Inhoudsopgave

Hoofdstuk 1

Inleiding tot de theorie van de foutverbeterende codes

1.1 Inleiding

Foutverbeterende codes worden gebruikt om fouten te verbeteren wanneer berichten gestuurd worden door een *kanaal met geruis* (*noisy channel*), dit is een communicatiekanaal dat onderhevig is aan storingen. Het kanaal kan een telefoonlijn zijn, een communicatielijn vanuit een ruimteschip, een systeem bedoeld voor het opslaan van informatie .... De storingen kunnen veroorzaakt worden door menselijke fouten, bliksems, temperatuurschommelingen, onnauwkeurigheden van de uitrusting, $\cdots$. Als gevolg van deze storingen kunnen de ontvangen berichten verschillen van de verzonden berichten. De bedoeling van een foutverbeterende code is, door het toevoegen van *overtalligheid (redundancy)* aan het bericht, het ontvangen bericht zodanig te decoderen dat het uitgezonden bericht teruggevonden wordt indien (niet teveel) fouten optreden.

Een algemeen communicatiesysteem ziet er als volgt uit:

$$\boxed{\text{berichtenbron}} \xrightarrow{\text{bericht}} \boxed{\text{coderen}} \xrightarrow{\text{codewoord}} \boxed{\begin{matrix}\text{storingen}\\ \text{kanaal}\end{matrix}} \xrightarrow{\text{ontvangen vector}}$$

$$\boxed{\text{decoderen}} \xrightarrow[\text{bericht}]{\text{gedecodeerd}} \boxed{\text{gebruiker}}$$

Een eenvoudig voorbeeld waarbij slechts de berichten JA en NEEN verzonden worden:

Voorbeeld 1.1.1

$$\boxed{\text{bericht = JA of NEEN}} \xrightarrow{\text{JA}} \boxed{\text{coderen: JA=00000, NEEN=11111}} \xrightarrow{00000} \boxed{01001} \xrightarrow{01001}$$

$$\boxed{\text{decoderen: } 01001 \sim 00000\text{=JA}} \xrightarrow{\text{JA}} \boxed{\text{gebruiker}}$$

Hier traden twee fouten op, en de ontvangen vector 01001 werd gedecodeerd als het "dichtstbijzijnde" codewoord 00000, dit is, JA.

Een *binaire code* is een niet-ledige verzameling rijen (woorden) samengesteld met de symbolen 0 en 1. De code uit Voorbeeld 1.1.1 is de verzameling $\{00000, 11111\}$. Had men in plaats van deze code gebruik gemaakt van de code $\{0, 1\}$, dan zou bij het maken van één enkele fout het uitgezonden codewoord 0 (=JA) ontvangen worden als 1, en gedecodeerd worden als 1 (=NEEN). De code {0,1} is dan ook een inefficiënte code. In ons voorbeeld hebben wij de symbolen 0 en 1 vijfmaal herhaald. Men spreekt van een *binaire herhalingscode* (*binary repetition code*) van *lengte* 5. Dit is een eerste voorbeeld waarbij van overtalligheid gebruik gemaakt wordt om de berichten te beschermen tegen storingen. De overtallige symbolen zijn ook onderhevig aan storingen, zodat een exacte decodering niet gegarandeerd wordt; wat we willen is de waarschijnlijkheid op een exacte decodering zo groot mogelijk maken. Een goede code is een code in dewelke de woorden weinig op elkaar gelijken.

1.2 q-aire codes

Een *q-aire code* C is een niet-ledige verzameling rijen samengesteld met symbolen uit een verzameling $F_q = \{\lambda_1, \lambda_2, \cdots, \lambda_q\}$ van de orde q. De verzameling F_q wordt het *alfabet* genoemd, en gewoonlijk kiest men voor F_q de verzameling $\{0, 1, \cdots, q-1\}$. De elementen van C worden de *codewoorden* genoemd. Als $q = p^h$, met p een priemgetal en $h \in \mathbb{N} - \{0\}$, dan kiest men voor F_q gewoon het Galois veld $\mathrm{GF}(q)$. Is $q = 2$, dan spreekt men van een *binaire code*; is $q = 3$, dan spreekt men van een *ternaire code*.

Een code waarin alle codewoorden evenveel symbolen hebben noemt men een *blokcode*; het aantal symbolen n van elk codewoord noemt men de *lengte* van de code. Meestal zullen wij ons beperken tot blokcodes, en in het vervolg bedoelen wij met "code" altijd een "blokcode". Is C een code met lengte n over F_q, dan is C dus een deelverzameling van $(F_q)^n$. De elementen van $(F_q)^n$ worden de *vectoren* of de *woorden* genoemd. Is F_q =GF(q), dan is $(F_q)^n$ de n-dimensionale vectorruimte $V(n, q)$ over het Galois veld $\mathrm{GF}(q)$. Zo is de code uit Voorbeeld 1.1.1 een deelverzameling van $V(5, 2)$.

Een code C met M codewoorden van lengte n wordt dikwijls voorgesteld als een $M \times n$-matrix met als rijen de codewoorden. De binaire repetitiecode met lengte 3 bijvoorbeeld, wordt voorgesteld door de matrix $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$.

1.3 Hamming afstand, foutverbeterende en foutdetecterende codes

Wij leiden deze drie nieuwe begrippen in met een voorbeeld.

Voorbeeld 1.3.1
Onderstel dat HK en X identieke landkaarten hebben (zie figuur), maar dat alleen HK de veilige weg kent waarlangs X naar HK moet terugkeren. HK kan binaire data naar X versturen en wenst de route $NNWNNWWZZWW$
$NNNNWWN$ door te zenden. Hier bevinden wij ons in een situatie waar betrouwbaarheid belangrijker is dan snelheid van transmissie.

Figuur 1.1

De verzameling der berichten is hier $\{N, Z, W, O\}$. De snelste (dit is de kortste) code die wij kunnen gebruiken is

$$C_1 \begin{cases} 00 = N \\ 01 = W \\ 10 = O \\ 11 = Z. \end{cases}$$

Hier is dus $C_1 = (F_2)^2 = V(2, 2)$. In deze code is er geen overtalligheid, maar bij het maken van één enkele fout in een codewoord zal er reeds een verkeerde decodering plaatsvinden. Het is duidelijk dat hier C_1 geen bruikbare code is.

Wij zullen nu overtallige symbolen toevoegen om de berichten te beschermen tegen storingen. Beschouw de code C_2 die uit C_1 verkregen wordt door een extra symbool toe te voegen.

$$C_2 \begin{cases} 000 = N \\ 011 = W \\ 101 = O \\ 110 = Z. \end{cases}$$

De code C_2 heeft lengte 3 en is een deelverzameling van $V(3,2)$. Het doorzenden zal nu langer duren, maar als er in een codewoord één enkele fout gemaakt wordt dan is het ontvangen woord geen codewoord meer. De ontvanger X zal dus zien dat er een fout gemaakt is, en kan mogelijk om heruitzending vragen. De code C_2 kan dus één fout *detecteren*, en wordt daarom een *één-foutdetecterende* (*single error detecting*) code genoemd.

Onderstel nu dat het onmogelijk is om heruitzending te vragen, dit is, wij hebben een *éénwegskanaal* (*one-way channel*). Deze situatie doet zich bijvoorbeeld voor bij de transmissie van foto's uit de ruimte. In zulk geval is het essentieel om zoveel mogelijk informatie te halen uit de ontvangen vectoren. Beschouw daarom de code

$$C_3 \begin{cases} 00000 = N \\ 01101 = W \\ 10110 = O \\ 11011 = Z. \end{cases}$$

De binaire code C_3 heeft lengte 5 en is een deelverzameling van $V(5,2)$ (de overtalligheid is hier 3). Indien in een codewoord $\bar{x}$ één enkele fout gemaakt wordt, dan is het ontvangen woord $\bar{y}$ "dichter" gelegen bij het uitgezonden codewoord dan bij elk ander codewoord. Wij zijn dus in staat om één fout te *verbeteren*. Worden er ten hoogste twee fouten in een codewoord gemaakt, dan is de ontvangen vector opnieuw geen codewoord. Men spreekt hier van een *één-foutverbeterende* (*single error correcting*) en *twee-foutdetecterende* code.

