Printed at the Mathematical Centre at Amsterdam,49,2nd Boerhaavestraat, The Netherlands.

The Mathematical Centre, founded the 11th of February 1946, is a non - profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.) and the Central Organization for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

MC SYLLABUS

5

MC SYLLABUS

5

COLLOQUIUM DISCRETE WISKUNDE

DOOR

J.H. VAN LINT
J.J. SEIDEL
P.C. BAAYEN

MATHEMATISCH CENTRUM AMSTERDAM

1968

Hoofdstuk I

Hoofdstuk II

Hoofdstuk III

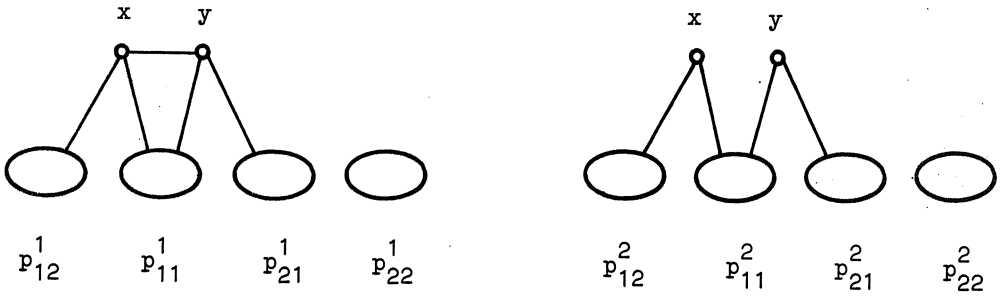
Hoofdstuk I. Configuraties

1. Sterke grafen

Wij beschouwen gewone grafen van eindige orde v, niet gericht, met enkelvoudige verbindingen en zonder lussen.

Zij x een punt van een graaf. Noem $n_1(x)$ het aantal punten dat met x is verbonden en $n_2(x)$ het aantal punten dat niet met x is verbonden. Dan is $n_1(x) + n_2(x) = v - 1$. Een graaf heet regulier wanneer $n_1(x)$ en $n_2(x)$ onafhankelijk zijn van x.

Laat x en y twee verschillende punten zijn van een graaf, verbonden (h = 1) dan wel niet verbonden (h = 2). Noem $p_{ij}^h(x,y)$ het aantal punten dat met x en met y (i = j = 1), dat wel met x en niet met y (i = 1, j = 2), dat niet met x en wel met y (i = 2, j = 1), dat niet met x en niet met y (i = j = 2) is verbonden:



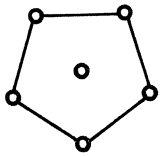
Een graaf heet sterk wanneer hij niet leeg en niet volledig is en wanneer

$$p_{12}^1(x,y) + p_{21}^1(x,y) \qquad \text{en} \qquad p_{12}^2(x,y) + p_{21}^2(x,y)$$

onafhankelijk zijn van x en y. Een graaf heet sterk regulier wanneer hij sterk en regulier is. In een sterk reguliere graaf zijn de getallen $p_{ij}^h(x,y)$, voor alle h,i,j = 1, 2, onafhankelijk van x en y.

Het eerste en het vierde van de volgende voorbeelden betreft een sterke graaf die niet regulier is. De overige voorbeelden betreffen sterk reguliere grafen.

Vb. 1

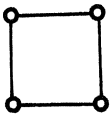


De icosaëder graaf, met

$$p_{12}^1(x,y) + p_{21}^1(x,y) = 2,$$

$$p_{12}^2(x,y) + p_{21}^2(x,y) = 2.$$

Vb. 2

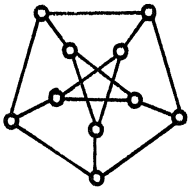


De graaf $L_2(2)$ met

$$(p_{ij}^1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$(p_{ij}^2) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Vb. 3



De Petersen graaf, met

$$(p_{ij}^1) = \begin{pmatrix} 0 & 2 \\ 2 & 4 \end{pmatrix},$$

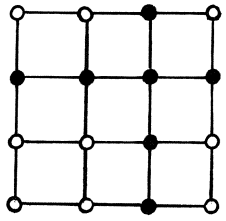
$$(p_{ij}^2) = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}.$$

Vb. 4 De volledige paargraaf $K(\alpha,\beta)$, $\alpha + \beta = v$, $\alpha > 0$, $\beta > 0$ is de graaf waarvan de verzameling der punten bestaat uit twee niet lege disjuncte delen van ordes α en β, elk zonder verbindingen, terwijl elk paar punten die tot verschillende delen behoren is verbonden. $K(\alpha,\beta)$ is een sterke graaf met

$$p_{12}^1(x,y) + p_{21}^1(x,y) = v - 2,\ p_{12}^2(x,y) + p_{21}^2(x,y) = 0,$$

maar is slechts regulier als $\alpha = \beta$.

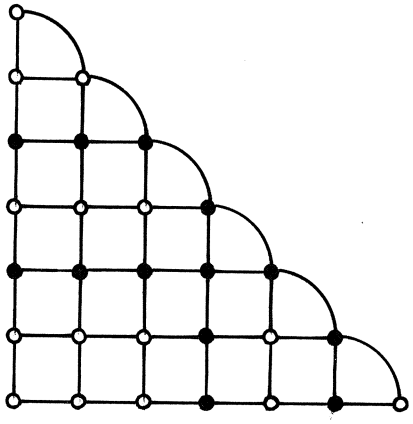
Vb. 5



$L_2(4)$, de lattice graaf van de orde 4, is de hiernaast weergegeven graaf, waarin elk punt x verbonden is met alle punten die met x op dezelfde horizontale of verticale lijn liggen; er geldt

$$(p^1_{ij}) = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}, (p^2_{ij}) = \begin{pmatrix} 2 & 4 \\ 4 & 4 \end{pmatrix}.$$

Vb. 6



T(8), de triangulaire graaf van de orde 8, is de hiernaast weergegeven graaf, waarin elk punt x verbonden is met alle punten die met x op eenzelfde lijn liggen; er geldt

$$(p^1_{ij}) = \begin{pmatrix} 6 & 5 \\ 5 & 10 \end{pmatrix}, (p^2_{ij}) = \begin{pmatrix} 4 & 8 \\ 8 & 6 \end{pmatrix}.$$

Vb. 7 $L_3(3)$. Verbind in $L_2(3)$ de door eenzelfde letter aangeduide punten in

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \quad \cdot \quad (p^1_{ij}) = \begin{pmatrix} 3 & 2 \\ 2 & 0 \end{pmatrix}, (p^2_{ij}) = \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}.$$

Opmerking. De configuratie van Desargues, waarbij twee punten verbonden heten als zij op een rechte lijn liggen, is het complement van de Petersen graaf. De configuratie van Pappus is dezelfde als de in vb. 7 genoemde $L_3(3)$.

Stelling 1.1. Voor een sterke graaf, die niet is $K(\alpha,\beta)$ of het complement daarvan, zijn de getallen

$$p^1_{12}(x,y) + p^1_{21}(x,y) \quad \text{en} \quad p^2_{12}(x,y) + p^2_{21}(x,y)$$

beide even.

Bewijs. Zij h = 1 of h = 2. Als voor de punten x en y een graaf $p_{12}^{h}(x,y) + p_{21}^{h}(x,y)$ even (oneven) is, dan hebben $n_1(x)$ en $n_1(y)$ dezelfde (verschillende) pariteit. Zou nu voor een sterke graaf $p_{12}^{1}(x,y) + p_{21}^{1}(x,y)$ even en $p_{12}^{2}(x,y) + p_{21}^{2}(x,y)$ oneven zijn, dan zou $n_1(x) \equiv n_1(y) \pmod 2$ voor elk verbonden, en $n_1(x) \not\equiv n_1(y) \pmod 2$ voor elk niet verbonden paar x,y. Dus zou uit het verbonden zijn van x,y en van y,z volgen dat x en z niet verbonden zijn. Eveneens zou uit het niet verbonden zijn van x,y en van y,z volgen dat x en z niet verbonden zijn. De graaf zou dan $K(\alpha,\beta)$ zijn, die is uitgesloten. De veronderstelling dat $p_{12}^{1}(x,y) + p_{21}^{1}(x,y)$ oneven en $p_{12}^{2}(x,y) + p_{21}^{2}(x,y)$ even is leidt tot het complement van $K(\alpha,\beta)$. Daar de getallen niet beide oneven kunnen zijn is de stelling bewezen.

2. Verbindingsmatrices

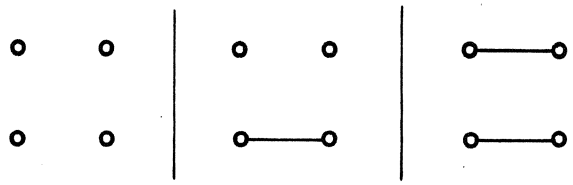
Een graaf wordt beschreven door de verzameling V van zijn punten en de symmetrische matrix A van de orde v met de elementen

$$\begin{aligned} A(x,y) &= -1 \quad \text{als } x \in V \text{ en } y \in V \text{ verbonden,} \\ &= 1 \quad \text{als } x \in V \text{ en } y \in V \text{ niet verbonden,} \\ &= 0 \quad \text{als } x = y \in V. \end{aligned}$$

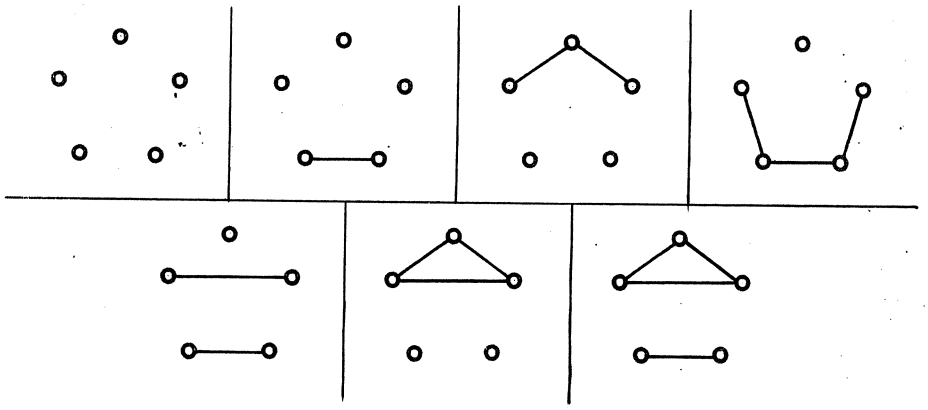
De matrix A heet de verbindingsmatrix van de graaf $\{V,A\}$.

Voor een graaf $\{V,A\}$ wordt de operatie complementatie aan $x \in V$ als volgt gedefinieerd: schrap de bestaande verbindingen van x en voeg toe de niet bestaande verbindingen van x. Het effect van complementatie aan x op de verbindingsmatrix is, dat de met x corresponderende rij en kolom met -1 worden vermenigvuldigd. Complementatie aan de diverse punten van een gegeven verzameling V genereert een equivalentierelatie op de verzameling van alle grafen op V.

Vb. 1 Er zijn drie klassen van grafen op 4 punten, gerepresenteerd door de volgende grafen



Vb. 2 Er zijn zeven klassen van grafen op 5 punten, gerepresenteerd door de volgende grafen



Probleem. Geef, voor alle v, een overzicht van de equivalentieklassen, onder complementatie, van alle v-grafen.

Voor tabellen voor n = 2, ..., 7, zie [23].

Wij karakteriseren regulariteit en sterkheid van een graaf in termen van de verbindingsmatrix A van de graaf. De eenheidsmatrix van de orde v wordt aangeduid door I, de matrix van de orde v waarvan alle elementen 1 zijn door J.

Stelling 2.1. Een graaf $\{V,A\}$ is regulier dan en slechts dan als er een getal ρ_0 bestaat zodat $AJ = \rho_0 J$.

Bewijs. Een punt x van een graaf is verbonden met n_1 andere en niet verbonden met n_2 andere punten dan en slechts dan als de met het punt corresponderende rij van de verbindingsmatrix de som ρ_0 heeft, met $\rho_0 = n_2 - n_1$, $n_1 + n_2 = v - 1$. Hieruit volgt de bewering.

Stelling 2.2. Een graaf $\{V,A\}$ is sterk dan en slechts dan als er getallen ρ_1 en ρ_2 bestaan zodat geldt

$$(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J.$$

Bewijs. Zij $\{V,A\}$ niet leeg en niet volledig. Wij berekenen het element met indices x,y van de matrix $(A - \rho_1 I)(A - \rho_2 I)$, gebruikmakend van de bovengedefinieerde getallen $p_{ij}^h(x,y)$ voor de punten x en y van de graaf, waarvoor $A(x,y) = (-1)^h$, h = 1, 2. Het gevraagde matrix element is het inproduct van de rijen

$$-\rho_1 \quad (-1)^h \quad - \cdot\cdot - \quad - \cdot\cdot - \quad + \cdot\cdot + \quad + \cdot\cdot + \quad \text{van } A - \rho_1 I,$$

$$(-1)^h \quad -\rho_2 \quad - \cdot\cdot - \quad + \cdot\cdot + \quad - \cdot\cdot - \quad + \cdot\cdot + \quad \text{van } A - \rho_2 I,$$

$$(1 \quad , \quad 1 \quad , \quad p_{11}^h \quad , \quad p_{12}^h \quad , \quad p_{21}^h \quad , \quad p_{22}^h \quad \text{stuks}),$$

en is gelijk aan

$$-(-1)^h(\rho_1 + \rho_2) + p_{11}^h + p_{22}^h - p_{12}^h - p_{21}^h =$$

$$= v - 1 - (-1)^h(\rho_1 + \rho_2) - 2p_{12}^h - 2p_{21}^h - 1.$$

Zij nu $\{V,A\}$ sterk, dus zij $p_{12}^h + p_{21}^h$ onafhankelijk van x en y, voor h = 1, 2. Neem ρ_1 en ρ_2 zo, dat

$$\rho_1 + \rho_2 = p_{12}^1 + p_{21}^1 - p_{12}^2 - p_{21}^2, \; -1 - \rho_1\rho_2 = p_{12}^1 + p_{21}^1 + p_{12}^2 + p_{21}^2, \rho_1 > \rho_2.$$

Dan is het boven berekende inproduct onafhankelijk van h, x, y en gelijk aan $v - 1 + \rho_1\rho_2$. Omgekeerd, zij

$$(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J$$

voor zekere getallen ρ_1 en ρ_2. Dan volgt uit

$$v - 1 - (-1)^h(\rho_1 + \rho_2) - 2p_{12}^h - 2p_{21}^h - 1 = v - 1 + \rho_1\rho_2$$

voor h = 1, 2 en voor alle x en y, dat

$$2(p_{12}^1 + p_{21}^1) = (\rho_1 - 1)(1 - \rho_2) \text{ en } 2(p_{12}^2 + p_{21}^2) = (\rho_1 + 1)(-1 - \rho_2)$$

onafhankelijk zijn van x en y, dus dat de graaf sterk is.

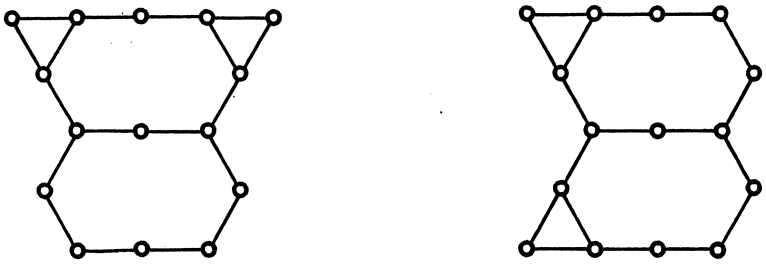
3. Eigenwaarden

Er is in de afgelopen jaren nogal wat aandacht besteed aan de vraag in hoeverre een graaf, of een equivalentieklasse van grafen, eenduidig wordt bepaald door het spectrum van zijn verbindingsmatrix ([1], [9], [18], [19], [20], [21], [33], [34], [37]). De meer algemene vraag, welke eigenschappen van grafen worden gekarakteriseerd door het spectrum van de verbindingsmatrix, schijnt een belang te hebben dat zich niet beperkt tot de grafentheorie.

Vb. 1 Kac [22] stelde de vraag "can one hear the shape of a drum". Zij Ω een gebied in R_2, begrensd door Γ. Indien alle eigenwaarden van het probleem

$$\frac{1}{2}\nabla^2 U + \lambda U = 0 \quad \text{in } \Omega\ , \quad U = 0 \quad \text{op} \quad \Gamma$$

bekend zijn, is dan de vorm van Ω te bepalen? Fisher [13] discretiseerde het probleem en gaf de relatie met de grafentheorie. De door hem gestelde vraag, of speciale deelgrafen van een driehoeksweefsel worden bepaald door de eigenwaarden van hun verbindingsmatrix, is inmiddels door Baker [1] in ontkennende zin beantwoord, onder andere door het volgende tegenvoorbeeld van twee verschillende grafen met dezelfde eigenwaarden.



Wij onderzoeken het spectrum van de verbindingsmatrix van sterke en van sterk reguliere grafen. Uit stelling 2.1 volgt

Stelling 3.1. Een reguliere graaf met $AJ = \rho_0 J$ heeft eigenwaarde ρ_0 bij de eigenvector $j = (1, 1, \ldots, 1)$.

Stelling 3.2. Het spectrum van een sterke graaf $\{V,A\}$ met $(A - \rho_1 I)(A - \rho_2 I) = 0$ bestaat uit ρ_1 en ρ_2. Deze eigenwaarden zijn, indien $\{V,A\}$ niet is $K(\alpha,\beta)$ of diens complement, oneven geheel of tegengesteld reëel. Zij voldoen aan

$$v - 1 + \rho_1\rho_2 = 0, \quad v(\rho_1 + \rho_2) + (\mu_1 - \mu_2)(\rho_1 - \rho_2) = 0,$$

waarin μ_i de multipliciteit van ρ_i is, $i = 1, 2$.

Bewijs. Het bewijs van de eerste bewering is triviaal. De gestelde betrekkingen voor ρ_1 en ρ_2 volgen uit

$$\mu_1 + \mu_2 = v, \quad \text{tr } A = \mu_1\rho_1 + \mu_2\rho_2 = 0, \quad \text{tr } A^2 = \mu_1\rho_1^2 + \mu_2\rho_2^2 = v(v - 1).$$

Voor $\mu_1 = \mu_2 = \frac{1}{2} v$ geldt $\rho_1 = -\rho_2 = \sqrt{v - 1}$. Voor $\mu_1 \neq \mu_2$ is $\rho_1 - \rho_2$, en dus ρ_1 en ρ_2, rationaal. Daar som en product geheel zijn, zijn ρ_1 en ρ_2 geheel en wel oneven op grond van stelling 1.1 en de betrekkingen

$$2(p_{12}^1 + p_{21}^1) = (\rho_1 - 1)(1 - \rho_2), \quad 2(p_{12}^2 + p_{21}^2) = (\rho_1 + 1)(-1 - \rho_2).$$

Stelling 3.3. Een sterke graaf $\{V,A\}$ met $(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J \neq 0$ is sterk regulier. Zijn spectrum bestaat uit ρ_1, ρ_2 en een derde getal ρ_0 dat multipliciteit 1 heeft. De getallen ρ_1, ρ_2 resp. ρ_0 zijn tegengestelde reëlen resp. nul, of oneven gehelen resp. geheel. Zij voldoen aan

$$(\rho_0 - \rho_1)(\rho_0 - \rho_2) = v(v - 1 + \rho_1\rho_2),$$

$$2\rho_0 + (v - 1)(\rho_1 + \rho_2) + (\mu_1 - \mu_2)(\rho_1 - \rho_2) = 0,$$

waarin μ_i de multipliciteit van ρ_i is, $i = 1, 2$.

Bewijs. Wegens $v - 1 + \rho_1\rho_2 \neq 0$ is J lineaire combinatie van A^2, A, I. Deze vier matrices zijn dus simultaan diagonaliseerbaar. J heeft eigenwaarden v en 0 met multipliciteiten 1 en $v - 1$. De vector $(1, 1, \ldots, 1)$ is eigenvector van J bij eigenwaarde v, dus eigenvector van A, zeg bij eigenwaarde ρ_0. Hieruit volgt $AJ = \rho_0 J$ met ρ_0 geheel en $1 - v < \rho_0 < v - 1$. De gestelde betrekkingen volgen uit

$$1 + \mu_1 + \mu_2 = v, \quad \operatorname{tr} A = \rho_0 + \mu_1\rho_1 + \mu_2\rho_2 = 0, \quad \operatorname{tr} A^2 = \rho_0^2 + \mu_1\rho_1^2 + \mu_2\rho_2^2 = v(v - 1).$$

Voor $\mu_1 = \mu_2$ volgt $\rho_0 = 0$, $\rho_1 = -\rho_2 = \sqrt{v}$. Voor $\mu_1 \neq \mu_2$ zijn ρ_1 en ρ_2 rationaal, dus geheel en oneven.

Op grond van deze stellingen onderscheiden wij drie (deels overlappende) typen van sterke grafen $\{V,A\}$:

I. Sterke grafen met $(A - \rho_1 I)(A - \rho_2 I) = 0$; ρ_1, ρ_2 oneven geheel.

II. Sterk reguliere grafen met $(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J \neq 0$; ρ_1, ρ_2 oneven geheel, ρ_0 geheel.

III. Sterke grafen met $A^2 = (v - 1)I$.

Opmerking. De in stelling 3.3 genoemde sterk reguliere graaf $\{V,A\}$ met $\rho_0 = 0$, $\rho_1 = -\rho_2 = \sqrt{v}$ correspondeert met de sterke graaf van orde

v + 1 en verbindingsmatrix

$$B = \begin{pmatrix} 0 & j^T \\ j & A \end{pmatrix}, \text{ met } B^2 = vI.$$

4. Gelijkhoekige rechten

Vb. 1 De vier lichaamsdiagonalen van een kubus maken twee aan twee de hoek $\arccos \frac{1}{3}$.

Vb. 2 De zes antipodenverbinders van een icosaëder maken twee aan twee de hoek $\arccos 1/\sqrt{5}$.

Een stelsel rechten heet gelijkhoekig wanneer elk paar rechten uit het stelsel dezelfde hoek maakt.

Probleem. Welke gelijkhoekige stelsels van n rechten bevat de r-dimensionale euklidische R_r? Bij gegeven r, wat is het maximum n(r) van n?

Stelling 4.1. $n(2) = 3$, $n(3) = n(4) = 6$, $n(5) = 10$, $n(6) = 16$, $n(7) \geq 28$.

Wij leggen het verband met sterke grafen, construeren enkele maximale stelsels en verwijzen voor het bewijs verder naar [23].

Een stelsel van n rechten in R_r, gedragen door de eenheidsvectoren $\underline{p}_1, \ldots, \underline{p}_n$, is gelijkhoekig als

$$|(\underline{p}_i, \underline{p}_j)| = \cos \phi = \text{constant}, \; i \neq j, \; i,j = 1, \ldots, n.$$

De Gram matrix van de vectoren,

$$P = ((\underline{p}_i, \underline{p}_j)) = \begin{pmatrix} 1 & & & \\ & \ddots & \pm \cos \phi & \\ & \pm \cos \phi & \ddots & \\ & & & 1 \end{pmatrix}$$

heeft orde n en is semidefiniet van rang r, met andere woorden, heeft kleinste eigenwaarde 0 met multipliciteit n - r. Dan heeft

$$A = \frac{1}{\cos \phi}(P - I) = \begin{pmatrix} 0 & & \\ & \ddots & \pm 1 \\ & \pm 1 & \ddots \\ & & & 0 \end{pmatrix}$$

kleinste eigenwaarde $\rho_2 = -1/\cos \phi$ met multipliciteit n - r. De matrix A kan worden geïnterpreteerd als de verbindingsmatrix van een graaf. Elke rechte wordt gedragen door twee elkaar tegengestelde eenheidsvectoren. Verandering in de keuze van de dragende vector van een rechte komt neer op complementatie ten opzichte van het met de rechte corresponderende punt van de graaf. Omgekeerd kunnen wij aan een graaf, met behulp van de kleinste eigenwaarde van zijn verbindingsmatrix, een niet triviaal stelsel van gelijkhoekige rechten toevoegen. Wij concluderen [23]:

Stelling 4.2. Er is een eeneenduidig verband tussen de niet triviale stelsels gelijkhoekige rechten en de equivalentieklassen van grafen.

Maximale stelsels van gelijkhoekige rechten corresponderen met symmetrische matrices A, met diagonaalelementen 0 en overige elementen ± 1, waarvan de kleinste eigenwaarde een zo groot mogelijke multipliciteit heeft. De in verband met stelling 4.1 gevonden maximale stelsels in R_r, $r < 8$, corresponderen alle met sterke grafen. Voor $r \geq 8$ is weinig bekend.

Vb. 3 $n(3) = n(4) = 6$. Een maximaal stelsel wordt gevormd door de 6 diagonalen van de icosaëder. Dit stelsel correspondeert met de in §1, Vb. 1 genoemde graaf. Zijn verbindingsmatrix A voldoet aan $A^2 = 5I$ en heeft eigenwaarden $\sqrt{5}$ en $-\sqrt{5}$, in overeenstemming met Vb. 2.

