒ1,-- en ganzen kosten ƒ5,--.
Bepaal alle oplossingen.

A.3. Vier schipbreukelingen stranden op een eiland. Het enige voedsel dat ze vinden is een berg cocosnoten onder een grote palm. De nacht valt en iedereen slaapt. Eén van de schipbreukelingen wordt wakker en besluit alvast zijn vierde deel van de berg cocosnoten in veiligheid te brengen. Al tellend merkt hij, dat er één cocosnoot teveel is voor een eerlijke verdeling. Die ene eet hij maar snel op, en hij verbergt zich met zijn cocosnoten op een hoek van het eiland. Een tweede schipbreukeling wordt wakker en komt op hetzelfde idee. Ook nu is er één cocosnoot over en ook deze wordt snel verobert. De geschiedenis herhaalt zich, totdat alle vier schipbreukelingen in het donker op een hoek van het eiland zitten, denkend dat ze hun eerlijke portie alvast te pakken hebben! Hoeveel cocosnoten lagen er onder de palmboom vóór het onderlinge wantrouwen zich van de schipbreukelingen meester maakte?

Discrete Wiskunde 1971.

Hoofdstuk 5. Block designs

5.1. Steiner tripel systemen

Zij V een verzameling van v elementen, zeg punten. Een tripel is een deelverzameling van 3 punten. Bestaat er een collectie tripels zo, dat elk paar punten in precies één tripel zit? Dan moet v aan voorwaarden voldoen.
Inderdaad,
elk punt zit met elk van de v−1 andere punten in een tripel,

dus zit in $\frac{1}{2}(v-1)$ tripels;

totaal zijn er $\frac{1}{3}\, v \cdot \frac{1}{2}(v-1) = \frac{1}{6}\, v(v-1)$ tripels.

Hieruit volgt, dat v moet voldoen aan

$$v \equiv 1 \text{ of } 3 \pmod 6.$$

Omgekeerd kan men bewijzen dat deze voorwaarde voldoende is. Zo'n collectie tripels heet een Steiner tripel systeem, naar Jacob Steiner (1853), en heeft de eigenschap:

Er zijn v punten en $b = \frac{1}{6}\, v(v-1)$ tripels,

elk tripel bevat $k = 3$ punten, door elk punt gaan $r = \frac{1}{2}\,(v-1)$ tripels,

elk paar punten ligt in $\lambda = 1$ tripel.

$(v, k, b, r, \lambda) = (v, 3, \frac{1}{6}\, v(v-1), \frac{1}{2}\,(v-1), 1)$.

Existentie ddan als $v \equiv 1,3 \pmod 6$.

Voorbeeld 1. $(v, k, b, r, \lambda) = (7, 3, 7, 3, 1)$.

Dit is de meetkunde van Fano, zie Inleiding 1.2, met punt-tripel incidentie matrix

$$N = \operatorname{circ}\ (1\ 1\ 0\ 1\ 0\ 0\ 0).$$

Deze matrix voldoet aan

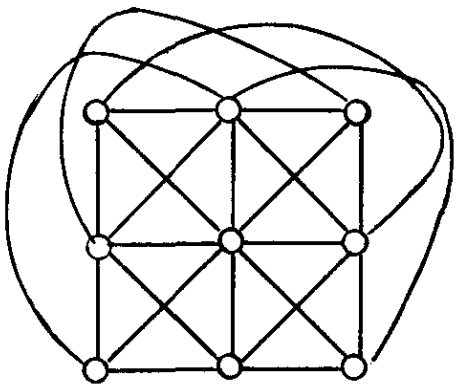
$$Nj = 3j\ ,\ j^T N = 3j^T\ ,\ NN^T = 2I + J\ .$$

Voorbeeld 2. $(v, k, b, r, \lambda) = (9, 3, 12, 4, 1)$.

De punt-tripel incidentie matrix N voldoet aan

$Nj = 4j$, $j^T N = 3j^T$, $NN^T = 3I + J$.

Hieraan voldoet het tripel systeem aangegeven door de volgende 12 lijnen, later AG(2,3) te noemen.



Voorbeeld 3. $(v, k, b, r, \lambda) = (13, 3, 26, 6, 1)$.

$Nj = 6j$, $j^T N = 3j^T$, $NN^T = 5I + J$.

Hieraan voldoet $N = [N_1 \quad N_2]$ met

$N_1 = \text{circ}\ (1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0)$,
$N_2 = \text{circ}\ (0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0)$.

Voorbeeld 4. $(v, k, b, r, \lambda) = (15, 3, 35, 7, 1)$.

$Nj = 7j$, $j^T N = 3j^T$, $NN^T = 6I + J$.

Hieraan voldoen de 15 punten en 35 lijnen van PG(3,2).

Opmerking.

Voorbeeld 3 heeft 2 oplossingen, voorbeeld 4 heeft 80 oplossingen.

5.2. Block designs

Lemma. Zij M een (rechthoekige of vierkante) matrix. Dan hebben MM^T en M^TM dezelfde eigenwaarden $\neq 0$, met dezelfde multipliciteiten.

Bewijs. Zij $\lambda \neq 0$ eigenwaarde van MM^T, met eigenvector $\underline{x} \neq \underline{0}$.

$$MM^T \underline{x} = \lambda \underline{x} \ , \ M^T \underline{x} \neq \underline{0} \ , \ M^T MM^T \underline{x} = \lambda M^T \underline{x} \ .$$

Dus λ is eigenwaarde van M^TM, met eigenvector $M^T \underline{x}$.
Evenzo, als $\alpha\underline{x} + \beta\underline{y} \neq \underline{0}$ in de eigenruimte bij de eigenwaarde $\lambda \neq 0$ van MM^T, dan is $\alpha M^T \underline{x} + \beta M^T \underline{y} \neq \underline{0}$ in de eigenruimte bij de eigenwaarde λ van M^TM. Q.e.d.

Zij V een eindige verzameling van v punten. De delen van V heten blokken.
Een IBD, incomplete block design, is een verzameling van, zeg b, blokken.
Een BIBD, balanced IBD, is een IBD met

(1) elk blok heeft evenveel, zeg k, elementen,
(2) elk paar punten ligt in evenveel, zeg λ, blokken,
(3) $0 < \lambda$ en $k < v-1$.

Voor een BIBD gelden dan de volgende eigenschappen:

(4) elk punt ligt in evenveel, zeg r, blokken,
(5) $r(k-1) = \lambda(v-1)$, $bk = vr$,

die wij weldra zullen bewijzen.

Een BIBD, zeg block design, wordt beschreven door zijn $v \times b$ punt-blok incidentie matrix $N = [n_{ij}]$ gedefinieerd door

$$n_{ij} = \begin{cases} 1 \text{ als punt } i \text{ ligt in blok } j, \\ 0 \text{ als punt } i \text{ niet ligt in blok } j. \end{cases}$$

Volgens definitie geldt dat

(1) elke kolom van N heeft k enen,
(2) elk paar rijen van N heeft inproduct λ.

Stel de i^e rij van N heeft r_i enen. Tel het aantal paren $\{h,j\}$ waarvoor geldt

$$(n_{ij}, n_{hj}) = (1,1).$$

Volgens (2) is dit aantal $(v-1)\lambda$. Volgens (1) is dit aantal $r_i(k-1)$.
Hieruit volgt:

(4) elke rij van N heeft evenveel, zeg r, enen, en $r(k-1) = \lambda(v-1)$.

Tel nu op twee manieren het totale aantal enen in N, dan volgt $vr = bk$.

In termen van de punt-blok incidentie matrix N wordt een block design dus gedefinieerd door

$$NN^T = (r-\lambda)\, I + \lambda J\ ,\quad Nj = rj\ ,\quad j^T N = kj\ ,$$
$$vr = bk\ ,\quad r(k-1) = \lambda(v-1)\ .$$

Voorbeeld 1. Steiner tripel systemen.

Voorbeeld 2. N = circ (1 1 1 0 1 0 0)

definieert een block design met $(v, k, b, r, \lambda) = (7, 4, 7, 4, 2)$.

Voorbeeld 3. Een block design met $(v, k, b, r, \lambda) = (8, 4, 14, 7, 3)$ wordt gegeven door de 8 hoekpunten van een kubus en de volgende 14 blokken: de 6 zijvlakken, de 6 diagonaalvlakken, de 2 regelmatige viervlakken gevormd door de hoekpunten. Een betere voorstelling wordt verkregen door de 8 punten van de vectorruimte van dimensie 3 over GF(2), en de 14 vlakken

$x = 0,\ y = 0,\ z = 0,\ x+y = 0,\ x+z = 0,\ y+z = 0,\ x+y+z = 0,$
$x = 1,\ y = 1,\ z = 1,\ x+y = 1,\ x+z = 1,\ y+z = 1,\ x+y+z = 1.$

Stelling (Fisher). In een block design geldt $v \leq b$.

Bewijs. De eigenwaarden van de $v \times v$ matrix

$$NN^T = (r-\lambda)\, I + \lambda J$$

zijn $(v-1)$ maal $(r-\lambda)$ en éénmaal
$r - \lambda + \lambda v = rk$.

Deze eigenwaarden zijn $\neq 0$. Volgens het Lemma heeft de $b \times b$ matrix $N^T N$ tenminste deze v eigenwaarden, benevens eventueel $b-v$ eigenwaarden 0. Daarom is $b \geq v$.
Een BIBD met $b = v$ heet een symmetrisch block design. De matrix N is dan vierkant, en $r = k$, en we hebben
$Nj = kj$, $j^T N = kj^T$, $NN^T = N^T N = (k-\lambda)\, I + \lambda J$;

$$(\det N)^2 = k^2 (k-\lambda)^{v-1}\ ,$$

dus $k-\lambda$ moet een kwadraat zijn.
Een projectief vlak PG(2,n) van orde $n > 1$ is een symmetrisch block design met

$$b = v = n^2 + n + 1,\ r = k = n + 1,\ \lambda = 1.$$

Voorbeeld. De meetkunde van Fano, zie 1.2.
Omtrent het bestaan van PG(2,n) is het volgende bekend.

Stelling. $PG(2,p^m)$, p priem, bestaat, zie Hfdst. 6.

Stelling. Als PG(2,n) bestaat, en $n \equiv 1$ of 2 (mod 4),
dan geldt $n = a^2 + b^2$, a en b geheel.

Een gevolg hiervan is, dat PG(2,6) niet bestaat. Het bestaan van PG(2,10) is een open probleem.

5.3. Block designs en orthogonale matrices

Stelling. Een genormaliseerde Hadamard matrix van de orde $4t \geq 8$ is equivalent met een symmetrisch block design met parameters
$(v, k, \lambda) = (4t-1, 2t-1, t-1)$.

Bewijs. Schrijf de Hadamard matrix volgens

$$H = \begin{bmatrix} 1 & j^T \\ j & R \end{bmatrix}$$

dan voldoet de vierkante R van orde 4t-1 wegens $HH^T = 4tI$ aan

$$RR^T = 4tI - J,\ Rj = -j,\ j^TR = -j^T.$$

De incidentie matrix N van het symmetrische block design voldoet aan

$$NN^T = tI + (t-1)\,J,\ Nj = (2t-1)\,j,\ j^TN = (2t-1)\,j^T.$$

Het verband tussen R en N wordt gegeven door

$$R = 2N - J\ .$$

Voorbeeld: opgave 2 van de Inleiding.

Stelling. Als er een C-matrix van orde n bestaat, dan is er een block design met parameters
$(v, k, b, r, \lambda) = (n, \frac{1}{2}n, 2n-2, n-1, \frac{1}{2}n-1)$.

Bewijs. Normaliseer de C-matrix volgens

$$C = \begin{bmatrix} 0 & j^T \\ \pm j & S \end{bmatrix}$$

dan voldoet de matrix S, van orde n-1, aan

$$SS^T = (n-1)\,I - J\ ,\ Sj = 0,\ j^TS = 0^T\ .$$

Het gevraagde block design wordt nu gegeven door

$$N = \begin{bmatrix} j^T & 0^T \\ \frac{1}{2}(J-S-I) & \frac{1}{2}(J-S+I) \end{bmatrix}\ .$$

5.4. Toepassingen

Voor toepassingen zie D.W. p.45, en het hoofdstuk over codes.

Hoofdstuk 6. Eindige meetkunde

6.1. Vectorruimten over Galois lichamen

Definitie. V(n,q) is de vectorruimte van de dimensie n, waarbij de getallen worden genomen uit het Galois lichaam GF(q).

De lineaire algebra van V(n,q) heeft veel gemeen met de gewone lineaire algebra over R, het lichaam der reële getallen. Er zijn echter ook verschillen, bijvoorbeeld omdat het aantal vectoren van V(n,q) eindig is, nl. q^n.

Voorbeeld. V(3,2) heeft 8 lineaire vectoren (x,y,z), met coördinaten 0 of 1.

Voorbeeld. V(2,3) heeft 9 ternaire vectoren (x,y), met coördinaten 0, 1, -1.

Zij A(s,n; q) het aantal lineaire deelruimten V(s,q) van V(n,q).

Stelling. $A(1,n;\ q) = A(n-1,n;\ q) = \frac{q^n-1}{q-1}$,

$$A(s,n;\ q) = \prod_{i=1}^{s} \frac{q^{n+1-i}-i}{q^i-1} .$$

Bewijs. Elke rechte door $\mathcal{O}$ bevat behalve $\mathcal{O}$ nog q-1 vectoren. Daarom zijn er $(q^n-1)/(q-1)$ rechten door $\mathcal{O}$, en evenveel hypervlakken door $\mathcal{O}$. Het aantal der V(s+1,q) in V(n,q), die een gegeven V(s,q) bevatten, is

$$\frac{q^n-q^s}{q^{s+1}-q^s} = \frac{q^{n-s}-1}{q-1} .$$

Daarom geldt

$$A(s,s+1;\ q)\ A(s+1,n;\ q) = A(s,n;\ q)\ \frac{q^{n-s}-1}{q-1} .$$

Wegens $A(s,s+1;\ q) = (q^{s+1}-1)/(q-1)$ volgt het gestelde.