Thans gaan wij de term "dichter" preciseren door een afstandsfunctie in te voeren op de verzameling $(F_q)^n$. De (*Hamming*) *afstand* (*Hamming distance*) tussen twee vectoren $\bar{x}$ en $\bar{y}$ van $(F_q)^n$ is het aantal posities in dewelke die twee vectoren verschillen. De afstand tussen $\bar{x}$ en $\bar{y}$ wordt voorgesteld door $d(\bar{x},\bar{y})$. In $(F_2)^5$ is bijvoorbeeld $d(00101, 11111) = 3$, in $(F_3)^3$ is $d(012, 201) = 3$.

Stelling 1.3.2
De Hamming afstand voldoet aan de drie metrische eigenschappen:

(i) $d(\bar{x},\bar{y}) = 0$ *als en slechts als* $\bar{x} = \bar{y}$,

(ii) $d(\bar{x},\bar{y}) = d(\bar{y},\bar{x})$ *voor alle* $\bar{x},\bar{y} \in (F_q)^n$,

(iii) $d(\bar{x},\bar{y}) \leq d(\bar{x},\bar{z}) + d(\bar{z},\bar{y})$ *voor alle* $\bar{x},\bar{y},\bar{z} \in (F_q)^n$.

Bewijs. Eigenschappen (i) en (ii) zijn triviaal. Eigenschap (iii), dit is de driehoeksongelijkheid, wordt als volgt aangetoond. De afstand $d(\bar{x},\bar{y})$ is het minimaal aantal wijzigingen van symbolen dat nodig is om $\bar{x}$ in $\bar{y}$ om te zetten. Maar we kunnen $\bar{x}$ in $\bar{y}$ omzetten door eerst $d(\bar{x},\bar{z})$ wijzigingen door te voeren (en zo $\bar{x}$ in $\bar{z}$ om te zetten) en daarna $d(\bar{z},\bar{y})$ wijzigingen door te voeren (en zo $\bar{z}$ in $\bar{x}$ om te zetten). Bijgevolg is $d(\bar{x},\bar{y}) \leq d(\bar{x},\bar{z}) + d(\bar{z},\bar{y})$. □

De Hamming afstand is de enige metriek die wij in deze cursus zullen beschouwen. Dat de Hamming afstand niet altijd best geschikt is illustreren wij met volgend voorbeeld. In

$(F_{10})^3$ is $d(428, 438) = d(428, 498)$, terwijl, als het over het intikken van een telefoonnummmer gaat bijvoorbeeld, het zinniger is een metriek te gebruiken waarbij 428 dichter ligt bij 438 dan bij 498.

Dichtste gebuur decodering

Onderstel dat een codewoord $\bar{x}$, door ons niet gekend, verzonden wordt en dat een vector $\bar{y}$ ontvangen wordt. Het is dan logisch om $\bar{y}$ te decoderen als een codewoord $\bar{x}'$, hopelijk $\bar{x}$, waarvoor $d(\bar{x}', \bar{y})$ minimaal is. Dit procédé noemt men *dichtste gebuur decodering* (*nearest neighbour decoding*). Hierbij moeten wij echter aannemen dat het kanaal aan volgende twee voorwaarden voldoet.

(i) Elk verzonden symbool heeft dezelfde waarschijnlijkheid p ($< \frac{1}{2}$) om fout toe te komen.

(ii) Als een symbool fout toekomt, dan is elk van de $q - 1$ mogelijke fouten even waarschijnlijk.

Zulk een kanaal wordt een *q-air symmetrisch kanaal* (*q-ary symmetric channel*) genoemd. Het getal p wordt de *symboolfout waarschijnlijkheid* (*symbol error probability*) van het kanaal genoemd.

Laten wij het binair symmetrisch kanaal nader onderzoeken.

Onderstel dat de code C lengte n heeft. Wordt een codewoord verstuurd, dan is $(1-p)^n$ de waarschijnlijkheid dat geen fouten optreden. De waarschijnlijkheid dat i ($0 \leq i \leq n$) fouten optreden in gegeven posities is $p^i(1-p)^{n-i}$; de waarschijnlijkheid dat i fouten optreden (zonder de posities te specifiëren) is $\binom{n}{i} p^i(1-p)^{n-i}$. Is $\bar{y}$ een vector en is $\bar{x}$ een codewoord met $d(\bar{x}, \bar{y}) = i$, dan is de waarschijnlijkheid dat bij het verzenden van $\bar{x}$ de vector $\bar{y}$ ontvangen wordt $p^i(1-p)^{n-i} = P(i)$. Uit $p < \frac{1}{2}$ volgt nu gemakkelijk dat $P(i)$ groter wordt naarmate $d(\bar{x}, \bar{y}) = i$ kleiner wordt.

De *woordfout waarschijnlijkheid* (*word error probability*) $P_{err}(C)$ van een code C over F_q is de waarschijnlijkheid op het maken van een foutieve decodering, op voorwaarde dat

deze waarschijnlijkheid onafhankelijk is van het verzonden codewoord. Wij illustreren dit met een voorbeeld.

Voorbeeld 1.3.3
Beschouw de binaire repetitiecode $C = \{000, 111\}$ van lengte 3. Onderstel dat p de symboolfout waarschijnlijkheid is. Wordt 000 verzonden dan zal de ontvangen vector $\bar{y}$ gedecodeerd worden als 000 als en slechts als $\bar{y} \in \{000, 100, 010, 001\}$. De waarschijnlijkheid dat er een correcte decodering plaatsvindt is dus $(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p)$. Wij bekomen dezelfde waarschijnlijkheid indien 111 verzonden wordt. Dus is $P_{err}(C) = 1 - (1-p)^2(1+2p) = 3p^2 - 2p^3$. Is bijvoorbeeld $p = 0,01$, dan is $P_{err}(C) = 0,000298$, en bijgevolg zal ongeveer één bericht op 3555 de gebruiker foutief bereiken.

Minimum afstand

De *minimum afstand* (*minimum distance*) van een code C, met $|C| > 1$, wordt gedefinieerd als

$$d(C) = \min\{d(\bar{x}, \bar{y}) \parallel \bar{x}, \bar{y} \in C, \bar{x} \neq \bar{y}\}.$$

Deze zeer belangrijke parameter geeft een maat van hoe goed de code is voor foutverbetering en foutdetectie. In Voorbeeld 1.3.1 is $d(C_1) = 1, d(C_2) = 2, d(C_3) = 3$.

Stelling 1.3.4
(i) Is $d(C) = s + 1$, dan kan C tot s fouten detecteren in een codewoord.

(ii) Is $d(C) = 2t + 1$ of $2t + 2$, dan kan C tot t fouten verbeteren in een codewoord.

Bewijs.

(i) Onderstel dat $d(C) = s + 1$. Onderstel dat $\bar{x} \in C$ verzonden wordt, en dat ten hoogste s fouten optreden. Wordt $\bar{y}$ ontvangen, dan is dus $d(\bar{x}, \bar{y}) \leq s$, zodat $\bar{y} \notin C$. Bij het ontvangen van $\bar{y}$ ziet men bijgevolg dat er fouten gemaakt werden.

(ii) Onderstel dat $d(C) = 2t + 1$ of $2t + 2$. Onderstel dat $\bar{x} \in C$ verzonden wordt en dat $\bar{y}$ ontvangen wordt, waarbij ten hoogste t fouten gemaakt worden. Er geldt dus $d(\bar{x}, \bar{y}) \leq t$. Is $\bar{x}' \in C$ met $\bar{x} \neq \bar{x}'$, dan tonen wij aan dat $d(\bar{x}', \bar{y}) \geq t + 1$. Moest $d(\bar{x}', \bar{y}) \leq t$, dan zou $d(\bar{x}, \bar{x}') \leq d(\bar{x}, \bar{y}) + d(\bar{y}, \bar{x}') \leq 2t$, wat strijdig is met $d(C) = 2t+1$ of $2t + 2$. Dus is $d(\bar{x}', \bar{y}) \geq t + 1$, zodat $\bar{x}$ het codewoord is dat het dichtst bij $\bar{y}$ is gelegen. De vector $\bar{y}$ zal dus gedecodeerd worden als $\bar{x}$, zodat de fouten hier verbeterd worden. □

Definitie 1.3.5
Een *(n, M, d)-code* ($M > 1$) is een code van lengte n, met M codewoorden, en met minimum afstand d.

Voorbeelden 1.3.6
(i) In Voorbeeld 1.3.1 is C_1 een (2,4,1)-code, C_2 een (3,4,2)-code, en C_3 een (5,4,3)-code.