Vb. 4 $n(7) \geq 28$. De eindpunten van de eenheidsvectoren in R_8 liggen in het hypervlak

$$x_1 + x_2 + \ldots + x_8 = 1$$

en vormen de 8 hoekpunten van een regelmatig simplex α_7. Verschuif dit hypervlak evenwijdig naar de oorsprong dan ligt α_7 in

$$x_1 + x_2 + \ldots + x_8 = 0.$$

De 28 middens $P_{h,i}$, $h < i$, $h,i = 1, \ldots, 8$, van de ribben α_7 hebben, op een gemene factor na, de coördinaten

$$P_{1,2} = (3,3,-1,-1,-1,-1,-1,-1), \text{ etc.}$$

Verbind O met alle $P_{h,i}$ dan is een gelijkhoekig stelsel rechten verkregen met hoek arccos $\frac{1}{3}$. De bijbehorende graaf is het complement van de in §1, Vb. 6 genoemde graaf.

Vb. 5 $n(6) = 16$. De 16 punten $P_{h,i}$ van Vb. 4, die voldoen aan $x_1 = x_2$, vormen, indien verbonden met O, een gelijkhoekig stelsel van 16 rechten in R_6 met hoek arccos $\frac{1}{3}$. Deze rechten zijn ook voor te stellen door (1,1,1,1,1,1) en de 15 permutaties van (1,1,1,1,-1,-1). De bijbehorende graaf is equivalent met het complement van de in §1, Vb. 5 genoemde graaf.

Vb. 6 $n(5) = 10$. De 10 punten $P_{h,i}$ van Vb. 4 die voldoen aan $x_1 = x_2 = x_3$, vormen, indien verbonden met O, een gelijkhoekig stelsel van 10 rechten in R_5 met hoek arccos $\frac{1}{3}$. De bijbehorende graaf is de Petersen graaf van §1, Vb. 3.

5. Latijnse vierkanten en netten

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

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

Vb. 2 Twee aan twee orthogonaal is het drietal

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

Echter $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ bezit geen orthogonale collega.

Een <u>transversaal</u> van een latijns vierkant van orde n is een verzameling van n elementen van de matrix, geen twee in dezelfde rij of kolom, die alle symbolen 1, 2, ..., n bevat.

<u>Vermoeden</u> (Ryser): Elk latijns vierkant van oneven orde bezit een transversaal.

<u>Stelling 5.1</u>. Bij elke eindige groep van oneven orde n kan een paar orthogonale latijnse vierkanten van de orde n worden geconstrueerd.

Bewijs. Zij G een groep van de orde $n \equiv 1 \pmod 2$. De matrices

$$(a_i\ a_j) \text{ en } (a_j^{-1}\ a_i);\ a_1, \ldots, a_n \in G;\ i,j = 1, \ldots, n,$$

zijn latijnse vierkanten van de orde n. Inderdaad, in elk der beide matrices komt elk groepselement in elke rij en in elke kolom eenmaal voor, terwijl uit

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

volgt dat $a_i^2 = a_k^2$ en dus, omdat n + 1 even is, dat $a_i = a_k$.

Stelling 5.2. 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.
Dus $t \leq n - 1$.
Een stelsel van n - 1 twee aan twee orthogonale latijnse vierkanten van de orde n heet een volledig stelsel (dit is een affien vlak van orde n).

Stelling 5.3. Er bestaat een volledig stelsel van twee aan twee orthogonale latijnse vierkanten van de orde $n = p^k \geq 3$, p priem.

Bewijs. Zij $GF(p^k)$ een Galois lichaam met elementen $\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{n-1}$. Definieer $A_e = (\alpha_e \alpha_i + \alpha_j)$, i,j = 0, 1, ..., n-1, e = 1, ..., n-1.
De A_e zijn latijnse vierkanten wegens

$$\alpha_e \alpha_i + \alpha_j = \alpha_e \alpha_i + \alpha_{j'} \Rightarrow \alpha_j = \alpha_{j'}, \quad \alpha_e \alpha_i + \alpha_j = \alpha_e \alpha_{i'} + \alpha_j \Rightarrow \alpha_i = \alpha_{i'}$$

Voor $1 \leq e < f \leq n-1$ zijn A_e en A_f orthogonaal wegens

$$\alpha_e \alpha_i + \alpha_j = \alpha_e \alpha_{i'} + \alpha_{j'}, \quad \alpha_f \alpha_i + \alpha_j = \alpha_f \alpha_{i'} + \alpha_{j'} \Rightarrow \alpha_i = \alpha_{i'}, \alpha_j = \alpha_{j'}.$$

Stelling 5.4. Er bestaan tenminste $\min_i (p_i^{k_i} - 1)$ twee aan twee orthogonale latijnse vierkanten van de orde $n = p_1^{k_1} \ldots p_s^{k_s}$, p_i priem.

Stelling 5.5. Er bestaat tenminste een paar orthogonale latijnse vierkanten van de orde $n \equiv 2 \pmod 4$, $n > 6$.

Voor de bewijzen van deze stellingen zie [31] en [17].

Stelling 5.5, van Bose, Shrikhande en Parker (1959) weerlegt een beroemd vermoeden van Euler (1782), dat voor n = 6 werd bewezen door Tarry (1900).

Wij leggen het verband met sterk reguliere grafen. Een n-kliek in een graaf is een volledige deelgraaf op n punten. Een parallelklasse van een graaf op n^2 punten is een stelsel van n stuks n-klieks zodat elk der n^2 punten tot één n-kliek behoort. Twee parallelklassen van een graaf op n^2 punten heten orthogonaal als elke kliek uit de ene klasse met elke kliek uit de andere klasse precies één punt gemeen heeft. Een latijns vierkant van de orde n is een graaf op n^2 punten waarvan de verbindingen drie parallelklassen vormen die twee aan twee orthogonaal zijn. Een net (n,k), dat zijn k - 2 orthogonale latijnse vierkanten van de orde n, is een graaf op n^2 punten waarvan de verbindingen k twee aan twee orthogonale parallelklassen vormen.

Naast het aantal k der parallelklassen van een net (n,k) wordt ingevoerd het getal d = n + 1 - k, de deficiency, het aantal parallelklassen dat ontbreekt opdat het net een volledig stelsel zou zijn.

Een net (n,k) is een sterk reguliere graaf met $n_1 = k(n - 1)$, $n_2 = d(n - 1)$, $p_{12}^1 = (k - 1)d$, $p_{12}^2 = (d - 1)k$, $v = n^2$, $\rho_0 = (d-k)(n-1)$, $\rho_1 = 2k - 1$, $\rho_2 = 1 - 2d$.
Het complement van een net is ook sterk regulier met

$$v = n^2,\ \rho_0 = (k - d)(n - 1),\ \rho_1 = 2d - 1,\ \rho_2 = 1 - 2k.$$

Het complement van een net is echter slechts dan een net als het oorspronkelijke net uitbreidbaar is tot een volledig stelsel. Omtrent de existentie van netten zijn slechts zeer partiële resultaten bekend (zie Bruck [7]).

6. Klieken en klauwen

Wij geven enige schattingen betreffende de maximale lengte van klieken en klauwen in sterke grafen. Een p-kliek is een volledige graaf K(p). Een q-klauw is een volledige paargraaf K(q,1), van de orde q + 1.

Stelling 6.1. Nodig voor het bestaan van een p-kliek in een sterke graaf is $(p - 1 + \rho_1)(p - 1 + \rho_2) \leq p(v - 1 + \rho_1\rho_2)$.

Bewijs. Wij schrijven de definiërende vergelijking van de sterke graaf

$$(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J$$

door geschikte arrangering der punten als volgt

$$\begin{pmatrix} (1-\rho_1)I - J & D \\ D^T & E-\rho_1 I \end{pmatrix} \begin{pmatrix} (1-\rho_2)I - J & D \\ D^T & E-\rho_2 I \end{pmatrix} = (v-1+\rho_1\rho_2) \begin{pmatrix} J & J \\ J & J \end{pmatrix},$$

waarin D de afmeting $p \times (v - p)$ heeft. Dan volgt

$$DD^T = -(1 - \rho_1)(1 - \rho_2)I + (v - p + (1 - \rho_1)(1 - \rho_2))J.$$

Omdat deze matrix niet-negatieve eigenwaarden heeft, geldt

$$-(1 - \rho_1)(1 - \rho_2) + p(v - p + (1 - \rho_1)(1 - \rho_2)) \geq 0.$$

Hieruit volgt de gestelde voorwaarde voor p.

Stelling 6.2. Nodig voor het bestaan van een q-klauw in een sterke graaf is $4q \leq (\rho_1 - 3)(3 - \rho_2) + 12$.

Bewijs. Arrangeer de punten van de sterke graaf $\{V,A\}$ zo, dat de eerste $q + 1$ rijen van A er als volgt uitzien:

0	-	-	••	-	-	••	-	+	••	+	+	••	+	-	••	-
-	0	+	••	+	+	••	+	-	••	-	+	••	+	-	••	-
-j	j	J-I			D			E			F			G		

met afmetingen

$$1,\ 1,\ q-1,\ p_{12}^1-q+1,\ p_{21}^1,\ p_{22}^1,\ p_{11}^1 .$$

Toepassing van de definiërende vergelijking van $\{V,A\}$ op de blokrij met de eerste en met de tweede kolom levert

$$\rho_2 J - J - (J - I - \rho_1 I)J - DJ + EJ + FJ - GJ = (v - 1 + \rho_1\rho_2)J,$$

$$J - \rho_2 J + (J - I - \rho_1 I)J + DJ - EJ + FJ - GJ = (v - 1 + \rho_1\rho_2)J.$$

Hieruit volgt

$$(q - 1 - \rho_1 - \rho_2)J = - DJ + EJ$$

en dus, gezien de afmetingen van D en E,

$$q - 1 - \rho_1 - \rho_2 \leq p_{12}^1 - q + 1 + p_{21}^1,$$

waarbij het gelijkteken slechts optreedt als $D = -J$ en $E = J$. Hieruit volgt de gestelde voorwaarde voor q.

Stelling 6.3. Nodig voor het bestaan van een klauw ter lengte $3 + \frac{1}{4}(\rho_1 - 3)(3 - \rho_2)$ in een sterk reguliere graaf is

$$|2\rho_0 + \rho_1\rho_2 - 3\rho_1 - 3\rho_2 + 3| \leq 2(v - 1 + \rho_1\rho_2).$$

Bewijs. Wij refereren aan het bewijs van stelling 6.2, volgens hetwelk een maximale klauw slechts optreedt als $D = -J$, $E = J$. Uit beschouwing van twee punten van het blok, dus niet verbonden, volgt

$$p_{21}^1 + q - 2 \leq p_{22}^2 \quad \text{en} \quad p_{12}^1 - q + 2 \leq p_{11}^2,$$

waaruit na substitutie het gestelde.

Stelling 6.4. Een sterk reguliere graaf met $\rho_1 = 3$, $\rho_0 \neq 3$ bezit geen 3-klauwen.

Bewijs. Toepassing van de stellingen 6.2 en 6.3 voor $\rho_1 = 3$ levert $q \leq 3$ voor de klauwlengte q. Voor $q = 3$ is nodig dat

$$|\rho_0 - 3| \leq v - 1 + 3\rho_2.$$

Met

$$(\rho_0 - 3)(\rho_0 - \rho_2) = v(v - 1 + 3\rho_2)$$

volgt hieruit, wegens $\rho_0 \neq 3$, dat

$$|\rho_0 - 3| \leq |\rho_0 - \rho_2| - 1 + 3\rho_2,$$

waaruit $\rho_2 = -1$. Maar

$$(\rho_0 - 3)(\rho_0 + 1) = v(v - 4) \quad \text{en} \quad 1 - v < \rho_0 < v - 1$$

hebben ten gevolge dat $v = 3 - \rho_0$ en $n_2 = 1$. Een 3-klauw bestaat dus niet.

Stelling 6.5. Elke sterke graaf $\{V,A\}$ met

$$(A - 3I)(A - \rho_2 I) = 0$$

is equivalent met een graaf die 3-klauwen bezit.

Bewijs. Complementeer zo, dat de verbindingsmatrix wordt

$$\begin{pmatrix} 0 & -j^T \\ -j & B \end{pmatrix}.$$

Deze matrix voldoet aan de definiërende vergelijking. Hieruit volgt dat B, van de orde $v - 1$, voldoet aan

$$(B - 3I)(B - \rho_2 I) = -J, \quad BJ = (3 + \rho_2)J, \quad v - 1 + 3\rho_2 = 0.$$

Zij V' de verzameling V behalve het eerste punt. $\{V',B\}$ is sterk regulier met

$$v' = v - 1, \quad \rho_0' = 3 + \rho_2, \quad \rho_1' = 3, \quad \rho_2' = \rho_2, \quad p_{22}^2 = 1.$$

In $\{V',B\}$ behoort dus bij elk paar niet verbonden punten een punt dat met geen van beide is verbonden. Hieruit volgt de bewering.

7. Lijngrafen

In het volgende zal het soms voorkeur verdienen om een graaf G te beschrijven door zijn (1,0) verbindingsmatrix $\bar{A}(G)$, gedefinieerd door $\bar{A}(x,y) = 1$ als x en y verbonden, $= 0$ overigens. De relatie tot de (-1,1,0) verbindingsmatrix A(G) is

$$A = J - I - 2\bar{A}.$$

Tussen de eigenwaarden λ_i van $\bar{A}(G)$ en ρ_i van A(G) bestaat de relatie $\rho_i = -1 - 2\lambda_i$, met één uitzondering $\rho_0 = v - 1 - 2\lambda_0$. De kleinste eigenwaarde van $\bar{A}(G)$ wordt volgens Hoffman [20] aangeduid door $\lambda(G)$, terwijl wij definiëren $\rho(G) = -1 - 2\lambda(G)$.

De incidentiematrix van een graaf G is een v × e matrix, waar v het aantal punten en e het aantal verbindingen in G is. De (1,0) incidentiematrix $\bar{K}$ van G wordt gedefinieerd door zijn elementen 1 als punt en verbinding incident zijn, 0 als niet incident. Ook voor de incidentiematrix bestaat een (-1,1) versie, namelijk $K = J - 2\bar{K}$.

Het verband tussen de verbindingsmatrix $\bar{A}$ en de incidentiematrix $\bar{K}$ van een graaf wordt gegeven door

$$\bar{K}\,\bar{K}^T = \bar{N} + \bar{A},$$

waarin $\bar{N}$ de diagonaalmatrix is die de diagonaalelementen $n_1(x)$ heeft.

Zij G een graaf. Zijn lijngraaf Γ is de graaf waarvan de punten zijn de verbindingen van G, terwijl twee punten van Γ verbonden zijn dan en slechts dan als de corresponderende verbindingen van G een gemeenschappelijk punt hebben.

Stelling 7.1. Lijngrafen bezitten geen 3-klauw.

Stelling 7.2. Wanneer G meer verbindingen dan punten bezit, dan geldt
$\lambda(\Gamma) = -2$ en $\rho(\Gamma) = 3$ voor de lijngraaf Γ van G.

Bewijs. Zij Γ de lijngraaf van G. Als $\bar{K}$ de incidentiematrix van G is, dan is

$$\bar{K}^T\bar{K} = 2I + \bar{A}(\Gamma).$$

Als G meer verbindingen dan punten bezit, heeft $\bar{K}^T\bar{K}$ tenminste één eigenwaarde 0, terwijl de overige eigenwaarden ≥ 0 zijn. Hieruit volgt de bewering.

Vb. 1 H(n), $n > 3$, is de graaf, die uit de volledige graaf op 2n punten wordt verkregen door een 1-factor weg te laten. H(n) is sterk regulier met

$$v = 2n \ , \quad \rho_0 = 3 - 2n \ , \quad \rho_1 = 3 \ , \quad \rho_2 = -1.$$

H(n) is de enige sterke graaf met deze parameters. H(n) is geen lijngraaf.

Vb. 2 $L_2(n)$, $n > 1$, de lattice graaf, is de lijngraaf van K(n,n). $L_2(n)$ is sterk regulier met

$$v = n^2 \ , \quad \rho_0 = (n - 1)(n - 3) \ , \quad \rho_1 = 3 \ , \quad \rho_2 = 3 - 2n.$$

Voor $n \neq 2, 4$ is $L_2(n)$ de enige sterke graaf met deze parameters. Voor $n = 2$ voldoet ook de 3-klauw. Voor $n = 4$ voldoet er nog één sterk reguliere graaf, namelijk het complement van het net (4,3) dat correspondeert met een niet uitbreidbaar latijns vierkant. Deze pseudo lattice graaf bezit 3-klauwen. (Shrikhande [37]).

Vb. 3 T(n), $n > 3$, de triangulaire graaf, is de lijngraaf van de volledige graaf op n punten. T(n) is sterk regulier met

$$v = \frac{1}{2} n(n - 1), \ \rho_0 = \frac{1}{2} (n - 2)(n - 7), \ \rho_1 = 3, \ \rho_2 = 7 - 2n.$$

Voor $n \neq 5$, $n \neq 8$ is T(n) de enige sterke graaf met deze parameters. Voor $n = 5$ zijn er geen, voor $n = 8$ zijn er nog drie sterk reguliere grafen met deze parameters. Elk van deze pseudo triangulaire grafen bezit 3-klauwen. (Hoffman [19], Chang [8]).

Vb. 4 De Petersen graaf heeft als punten de 10 ongeordende paren uit 5 symbolen. Twee paren zijn verbonden dan en slechts dan als ze geen symbool gemeen hebben. De Petersen graaf, die het complement is van de Desargues graaf T(5), is sterk regulier met

$$v = 10 \ , \quad \rho_1 = \rho_0 = 3 \ , \quad \rho_2 = -3.$$

Vb. 5 De Clebsch graaf definiëren wij op twee manieren. Hij is het complement van de graaf die bestaat uit een 5-klauw en een Petersen graaf, wier verbindingen door inclusie worden beschreven als de 5 eindpunten van de 5-klauw worden beschouwd als symbolen van de Petersen graaf. De Clebsch graaf wordt verkregen uit de hyperkubus γ_5 door

identificatie van antipodale punten, waarbij punten verbonden worden wanneer zij in 2 of 3 coördinaten verschillen. Volgens deze laatste definitie houdt de graaf verband met de 16 rechten van het vierdegraads oppervlak van Clebsch; vandaar de naam (Coxeter [10]). De Clebsch graaf is sterk regulier met

$$v = 16 \ , \quad \rho_1 = 3 \ , \quad \rho_2 = \rho_0 = -5,$$

heeft geen 3-klauwen, maar is geen lijngraaf.

Vb. 6 De Schläfli graaf is de graaf waarvan de punten zijn de 27 rechten van een algemeen derdegraads oppervlak, waarbij punten verbonden worden wanneer de corresponderende rechten kruisen. De Schläfli graaf wordt uit T(8) verkregen door complementatie ten opzichte van de 12 punten die verbonden zijn met één hoekpunt, dat daarna wordt weggelaten. De Schläfli graaf is sterk regulier met

$$v = 27 \ , \quad \rho_1 = 3 \ , \quad \rho_2 = -9 \ , \quad \rho_0 = -6,$$

heeft geen 3-klauwen, maar is geen lijngraaf.

Stelling 7.3. De enige sterk reguliere grafen met $\rho_1 = 3$ zijn H(n), de lattice grafen, de triangulaire grafen, de pseudo lattice graaf, de pseudo triangulaire grafen, en de grafen van Petersen, Clebsch en Schläfli.

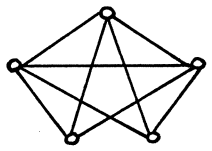
Stelling 7.4. Sterke grafen met $(A - 3I)(A - \rho_2 I) = 0$ bestaan slechts voor $\rho_2 = -1, -3, -5, -9$, en zijn equivalent met respectievelijk $L_2(2)$, T(5), $L_2(4)$, T(8).

Voor het bewijs van deze stellingen zie [33], [34]. Hiermee is de vraag beantwoord welke sterke grafen lijngraaf zijn. Blijft de meer algemene

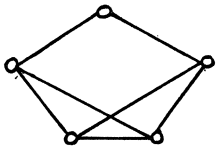
Vraag: Welke grafen zijn lijngraaf?

Gedeeltelijke antwoorden worden gegeven door de volgende stellingen.

Stelling 7.5. (van Rooy en Wilf [30]). Een graaf is een lijngraaf, wanneer hij geen 3-klauw bezit en geen deelgrafen



,



.

Stelling 7.6. (Hoffman en Ray Chaudhuri). Een reguliere graaf $G \neq H(n)$, met $\lambda(G) = -2$ en $n_1 > 16$, is een lijngraaf.

Het bewijs van stelling 7.6 is nog niet gepubliceerd.

8. Paley matrices

Wij onderzoeken symmetrische en scheve matrices C van orde v, met diagonaalelementen 0 en andere elementen +1 of -1, die voldoen aan

$$CC^T = (v - 1)I.$$

Zulke matrices duiden wij aan met de naam C-matrices. In het symmetrische geval komt dit neer op het onderzoek van sterke grafen $\{V,A\}$ met $A^2 = (v - 1)I$. Het scheve geval kan worden geïnterpreteerd als het onderzoek van een speciale klasse van tournaments (volledige asymmetrische gerichte grafen).

Bij een gegeven C-matrix kan steeds, door geschikte complementatie, worden gevonden een C-matrix met eerste rij (0 + + . . . +). Zo'n C-matrix heet genormaliseerd.

Stelling 8.1. Nodige voorwaarde voor het bestaan van een symmetrische (resp. scheve) C-matrix van de orde v is $v \equiv 2 \pmod 4$, (resp. $v = 2$ of $v \equiv 0 \pmod 4$).

Bewijs. Voor $v = 2$ bestaat een symmetrische en een scheve C-matrix. Voor $v = 3$ niet. Stel voor $v > 3$ bestaat een C-matrix. Normaliseer en permuteer rijen en kolommen zo dat de drie eerste rijen van C er als volgt uitzien:

$$\begin{array}{ccccccccccccc} 0 & + & + & + & \cdots & + & + & \cdots & + & + & \cdots & + & + & \cdots & + \\ & 0 & + & + & \cdots & + & + & \cdots & + & - & \cdots & - & - & \cdots & - \\ & & 0 & + & \cdots & + & - & \cdots & - & + & \cdots & + & - & \cdots & - \end{array}$$

Noem de aantallen kolommen 3, x, y, z, w dan volgt uit $CC^T = (v - 1)I$ in het symmetrische, resp. het scheve geval

$$\begin{array}{ll} 1 + x + y + z + w = v - 2 & \text{resp. } 1 + x + y + z + w = v - 2 \\ 1 + x + y - z - w = 0 & \quad 1 + x + y - z - w = 0 \\ 1 + x - y + z - w = 0 & -1 + x - y + z - w = 0 \\ 1 + x - y - z + w = 0 \quad , & \quad 1 + x - y - z + w = 0 \quad , \end{array}$$

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

Hieruit volgt de bewering.

Van de nu in te voeren matrices heten K_4, L_4, M_4 op grond van hun eigenschappen, de <u>quaternion</u> matrices van de orde 4:

$$P_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad L_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$PP^T = I$, $KK^T = LL^T = MM^T = I$, $KL = M$, $LM = K$, $MK = L$.

Voor symmetrische C-matrices is er een tweede nodige voorwaarde, namelijk

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

Deze voorwaarde, die bijvoorbeeld v = 22 uitsluit, is een gevolg van de volgende stelling [23], [2]:

Stelling 8.2. Een nodige voorwaarde voor het bestaan van een vierkante rationale matrix Q van de orde $q \equiv 2 \pmod 4$ die voldoet aan $Q^TQ = nI$, n geheel, is dat n de som is van twee kwadraten van gehelen.

Bewijs. Volgens Lagrange geldt voor elke natuurlijke n

$$n = n_1^2 + n_2^2 + n_3^2 + n_4^2 \ , \quad n_1, n_2, n_3, n_4 \text{ geheel.}$$

Vorm de vierkante matrix van orde 4

$$N = n_1 I_4 + n_2 K_4 + n_3 L_4 + n_4 M_4,$$

dan geldt $N^TN = nI_4$. Laat nu Q, q, n zijn zoals aangegeven in de stelling, en $q > 4$. Schrijf

$$Q = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad , \quad R = \begin{pmatrix} -(A - N)^{-1}B \\ I_{q-4} \end{pmatrix} ,$$

met A vierkant van de orde 4 (wij mogen A - N niet-singulier veronderstellen). Dan geldt

$$QR = \begin{pmatrix} -A(A - N)^{-1}B + B \\ -C(A - N)^{-1}B + D \end{pmatrix} = \begin{pmatrix} N(A - N)^{-1}B \\ Q^* \end{pmatrix}$$

voor vierkante $Q^* = D - C(A - N)^{-1}B$ van de orde $q - 4$. Uit

$$(QR)^T(QR) = R^T(Q^TQ)R$$

volgt dat $Q^{*T}Q^* = nI_{q-4}$. De matrix Q^* voldoet aan de eisen van de stelling voor $q - 4$ in plaats van q. Na iteratie komen zij tot een matrix van de orde 2, die voldoet aan de eisen van de stelling. Hieruit volgt dat n de som is van twee kwadraten van rationale getallen. Daar n geheel is concluderen wij dat n de som is van twee kwadraten van gehelen.