Voorbeeld. V(3,2) bevat 7 rechten en 7 vlakken door $\mathcal{O}$.
Elk vlak door $\mathcal{O}$ bevat 3 rechten door $\mathcal{O}$.

Voorbeeld. V(2,q) bevat q+1 rechten door $\mathcal{O}$.

Voorbeeld. V(3,q) bevat q^2+q+1 rechten, en
q^2+q+1 vlakken door $\mathcal{O}$.

Voorbeeld. V(4,2) bevat 15 rechten, 35 vlakken, en 15 drie-ruimten door $\mathcal{O}$.

6.2. Block designs uit V(n,q)

Stelling. De V(1,q) en de V(s,q) van V(n,q), $1 < s < n$, vormen de punten en de blokken van een block design met

$v = A(1,n; q)$, $k = A(1,s; q)$, $b = A(s,n; q)$,

$r = A(s-1, n-1; q)$, $\lambda = A(s-2, n-2; q)$.

Dit block design is symmetrisch ddan als $n = n-1$.

Bewijs. Elke V(s,q) bevat evenveel V(1,q), namelijk $(q^s-1)/(q-1)$. Voorts liggen twee gegeven rechten door $\mathcal{O}$ in een aantal λ deelruimten V(s,q), dat onafhankelijk is van die rechten. Inderdaad, zo'n V(s,q) is bepaald door s van de n basisvectoren van V(n,q), waarvan er twee langs de gegeven rechten kunnen worden gekozen. Er zijn dus s-2 basisvectoren vrij te kiezen uit de overige n-2 basisvectoren van V(n,q). Daarom is $\lambda = A(s-2, n-2; q)$.

Voorbeeld. De 7 rechten en de 7 vlakken door $\mathcal{O}$ van V(3,2) vormen PG(2,2).

Voorbeeld. De 15 rechten en de 15 drie-ruimten door $\mathcal{O}$ van V(4,2) vormen $(v,k,\lambda) = (15, 7, 3)$.

Voorbeeld. De 15 rechten en de 35 vlakken door $\mathcal{O}$ van V(4,2) vormen $(v,k,b,r,\lambda) = (15, 3, 35, 7, 1)$.

6.3. Het projectieve vlak PG(2,q)

Stelling. PG(2,q), $q = p^m$, p priem, met

$$b = v = q^2 + q + 1, \quad r = k = q + 1, \quad \lambda = 1,$$

bestaat.

Bewijs. Pas de stelling uit 6.2 toe op V(3,q), namelijk op de $(q^3-1)/(q-1)$ rechten door $\mathcal{O}$ en de $(q^3-1)/)q-1)$ vlakken door $\mathcal{O}$. Elk vlak door $\mathcal{O}$ bevat q+1 rechten door $\mathcal{O}$ en door elk tweetal rechten door $\mathcal{O}$ gaat één vlak.

Bij projectieve vlakken is men gewend om, in plaats van over punten en blokken, te spreken over punten en lijnen. Blijkbaar geldt in PG(2,n)

P1. Door elk paar punten gaat één lijn.

P2. Elk paar lijnen heeft één punt gemeen.

P3. Er zijn 4 verschillende punten waarvan geen drietal op één lijn ligt.

Projectieve vlakken laten zich ook omgekeerd uit deze 3 axioma's opbouwen (zie D.W. p.38, 39).

Wanneer uit een projectief vlak één lijn ℓ en de punten van die lijn worden weggelaten, dan blijven er over n^2 punten en $n(n+1)$ lijnen, die het z.g. affiene vlak AG(2,n) vormen. Twee lijnen heten evenwijdig, wanneer ze in de oorspronkelijke PG(2,n) een snijpunt op ℓ hebben. De eigenschappen P1, P2, P3 gaan over in de bekende axioma's van de vlakke meetkunde.

Voorbeeld. Voor AG(2,3) zie voorbeeld 2 van 5.1.

6.4. 3-designs

Een 3-design $(v, k, b_0, b_1, b_2, b_3)$ is een verzameling V van v punten en een collectie van b_0 blokken zodat

(1) elk blok heeft k punten,

(2) elk drietal punten van V ligt in b_3 blokken.

Zij b_i het aantal blokken dat gaat door de punten $P_1, \ldots, P_i$.

Stelling. $b_i(k-i) = b_{i+1}(v-i)$, $i = 0,1,2$,
dus b_1 en b_2 zijn onafhankelijk van de keuze der punten P_1, P_2.

Bewijs. De blokken P_1 hebben k-1 overige punten.
Wegens (2) ligt elk paar punten $\neq P_1$ in b_3 van zulke blokken.
Op $V \setminus \{P_1\}$ hebben wij dus een block design met

$v^* = v-1$, $k^* = k-1$, $b^* = b_1$, $r^* = b_2$, $\lambda^* = b_3$.

Het gestelde volgt uit de betrekkingen

$$b^*k^* = v^*r^*, \quad (v^*-1)\lambda^* = r^*(k^*-1).$$

Voorbeeld 1. Beschouw in V(3,2) alle verzamelingen van 4 verschillende vectoren met som 0. Dit is een 3-design met
$(v, k, b_0, b_1, b_2, b_3) = (8, 4, 14, 7, 3, 1)$.

Voorbeeld 2. Beschouw in V(4,2) alle verzamelingen van 4 verschillende vectoren met som 0. Dit is een 3-design met
$(v, k, b_0, b_1, b_2, b_3) = (16, 4, 140, 35, 7, 1)$.

Voorbeeld 4. Beschouw in V(4,2) alle verzamelingen van 8 verschillende vectoren met som 0. Dit is een 3-design met
$(v, k, b_0, b_1, b_2, b_3) = (16, 8, 30, 15, 7, 3)$.

Voorbeeld 4. Beschouw in V(4,2) alle verzamelingen van 6 verschillende vectoren met som 0. Geen twee vectoren in een blok hebben som 0.
Als 3 vectoren in een blok,dan zit hun som niet in dat blok. Daarom is $b_3 = 16$ en $(v, k, b_0, b_1, b_2, b_3) = (16, 6, 448, 168, 56, 16)$.

Hoofdstuk 7. Latijnse vierkanten

7.1. Definitie

Een Latijns vierkant van de orde n is een vierkante matrix van de orde n, waarvan elke rij en elke kolom een permutatie is van n symbolen $\{1,2,\ldots,n\}$. Twee Latijnse vierkanten van de orde n zijn orthogonaal, als hun superpositie elk van de n^2 geordende paren (i,j) met $i,j \in \{1,2,\ldots,n\}$ precies eenmaal bevat. Neem verder $n > 2$.

Voorbeeld.

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \text{ en } \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \quad \text{orthogonaal wegens} \quad \begin{bmatrix} 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \end{bmatrix} .$$

Voorbeeld. Twee aan twee orthogonaal is het drietal

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

Het volgende Latijnse vierkant echter bezit geen orthogonale collega:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix} .$$

7.2. Toepassingen

1. Uit elk van de landen Engeland, Frankrijk, Rusland en Amerika worden een generaal, een kolonel, een kapitein en een luitenant afgevaardigd. Kunnen deze 16 officieren worden opgesteld in een 4×4 vierkant, zodat elke rang en elke nationaliteit precies éénmaal voorkomt in elke rij en in elke kolom? De oplossing wordt gegeven door een paar orthogonale Latijnse vierkanten van de orde 4.

2. Wij wensen de opbrengst van 4 graansoorten te vergelijken. Het proefveld wordt verdeeld in 16 vierkante stukken, gearrangeerd in 4 rijen en 4 kolommen. De 4 graansoorten worden over deze stukken verdeeld volgens

een Latijns vierkant, zodat elke graansoort eenmaal in elke rij en in elke kolom wordt geplant. Zo kunnen systematische verschillen in de vruchtbaarheid van de grond worden geëlimineerd. In hetzelfde experiment kunnen ook vier verschillende bemestingsmethoden worden onderzocht, wanneer deze methoden worden toegepast volgens een Latijns vierkant orthogonaal met het vorige, zodat elke methode eenmaal op elke graansoort wordt toegepast.

3. De slijtage van 4 soorten van autobanden moet worden vergeleken met behulp van een experiment. De slijtage is verschillend op elk van de 4 wielen, en varieert van week tot week door de weersomstandigheden. Teneinde deze effecten te elimineren dient het experiment zo te worden opgezet dat de 4 banden gedurende 4 weken worden beproefd, en dat de 4 posities van week tot week worden veranderd volgens een Latijns vierkant.

4. Een televisiescherm wordt verdeeld in n × n vierkanten. Wij wensen n verschillende kleuren in paren te vergelijken, als geordende buren, zowel horizontaal als verticaal. Dit kan als volgt met behulp van Latijnse vierkanten gebeuren, voor n = 4 en voor n = 6:

$$\begin{bmatrix} a & b & c & d \\ c & a & b & d \\ b & d & a & c \\ d & c & b & a \end{bmatrix},$$

$$\begin{bmatrix} a & b & c & d & e & f \\ b & d & f & a & c & e \\ c & f & b & e & a & d \\ d & a & e & b & f & c \\ e & c & a & f & d & b \\ f & e & d & c & b & a \end{bmatrix}.$$

5. In een paar orthogonale Latijnse vierkanten van de orde 4 worden de rijen, de kolommen, de symbolen in het ene, de symbolen in het andere vierkant, aangegeven met dezelfde verzameling {1,2,3,4}. Dan kan het paar orthogonale Latijnse vierkanten worden opgevat als een verzameling van 16 4-vectoren met coördinaten uit {1,2,3,4} zodat voor elk paar coördinaten elk paar symbolen precies eenmaal voorkomt. Elk paar vectoren verschilt dus in tenminste 3 coördinaten. Daarom hebben wij een code, bestaande uit 16 codewoorden van lengte 4 met een alfabet van 4 letters, met minimum afstand 3, dus een 1-error correcting code.

7.3. Het vermoeden van Euler

Stelling. Bij elke eindige groep van oneven orde n kan een paar orthogonale Latijnse vierkanten van de orde n worden geconstrueerd.

Bewijs. Zij $G = \{a_1, a_2, \ldots, a_n\}$ een multiplicatieve groep van orde n. De matrices

$$[a_i\ a_j] \quad \text{en} \quad [a_j^{-1}\ a_i] \quad , \quad a_i, a_j \in G$$

zijn Latijnse vierkanten van de orde n. Inderdaad, in elk der matrices komt elk der groepselementen in elke rij en in elke kolom eenmaal voor. Uit

$$(a_i\ a_j\ ,\ a_j^{-1}\ a_i) = (a_k\ a_\ell,\ a_\ell^{-1}\ a_k)$$

volgt echter $a_i^2 = a_k^2$. Verhef in de macht $\frac{1}{2}(n+1)$ dan

$$a_i^{n+1} = a_k^{n+1} \text{ , dus } a_i = a_k \text{ ,}$$

omdat de n^e macht van elk groepselement gelijk is aan het eenheidselement (waarom?).

Euler formuleerde in 1782 het volgende.

Vermoeden. Er bestaat geen paar orthogonale Latijnse vierkanten van orde $n \equiv 2 \pmod 4$, $n > 2$.

Dit vermoeden werd in 1900 voor n = 6 bevestigd door Tarry. Voor alle andere n werd het echter in 1959 weerlegd door Bose, Shrikhande en Parker, die de volgende stelling bewezen:

Stelling. Er bestaat een paar orthogonale Latijnse vierkanten van elke orde $n \neq 6$.

7.4. Orthogonale Latijnse vierkanten

Stelling. Er bestaan ten hoogste n-1 twee aan twee orthogonale Latijnse vierkanten van de orde $n \geq 3$.

Bewijs. Stel $A_1, A_2, \ldots, A_t$ vormen t twee aan twee orthogonale Latijnse vierkanten van de orde n. Arrangeer de symbolen van elk der Latijnse vierkanten zo, dat de eerste rij van elke A_i bestaat uit de symbolen 1,2,...,n, in deze volgorde. De (2,1) plaatsen van de t Latijnse vierkanten zijn alle verschillend, en bevatten niet het symbool 1. Daarom is $t \leq n-1$.

Stelling. Als $n = p^m \geq 3$, p priem, dan bestaan er n-1 twee aan twee orthogonale Latijnse vierkanten van de orde n.

Bewijs. Zij $GF(n) = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_{n-1}\}$ het Galois lichaam van orde n. Definieer de n-1 matrices

$A_e = [a_e\ a_i + a_j]$, $i,j = 0,1,\ldots,n-1$, $e = 1,\ldots,n-1$.

Deze A_e zijn Latijnse vierkanten, wegens

$(a_e\ a_i + a_j = a_e\ a_{i'} + a_{j'}) \Rightarrow (a_j = a_{j'})$,

$(a_e\ a_i + a_j = a_e\ a_{i'} + a_j) \Rightarrow (a_i = a_{i'})$.

Voor $e \neq f$ zijn A_e en A_f orthogonaal omdat uit

$a_e\ a_i + a_j = a_e\ a_{i'} + a_{j'}$, $a_f\ a_i + a_j = a_f\ a_{i'} + a_{j'}$

volgt dat $a_i = a_{i'}$ en $a_j = a_{j'}$.

Opmerking. Voor een ander bewijs, zie D.W. p.42.
Inderdaad, wij hebben geconstrueerd een affien vlak AG(2,n).

Stelling. Als $n = p^m > 3$, p priem, dan bestaat er een Latijns vierkant van orde n dat orthogonaal is met zijn getransponeerde.