(ii) De codewoorden van de *q-aire herhalingscode* van lengte n zijn

$$\begin{array}{cccc} 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ q-1 & q-1 & \dots & q-1. \end{array}$$

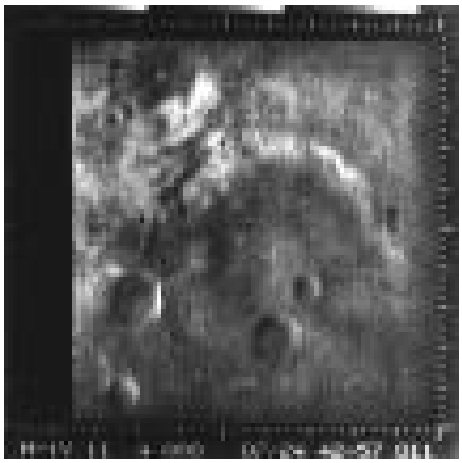
Deze code is een (n, q, n)-code.

1.4 Enkele codes uit de praktijk

(i) Foto's uit de ruimte

1965: Mariner 4 was het eerste ruimteschip dat foto's nam van een andere planeet. Er werden 22 foto's van Mars genomen. Elke foto was onderverdeeld in 200×200 rechthoekjes. Aan elk rechthoekje werd een binair 6-tal toegekend dat één der 64 helderheidsgraden tussen wit (=000000) en zwart (=111111) voorstelde. Het aantal symbolen per foto was dus 240.000. Gegevens werden doorgezonden aan een snelheid van $8\frac{1}{3}$ symbool per seconde. Bijgevolg nam het ongeveer 8 uren om een foto door te zenden.

De foto hierna is genomen door Mariner 4. Het is een foto van het Atlantis gebied op Mars.



Figuur 1.2: Mariner 4 foto van Mars

(http://photojournal.jpl.nasa.gov/catalog/PIA02980)

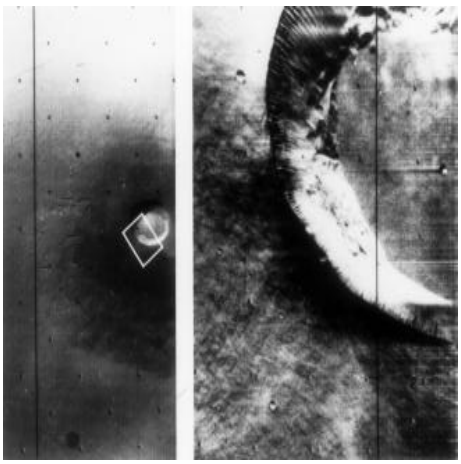
1969-72: Veel betere foto's van Mars werden bekomen door Mariners 6,7 en 9 (Mariner 8 ging verloren tijdens het lanceren). Er waren drie belangrijke redenen voor deze verbetering:

(1) Elke foto werd opgedeeld in 700×832 rechthoekjes.

(2) Mariner 9 was het eerste ruimteschip dat in een baan rond Mars werd gebracht.

(3) De zogenaamde Reed-Muller (32,64,16)-code werd gebruikt voor foutverbetering. Een binair 6-tal dat de helderheid voorstelde werd nu gecodeerd als een codewoord van lengte 32 (dus met 26 overtallige symbolen). De transmissiesnelheid werd opgedreven van $8\frac{1}{3}$ tot 16.200 symbolen per seconde. Meer dan 100.000 symbolen per seconde werden geproduceerd door de camera's, zodat de gegevens op magnetische band moesten opgeslagen worden voor transmissie.

De twee volgende foto's, van een vulkaankrater op Mars, werden genomen door Mariner 9. De eerste foto werd met een breedhoeklens genomen, de tweede met een telelens.



Figuur 1.3: Vulkaankrater op Mars

(http://photojournal.jpl.nasa.gov/catalog/PIA02983)

1976: Viking 1 voerde een zachte landing uit op Mars en bezorgde ons kleurfoto's van zeer hoge kwaliteit. De transmissie van kleurfoto's is om zo te zeggen niet meer ingewikkeld dan de transmissie van zwart-wit foto's. Men neemt hierbij dezelfde zwart-wit foto verschillende malen, telkens door een andere gekleurde filter. De bekomen zwart-wit foto's worden dan verzonden zoals hierboven beschreven, en de kleurfoto wordt op aarde dan gereconstrueerd.

De volgende foto is de allereerste foto die Viking 1 van Mars genomen heeft. Voor de effectieve kleurenfoto verwijzen we naar het bijhorende website adres.

Figuur 1.4: Eerste Viking 1 foto van Mars

(http://photojournal.jpl.nasa.gov/catalog/PIA00563)

Andere foto's genomen door ruimtesondes kunnen gevonden worden op het adres: http://photojournal.jpl.nasa.gov/

(ii) De ISBN code

Deel 1: De ISBN code standaard tot 31 december 2006

Elk boek heeft een International Standard Book Number (ISBN). Dit is een codewoord van lengte 10 toegekend door de uitgever. Er is bijvoorbeeld een boek met ISBN 0-19-853537-6 (de streepjes kunnen op andere plaatsen voorkomen en zijn in feite niet belangrijk). Het eerste symbool "0" duidt de taal aan (hier engels), de volgende twee symbolen duiden de uitgever aan (hier Oxford University Press), de volgende 6 symbolen vormen het boeknummer toegekend door de uitgever (hier staan zij voor het boek General Galois Geometries door J.W.P. Hirschfeld en J.A. Thas). Al deze symbolen komen uit de verzameling $\{0, 1, 2, \cdots, 9\}$. Het laatste symbool wordt zodanig gekozen dat het ISBN $x_1 x_2 \cdots x_{10}$ voldoet aan

$$\sum_{i=1}^{10} i x_i = 0$$

in $\mathrm{GF}(11) = \{0, 1, 2, \cdots, 10\}$. Bijgevolg is

$$x_{10} = \sum_{i=1}^{9} i x_i \pmod{11}$$

in $\mathbb{N}$. Is $x_{10} = 10$, dan schrijft men "X" voor x_{10}. De Chambers Twentieth Century Dictionary bijvoorbeeld heeft als ISBN 0550-10206-X.

De ISBN code is ontworpen voor de detectie van (a) één enkele fout en (b) een dubbele fout veroorzaakt door de transpositie van twee verschillende symbolen. Onderstel dat $\bar{x} = x_1 x_2 \cdots x_{10}$ het verzonden codewoord is (dit is hier het toegekende ISBN nummer) en dat $\bar{y} = y_1 y_2 \cdots y_{10}$ het ontvangen woord is (het getypte, gedrukte, $\cdots$ nummer). Werd er juist één enkele fout gemaakt, is bijvoorbeeld $y_j = x_j + a$ met $a \neq 0$ (in GF(11)) en $x_i = y_i$ voor alle $i \neq j$, dan is

$$\sum_{i=1}^{10} i y_i = (\sum_{i=1}^{10} i x_i) + ja \neq 0 \quad \text{(in GF(11))}.$$

In zulk geval detecteert men dus fouten. Onderstel vervolgens dat $\bar{y}$ uit $\bar{x}$ verkregen wordt door de transpositie van x_j en x_k, met $j \neq k$ en $x_j \neq x_k$.
Dan is

$$\sum_{i=1}^{10} i y_i = (\sum_{i=1}^{10} i x_i) + (k-j)x_j + (j-k)x_k = (k-j)(x_j - x_k) \neq 0$$

(in GF(11)). Hier detecteert men dus eveneens fouten.

Deel 2: De ISBN code standaard vanaf 1 januari 2007

Om te vermijden dat de ISBN nummers bestaande uit 10 karakters uitgeput zouden geraken, werd beslist om een nieuwe standaard voor de ISBN nummers in te voeren.

Het nieuwe ISBN nummer bestaat uit 13 cijfers; die opgesplitst kunnen worden in 5 delen. Hier is een voorbeeld van een nieuw ISBN nummer; we zullen dit als leidraad door de bespreking gebruiken:

ISBN: 978-0-11-000222-4.

1. *Het prefix element*: Dit werd vastgelegd door EAN International (European Article Number). Nu is dit 978 of 979.

2. *Het registratie groep element*: Het tweede element legt het land/geografische regio/taal vast. Dit tweede element bestaat uit minstens één cijfer en hoogstens 5 cijfers. Hoe groter de verwachte output, hoe minder cijfers hier gebruikt worden.