Na deze nonexistentiestellingen, de enige die bekend zijn, zullen enige C-matrices worden geconstrueerd. Daarbij wordt gebruik gemaakt van een Galois lichaam GF(q) van de orde $q = p^k$, p priem, $p \neq 2$. Het

Legendre symbool χ over GF(q) wordt gedefinieerd door

$$\chi(0) = 0 , \quad \chi(\alpha) = 1 \quad \text{of} \quad -1,$$

naar gelang $\alpha \neq 0$ een kwadraat in GF(q) is of niet.
Er geldt $\chi(-1) = 1$ resp. -1 naar gelang $q \equiv 1$ resp. $-1 \pmod 4$.

Stelling 8.3. $\sum_{\alpha \in GF(q)} \chi(\alpha)\chi(\alpha + \beta) = -1$, $\beta \in GF(q)$, $\beta \neq 0$.

Bewijs. $\chi(0)\chi(0 + \beta) = 0$. Definieer γ, voor $\alpha \neq 0$, door $\alpha + \beta = \alpha\gamma$. Als α doorloopt $GF(q) \setminus \{0\}$, dan doorloopt γ juist $GF(q) \setminus \{1\}$. Daarom geldt

$$\sum_{\alpha} \chi(\alpha)\chi(\alpha + \beta) = \sum_{\alpha} \chi(\alpha)\chi(\alpha\gamma) = \sum_{\gamma} \chi(\gamma) - \chi(1) = 0 - 1 = -1.$$

Beschouw de vectorruimte R_2 van dimensie 2 over GF(q). Beschouw $q + 1$ vectoren $x_0, x_1, \ldots, x_q$ waarvan geen tweetal afhankelijk is, dus die elk opspannen één der $q + 1$ eendimensionale deelruimten van R_2 (één der $q + 1$ projectieve punten van de projectieve rechte PG(1,q)). Zij voorts det een determinant over R_2, dat is een alternerende bilineaire vorm over R_2.

De Paley matrix van $q + 1$ twee aan twee onafhankelijke vectoren $x_0, x_1, \ldots, x_q \in R_2$ is de matrix

$$C = (\chi \det(x_i, x_j))_{i,j=0,1,2,\ldots,q}.$$

De lijnmatrix van q op een niet door de oorsprong gaande rechte gelegen vectoren $y_1, \ldots, y_q \in R_2$ is de matrix

$$S = (\chi \det(y_i, y_j))_{i,j=1,2,\ldots,q}.$$

De operaties op vierkante matrices:

(1) vermenigvuldiging met -1 van een rij en van de corresponderende kolom,
(2) verwisseling van twee rijen en van de corresponderende kolommen,

genereren een relatie, genaamd equivalentie. De operatie (2) alleen genereert ook een relatie, genaamd permutatie-equivalentie.

Stelling 8.4. Bij elke projectieve rechte PG(1,q) behoort een klasse van equivalente Paley matrices van orde q + 1. Deze Paley matrices zijn C-matrices, symmetrisch als $q + 1 \equiv 2 \pmod 4$ en scheef als $q + 1 \equiv 0 \pmod 4$.

Bewijs. De operatie (1), resp. (2), op een Paley matrix komt overeen met vermenigvuldiging van de corresponderende vector met een nietkwadraat, resp. met verwisseling van de twee corresponderende vectoren. Daarom zijn alle Paley matrices van de orde q + 1 equivalent. De eigenschap $CC^T = qI$ bewijzen wij voor de Paley matrix van de vectoren x en $y + \alpha_i x$, waarin x en y onafhankelijk en α_i doorloopt GF(q).

$$C = \chi\ \det(x,y) \begin{pmatrix} 0 & j^T \\ j\chi(-1) & \chi(\alpha_i - \alpha_j) \end{pmatrix}_{i,j=1,2,\ldots,q}.$$

Met de uit stelling 8.3 voor $h \neq i$ volgende formule

$$\sum_{j=1}^{q} \chi(\alpha_i - \alpha_j)\chi(\alpha_h - \alpha_j) + 1 = 0 \quad \text{en} \quad \sum_{j=1}^{q} \chi(\alpha_i - \alpha_j) = 0$$

zien wij dat inderdaad $CC^T = qI$.

Stelling 8.5. Alle lijnmatrices S van de orde q zijn permutatie-equivalent. Zij voldoen aan

$$SS^T = qI - J\ ,\quad SJ = JS = 0.$$

Zij zijn permutatie-equivalent met een matrix van de vorm

$$\begin{pmatrix} 0 & j^T & -j^T \\ j\chi(-1) & A & B \\ -j\chi(-1) & \chi(-1)B^T & -A \end{pmatrix},$$

waarin A en B circulanten zijn van de orde $\frac{1}{2}(q - 1)$.

Bewijs. De lijnmatrix van de vectoren $y + \alpha_1 x, \ldots, y + \alpha_q x$, $\alpha_i \in GF(q)$, is

$$S = \chi\ \det(x,y)(\chi(\alpha_i - \alpha_j))_{i,j=1,2,\ldots,q},$$

welke permutatie-equivalent is met $(\chi(\alpha_i - \alpha_j))$. De relaties voor S volgen uit

$$qI = CC^T = \begin{pmatrix} 0 & j^T \\ j\chi(-1) & S \end{pmatrix} \begin{pmatrix} 0 & j^T\chi(-1) \\ & S^T \end{pmatrix}.$$

De standaardvorm wordt verkregen door de vectoren te arrangeren volgens

$$y,\ y + x\eta^2,\ y + x\eta^4,\ \ldots,\ y + x\eta^{q-1},\ y + x\eta,\ y + x\eta^3,\ \ldots,\ y + x\eta^{q-2},$$

waarin η een primitief element van GF(q) is.

Voorbeeld. Modulo q = 7 zijn 1, 2, 4 kwadraatrest en 3, 5, 6 niet kwadraatrest. De volgende matrix is een scheve C-matrix van de orde 8

$$C_8 = \begin{pmatrix} 0 & + & + & + & + & + & + & + \\ - & 0 & + & + & - & + & - & - \\ - & - & 0 & + & + & - & + & - \\ - & - & - & 0 & + & + & - & + \\ - & + & - & - & 0 & + & + & - \\ - & - & + & - & - & 0 & + & + \\ - & + & - & + & - & - & 0 & + \\ - & + & + & - & + & - & - & 0 \end{pmatrix}.$$

9. Hadamard matrices

Het Kronecker product $A \times B$ van de vierkante matrices A van orde m en B van orde n is de matrix van orde mn gedefinieerd door

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

Eigenschappen: voor scalaire α, β, γ, δ geldt

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

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

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

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

In deze paragraaf beperken wij ons tot symmetrische, resp. scheve, C-matrices van de orde v van de vorm

$$C_v = \begin{pmatrix} 0 & j^T \\ \pm j^T & S_{v-1} \end{pmatrix}$$

met teken +, resp. -. Dan voldoet S_{v-1} aan

$$SS^T = (v - 1)I - J, \quad SJ = JS = 0, \quad S^T = \pm S.$$

Omgekeerd bepaalt zo'n S_{v-1} weer C_v. Wij noemen twee op deze wijze bij elkaar behorende matrices een paar S_{v-1}, C_v.

Stelling 9.1. Wanneer er een paar S_n, C_{n+1} bestaat, dan bestaat er een paar symmetrische S_{n^2}, C_{n^2+1}.

Bewijs. Zij

$$T = S_n \times S_n + I_n \times J_n - J_n \times I_n.$$

T heeft orde n^2 en voldoet wegens de eigenschappen van het Kronecker product aan $T^T = T$,

$$T(J \times J) = SJ \times SJ + IJ \times JJ - JJ \times IJ = 0,$$

$$TT^T = SS^T \times SS^T + nI \times J + nJ \times I + S \times SJ + S \times JS - SJ \times S - JS \times S -$$

$$- 2J \times J = n^2 I \times I - J \times J = n^2 I_{n^2} - J_{n^2}.$$

Daarom voldoen T en de met (0 + ... +) gerande T.

Stelling 9.2. Wanneer C_v een scheve C-matrix is, dan is

$$C_{2v} = \begin{pmatrix} C_v & C_v + I_v \\ C_v - I_v & -C_v \end{pmatrix}$$

een scheve C-matrix.

Bewijs.

$$C_{2v}C_{2v}^T = \begin{pmatrix} C_v & C_v + I_v \\ C_v - I_v & -C_v \end{pmatrix} \begin{pmatrix} C_v^T & C_v^T - I_v \\ C_v^T + I_v & -C_v^T \end{pmatrix} =$$

$$= \begin{pmatrix} 2C_vC_v^T + I_v & 0 \\ 0 & 2C_vC_v^T + I_v \end{pmatrix} = (2v - 1)I_{2v}.$$

Voorbeeld. Er bestaat een C-matrix van de orde 226. Immers, uit C_8 van het voorbeeld in §8 kan met stelling 9.2 een scheve C_{16} worden geconstrueerd. Uit de bijbehorende S_{15} maken wij volgens stelling 9.1 een S_{225} en een C_{226}. Dit voorbeeld toont aan, dat er C-matrices bestaan die niet Paley matrix zijn.

Stelling 9.3. Wanneer $q = p^k + 1 \equiv 0 \pmod 4$, p priem en wanneer er een scheve C-matrix van de orde n bestaat, dan bestaat er een scheve C-matrix van de orde qn.

Bewijs. Zij $q = p^k + 1 \equiv 0 \pmod 4$, p priem. Nummer de elementen van GF(q) zodat $\alpha_0 = 0$, $\alpha_{q-i} = -\alpha_i$, $i = 1, \ldots, q-1$. Zij de bijbehorende genormaliseerde Paley matrix

$$C_q = \begin{pmatrix} 0 & j^T \\ -j & S_{q-1} \end{pmatrix}. \quad \text{Zij} \quad U_{q-1} = \begin{pmatrix} 0 & & 1 \\ & \cdot & \\ 1 & & 0 \end{pmatrix}$$

de antidiagonaalmatrix van de orde q - 1. Dan is US symmetrisch wegens

$$US = \begin{pmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{pmatrix} (\chi(\alpha_i - \alpha_j)) = (\chi(\alpha_{q-i} - \alpha_j)) = (\chi(-\alpha_i - \alpha_j)).$$

Zij voorts C_n een scheve C-matrix van de orde n. Dan is

$$K_{qn} = C_q \times I_n + \begin{pmatrix} -1 & 0 \\ 0 & U \end{pmatrix}_q \times C_n + \begin{pmatrix} -1 & 0 \\ 0 & U \end{pmatrix}_q C_q \times C_n$$

een scheve C-matrix van de orde qn. Inderdaad, $K^T = -K$ volgt uit

$$\begin{pmatrix} -1 & 0 \\ 0 & U \end{pmatrix} C_q = \begin{pmatrix} -1 & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} 0 & j^T \\ -j & S \end{pmatrix} = \begin{pmatrix} 0 & -j^T \\ -j & US \end{pmatrix},$$

terwijl $KK^T = (qn - 1)I$ volgt uit het feit dat C_q en C_n scheve C-matrices zijn.

Stelling 9.4. Er bestaat een scheve C-matrix van de orde

$$v = 2^t \prod_{i=1}^{r} (p_i^{k_i} + 1), \quad p_i^{k_i} + 1 \equiv 0 \pmod 4,$$

p_i priem, t, r, k_i nietnegatief geheel.

Bewijs. Combineer de stellingen 8.4, 9.2, 9.3.

Een Hadamard matrix H_v is een vierkante matrix van de orde v met elementen ± 1, die voldoet aan $H_v H_v^T = vI_v$.

Stelling 9.5. Nodige voorwaarde voor het bestaan van een Hadamard matrix van de orde v is $v = 1$, $v = 2$ of $v \equiv 0 \pmod 4$.

Bewijs. Zoals dat van stelling 8.1.

Stelling 9.6. Er bestaat een Hadamard matrix van de orde v die wordt genoemd in stelling 9.4.

Bewijs. Wanneer C_v een scheve C-matrix is, dan is $H_v = C_v + I_v$ een Hadamard matrix.

Stelling 9.7. Wanneer er Hadamard matrices bestaan van de orde m en van de orde n, dan bestaat er een Hadamard matrix van de orde mn.

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

Stelling 9.8. Wanneer er een Hadamard matrix van de orde $m > 1$ en een symmetrische C-matrix van de orde n bestaat, dan bestaat er een Hadamard matrix van de orde mn.

Bewijs. Zij H_m, $m > 1$, Hadamard matrix, zij $P_m = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \times I_{\frac{1}{2}m}$ en zij C_n een symmetrische C-matrix. Dan is

$$H_{mn} = H_m \times C_n + P_m H_m \times I_n$$

een Hadamard matrix van de orde mn.

Opmerking. Reeds Sylvester construeerde Hadamard matrices van de orde 2^t. Paley [26] gebruikte C-matrices voor de constructie van H_n, $v = 2(p^k + 1)$, p priem, $p^k \equiv 1 \pmod 4$. Williamson [40] vond o.a. de in stelling 9.3, 9.4, 9.6, 9.8 genoemde constructies. Het vermoeden, dat voor alle $v \equiv 0 \pmod 4$ Hadamard matrices van de orde v bestaan, werd voor $v < 156$ bevestigd en is niet weersproken. Voor de stand van zaken wat betreft de existentie, zie [17] en [15]. Over het aantal Hadamard matrices van gegeven orde is minder bekend [17]. De matrices danken hun naam aan de ongelijkheid van Hadamard:

> Wanneer de elementen m_{ij} van een vierkante matrix M van orde v voldoen aan $-1 \leq m_{ij} \leq 1$, dan geldt $\det M \leq v^{\frac{1}{2}v}$, met gelijkheid dan en slechts dan als M een Hadamard matrix is.

In meetkundige formulering komt het probleem van de constructie van Hadamard matrices op de volgende vraag neer:

Kan men uit de 2^{v-1} hoekpunten van een hyperkubus γ_{v-1} er v kiezen, die de hoekpunten zijn van een regelmatig simplex α_{v-1}?

10. Toepassingen

10.1. Conferentie telefonie

De v directeuren van een bedrijf wensen de gelegenheid te hebben om conferentie per telefoon te houden en wel zo dat ieder met ieder kan spreken en dat de anderen het gesprokene kunnen beluisteren. Hoe dient het communicatienetwerk te worden geconstrueerd?

Beschouw een lineaire v-poort, dat is een netwerk met v klemmenparen (poorten). Tussen de klemspanningen V_i en de klemstromen I_i, $i = 1, 2, \ldots, v$, bestaan v lineaire afhankelijkheden. Evenzo zijn er v lineaire afhankelijkheden tussen de grootheden

$$b_i = \frac{V_i - R_i I_i}{2\sqrt{R_i}} \quad \text{en} \quad a_i = \frac{V_i + R_i I_i}{2\sqrt{R_i}}, \quad i = 1, 2, \ldots, v,$$

(R_i zijn de zogenaamde normeringsweerstanden), die worden uitgedrukt door

$$\underline{b} = S\underline{a},$$

met behulp van de $v \times v$ verstrooiingsmatrix S. Voor de elementen s_{ij} van S geldt

$$|s_{ij}|^2 = P_i/P_{j,max},$$

waarin P_i het in R_i omgezette arbeidsvermogen en $P_{j,max}$ het maximale door een bron in poort j leverbare arbeidsvermogen. Het totale door de n-poort opgenomen arbeidsvermogen is

$$\mathrm{Re} \sum_{i=1}^{v} V_i I_i^C = \sum_{i=1}^{v} (a_i a_i^C - b_i b_i^C) = \underline{a}^{CT}(I - S^{CT}S)\underline{a}.$$

Voor een passief netwerk is $I - S^{CT}S \geq 0$. Voor een verliesvrij netwerk is $I - S^{CT}S = 0$. Voor een reciprook netwerk is S symmetrisch: $S^T = S$. Voor een frequentie-onafhankelijk netwerk is S reëel: $S^C = S$. Wanneer bij voeding aan poort j alle overige poorten zoveel mogelijk arbeidsvermogen leveren en wel uniform verdeeld over de v - 1 overige poorten, dan moet

$$s_{ii} = 0 \ , \quad |s_{ij}| = 1/\sqrt{v - 1} \ , \quad i \neq j.$$

Wanneer aan al deze eisen is voldaan, dan voldoet $C = \sqrt{v - 1}\, S$ aan alle voorwaarden die wij voor symmetrische C-matrices hebben gesteld. Belevitch [2] bewees dat omgekeerd bij een gegeven symmetrische C-matrix een netwerk kan worden geconstrueerd dat voldoet aan alle bovengenoemde eisen. Hij voerde dit uit voor v = 2, 6, 10, 14, 18, 26 en vermoedde reeds in 1950 de in stelling 8.2 genoemde nodige voorwaarde, waaraan v = 22 niet voldoen. Het bewijs van stelling 8.2 is in wezen van hem afkomstig, evenals de in stelling 9.1 genoemde constructie.

10.2. Weegschema's

Stel wij moeten v objecten wegen in v wegingen met een chemische balans. De strategie van het wegen wordt beschreven door een matrix A die wordt gedefinieerd door zijn elementen

$a_{ij} = 1$, als het j^e object bij de i^e weging op de linkerschaal ligt,

$a_{ij} = -1$, als het j^e object bij de i^e weging op de rechterschaal ligt,

$a_{ij} = 0$, als het j^e object bij de i^e weging niet meedoet.

Neem aan dat geëist wordt dat

(1) de varianties van de geschatte gewichten gelijk zijn,

(2) de geschatte gewichten gelijk gecorreleerd zijn.

De vraag is welke weegstrategie de beste is, onder een geschikte definitie van "best", bijvoorbeeld de minimaliteit van de gemiddelde variantie.

Hotelling bewees dat voor $v \equiv 0 \pmod 4$ een Hadamard matrix het beste weegschema geeft. Raghavarao bewees dat voor $v \equiv 2 \pmod 4$ een C-matrix het beste weegschema geeft. Hij bewees voor het eerst de in stelling 8.2 genoemde nodige voorwaarde, met Hasse-Minkowski methoden. Voor literatuur, zie [29] en de daarin gegeven references.

11. Block designs

V is een eindige verzameling van de orde $|V| = v$. De delen van V heten blokken. Een IBD, incomplete block design, is een verzameling van, zeg b, verschillende blokken.

Een BIBD, balanced IBD, is een IBD met

(1) elk blok heeft evenveel, zeg k, elementen,

(2) elk paar van V ligt in evenveel, zeg λ, blokken,

(3) $0 < \lambda$ en $k < v - 1$.

Uit de beschouwing van de $v - 1$ paren uit V, die een gegeven $x \in V$ bevatten, volgt

(4) elk element van V ligt in evenveel, zeg r, blokken,

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

De $v \times b$ incidentiematrix N van een BIBD wordt gedefinieerd door

$$n_{ij} = \begin{cases} 1 & \text{als } x_i \in V \text{ ligt in blok } B_j, \\ 0 & \text{anders.} \end{cases}$$

In termen van N luiden de voorwaarden (1), (4), (2)

$$JN = kJ, \quad NJ = rJ, \quad NN^T = (r - \lambda)I + \lambda J.$$

Daar $r = \lambda$ strijdig is met $k < v - 1$, geldt $r > \lambda$ en

$$\det NN^T = [r + (v - 1)\lambda][r - \lambda]^{v-1} \neq 0.$$

Wegens rang $NN^T \leq$ rang N volgt hieruit dat $v \leq b$, de ongelijkheid van Fisher.

Een SBIBD, symmetric BIBD, is een BIBD met $b = v$, d.w.z. $r = k$. Voor de nu vierkante incidentiematrix N geldt

$$NJ = JN = kJ, \quad NN^T = N^TN = (k - \lambda)I + \lambda J, \quad (\det N)^2 = k^2(k - \lambda)^{v-1}.$$

Als v even is dan moet noodzakelijk $k - \lambda$ een kwadraat zijn.

Vraagstuk: Zij A een symmetrische (0,1) matrix van de orde v zodat (Ryser)

$AA^T = (k - \lambda)I + \lambda J$, $0 < \lambda < k < v - 1$, $k - \lambda = k^2 - \lambda v$.

Stel $k - \lambda$ is geen kwadraat van een geheel getal.

Bewijs dat A precies k enen op zijn hoofddiagonaal heeft.

In het volgende behandelen wij vier algemene constructiemethoden voor block designs. De eerste methode, toegelicht in stellingen 11.1, 11.2, 11.3, maakt gebruik van resp. C-matrices, netten en Hadamard matrices.

Stelling 11.1. Wanneer er een C-matrix van de orde n bestaat, dan bestaat er een BIBD met parameters

$$v = n,\ b = 2n - 2,\ k = \frac{1}{2}n,\ r = n - 1,\ \lambda = \frac{1}{2}n - 1.$$

Bewijs. Neem aan dat het paar C_n, S_{n-1} bestaat. Dan voldoet

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

aan de definiërende eigenschappen van een BIBD met de gevraagde parameters.

Stelling 11.2. Er bestaat een SBIBD met parameters

$$v = n^2 + n + 1,\ k = n + 1,\ \lambda = 1, \text{ waar } n = p^\alpha,\ p \text{ priem}.$$

Bewijs. Volgens stelling 5.3 bestaat er een volledig stelsel latijnse vierkanten van de orde $n = p^\alpha$, p priem, m.a.w. bestaat er een net(n,n+1). Zij V de verzameling van de orde $n^2 + n + 1$ bestaande uit de n^2 punten en de n + 1 parallelklassen van het net. Beschouw als blokken de n-klieks en de verzameling der parallelklassen van het net. De incidentiematrix van dit IBD voldoet aan de definiërende eigenschappen van een SBIBD met de gevraagde parameters.

Stelling 11.3. Wanneer er een Hadamard matrix van de orde $n = 4t \geq 8$ bestaat, dan bestaat er een SBIBD met parameters

$$v = 4t - 1,\ k = 2t - 1,\ \lambda = t - 1.$$

Bewijs. Normaliseer de Hadamard matrix van de orde n = 4t tot

$$H = \begin{pmatrix} 1 & j^T \\ r & R \end{pmatrix},$$

dan geldt voor R

$$RJ = JR = -J, \quad RR^T = 4tI - J.$$

De (0,1) matrix $N = \frac{1}{2}(R + J)$ voldoet aan de definiërende eigenschappen van een SBIBD met de gevraagde parameters.

Een PBIBD, partially balanced IBD met twee associatieklassen, is een IBD waarvan de verzameling V de structuur van een sterk reguliere graaf $\{V,A\}$ heeft en waarvoor geldt

(1) elk blok heeft evenveel, zeg k, elementen,

(2) elk element van V ligt in evenveel, zeg r, blokken,

(3) elk verbonden paar van V ligt in evenveel, zeg λ_1, blokken,

(4) elk niet verbonden paar van V ligt in evenveel, zeg λ_2, blokken.

In termen van verbindingsmatrix A en incidentiematrix N luiden deze voorwaarden

$$JN = kJ, \quad NJ = rJ, \quad NN^T = rI + \frac{1}{2}(\lambda_1 + \lambda_2)(J - I) + \frac{1}{2}(\lambda_2 - \lambda_1)A.$$

Opmerking. Een PBIBD is, anders gezegd, een sterk reguliere graaf met een blokstructuur die voldoet aan bovengestelde eisen. De ongelijkheid van Fisher behoeft niet te gelden. Voor de (schaarse) voldoende voorwaarden voor het bestaan van zulk een blokstructuur, zie [3] en [7]. Voor tabellen van BIBD, zie [14] pp. 90-93. Voor tabellen van PBIBD, zie [6]. Voor een literatuuroverzicht, zie [16].

Tweede methode. De volgende constructies van PBIBD berusten op dualisering en zijn ontleend aan [38].

Stelling 11.4. Het duale IBD van een niet symmetrisch BIBD met parameters v, b, r, k, $\lambda = 1$ is een PBIBD met parameters b, v, k, r, $\lambda_1 = 1$, $\lambda_2 = 0$.

Bewijs. Elk tweetal blokken van een BIBD met $\lambda = 1$ heeft één of geen punt gemeen. Elk blok is incident met k punten. Daarom is

$$N^TN = kI + B$$

waarin B een reguliere symmetrische (0,1) matrix is. NN^T heeft de eigenwaarden $r - 1$ en rk met multipliciteiten $v - 1$ en 1. Wegens $b > v$ heeft N^TN de eigenwaarden $r - 1$, 0 en rk met multipliciteiten $v - 1$, $b - v$, 1. Schrijf

$$N^TN = kI + \frac{1}{2}(J - I) - \frac{1}{2}A \text{ , met } A = J - I - 2B.$$

A is de verbindingsmatrix van een sterk reguliere graaf, omdat A een symmetrische (0,1,-1) matrix is met diagonaal 0 en met drie eigenwaarden waarvan één de multipliciteit 1 heeft en eigenvector (1, 1, ..., 1). Daarom is N^T de incidentiematrix van een PBIBD met de gevraagde parameters.