Bewijs. Zij GF(n) het Galois lichaam van orde n en zij $\lambda \in GF(n)$, $\lambda \neq 0$, $\lambda \neq 1$, $\lambda^{-1} \neq 2$. Beschouw de matrices

$$[\lambda a_i + (1-\lambda)\ a_j] \quad , \quad [\lambda a_j + (1-\lambda) a_i] \ , \ a_i, a_j \in GF(n).$$

Dit zijn Latijnse vierkanten van de orde n. Zij zijn orthogonaal omdat uit

$$\lambda a_i + (1-\lambda) a_j = \lambda a_{i'} + (1-\lambda) a_{j'}, \ \lambda a_j + (1-\lambda) a_i = \lambda a_{j'} + (1-\lambda)\ a_{i'}$$

volgt dat $a_i + a_j = a_{i'} + a_{j'}$, en dus

$$(1-2\lambda)\ a_j = (1-2\lambda)\ a_{j'} \ ,$$

waaruit $a_j = a_{j'}$ en $a_i = a_{i'}$.

Hoofdstuk 8. Codes

8.1. Codes met twee symbolen

Met twee symbolen a en b kunnen 2^n woorden van lengte n worden gemaakt, bijvoorbeeld

$\underline{x}$ = aabbbaabbba

$\underline{y}$ = abaabaaabbb , n = 11, $d(\underline{x},\underline{y}) = 5$.

De Hamming afstand $d(\underline{x},\underline{y})$ van twee woorden $\underline{x}$ en $\underline{y}$ is het aantal coördinaten waarin $\underline{x}$ en $\underline{y}$ verschillen. Dit is een afstand, omdat voldaan is aan

$$d(\underline{x},\underline{x}) = 0 \ , \ d(\underline{x},\underline{y}) = d(\underline{y},\underline{x}) \ , \ d(\underline{x},\underline{y}) + d(\underline{y},\underline{z}) \geq d(\underline{x},\underline{z}) \ .$$

Bij het overseinen van zulke woorden (per telefoon, bij communicatie met rekenmachines, met satellieten) kunnen door ruis (= noise) fouten optreden. Teneinde een mogelijkheid te hebben om zulke fouten te corrigeren, hebben wij nodig een deelverzameling (= code) van speciale woorden (= codewoorden) die onderling op een voldoende Hamming afstand van elkaar liggen.

Definitie. Een (m,n,d) code is een verzameling van m codewoorden van lengte n die paarsgewijs een Hamming afstand $\geq$ d hebben.

Wanneer $d = 2e + 1$, dan kan de code e fouten corrigeren en heet hij e-error-correcting code.

Voor de symbolen a en b worden soms de elementen 0 en 1 van GF(2) gebruikt, maar soms ook de gehele getallen +1 en −1. Dit hangt samen met de opteleigenschappen van GF(2), en met de vermenigvuldigingseigenschappen van Z:

$$\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 \end{array} + \qquad \begin{array}{cccc} + & + & - & - \\ + & - & + & - \\ \hline + & - & - & + \end{array} \times$$

Beschouw twee woorden van de lengte n

$$\begin{array}{ll} 0 \ldots 0 \ 0 \ldots 0 \ 1 \ldots 1 \ 1 \ldots 1 & + \ldots + \ + \ldots + \ - \ldots - \ - \ldots - \\ 0 \ldots 0 \ 1 \ldots 1 \ 0 \ldots 0 \ 1 \ldots 1 & + \ldots + \ - \ldots - \ + \ldots + \ - \ldots - \\ p \ , \ q \ , \ r \ , \ s \ \text{stuks} & p \ , \ q \ , \ r \ , \ s \end{array}$$

Hamming afstand $d = q + r$, inproduct $= p - q - r + s = n - 2d$.

Een "goede" (m,n,d) code bevat veel codewoorden (grote m) met onderling een grote Hamming afstand d, dus met een klein inproduct n − 2d.

8.2. Plotkin bound

Wij gebruiken voorlopig de symbolen {+,-}. De m codewoorden van lengte n vormen de rijen van een m × n matrix P. Zonder beperking der algemeenheid kan de eerste rij van P als j^T worden genomen, dus

$$P = \begin{bmatrix} j^T \\ Q \end{bmatrix} .$$

De codewoorden hebben onderling Hamming afstand ≥ d ddan als

$$G = PP^T \leq nI + (n - 2d)(J - I) ,$$

d.w.z. als $g_{ij} \leq n - 2d$ voor alle niet-diagonaal elementen g_{ij} van G. Wij beschouwen nu eerst het geval $n < 2d$. Dan volgt uit

$$0 \leq j^T PP^T j = nm + \sum_{i \neq j} g_{ij} \leq 2dm - (2d - n)m^2 ,$$

$$m \leq \frac{2d}{2d - n} \qquad \text{(Plotkin bound)} ,$$

met gelijkheid ddan als $g_{ij} = n - 2d$ voor alle $i \neq j$, dus als

$$PP^T = nI - (2d - n)(J - I) , \quad j^T P = 0^T .$$

In het extreme geval $m(2d - n) = 2d$ betekent dit voor Q dat

$$QQ^T = 2dI - (2d - n)J , \quad Qj = (n - 2d)j , \quad j^T Q = - j^T .$$

Om dit extreme geval te onderzoeken gaan wij over op de symbolen {0,1}, dus op de (m-1) × n matrox

$$N = \tfrac{1}{2}(J - Q) .$$

Deze (0,1) matrix voldoet aan

$$Nj = dj , \quad j^T N = \tfrac{1}{2}mj^T , \quad NN^T = \tfrac{1}{2}d(I + J) .$$

Hieruit volgt dat N, en dus ook Q, de punt-blok incidentie matrix is van een block design met

$$(v,k,b,r,\lambda) = (m-1, \tfrac{1}{2}m, n, d, \tfrac{1}{2}d) , \quad m(2d - n) = 2d .$$

Blijkbaar moeten m en d even zijn. Voor $2d - n = 1$, $m = 4t$, staat er het Hadamard design

$$(v,k,b,r,\lambda) = (4t-1,2t,4t-1,2t,t) .$$

Voor $2d - n = 2$ staat er

$$(v,k,b,r,\lambda) = (d-1,\tfrac{1}{2}d,2d-2,d,\tfrac{1}{2}d) .$$

Voor even $\frac{1}{2}d$ voldoet het herhaalde Hadamard design, voor oneven $\frac{1}{2}d = 2t + 1$ staat er

$$(v,k,b,r,\lambda) = (4t+1,2t+1,8t+2,4t+2,2t+1)$$

waaraan wordt voldaan door

$$[I+S \quad I-S] , \quad \text{met S uit} \quad C = \begin{bmatrix} 0 & j^T \\ j & S \end{bmatrix} ,$$

waarin C een symmetrische C-matrix van de orde $4t + 2$ is.
Ook voor $2d - n > 2$ zijn extreme codes te vinden, waarvoor de Plotkin bound wordt bereikt. De codes worden echter slechter bij toenemende $2d - n$.

Voorbeeld. $N = \text{circ}(1\ 1\ 1\ 0\ 1\ 0\ 0)$ is een (7,7,4) code.

8.3. Codes met $n = 2d$ en $n = 2d + 1$

In het geval $n \geq 2d$ geldt de Plotkin bound niet, en bestaan betere codes. Wij construeren eerst codes in het geval $n = 2d$. Voor de Hadamard matrix van de orde $4t$

$$H = [j \quad K] = [j \quad \ell \quad L]$$

geldt

$$HH^T = 4tI , \quad KK^T = 4tI - J , \quad LL^T \leq (4t - 2)I .$$

De rijen van L leveren $4t$ codewoorden van lengte $4t - 2$ met Hamming afstand $\geq 2t - 1$. De rijen van

$$P = \begin{bmatrix} H \\ -H \end{bmatrix}$$

leveren $8t$ codewoorden van lengte $4t$ met afstand $\geq 2t$, dus een $(8t,4t,2t)$ code. Dit is het best bereikbare voor het geval $n = 2d$.

Voorbeeld. Opgave 4 van Inleiding, 1.4.

Vervolgens beschouwen wij het geval $n = 2d + 1$. Wij zullen, voor geschikte d, construeren een $(4d+4, 2d+1, d)$ code. Zij H een Hadamard matrix van de orde $4t$. Volgens

$$H = [j \quad K], \quad P = \begin{bmatrix} K \\ -K \end{bmatrix}, \quad PP^T \leq (4t - 1)I + J - I$$

vormen de rijen van P juist $8t$ codewoorden van lengte $4t - 1$ met afstand $\geq 2t - 1$.

Zij S een symmetrische S-matrix van orde $4t + 1$, afgeleid van een symmetrische C-matrix van orde $4t + 2$ als in 7.2. Dan vormen de rijen van P:

$$P = \begin{bmatrix} j^T \\ -j^T \\ I+S \\ I-S \end{bmatrix}, \quad PP^T \leq (4t + 1)I + J - I,$$

juist $8t + 4$ codewoorden van lengte $4t + 1$ met afstand $\geq 2t$.

Opmerking. Voor oneven d is de hierboven gegeven code de best bereikbare. Voor even d zijn er betere, bijvoorbeeld de (16,5,2) code bestaande uit de 16 codewoorden van lengte 5 met een even aantal enen en verder nullen.

Hoofdstuk 9. Lineaire codes

9.1. Definities

Een lineaire (n,k) code over GF(q) is een lineaire deelruimte van dimensie k van de vectorruimte V(n,q) van dimensie n over GF(q). De codewoorden, dat zijn de vectoren van de lineaire deelruimte, hebben de volgende eigenschap: het verschil van twee codewoorden is weer een codewoord. Daarom worden de Hamming afstanden tussen de paren codewoorden bepaald door de Hamming afstanden van het codewoord $\underline{0}$ tot de andere codewoorden.

Definitie. Het gewicht van een codewoord is het aantal coördinaten $\neq 0$ van het codewoord.

Voorbeeld. Het vlak in V(4,3), opgespannen door

$$\underline{f} = (1,0,1,2)$$

$$\underline{g} = (0,1,1,1)$$

is een ternaire lineaire (4,2) code; $n = 4$, $k = 2$, $q = 3$, zie Inleiding 1.4. Alle codewoorden $\neq \underline{0}$ hebben gewicht 3, dus de onderlinge Hamming afstanden der 9 codewoorden zijn 3.

Een lineaire code kan op verschillende manieren worden beschreven:

Een generator matrix G van een lineaire (n,k) code is een $k \times n$ matrix, waarvan de rijen worden gevormd door k basisvectoren van de code. De q^k codewoorden zijn

$$\underline{u}^T G \quad , \quad \text{met} \quad \underline{u}^T = (u_1,\ldots,u_k) \quad , \quad u_i \in GF(q) \quad .$$

Een parity check matrix H van een lineaire (n,k) code is een $(n-k) \times n$ matrix over GF(q) zo, dat de q^k codewoorden zijn de vectoren

$$\underline{x} = (x_1,\ldots,x_n)^T \quad \text{met} \quad H\underline{x} = \underline{0} \quad .$$

Voorbeeld

$$G = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \qquad H = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

duiden aan de generator en de parity check matrix van het vorige voorbeeld.

Inderdaad, er geldt

$$GH^T = 0 \ .$$

Door geschikte basiskeuze kan de generator matrix van een lineaire (n,k) code worden gekozen als volgt:

$$G = [I_k \quad N] \ , \quad \text{met } k \times (n-k) \text{ matrix } N = [n_{ij}] \ .$$

Dan luidt de parity check matrix van die code:

$$H = [-N^T \quad I_{n-k}] \ ,$$

omdat $GH^T = 0$. De codewoorden zijn nu eenvoudig op te schrijven, immers kies

$$x_1,\ldots,x_k \text{ willekeurig, en } x_{k+j} = \sum_{i=1}^{k} x_i \, n_{ij} \ .$$

Opmerking. $x_1,\ldots,x_k$ heten de information symbols, $x_{k+1},\ldots,x_n$ heten de parity check symbols.

9.2. Hamming codes

Binaire Hamming codes zijn lineaire codes met de volgende parity check matrix H van afmeting $m \times (2^m - 1)$. De kolommen van H zijn $\neq \underline{0}$, verschillend, en bevatten slechts de elementen 0 en 1 van GF(2).

Voorbeeld, voor $m = 3$,

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} .$$

De lengte van de binaire Hamming code is $n = 2^m - 1$, en de dimensie is $k = 2^m - 1 - m$. Het minimum gewicht van de codewoorden $\neq \underline{0}$ is 3. Inderdaad, een codevector is een oplossing $\underline{x}$ van

$$H\underline{x} = \underline{0} \ ,$$

en elke $\underline{x} = (x_1,\ldots,x_n)^T \neq \underline{0}$ heeft tenminste 3 coördinaten $\neq 0$, omdat elk tweetal kolommen van H een som $\neq 0$ mod 2 heeft. Daarom zijn de Hamming codes 1-error-correcting. Het corrigeren van één fout geschiedt als volgt. Stel

$\underline{y} = \underline{x} + \underline{e}$ is het ontvangen woord, afkomstig van een codewoord $\underline{x}$, doch met een fout in de j-de coördinaat, $\underline{e} = (0 \,..\, 0\ 1\ 0 \,..\, 0)^T$. Dan wordt door

$$H\underline{y} = H\underline{x} + H\underline{e} = H\underline{e} = \text{j-de kolom van H}$$

de plaats van de fout aangeduid, omdat de j-de kolom van H juist de binaire representatie van het getal j is.

Opmerking.

$$H^* = \begin{bmatrix} 1 & j^T \\ 0 & H \end{bmatrix}$$

is de parity check matrix van een lineaire code van lengte 2^m en dimensie $2^m - m - 1$, met $d \geq 4$. Inderdaad, elk drietal kolommen van H^* heeft som $\neq 0$ mod 2. Deze lineaire code is dus 2-error-detecting.

Voorbeeld.

$$\begin{bmatrix} 1 & j^T \\ 0 & H_3 \end{bmatrix}$$

is de H van een lineaire (8,4) code met $d \geq 4$. Deze code, die $2^4 = 16$ codewoorden van lengte 8 bezit, is een Hadamard code volgens 8.3. Zie ook D.W. p. 31.

Hamming codes over GF(q) zijn lineaire codes met een $m \times (q^m - 1)/(q - 1)$ parity check matrix H. De kolommen van H zijn $\neq \underline{0}$, twee aan twee onafhankelijk, en bevatten de elementen van GF(q).

Voorbeeld.