   Enkele voorbeelden:

   (a) 3 = duitse taalgroep,

   (b) 982 = regio zuiden stille oceaan.

3. *Het registrant element*: Het derde element identificeert een uitgever. Dit derde element bestaat uit minstens één en hoogstens 7 cijfers. Hoe groter de verwachte output, hoe minder cijfers hier gebruikt worden.

4. *Het publikatie element*: Het vierde element identificeert een specifieke uitgave van een uitgever. Het bestaat uit minstens één cijfer en hoogstens 6 cijfers. Uitgevers met het grootste aantal verwachte uitgaven krijgen hier 6 cijfers.

5. *Het controlegetal*: Nu zijn in de eerste vier delen al 12 cijfers gebruikt. We noteren deze met $a_1 \cdots a_{12}$. Het laatste cijfer is a_{13}. Dit wordt als volgt berekend:

   (a) Bereken eerst

   $$\begin{aligned} r &= 1 \cdot (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + \\ &\quad 3 \cdot (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \pmod{10}. \end{aligned}$$

   (b) Als $r = 0$, dan $a_{13} = 0$.
   Als $1 \leq r \leq 9$, dan $a_{13} = 10 - r$.

(http://www.isbn-international.org/en/manual.html)

(iii) Compact discspelers

Foutverbetering bij compact discspelers gebeurt via een combinatie van twee Reed-Solomon codes over GF(2^8). De eerste code heeft lengte 32, de andere lengte 28. Voor elk van de codes is $d = 5$. Dankzij deze code kan men een opeenhoping van ongeveer 8871 opeenvolgende fouten verbeteren, dit is een CD-"track" van ongeveer 2,5mm. Een opeenhoping van fouten die tot ongeveer driemaal zo lang is wordt verbeterd door lineaire interpolatie van het audiosignaal.

Hoofdstuk 2

Het hoofdprobleem van de codeertheorie

2.1 Het hoofdprobleem uit de codeertheorie

Een goede (n, M, d)-code heeft kleine n (voor snelle transmissie van berichten), grote M (om transmissie toe te laten van een groot aantal berichten), en grote d (om veel fouten te kunnen verbeteren). Het hoofdprobleem uit de codeertheorie is het optimaliseren van één der parameters n, M, d voor gegeven waarden van de andere twee. Gewoonlijk tracht men de grootste code te vinden voor gegeven lengte en gegeven minimum afstand. De grootste waarde van M waarvoor een q-aire (n, M, d)-code bestaat wordt voorgesteld door $A_q(n, d)$.

Stelling 2.1.1

(i) $A_q(n, 1) = q^n$,

(ii) $A_q(n, n) = q$.

Bewijs.

(i) Afstand ten minste 1, betekent gewoon dat de codewoorden verschillend zijn. Bijgevolg is de grootste q-aire $(n, M, 1)$-code de volledige verzameling $(F_q)^n$. Dit betekent dat $A_q(n, 1) = q^n$.

(ii) Onderstel dat C een q-aire (n, M, n)-code is. Elke twee codewoorden verschillen dan in alle posities. Dus voor de M codewoorden zijn de symbolen in de eerste positie allen verschillend, zodat $M \leq q$. Bijgevolg is $A_q(n, n) \leq q$. Nu is de q-aire herhalingscode een (n, q, n)-code. Wij besluiten dat $A_q(n, n) = q$. □

2.2 Gelijkwaardigheid van codes; gewicht van een woord

Gelijkwaardigheid van codes wordt ingeleid met volgend voorbeeld.

Voorbeeld 2.2.1
Het ligt in onze bedoeling $A_2(5,3)$ te bepalen. De code C_3 uit Voorbeeld 1.3.1 is een binaire $(5,4,3)$-code, zodat $A_2(5,3) \geq 4$. Om aan te tonen of er al dan niet een binaire $(5,5,3)$-code bestaat zou men alle deelverzamelingen van de orde 5 van $(F_2)^5$ kunnen beschouwen, en daarvan telkens de minimum afstand bepalen. Er zijn echter meer dan 200.000 dergelijke deelverzamelingen. Door het begrip "gelijkwaardigheid" zal het probleem sterk vereenvoudigd worden.

Definitie 2.2.2
Twee q-aire codes over F_q worden *gelijkwaardig* genoemd als de tweede uit de eerste kan verkregen worden door een opeenvolging van bewerkingen van de volgende gedaante:

(i) een permutatie op de posities van de code;

(ii) in een vaste positie, een permutatie op de symbolenverzameling.

Als de code voorgesteld wordt door een $M \times n$-matrix met de codewoorden als rijen, dan is (i) een permutatie op de kolommenverzameling, en is (ii) een permutatie op de symbolenverzameling, doorgevoerd in een vaste kolom. Het is duidelijk dat gelijkwaardige codes dezelfde parameters n, M, d hebben. Gelijkwaardige codes zullen dus evenveel fouten detecteren en verbeteren.

Voorbeelden 2.2.3
(i) De code

$$C \begin{cases} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{cases}$$

is gelijkwaardig met de code C_3 uit Voorbeeld 1.3.1. Duiden wij de i-de kolom met Ki voor, dan ontstaat C uit C_3 door de permutatie $K1 \mapsto K5, K2 \mapsto K4, K3 \mapsto K3, K4 \mapsto K2, K5 \mapsto K1$ gevolgd door de permutatie $0 \leftrightarrow 1$ in $K1$.

(ii) De ternaire code

$$C \begin{cases} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{cases}$$

is gelijkwaardig met de ternaire herhalingscode $\{000, 111, 222\}$. Voer daartoe in $K2$ de permutatie $1 \mapsto 0, 2 \mapsto 1, 0 \mapsto 2$ door, en in $K3$ de permutatie $2 \mapsto 0, 0 \mapsto 1, 1 \mapsto 2$.

Definitie 2.2.4
Twee q-aire codes C en C' over respectievelijke alfabetten F_q en F'_q noemt men *gelijkwaardig* als voor ten minste één (en dan elke) bijectie α van F'_q op F_q de code $(C')^\alpha$ over F_q, die met C' correspondeert onder α, gelijkwaardig is met C. Het is duidelijk dat gelijkwaardige codes dezelfde parameters n, M, d hebben.

Lemma 2.2.5
Elke q-aire (n, M, d)-code C over F_q is gelijkwaardig met een (n, M, d)-code over $\{0, 1, 2, \cdots, q-1\}$ die de vector $\bar{0} = 00\cdots0$ bevat.

Bewijs. Noem α een willekeurige bijectie van F_q op $\{0, 1, 2, \cdots, q-1\}$, en beschouw C^α. Kies in C^α een codewoord $x_1x_2\cdots x_n$ en pas voor elke Ki met $x_i \neq 0$, volgende permutatie toe: $0 \mapsto x_i, x_i \mapsto 0, j \mapsto j$ voor alle $j \neq 0, x_i$. □

Voorbeeld 2.2.6
Wij hernemen Voorbeeld 2.2.1. Daarin zagen wij dat $A_2(5, 3) \geq 4$. Onderstel dat C een $(5, M, 3)$-code is over $F_2 = \{0, 1\}$ met $M \geq 4$. Wegens Lemma 2.2.5 mogen wij veronderstellen dat $\bar{0} = 00000 \in C$. Moesten er twee codewoorden $\bar{x}, \bar{y}$ zijn die ten minste viermaal het symbool 1 bevatten, dan zou $d(\bar{x}, \bar{y}) \leq 2$, een strijdigheid aangezien $d(C) = 3$. Er is dus ten hoogste één codewoord dat ten minste viermaal het symbool 1 bevat. Aangezien $\bar{0} \in C$ is er geen enkel codewoord dat juist eenmaal of tweemaal het symbool 1 bevat. Aangezien $M \geq 4$ zijn er dus ten minste 2 codewoorden die juist driemaal het symbool 1 bevatten, bijvoorbeeld $\bar{x}$ en $\bar{y}$. Omdat $d(\bar{x}, \bar{y}) \geq 3$, zullen $\bar{x}$ en $\bar{y}$ in juist één gemeenschappelijke positie het symbool 1 bevatten. Na eventuele permutatie op de kolommen mogen wij onderstellen dat C volgende vectoren bevat:

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1. \end{array}$$

Nu is het gemakkelijk om aan te tonen dat elk ander codewoord noodzakelijk het woord 11011 is. Hieruit volgt onmiddellijk dat $M = 4$, met andere woorden $A_2(5, 3) = 4$. Ook is tevens aangetoond dat er op gelijkwaardigheid na juist één binaire $(5, 4, 3)$-code bestaat.