Met dezelfde methode als hierboven gebruikt kan men door dualisering ook uit sommige andere BIBD nieuwe PBIBD construeren. Immers uit

$$NN^T = rI + \lambda(J - I),\ JN = kJ,\ NJ = rJ$$

volgt dat NN^T eigenwaarden $r - \lambda$ en rk heeft met multipliciteiten $v - 1$ en 1. Dan heeft de symmetrische matrix met nuldiagonaal

$$N^TN - kI - \lambda_2(J - I)$$

de eigenwaarden $r - \lambda - k + \lambda_2$, $-k + \lambda_2$, $rk - k - \lambda_2(b - 1)$ met multipliciteiten $v - 1$, $b - v$, 1. Wanneer nu deze matrix een geheel veelvoud, zeg $\lambda_1 - \lambda_2$, is van een (0,1) matrix B, dan is de verlangde PBIBD verkregen. Immers dan geldt voor $A = J - I - 2B$ dat

$$N^TN = kI + \lambda_2(J - I) + (\lambda_1 - \lambda_2)B = kI + \frac{1}{2}(\lambda_1 + \lambda_2)(J - I) + \frac{1}{2}(\lambda_2 - \lambda_1)A$$

en is A de verbindingsmatrix van een sterk reguliere graaf. In dit verband is het volgende criterium soms nuttig.

Lemma. Een vierkante gehele matrix B is een (0,1) matrix dan en slechts dan als $\operatorname{tr} BB^T = \sum_{i,j} b_{ij}$.

Bewijs. Voor gehele b_{ij} geldt $b_{ij}^2 \geq b_{ij}$ met gelijkheid dan en slechts dan als $b_{ij} = 0$ of 1.

Voorbeeld. Het duale IBD van een BIBD met parameters

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

is een PBIBD met parameters b, v, k, r, $\lambda_1 = 1$, $\lambda_2 = 2$.

Bewijs. $B = -N^TN + (r-2)I + 2(J-I)$ voldoet aan de voorwaarden van het Lemma.

Stelling 11.5. Het duale IBD van een symmetrisch PBIBD met $\lambda_1 = \lambda_2 \pm 1$ is een PBIBD met dezelfde parameters.

Bewijs. Daar $r = k$ en $\lambda_1 - \lambda_2 = \pm 1$, geldt voor het gegeven PBIBD

$$JN = NJ = rJ,\ NN^T = rJ + \lambda_2(J-I) \pm C$$

met (0,1) verbindingsmatrix C van een sterk reguliere graaf.
De matrix

$$B = \pm [N^TN - rJ - \lambda_2(J-I)]$$

heeft dezelfde eigenwaarden met dezelfde multipliciteiten en dezelfde elementensom als C. Daarom is B eveneens een (0,1) matrix en is het duale design weer een PBIBD met

$$JN^T = N^TJ = rJ,\ N^TN = rJ + \lambda_2(J-I) \pm B.$$

Derde methode. De derde algemene constructiemethode voor block designs is een toepassing van eindige meetkunde, zie [11].

Een permutatiegroep Γ van een eindige verzameling V heet 2-homogeen, als bij elk tweetal paren $P = \{x,y\}$ en $P' = \{x',y'\}$, $x,y,x',y' \in V$, een

een permutatie $\gamma \in \Gamma$ bestaat zodat $P' = \gamma(P)$.
Merk op dat Γ zeker 2-homogeen is als Γ 2-transitief is. Voorts volgt, voor $v \geq 3$, uit de 2-homogeniteit van Γ de 1-transitiviteit. Inderdaad, om te bewijzen dat een 2-homogene Γ een permutatie bevat die $a \in V$ overvoert in $b \in V$, beschouwen wij $c \in V$ en $\alpha \in \Gamma$ met $\{\alpha(a), \alpha(c)\} = \{a,b\}$. Zou $\alpha(a) \neq b$, dan is $\alpha(c) = b$. Beschouw dan $\beta \in \Gamma$ met $\{\beta(a), \beta(c)\} = \{b,c\}$. Zou $\beta(a) \neq b$, dan is $\beta(a) = c$. Dan voldoet $\alpha\beta$ wegens $\alpha\beta(a) = \alpha(c) = b$.

Beschouw nu een deelverzameling $B_0 \subset V$ met $2 \leq |B_0| = k \leq v - 2$.

Stelling 11.6. $\mathcal{B} = \{\gamma(B_0) \mid \gamma \in \Gamma, \Gamma \text{ 2-homogeen op } V\}$ is een BIBD, waarvan Γ een automorfismengroep is die transitief is op de punten en op de blokken.

Bewijs. Elk blok, element van $\mathcal{B}$, bevat k elementen van V. Wegens $(\alpha(B_0) \neq \beta(B_0)) \Rightarrow (\gamma\alpha(B_0) \neq \gamma\beta(B_0))$ voor alle α, β, $\gamma \in \Gamma$ en de 2-homogeniteit ligt elk paar van V in evenveel blokken. De bloktransitiviteit volgt uit de definitie; de punttransitiviteit volgt uit de 2-homogeniteit.

Opmerking. Voor de stabilisator Λ van B_0, gedefinieerd door

$$\Lambda = \{\gamma \in \Gamma \mid \gamma(B_0) = B_0\},$$

geldt $|\Gamma| = |\Lambda| \cdot |\mathcal{B}|$. Het aantal blokken b is dus gelijk aan de index $|\Gamma : \Lambda|$ van de ondergroep Λ in Γ.

Beschouw de vectorruimte V(n,q) van dimensie n over GF(q), $q = p^k$, p priem. Dan is $|V(n,q)| = q^n$.

Stelling 11.7. Voor het aantal N(s,n,q) van de deelruimten V(s,q) in V(n,q) geldt

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

Bewijs. Het aantal der V(s+1,q) in V(n,q), dat een gegeven V(s,q) bevat, is

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

Daarom geldt

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

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

Stelling 11.8. De V(1,q) en de V(s,q) van een V(n,q), $1 < s < n$, vormen de punten en de blokken van een BIBD met

$v = N(1,n,q)$, $b = N(s,n,q)$, $k = N(1,s,q)$, $r = N(s-1,n-1,q)$,

$\lambda = N(s-2,n-2,q)$.

Dit is een SBIBD dan en slechts dan als $s = n - 1$.

Bewijs. Pas toe stelling 11.6 voor de groep der reguliere lineaire afbeeldingen van V(n,q).

Wij geven nog een toepassing van stelling 11.6. Beschouw de vectorruimte $V(2,q^2)$ van dimensie 2 over $GF(q^2)$, $q = p^k$, $p \neq 2$ priem. De $q^2 + 1$ rechten door O zijn de $q^2 + 1$ projectieve punten op de projectieve lijn $PG(1,q^2)$. De projectieve symplectische groep $PSP(2,q^2)$, die isomorf is met de projectieve speciale lineaire groep $PSL(2,q^2)$, werkt 2-transitief op de punten van $PG(1,q^2)$. Inderdaad, de rechten door $(\alpha,1)$ resp. $(\beta,1)$ worden overgevoerd in de rechten door $(\alpha',1)$ resp. $(\beta',1)$ door de transformatie

$$\begin{pmatrix} \alpha' & \beta' \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ -1 & \alpha \end{pmatrix}$$

voor elke $\lambda \neq 0$, $\lambda \in GF(q^2)$. Echter $PSP(2,q^2)$ is niet 3-transitief omdat de (1,0) en (0,1) invariant latende transformatie

(1)
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

de rechte door $(\alpha,1)$ overvoert in de rechte door $(\lambda^2\alpha,1)$. Nu is $GF(q^2)$ te beschouwen als de kwadratische uitbreiding van $GF(q)$, het deellichaam der kwadraten van $GF(q^2)$. Zij B_0 de verzameling der "rationale" rechten door O in $V(2,q^2)$, d.w.z. de rechten met richtingscoëfficiënt in $GF(q)$. Toepassing van stelling 11.6 geeft een BIBD met de parameters

$$v = q^2 + 1,\ b = q(q^2 + 1),\ r = q(q + 1),\ k = \lambda = q + 1.$$

Inderdaad, $k = |B_0| = q + 1$ en $b = q(q^2 + 1)$ wegens

$$|\Gamma| = \tfrac{1}{2}(q^2 + 1)q^2(q^2 - 1) \quad \text{en} \quad |\Lambda| = \tfrac{1}{2}(q + 1)q(q - 1).$$

Dat de orde van $PSP(2,q)$ gelijk is aan $\frac{1}{2}q(q^2 - 1)$ volgt uit

$$|GL(2,q)| = (q^2 - 1)(q^2 - q) = \text{aantal bases in } V(2,q),$$

$$|GL(2,q)/SL(2,q)| = |GF^*(q)| = q - 1.$$

Een derde toepassing [25] van stelling 11.6 is de volgende. Zij

$$v \equiv 3 \pmod 4,\ v \equiv 1 \pmod 3,\ v = p^r,\ p \text{ priem}.$$

Zij Q de groep der kwadraten in $GF(v)\setminus\{0\}$. Omdat $|Q| = \frac{1}{2}(v - 1)$ deelbaar is door 3 is er een element $q \in Q$ van de orde 3. Zij voorts

$$\Gamma = \{\gamma : \gamma(x) = mx + a,\ m \in Q,\ a \in GF(v)\} \text{ en } B_0 = \{0,1,q\}.$$

Dan geldt $|\Gamma| = \frac{1}{2}v(v - 1)$ en $|\Lambda| = 3$ voor de stabilisator Λ van B_0. Inderdaad, wegens $v = p^r \equiv 3 \pmod 4$ zijn er geen permutaties γ die één element van B_0 fixeren en de beide andere elementen van B_0 verwisselen. Voorts permuteren $\lambda(x) = qx + 1$ en $\lambda^2(x) = q^2(x - 1)$ de elementen van B_0 cyclisch. Toepassing van stelling 11.6 levert een BIBD met

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

en wel, wegens $k = 3$, $\lambda = 1$, een zogenaamd Steiner tripel.

Vierde methode. Tenslotte behandelen wij een constructiemethode van een PBIBD volgens E. Seiden [36], met behulp van ovalen in een eindig projectief vlak.
Een eindig projectief vlak van orde n is een SBIBD met

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

Volgens stelling 11.2 bestaan zij voor $n = p^\alpha$, p priem, ook $p = 2$.
De zo geconstrueerde eindige projectieve vlakken laten zich coördinatiseren met behulp van $GF(p^\alpha)$ en zijn Desargues. Er bestaan, reeds voor $n = 9$, ook niet-desarguese projectieve vlakken. Nodig voor het bestaan van een eindig projectief vlak van de orde n is de voorwaarde van Bruck en Ryser:

$$(n \equiv 1, 2 \pmod 4) \Rightarrow (n = a^2 + b^2,\ a \text{ en } b \text{ geheel}).$$

Hierdoor zijn $n = 6$, $n = 14$, $n = 21$, $n = 22$ uitgesloten. De kleinste orden, waarvoor de existentie van een projectief vlak onbeslist is, zijn $n = 10$ en $n = 12$.
Een ovaal van de orde k is een verzameling van k punten van een eindig projectief vlak, waarvan geen drietal collineair is. Een voorbeeld van een ovaal van de orde $n + 1$ is een kegelsnede in een projectief vlak over GF(n).

Stelling 11.9. (Segre [32]). Een ovaal van orde $n + 1$ in een projectief vlak over GF(n), $n = p^\alpha$, p priem, $p \neq 2$, is een kegelsnede.

Zij nu verder n even, $n = 2h$ met h natuurlijk. Zij K een ovaal van de orde $2h + 1$. De rechten worden onderscheiden in secanten die 2 punten met K gemeen hebben, tangenten die 1 punt met K gemeen hebben, en nietsnijders die geen punt met K gemeen hebben. Door elk punt van K gaat één tangent. Er geldt [28]:

Stelling 11.10. De $2h + 1$ tangenten van een ovaal K van de orde $2h + 1$ in een projectief vlak van de orde $2h$ gaan door één punt.

Bewijs. Omdat 2h + 1 oneven is, gaat er door elk punt van elke secant tenminste één tangent. Omdat er in totaal 2h + 1 tangenten zijn, gaat er door elk punt van elke secant precies één tangent. Het snijpunt van twee tangenten kan dus slechts door tangenten verbonden worden met de punten van K. Hieruit volgt dat de tangenten door één punt gaan.

Indien er in een projectief vlak van even orde 2h een ovaal K van de orde 2h + 1 bestaat, dan bestaat er dus ook een ovaal L van de orde 2h + 2. Deze L heeft geen tangenten. Door elk punt $\notin$ L gaan 2h + 1 rechten, namelijk h + 1 secanten en h nietsnijders. In totaal zijn er (h+1)(2h+1) secanten. Elke secant bevat 2h - 1 punten $\notin$ L. Beschouw nu de punten van het projectieve vlak die $\notin$ L en neem de secanten als blokken. Dan

$$v = 4h^2 - 1,\ b = (h+1)(2h+1),\ r = h + 1,\ k = 2h - 1.$$

Dit is een PBIBD wanneer de $4h^2 - 1$ punten tot een graaf worden gemaakt door puntenparen te verbinden wanneer zij op een secant liggen. Inderdaad wordt zo een sterk reguliere graaf verkregen, immers

$$n_1 = 2h^2 - 2,\ n_2 = 2h^2,\ p_{12}^1 = h^2,\ p_{12}^2 = h^2 - 1, \text{ dus}$$

$$\rho_0 = 2,\ \rho_1 = 1 + 2h,\ \rho_2 = 1 - 2h.$$

De verbindingsmatrix A van de graaf voldoet aan

$$(A - I - 2hI)(A - I + 2hI) = -J,\ AJ = 2J.$$

Na toevoeging van een geisoleerd punt wordt hieruit verkregen de matrix B van orde $4h^2$ met

$$(B - I - 2hI)(B - I + 2hI) = 0,$$

dus een symmetrische Hadamard matrix B - I met constante diagonaal.

Opmerking. Deze constructie is slechts gerealiseerd in het geval $h = 2^{\alpha}$.

12. Kirkman systemen

Een BIBD heet oplosbaar = resolvable wanneer hij een parallelisme bezit. Een parallelisme van een BIBD met puntverzameling V en blokverzameling $\mathfrak{B}$ is een equivalentierelatie $\|$ op $\mathfrak{B}$ die voldoet aan het axioma van Euclides

$$\forall_{p} \in V \; \forall B \in \mathfrak{B} \; \exists C \in \mathfrak{B} (p \in C, \; B \| C).$$

Voor een oplosbaar BIBD geldt $v = km$ en $b = rm$, waarin m het aantal blokken in elke parallelklasse is.

Voorbeeld. Vijftien schoolmeisjes wandelen op elk van de 7 dagen van de week in 5 rijen van 3. Is het mogelijk dat elk meisje met elk ander meisje slechts eenmaal per week in dezelfde rij loopt? Deze vraag naar een oplosbaar BIBD met

$$v = 15 \; , \quad b = 35 \; , \quad k = 3 \; , \quad r = 7 \; , \quad \lambda = 1$$

wordt opgelost door het volgende arrangement:

(1,2,5)	(3,14,15)	(4,6,12)	(7,8,11)	(9,10,13) ,
(1,3,9)	(2,8,15)	(4,11,13)	(5,12,14)	(6,7,10) ,
(1,4,15)	(2,9,11)	(3,10,12)	(5,7,13)	(6,8,14) ,
(1,6,11)	(2,7,12)	(3,8,13)	(4,9,14)	(5,10,15) ,
(1,8,10)	(2,13,14)	(3,4,7)	(5,6,9)	(11,12,15) ,
(1,7,14)	(2,4,10)	(3,5,11)	(6,13,15)	(8,9,12) ,
(1,12,13)	(2,3,6)	(4,5,8)	(7,9,15)	(10,11,14) .

Voorbeeld. Opdat het in stelling 11.8 genoemde BIBD der lineaire deelruimten V(1,q) en V(s,q) van een V(n,q) een parallelisme bezit, is nodig dat v deelbaar is door k, dus dat $q^n - 1$ deelbaar is door $q^s - 1$, dus dat n deelbaar is door s. Het is niet bekend of deze voorwaarde ook voldoende is. Dit is volgens het vorige voorbeeld wel het geval als $n = 4$, $s = 2$, $q = 2$.

Het probleem van de schoolmeisjes is een bijzonder geval van het in 1850 door Kirkman gestelde

probleem: Voor welke m, k is het mogelijk om mk symbolen op r verschillende manieren te verdelen in m blokken van elk k symbolen zodat elk paar symbolen precies éénmaal wordt gebruikt?

Een oplossing heet een Kirkman systeem.

Stelling 12.1. Een Kirkman systeem K(k,t) is een oplosbaar BIBD met $\lambda = 1$.

Bewijs. Beschouwing van alle paren die een vast symbool bevatten leert dat $mk - 1 = r(k - 1)$. Noem

$$\frac{m - 1}{k - 1} = t$$

dan $m = t(k - 1) + 1$, $r = kt + 1$ en

$$v = k[t(k - 1) + 1],\ b = (kt + 1)[t(k - 1) + 1],\ k = k,\ \lambda = 1.$$

Opmerking. Voor $t = 1$ staat er

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

en komt het Kirkman probleem neer op het zoeken naar $k - 1$ orthogonale latijnse vierkanten van de orde k.

Opmerking. K(3,2) is het schoolmeisjes probleem.

Thans volgen twee voorbeelden van constructie van oplosbare BIBD. Het tweede voorbeeld betreft een Kirkmansysteem.

Beschouw de projectieve ruimte PG(3,q) over een Galois lichaam van de orde $q = p^k$, p priem. Volgens stelling 11.7 is het aantal punten

$$v = (q^2 + 1)(q + 1).$$

Er zijn drie typen van niet ontaarde kwadrieken, namelijk kegels met $q^2 + q + 1$ punten, regelvlakken met $(q + 1)^2$ punten en elliptische kwadrieken, zonder rechten, met $k = q^2 + 1$ punten. De verzameling der elliptische kwadrieken is een BIBD met

$$v = (q^2 + 1)(q + 1),\ b = \frac{1}{2} q^4(q^3 - 1)(q^2 - 1),\ k = q^2 + 1,$$

$$r = \frac{1}{2} q^4(q^3 - 1)(q - 1),\ \lambda = \frac{1}{2} q^5(q - 1)^2.$$

Opdat deze BIBD oplosbaar is moet de verzameling der b elliptische kwadrieken kunnen worden gesplitst in r deelverzamelingen van elk q + 1 kwadrieken, zodat elke deelverzameling alle v punten bevat, m.a.w. zodat elk paar kwadrieken uit elke deelverzameling disjunct is. Het ligt voor de hand te proberen om voor de deelverzamelingen de bundels van kwadrieken te nemen omdat die precies q + 1 stuks bevatten. Wanneer Q en Q' geen punt gemeen hebben, dan heeft geen paar kwadrieken uit de bundel $\lambda Q + \mu Q'$ een punt gemeen. Als Q en Q' elliptisch zijn, dan is ook elke kwadriek van de bundel elliptisch omdat $v = (q^2 + 1)(q + 1)$. Het komt er dus op neer om twee disjuncte elliptische kwadrieken te vinden. Dit is een moeilijke zaak. Voor q = 2 voldoen de kwadrieken door de punten

(1,0,0,0), (0,1,0,0), (1,1,1,0), (1,1,0,1), (1,1,1,1), en

(0,0,1,0), (0,0,0,1), (1,1,0,0), (1,0,1,0), (0,1,0,1).

Ook voor q = 3 bestaat er een oplossing, zie [27] dat geen oplossingen voor q > 3 aangeeft.

Wij construeren tenslotte een Kirkmansysteem K(k,t) met t = k - 2, k - 1 = q, m.a.w. een oplosbaar BIBD met

$$v = (q + 1)(q^2 - q + 1),\ b = q^2(q^2 - q + 1),\ r = q^2,\ k = q + 1,\ \lambda = 1.$$

Beschouw daartoe in $PG(2,q^2)$, $q = p^k$, p priem, de kromme

$$\Sigma : x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0.$$

Onder de afbeelding

$$\phi : x \in GF(q^2) \to y = x^{q+1} \in GF(q)$$

gaan de punten van Σ over in de q + 1 punten van de rechte

$$y_1 + y_2 + y_3 = 0 \quad \text{in} \quad PG(2,q).$$

De kromme Σ in $PG(2,q^2)$ bevat $q^3 + 1$ punten. Inderdaad, $\phi^{-1}(1,-1,0)$ bevat $q + 1$ punten, $\phi^{-1}(y_1,y_2,-y_1,-y_2)$ voor $y_1 \neq 0$, $y_2 \neq 0$, $y_1 + y_2 \neq 0$ bevat $(q + 1)^2$ punten, dus Σ bevat er

$$3(q + 1) + (q - 2)(q + 1)^2 = q^3 + 1.$$

De kromme Σ wordt door een rechte in $PG(2,q^2)$ in ten hoogste $q + 1$ punten gesneden. Inderdaad, het linkerlid is niet deelbaar door $ax_1 + bx_2 + cx_3$ omdat (neem $c = -1$) de volgende uitdrukking niet identiek nul is

$$x_1^{q+1} + x_2^{q+1} + (ax_1 + bx_2)^{q+1} =$$

$$= (1 + a^{q+1})x_1^{q+1} + (1 + b^{q+1})x_2^{q+1} + a^q b x_1^q x_2 + ab^q x_1 x_2^q.$$

De poollijn van een punt $(a_1,a_2,a_3) \in PG(2,q^2)$ t.o.v. Σ is de rechte

$$a_1^q x_1 + a_2^q x_2 + a_3^q x_3 = 0.$$

Hierdoor is een polariteit gedefinieerd wegens

$$a_1 b_1^q + a_2 b_2^q + a_3 b_3^q = (a_1^q b_1 + a_2^q b_2 + a_3^q b_3)^q.$$

De raaklijn van $(a_1,a_2,a_3) \in \Sigma$ is de poollijn van (a_1,a_2,a_3) t.o.v. Σ. Deze raaklijn heeft geen andere snijpunten met Σ. Immers, zouden de raaklijnen in A en B dezelfde zijn, dan is A = B wegens

$$a_i^q = \lambda b_i^q \Rightarrow a_i = \mu b_i.$$

Elk der q^2 nontangenten door $A \in \Sigma$ snijdt Σ in precies $q + 1$ punten, inclusief A. Inderdaad, Σ bevat q^3 punten $\neq A$ die, met A verbonden, ten hoogste q^2 rechten opleveren, die elk met Σ ten hoogste q snijpunten $\neq A$ bezitten. Deze maximale aantallen worden dus bereikt.
Het aantal raaklijnen aan Σ is $q^3 + 1$, het aantal nontangenten is dus $q^2(q^2 - q + 1)$. De punten van Σ en de nontangenten in $PG(2,q^2)$ vormen een BIBD met $v = q^3 + 1$, $b = q^2(q^2 - q + 1)$, $r = q^2$, $k = q + 1$, $\lambda = 1$.

Dit BIBD is oplosbaar, is een K(k,t) met

$$k = q + 1,\ t = q - 1,\ m = q^2 - q + 1.$$

Om dit aan te tonen beschouwen wij een punt $Q \in \Sigma$, zijn raaklijn ρ met de q^2 andere punten $P_1, \ldots, P_{q^2}$. Door elk van deze P_i gaan $q + 1$ raaklijnen aan Σ dus $q^2 - q$ nontangenten. Voeg daarbij de poollijn van P_i dan zijn aan P_i toegevoegd $q^2 - q + 1$ nontangenten, elk $q + 1$ punten van Σ bevattend en samen alle $q^3 + 1$ punten van Σ bevattend. Door nu $i = 1, 2, \ldots, q^2$ te nemen doen wij zulks op q^2 manieren, en zo dat elk paar punten van Σ, dus elke nontangent, precies éénmaal wordt gebruikt.

Opmerking. Door Q de $q^3 + 1$ punten van Σ te laten doorlopen zien wij dat er $q^3 + 1$ verschillende manieren zijn om het BIBD op te lossen.

Opmerking. De eerste der hierboven aangegeven constructies is van Primrose [27]. De tweede constructie is van Bose [4]. Onlangs hebben Bose-Chakravarti [5] en ook Wan Zhe Xian = Wan Che Hsien, in een serie artikelen beginnend met [39], dit soort constructies gegeneraliseerd.

Opmerking. Actueel is de belangstelling voor algemenere systemen zoals orthogonal arrays (zie [35]) en partiële meetkunden (zie [3]). Voor een overzicht van eindige meetkunden zie [12]. Voor andere toepassingen van eindige meetkunden en hun groepen zie [24] en [32].

Hoofdstuk II. Coding Theory

1. Inleiding

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

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

bij blikseminslag tijdens een telefoongesprek. Fouten in magneetbanden komen ook in series voor. Men spreekt in dat geval van "burst-errors".