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

is de parity check matrix van een lineaire code met 3^{10} codewoorden van lengte 13, die 1-error-correcting is. Zie D.W. p. 26.

9.3. De ternaire Golay code

Zij C_6 een conferentie matrix van de orde 6, zie Hst. 4.2 en Hst. 1.5. Beschouw de 6 × 12 ternaire matrix

$$H = [C_6 \quad I_6] .$$

Op elementaire wijze kan worden geverifieerd dat de 12 kolommen $\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_{12}$ van H de eigenschap hebben, dat geen vijf ervan afhankelijk zijn over GF(3). Dit betekent, dat van elk twaalftal getallen $(\alpha_1, \alpha_2, \ldots, \alpha_{12})$, niet alle 0, met

$$\alpha_1\underline{c}_1 + \alpha_2\underline{c}_2 + \ldots + \alpha_{12}\underline{c}_{12} = \underline{0} , \quad \alpha_i \in GF(3) ,$$

er tenminste 6 ongelijk 0 zijn. Het is niet moeilijk om zulke getallen te vinden, immers de rijen van

$$G = [I_6 \quad -C_6]$$

voldoen wegens $GH^T = 0$. Hieruit volgt, dat G de generator matrix (en H de parity check matrix) is van een lineaire (12,6) code, die de eigenschap heeft dat de afstand van elk tweetal codewoorden ≥ 6 is. Dit is de extended ternary Golay code, die dus 2-error-correcting en 3-error-detecting is. Door één coördinaat weg te laten wordt een lineaire (11,6) code met minimale afstand 5 verkregen, genaamd de ternaire Golay code. Deze code is een 6-deelruimte van V(11,3), bevat dus 3^6 codewoorden op een totaal van 3^{11} woorden. Omdat de afstand van elk tweetal codewoorden tenminste 5 is, hebben bollen met straal 2 rond de codewoorden geen vector gemeen. Wegens

$$3^6(1 + 22 + 220) = 3^{11}$$

vullen deze bollen de gehele V(11,3) op. Daarom is de ternaire Golay code een perfecte code.

9.4. De binaire Golay code

Zij $\underline{x}$ en $\underline{y}$ binaire vectoren van dezelfde dimensie. Naast hun somvector $\underline{x} + \underline{y}$ beschouwen wij hun productvector $\underline{xy}$, de vector waarvan de coördinaten zijn de producten van de corresponderende coördinaten van $\underline{x}$ en $\underline{y}$. Bijvoorbeeld:

$$\underline{x} = (1,1,0,0)$$
$$\underline{y} = (1,0,1,0)$$
$$\underline{x} + \underline{y} = (0,1,1,0)$$
$$\underline{xy} = (1,0,0,0) .$$

Zij $|\underline{x}|$ het gewicht van $\underline{x}$, dus het aantal coördinaten $\neq 0$.

Lemma 1.

$$|\underline{x} + \underline{y}| = |\underline{x}| + |\underline{y}| - 2|\underline{xy}| ,$$
$$|\underline{x} + \underline{y} + \underline{z}| = \Sigma\ |\underline{x}| - 2\Sigma\ |\underline{xy}| + 4|\underline{xyz}| ,$$
$$|\underline{x} + \underline{y} + \underline{z} + \underline{u}| = \Sigma\ |\underline{x}| - 2\Sigma\ |\underline{xy}| + 4\Sigma\ \underline{xyz} - 8|\underline{xyzu}| .$$

Bewijs. Door verificatie.

Lemma 2. Zij Q = circul(0,1,0,1,1,1,0,0,0,1,0) en zij j de all-one vector van dimensie 11. Dan zijn alle 55 + 11 sommen mod 2 van twee vectoren uit de rijen van Q en j^T verschillend.

Bewijs. Verifieer met behulp van de eerste zes rijen a, b, c, d, e, f van Q, immers

$$j^T + a = (1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1) , \quad a + d = (0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0)$$
$$a + b = (0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1) , \quad a + e = (0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0)$$
$$a + c = (1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0) , \quad a + f = (0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1) .$$

Merk nog op, dat elk paar rijen van Q heeft

$$2 \times \binom{1}{1} , \quad 3 \times \binom{1}{0} , \quad 3 \times \binom{0}{1} , \quad 3 \times \binom{0}{0} .$$

Stelling. De 4096 codewoorden van de lineaire (24,12) code met generator matrix

$$G = \left[\begin{array}{cc:cc} 0 & 0^T & 1 & j^T \\ j & I & j & Q \end{array}\right]$$

hebben slechts de afstanden 8, 12, 16, 24.

Bewijs. De generatoren hebben gewicht 12 en 8. De som van twee generatoren heeft gewicht 2 + 6 = 8. Het product van twee generatoren heeft gewicht 1 + 3 = 4 of 0 + 6 = 6. Volgens Lemma 1 heeft dus elk codewoord een gewicht dat deelbaar is door 4. Elke 3-som heeft gewicht 2 + 6 als hij j bevat, en gewicht $\geq 4 + 1 = 5$ als hij j niet bevat. Dus elke 3-som heeft gewicht ≥ 8. Voor elke 4-som geldt:

$$|\underline{x} + \underline{y} + \underline{z} + \underline{u}| = |\underline{x} + \underline{y}| + |\underline{z} + \underline{u}| - 2|(\underline{x} + \underline{y})(\underline{z} + \underline{u})| .$$

Nu hebben $\underline{x} + \underline{y}$ en $\underline{z} + \underline{u}$ in hun laatste 11 coördinaten 6 enen die, wegens Lemma 2, ten hoogste 4 plaatsen gemeen hebben. Dus

$$|\underline{x} + \underline{y} + \underline{z} + \underline{u}| \geq 8 + 8 - 2.4 = 8 .$$

Omdat ook elke 5-som (en hoger) gewicht ≥ 5 heeft, concluderen wij dat elk codewoord $\neq 0$ gewicht ≥ 8 heeft. Omdat wegens het voorkomen van j gewicht 20 is uitgesloten, heeft elk codewoord, behalve 0 en j, gewicht 8, 12, 16.

De hierboven geconstrueerde code heet de extended binary Golay code. De Golay code zelf is een lineaire (23,12) code, verkregen door weglating van één coördinaat. Deze code is weer perfect wegens

$$2^{12}[1 + 23 + \binom{23}{2} + \binom{23}{3}] = 2^{23} .$$

Stelling. De vectoren van gewicht 8 van de extended Golay (24,12) code vormen een 5-design.

Bewijs. Zij

$$\underline{x} \in V(24,2) \quad \text{met} \quad |\underline{x}| = 5 .$$

Laat weg een coördinaat waar $\underline{x}$ niet nul is. Dan is verkregen $\underline{x}' \in V(23,2)$ van gewicht 4. De (23,12) Golay code is perfect, met minimum gewicht 7, en daarom bevat de code een eenduidig codewoord $\underline{y}'$ van gewicht 7 op afstand 3 van $\underline{x}'$. Deze $\underline{y}'$ is afkomstig van een eenduidig bepaalde $\underline{y} \in V(12,2) \subset V(24,2)$ van gewicht 8 en op afstand 3 van $\underline{x}$.
Zij V de verzameling van 24 punten die correspondeert met de 24 coördinaat plaatsen van V(24,2). Zij B de verzameling der blokken die correspondeert met de codewoorden van gewicht 8 in V(12,2). Een punt ligt in een blok als d de corresponderende coördinaat van het corresponderende codewoord het getal 1 bevat. Er is een eenduidig codewoord van gewicht 8 op afstand 3 van een

gegeven woord van gewicht 5. Daarom ligt ieder vijftal punten van V in één blok. Hieruit volgt dat {V,B} een 5-design is met

$$v = 24,\ k = 8,\ b_5 = 1,\ b_4 = 5,\ b_3 = 21,\ b_2 = 77,\ b_1 = 253,\ b_0 = 759\ .$$

De gevallen b_i worden berekend met behulp van de formule (vgl. 6.4)

$$b_i(8 - i) = b_{i+1}(24 - i)\ ,\quad \text{voor } 0 \le i \le 4\ .$$

Opmerking. De beide Golay codes hebben verband met de groepen van Mathieu. Het boven genoemde 5-design is afkomstig van Steiner.

Hoofdstuk 9. Grafen

9.1. Picture transmission.

Acht verschillende tinten grijs, van wit tot zwart, worden voorgesteld door de getallen $0,1,\ldots,7$. Een encoder voegt aan zo'n getal a een binair getal van 3 bits $\varphi^{-1}(a)$ toe. Dit binaire getal wordt overgeseind via een B.S.C. (= binary symmetric channel), dat ten hoogste fouten in één bit maakt. Het ontvangen binaire getal wordt tenslotte gedecodeerd tot één van de tinten $0,1,\ldots,7$. Wegens het optreden van ruis dient de toevoeging $a \leftrightarrow \varphi^{-1}(a)$ zo te geschieden, dat het ontvangen beeld zo min mogelijk wordt vervormd.

De B.S.C. wordt weergegeven door de kubusgraaf, waarvan E de verzameling der ribben (= edges), en

$$V = \{000,100,010,001,011,101,110,111\}$$

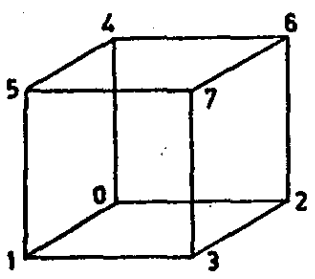
de verzameling der hoekpunten (= vertices) is. De toevoeging der getallen $0,1,\ldots,7$ aan V wordt weergegeven door

$$\varphi : V \xleftrightarrow{1-1} \{0,1,\ldots,7\}.$$

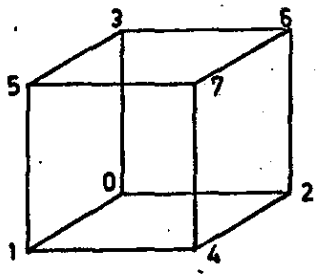
Als eis voor minimale vervorming wordt gesteld de voorwaarde, dat de waarde van de noise power

$$\Phi = \sum_{(\underline{v},\underline{w})\in E} [\varphi(\underline{v}) - \varphi(\underline{w})]^2$$

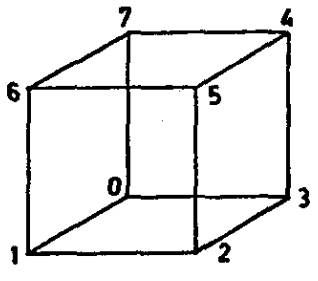
zo klein mogelijk is. Voor de drie voorbeelden is de waarde van Φ respectie-



Natural code, $\Phi = 84$;



$\Phi = 86$;



Gray code, $\Phi = 108$.

Fig. 16.

velijk 84, 86, 108. Wij zullen nu aantonen dat de eerste toevoeging (= natural code), of een daarmee gelijkwaardige, de beste is onder alle $8! = 40320$ mogelijk toevoegingen. Noem $\underline{v}$ even, resp. oneven, als zijn gewicht even, resp. oneven, is. Zij $\underline{v}^c = \underline{j} - \underline{v}$ het complement van $\underline{v}$.

$$\Phi = \sum_{(\underline{v},\underline{w})\in E} [\varphi(\underline{v}) - \varphi(\underline{w})]^2 = 3 \sum_{\underline{v}\in V} \varphi^2(\underline{v}) - 2 \sum_{(\underline{v},\underline{w})\in E} \varphi(\underline{v})\varphi(\underline{w}) =$$

$$= 3 \sum_{\underline{v}\in V} \varphi^2(\underline{v}) - 2 \sum_{\underline{v} \text{ oneven}} \varphi(\underline{v}) \sum_{\underline{w} \text{ even}} \varphi(\underline{w}) + 2 \sum_{\underline{v},\underline{v}^c\in V} \varphi(\underline{v})\varphi(\underline{v}^c) .$$

De eerste term is onafhankelijk van φ. De tweede term is maximaal wanneer

$$\sum_{\underline{v} \text{ oneven}} \varphi(\underline{v}) = \sum_{\underline{w} \text{ even}} \varphi(\underline{w}) = 14,$$

daar

$$\sum_{\underline{v}\in V} \varphi(\underline{v}) = 0 + 1 + \ldots + 7 = 28 .$$

De derde term is minimaal wanneer hij bestaat uit

$$0 \times 7 + 1 \times 6 + 2 \times 5 + 3 \times 4 .$$

Aan beide eisen wordt voldaan door

$$\varphi(\underline{v}) = v_0 + v_1.2 + v_2.2^2 .$$

Dit is ook de enige φ die voldoet, immers uit

$$\sum_{\text{oneven}} \varphi(\underline{v}) = x + y + z + 7 = 14, \quad 1 \le x < y < z \le 6$$

volgt dat $x = 1$, $y = 2$, $z = 4$.

De verkregen oplossing heet de natural code; aan elk hoekpunt wordt toegevoegd het getal, waarvan zijn coördinaten de binaire ontwikkeling vormen.

Opmerking. De "average absolute error" $\sum |\varphi(\underline{v}) - \varphi(\underline{w})|$ wordt geminimaliseerd door de eerste en de derde toevoeging.

Literatuur: IEEE Spectrum, dec. 1965, p. 60.
IEEE, IT, 15 (1969) 72-78.

9.2. Sterk reguliere grafen

Laat een graaf met n punten de volgende eigenschappen hebben. Er zijn natuurlijke getallen k, λ, μ zodat geldt

i) elk punt is verbonden met $\le k$ andere punten,

ii) elk verbonden paar punten heeft $\ge \lambda$ tussenpunten,

iii) elk niet-verbonden paar punten heeft $\ge \mu$ tussenpunten.