Notatie

Is $F_2 = \{0, 1\}$ en zijn $\bar{x} = x_1x_2\cdots x_n, \bar{y} = y_1y_2\cdots y_n$ vectoren in $(F_2)^n$, dan stelt men

$$\bar{x} \cap \bar{y} = (x_1y_1, x_2y_2, \cdots, x_ny_n).$$

De vector $\bar{x} \cap \bar{y}$ noemt men de *intersectie* van $\bar{x}$ en $\bar{y}$.

Definitie 2.2.7
Is $\bar{x} = x_1x_2\cdots x_n$ een vector in $(F_q)^n$, met $F_q = \{0, \lambda_1, \lambda_2, \cdots, \lambda_{q-1}\}$, dan is het *gewicht* $w(\bar{x})$ van $\bar{x}$ het aantal x_i's dat verschillend is van nul.

Stelling 2.2.8
Is $\bar{x}, \bar{y} \in (F_q)^n = V(n, q)$ (dus $F_q = \mathrm{GF}(q)$), dan is

$$d(\bar{x}, \bar{y}) = w(\bar{x} - \bar{y}).$$

Bewijs. De posities waarin $\bar{x}$ en $\bar{y}$ verschillen, zijn juist de posities waarin $\bar{x}-\bar{y}$ verschillend is van nul. □

Lemma 2.2.9
Zijn $\bar{x}$ en $\bar{y}$ vectoren van $(F_2)^n$, dan is

$$d(\bar{x}, \bar{y}) = w(\bar{x}) + w(\bar{y}) - 2w(\bar{x} \cap \bar{y}).$$

Bewijs. Er geldt $d(\bar{x}, \bar{y}) = w(\bar{x} - \bar{y}) = w(\bar{x} + \bar{y})$= (het aantal symbolen 1 in $\bar{x}$) + (het aantal symbolen 1 in $\bar{y}$) – 2(het aantal posities waarin $\bar{x}$ en $\bar{y}$ beide het symbool 1 hebben) $= w(\bar{x}) + w(\bar{y}) - 2w(\bar{x} \cap \bar{y})$. □

Stelling 2.2.10
Onderstel dat $d \in \mathbb{N}$ oneven is. Dan bestaat voor $M > 1$ een binaire (n, M, d)-code als en slechts als een binaire $(n + 1, M, d + 1)$-code bestaat.

Bewijs. Onderstel dat C een binaire (n, M, d)-code is, $M > 1$, met d oneven. De code $\hat{C}$ is de binaire code van lengte $n + 1$ die uit C ontstaat door elk codewoord $\bar{x} = x_1 x_2 \cdots x_n$ te vervangen door $\hat{\bar{x}} = x_1 x_2 \cdots x_{n+1}$, met

$$\sum_{i=1}^{n+1} x_i = 0, \text{ dit is, } x_{n+1} = \sum_{i=1}^{n} x_i \text{ (over GF(2))}.$$

Met andere woorden, $x_{n+1} = 0$ als $w(\bar{x})$ even is en $x_{n+1} = 1$ als $w(\bar{x})$ oneven is. Men zegt dat men $\hat{C}$ uit C verkrijgt door het toevoegen van een *pariteit controlesymbool* (*overall parity check*). Men zegt ook dat $\hat{C}$ de *uitgebreide code* (*extended code*) van C is. Aangezien $w(\hat{\bar{x}})$ even is voor elk codewoord van $\hat{C}$, volgt uit Lemma 2.2.9 dat $d(\hat{\bar{x}}, \hat{\bar{y}})$ even is voor alle $\hat{\bar{x}}, \hat{\bar{y}} \in \hat{C}$. Bijgevolg is $d(\hat{C})$ even. Aangezien $d \leq d(\hat{C}) \leq d + 1$ en aangezien d oneven is, is dus $d(\hat{C}) = d + 1$. Wij besluiten dat $\hat{C}$ een binaire $(n + 1, M, d + 1)$-code is.

Onderstel vervolgens dat C' een binaire $(n+1, M, d+1)$-code is, met d oneven. Stel dat $\bar{x}$ en $\bar{y}$ codewoorden zijn met $d(\bar{x}, \bar{y}) = d+1$. Kies een positie in dewelke $\bar{x}$ en $\bar{y}$ verschillen, en laat deze positie uit alle codewoorden van C' weg. Dan ontstaat een binaire code C'' met lengte n. Zijn $\bar{z}$ en $\bar{u}$ verschillende codewoorden van C', dan zijn de corresponderende woorden van C'' ook verschillend omdat anders $d(\bar{z}, \bar{u}) = 1$ hetgeen strijdig is met $d(C')$ even. Bijgevolg is C'' een binaire (n, M, d)-code. □

Gevolg 2.2.11
Is d oneven, dan geldt

$$A_2(n + 1, d + 1) = A_2(n, d).$$

Voorbeeld 2.2.12
Wegens Voorbeeld 2.2.6 is $A_2(5, 3) = 4$, zodat ook $A_2(6, 4) = 4$.

2.3 Perfecte codes en de bolpakkingsgrens

Definitie 2.3.1
De *bol* met *middelpunt* $\bar{u} \in (F_q)^n$ en straal $R \in \mathbb{N}$, $R \leq n$, is de verzameling

$$S(\bar{u}, R) = \{\bar{x} \in (F_q)^n \parallel d(\bar{x}, \bar{u}) \leq R\}.$$

Lemma 2.3.2
De bol $S(\bar{u}, R)$ *in* $(F_q)^n$ *bevat juist*

$$\left(\begin{array}{c} n \\ 0 \end{array}\right) + \left(\begin{array}{c} n \\ 1 \end{array}\right)(q-1) + \left(\begin{array}{c} n \\ 2 \end{array}\right)(q-1)^2 + \cdots + \left(\begin{array}{c} n \\ R \end{array}\right)(q-1)^R$$

vectoren.

Bewijs. Kies een vector $\bar{u}$ in $(F_q)^n$. Het aantal vectoren $\bar{x}$ waarvoor $d(\bar{u}, \bar{x}) = 0$ is 1; het aantal vectoren $\bar{x}$ waarvoor $d(\bar{u}, \bar{x}) = 1$ is $n(q-1)$; het aantal vectoren $\bar{x}$ waarvoor $d(\bar{u}, \bar{x}) = 2$ is $\left(\begin{array}{c} n \\ 2 \end{array}\right)(q-1)^2$; $\cdots$; het aantal vectoren $\bar{x}$ waarvoor $d(\bar{u}, \bar{x}) = m$ is $\left(\begin{array}{c} n \\ m \end{array}\right)(q-1)^m$ (m posities kunnen op $\left(\begin{array}{c} n \\ m \end{array}\right)$ manieren gekozen worden en in elk van die posities kan de coördinaat van $\bar{x}$ op $q-1$ manieren verschillend van de corresponderende coördinaat van $\bar{u}$ gekozen worden); $\cdots$; het aantal vectoren $\bar{x}$ waarvoor $d(\bar{u}, \bar{x}) = R$ is $\left(\begin{array}{c} n \\ R \end{array}\right)(q-1)^R$. Wij besluiten dat

$$|S(\bar{u}, R)| = \left(\begin{array}{c} n \\ 0 \end{array}\right) + \left(\begin{array}{c} n \\ 1 \end{array}\right)(q-1) + \left(\begin{array}{c} n \\ 2 \end{array}\right)(q-1)^2 + \cdots + \left(\begin{array}{c} n \\ R \end{array}\right)(q-1)^R.$$

□

Lemma 2.3.3
Is $d(C) = 2t+1$ *of* $2t+2$*, dan zijn elke twee bollen* $S(\bar{x}, t)$ *en* $S(\bar{y}, t)$*, met* $\bar{x}, \bar{y}$ *verschillende elementen van* C*, disjunct.*

Bewijs. Onderstel dat $S(\bar{x}, t) \cap S(\bar{y}, t)$ de vector $\bar{z}$ bevat. Dan is $d(\bar{x}, \bar{y}) \leq d(\bar{x}, \bar{z}) + d(\bar{y}, \bar{z}) \leq t + t = 2t$, een strijdigheid aangezien $d(\bar{x}, \bar{y}) \geq 2t + 1$. □

Opmerking 2.3.4
Onderstel dat $d(C) = 2t+1$ of $2t+2$, en dat $\bar{x} \in C$ verzonden wordt. Worden ten hoogste t fouten gemaakt, dan zal de ontvangen vector $\bar{y}$ tot de bol $S(\bar{x}, t)$ behoren. De vector $\bar{y}$ ligt dan dichter bij het middelpunt $\bar{x}$ van $S(\bar{x}, t)$, dan bij elk ander codewoord. Met dichtste gebuur decodering zal $\bar{y}$ gedecodeerd worden als het middelpunt van de bol $S(\bar{x}, t)$.