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

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

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

2. De stelling van Shannon (speciaal geval)

We geven nu een idee van de grote mogelijkheden van coding door een voorbeeld (van D. Slepian [4]). We hebben een binair symmetrisch kanaal ter beschikking met kans p dat een symbool verkeerd wordt ontvangen en kans q = 1 - p dat het goed aankomt. Via dit kanaal willen we de resultaten overbrengen van een experiment waarbij met constante snelheid met een munt kruis of munt wordt geworpen. Stel dat we over het kanaal met twee keer zo grote snelheid symbolen kunnen overbrengen. Als we niet aan deze snelheden gebonden waren zouden we voor een overbrenging met willekeurig grote nauwkeurigheid kunnen zorgen en wel als volgt. Bij de worp kruis zenden we N keer een 1 over het kanaal, bij munt N keer een 0. De ontvanger vertaalt een serie van N signalen in kruis als meer dan de helft van de signalen 1 is. Neem nu als voorbeeld p = 0,001. De kans dat de ontvanger verkeerd decodeert is dan

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

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

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

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

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

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

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

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

We construeren de signalen en het decodeervoorschrift zó dat deze kans inderdaad $< \varepsilon$ is. De constructie levert k van die signalen. We moeten dan aantonen dat voor grote n geldt: $k \geq 2^{\frac{1}{2}n} = 2^s$. Als met n symbolen, bij zekere code, k verschillende mededelingen kunnen worden gezonden over het kanaal noemt men $\frac{^2\log k}{n}$ de <u>transmissiesnelheid</u>. Dit is een maat voor de hoeveelheid informatie per symbool. In ons voorbeeld moet deze snelheid tenminste $\frac{1}{2}$ zijn. (In dit bewijs schrijven we log i.p.v. $^2\log$.) Voor het bewijs zijn de volgende voorbereidingen nodig:

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

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

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

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

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

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

$$\sum_{w \leq np+b} \binom{n}{w} < \frac{1}{2} n \binom{n}{\rho}.$$

(5) Als we n objecten willen kleuren met n kleuren kan dit op n^n manieren. Als we eisen dat de eerste m kleuren op precies m objecten voorkomen is het aantal mogelijkheden $\binom{n}{m} m^m (n - m)^{n-m}$. Dus is

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

Dit is ook in te zien door op te merken dat $1 = (\frac{m}{n} + \frac{n - m}{n})^n \geq$
$\geq \binom{n}{m} (\frac{m}{n})^m (\frac{n - m}{n})^{n-m}$.

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

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

en analoog

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

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

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

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

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

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

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

3. Lineaire codes (groep-codes) (zie [3]).

Beschouw een kanaal waarvoor het aantal mogelijke symbolen gelijk is aan q, waarin q een macht van een priemgetal is. De symbolen kunnen dan worden opgevat als elementen van GF(q). Vaak zullen we ons tot q = 2 beperken (symbolen 0 en 1). De verzameling n-tallen van dergelijke symbolen is een vectorruimte R over GF(q). Als een collectie n-tallen een k-dimensionale lineaire deelruimte V van R vormt noemen we het een lineaire code en wel een (n,k) code. Het gewicht van een vector (= Hamming weight) is het aantal componenten $\neq 0$. Daar het verschil van 2 vectoren uit de code weer een codevector is, is de minimale afstand tussen vectoren van de code gelijk aan het minimale gewicht van de vectoren $\neq (0, 0, \ldots, 0)$ uit V.

We kunnen de code op de volgende 2 manieren beschrijven:

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

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

De eigenschappen van de code die ons interesseren veranderen niet als we de kolommen van de voortbrenger G permuteren. De codes die zo uit G ontstaan noemen we equivalent met de oorspronkelijke. Het is eenvoudig in te zien dat er bij een gegeven code een equivalente code

is waarvan de matrix G de vorm $(I_k P)$ heeft waarin I_k de $k \times k$ eenheidsmatrix is en P een $k \times (n - k)$ matrix. De bijbehorende parity-check matrix is $(-P^T I_{n-k})$. Een codevector vinden we door $v_1, v_2, \ldots, v_k$ willekeurig te kiezen en $v_{k+j} = \sum_{i=1}^{k} v_i p_{ij}$ (voor $j = 1, 2, \ldots, n-k$) te nemen. Het coderen is nu een eenvoudige zaak geworden! Men noemt v_1 t/m v_k information symbols, v_{k+1} t/m v_n parity-check symbols.

Een tabel voor het decoderen maken we als volgt. We merken op dat V een ondergroep is van R. Uit iedere nevenklasse van V kiezen we een representant en wel zo dat de kans op ontvangst van deze representant, als (0, 0, ..., 0) het gezonden signaal is, maximaal is. Dat wil dus zeggen dat we uit iedere nevenklasse een element met minimaal gewicht kiezen. Schrijf in een rij, achter elkaar, de codewoorden $\underline{v}_1 = 0, \underline{v}_2, \ldots$ $\ldots, \underline{v}_{q^k}$. Schrijf onder $\underline{v}_1$ de gekozen representanten van de nevenklassen en achter zo'n representant in een rij $\underline{v} + \underline{v}_2$, $\underline{v} + \underline{v}_3$, etc. Een ontvangen woord wordt vertaald in het codewoord waar het onder staat in dit schema. Als $\underline{u}$ wordt gezonden en $\underline{v}$ ontvangen dan is deze manier van decoderen goed als $\underline{v} - \underline{u}$ één van de gekozen representanten is.

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

$$v_3 = v_1 + v_2,$$

$$v_4 = 2v_1 + v_2.$$

De code V bestaat uit de woorden: (0, 0, 0, 0), (0, 1, 1, 1), (0, 2, 2, 2) (1, 0, 1, 2), (2, 0, 2, 1), (1, 1, 2, 0), (2, 1, 0, 2), (1, 2, 0, 1) en (2, 2, 1, 0). We zien dat alle woorden behalve (0, 0, 0, 0) gewicht 3 hebben. Dus hebben alle paren afstand 3. Deze code is dus een single-error-correcting code. Met de boven beschreven manier van decoderen zien we dit als volgt: twee verschillende vectoren met gewicht 1 hebben afstand 2 en liggen dus niet in dezelfde nevenklasse van V. Er zijn

8 zulke vectoren. Deze vormen samen met (0, 0, 0, 0) de 9 representanten van de nevenklasse van V. Ieder ontvangen signaal dat geen of één fout bevat wordt dan goed gedecodeerd. Zo'n code waarin alle woorden van gewicht $\leq$ m het representantensysteem vormen heet perfect (= close-packed).

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

4. Hamming codes

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

Het opsporen en verbeteren van één fout met deze code is bijzonder eenvoudig. Als de ontvangen vector $\underline{v}$ op de j-de plaats van de gezonden

vector afwijkt is nl. $\underline{v}H^T$ de binaire representatie van het getal j.

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

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

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

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

Een Hamming code over GF(q) wordt op analoge wijze geconstrueerd. Om er voor te zorgen dat H geen 2 kolommen bevat die lineair afhankelijk zijn, laten we alleen kolomvectoren toe waarvan het eerste symbool $\neq 0$ een 1 is. Als voorbeeld beschouwen we GF(3) en nemen

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

H is de parity-check matrix van een (13,10) code V. Dit is weer een single-error-correcting code. De code bestaat uit 3^{10} woorden. Als we elk van deze woorden als een kolom voorspellingen voor de voetbalpool insturen zijn we er zeker van de tweede prijs of de eerste te winnen. (Men moet dan wel $\pm$ *f* 18.000 inzetten!)

Probleem: Hamming codes zijn close-packed single-error-correcting. Voor $k \geq 2$ zijn bekend de volgende close-packed k-error-correcting codes:

a) de code over GF(2) die bestaat uit twee woorden t.w. (0, 0, ..., 0) en (1, 1, ..., 1) van 2n + 1 symbolen.

b) de door Golay ontdekte (23,12) code over GF(2) (zie [3]). Deze is 3-error-correcting.

c) de door Golay ontdekte (11,6) code over GF(3) (zie [1]; de opmerking in [3] is onjuist).

Bestaan er andere? (Enkele studenten in Eindhoven hebben aangetoond dat een perfecte k-error-correcting code met blocklengte n over GF(q) voor $q < 20$, $k \leq 5$, $n \leq 1000$ één van de bovengenoemde codes moet zijn!)

5. Reed-Muller codes

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

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

Voor $\nu = 0, 1, \ldots, 7$ is er in dit schema een vector die met ν nullen begint. De vectoren zijn dus lineair onafhankelijk. Merk op dat alle

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

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

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

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

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

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

6. Product codes (Slepian [5])

Als A een n × m-matrix is met elementen a_{ij} en B een r × s-matrix, dan verstaan we onder het Kronecker-product A × B de nr × ms-matrix van de vorm

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

Voorbeeld:

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

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

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

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

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

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

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

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

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

7. Hadamard codes

Zij H een Hadamard matrix van de orde n. We beschouwen de matrix

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

De rijen van deze matrix vormen de 2n woorden van een binaire code met woordlengte n en minimale afstand $\frac{1}{2}$ n. Dit volgt direct uit het feit dat 2 rijen van H op $\frac{1}{2}$ n plaatsen overeenkomen. Dit is i.h.a. niet een lineaire code. Nemen we voor H een symmetrische Hadamard matrix van de orde 8 in standaardvorm dan ontstaat een lineaire code met voortbrenger

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

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

8. Cyclische codes

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

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

Stelling 8.1. V is een cyclische code dan en slechts dan als V een ideaal in de ring R/S is.

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

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

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

$$\{x\}\{a_0 + \ldots + a_{n-1}x^{n-1}\} \in V \text{ d.w.z. } (a_{n-1}, a_0, \ldots, a_{n-2}) \in V.$$

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

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

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

Het polynoom $g(x) = 1 + x^2 + x^3$ is irreducibel over GF(2). We merken op dat volgens de gebruikelijke constructie het lichaam $GF(2^3)$ kan worden

voorgesteld door de elementen 0, 1, α, α^2, ..., α^6 waarin $1 + \alpha^2 + \alpha^3 = 0$, d.w.z. dat in $GF(2^3)$ het polynoom $g(x)$ is te ontbinden als $g(x) = 1 + x^2 + x^3 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$.
De vectorruimte R/S der polynomen over GF(2) mod $x^7 - 1$ is een 7-dimensionale ruimte over GF(2). Hierin vormen alle veelvouden van $g(x)$ een ideaal V, te weten de 4-dimensionale lineaire deelruimte van R/S opgespannen door

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

In de terminologie van §3 is de matrix

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

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

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

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

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

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

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

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

Een cyclische code kan ook gegeven worden door de nulpunten van g (in een geschikt lichaam) te noemen. Alle veeltermen van het ideaal zijn in die punten ook 0. Zo bestaat de in bovenstaand voorbeeld genoemde code uit alle $(a_0, \ldots, a_6)$ waarvoor $a_0 + a_1\alpha + a_2\alpha^2 + \ldots$ $\ldots + a_6\alpha^6 = 0$ waarin α primitief element van GF(8) is. Zoals boven reeds gezegd is kunnen we a_3 t/m a_6 als information symbols kiezen en dan is $a_0 + a_1\alpha + \ldots + a_6\alpha^6 = 0$ een vergelijking waaruit a_0, a_1 en a_2 zijn op te lossen. De kolommen van de parity-check matrix zijn de voorstellingen van $1, \alpha, \ldots, \alpha^6$ als vectoren over GF(2).

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

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

Stelling 8.2. In een (n,k) cyclische code V is geen enkele codevector een burst van de lengte $d \leq n - k$.

Bewijs. Zij g(x) de voortbrenger van het ideaal V. Dan is g(x) een polynoom van de graad n - k. Een burst van de lengte $d \leq n - k$ is op te vatten als restklasse $\{r(x)\}$ met $r(x) = x^a s(x)$ en s(x) een

polynoom van graad < n - k. Als $\{r(x)\} \in V$ is ook $\{s(x)\}$ een element van V en dit is niet mogelijk daar s(x) niet door g(x) deelbaar is.

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

9. BCH-codes

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

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

$$\alpha_0^{m_0}, \alpha_0^{m_0+1}, \ldots, \alpha_0^{m_0+d-2}$$

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

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

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

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

Als er een codewoord met gewicht < d was dan zouden er d - 1 kolommen van H zijn behorend bij $\alpha^{j_1}, \ldots, \alpha^{j_{d-1}}$ zó dat de uit deze

kolommen bestaande determinant 0 is. Schrijven we $\xi_i = \alpha^{j_i}$ dan betekent dit

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

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

Stelling 9.2. Is in (9.1) α primitief element van $GF(2^m)$, $m_0 = 1$ en $d = 2t + 1$ dan is de afstand van codewoorden tenminste d, d.w.z. de code is t-error-correcting.

Een parity-check matrix voor de code kunnen we nu als volgt beschrijven. We beginnen met $1, \alpha, \dots, \alpha^{n-1}$ als kolomvectoren van nullen en enen. Onder α^i komen de kolommen $\alpha^{3i}, \alpha^{5i}, \dots, \alpha^{(2t-1)i}$. We hebben dan een matrix H met mt rijen en $2^m - 1 = n$ kolommen. Voor een codevector $\underline{c} = (c_0, c_1, \dots, c_{n-1})$ betekent $\underline{c}H^T = \underline{0}$ hetzelfde als $c(\alpha) = c(\alpha^3) = \dots = c(\alpha^{2t-1}) = 0$ waarin $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$. We zien hieruit de grote kracht van de code. Van de $2^m - 1$ symbols zijn ten hoogste mt check symbols nodig om tenminste t fouten te kunnen verbeteren.

Nemen we als voorbeeld het binaire symmetrische kanaal van §2. Kiezen we m = 10 en t = 4 dan heeft de BCH code een transmissiesnelheid 0,96. We werken met woorden van de lengte 1023. De kans dat een woord onveranderd door het kanaal komt is slechts 36%. Door maximum-likelihood-decoding is de kans dat een gezonden woord verkeerd aankomt kleiner dan 0,4% (voor het kanaal is p = 0,001).

De methode van decoderen behandelen we nu aan de hand van een voorbeeld. We beschouwen de (15,7) double-error-correcting BCH code waarbij α primitief element van $GF(2^4)$ is en wel $\alpha^4 + \alpha + 1 = 0$. Als een signaal $\underline{s}$ ontvangen wordt vullen we dit in in de parity-check vergelijkingen.

Stel dat we vinden $\underline{s}\underline{H}^T = (1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)$. Nu is $\underline{s} = \underline{c} + \underline{e}$ waarin $\underline{c}$ het gezonden signaal en $\underline{e}$ foutenpatroon is. Daar $\underline{c}\underline{H}^T = \underline{0}$ moeten we om de fouten te verbeteren $\underline{e}$ bepalen uit $\underline{e}\underline{H}^T = (1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)$. Als er één fout gemaakt is op de plaats α^i dan is $\alpha^i = (1\ 1\ 1\ 1)$ d.w.z. $i = 12$, dus $\alpha^{3i} = \alpha^6 = (0\ 0\ 1\ 1) \neq (1\ 1\ 0\ 1)$. We zien dat er meer dan één fout is gemaakt. Neem aan dat er twee fouten zijn gemaakt op de plaats α^i en de plaats α^j. Dan moet

$$\alpha^i + \alpha^j = (1\ 1\ 1\ 1) = \alpha^{12},$$

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

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

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

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

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

10. Latijnse vierkanten, eindige meetkunde en error-correcting codes

We beschouwen weer het probleem van block-codes. We nemen als alfabet niet meer een lichaam maar de symbolen $1, 2, \ldots, n$. Een block code met lengte k was gedefinieerd als deelverzameling van de verzameling R_k van alle k-tallen $(a_1, a_2, \ldots, a_k)$ met $a_i \in \{1, 2, \ldots, n\}$ voor $i = 1, 2, \ldots, k$. De definitie van Hamming distance (zie §1) maakt van R_k een metrische ruimte. Als de verzameling bollen met middelpunt een codewoord en straal r de eigenschap heeft dat de bollen onderling disjunct zijn hebben we een r-error-correcting code. In het geval $k = 2$ is R_k op te vatten als schaakbord met $n \times n$ vierkanten, genummerd (1,1) t/m (n,n). De bol met straal 1 en middelpunt (x,y)

bestaat uit alle vierkanten (a,b) waarvoor x = a of y = b, d.i. de verzameling plaatsen die een op (x,y) geplaatste toren beheerst. Door Golomb en Posner ([2]) is hiervoor de naam "rook domain" ingevoerd. We noemen in het vervolg, ook voor k > 2, een bol met straal 1 in R_k een rook domain (en een bol met straal r een super-rook domain behorende bij torens van de macht r). Het probleem een aantal "torens" in R_k zó te plaatsen dat ieder punt van R_k door precies één toren beheerst wordt komt dus neer op het construeren van een perfect (= close packed) single-error-correcting code met $\{1, 2, \ldots, n\}$ als alfabet. In §3 en §4 hebben we voorbeelden van zulke codes gezien.

We bespreken nu een verband met Hoofdstuk I §5.

Stelling 10.1. Er is een 1-1 verband tussen de begrippen

a) latijns vierkant van de orde n,

b) n^2 torens in een n × n × n kubus, die elkaar niet aanvallen,

c) een uit n^2 woorden bestaande single-error-detecting code in R_3 over een alfabet met n letters.

Bewijs. Zij $A = (a_{ij})$ een latijns vierkant. De n^2 woorden (i, j, a_{ij}), $i, j = 1, 2, \ldots, n$, hebben dan volgens de definitie van latijns vierkant onderlinge afstand ≥ 2 en dus vormen ze een single-error-detecting code. Torens op de plaatsen (i, j, a_{ij}) vallen elkaar niet aan. Is verder (a_ν, b_ν, c_ν), $\nu = 1, 2, \ldots, n$, een single-error-detecting code met $\{1, 2, \ldots, n\}$ als alfabet dan zijn alle paren (a_ν, b_ν) verschillend. Definiëren we A door $a_{ij} = c_\nu$ als $i = a_\nu$ en $j = b_\nu$ dan is A een latijns vierkant van de orde n. De andere equivalenties zijn triviaal.

Ook voor orthogonale latijnse vierkanten kunnen we een verband met codes aangeven:

Stelling 10.2. De volgende begrippen zijn equivalent:

a) 2 orthogonale latijnse vierkanten van de orde n,

b) n^2 torens op een n × n × n × n kubus zó dat geen plaats door 2 verschillende torens wordt beheerst,

c) een uit n^2 woorden bestaande single-error-correcting code in R_4 over een alfabet $\{1, 2, \ldots, n\}$.

Bewijs. Als boven via de toevoeging:

$$A = (a_{ij}),\ B = (b_{ij}) \rightleftarrows (i, j, a_{ij}, b_{ij}),\ (i, j = 1, 2, \ldots, n).$$

Analoog zien we dat een uit n^2 woorden van de lengte $t + 2$ bestaande code met minimale afstand $t + 1$ equivalent is met t twee aan twee orthogonale latijnse vierkanten van de orde n. Volgens Hfdst. I stelling 5.2 is dan $t \leq n - 1$.

In Hfdst. I stelling 5.3 is bewezen dat voor $n = p^k \geq 3$, p priem, een affien vlak bestaat hetgeen equivalent is met de existentie van een volledig stelsel orthogonale latijnse vierkanten. De bijbehorende code noemen we affiene code. Dit brengen we nu ook in verband met Hamming codes en cyclische codes. We beperken ons tot $p = 2$ en construeren een affiene code:

Zij $q = 2^m$. Kies GF(q) als alfabet. Laat β een primitief element van $GF(q^2)$ zijn en $\alpha = \beta^{q-1}$. We merken op dat $\alpha^{q+1} = 1$ d.w.z. $n = q + 1$ is de orde van α. Verder is het minimaal polynoom van α over GF(q) een polynoom $g(x)$ van de graad 2 met $g(x) \mid x^{q+1} - 1$. De cyclische code V waarvan alle woorden $\underline{c}$ de eigenschap $c(\alpha) = 0$ hebben is een generalisatie van het idee van §4. Stel immers dat een codewoord $\neq \underline{0}$ gewicht < 3 had. Dit zou betekenen dat er getallen i en j zijn en $\lambda \in GF(q)$ zó dat

$$\alpha^i = \lambda\alpha^j,\ \text{d.w.z.}\ \beta^{(i-j)(q-1)} = (\beta^{q+1})^\nu$$

met $0 \leq \nu < q - 1$ (immers β^{q+1} is primitief element van GF(q)). Daar echter $(q - 1, q + 1) = 1$ en β primitief element van $GF(q^2)$ is kan dit niet. Dit betekent dat we met een single-error-correcting code te doen hebben. Deze code is weer perfect (nl. $q^{q-1}(1 + n(q - 1)) = q^{q+1}$). De duale code van V is een cyclische code V^* voortgebracht door $\frac{x^{q+1} - 1}{g(x)}$, dus een code van dimensie 2. Stel dat in V^* een woord was met 2 componenten 0. Neem een onafhankelijk woord erbij als basis van V^*.

Dan bevat het orthogonale complement van V^*, dat is V, een woord $\neq \underline{0}$ met gewicht ≤ 2. Dit is niet zo en dus hebben alle woorden $\neq \underline{0}$ van V^* een gewicht $\geq n - 1 = q$. We zien dat V^* een code is met q^2 woorden van de lengte $n = q + 1$ en minimale afstand q over een alfabet van q symbolen, d.i. een affiene code van de orde q.

Nu we dit verband tussen affiene codes en close-packed single-error-correcting codes gezien hebben verbaast het ons niet (gezien het feit dat Hfdst. I stelling 5.3 de enige bekende affiene vlakken beschrijft) dat er alléén voor $n = p^k$, p priem, close-packed single-error-correcting codes bekend zijn.

Eén geval kunnen we uitsluiten:

Stelling 10.3. (R.E. Block en M. Hall) Een close-packed single-error-correcting code met woorden van de lengte 7 over een alfabet van 6 letters bestaat niet.

Bewijs. Stel dat zo'n code bestaat. Deze bestaat dan uit 6^5 woorden met afstand ≥ 3. Dat heeft tot gevolg dat alle beginstukken van 5 letters precies één keer voorkomen. Bij een gegeven beginstuk van 3 letters zijn er dus precies 6^2 woorden met dit beginstuk. De eindstukken van 4 letters van deze woorden hebben afstand ≥ 3. Ze vormen dus zelf een single-error-correcting code bestaande uit 6^2 woorden van de lengte 4 over een alfabet van 6 letters. Volgens stelling 10.2 bestaan er dan 2 orthogonale latijnse vierkanten van de orde 6. Dit is niet zo.

We beschouwen nu nog een geheel ander combinatorisch probleem waarvan zal blijken dat het verband heeft met het voorafgaande. Beschouw een $n \times n \times \ldots \times n$ hyperkubus (verdeeld in n^k cellen) in R_k en kleur de cellen met w verschillende kleuren zó dat ieder rook-domain elke kleur tenminste éénmaal bevat. Probeer w te maximaliseren. Dit maximum noemen we w(k,n). Men noemt dit een error-distributing code. Om deze naam te begrijpen formuleren we het probleem als volgt. Beschouw R_k als de verzameling woorden van k letters uit een alfabet van n letters. Aan een aantal objecten $O_1, O_2, \ldots, O_w$ voegen we codewoorden toe, even-

tueel meerdere codewoorden per object. We eisen dat voor ieder codewoord $\underline{c}$ behorend bij O_i en iedere O_j een codewoord voor O_j bestaat met afstand 1 tot $\underline{c}$.

Ook hier gaat het er om w zo groot mogelijk te maken. (Delbrück vermoedde in 1957 dat dit idee in de natuur werd gebruikt. Er zijn 20 aminozuren. Hiervoor is een codering met een 4-letter alfabet. Er is maximale mutatie-vrijheid als door één verwisseling elk aminozuur in elk ander aminozuur kan worden overgevoerd. Dit kan als $w(3,4) = 20$ maar helaas is $w(3,4) = 8$.)

Men ziet onmiddellijk dat $w(k,n) \leq 1 + k(n - 1)$. In geval van gelijkheid spreken we van een close-packed error distributing code.

Stelling 10.4. Een close packed error-distributing code met parameters k, n bestaat dan en slechts dan als een close-packed single-error-correcting code bestaat met dezelfde parameters.

Bewijs. a) Zij $V \subset R_k$ een perfect single-error-correcting code (V is niet noodzakelijk lineair!). Aan ieder woord $\underline{c}$ van gewicht ≤ 1 voegen we een kleur toe en kennen dan deze kleur toe aan de punten van $V + \underline{c}$ (mod n). We hebben $1 + k(n - 1)$ kleuren nodig. De verzamelingen $V + \underline{c}$ zijn disjunct en vullen R_k op. De kleuring voldoet aan de gestelde eisen.

b) Is omgekeerd een close-packed error-distributing code gegeven dan is de afstand van twee woorden van dezelfde kleur ≥ 3. Het aantal woorden van één kleur is $n^k/(1 + k(n - 1))$. Dus vormen de woorden van één kleur een perfect single-error-correcting code.

Uit vorige stellingen zien we dat $w(n + 1, n) = n^2$ als $n = p^k$, p priem en $w(7,6) < 36$.

Vermoeden: $w(k,n) \leq (k - 1)n$.