Dan geldt

$$(n - k - 1)\mu \leq k(k - 1 - \lambda) .$$

Bewijs. Met een punt P zijn $\leq k$ punten verbonden (niveau I), en $\geq n - k - 1$ punten niet-verbonden (niveau II). Er zijn $\geq (n - k - 1)\mu$ verbindingen van II naar I. Er zijn $\leq k(k - 1 - \lambda)$ verbindingen van I naar II. Dit bewijst de formule. Dit bewijst tevens dat in de formule het gelijkteken geldt,

$$(n - k - 1)\mu = k(k - 1 - \lambda),$$

dan en slechts dan als

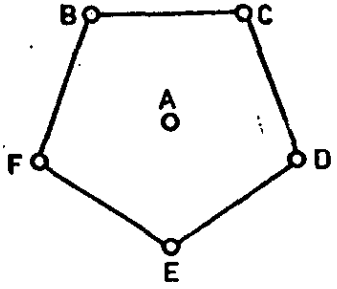
1) elk punt is verbonden met precies k andere punten,
2) elk verbonden paar punten heeft precies λ tussenpunten,
3) elk niet-verbonden paar punten heeft precies μ tussenpunten.

Een graaf met 1), 2), 3) heet een sterk reguliere graaf.

Vb. 1, $n = 4$, $k = 1$, $\lambda = 0$, $\mu = 0$.

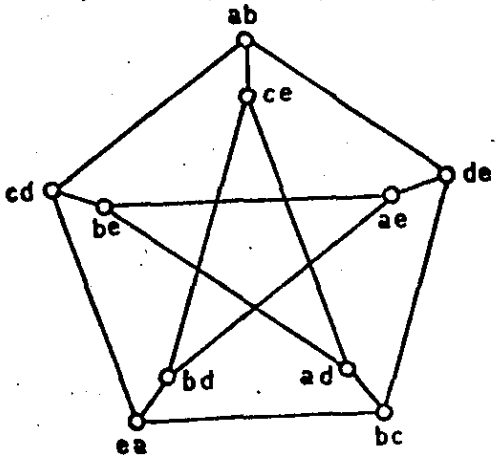
$$A_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} .$$

Vb. 2, $n = 5$, $k = 2$, $\lambda = 0$, $\mu = 1$.



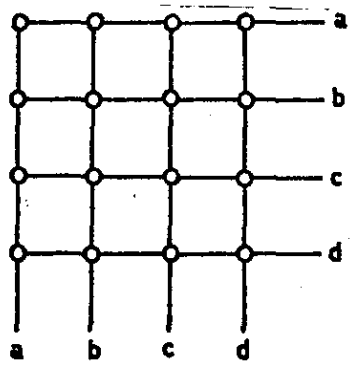
$$A_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} .$$

Vb. 3, $n = 10$, $k = 3$, $\lambda = 0$, $\mu = 1$.



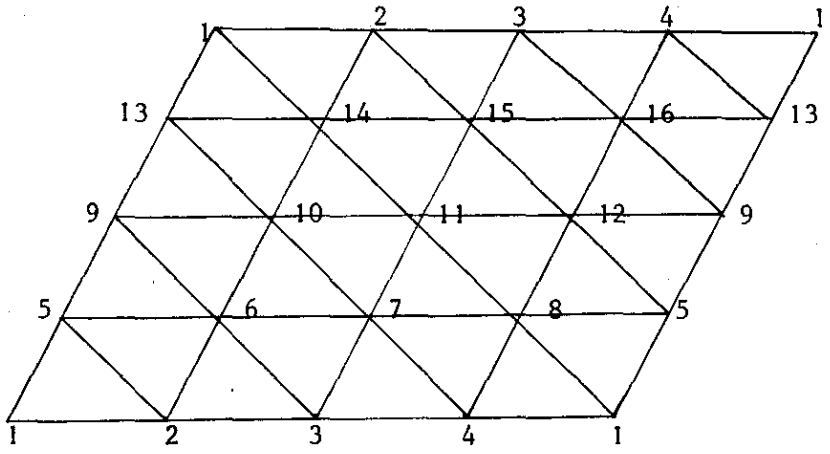
$$A_{10} = \begin{bmatrix} A_5 & I \\ I & J-I-A_5 \end{bmatrix} .$$

Vb. 4, n = 16, k = 6, $\lambda = 2$, $\mu = 2$.



$$A_{16} = \begin{vmatrix} J-I & I & I & I \\ I & J-I & I & I \\ I & I & J-I & I \\ I & I & I & J-I \end{vmatrix} .$$

Vb. 5, n = 16, k = 6, $\lambda = 2$, $\mu = 2$, de torusgraaf.



Reguliere grafen, met valentie k, worden in termen van hun verbindingsmatrix A gekarakteriseerd door

$$Aj = kj .$$

Stelling. Sterk reguliere grafen worden beschreven door

$$Aj = kj, \quad (A - rI)(A - sI) = \mu J .$$

Bewijs. Bewchouw het matrix product $(A - rI)(A - sI)$. Bij twee niet-verbonden punten behoort het inproduct van

$$\begin{matrix} -r & 0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 \\ 0 & -s & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \end{matrix} .$$

Bij twee verbonden punten behoort het inproduct van

$$\begin{matrix} -r & 1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 \\ 1 & -s & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \end{matrix} .$$

Op de diagonaal staat het inproduct van

$$\begin{matrix} -r & 0\ldots.0 & 1\ldots.1 \\ -s & 0\ldots.0 & 1\ldots.1 \end{matrix} .$$

Als de matrixvergelijking waar is voor zekere getallen r en s, dan zijn μ en λ constant. Omgekeerd, als k, μ, λ constant zijn, dan kunnen getallen r en s worden gevonden zodat de matrixvergelijking geldt.

Gevolg. Voor sterk reguliere grafen geldt

$$(n - k - 1)\mu = k(k - 1 - \lambda),\ -r - s = \mu - \lambda,$$

$$k + rs = \mu,\ (k - r)(k - s) = \mu n.$$

Stelling. De verbindingsmatrix A van een sterk reguliere graaf heeft drie eigenwaarden, namelijk r, s en k (enkelvoudig). Als $r + s \neq -1$, dan zijn r en s geheel.

Bewijs. Bij overgang op een basis van eigenvectoren wordt de symmetrische matrix A overgevoerd in een diagonaalmatrix. Dan neemt ook A^2 de diagonaalvorm aan, en eveneens J (wegens de matrixvergelijking van de vorige stelling). Voor de eigenwaarden α van A geldt dus dat $(\alpha - r)(\alpha - s)$ gelijk is aan μn (éénmaal) en 0 (n-1 maal). Dus k, r, s zijn de eigenwaarden. Laat hun multipliciteiten zijn 1, x, y, dan geldt

$$\mathrm{tr}\ A = 0 = k + xr + ys,\ 1 + x + y = n,$$

$$2k + (n - 1)(r + s) + (x - y)(r - s) = 0\ .$$

Voor $x \neq y$ volgt hieruit dat $r - s$, en ook r en s geheel zijn. Voor $x = y$ behoeven r en s niet geheel te zijn, maar volgt

$$2k + (n - 1)(r + s) = 0,\ r + s = -1,\ n = 2k + 1.$$

Opmerking. Het is niet moeilijk om in te zien dat in het geval $x = y$ de matrix

$$\begin{bmatrix} 0 & j^T \\ j & J-I-2A \end{bmatrix}$$

een conferentiematrix (zie 4.3) is.

Vb. 1, $n = 4$, $k = 1$, $r = 1$, $s = -1$, $A_4^2 - I = 0$.

Vb. 2, $n = 5$, $k = 2$, $r = \frac{1}{2}(-1 + \sqrt{5})$, $s = \frac{1}{2}(-1 - \sqrt{5})$, $A_5^2 + A_5 - I = J$.

Vb. 3, $n = 10$, $k = 3$, $r = 1$, $s = -2$, $A_{10}^2 + A_{10} - 2I = J$.

Vb. 4, $n = 16$, $k = 6$, $r = 2$, $s = -2$, $A_{16}^2 - 4I = 2J$.

Vb. 5, $n = 16$, $k = 6$, $r = 2$, $s = -2$, $A^2 - 4I = 2J$.

Opmerking. Vb. 4 en 5 tonen aan dat een graaf niet eenduidig bepaald behoeft te zijn door zijn eigenwaarden.

Wij beschouwen sterk reguliere grafen met $\lambda = 1$, $\mu = 2$. Elk verbonden paar punten ligt in één driehoek; elk niet-verbonden paar punten ligt in één vierhoek. Een voorbeeld is de graaf met $n = 9$, $k = 4$:

Een ander voorbeeld wordt gevonden met behulp van de ternaire (11,6) Golay code, zie 9.3. Zij H de 5×11 parity check matrix van deze code, waarvan de kolommen $x_1, x_2, \ldots, x_{11}$ dus vectoren van V(5,3) zijn. Omdat in de ternaire Golay code elk codewoord gewicht ≥ 5 heeft, zijn van deze kolommen geen 4 afhankelijk. Er zijn 22 vectoren van het type $\pm x_i$, en 220 vectoren van het type $\pm x_i \pm x_j$. Deze vectoren zijn verschillend, en vormen tesamen met de vector 0 alle vectoren van V(5,3). Beschouw nu de 243 vectoren als de 243 punten van een graaf. Twee punten van de graaf worden verbonden, als het verschil van de corresponderende vectoren behoort tot

$$\{\pm x_1, \pm x_2, \ldots, \pm x_{11}\}.$$

Nu is eenvoudig te verifieren dat voor de graaf geldt $\lambda = 1$, $\mu = 2$.

Literatuur: Berlekamp, van Lint, Seidel in "Bose anniversary volume", (to appear).

Bijlage

behorend bij "Discrete Wiskunde", bedoeld voor niet-WSK studenten.

Literatuur:

Ackermans-Van Lint, Algebra en Analyse, Wolters-Noordhoff 1970.

Van Lint, THE syllabus Discrete Wiskunde.

1. Equivalentierelaties
2. Groepen
3. Ringen en lichamen.

1. Equivalentierelaties (A en A , 65-74).

1.1. Verzamelingen

N = {natuurlijke getallen} = {1,2,3,...}.

Z = {gehele getallen} = {...,-3,-2,-1,0,1,2,...}.

Q = {rationale getallen}, bijvoorbeeld $\frac{3}{5}$, $\frac{7}{5}$, $\frac{10}{5}$, $\frac{0}{5}$.

R = {reële getallen}, bijvoorbeeld $\sqrt{2}$, $\frac{22}{7}$, π, 87 .

$\emptyset$ = lege verzameling.

$\emptyset \subset N \subset Z \subset Q \subset R$.

1.2. Relaties

Zij V een verzameling. Het Cartesisch product van V met V is de verzameling der geordende paren van elementen van V:

$$V \times V = \{(x,y) \mid x \in V,\ y \in V\} .$$

Vb. $R \times R$ is het gewone vlak R^2 uit de analytische meetkunde.

Vb. $Z \times Z$ is het rooster van de punten met gehele coördinaten.

Een relatie op V is een deelverzameling van $V \times V$. De elementen x en y van V zijn in de relatie, schrijf $x \sim y$, als (x,y) in de deelverzameling ligt.

Een relatie heet

reflexief als steeds geldt $x \sim x$,

symmetrisch als steeds uit $x \sim y$ volgt $y \sim x$,

transitief als steeds uit $x \sim y$ en $y \sim z$ volgt $x \sim y$.

Voorbeelden, waarin de verzameling is de verzameling der reëlen.

relatie $x \sim y$	reflexief	symmetrisch	transitief
$x = y + 1$			
$x > y$			
$x \neq y$			
$x \leq y < x + 2$			
$xy > 0$			
$x \geq y$			
$\lvert x-y \rvert < 1$			
$x = y$			

1.3. Equivalentierelaties

Een relatie, die reflexief, symmetrisch en transitief is, heet een equivalentierelatie.

Vb. I. Zij V = R. De relatie $x - y \in Z$ is een equivalentierelatie.

Vb. II. Zij V de verzameling van alle driehoeken in het vlak. Congruentie van driehoeken is een equivalentierelatie.

Vb. III. Zij V de verzameling der rechten in het vlak. De relatie gedefinieerd door evenwijdigheid (of samenvallen) is een equivalentierelatie.

Vb. IV. Zij V = Z. Definieer congruentie modulo 7 door
$x \equiv y \pmod 7$ als $x - y$ een 7-voud is.
Dit is een equivalentierelatie.

1.4. Equivalentieklassen

Zij $\sim$ een equivalentierelatie, gedefinieerd op een verzameling V.
De bij $a \in V$ behorende equivalentieklasse $Kl(a)$ is de verzameling van alle x die in de relatie $\sim$ tot a staan:

$$Kl(a) = \{x \mid x \in V, x \sim a\}.$$

Vb. I. $Kl(\frac{1}{3}) = \{\frac{1}{3}, \frac{4}{3}, \frac{7}{3}, \ldots, -\frac{2}{3}, -\frac{5}{3}, \ldots\}$.

Vb. II. $Kl(\Delta) = \{$alle driehoeken die congruent zijn met $\Delta\}$.

Vb. III. $Kl(\ell) = \{$alle rechten die evenwijdig zijn aan $\ell\}$.

Vb. IV. $Kl(2) = \{2,9,16,\ldots, -5, -12,\ldots\} = Kl(9) = Kl(-5)$.

Stelling: De diverse equivalentieklassen verdelen V in een aantal niet-lege, disjuncte parten met de eigenschap dat elk equivalent paar in één part ligt.

Voor het bewijs van deze stelling wordt verwezen naar A en A. pag.71 en 72.

Vb. Door $x \equiv y \pmod 7$ wordt Z verdeeld in 7 equivalentieklassen, namelijk de 7-vouden, de 7-vouden + 1, de 7-vouden + 2, ... , de 7-vouden + 6.
De getallen 0, 1, 2, ..., 6 representeren deze klassen.
De getallen 14, 1, 9, ..., -1 eveneens.

Vb. Door $x \equiv y \pmod m$ wordt Z verdeeld in m equivalentieklassen.
Een stel representanten, bijvoorbeeld $0,1,2,\ldots,m-1$, heet een volledig restsysteem modulo m, vgl. D.W. pag.2.