Stelling 2.3.5 (De bolpakkingsgrens of de Hamming grens)
Elke q*-aire* (n, M, d)*-code,* $M > 1$*, met* $d = 2t + 1$ *of* $d = 2t + 2$*, voldoet aan*

$$M\left[\left(\begin{array}{c} n \\ 0 \end{array}\right) + \left(\begin{array}{c} n \\ 1 \end{array}\right)(q-1) + \left(\begin{array}{c} n \\ 2 \end{array}\right)(q-1)^2 + \cdots + \left(\begin{array}{c} n \\ t \end{array}\right)(q-1)^t\right] \leq q^n. \qquad (2.1)$$

Bewijs. Onderstel dat C een q-aire (n, M, d)-code is, $M > 1$, met $d = 2t+1$ of $d = 2t+2$. De M bollen $S(\bar{x}, t)$ met middelpunt $\bar{x} \in C$ en straal t zijn dan onderling disjunct wegens Lemma 2.3.3. Bijgevolg is, rekening houdend met Lemma 2.3.2,

$$|\bigcup_{\bar{x}\in C} S(\bar{x}, t)| = M\left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right].$$

Anderzijds bevat de unie van deze bollen ten hoogste $|(F_q)^n| = q^n$ vectoren. Hieruit volgt onmiddellijk de ongelijkheid (2.1). □

Gevolgen 2.3.6

(i) Elke binaire (n, M, d)-code, $M > 1$, met $d = 2t + 1$ of $d = 2t + 2$, voldoet aan

$$M\left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right] \leq 2^n. \tag{2.2}$$

(ii) Is $d = 2t + 1$ of $2t + 2$, dan is

$$A_q(n, d) \leq q^n / \left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right]. \tag{2.3}$$

In het bijzonder is voor $d = 2t + 1$ of $2t + 2$,

$$A_2(n, d) \leq 2^n / \left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right]. \tag{2.4}$$

Voorbeelden 2.3.7

Uit (2.4) volgt dat $A_2(5, 3) \leq 2^5/6$, zodat $A_2(5, 3) \leq 5$. In Voorbeeld 2.2.6 zagen wij dat $A_2(5, 3) = 4$.

Perfecte codes

Wordt voor een code C de bolpakkingsgrens bereikt, dit wil zeggen, hebben wij voor C gelijkheid in (2.1), dan noemt men C een *perfecte code*. Voor dergelijke code C is $(F_q)^n$ de unie van de disjuncte bollen $S(\bar{x}, t), \bar{x} \in C$. Elke ontvangen vector $\bar{y} \in F_q^n$ wordt dan gedecodeerd als het middelpunt $\bar{x} \in C$ van de unieke bol $S(\bar{x}, t)$ die $\bar{y}$ bevat. Is $|C| = 1$, dan noemt men bij definitie C perfect. De *triviale* perfecte codes zijn de singletons, de gehele verzameling $(F_q)^n$ (hier is $t = 0$), en de binaire herhalingscodes met oneven lengte n (dit zijn perfecte binaire $(n, 2, n)$-codes).

Voor een perfecte code C, met $|C| > 1$, is $d(C)$ noodzakelijk oneven. Inderdaad, onderstel dat C perfect is, met $d(C) = 2t+2$. Kies een woord $\bar{z}$ met $d(\bar{x}, \bar{z}) = t+1, \bar{x} \in C$. Moest $\bar{z} \in S(\bar{y}, t)$, met $\bar{y}$ een codewoord verschillend van $\bar{x}$, dan zou $d(\bar{x}, \bar{y}) \leq d(\bar{x}, \bar{z}) +$

$d(\bar{y}, \bar{z}) \leq t + 1 + t = 2t + 1$, een strijdigheid aangezien $d(C) = 2t + 2$. Bijgevolg is $\bar{z}$ een woord dat tot geen enkele van de bollen $S(\bar{u}, t)$, met $\bar{u} \in C$, behoort, een strijdigheid.

In Hoofdstuk 9 komen wij op de perfecte codes terug. Om Hoofdstuk 2 te besluiten geven wij een voorbeeld van een niet-triviale perfecte code.

Voorbeeld 2.3.8
Beschouw het projectieve vlak PG$(2, 2)$ over het Galois veld GF(2). De punten van PG$(2, 2)$ zijn: $p_1(1, 0, 0), p_2(0, 1, 0), p_3(0, 1, 1), p_4(1, 1, 1), p_5(1, 0, 1)$,
$p_6(1, 1, 0), p_7(0, 0, 1)$. De rechten van PG$(2, 2)$ hebben als vergelijkingen: $L_1 : X_1 = 0, L_2 : X_2 = 0, L_3 : X_0 = 0, L_4 : X_1 + X_2 = 0, L_5 : X_0 + X_2 = 0, L_6 : X_0 + X_1 + X_2 = 0, L_7 : X_0 + X_1 = 0$. Noem $A = (a_{ij})_{1 \leq i,j \leq 7}$ de 7×7-matrix waarvoor $a_{ij} = 1$ als p_i op L_j ligt, en $a_{ij} = 0$ als p_i niet op L_j ligt. Dan is

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

Men zegt dat A een *incidentiematrix* (*incidence matrix*) is van het projectieve vlak PG$(2, 2)$. Beschouw nu de binaire code C van lengte 7, met als codewoorden

$$\begin{array}{lcccccccc} \bar{0} & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \bar{1} & = & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \bar{a}_1 & = & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ \bar{a}_2 & = & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \bar{a}_3 & = & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ \bar{a}_4 & = & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \bar{a}_5 & = & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ \bar{a}_6 & = & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ \bar{a}_7 & = & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \bar{b}_1 & = & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \bar{b}_2 & = & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \bar{b}_3 & = & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \bar{b}_4 & = & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ \bar{b}_5 & = & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \bar{b}_6 & = & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \bar{b}_7 & = & 0 & 1 & 0 & 1 & 1 & 1 & 0. \end{array}$$

Hier is dus $M = 16$. De codewoorden $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_7$ zijn de rijen van de matrix A; de codewoorden $\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_7$ verkrijgt men uit de respectievelijke codewoorden $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_7$

als men overal 0 door 1 vervangt en 1 door 0 vervangt (met andere woorden $\bar{b}_i = \bar{1} + \bar{a}_i$, $i = 1, 2, \cdots, 7$). Wij tonen nu aan dat $d(C) = 3$. Omdat PG$(2, 2)$ een projectief vlak is gaat door elke twee verschillende punten juist één rechte, met andere woorden elke twee verschillende rijen van A hebben in juist één gemeenschappelijke positie het symbool 1. Uit Lemma 2.2.9 volgt nu dat

$$d(\bar{a}_i, \bar{a}_j) = w(\bar{a}_i) + w(\bar{a}_j) - 2w(\bar{a}_i \cap \bar{a}_j) = 3 + 3 - 2.1 = 4 \quad (i \neq j).$$

Aangezien $d(\bar{a}_i, \bar{a}_j) = d(\bar{b}_i, \bar{b}_j)$, is ook $d(\bar{b}_i, \bar{b}_j) = 4 \quad (i \neq j)$. Verder is $d(\bar{0}, \bar{a}_i) = 3, d(\bar{1}, \bar{a}_i) = 4, d(\bar{1}, \bar{b}_i) = 4, d(\bar{0}, \bar{b}_i) = 3, d(\bar{0}, \bar{1}) = 7$. Vanzelfsprekend is $d(\bar{a}_i, \bar{b}_i) = 7$. De codewoorden $\bar{a}_i$ en $\bar{b}_j$ $(i \neq j)$ verschillen in juist deze posities waar $\bar{a}_i$ en $\bar{a}_j$ overeenkomen. Bijgevolg is $d(\bar{a}_i, \bar{b}_j) = 7 - d(\bar{a}_i, \bar{a}_j) = 7 - 4 = 3 \quad (i \neq j)$. Zo hebben wij aangetoond dat $d(C) = 3$. De code C is dus een binaire $(7, 16, 3)$-code.