Het is eenvoudig voorbeelden aan te geven waaruit blijkt dat $w(3,n) \geq 2n$ als n even en $w(3,n) \geq 2n - 1$ als n oneven. We bewijzen nu de

Stelling 10.5. $w(3,n) = \begin{cases} 2n & \text{als n even,} \\ 2n - 1 & \text{als n oneven.} \end{cases}$

Bewijs. Beschouw een $n \times n \times n$ kubus zó gekleurd dat ieder rook-domain elke gebruikte kleur tenminste éénmaal bevat. Neem een vaste kleur. Zij a_{ij} het aantal cellen (i, j, z) met deze kleur. In de matrix $A = (a_{ij})$ zoeken we onder de rijen en kolommen die met de kleinste som. Laat dit de eerste rij zijn en r de som. Als $a_{1j} \neq 0$ dan is $\sum_{i=1}^{n} a_{ij} \geq r$. Als $a_{1j} = 0$ is $\sum_{i=1}^{n} a_{ij} \geq n - r$ op grond van de definitie van a_{ij} en de eigenschap van de kleuring. Dus is

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} \geq r^2 + (n - r)^2.$$

Het rechterlid is minimaal $\frac{n^2}{2}$ als n even en minimaal $\frac{n^2 + 1}{2}$ als n oneven is. We weten nu hoe vaak iedere kleur tenminste moet voorkomen. Het aantal cellen is n^3. Het gestelde volgt door deling.

Om het boven genoemde vermoeden te bewijzen moet deze redenering gegeneraliseerd worden. Dit is tot nu toe niet gelukt.

Hoofdstuk III. Een combinatorisch probleem voor eindige abelse groepen

1. Inleiding; het hoofdvermoeden

Zij G een willekeurige verzameling. Een G-rij is een eindige rij

$$S = (g_1, g_2, \ldots, g_n) \tag{1}$$

van elementen van G (waarbij herhalingen zijn toegestaan); n heet de lengte van S. Lengte 0 wordt toegekend aan de lege rij $\emptyset$.

Een deelrij S_1 van S - notatie: $S_1 \leq S$ - is een G-rij

$$S_1 = (g_{i_1}, g_{i_2}, \ldots, g_{i_h})$$

met $1 \leq i_1 \leq i_2 \leq \ldots < i_h \leq n$. Als ook $S_2 \leq S$,

$$S_2 = (g_{j_1}, g_{j_2}, \ldots, g_{j_k})$$

en als $\{i_1, i_2, \ldots, i_h\} \cup \{j_1, j_2, \ldots, j_k\} = \{u_1, u_2, \ldots, u_r\}$ met $u_1 < u_2 < \ldots < u_r$, dan heet

$$S_1 \vee S_2 = (g_{u_1}, g_{u_2}, \ldots, g_{u_r})$$

de vereniging van S_1 en S_2; de doorsnede van S_1 en S_2 is de deelrij

$$S_1 \wedge S_2 = (g_{v_1}, g_{v_2}, \ldots, g_{v_s})$$

behorende bij de doorsnede $\{v_1, v_2, \ldots, v_s\} = \{i_1, i_2, \ldots, i_h\} \cap \{j_1, j_2, \ldots, j_k\}$ der indexverzamelingen. Indien $S_1 \wedge S_2 = \emptyset$, dan heten S_1 en S_2 disjuncte deelrijen van S.

Wij nemen nu aan dat G een eindige additieve abelse groep is; de orde van G geven we aan met $\omega(G)$. De waarde van de rij (1) is dan

$$|S| = g_1 + \ldots + g_n;$$

de waarde van de lege rij is 0 (het nul element van G). Een rij $S \neq \emptyset$ met $|S| = 0$ heet een nulrij. Voorts zij

$$[S] = \{|T| : \emptyset\ T \leq S\}$$

en

$$[S]^* = \{|T| : T \leq S\} = [S] \cup \{0\}.$$

Een G-rij S heet primitief als $0 \notin [S]$ en maximaal als S primitief is, terwijl $S \leq T$, T primitief, impliceert $S = T$. Ons hoofdprobleem is:

HOE LANG KUNNEN PRIMITIEVE RIJEN ZIJN?

Anders gezegd, als we definieren

$$\mu(G) = \sup \{n \in \mathbb{N} : \exists \text{ primitieve G-rij ter lengte } n\}$$

dan is ons doel μG te bepalen.
We kunnen μG ook als volgt beschrijven:

$$\mu(G) = \sup \{n \in \mathbb{N} : (\exists g_1, \ldots, g_n \in G)(\forall \varepsilon_1, \ldots, \varepsilon_n \in \{0,1\})$$
$$(\varepsilon_1 g_1 + \ldots \cdot \varepsilon_n g_n = 0 \Rightarrow \varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_n = 0)\}.$$

De tweede formulering laat zien dat μG een zekere analogie bezit met het begrip (lineaire) dimensie; als G een vectorruimte is over het lichaam $\mathbb{Z}_2 = \{0,1\}$, dan is μG inderdaad de dimensie van G:

$$\mu(\underbrace{C_2 \times C_2 \times \ldots \times C_2}_{k\times}) = k.$$

Naast μG introduceren we een tweede constante λG, als volgt. Iedere eindige abelse groep is isomorph met een direct product van cyclische groepen

$$G \simeq C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k} \tag{2}$$

("hoofdstelling van de abelse groepen"); i.h.a. is deze ontbinding niet ondubbelzinnig (denk bv. aan $C_6 \simeq C_2 \times C_3$), maar als we ook nog eisen dat

$$n_i \mid n_{i+1} \quad (i = 1, 2, \ldots, k-1) \tag{3}$$

dan zijn de ordes n_i ondubbelzinnig bepaald (afgezien van de triviale mogelijkheid dat een onbepaald aantal beginordes $n_1 = n_2 \ldots = n_h = 1$).

We definieren nu, als G voldoet aan (2) met (3):

$$\lambda(G) = \sum_{i=1}^{k} (n_i - 1)$$

(merk op dat de waarde λG niet wordt beïnvloed door een aantal (triviale) sommanden C_1 vóóraan in de ontbinding (2)).

Als G voldoet aan (2) met (3) en als bovendien $n_1 \neq 1$, dan heet k de dimensie van G, k = dim G.

Wij hebben gezien dat $\mu G = \lambda G$ voor elke groep G die isomorph is met een direct product van factoren C_2. Dit is geen toeval. Wij vermoeden zelfs dat het regel is.

HOOFDVERMOEDEN: $\mu G = \lambda G$ voor iedere eindige abelse groep G.
In dit hoofdstuk zullen we de juistheid van dit hoofdvermoeden aantonen voor alle groepen G die behoren tot één van de navolgende typen.

I. G is een p-groep (d.w.z. ieder element van G heeft een orde die macht is van een vast priemgetal p).

II. dim $G \leq 2$.

III. $G \simeq H \times C_{p^n m}$ met H een p-groep, p priem, en $p^n > \lambda H$.

IV. $G \simeq C_{2p^{n_1}} \times C_{2p^{n_2}} \times C_{2p^{n_3}}$.

V. $G \simeq C_2 \times C_{2nm_1} \times C_{2nm_2}$, met $n = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4}$ en óf $m_1 = 1$, m_2 willekeurig, óf $m_1 = p^r$, $m_2 = p^s$, p priem.

Naast deze series zijn er nog enkele groepen bekend waarvoor het hoofdvermoeden waar is, waaronder (zie [2])

$$G \simeq C_2 \times C_2 \times C_2 \times C_6.$$

Tegenvoorbeelden zijn niet bekend. De enige groepen met orde ≤ 100 waarvoor μG nog niet bepaald is, zijn (op isomorphie na)

$$G = C_3 \times C_3 \times C_6 \; ; \quad \omega G = 54 \; ; \quad \lambda G = 9,$$

en

$$G = C_2 \times C_2 \times C_2 \times C_2 \times C_6; \; \omega G = 96; \; \lambda G = 9.$$

Wat betreft groepen van het type $C_n \times C_n$ dient nog het volgende te worden opgemerkt. Nadat enkele medewerkers van het Mathematisch Centrum zich reeds enige tijd hadden bezig gehouden met het hoofdvermoeden (geformuleerd door P.C. BAAYEN in 1965) werden wij er op attent gemaakt dat voor het speciale geval $G \simeq C_p \times C_p$ reeds eerder door P. ERDÖS was vermoed dat $\mu G = 2(p - 1)$. In 1961 bewezen P. ERDÖS, A. GINZBURG en A. ZIV [11] het volgende:

Indien $G \simeq C_n \times C_n$, H een cyclische ondergroep is van G van de orde n, en S een primitieve rij waarvan alle elementen liggen in één nevenklasse van H, dan is de lengte van S ten hoogste $G = 2(n - 1)$.

Ditzelfde resultaat was onafhankelijk verkregen door N.G. DE BRUIJN, het is een zeer bijzonder geval van stelling 8 hieronder. Niet bevat in onze resultaten is de volgende stelling die H.B. MANN en J.E. OLSON [15] in 1967 publiceerden:

Indien $G \simeq C_p \times C_p$ en S is een primitieve G-rij waarvan alle elementen onderling verschillend zijn, dan is de lengte van S ten hoogste $\lambda G - 1 = 2p - 3$.

Verdere verwante resultaten kan men aantreffen in H.B. MANN [14].

We zullen de klasse van alle groepen waarvoor het hoofdvermoeden correct is aangeven met $\mathcal{A}$; dus

$$G \in \mathcal{A} \Longleftrightarrow \mu G = \lambda G.$$

Een aantal deelklassen $\mathcal{B}, \mathcal{C}, \mathcal{D}$ van $\mathcal{A}$, zullen later worden ingevoerd, al naar gelang ze nodig zijn.

De meeste bewijzen van dit hoofdstuk zijn afkomstig van D. KRUYSWIJK en P. VAN EMDE BOAS, met bijdragen van J.H. VAN LINT en P.C. BAAYEN. Slechts in enkele gevallen zullen we expliciet de (eerste) auteur(s) van de betreffende resultaten vermelden.

2. Elementaire resultaten

Stelling 2.1. $\mu G < \omega G$.

Bewijs. Zij $n = \omega G$ en zij $S = (g_1, \ldots, g_n)$ een G-rij. Onder de $n + 1$ elementen $0, g_1, g_1 + g_2, \ldots, g_1 + g_2 \ldots + g_n$ zijn er zeker twee gelijk; hun verschil is 0 en behoort tot $[S]$. Dus S is niet primitief.

Het is triviaal dat $\lambda G = \omega G - 1$ dan en slechts dan als G cyclisch is. Minder voor de hand liggend is

Stelling 2.2. $\mu G = \omega G - 1 \iff$ G cyclisch.

Bewijs. a) Stel G cyclisch, van de orde n, met voortbrengende a. Daar $S = \underbrace{(a, a, \ldots, a)}_{(n-1)\times}$ een primitieve G-rij is, is $\mu G \geq \omega G - 1$, dus (stelling 2.1) $\mu G = \omega G - 1$.

b) Stel $\mu G = \omega G - 1$, en zij $S = (g_1, \ldots, g_{n-1})$ een primitieve G-rij (waar $n = \omega G$). Als m_i het aantal elementen van $[(g_1, \ldots, g_i)]$ is, dan is steeds $m_{i+1} \geq m_i + 1$, want als $[(g_1, \ldots, g_i)] = \{a_1, \ldots, a_{m_i}\}$ dan $[(g_1, \ldots, g_{i+1})] \supset \{g_{i+1}, a_1+g_{i+1}, \ldots, a_{m_i}+g_{i+1}\}$. Dus $m_{n-1} \geq m_2+n-3$. Stel nu dat in S twee verschillende elementen kunnen voorkomen; zonder beperking der algemeenheid zij dan $g_1 \neq g_2$. Dan is $m_2 = 3$ (g_1, g_2 en g_1+g_2 zijn onderling verschillend), dus $m_{n-1} \geq n$, dus $0 \in G \subset [S]$, in strijd met de primitiviteit van S. We concluderen dat $S = (a, a, \ldots, a)$; dan is $\omega(a) = \omega(G)$, dus G is cyclisch. $\underbrace{}_{(n-1)\times}$

Gevolg. $C_n \in \mathcal{A}$ voor iedere n.

Stelling 2.3. $\mu G + \mu H \leq \mu(G \times H) < (\mu G + 1)(\mu H + 1)$.

Bewijs. a) Zij $\mu G = n$ en $\mu H = m$. Als $S = (g_1, \ldots, g_n)$ een primitieve G-rij is, en $T = (h_1, \ldots, h_m)$ een primitieve H-rij, dan is

$$\left(\begin{pmatrix} g_1 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} g_n \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ h_1 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ h_m \end{pmatrix}\right)$$

een primitieve $G \times H$-rij ter lengte $m + n$. Dus $\mu(G \times H) \geq m + n$.
b) Er is een exacte rij $0 \to H \xrightarrow{\iota} G \times H \xrightarrow{\pi} G \to 0$. Zij ditmaal $n = \mu G + 1$ en $m = \mu H + 1$ en zij S een $G \times H$-rij ter lengte nm. Daar iedere deelrij van πS met lengte n in G een nulrij bevat is S een disjuncte vereniging $S_1 \vee \ldots \vee S_m \vee R$ met $S_i \neq \emptyset$ en $\pi|S_i| = |\pi S_i| = 0$ $(1 \leq i \leq m)$. Laat $a_i \in H$ zodat $\iota a_i = |S_i|$, voor $1 \leq i \leq m$; de H-rij $(a_1, \ldots, a_m)$ bevat een nulrij $(a_{i_1}, \ldots, a_{i_k})$. Dan is $S_{i_1} \vee \ldots \vee S_{i_k} \leq S$ een nulrij in $G \times H$; dus S is niet primitief.

Opmerking. We zien dat de bovenschatting $\mu K < (\mu G + 1)(\mu H + 1)$ reeds geldt als er maar een exacte rij $0 \to H \to K \to G \to 0$ bestaat, dus niet alleen als K het directe product is van G en H. In verband met stelling 2.1 is deze schatting overigens alleen zinvol indien $\mu G < \omega G - 1$ of $\mu H < \omega H - 1$. Dat deze bovenschatting in zijn algemeenheid niet verbeterd kan worden kan men verifiëren aan $K = C_2 \times C_3$.

Gevolg. $\mu G \geq \lambda G$.

Bewijs. Als $G \simeq C_{n_1} \times \ldots \times C_{n_k}$ met $n_i | n_{i+1}$ dan is volgens stelling 2.3 (en stelling 2.2)

$$\mu G \geq \sum_{i=1}^{k} \mu C_{n_i} = \sum_{i=1}^{k} (n_i - 1) = \lambda G.$$

Opmerking. Om te bewijzen dat het hoofdvermoeden geldt voor G behoeft men dus slechts aan te tonen dat $\mu G \leq \lambda G$, dus dat een G-rij ter lengte $\lambda G + 1$ nooit primitief is.

Stelling 2.4. Een G-rij is dan en slechts dan maximaal als $[S] = G \setminus \{0\}$. In dat geval is $[S]^* = G$.

Bewijs. a) S maximaal $\Rightarrow$ S primitief $\Rightarrow$ $[S] \subset G \setminus \{0\}$. Als $[S] \neq G \setminus \{0\}$ en $g \in G \setminus [S]^*$, dan is S een echte deelrij van de primitieve rij $T = S \vee (-g)$, in strijd met de maximaliteit van S.
b) Als $[S] = G \setminus \{0\}$ dan is S kennelijk maximaal.

3. p-Groepen

Het hoofdvermoeden $\mu G = \lambda G$ werd eind 1967 door verschillende onderzoekers, onafhankelijk van elkaar, voor p-groepen bewezen.
Het hier weergegeven bewijs is van D. KRUYSWIJK (persoonlijke communicatie); ook J.E. OLSON [16] deelt mee μG voor p-groepen bepaald te hebben.

Voor p-groepen van de vorm

$$G \simeq C_{p^{n_1}} \times \ldots \times C_{p^{n_k}} \tag{1}$$

met $n_1 = n_2 = \ldots = n_k = 1$ - suggereerde H. DAVENPORT naderhand een fraai kort bewijs dat berust op de volgende welbekende stelling van C. CHEVALLEY ([6]; zie bv. ook [5] en [7]):

" Als $f_1, \ldots, f_m \in GF(p^k)[x_1, \ldots, x_n]$, als $f_i(0, 0, \ldots, 0) = 0$ $(1 \leq i \leq m)$ en als $\sum_{i=1}^{m}$ graad $(f_i) < n$, dan heeft het stelsel vergelijkingen

$$f_i(x_1, x_2, \ldots, x_n) = 0 \ , \quad 1 \leq i \leq m$$

een niet-triviale (i.e. van de nuloplossing verschillende) oplossing".

Zij nu $G = C_p \times C_p \times \ldots \times C_p$ (m factoren) en zij $S = (a_1, \ldots, a_n)$ een G-rij, met

$$a_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ . \\ . \\ . \\ a_{mi} \end{bmatrix} \qquad (1 \leq i \leq n;\ a_{ji} \in C_p).$$

Als nu $n > \lambda G = m(p - 1)$ dan heeft volgens de stelling van CHEVALLEY het stelsel vergelijkingen

$$\begin{aligned} a_{11}x_1^{p-1} + a_{12}x_2^{p-1} + \ldots + a_{1n}x_n^{p-1} &= 0 \\ &\vdots \\ a_{m1}x_1^{p-1} + a_{m2}x_2^{p-1} + \ldots + a_{mn}x_n^{p-1} &= 0 \end{aligned}$$

een oplossing $(e_1, e_2, \ldots, e_n) \neq (0, 0, \ldots, 0)$. Zij $\varepsilon_i = e_i^{p-1}$; daar de multiplicatieve groep van een eindig lichaam cyclisch is zal $\varepsilon_i \in \{0,1\}$ $(1 \leq i \leq n)$, terwijl ook

$$a_1\varepsilon_1 + a_2\varepsilon_2 + \ldots + a_n\varepsilon_n = 0;$$

dus S is niet primitief, $\mu G \leq \lambda G$ en derhalve (cf. Gevolg van stelling 2.3) $\mu G = \lambda G$.

Het bewijs van de algemenere stelling 3.1 is onafhankelijk van dit deelresultaat; we reproduceerden hier DAVENPORT's bewijs om zijn kortheid en elegance.

In het bewijs van stelling 3.1 willen we gebruik maken van de groepsalgebra van G over $\mathbf{Z}_p$; daartoe hebben we een multiplicatieve copie van G nodig. Zij G gegeven door (1) en zij $\overline{C}_{p^{n_i}}$ een <u>multiplicatieve</u> cyclische groep van de orde p^{n_i}, met voortbrengende a_i $(1 \leq i \leq k)$. Als $\overline{G} = \overline{C}_{p^{n_i}} \times \ldots \times C_{p^{n_k}}$, dan wordt een isomorphisme van G op $\overline{G}$ gedefinieerd door aan

$$g = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in G \quad \text{toe te voegen}$$

$$A^g = a_1^{g_1} \cdot a_2^{g_2} \cdot \ldots \cdot a_k^{g_k}.$$

We definieren verder een epimorphisme ϕ van de polynoomring $\mathbf{Z}_p[x_1, \ldots, x_k]$ op de groepsalgebra $\mathbf{Z}_p(\overline{G})$ door

$$\phi X^g = A^g$$

waar

$$X^g = x_1^{g_1} \cdot x_2^{g_2} \cdot \ldots \cdot x_k^{g_k}.$$

Aangezien $(1 - X^g)\ (1, 1, \ldots, 1) = 0$ moeten er voor iedere $g \in G$ polynomen $P_{g,i} \in \mathbb{Z}_p[x_1, \ldots, x_k]$ bestaan zodanig dat

$$1 - X^g = P_{g,1} \cdot (1 - x_1) + P_{g,2} \cdot (1 - x_2) + \ldots$$

$$\ldots + P_{g,k} \cdot (1 - x_k).$$

Tenslotte merken we op dat $(1 - x)^{p^n} = 1 - x^{p^n}$ en $(1 - x)^{p^n-1} =$

$= 1 + x + \ldots + x^{p^n-1}$ in $\mathbb{Z}_p[x]$, terwijl uit de laatste betrekking door differentiatie nog volgt dat $(1 - x)^{p^n-2} = 1 + 2x + \ldots + (p^n-1)x^{p^n-2}$.
Daarom geldt voor willekeurige $a \in \mathbb{Z}_p(\overline{G})$:

$$(2) \qquad (1 - a)^{p^n} = 1 - a^{p^n}\ ;\ (1 - a)^{p^n-1} = \sum_{v=0}^{p^n-1} a^v\ ;\ (1-a)^{p^n-2} = \sum_{v=0}^{p^n-1} v.a^{v-1}$$

Na deze voorbereidingen bewijzen we

<u>Stelling 3.1</u>. G p-groep $\Rightarrow \mu G = \lambda G$.

Bewijs. Zij $\lambda = \lambda G$, waar G gegeven is door (1), en zij $S = (g^{(1)}, \ldots$
$\ldots, g^{(\lambda)})$ een G-rij.
Wij berekenen op twee manieren $\prod_{j=1}^{\lambda} (1 - A^{g^{(j)}})$. Directe ontwikkeling geeft

$$(3) \qquad \prod_{j=1}^{\lambda} (1 - A^{g^{(j)}}) = \sum_{g \in G} \mu(S,g) A^g,$$

waar

$$\mu(S,g) = N_{even} - N_{oneven} \text{ (berekend in } \mathbb{Z}_p)$$

met

$$N_{(on)even} = \text{aantal}\,\{(\varepsilon_1, \ldots, \varepsilon_\lambda) \in \{0,1\}^\lambda : \sum_{i=1}^{\lambda} \varepsilon_i g_i = g$$

$$\& \sum_{i=1}^{\lambda} \varepsilon_i \ (on)even\}.$$

Anderzijds is

$$\prod_{j=1}^{\lambda} (1 - X^{g^{(j)}}) = \prod_{j=1}^{\lambda} \sum_{i=1}^{k} P_{g^{(j)},i} \cdot (1 - x_i) = \sum_{i=1}^{k} Q_i \cdot (1 - x_i)^{p^{n_i}} +$$

$$+ c \prod_{i=1}^{k} (1 - x_i)^{p^{n_i - 1}}$$

(voor zekere $Q_i \in \mathbb{Z}_p[x_1, \ldots, x_k]$ en $c \in \mathbb{Z}_p$), waaruit door toepassing van ϕ volgt:

$$(4) \quad \prod_{j=1}^{\lambda} (1 - A^{g^{(j)}}) = \sum_{i=1}^{k} \phi(Q_i) \cdot 0 + c \prod_{i=1}^{k} \sum_{\nu=0}^{p^{n_i}-1} a_i^{\nu} = c \sum_{g \in G} A^g.$$

Daar $\{A : g \in G\}$ een basis is voor de vectorruimte $\mathbb{Z}_p(\overline{G})$ over $\mathbb{Z}_p$ volgt uit (3) en (4) dat

$$\mu(S,g) = c \quad \text{voor alle} \quad g \in G.$$

Neem nu aan dat S primitief is. Dan is $\mu(S,0) = 1$, dus $\mu(S,g) = 1$ voor iedere $g \in G$, en voor zo'n g zijn er dus $\varepsilon_i \in \{0,1\}$ met $\sum_{i=1}^{k} \varepsilon_i g_i = g$; als $g \neq 0$ moet $\sum_{i=1}^{k} \varepsilon_i \neq 0$, zodat $g \in [S]$. Dus $G \setminus \{0\} \subset [S]$, oftewel S is maximaal (stelling 2.4). Hiermee is het bewijs voltooid.

Dezelfde techniek is door P. VAN EMDE BOAS toegepast om een resultaat af te leiden dat belangrijk blijkt bij groepen van het type $C_{2n_1} \times C_{2n_2} \times C_{2n_3}$.

Voor een primitieve rij S ter lengte μG geldt altijd: $[S]^* = G$ (stelling 2.4). Men kan zich afvragen hoe $[S]^*$ er uit ziet voor een primitieve rij S ter lengte $\mu G - 1$. Mijn vermoeden is dat voor zo'n S altijd het volgende geldt: er is een ondergroep N van G en een

$a \in G \setminus N$ zodat $G \setminus [S]^* \subset a + N$.

Laten we een deelverzameling K van G een <u>echte nevenklasse</u> noemen indien $K = a + N$ voor een ondergroep N van G en een $a \notin N$. Dan definieren we:

<u>Definitie</u>. $\mathcal{C}$ zij de klasse van alle eindige abelse groepen G met de volgende eigenschap: voor iedere primitieve G-rij S ter lengte $\lambda G - 1$ is er een echte nevenklasse K in G zodanig dat

$$G \setminus [S]^* \subset K.$$

Opmerking. Het is eenvoudig in te zien dat $\mathcal{C} \subset \mathcal{A}$.

<u>Stelling 3.2</u>. G p-groep $\Rightarrow G \in \mathcal{C}$.