1.5. Bewerkingen met equivalentieklassen

Beschouw weer de equivalentierelatie

$$x \equiv y \pmod m$$

gedefinieerd op de verzameling Z der gehelen.
De equivalentieklasse van $a \in Z$ wordt aangeduid door Kl(a). Definieer

$$Kl(a) + Kl(b) := Kl(a+b) ,$$

$$Kl(a) \cdot Kl(b) := Kl(ab) ,$$

$$k \cdot Kl(a) := Kl(ka) .$$

Wegens D.W. stelling (1.8) is deze definitie onafhankelijk van de representanten van de klassen.
Voor de zojuist gedefinieerde opstelling en vermenigvuldiging geldt een aantal eigenschappen die de verzameling der klassen tot een ring maken.
In het algemeen geldt niet dat uit

$$Kl(a) \cdot Kl(b) = Kl(0) \text{ volgt } Kl(a) = Kl(0) \text{ of } Kl(b) = Kl(0),$$

omdat uit $ab \equiv 0 \pmod m$ niet behoeft te volgen $a \equiv 0 \pmod m$ of $b \equiv 0 \pmod m$. Dit is wel het geval wanneer m een priemgetal is. Daarom vormen de klassen modulo en priemgetal p een lichaam. Dit is het Galois lichaam GF(p), p priem, waarover in D.W. pag. 15 wordt gesproken.

Voorbeelden. $GF(2) = \{0,1\}$; $GF(5) = \{0,1,2,3,4\}$; $GF(3) = \{0,+,-\}$
met optelling en vermenigvuldiging volgens respectievelijk

+	0	1
0	0	1
1	1	0

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	+	−
0	0	+	−
+	+	−	0
−	−	0	+

×	0	1
0	0	0
1	0	1

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

×	0	+	−
0	0	0	0
+	0	+	−
−	0	−	+

2. Groepen (A en A , 113-136)

2.1. Productoperaties

Een verzameling met productoperatie is een paar (V,φ) van een verzameling V en een afbeelding $\varphi : V \times V \to V$.
Met andere woorden, aan elk geordend paar elementen $(a,b) \in V \times V$ wordt toegevoegd een element $\varphi(a,b) \in V$.

Vb. 1. $(R, \cdot)$. Hier is $V = R$ en $\varphi(a,b) = a \cdot b$, de gewone vermenigvuldiging.

Vb. 2. $(R, +)$. Hier is $V = R$ en $\varphi(a,b) = a + b$, de gewone optelling.

Vb. 3. $(R^2, +)$. Hier is $V = R^2$ en $\varphi(\underline{a}+\underline{b}) = \underline{a} + \underline{b}$, de optelling van vectoren.

Vb. 4. $(V, \circ)$, met V = {lineaire afbeeldingen $R^2 \to R^2$} en $\varphi(\alpha,\beta) = \alpha \circ \beta$, de productafbeelding (eerst β, dan α).

Vb. 5. $(R^3, \times)$, met $V = R^3$ en $\varphi(\underline{a},\underline{b}) = \underline{a} \times \underline{b}$, het uiwendig product.

In de volgende definities schrijven wij ab in plaats van $\varphi(a,b)$, dus gebruiken wij de verzameling met productoperatie $(V, \ )$.
$(V, \ )$ heet commutatief, als steeds geldt $ab = ba$.
Voorbeelden: 1,2,3 commutatief, 4 en 5 niet.
$(V, \ )$ heet associatief, als steeds geldt $(ab)c = a(bc)$.
Voorbeelden: 1,2,3,4 associatief, 5 niet.
$(V, \ )$ heeft eenheid e, als er een $e \in V$ is, zodat steeds geldt $ae = ea = a$.
Voorbeelden: 1,2,3,4 hebben als eenheid resp. 1,0,$\underline{0}$, id. Vb. 5 heeft geen eenheid.
In $(V, \ )$, voorzien van eenheid e, heeft $a \in V$ een inverse, als er een $b \in V$ is zodat $ab = ba = e$. Schrijf a^{-1}.
Voorbeelden: In 1,2,3,4 is de inverse van $a, a, \underline{a}, \alpha$ resp. $\frac{1}{a}$ voor $a \neq 0$, $-a$, $-\underline{a}$, α^{-1}.

2.2. Groepen

Een verzameling met productoperatie $(V, \ )$ heet een groep, wanneer geldt

G_1 : de productoperatie is associatief,

G_2 : er is een eenheid,

G_3 : elk element heeft een inverse.

De groep heet Abels (commutatief), als de productoperatie commutatief is.

Voorbeelden 1, 2, 3 zijn Abelse groepen, vb. 4 is een niet-Abelse groep, vb. 5 is geen groep.

Vb. 6. $(R \setminus \{0\}, \ )$, met de gewone vermenigvuldiging, heet de multiplicatieve groep der reëlen $\neq 0$. Eenheid 1; inversen: a en $\frac{1}{a}$.

Vb. 7. $(Q, +)$, met de gewone optelling, heet de additieve groep der rationale getallen. Eenheid 0; inversen: a en -a.

Vb. 8. De complexe getallen

$$e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2\pi k i}{n}}, \ldots, e^{\frac{2\pi(n-1)i}{n}}, e^{2\pi i},$$

met de gewone vermenigvuldiging, vormen een groep van de orde n.

Inversen: $e^{\frac{2\pi k i}{n}}$ en $e^{-\frac{2\pi k i}{n}}$.

Vb. 9. De equivalentieklassen modulo n, met de hierboven gedefinieerde opstelling mod n, vormen een groep van de orde n. Hierin is Kl(0) eenheid; inversen: Kl(a) en Kl(-a).

Vb. 10. De groepen van vb. 8 en vb. 9 zijn isomorf.

2.3. Ondergroepen

Zij $(G, \ )$ een groep, en zij $H \subset G$. Wanneer $(H, \ )$ zelf weer een groep is, dan heet $(H, \ )$ ondergroep van $(G, \ )$.

Voorbeeld: $(Z, +)$ is ondergroep van $(R, +)$.

Voorbeeld: $(R^2, +)$ is ondergroep van $(R^3, +)$.

Zij $(G, \ )$ een Abelse groep met ondergroep $(H, \ )$.
Definieer de relatie $\sim$ door

$$x \sim y \quad \text{betekent} \quad xy^{-1} \in H \qquad (x,y \in G).$$

Dit is een equivalentierelatie wegens

$$x\,x^{-1} = e \in H, \; y\,x^{-1} = (xy^{-1})^{-1}, \; x\,y^{-1}\,y\,z^{-1} = x\,z^{-1}.$$

De equivalentieklasse van $a \in G$ is

$$\{x \mid x\,a^{-1} \in H\} = \{ah \mid h \in H\} =: a\,H.$$

Dit zijn de nevenklassen van H, zie D.W. 14.
Definieer vermenigvuldiging van nevenklassen door

$$a\,H \cdot b\,H := ab\,H.$$

Dan vormen de nevenklassen een groep, de factorgroep G / H. Hierin is
$e\,H = H$ eenheid; inversen: $a\,H$ en $a^{-1}\,H$.

Voorbeeld: $(Z, +)$ is een Abelse groep. Alle 6-vouden vormen een ondergroep H.
De congruentie

$$x \equiv y \pmod 6 \text{ betekent } x-y \in G.$$

De restklassen modulo 6 vormen de additieve groep $(Z \bmod 6, +)$,
de factorgroep Z / H.

Voorbeeld: Zij $V = \{a, a^2, a^3, a^4, a^5, a^6 = 1\}$. Dan is $(V, \ )$, met de gewone vermenigvuldiging, een groep.
$(W, \ )$, met $W = \{1, a^2, a^4\}$ is een ondergroep.
De factorgroep V / W heeft de elementen W en a W.

Opmerking. Bij niet-Abelse groepen is een meer genuanceerd begrip factorgroep.
Zie A en A , 127-134.

Semi-groepen en eindige Automaten

1. Verzamelingen met een Productoperatie (Groepoïden)

X is een willekeurige niet-lege verzameling. Een productoperatie op X is een functie $\psi: X^2 \to X$. De productoperatie ψ voegt dus aan ieder element $(a,b) \in X^2$, een element $\psi(a,b) \in X$ toe.
Bovenstaande verzameling met productoperatie (groepoïde) wordt genoteerd als $\langle X,\psi \rangle$. In het vervolg zullen we het product $\psi(a,b)$ ook wel schrijven als: $a * b$.

Voorbeeld 1. $\langle N,+ \rangle$. Hier is $X = N$ (verzameling van natuurlijke getallen) en het product is de "gewone" optelling.

Voorbeeld 2. $\langle X,\circ \rangle$ met $X = \{f \mid f: S \to S\}$, S is een willekeurige verzameling en $S \neq \emptyset$, en $\circ$ is de functie compositie $((f \circ g)(x) = f(g(x)), x \in S)$.

Voorbeeld 3. $\langle N,\psi \rangle$ met $\psi(a,b) = a + b^2 \quad (a,b \in N)$.

Voorbeeld 4. $\langle \{a,b\},\psi \rangle$. ψ is gedefinieerd met behulp van onderstaande tabel. Bijvoorbeeld $\psi(b,a) = b$.

	a , b	
a	b	a
b	b	b

De productoperatie op X is commutatief, als voor alle $a,b \in X$ geldt:
$a * b = b * a \quad (\psi(a,b) = \psi(b,a))$.
De productoperatie op X is associatief, als voor alle $a,b,c \in X$ geldt:
$(a * b) * c = a * (b * c) \quad (\psi(\psi(a,b),c) = \psi(a,\psi(b,c)))$.
Een element e, $e \in X$ en $\langle X,* \rangle$, is een linker (rechter) eenheidselement, als voor alle $x \in X$ geldt: $e * x = x$ $(x * e = x)$.
In het geval e tegelijkertijd het linker- en het rechtereenheidselement is dan noemt men e het neutrale element of de eenheid.
Ga voor de voorbeelden 1,2,3 en 4 na, of de productoperatie commutatief en/of associatief is; idem of de betreffende groepoïden een eenheid bevatten.

Stelling (1.1): Als de groepoïde $\langle X,\psi \rangle$ een linkereenheidselement u en een rechtereenheidselement v bevat, dan geldt $u = v$.
Bewijs dit.

2. Semi-groepen

Een semi-groep is een groepoïde waarvan de productoperatie associatief is.
Een monoïde is een semi-groep die een eenheid bevat.
De groepoïde in vb. 1 is een semi-groep, in vb. 2 een monoïde; de groepoïden in vb. 3 en in vb. 4 zijn geen semi-groepen.
Een semi-groep (monoïde) $\langle X,\psi\rangle$ is commutatief, als voor alle $a,b \in X$ geldt $\psi(a,b) = \psi(b,a)$ (of: $a * b = b * a$).
Een verzameling W ($W \subseteq X$ en $\langle X,\psi\rangle$ is een semi-groep) wordt stabiel genoemd, als voor alle $a,b \in W$ geldt: $\psi(a,b) \in W$.
Voor elke stabiele verzameling W, $W \subseteq X$ geldt dat $\langle W,\psi/W\rangle$ een semi-groep is; deze semi-groep wordt een subsemi-groep van $\langle X,\psi\rangle$ genoemd. Is $\langle X,\psi\rangle$ een monoïde en $e \in W$, dan is $\langle W,\psi/W\rangle$ ook een monoïde (een submonoïde van $\langle X,\psi\rangle$).

Stelling (2.1): De doorsnede van een niet-lege klasse van subsemi-groepen (submonoïden) van de semi-groep (monoïde) $\langle X,\psi\rangle$ is meer een subsemi-groep (submonoïde) van $\langle X,\psi\rangle$.

Bewijs: Zij K ($K \neq \emptyset$) een willekeurige indexverzameling en W_k, $W_k \subseteq X$, stabiel voor alle $k \in K$.
$\langle W_k,\psi/W_k\rangle$, $k \in K$ is dus een subsemi-groep van $\langle X,\psi\rangle$.
Definieer $W = \bigcap_{k\in K} W_k$. W is nu ook een stabiele deelverzameling van X. Hieruit volgt het gestelde nl.: $\langle W,\psi/W\rangle$ is subsemi-groep van $\langle X,\psi\rangle$.
Als $\langle X,\psi\rangle$ een monoïde is en $e \in W_k$ voor alle $k \in K$, dan ook $e \in W$; dus $\langle W,\psi/W\rangle$ is een monoïde.

U is een niet-lege deelverzameling van X ($\langle X,\psi\rangle$ een semi-groep) en $\langle W,\psi/W\rangle$ de doorsnede van alle semi-groepen die de elementen van U bevatten. Men zegt nu dat de semi-groep $\langle W,\psi/W\rangle$ gegenereerd wordt door U. In het geval $W = X$ noemt men U de verzameling generators van $\langle X,\psi\rangle$.

Voorbeeld 5. $\Sigma = \{\sigma_0,\sigma_1,\ldots,\sigma_{n-1}\}$ is een alfabet waarmede eindige symboolrijen of woorden worden gevormd; bijvoorbeeld $x = \sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$ ($\sigma_{i_j} \in \Sigma$ $j = 1,2,\ldots,k$). Het zgn. lege woord wordt aangegeven met Λ. De woordlengte $\ell(x)$ van $x = \sigma_{i_1}\ldots\sigma_{i_k}$ ($k = 1,2,3,\ldots$) wordt gedefinieerd als
$\ell(x) = k$ $n\ell(\Lambda) = 0$.
De concatenatie van $x = \sigma_{i_1}\ldots\sigma_{i_k}$ en $y = \sigma_{j_1}\ldots\sigma_{j_\ell}$ wordt gedefinieerd als:

$$x * y = (\sigma_{i_1}\ldots\sigma_{i_k}) * (\sigma_{j_1}\ldots\sigma_{j_\ell}) = \sigma_{i_1}\ldots\sigma_{i_k}\,\sigma_{j_1}\ldots\sigma_{j_\ell};$$

$$x * \Lambda = \Lambda * x = x.$$

$\Sigma^k = \{x \mid x = \sigma_{i_1} \ldots \sigma_{i_k},\ \sigma_{i_j} \in \Sigma,\ j = 1,2,\ldots,k\}$ voor $k = 1,2,\ldots$ en $\Sigma^0 = \{\Lambda\}$.