Uit $16\left[\begin{pmatrix} 7 \\ 0 \end{pmatrix} + \begin{pmatrix} 7 \\ 1 \end{pmatrix}\right] = 2^7$ volgt nu dat wij gelijkheid hebben in (2.1), zodat C een perfecte code is. Hieruit volgt tevens dat $A_2(7, 3) = 16$.

Opmerking 2.3.9
In het hoofdstuk over perfecte codes zullen wij zien dat perfecte codes zeldzaam zijn.

Hoofdstuk 3

Inleiding tot de lineaire codes

3.1 Lineaire codes

In dit hoofdstuk onderstellen wij steeds dat het alfabet F_q het Galois veld GF(q) is.

Definitie 3.1.1
Een *lineaire code* over GF(q) is een deelruimte van de vectorruimte $V(n, q)$.

Een niet-ledige deelverzameling C van $V(n, q)$ is dus een lineaire code a.s.a.

(i) $\bar{u} + \bar{v} \in C$, voor alle $\bar{u}, \bar{v} \in C$, en

(ii) $a\bar{u} \in C$, voor alle $\bar{u} \in C, a \in$GF(q).

Een binaire code is lineair a.s.a. de som van elke twee codewoorden opnieuw een codewoord is. De codes C_1, C_2, C_3 uit 1.3 en de niet-triviale perfecte code uit 2.3 bijvoorbeeld zijn lineair.

Opmerkingen 3.1.2

(i) Is C lineair, dan geldt $\bar{0} \in C$.

(ii) Lineaire codes worden soms "*groep codes*" genoemd.

Definitie 3.1.3
Elke matrix waarvan de rijen een basis vormen voor de lineaire code C noemen wij een *voortbrengende matrix (generator matrix*) van C.

Notaties
Als C een k-dimensionale deelruimte is van $V(n, q)$, dan wordt de lineaire code C een $[n, k]$-code genoemd, of soms, als we de minimum afstand d willen specifiëren, een $[n, k, d]$-*code*. Vanzelfsprekend is elke q-aire $[n, k, d]$-code ook een q-aire (n, q^k, d)-code, maar niet omgekeerd. Elke voortbrengende matrix van een $[n, k]$-code over GF(q) is een $k \times n$-matrix over GF(q).

Definitie 3.1.4
Het *minimum gewicht* $w(C)$ van een lineaire code C is het minimum der gewichten van alle codewoorden $\bar{x} \in C - \{\bar{0}\}$.

Stelling 3.1.5
Voor elke lineaire code C geldt

$$d(C) = w(C).$$

Bewijs. Er bestaan codewoorden $\bar{x}, \bar{y} \in C, \bar{x} \neq \bar{y}$, waarvoor $d(C) = d(\bar{x}, \bar{y})$. Wegens Stelling 2.2.8 is $d(\bar{x}, \bar{y}) = w(\bar{x} - \bar{y})$. Aangezien C lineair is, geldt $\bar{x} - \bar{y} \in C$, zodat $w(\bar{x} - \bar{y}) \geq w(C)$. Dus is $d(C) \geq w(C)$.

Er bestaat een codewoord $\bar{x} \in C - \{\bar{0}\}$, waarvoor $w(C) = w(\bar{x})$. Aangezien C lineair is, geldt $\bar{0} \in C$, zodat $w(\bar{x}) = w(\bar{x} - \bar{0}) = d(\bar{x}, \bar{0}) \geq d(C)$. Dus is $w(C) \geq d(C)$.

Wij besluiten dat $d(C) = w(C)$. □

Voordelen van lineaire codes

(i) Voor een algemene code met M codewoorden is het mogelijk dat wij $M(M-1)/2$ afstanden moeten berekenen om de minimum afstand te vinden. Voor een lineaire code C met M codewoorden is het voldoende de gewichten te bepalen van de $M-1$ codewoorden in $C - \{\bar{0}\}$ om de minimum afstand te vinden.

(ii) Om een niet-lineaire code C vast te leggen is het mogelijk dat wij de M codewoorden moeten opsommen. Een lineaire $[n, k]$-code C is volledig bepaald door het geven van een voortbrengende $k \times n$-matrix. De $[3, 2, 2]$-code C_2 van Voorbeeld 1.3.1 wordt volledig bepaald door de voortbrengende matrix

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$

de $[7, 4, 3]$-code van Voorbeeld 2.3.8 door de voortbrengende matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix},$$

de q-aire herhalingscode van lengte n over GF(q) is een $[n, 1, n]$-code met voortbrengende matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}.$$

(iii) In de volgende twee hoofdstukken zullen wij zien dat er eenvoudige procedures bestaan voor het coderen en decoderen bij lineaire codes.

Nadelen van lineaire codes

(i) Lineaire q-aire codes zijn niet gedefinieerd indien q geen priemmacht is. In de praktijk is het dikwijls zo dat q-aire codes, met q geen priemmacht, kunnen afgeleid worden uit lineaire codes over een groter alfabet.

In Hoofdstuk 5 zullen wij een goede decimale code, dat is een 10-aire code, beschrijven die afgeleid wordt uit een lineaire 11-aire code.

(ii) Vanzelfsprekend is de lineariteit een beperking. Het blijkt echter dat codes die in een bepaald opzicht optimaal zijn dikwijls lineair zijn, of dat er lineaire codes met dezelfde parameters bestaan. Bijvoorbeeld, voor elk stel parameters waarvoor een niet-triviale perfecte code gekend is, is eveneens een lineaire perfecte code met die parameters gekend.

Regelmatig is ook een niet-lineaire code over $\mathrm{GF}(q)$ gemakkelijk af te leiden uit een lineaire code over hetzelfde alfabet. De ISBN code uit 1.4 bijvoorbeeld is een deelverzameling van de lineaire 11-aire code

$$\{x_1x_2\ldots x_{10} \in V(10,11) \parallel \sum_{i=1}^{10} ix_i = 0\}.$$

3.2 Gelijkwaardigheid van lineaire codes

Zijn C en C' gelijkwaardige codes over $\mathrm{GF}(q)$ en is C lineair, dan is niet noodzakelijk C' lineair. Daarom wordt voor lineaire codes een andere definitie voor gelijkwaardigheid gegeven. Men zegt dat de lineaire codes C en C' over $\mathrm{GF}(q)$ gelijkwaardig zijn als C' uit C kan verkregen worden door een opeenvolging van bewerkingen van de volgende gedaante:

(i) een permutatie op de posities van de code;

(ii) in een vaste positie vermenigvuldiging van al de elementen met een scalair in $\mathrm{GF}(q) - \{0\}$.

Stelling 3.2.1
Twee $k \times n$-matrices van rang k over $\mathrm{GF}(q)$ brengen gelijkwaardige lineaire $[n,k]$-codes over $\mathrm{GF}(q)$ voort a.s.a. de tweede matrix uit de eerste kan verkregen worden door een opeenvolging van bewerkingen van de volgende gedaante :

(R1) een permutatie van de rijen;

(R2) vermenigvuldiging van een rij met een scalair in $\mathrm{GF}(q) - \{0\}$;

(R3) optelling bij een rij van het product van een rij met een scalair;

(C1) een permutatie van de kolommen;

(C2) vermenigvuldiging van een kolom met een scalair in $\mathrm{GF}(q) - \{0\}$.

Bewijs. De rijbewerkingen (R1), (R2) en (R3) bewaren de onafhankelijkheid van de rijen en vervangen een voortbrengende matrix van een lineaire code door een voortbrengende matrix van dezelfde code. De kolombewerkingen (C1) en (C2) vervangen een voortbrengende matrix van een lineaire code door een voortbrengende matrix van een gelijkwaardige code. □

3.3 Standaardgedaante van een voortbrengende matrix

Definitie 3.3.1
Is de voortbrengende matrix G van de $[n, k]$-code C van de gedaante

$$[I_k \quad A]$$

met I_k de eenheidsmatrix van de orde k en A een $k \times (n-k)$-matrix, dan zegt men dat G in *standaard gedaante* is.

Stelling 3.3.2
Onderstel dat G een voortbrengende matrix is van de $[n, k]$-code C. Door een opeenvolging van bewerkingen van de gedaante (R1), (R2), (R3) en (C1) kan G in standaard gedaante gebracht worden.