Bewijs. We gebruiken dezelfde notatie als in het bewijs van stelling 3.1 maar nu met S van lengte $\lambda - 1$. Nog steeds geldt (3), maar ditmaal is

$$\prod_{j=1}^{\lambda-1} (1 - X^{g^{(j)}}) = \prod_{j=1}^{\lambda-1} \sum_{i=1}^{k} P_{g^{(j)},i} \cdot (1 - x_i) =$$

$$= \sum_{i=1}^{k} Q_i \cdot (1 - x_i)^{p^{n_i}} + c_0 \prod_{i=1}^{k} (1 - x_i)^{p^{n_i}-1} +$$

$$+ \sum_{i=1}^{k} c_i \prod_{l=1}^{k} (1 - x_i)^{p^{n_i-1-\delta_{il}}},$$

met $Q_i \in \mathbb{Z}_p[x_1, \ldots, x_k]$, $c_i \in \mathbb{Z}_p$, en $\delta_{il} = 0$ als $i \neq l$, $\delta_{ii} = 1$. Via het homomorphisme ϕ en de identiteiten (2) volgt dat

$$\prod_{j=1}^{\lambda-1} (1 - A^{g^{(j)}}) =$$

$$0 + c_0 \prod_{i=1}^{k} \sum_{\nu=1}^{p^{n_i}-1} a_i^{\nu} + \sum_{i=1}^{k} \{ c_i \sum_{\nu=1}^{p^{n_i}-1} \nu a_i^{\nu-1} \cdot \prod_{\substack{l=1 \\ l \neq i}}^{k} \sum_{\sigma=0}^{p^{n_l}-1} a_i^{\sigma} \} =$$

$$= \sum_{g \in G} (c_0 + c_1(g_1 + 1) + \ldots + c_k(g_k + 1))A^g.$$

Dus

$$\mu(S,g) = c_0 + \sum_{i=1}^{k} c_i(g_i + 1) = \sum_{i=1}^{k} c_i g_i - \sum_{i=0}^{k} c_i.$$

Stel nu S primitief. Dan $\mu(S,0) = 1$, dus $\sum_{i=0}^{k} c_i = 1$. Als nu $g \in G \setminus [S]^*$, dan is $\mu(S,g) = 0$ en dus

$$\sum_{i=1}^{k} c_i g_i = -1$$

welke vergelijking een echte nevenklasse K in G definieert, tenzij $c_1 = c_2 = \ldots = c_k = 0$. Maar dan is S maximaal; neem dan $K = \{g\}$ met (willekeurig gekozen) $g \neq 0$ (dit is een echte nevenklasse van de ondergroep $\{0\}$).

4. Een inductie-methode

Lemma 4.1. Als $G \times H \in \mathcal{A}$ en $\lambda(G \times H) \leq \lambda G + \mu H$, dan $G \in \mathcal{A}$. Is bovendien H cyclisch, dan bevat iedere G-rij $(g_1, \ldots, g_L)$ met $L \geq \lambda G + \lambda H + 1$ een nulrij waarvan de lengte deelbaar is door $\omega H = \lambda H + 1$.

Bewijs. a) Uit $\mu G + \mu H \leq \mu(G \times H) = \lambda(G \times H) \leq \lambda G + \mu H$ volgt $\mu G \leq \lambda G$, dus (Stelling 2.3, Gevolg) $\mu G = \lambda G$.

b) Stel H is cyclisch, met voortbrengende a; dan is $\mu H = \lambda H$. Zij $L \geq \lambda G + \lambda H + 1 \leq \mu(G \times H) + 1$, en zij $S = (g_1, \ldots, g_L)$ een G-rij. De rij

$$\left(\begin{pmatrix} g_1 \\ a \end{pmatrix}, \begin{pmatrix} g_2 \\ a \end{pmatrix}, \ldots, \begin{pmatrix} g_L \\ a \end{pmatrix} \right)$$

bevat een nulrij, zeg ter lengte N. Dan is $Na = 0$, dus N is een veelvoud van ωH.

Definitie. Zij $\mathcal{B}$ de klasse van alle $G \in \mathcal{A}$ die bovendien de volgende eigenschap bezitten: als $G \simeq C_{n_1} \times \ldots \times C_{n_k}$ met $n_i | n_{i+1}$ $(1 \leq i \leq k-1)$, dan bevat iedere G-rij S ter lengte $\lambda G + n_k$ een nulrij met lengte $\leq n_k$.

Opmerking 4.1. Als $G \simeq C_{n_1} \times \ldots \times C_{n_k} \in \mathcal{B}$ $(n_i | n_{i+1})$ dan bevat iedere G-rij S met lengte $\geq \lambda G + m \cdot n_k$ tenminste m onderling disjuncte nulsubrijen met lengte $\leq n_k$.

Opmerking 4.2. $C_n \in \mathcal{B}$, voor iedere n.

Lemma 4.2. Stel $\lambda(G \times H) = \lambda G + \lambda H$, $\lambda G \leq \lambda H$, en zij H cyclisch.
Dan $G \times H \times H \in \mathcal{A} \Rightarrow G \times H \in \mathcal{B}$.

Bewijs. Als $G = C_{n_1} \times \ldots \times C_{n_k}$ $(n_i | n_{i+1})$ en $H = C_n$, dan $n_k | n$. Uit lemma 4.1 volgt $G \times H \times H \in \mathcal{A} \Rightarrow G \times H \in \mathcal{A}$. Zij nu S een $G \times H$-rij ter lengte $L = \lambda(G \times H) + n = \lambda(G \times H) + \lambda H + 1$. Volgens lemma 4.1 is er een $\emptyset \neq T \leq S$ met $|T| = 0$ en lengte (T) deelbaar door n. We moeten bewijzen dat S een nulrij bevat met lengte $\leq n$, en hebben die gevonden in T tenzij lengte (T) = 2n. Maar dan is $T = T_1 \vee T_2$ met $T_1 \wedge T_2 = \emptyset$, $T_1 \neq \emptyset$, $T_2 \neq \emptyset$ en $|T_1| = |T_2| = 0$, omdat $2n > \lambda(G \times H) + 1$.
Tenminste één der T_i heeft een lengte $\leq n$.

Gevolg. Iedere p-groep G van de vorm $G \simeq H_1 \times H_2$ met H_2 cyclisch en $\lambda H_2 \geq \lambda H_1$ behoort tot $\mathcal{B}$.

Stelling 4.1. Als $N = C_{n_1} \times \ldots \times C_{n_k} \in \mathcal{B}$ en $M = C_{m_1} \times \ldots \times C_{m_k} \in \mathcal{B}$ $(n_i | n_{i+1}, m_i | m_{i+1})$, en als $n_i = n_k$ voor iedere i waarvoor $m_i > 1$, dan ook $G = C_{n_1 m_1} \times \ldots \times C_{n_k m_k} \in \mathcal{B}$.

Bewijs. Er is een exacte rij $0 \to M \xrightarrow{\iota} G \xrightarrow{\pi} N \to 0$. Zij $S = (g_1, \ldots, g_L)$ een G-rij ter lengte $L = \lambda G + n_k m_k$, Beschouw de N-rij $\pi S = (\pi g_1, \ldots, \pi g_L)$ Daar

$$L = n_1 + \ldots + n_{k-1} - k + 2n_k m_k + (m_1 - 1)n_1 + \ldots + (m_{k-1} - 1)n_{k-1} \geq$$

$$\geq (n_1 + \ldots + n_{k-1} - k) + n_k(m_1 + \ldots + m_{k-1} + 2m_k - k + 1)$$

en $N \in \mathcal{B}$, moet S een disjuncte vereniging $S_1 \vee S_2 \vee \ldots \vee S_r$ bevatten met $0 \neq$ lengte $(S_i) \leq n_k$ en $|\pi S_i| = 0$, waar $r = m_1 + \ldots + m_{k-1} + 2m_k - k$. Voor $1 \leq i \leq r$ zij $h_i \in M$ zodat $\iota h_i = |S_i|$. Daar $M \in \mathcal{B}$, bevat de M-rij $(h_1, \ldots, h_r)$ een nulrij - zeg $(h_{i_1}, \ldots, h_{i_m})$ - met lengte $\leq m_k$. Dan is $S_{i_1} \vee \ldots \vee S_{i_m}$ een nul-deelrij van S met lengte $\leq n_k \cdot m_k$.

We moeten ook nog verifieren dat $G \in \mathcal{A}$. Zij dus S een G-rij ter lengte $\lambda G + 1$. Dan is S een N-rij met lengte

$$n_1 + \ldots + n_{k-1} + (m_1 - 1)n_1 + \ldots + (m_{k-1} - 1)n_{k-1} + n_k m_k - k + 1 \geq$$

$$\geq n_1 + \ldots + n_{k-1} + n_k(m_1 + \ldots + m_k - k + 1) - k + 1$$

en dus bevat πS zeker $m_1 + \ldots + m_k - k = \lambda M$ disjuncte nulrijen $\pi S_1, \ldots, \pi S_{\lambda M}$ met lengte $\leq n_k$, en de resterende elementen van πS (tenminste $n_1 + \ldots + n_k - 1 + 1 = \lambda N + 1$ in aantal) bevatten nog een nulrij $\pi S_{\lambda M+1}$. Als $h_i \in M$ zodat $\iota h_i = |S_i|$, dan bevat $(h_1, \ldots, h_{\lambda M+1})$ een nulrij $(h_{i_1}, \ldots, h_{i_s})$. De deelrij $S_{i_1} \vee \ldots \vee S_{i_s}$ van S is dan een nulrij en S blijkt niet primitief te zijn.

Gevolg 4.1.1. Als $N = C_{n_1} \times \ldots \times C_{n_k} \in \mathcal{B}(n_i | n_{i+1})$ dan
$C_{n_1} \times \ldots \times C_{n_{k-1}} \times C_{mn_k} \in \mathcal{B}$.

Bewijs. Pas stelling 4.1 toe met $M = C_1 \times \ldots \times C_1 \times C_m$.

Gevolg 4.1.2. Als $\lambda(G \times C_n) = \lambda G + n - 1$ en $n > \lambda G$, en $G \times C_n \times C_n \in \mathcal{A}$, dan $G \times C_{mn} \in \mathcal{B}$.

Bewijs. Dit is een consequentie van Gevolg 4.1.1 en lemma 4.2.
Een bijzonder geval hiervan is

Gevolg 4.1.3. Als G een p-groep is, en $p^n > \lambda G$, dan $G \times C_{mp^n} \in \mathcal{B} \subset \mathcal{A}$.

Dit is een serie III uit §1. Hieronder valt o.a. $C_2 \times C_2 \times C_2 \times C_{12}$ maar net niet $C_2 \times C_2 \times C_6$ of $C_3 \times C_3 \times C_6$.

Gevolg 4.1.4. Als $C_{n_1} \times C_{n_2} \in \mathfrak{B}(n_1/n_2)$ en p is priem dan

$$C_{n_1 p^k} \times C_{n_2 p^k} \in \mathfrak{B}.$$

Bewijs. Volgens Gevolg 4.1.3 is $C_{p^k} \times C_{p^k} \in \mathfrak{B}$; pas nu stelling 4.1 toe.

Stelling 4.2. dim $G \leq 2 \rightarrow G \in \mathfrak{B} \subset \mathfrak{A}$.

Bewijs. Dit volgt door inductie naar het aantal verschillende priemfactoren van n_1, met als basis voor de inductie

$$C_1 \times C_{n_2/n_1} \in \mathfrak{B}$$

terwijl de inductiestap berust op Gevolg 4.1.4.

Gevolg. Als $N = C_{n_1} \times \ldots \times C_{n_k} \in \mathfrak{B}(n_i | n_{i+1})$ en als $n_{k-1} = n_k$, dan

$$C_{n_1} \times \ldots \times C_{n_{k-2}} \times C_{an_{k-1}} \times C_{bn_k} \in \mathfrak{B} \text{ voor alle a, b zodat } a|b.$$

Bewijs. Pas stelling 4.1 toe met $M = C_1 \times \ldots \times C_1 \times C_a \times C_b$.

Opmerking. Wij hebben een inductie-procédé toegepast op groepen uit $\mathfrak{B}$. Men zou kunnen trachten zulks regelrecht te doen voor groepen uit $\mathfrak{A}$. Voor een exacte rij $0 \rightarrow M \overset{\iota}{\rightarrow} G \overset{\pi}{\rightarrow} N \rightarrow 0$ zou men dan uit $M \in \mathfrak{A}$ en $N \in \mathfrak{A}$ willen concluderen dat $G \in \mathfrak{A}$. Dit stuit echter op grote moeilijkheden; vgl. de opmerking na stelling 2.3.

Er is ook nog geen inductie-methode gevonden voor willekeurige groepen van dimensie 3. Men beschouwe bij wijze van voorbeeld de exacte rij

$$0 \rightarrow C_3 = C_1 \times C_1 \times C_3 \rightarrow C_2 \times C_2 \times C_6 \overset{\pi}{\rightarrow} C_2 \times C_2 \times C_2 \rightarrow 0.$$

Om te bewijzen dat $\mu(C_2 \times C_2 \times C_6) = \lambda(C_2 \times C_2 \times C_6) = 7$ met de methoden van deze paragraaf moet men, uitgaande van een $C_2 \times C_2 \times C_6$-rij S ter lengte 8, in πS drie disjuncte nulrijen opsporen, liefst door afsplitsing van "korte" nulrijen. Dit lukt echter in het algemeen niet; zo heeft

$$\left(\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}\right)$$

in $C_2 \times C_2 \times C_2$ niet drie disjuncte nul-deelrijen. Desondanks is het hoofdvermoeden correct voor $C_2 \times C_2 \times C_6$ (J.H. VAN LINT [12], [13]).

5. Groepen van de gedaante $C_{2n_1} \times C_{2n_2} \times C_{2n_3}$

Het hoofdvermoeden is nu bewezen voor de groepen der typen I, II, III in §1. De groepen van de resterende typen IV en V zijn alle van de gedaante $C_{2n_1} \times C_{2n_2} \times C_{2n_3}$. Voor deze groepen maken we gebruik van de volgende stelling.

Stelling 5.1. Als $C_{n_1} \times C_{n_2} \times C_{n_3} \in \mathcal{C}(n_i | n_{i+1})$ dan $C_{2n_1} \times C_{2n_2} \times C_{2n_3} \in \mathcal{A}$.

Bewijs. Zij $G = C_{2n_1} \times C_{2n_2} \times C_{2n_3}$, $H = C_{n_1} \times C_{n_2} \times C_{n_3}$; in plaats van $C_2 \times C_2 \times C_2$ schrijven we ook $(C_2)^3$. Zij $\lambda = \lambda G$ en $L = \lambda H$. Zij $S = (g_1, \ldots, g_{\lambda+1})$ een G-rij; we moeten aantonen dat S niet primitief is.

Er is een exacte rij $0 \to H \overset{\iota}{\to} G \overset{\pi}{\to} (C_2)^3 \to 0$. Daar $\omega(C_2)^3 = 8$ komen in πS tenminste $n_1 + n_2 + n_3 - 5 = L - 2$ disjuncte paren onderling gelijke elementen voor; dit zijn evenzovele disjuncte nulrijen in $(C_2)^3$. Dus S is een disjuncte vereniging $S_1 \vee \ldots \vee S_{L-2} \vee R$ met $|\pi S_i| = 0$ ($S_i \neq \emptyset$) en lengte $(R) \geq 8$. Als lengte $(R) > 8$ of als 0 een element is van πR of als πR nog eens twee disjuncte paren van onderling gelijke elementen bevat, dan bevat πR nog drie disjuncte nulrijen πS_{L-1}, πS_L en πS_{L+1}; is dan $h_i \in H$ zodat $\iota h_i = |S_i|$, dan bevat $(h_1, \ldots, h_{L+1})$ een nulrij $(h_{i_1}, \ldots, h_{i_k})$ in H, en $S_{i_1} \vee \ldots \vee S_{i_k} \leq S$ is een nulrij in G. Stel daarom dat πR bestaat uit één paar onderling gelijke elementen (die dan nog een nulrij πS_{L-1} in $(C_2)^3$ vormen) en nog 6 onderling verschillende elementen $\neq 0$. Laat $h_i \in H$ met $\iota h_i = |S_i|$ $(1 \leq i \leq L-1)$. Zonder beperking van de algemeenheid mogen we aannemen dat $g_1, g_2, \ldots, g_6$ de resterende 6 elementen van S zijn, en als we in $(C_2)^3$ een geschikte basis kiezen kunnen we schrijven

$$\pi g_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}; \ \pi g_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}; \ \pi g_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}; \ \pi g_4 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}; \ \pi g_5 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}; \ \pi g_6 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Daar $\pi g_1 + \pi g_2 + \pi g_4 = 0$ moet $g_1 + g_2 + g_4 \in \pi^{-1}(0) = \iota H$, zeg $g_1 + g_2 + g_4 = \iota t_1$, $t_1 \in H$. Op analoge gronden zijn er $t_i \in H$ $(1 \leq i \leq 7)$ met

$$\iota t_2 = g_1 + g_2 + g_5 + g_6 \ ; \quad \iota t_5 = g_2 + g_3 + g_6 \ ;$$
$$\iota t_3 = g_1 + g_3 + g_5 \ ; \quad \iota t_6 = g_2 + g_3 + g_4 + g_5 \ ;$$
$$\iota t_4 = g_1 + g_3 + g_4 + g_6 \ ; \quad \iota t_7 = g_4 + g_5 + g_6 \ .$$

Als er een i is zodat de H-rij $(h_1, \ldots, h_{L-1}, t_i)$ een nulrij bevat, dan bevat ook S een nulrij. Is daarentegen $(h_1, \ldots, h_{L-1}, t_i)$ primitief voor $i = 1, 2, \ldots, 7$, dan bevat H een echte nevenklasse K met $t_i \in K$ $(1 \leq i \leq 7)$, daar $H \in \mathcal{C}$. Zij N de normaaldeler van H waarvan K een nevenklasse is; dan is $K = N + t_1$. Aangezien

$$t_1 + t_3 + t_5 + t_7 = t_2 + t_4 + t_6$$

zoals men onmiddellijk kan verifieren, moet $4t_1 \equiv 3t_1 \pmod{N}$, dus $t_1 \in N$, dus $K = N$: tegenspraak.

Gevolg. Als p priem, dan $C_{2p}^{n_1} \times C_{2p}^{n_2} \times C_{2p}^{n_3} \in \mathcal{A}$.

Bewijs. Dit volgt uit stelling 5.1 en stelling 3.2.

Hiermee is het type IV afgehandeld. Ook voor groepen van het type V zal uit stelling 5.1 volgen dat het hoofdvermoeden correct is, zodra wij hebben aangetoond dat $C_{nm_1} \times C_{nm_2} \in \mathcal{C}$ voor n, m_1 en m_2 omschreven in V.

6. Inductie in $\mathcal{C}$

Alle resultaten in deze paragraaf zijn afkomstig van P. VAN EMDE BOAS.

Bij onze poging tot inductie voor het hoofdvermoeden bleken wij ons te moeten beperken tot een deelklasse $\mathcal{B}$ van $\mathcal{A}$. Evenzo zullen we binnen

$\mathcal{C}$ een deelklasse $\mathfrak{D}$ beschouwen.

Definitie. $\mathfrak{D}$ is de klasse van alle groepen van de vorm $G \simeq C_p \times C_p$ met de volgende eigenschap: iedere G-rij S ter lengte $3(p-1)$ die niet bestaat uit 3 elementen, elk met multipliciteit $p-1$ voorkomend, bevat een nulrij met lengte $\leq p$.

Wij zullen een nulrij in $C_n \times C_n$ met lengte $\leq n$ een korte nulrij noemen.

Als $G = C_2 \times C_2$ en S is een G-rij ter lengte $3(2-1) = 3$ zonder korte nulrijen, dan moet G uit 3 verschillende elementen ongelijk 0 bestaan, die dan elk multipliciteit $1 = 2 - 1$ in S hebben. Dus

$$C_2 \times C_2 \in \mathfrak{D}.$$

Evenzo kan men betrekkelijk eenvoudig verifieren dat

$$C_3 \times C_3 \in \mathfrak{D},$$

terwijl met behulp van een electronische computer (de EL X8 van het Mathematisch Centrum) is vastgesteld dat

$$C_5 \times C_5 \; ; \quad C_7 \times C_7 \in \mathfrak{D}.$$

Wij zullen bewijzen:

Stelling 6.1. Als $C_p \times C_p \in \mathfrak{D}$ en $C_{n_1} \times C_{n_2} \in \mathcal{C}$ $(n_1 | n_2)$, dan

$$C_{pn_1} \times C_{pn_2} \in \mathcal{C}.$$

Daar $C_m = C_1 \times C_m \in \mathcal{C}$ voor iedere m en $C_p r \times C_p s \in \mathcal{C}$ als p priem (stelling 3.2) kunnen we dan concluderen:

Gevolg 6.1.1. Als $n = 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4}$, dan

a) $C_n \times C_{nm} \in \mathcal{C}$ voor iedere m;

b) $C_{np^r} \times C_{np^s} \in \mathcal{C}$ voor p priem.

Combineren we dit resultaat met stelling 5.1 dan vinden we

Gevolg 6.1.2. Als $n = 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4}$, dan

a) $C_2 \times C_{2n} \times C_{2nm} \in \mathcal{A}$ voor iedere m;

b) $C_2 \times C_{2np^r} \times C_{2np^s} \in \mathcal{A}$ voor p priem.

Hiermee is dan ten laatste type V uit §1 afgehandeld.

Opmerking. Zij S een rij bestaande uit 3 elementen van $C_p \times C_p$, ieder (p-1) keer optredend, die geen korte nulrij bevat. Na geschikte basis keuze heeft S de vorm

$$\underbrace{\begin{bmatrix}1\\0\end{bmatrix}, \ldots, \begin{bmatrix}1\\0\end{bmatrix}}_{p-1}, \underbrace{\begin{bmatrix}0\\1\end{bmatrix}, \ldots, \begin{bmatrix}0\\1\end{bmatrix}}_{p-1}, \underbrace{\begin{bmatrix}a\\b\end{bmatrix}, \ldots, \begin{bmatrix}a\\b\end{bmatrix}}_{p-1}$$

omdat

$$\underbrace{\begin{bmatrix}1\\0\end{bmatrix}, \ldots, \begin{bmatrix}1\\0\end{bmatrix}}_{p-a}, \underbrace{\begin{bmatrix}0\\1\end{bmatrix}, \ldots, \begin{bmatrix}0\\1\end{bmatrix}}_{p-b}, \begin{bmatrix}a\\b\end{bmatrix}$$

een nulrij is van lengte $2p + 1 - (a+b)$ moet gelden:

$$a + b \leq p.$$

Men kan zich afvragen welke elementen $\binom{a}{b}$ als derde element kunnen optreden. Het is gemakkelijk in te zien dat ieder paar a, b met a = 1 of b = 1 voldoet; evenzo ieder paar met a + b = p (deze situatie is tot de vorige te herleiden door middel van basistransformatie).
P. VAN EMDE BOAS heeft het vermoeden uitgesproken dat deze oplossingen (die in het p × p-rooster een rechthoekige gelijkbenige driehoek vormen) precies de enige oplossingen zijn. Dit vermoeden laat zich als volgt algemeen formuleren.

Vermoeden: Zij k een natuurlijk getal. Stel a, b zijn natuurlijke getallen, $1 \leq a, b \leq k$, met de volgende eigenschap:
Als $1 \leq n \leq k-1$ en als t_a en t_b zó bepaald zijn dat $t_a \cdot k < n \cdot a \leq (t_a + 1) \cdot k$ en $t_b \cdot k < n \cdot b \leq (t_b + 1) \cdot k$, dan geldt $n(a + b - 1) < k(t_a + t_b + 1)$.

Dan is $a = 1$ of $b = 1$ of $a + b = k$.

Dit vermoeden is met behulp van een computer (de EL X8 van het Mathematisch Centrum) bevestigd voor alle natuurlijke getallen k met $5 \leq k \leq 100$.

Een tweede vermoeden, uit het bovenstaande te verkrijgen door in plaats van "$n(a + b - 1) < k(t_a + t_b + 1)$" te lezen "$n(a + b - 1) \leq k(t_a + t_b + 1)$" en door in plaats van "of $a + b = k$" te lezen "of $a + b = k$, $k + 1$", blijkt voor priemgetallen k met het bovenstaande equivalent, maar kan voor sommige deelbare waarden van k gelogenstraft worden; men neme bijvoorbeeld $k = 4m$, $a = 2$, $b = 2m - 1$ of $k = 9$, $a = 2$, $b = 5$ of $k = 14$, $a = 3$ en $b = 5$.

Voor het bewijs van stelling 6.1 hebben we een hulpstelling nodig. Zij p priem, en zij Q een willekeurige eindige abelse groep. We beschouwen $C_p \times C_p \times Q$ en gebruiken de natuurlijke projecties π_1: $C_p \times C_p \times Q \to C_p \times C_p$ en π_2: $C_p \times C_p \times Q \to Q$. Dus als $a, b \in C_p$ en $x \in Q$, dan

$$\pi_1 \begin{pmatrix} a \\ b \\ x \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}; \quad \pi_2 \begin{pmatrix} a \\ b \\ x \end{pmatrix} = x.$$

Lemma 6.1. Zij S een rij ter lengte $3(p - 1)$ in $C_p \times C_p \times Q$ met de volgende drie eigenschappen:

(i) $\pi_1 S$ bestaat uit 3 elementen die elk met multipliciteit $p - 1$ voorkomen;

(ii) $\pi_1 S$ bevat geen korte nulrijen;

(iii) er is een $t \neq \emptyset$ in Q zodanig dat $|\pi_2 T| = t$ als $\emptyset \neq T \leq S$ en $|\pi_1 T| = 0$.