$\Sigma^+ = \bigcup_{k=1}^{\infty} \Sigma^k$ en $\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma^k$.

Bewijs dat Σ^+ een semi-groep en Σ^* een monoïde is.

Stelling (2.2): Iedere semi-groep $\langle X,\psi\rangle$ kan uitgebreid worden tot een monoïde $\langle X',\psi\rangle$ met $X' = X \cup \{e\}$, $e \notin X$.

Bewijs: Definieer $\psi(e,e) = e$, $\psi(e,x) = \psi(x,e) = x$ voor alle $x \in X$.

3. Homomorfismen

Een homomorfisme van een semi-groep $\langle X,\psi\rangle$ in een semi-groep $\langle X',\psi'\rangle$ is een functie $f: X \to X'$ met de eigenschap $f(\psi(a,b)) = \psi'(f(a), f(b))$ (of anders $f(a * b) = f(a) * f(b)$).
Als zo'n homomorfisme bestaat, dan noemt men de semi-groepen $\langle X,\psi\rangle$ en $\langle X',\psi'\rangle$ homomorf.
Een homomorfisme f is een isomofisme als f bijectief is (één - één en op); in dit geval noemt men de betreffende semi-groepen isomorf.

Voorbeeld 5. $\langle R,+\rangle$ en $\langle R,\times\rangle$ zijn resp. de additieve en multiplicatieve semi-groep over de reële getallen. $f: R \to R$ is gedefinieerd door $f(x) = e^x$ $x \in R$.

Voorbeeld 6. $\langle Z_{17},+\rangle$ is de additieve semi-groep van de restklassen modulo 17 over de natuurlijke getallen N. Een homomorfisme f van $\langle N,+\rangle$ in $\langle Z_{17},+\rangle$ wordt gedefinieerd door $f: N \to Z_{17}$; $f(n) = z_i$ voor $n = 17$ voud $+ i$ $(0 \leq i \leq 16)$ en $z_i \in Z_{17} = \{z_0,z_1,\ldots,z_{16}\}$.

Stelling (3.1): $\langle X,\psi_1\rangle$, $\langle Y,\psi_2\rangle$ en $\langle Z,\psi_3\rangle$ zijn semi-groepen. Als f een homomorfisme is van $\langle X,\psi_1\rangle$ in $\langle Y,\psi_2\rangle$ en g een homomorfisme van $\langle Y,\psi_2\rangle$ in $\langle Z,\psi_3\rangle$, dan is $f \circ g$ een homomorfisme van $\langle X,\psi_1\rangle$ in $\langle Z,\psi_3\rangle$.

Stelling (3.2): Als h een homomorfisme is van de semi-groep $\langle X,\psi_1\rangle$ in $\langle Y,\psi_2\rangle$, dan is het beeld van een subsemi-groep van $\langle X,\psi_1\rangle$ een semi-groep van $\langle Y,\psi_2\rangle$.

Stelling (3.3): Als $\langle X,\psi_1\rangle$ en $\langle Y,\psi_2\rangle$ monoïden zijn met respectievelijk e_1 en e_2 als eenheid en f een homomorfisme is van $\langle X,\psi_1\rangle$ in $\langle Y,\psi_2\rangle$ en $f(X) = Y$, dan geldt $f(e_1) = e_2$.

Een equivalentierelatie E over de semi-groep $\langle X,*\rangle$ is een congruentie als:

1) uit $x \, E \, y$ volgt, dat voor alle $u \in X$

$$x * u \, E \, y * u, \quad x,y \in X.$$

2) uit $x \, E \, y$ volgt, dat voor alle $z \in X$

$$z * x \, E \, z * y, \quad x,y \in X.$$

Een equivalentierelatie die alleen aan (1) voldoet noemt men een rechtercongruentie over $\langle X,*\rangle$; analoog definieert men het begrip linkercongruentie. Voor een commutatieve semi-groep vallen beide begrippen samen.
De equivalentieklassen van een congruentie over $\langle X,*\rangle$ noemt men de congruentieklassen.
Als E een congruentie is over $\langle X,*\rangle$, dan volgt uit $x \, E \, y$ en $z \, E \, u$ altijd: $x * z \, E \, y * u$ $(x,y,z,u \in X)$. Dit betekent dat voor elk tweetal congruentieklassen $[x]_E$ en $[y]_E$, $x,y \in X$, (definitie: $[x]_E = \{u \mid u \in X \text{ èn } x \, E \, u\}_k$), het product van een element uit $[x]_E$ met een element uit $[y]_E$ altijd indezelfde congruentieklasse ligt, nl. in $[x * y]_E$.
Uit het bovenstaande volgt, dat de groepoïde $\langle Y,\psi\rangle$ met $Y = \{[x]_E \mid x \in X\}$ en $\psi([x]_E, [y]_E) = [x * y]_E$ $([x]_E$ en $[y]_E \in Y)$ een semi-groep is. Deze semigroep, notatie $X|E$ of $\langle X,\psi\rangle \mid E$, noemt men de faktorsemi-groep van $\langle X,*\rangle$ ten opzichte van de congruentie E.

Voorbeeld 8. $\langle X,*\rangle$ met $X = \Sigma^*$ en $*$ is de concatenatie. Definieer de relatie E als volgt: $x \, E \, y \iff \ell(x) = \ell(y)$, $x,y \in \Sigma^*$.
E is een congruentie; de congruentieklassen zijn: Σ^k $k = 0,1,2,\ldots$. De index van E is oneindig groot.

Stelling (3.4). Als E een congruentie is over de semi-groep $\langle X,*\rangle$, dan is $f: X \to \{[x]_E \mid x \in X\}$, met $f(x) = [x]_E$ voor alle $x \in X$, een homomorfisme van $\langle X,*\rangle$ in $X|E$.

Voorbeeld 9. $\langle X,\psi_1\rangle$ en $\langle Y,\psi_2\rangle$ zijn semi-groepen. $f: X \to Y$ een homomorfisme van $\langle X,\psi_1\rangle$ in $\langle X,\psi_2\rangle$.
De relatie E over $\langle X,\psi_1\rangle$ gedefinieerd door: $x \, E \, y \iff f(x) = f(y)$ $(x,y \in X)$, is een congruentie.
$X|E$ en $\langle Y,\psi_2\rangle$ zijn isomorf.

4. Eindige Automaten

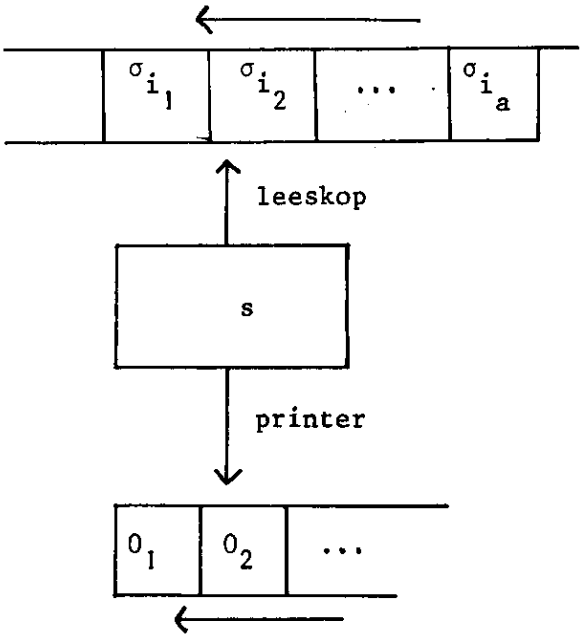
Een eindige automaat is een mathematische machine. Hiervan kan het volgende fysische model worden aangegeven

(a) Inputband. De eindige band is in vakjes verdeeld. In elk vakje staat een symbool van het woord $x(x \in \Sigma^*)$ dat op de band staat. De band beweegt van rechts naar links.

(b) Leeskop. De leeskop leest in elk vakje het betreffende symbool. Start in vak met σ_{i_1} en stopt in vak σ_{i_a}.

(c) Centrale eenheid. Deze kan in een bepaalde toestand verkeren. Het totaal aantal toestanden is eindig. De overgang naar een nieuwe toestand is afhankelijk van het gelezen band symbool en de toestand waarin de machine verkeert.

(d) Outputband. De band is in vakjes verdeeld. O is outputalfabet. De printer drukt, afhankelijk van het gelezen symbool en de toestand, een element van O in een vakje op de band. Ook de outputband beweegt van rechts naar links.



De meer formele beschrijving van een eindige automaat wordt gegeven door een quintuple $T = \langle \Sigma, S, M, N, O \rangle$.

$\Sigma = \{\sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$: inputalfabet

$S = \{s_0, s_1, \ldots, s_{k-1}\}$: verzameling van toestanden

$M : S \times \Sigma \to S$: transitofunctie

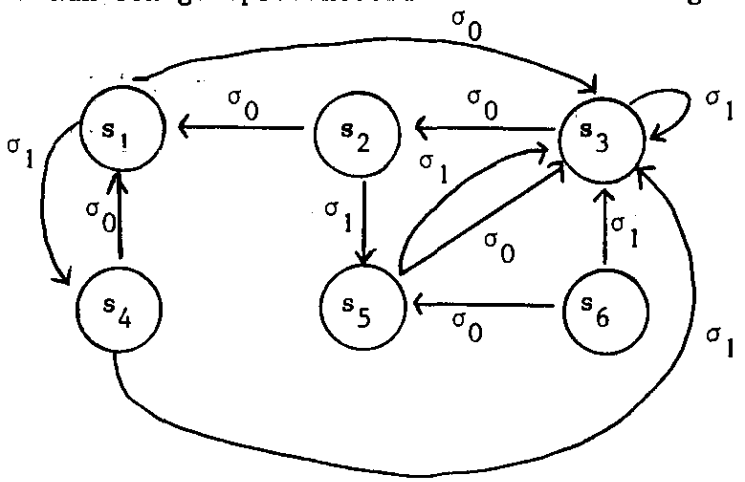
$N : S \times \Sigma \to O$: printfunctie

$O = \{O_0, \ldots, O_{m-1}\}$: outputalfabet

Als $N: S \to O$ dan spreekt men van een Moore-automaat, als $N: S \times \Sigma \to O$ van een Mealy-automaat.

In deze paragraaf zullen slechts eigenschappen besproken worden, die alleen afhankelijk zijn van de transitofunctie M. In verband hiermede definieren we het begrip semi-automaat of transitosysteem.
Een semi-automaat is een triple $A = \langle \Sigma, S, M \rangle$. Σ, S en M hebben dezelfde betekenis als in de definitie van T.
Definieer nu de afbeelding $M_\sigma: S \to S$, $\sigma \in \Sigma$ als volgt: $M_\sigma(s) = M(s,\sigma)$ voor alle $s \in S$.

Voorbeeld 10. $A = \langle \{\sigma_0,\sigma_1\}, \{s_1,s_2,s_3,s_4,s_5,s_6\}, M \rangle$. M is gedefinieerd door onderstaande tabel.
A kan ook gerepresenteerd worden door een gerichte graaf.



M	σ_0	σ_1
1	3	4
2	1	5
3	2	3
4	1	3
5	3	3
6	5	3

Met behulp van de afbeeldingen $M_\sigma (\sigma \in \Sigma)$ definieren we voor ieder woord $x \in \Sigma^*$ een afbeelding $M_x: S \to S$.
$x = \Lambda$ dan: M_x is de identieke afbeelding;
$x = \sigma_{i_1} \ldots \sigma_{i_n}$ dan: $M_x = M\sigma_{i_1} \circ M\sigma_{i_2} \circ \ldots \circ M\sigma_{i_k}$.
Voor deze afbeeldingen geldt: $M_x \circ M_y = M_{xy}$.

$G_A = \langle \{M_x \mid x \in \Sigma^*\}, 0 \rangle$ is de semi-groep van de semi-automaat $A = \langle \Sigma, S, M \rangle$.
Definieer nu de relatie E over de semi-groep $\langle \Sigma^*, * \rangle$ (zie vb. 9) als volgt:

$$x \; E \; y \iff M_x = M_y, \; x,y \in \Sigma^*.$$

E is een congruentie over $\langle \Sigma^*, * \rangle$. De index van E is eindig, want het aantal verschillende afbeeldingen van S in S is eindig.

Stelling (4.1). De semi-groepen G_A en Σ^*/E zijn isomorf.
Bewijs dit.
Analoog als bij semi-groepen kan men ook het homomorfie begrip voor semi-automaten definieren. In verband met de formulering van stelling (4.2) definieren we alleen de isomorfie van semi-automaten.

De semi-automaten $A_1 = \langle \Sigma, S_1, M_1 \rangle$ en $A_2 = \langle \Sigma, S_2, M_2 \rangle$ zijn isomorf als er een afbeelding $f: S \to S$ (één - één en op) bestaat met de eigenschap: $f(M_1(s,\sigma)) = M_2(f(s),\sigma)$ voor alle $s \in S$ en $\sigma \in \Sigma$.

Een semi-automaat $A = \langle \Sigma, S, M \rangle$ is sterk samenhangend, als er voor ieder tweetal elementen $s, s' \in S$ een woord $x \in \Sigma^*$ bestaat, zodat $M_x(s) = s'$.

Dit betekent dat er in de graaf van A (zie vb. 10) altijd een weg van s naar s' te vinden is.

Een semi-automaat $A = \langle \Sigma, S, M \rangle$ is een permutatie semi-automaat als G_A een groep is.

Hieruit volgt:

(a) Als $M_x(s) = M_x(s')$ dan $s = s'$.

(b) M_σ is voor iedere $\sigma \in \Sigma$ een permutatie van S.

$A_1 = \langle \Sigma, S_1, M_1 \rangle$ en $A_2 = \langle \Sigma, S_2, M_2 \rangle$ zijn semi-automaten met $1,2 \notin S_1, S_2$.