Dan is er in $C_p \times C_p$ een echte nevenklasse K zodanig dat er voor iedere $\binom{u}{v} \neq 0$ in $(C_p \times C_p) \setminus K$ deelrijen T_1, T_2 van S bestaan met $|\pi_1 T_1| = |\pi_1 T_2| = \binom{u}{v}$ en $|\pi_2 T_1| \neq |\pi_2 T_2|$.

Bewijs. We merkten al op dat we zonder beperking van de algemeenheid mogen aannemen dat

$$S = \left(\begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 0 \\ x_{p-1} \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ y_2 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 1 \\ y_{p-1} \end{bmatrix}, \begin{bmatrix} a \\ b \\ z_1 \end{bmatrix}, \ldots, \begin{bmatrix} a \\ b \\ z_{p-1} \end{bmatrix} \right)$$

met $a + b \leq p$. Dit laatste impliceert dat we mogen stellen:

(1) $a \leq \frac{1}{2} p$.

Als $T = \left(\begin{bmatrix} 1 \\ 0 \\ x_1 \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 0 \\ x_{p-a} \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ y_1 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 1 \\ y_{p-b} \end{bmatrix}, \begin{bmatrix} a \\ b \\ z_i \end{bmatrix} \right)$, dan

$|\pi_1 T| = 0$; dus

(2) $|\pi_2 T| = x_1 + \ldots + x_{p-a} + y_1 + \ldots + y_{p-b} + z_i = t$

waaruit volgt dat $z_1 = z_2 = \ldots = z_{p-1}$; noem de gemeenschappelijke waarde z

Zij $1 \leq n \leq p - 1$ zodat na $\equiv p - 1 \pmod p$ en $0 \leq m \leq p - 1$ zodat $m \equiv nb \pmod p$; dan moet ook

$$x_i + nz + y_1 + \ldots + y_{p-m} = t$$

zodat $x_1 = \ldots = x_{p-1}$, $= x$; evenzo $y_1 = \ldots = y_{p-1}$, y.

We bepalen nu n zo dat $0 \leq n \leq p - 1$ en $n \equiv 2b \pmod p$; dan

$$(p - 2a)x + (p - n)y + 2z = t.$$

Tezamen met (2) geeft dit

(3) $z = ax + by - \delta py$; $t = p(x + y) - \delta py$,

met $\delta = 0$ als $b \leq \frac{1}{2} p$ en $\delta = 1$ als $b > \frac{1}{2} p$. In het laatste geval volgt: $px = t \neq 0$; in het eerste geval is $px \neq 0$ of $py \neq 0$ daar $px + py = t \neq 0$. Zonder beperking van de algemeenheid mogen we dus aannemen dat

(4) $$px \neq 0.$$

We onderscheiden een drietal gevallen.

Geval 1. $a = b = 1$.

Zij

$$K = \{ \binom{u}{v} \in C_p \times C_p : u = p - 1 \}.$$

Als $0 \neq \binom{u}{v} \notin K$, en als $n_1 = u + 1$, $n_3 = p - 1$ en $n_2 = \begin{cases} 0 & \text{als } v = p - 1 \\ v+1 & \text{als } v < p - 1 \end{cases}$,

dan zijn

$$T_1 = (\underbrace{\begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix}}_{u^\times}, \underbrace{\begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix}}_{v^\times})$$

en

$$T_2 = (\underbrace{\begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix}}_{n_1^\times}, \underbrace{\begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix}}_{n_2^\times}, \underbrace{\begin{bmatrix} a \\ b \\ z \end{bmatrix}, \ldots, \begin{bmatrix} a \\ b \\ z \end{bmatrix}}_{n_3^\times})$$

deelrijen van S met $|\pi_1 T_1| = |\pi_1 T_2| = \binom{u}{v}$ en

$$|\pi_2 T_1| - |\pi_2 T_2| = (u+1)x + n_2 y + (p-1)z - (ux+vy) = \begin{cases} t \neq 0 & \text{als } n_2 = v+1 \\ px \neq 0 & \text{als } n_2 = 0 \end{cases}.$$

Geval 2. $a = 1$, $b \neq 1$.
We mogen zonder beperking van de algemeenheid aannemen dat $b \leq \frac{1}{2} p$, want anders nemen we als basis in $C_p \times C_p$ de elementen $e_1 = \binom{1}{b}$ en $e_2 = \binom{0}{1}$; het derde element $\binom{1}{0}$ krijgt dan nieuwe coördinaten 1 en $p - b \leq \frac{1}{2} p$.

Bepaal $m \in N$ zo dat $mb < p \leq (m+1)b$; daar $b \neq 1$ is $m \leq p - 2$. Dan moet

$$(p - m)x + (p - mb)y + mz = t$$

en

$$(p - (m+1))x + (2p - (m+1)b)y + (m+1)z = t$$

en daarom

$$-x + (p-b)y + z = 0$$

en omdat $z = x + by$ volgt: $py = 0$. Nemen we K als in geval 1, dan is indien $0 \neq \binom{u}{v} \notin K$:

$$u \cdot \begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix} + v \cdot \begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix} = \begin{bmatrix} u \\ v \\ ux+vy \end{bmatrix} \in [S]$$

als ook

$$(u+1)\begin{bmatrix} 1 \\ 0 \\ x \end{bmatrix} + n_2 \begin{bmatrix} 0 \\ 1 \\ y \end{bmatrix} + (p-1)\begin{bmatrix} 1 \\ b \\ z \end{bmatrix} \in [S],$$

waar $n_2 \equiv v + b \pmod{p}$, $0 \leq n_2 \leq p-1$; en daar $py = 0$ is

$$(u+1)x + n_2 y + (p-1)z = ux + vy + px \neq ux + vy.$$

Geval 3. $a \neq$ en $b \neq 1$.
Zij $1 \leq m \leq p-2$ en stel er is een k zodat $ma < kp \leq (m+1)a$. We bepalen s zo dat $(s-1)p < mb \leq sp$. Dan moet

$$(kp - ma)x + (sp - mb)y + mz = t$$

en

$$((k+1)p - (m+1)a)x + ((s+\varepsilon)p - (m+1)b)y + (m+1)z = t$$

waar $\varepsilon = 0$ als $(m+1)b \leq sp$ en $\varepsilon = 1$ als $(m+1)b > sp$. Dus ook

$$(p-a)x + (\varepsilon p - b)y + z = 0.$$

Is $b \leq \frac{1}{2}p$ en dus $z = ax + by$, dan vinden we dat $p(x + \varepsilon y) = 0$, en daar $px \neq 0$ moet $\varepsilon = 1$; maar dan volgt: $t = p(x + y) = 0$; tegenspraak!
Daarom moet $b > \frac{1}{2}p$ en dus $z = ax + by - py$; dan blijkt

$$p(x + (\varepsilon-1)y) = 0,$$

en daar $px \neq 0$ moet $\varepsilon = 0$ (en er volgt bovendien dat $py = px = t \neq 0$).

Als er een p-voud ligt tussen ma en (m+1)a, dan dus blijkbaar niet tussen mb en (m+1)b. Evenzo bewijst men: als tussen ma en (m+1)a géén p-voud ligt, dan wèl tussen mb en (m+1)b. Aangezien er (a-1) p-vouden liggen tussen a en (p-1)a, en (b-1) p-vouden tussen b en (p-1)b, terwijl aan elke $m \in \{1, \ldots, p-2\}$ precies één p-voud is toe te voegen die hetzij tussen ma en (m+1)a, hetzij tussen mb en (m+1)b ligt, moet $a - 1 + b - 1 = p - 2$ en dus $a + b = p$.
Maar dan kunnen we de situatie herleiden tot geval 2 door in $C_p \times C_p$ als nieuwe basis te nemen $e_1 = \binom{a}{b}$ en $e_2 = \binom{0}{1}$, omdat dan het derde element $\binom{1}{0}$, de nieuwe coördinaten c en 1 krijgt, waar $ca \equiv 1 \pmod p$.

<u>Bewijs van stelling 6.1</u>. Stel $C_p \times C_p \in \mathcal{C}$ en $C_{n_1} \times C_{n_2} \in \mathcal{C}(n_1|n_2)$. Er is een exacte rij

$$0 \to C_{n_1} \times C_{n_2} \xrightarrow{\iota} G = C_{pn_1} \times C_{pn_2} \xrightarrow{\pi} C_p \times C_p \to 0.$$

Zij $\lambda = \lambda(C_{n_1} \times C_{n_2}) = n_1 + n_2 - 2$. Zij S een primitieve G-rij ter lengte $pn_1 + pn_2 - 3$. Daar $C_p \times C_p \in \mathcal{B}$ (stelling 4.2) is S een disjuncte vereniging $S_1 \vee \ldots \vee S_{\lambda-1} \vee R$ met $|\pi S_i| = 0$ en $0 \neq$ lengte $(S_i) \leq p$; laat $a_i \in C_{n_1} \times C_{n_2}$ zodat $a_i = |S_i|$ $(1 \leq i \leq \lambda-1)$.

<u>Geval 1</u>. R is een disjuncte vereniging $S_\lambda \vee T$ met $0 \neq$ lengte $(S_\lambda) \leq p$ en $|\pi S_\lambda| = 0$. Laat $a_\lambda \in C_{n_1} \times C_{n_2}$ met $a_\lambda = |S_\lambda|$. Daar S primitief is, is de $C_{n_1} \times C_{n_2}$-rij $(a_1, \ldots, a_\lambda)$ primitief, dus maximaal. Evenzo is πT primitief in $C_p \times C_p$, met lengte $\geq 2p - 3 = \lambda(C_p \times C_p) - 1$. Daar $C_p \times C_p \in \mathcal{C}$ (stelling 3.2) moet $C_p \times C_p$ een echte nevenklasse K bevatten zodat

$$(C_p \times C_p) \setminus K \subset [\pi T]^*.$$

Dan

$$[S]^* \supset [S_1 \vee \ldots \vee S_\lambda]^* + [T]^* \supset G \setminus \pi^{-1}K.$$

Geval 2. πR bevat geen korte nulrij.

Daar $C_p \times C_p \in \mathfrak{D}$, volgens gegeven, is R een disjuncte vereniging $R_1 \vee R_2 \vee R_3$ met

$$\pi R_i = \underbrace{(b_i, b_i, \ldots, b_i)}_{(p-1)\times} \quad (i = 1, 2, 3).$$

Daar S primitief is, is ook de $C_{n_1} \times C_{n_2}$-rij $A = (a_1, \ldots, a_{\lambda-1})$ primitief. Omdat $C_{n_1} \times C_{n_2} \in \mathfrak{C}$ is er een ondergroep H van $C_{n_1} \times C_{n_2}$ en een $a \notin H$ zodanig dat

$$(C_{n_1} \times C_{n_2}) \setminus (a + H) \subset [A]^*.$$

Zij $Q = G / \iota H$, en zij ϕ het natuurlijke epimorphisme $G \to Q$. Zij $t = \phi \circ (-a) \neq 0$. Tenslotte definieren we een homomorphisme $\sigma: G \to C_p \times C_p \times Q$ door

$$\sigma(g) = \binom{\pi g}{\phi g} \quad (g \in C_p \times C_p \times Q).$$

Volgens lemma 6.1 zijn er nu twee mogelijkheden.

Geval 2a. $[\sigma R]$ bevat een element $\binom{0}{s}$ met $s \neq t$.

Zij $U \leq R$ met $|\sigma U| = \binom{0}{s}$; dan $\pi |U| = 0$, dus $|U| = \iota h$ voor een $h \in C_{n_1} \times C_{n_2}$, en $\phi|U| = s \neq t$, dus $h \notin a + H$. Maar dan kan S niet primitief zijn, want of $h = 0$, of $-h \in (C_{n_1} \times C_{n_2}) \setminus (a + H) \subset [A]^*$ en dus

$$[S] \supset [S_1 \vee \ldots \vee S_{\lambda-1}] + [U] \ni \iota h + (-h) = 0 = 0.$$

Geval 2b. $C_p \times C_p$ bevat een echte nevenklasse k zodanig dat $0 \neq c \in (C_p \times C_p) \setminus K \Rightarrow \exists T_1 \leq R,\ T_2 \leq R$ met $|\pi T_1| = |\pi T_2| = c$ en $|\phi T_1| \neq |\phi T_2|$.

Voor zo'n c is dan $|T_1| - |T_2| \in \pi^{-1}(0) = (C_{n_1} \times C_{n_2})$, zeg $|T_1| - |T_2| = \iota z$. Daar $\phi(|T_1| - |T_2|) \neq 0$ moet $z \notin H$; dus $z + (a+H) \neq a+H$.

Bijgevolg zal

$$[A] \cup (z + [A]) \cup \{0\} \supset C_{n_1} \times C_{n_2}$$

en dus ook

$$[S] \supset (|T_2| + [A]) \cup (|T_1| + [A]) \cup \{|T_2|\} \supset$$

$$\supset |T_2| + \iota(C_{n_1} \times C_{n_2}) = \pi^{-1}c.$$

Daar $3(p-1) > \lambda(C_p \times C_p)$ bevat R een deelrij U met $|\pi U| = 0$ en dus moet $|U| = \iota a_\lambda$ voor een $a_\lambda \in C_{n_1} \times C_{n_2}$. Daar S primitief is en $C_{n_1} \times C_{n_2} \in \mathcal{A}$ moet

$$C_{n_1} \times C_{n_2} = [(a_1, \ldots, a_\lambda)]^*$$

en dus

$$[S]^* \supset \iota(C_{n_1} \times C_{n_2}) = \pi^{-1}\, 0.$$

We hebben bewezen dat

$$[S]^* \supset G \setminus \pi^{-1} K.$$

7. Slotopmerkingen

Hoewel de opgave μG te bepalen voor eindige abelse groepen G voorlopig nog moeilijk genoeg lijkt willen we toch nog even wijzen op een generalisatie van dit probleem.

Zij H een halfgroep, dus een verzameling met daarin een associatieve binaire operatie $\circ$. Een idempotent van H is een element $e \in H$ met $e \circ e = e$. (Iedere eindige H bezit tenminste één idempotent.)
Een H-rij $S = (h_1, \ldots, h_n)$ heet idempotent indien

$$|S| = h_1 \circ h_2 \circ \ldots \circ h_n$$

een idempotent van H is. De rij S heet primitief als hij geen niet-lege

idempotente deelrijen bevat.

Als nu $A \subset H$, dan definieren we $\mu(A)$ als het supremum van de lengten van primitieve A-rijen. Voor het geval dat H een eindige commutatieve groep is komt μH dan overeen met de in §1 gedefinieerde constante.

Ook in een eindige abelse groep H is de nieuwe definitie een generalisatie. Zo is bijvoorbeeld $\mu\{h\}$ de orde van h, voor $h \in H$. In het algemeen geeft $\mu A (A \subset H)$ informatie over de mate van afhankelijkheid van A (triviaal voorbeeld: als $h_1 \neq 0$, $h_2 \neq 0$ en h_1, h_2 niet van de orde 2, dan $\mu\{h_1,h_2\} = 2 \Longleftrightarrow h_1$ en h_2 zijn elkaars inversen).

Onder de halfgroepen die geen groep zijn komen natuurlijk in de eerste plaats de eindige commutatieve halfgroepen voor nadere bestudering in aanmerking. Met name de berekening van μH in geval H een multiplicatieve halfgroep $\mathbb{Z}_n$ is (de restklassen modulo n onder vermenigvuldiging) lijkt ons niet zonder belang.

Een geheel ander probleem krijgt men als men de volgorde binnen de rij S, die in onze beschouwingen geen rol speelde, wel essentieel maakt door alleen zodanige deelrijen van S in de beschouwingen toe te laten die bestaan uit een aantal opeenvolgende elementen uit S. In willekeurige eindige halfgroepen wordt het behandeld in [3] en voor de multiplicatieve halfgroep der restklassen modulo n in [4]; men zie ook [8].

Indien we de bij dit probleem optredende constante voor een halfgroep H aangeven met $\bar{\mu}H$ dan bestaat voor een halfgroep H bestaande uit n elementen waaronder θ idempotenten de volgende algemene en niet te verbeteren bovengrens (cf. [3]):

Laten q en σ gedefinieerd zijn door

$$n = (2q - 1)\theta + \sigma, \quad 0 \leq \sigma \leq 2\theta - 1$$

Dan geldt

$$\bar{\mu}H \leq q^{2\theta-\sigma} \cdot (q+1)^{\sigma} - 1.$$

In het bijzonder geldt dus voor $\theta \geq n/3$:

$$\bar{\mu}H \leq 2^{n-\theta} - 1.$$

Voor de multiplicatieve halfgroep $\mathbb{Z}(n)$ van de restklassen modulo n geldt:

$$\overline{\mu}(\mathbb{Z}(n)) = \left[\prod_{i=1}^{t} \alpha_i \right] \cdot \phi(n) - 1$$

waarbij $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ de canonieke ontbinding van n is en ϕ de indicator van Euler voorstelt (zie [4]).

Voor de transformatie halfgroep T_k van alle afbeeldingen van een eindige verzameling bestaande uit k elementen in zichzelf geldt

$$\overline{\mu}T_k = k! - 1 \text{ (zie [8])}.$$

Literatuur

Hoofdstuk I

[1] Baker, G., Drum shapes and isospectral graphs, J. Math. Phys. 7, 2238-2242 (1966).

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

[3] Bose, R.C., Strongly regular graphs, partial geometries and partially balanced designs, Pacific J. Math. 13, 389-419 (1963).

[4] Bose, R.C., On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements, Calcutta Math. Soc. golden jubilee commemoration volume part I, 341-354 (1958-9).

[5] Bose, R.C. and I.M. Chakravarti, Hermitian varieties in a finite projective space $PG(N,q^2)$, Canad. J. Math. 18, 1161-1182 (1966).

[6] Bose, R.C., W.H. Clatworthy and S.S. Shrikhande, Tables of partially balanced designs with two associated classes, Techn. Bulletin No. 107, Univ. of North Carolina (1954).

[7] Bruck, R.H., Finite nets II, Uniqueness and imbedding, Pacific J. Math. 13, 421-457 (1963).

[8] Chang, L.C., Association schemes of partially balanced block designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$ and $p_{11}^2 = 4$, Sci. Record 4, 12-18 (1960).

[9] Collatz, L. und U. Sinogowitz, Spectren endlicher Graphen, Abh. Math. Sem. Hamburg 21, 63-77 (1957).

[10] Coxeter, H.S.M., Regular polytopes, second ed. New York (1963), Macmillan.

[11] Dembowski, P., Kombinatorik, Math. Semin. Univ. Frankfurt, (1965).

[12] Dembowski, P., Endliche Geometrien, Ergebnisse, Springer, to appear.

[13] Fisher, M.E., On hearing the shape of a drum, J. Combin. Theory 1, 105-125 (1966).

[14] Fisher, R.A. and F. Yates, Statistical tables, 6th edit., Oliver Boyd (1963).

[15] Goethals, J.M. and J.J. Seidel, Orthogonal matrices with zero diagonal, Canad. J. Math.

[16] Guérin, R., Vue d'ensemble sur les plans en blocks incomplets équilibrés en partiellement équilibrés, Revue de l'Inst. Intern. Statist. 33, 24-58 (1965).

[17] Hall, M., Combinatorial theory, (1967), Ginn Comp.

[18] Hoffman, A.J., On the polynomial of a graph, Amer. Math. Monthly 70, 30-36 (1963).

[19] Hoffman, A.J., On the uniqueness of the triangular association scheme, Ann. Math. Statist. 31, 492-497 (1960).

[20] Hoffman, A.J., The eigenvalues of the adjacency matrix of a graph, Research note, I.B.M. research center (1967).

[21] Hoffman, A.J., and D.K. Ray-Chaudhuri, On the line graph of a symmetric B.I.B., Trans. Amer. Math. Soc. 116, 238-252 (1965).

[22] Kac, M., Can one hear the shape of a drum, Amer. Math. Monthly 73, Papers in analysis, 1-23 (1966).

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

[24] Lüneburg, H., Die Suzukigruppen und ihre Geometrien, Lecture notes, No 10, Springer (1965).

[25] Lüneburg, H., Steinersche Tripelsysteme mit fahnentransitiver Kollineationsgruppe, Math. Annalen 149, 261-270 (1963).

[26] Paley, R.E.A.C., On orthogonal matrices, J. Math. Phys. 12, 311-320 (1933).

[27] Primrose, E.J.F., Resolvable balanced incomplete block designs, Sankhya, 12, 137-140 (1952).

[28] Qvist, B., Some remarks concerning curves of the 2nd. degree in a finite plane, Ann. Acad. Sci. Fennicae, Ser. A I, Math. Phys. No 134 (1962).

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

[30] Rooy, A.C.M. van, and H.S. Wilf, The interchange graph of a finite graph, Acta Mat. Acad. Sci. Hung. 16, 263-270 (1965).

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

[32] Segre, B., Introduction to Galois geometries, Memoria accad. Lincei (1967).

[33] Seidel, J.J., Strongly regular graphs of L_2-type and of triangular type, Kon. Ned. Akad. Wetensch. Amst. Proc. A 70 (= Indag. Math. 29), 188-196 (1967).

[34] Seidel, J.J., Strongly regular graphs with (-1, 1, 0) adjacency matrix having eigenvalue 3, Linear Algebra and Appl. 1, (1968).

[35] Seiden, E. and E. Zemach, On orthogonal arrays, Ann. Math. Statist. 37, 1355-1370 (1966).

[36] Seiden, E., On a method of construction of partial geometries and partial Bolyai-Lobachevsky planes, Amer. Math. Monthly 73, 158-161 (1966).

[37] Shrikhande, S.S., The uniqueness of the L_2 association scheme, Ann. Math. Statist. 30, 781-798 (1959).

[38] Shrikhande, S.S. and Bhagwandas, Duals of incomplete block designs, J. Indian Statist. Assoc. 3, 30-37 (1965).

[39] Wan Zhe Xian, PBIB designs based on symplectic geometry over finite fields, Acta Math. Sinica 15, 362-371 (1965).

[40] Williamson, J., Hadamard's theorem and the sum of four squares, Duke Math. J. 11, 65-81 (1944).

Hoofdstuk II

[1] Berlekamp, E.R., Algebraic Coding Theory, Mc. Graw-Hill, (1968).

[2] Golomb, S.W. and E.C. Posner, Rook domains, latin squares, affine planes and error-distributing codes, IEEE Trans. on Inf. Theory, IT-10, 196-208 (1964).

[3] Peterson, W.W., Error-correcting codes, M.I.T. Press (1961).

[4] Slepian, D., Coding Theory, Nuovo Cimento 13, 373-388 (1959).

[5] Slepian, D., Some further theory of group codes, Bell System Tech. J. 39, 1219-1252 (1960).

Hoofdstuk III

[1] Baayen, P.C., Een geval van een structuurprobleem voor abelse groepen, WN 24, Mathematisch Centrum, Amsterdam, 1968.

[2] Baayen, P.C., Een combinatorisch vermoeden bevestigd voor $C_2 \times C_2 \times C_2 \times C_6$, WN 25, Mathematisch Centrum, Amsterdam, 1968.

[3] Baayen, P.C., Van Emde Boas, P. and Kruyswijk, D., A combinatorial problem on finite semigroups, Report ZW 1965-006, Mathematical Centre, Amsterdam, 1965.

[4] Baayen, P.C., and Kruyswijk, D., A note on the multiplicative semigroup of residue classes modulo n, Report ZW 1965-007, Mathematical Centre, Amsterdam, 1965.

[5] Borewics, S.I. and Shafarewič, I.R., Zahlentheorie, Bazel & Stuttgart, 1966.

[6] C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Univ. Hamburg 11 (1936) 73-75.

[7] S. Chowla, On the congruence $\sum_{i=1}^{s} a_i x_i^k \equiv 0 \pmod{p}$, J. Ind. Math. Soc. 25 (1961) 47-48.

[8] P. van Emde Boas, A combinatorial problem on the semigroup of all transformations of a finite set. Report ZW 1965-009, Mathematical Ventre, Amsterdam 1965.

[9] P. van Emde Boas, Some ALGOL 60 algorithms for the verification of combinatorial conjectures on finite Abelian groups. Report ZW 1968-014, Mathematical Centre, Amsterdam, 1968.

[10] P. van Emde Boas, and D. Kruyswijk, A combinatorial problem on finite Abelian groups. Report ZW 1967-009, Mathematical Centre, Amsterdam, 1967.

[11] P. Erdös, A. Ginzburg and A. Ziv, Theorem in the additive number theory. Bulletin of the research Council of Israel 10F (1961), 41-43.

[12] J.H. van Lint, $(C_2 \oplus C_2 \oplus C_6)!$ is true. Notitie 26, Onderafdeling der Wiskunde van de Technische Hogeschool, Eindhoven, 1968.

[13] J.H. van Lint, $(C_2 \oplus C_2 \oplus C_{2p})!$ is true. Notitie 27, Onderafdeling der Wiskunde van de Technische Hogeschool, Eindhoven, 1968.

[14] H.B. Mann, Two addition theorems. Journal of combinatorial Theory 3 (1967) 233-235.

[15]H.B. Mann and J.E. Olson, Sums of sets in the Elementary Abelian Group of Type (p,p). Journal of combinatorial theory 2 (1967), 275-284.

[16] J.E. Olson, Notices Am. Math. Soc. 15/3 (1968), Abstract 656-97, p. 532.