De directe som van A_1 en A_2, notatie $A = A_1 \oplus A_2$, is een semi-automaat $A = \langle \Sigma, S, M \rangle$ met:

$$S = (S_1 \times \{1\}) \cup (S_2 \times \{2\}),$$

$$M((s,1),\sigma) = (M_1(s,\sigma),1) \text{ voor } s \in S_1,$$

$$M((s,2),\sigma) = (M_2(s,\sigma),2) \text{ voor } s \in S_2.$$

Het is duidelijk, dat men op analoge wijze de directe som van n semi-automaten $A_1,\ldots,A_n$ met $i \notin S_j$ (voor $i,j = 1,2,\ldots,n$) kan definieren.

Stelling (4.2). Iedere permutatie semi-automaat $A = \langle \Sigma, S, M \rangle$ is sterk samenhangend of isomorf met de directe som van n ($n \geq 2$) sterk samenhangende permutatie semi-automaten.

Bewijs.

(1) Definieer de relatie E over S als volgt:

$$s \; E \; s' \iff \exists x \quad x \in \Sigma^* \wedge M_x(s) = s', \; s,s' \in S.$$

E is een equivalentierelatie want A is een permutatie semi-automaat; bovendien is de index van E eindig.

2) De equivalentieklassen van E zijn $S_1, S_2, \ldots, S_k$. Definieer de semi-automaat $A_i = \langle \Sigma, S_i, M_i \rangle$. $M_i(s,\sigma) = M(s,\sigma)$ $(s \in S_i)$; A_i is sterk samenhangend.

(3) De directe som $\bar{A} = A_1 \oplus, A_2 \oplus \ldots \oplus A_k$ is isomorf met A. De functie $f(s) = (s,j)$. $s \in S_j$ is een één - één afbeelding van A op $\bar{A}$. Het is gemakkelijk in te zien dat f een isomorfisme is, want voor $M(s,\sigma) = s'$, $s,s' \in S_j$, geldt:

$$f(M(s,\sigma)) = f(s') = (s',j) = (M_j(s,\sigma),j) = \bar{M}((s,j),\sigma) = \bar{M}(f(s),\sigma).$$

5. Literatuur.

[1] Ginzburg A. - Algebraic Theory of Automata. New York - London 1968.

[2] Hartmanis J., Stearns R.E. - Algebraic Structure of Sequential Machines. London - Sydney - Toronto 1966.

[3] Nelson R.J. - Introduction to Automata. New York - London 1968.

[4] Rabin M.O., Scott D. - Finite Automata and Their Decision Problems. IBM. J. Res. Dev. 3 (1959), pp. 114-125.

[5] Ljapin E.S. - Semigroups. A.M. Soc. 1963.

TECHNISCHE HOGESCHOOL EINDHOVEN

Tentamen Discrete Wiskunde op vrijdag 25 juni 1971, 9.00-12.00 uur.

N.B. U behoeft niet alle vraagstukken te maken; U kunt een keuze maken. De vraagstukken zijn niet gelijkwaardig. Wij verwachten echter, dat U van de met letter A gemerkte vraagstukken er minstens 2, en van de met letter B gemerkte opgaven er minstens 3 maakt. Daarbij kunt U de met (*) aangegeven onderdelen in eerste instantie weglaten.

A1. Stel

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

Een binaire code C van lengte 8 wordt gedefinieerd door

$\underline{x} \in C$ dan en alleen dan, als $H\underline{x} = \underline{0}$.

Bewijs:

(a) C is een lineaire code.

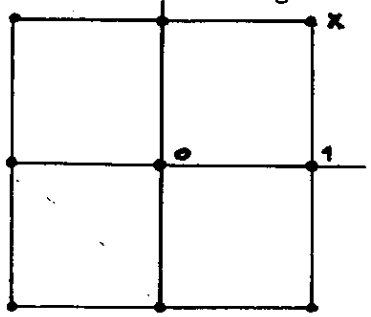
(b) De codewoorden van C hebben onderling een Hamming afstand ≥ 4.

(c) Elk codewoord heeft gewicht 0, 4 of 8.

(d) C bevat 14 codewoorden van gewicht 4.

(*) (e) De 14 codewoorden van gewicht 4 vormen een 3-design, waarbij elk drietal punten in één blok ligt.

A2.



(a) Zij GF(3) := {0,1,-1}. In de vectorruimte V(2,3) van dimensie 2 over GF(3), (zie figuur) is gegeven de nulvector 0 en de basisvectoren 1 en x.

Schrijf de overige zes vectoren van de figuur als lineaire combinaties van de vectoren 1 en x.

(b) $V(2,3)$ wordt tot $GF(3^2)$ gemaakt met behulp van het irreducibele polynoom $x^2 + x - 1$ over $GF(3)$.
Schrijf de overige zes vectoren van de figuur als machten van het primitieve element x.

(c) Welke elementen van $GF(3^2)$ zijn een kwadraat?

(d) Construeer een conferentiematrix van de orde 10.

A3. Gegeven zijn 16 punten, die worden gesymboliseerd door de 16 letters in het volgende vierkant

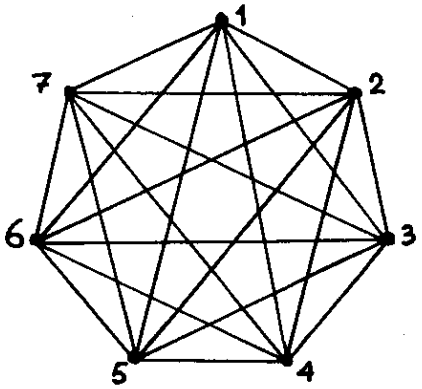
A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

(a) Beschrijf 16 blokken, die met de 16 punten een symmetrisch block design vormen, met 6 punten per blok, en 2 blokken door elk paar punten.

(b) Zij $N = (n_{ij})$ de punt-blok incidentiematrix van het onder (a) bedoelde block design, d.w.z. $n_{ij} = 1$ (0) als punt i wèl (niet) in blok j ligt. Bereken NN^T en $N\underline{j}$, waarbij $\underline{j}$ de vector met uitsluitend componenten 1 is.

(c) Hoe kan men uit het bovenstaande een Hadamardmatrix van de orde 16 maken? (Het is niet nodig deze H_{16} geheel uit te schrijven.)

B1.



(a) Bepaal 7 driehoeken met hoekpunten uit {1,2,3,4,5,6,7} zo, dat elk paar driehoeken één hoekpunt gemeen heeft.

(*) (b) Bepaal 14 verschillende driehoeken met hoekpunten uit {1,2,3,4,5,6,7} zo, dat elk paar punten in twee driehoeken ligt.

B2. Gegeven is dat er ten hoogste M binaire vectoren bestaan van lengte n, die onderling een Hamming afstand $\geq$ d hebben.
Bewijs dat elke binaire code van lengte n + 1, waarvan de codewoorden onderlinge afstand $\geq$ d hebben, uit hoogstens 2M woorden bestaat.

B3. De 100 plaatsen van een bioscoop voor militairen zijn bezet door soldaten, luitenants en generaals, die voor hun zitplaats respectievelijk 1, 5 en 20 gulden moeten betalen. De totale opbrengst bedraagt 325 gulden. Hoeveel soldaten, luitenants, generaals zijn er aanwezig?

B4. "Voor alle natuurlijke getallen $k \geq 5$ geldt

$$2^{4k} \equiv b \pmod 5\text{"} .$$

Gegeven is, dat deze zin in precies één van de volgende gevallen waar is (en dus in de overige drie gevallen onwaar)

(a) $b = 5^4$

(b) 5 is deelbaar op b - 2

(c) $b \equiv 1 \pmod 5$

(d) $b \equiv 2 \pmod 5$.

In welk geval is de zin waar?
Licht Uw antwoord toe.

B5. Gegeven

$$A := \begin{bmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \\ 3 & 4 & 5 & \ldots & 1 & 2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ n & 1 & 2 & \ldots & n-2 & n-1 \end{bmatrix}, \quad B := \begin{bmatrix} n & n-1 & \ldots & 3 & 2 & 1 \\ 1 & n & \ldots & 4 & 3 & 2 \\ 2 & 1 & \ldots & 5 & 4 & 3 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ n-1 & n-2 & \ldots & 2 & 1 & n \end{bmatrix}$$

Bewijs dat A en B orthogonale Latijnse vierkanten zijn dan en alleen dan als n oneven is.

TECHNISCHE HOGESCHOOL EINDHOVEN

Tentamen Discrete Wiskunde op zaterdag 25 september 1971, 9.00-12.00 uur.

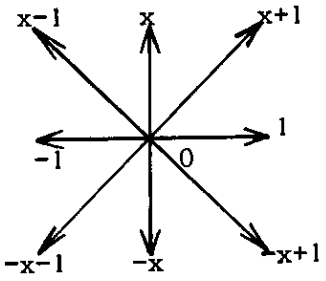
De tien vraagstukken zijn afkomstig uit de volgende hoofdstukken:

Hoofdstuk	Vraagstuk									
	1	2	3	4	5	6	7	8	9	10
2. Getaltheorie					5	6	7		9	
3. Galois lichamen	1									
4. Orthogonale matrices	1									10
5. Block designs		2	3						9	10
6. Eindige meetkunde			3						9	
7. Latijnse vierkanten						6				
8. Codes		2						8		
9. Grafen				4						

Vraagstukken 1 t/m 5 leveren ieder 10 punten op,
vraagstukken 6 t/m 10 leveren ieder 5 punten op, mits goed opgelost.
Niet alle vraagstukken behoeven te worden gemaakt. Men is vrij in zijn keuze.

N.B. Er zijn 35 punten nodig om een voldoende cijfer te krijgen.

(10) 1. De 9 elementen van GF(9) worden voorgesteld door alle getallen van de vorm $ax + b$, waarbij a en b doorlopen GF(3) en x voldoet aan $x^2 + 1 = 0$



(3) a) Welke elementen van GF(9) \ {0} zijn kwadraat?

(3) b) Welke van de 8 elementen $1 - y$, $y \in GF(0) \setminus \{1\}$ zijn kwadraat?

(4) c) Construeer een Conferentie matrix van de orde 10.

(10) 2. De (0,1) matrix N heeft afmeting 6×10. Elke rij bevat 5 enen en 5 nullen. De Hamming afstand van elk paar rijen is ≥ 6.

(2) a) Bewijs dat elk paar rijen ten hoogste 2 enen gemeen heeft.

(3) b) Bewijs dat elke kolom ten hoogste 3 enen heeft.

(2) c) Bewijs dat elke kolom precies 3 enen heeft.

(3) d) Bewijs dat N de incidentiematrix van een block design is en geef de parameters van dit block design.

(10) 3. Zij f(n) het maximum aantal tripels, dat kan worden gekozen uit een verzameling van n symbolen, zodat elk paar tripels één symbool gemeen heeft.

(2) a) Wat is f(7)?

(2) b) Bereken f(n) voor n = 3,4,5,6.

(2) c) Uit 15 symbolen kunnen twee totaal verschillende stelsels van 7 tripels worden gekozen, zodat elk paar tripels één symbool gemeen heeft. Geef deze stelsels aan.

(4) d) Bereken f(n) voor $n \geq 7$.

(10) 4. Zij G een graaf met n punten zodat

i) elk verbonden paar punten heeft $\lambda = 0$ tussenpunten (verbonden met beide),

ii) elk niet-verbonden paar punten heeft $\mu = 1$ tussenpunten (verbonden met beide),

iii) elk punt is verbonden met k andere punten (k constant).

(3) a) Bewijs dat er geen driehoeken en geen vierhoeken in G zijn (dus geen △ en geen □).

(4) b) Bewijs dat $n = 1 + k + k(k-1) = 1 + k^2$.

(3) c) Teken zo'n graaf G voor k = 3.

(10) 5. Is het mogelijk om de getallen 1,2,3,...,12 zo in een 3 × 4 matrix

$$A = [a_{ij}] \qquad (i = 1,2,3;\ j = 1,2,3,4)$$

te plaatsen zodat voor alle a_{ij} geldt

$$(a_{ij} - i)(a_{ij} - j) \equiv 0 \pmod{12}?$$

Zo neen, waarom niet? Zo ja, hoe?

(5) 6. Gegeven is het Latijnse vierkant

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix} = [a_{ij}], \quad \text{met} \quad a_{ij} = j - i + 1 \pmod 4.$$

Bewijs, dat er geen 4 × 4 Latijns vierkant B bestaat zodat A en B orthogonaal zijn.

(5) 7. Zij n een positief geheel getal. Wij delen alle getallen van

$$\{1,7,13,19,25,\ldots\} = \{6t + 1;\ t = 0,1,2,\ldots\}$$

door n en beschouwen de resten. Komen alle getallen 0,1,2,...,n-1 als rest voor?
Motiveer Uw antwoord!

(5) 8. Notatie: Onder een binaire (M,n,d)-code verstaan we een code bestaande uit M codewoorden van lengte n met onderlinge Hamming afstand ≥ d.

Voor de natuurlijke getallen n en M en het <u>oneven</u> getal d zij C een binaire (M,n,d)-code,

(2) a) Construeer uit C een binaire (M,n+1,d+1)-code.

(3) b) Stel dat code C het getal M maximaal heeft, d.w.z. dat voor iedere binaire (M_1,n,d)-code geldt $M_1 \leq M$.
Bewijs dat voor iedere binaire $(M_2,n+1,d+1)$-code geldt $M_2 \leq M$.

(5) 9. Een Steiner Tripel Systeem is een verzameling van v punten en b tripels van de v punten, zodat elk paar punten in precies één tripel zit.

(2) a) Bepaal b als een functie van v.

(2) b) Laat zien dat v aan $v \equiv 1$ of 3 (mod 6) voldoet.

(1) c) Teken een voorbeeld van een Steiner Tripel Systeem.

(5) 10. Gegeven is de 4t X 4t Hadamard matrix

$$H = \begin{bmatrix} 1 & j^T \\ j & R \end{bmatrix}.$$

(3) a) Bereken Rj, j^TR en RR^T.

(2) b) Welke zijn de parameters van het block design R^* dat ontstaat door in R de getallen +1 door 0 en de getallen −1 door 1 te vervangen?