Bewijs. Onderstel dat G na een aantal stappen reeds in volgende gedaante is gebracht

$$\begin{bmatrix} 1 & 0 & \dots & 0 & g_{1j} & \dots & g_{1n} \\ 0 & 1 & \dots & 0 & g_{2j} & \dots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & g_{j-1,j} & \dots & g_{j-1,n} \\ 0 & 0 & \dots & 0 & g_{jj} & \dots & g_{jn} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & g_{kj} & \dots & g_{kn} \end{bmatrix}.$$

De rijen van deze matrix stellen wij voor door $\bar{r}_1, \bar{r}_2, \dots, \bar{r}_k$, de kolommen door $\bar{c}_1, \bar{c}_2, \dots, \bar{c}_n$. Wij voeren nu volgende stappen uit.

Stap 1. Is $g_{jj} \neq 0$, dan gaan wij onmiddellijk naar Stap 2. Is $g_{jj} = 0$, en is voor een zekere $i > j$ voldaan aan $g_{ij} \neq 0$, dan verwisselen wij $\bar{r}_i$ en $\bar{r}_j$. Is $g_{jj} = 0$, en is $g_{ij} = 0$ voor alle $i > j$, dan kiezen wij een h waarvoor $g_{jh} \neq 0$ en verwisselen $\bar{c}_j$ en $\bar{c}_h$. In de nieuwe matrix zullen wij het element op de ide rij en de jde kolom nog altijd voorstellen door g_{ij}.

Stap 2. Nu is $g_{jj} \neq 0$. Wij vermenigvuldigen $\bar{r}_j$ met g_{jj}^{-1}. In de nieuwe matrix wordt het element op de ide rij en jde kolom nog altijd voorgesteld door g_{ij}.

Stap 3. Nu hebben wij $g_{jj} = 1$. Voor elke $i = 1, 2, \dots, k$, met $i \neq j$, vervangen wij nu $\bar{r}_i$ door $\bar{r}_i - g_{ij}\bar{r}_j$.

Thans heeft kolom $\bar{c}_j$ de gewenste gedaante.

Na toepassing van deze procedure voor $j = 1, 2, \ldots, k$ heeft de voortbrengende matrix de standaard gedaante. □

Opmerkingen 3.3.3

(i) Indien G in standaard gedaante G' kan gebracht worden uitsluitend met rijbewerkingen (R1),(R2),(R3) (dit is het geval a.s.a. de eerste k kolommen van G lineair onafhankelijk zijn), dan zal G' dezelfde code als G voortbrengen. Indien eveneens (C1) gebruikt wordt, dan zal G' een code voortbrengen die gelijkwaardig is met C. De procedure beschreven in voorgaand bewijs is zodanig dat, indien mogelijk, G' eveneens de gegeven code C voortbrengt.

(ii) In vele gevallen suggereert de gedaante van G een snellere manier om in standaard gedaante gebracht te worden.

Voorbeelden 3.3.4

(i) Beschouw de matrix

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

Verwisselen van de rijen geeft ons de standaard gedaante

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

(ii) Beschouw volgende voortbrengende matrix van de binaire $[7, 4, 3]$-code van Voorbeeld 2.3.8 :

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} \\ \longrightarrow \\ \bar{r}_2 \to \bar{r}_2 - \bar{r}_1 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{matrix} \\ \longrightarrow \\ \bar{r}_2 \to \bar{r}_3, \bar{r}_3 \to \bar{r}_2 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{matrix} \\ \longrightarrow \\ \bar{r}_1 \to \bar{r}_1 - \bar{r}_2 \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{matrix} \\ \longrightarrow \\ \bar{r}_2 \to \bar{r}_2 - \bar{r}_3, \bar{r}_4 \to \bar{r}_4 - \bar{r}_3 \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{matrix} \\ \longrightarrow \\ \bar{r}_1 \to \bar{r}_1 - \bar{r}_4 \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

(iii) Beschouw de $[7, 3]$-code over GF(3) met voortbrengende matrix

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

Door een permutatie van de kolommen vinden wij volgende matrix G' in standaard gedaante :

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

Hoofdstuk 4

Coderen en decoderen bij lineaire codes

4.1 Coderen bij lineaire codes

Beschouw een $[n, k]$-code C over GF(q) met voortbrengende matrix G. De code C bevat q^k codewoorden en kan dus gebruikt worden om q^k verschillende berichten te versturen. We kunnen deze berichten identificeren met de q^k vectoren van $V(k, q)$ en we *coderen* de *berichtvector (message vector)* $\bar{u} = u_1 u_2 \dots u_k \in V(k, q)$ door hem rechts met G te vermenigvuldigen. Zijn $\bar{r}_1, \bar{r}_2, \dots, \bar{r}_k$ de rijen van G, dan wordt $\bar{u}$ dus gecodeerd als

$$\bar{u}G = \sum_{i=1}^{k} u_i \bar{r}_i \in C.$$

De *codeerfunctie* $\bar{u} \mapsto \bar{u}G$ is een niet-singuliere lineaire afbeelding van $V(k, q)$ op de k-dimensionale deelruimte C van $V(n, q)$. Het getal $n - k = r$ noemt men de *overtalligheid (redundancy)* van de code C.

Onderstel nu dat G in standaard gedaante is, dat is, onderstel dat $G = [I_k \quad A]$, met $A = [a_{ij}]$ een $k \times (n - k)$-matrix over GF(q). De berichtvector $\bar{u} = u_1 u_2 \dots u_k$ wordt dan gecodeerd als

$$\bar{x} = \bar{u}G = x_1 x_2 \dots x_k x_{k+1} \dots x_n,$$

met $x_i = u_i, 1 \leq i \leq k$ en

$$x_{k+i} = \sum_{j=1}^{k} a_{ji} u_j, 1 \leq i \leq n - k.$$

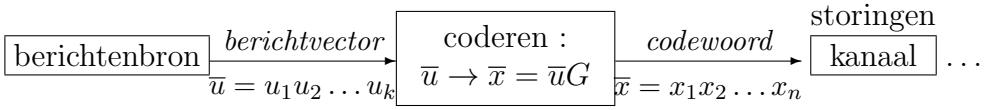
De coördinaten $x_1, \dots, x_k$ noemt men dan de *berichtsymbolen (message digits)*, en de coördinaten $x_{k+1}, \dots, x_n$ de *controlesymbolen (check digits)*.

Voorbeeld 4.1.1
Herneem de matrix

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

uit Voorbeeld 3.3.4 (ii). Een berichtvector $\bar{u} = u_1u_2u_3u_4$ wordt dan gecodeerd als $\bar{x} = u_1u_2u_3u_4x_5x_6x_7$ met $x_5 = u_1+u_3+u_4, x_6 = u_1+u_2+u_3, x_7 = u_2+u_3+u_4$. De berichtvector 0111 bijvoorbeeld wordt gecodeerd als 0111001.

Samenvatting 4.1.2
Wat coderen betreft hebben wij dus het volgende schema



4.2 Decoderen bij lineaire codes

Onderstel dat het codewoord $\bar{x} = x_1x_2 \ldots x_n \in C$, met C lineair, verzonden wordt, en dat de vector $\bar{y} = y_1y_2 \ldots y_n$ ontvangen wordt. De *foutvector* (*error vector*) $\bar{e}$ is dan bij definitie de vector

$$\bar{e} = \bar{y} - \bar{x} = e_1e_2 \ldots e_n.$$

Bij ontvangst van $\bar{y}$ moet de persoon die decodeert beslissen welk codewoord verzonden werd. Het volgende dichtste gebuur decodering schema werd ontworpen door Slepian in 1960.

De lineaire code C is een additieve deelgroep van de additieve groep van $V(n, q)$. Is C een $[n, k]$-code over GF(q), dan heeft de additieve deelgroep C q^{n-k} nevenklassen $\bar{a} + C$. De *nevenklasseleider (coset leader)* van $\bar{a} + C$ is een vector van kleinste gewicht in die nevenklasse. De nevenklasseleiders stellen wij voor door $\bar{0}, \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s$ met $s = q^{n-k} - 1$ ($\bar{0}$ is de nevenklasseleider van C). Er geldt dan

$$V(n, q) = (\bar{0} + C) \cup (\bar{a}_1 + C) \cup \ldots \cup (\bar{a}_s + C).$$

Een *(Slepian) standaard rooster ((Slepian) standard array)* voor de code C is dan een $q^{n-k} \times q^k$-rooster met als elementen alle vectoren van $V(n, q)$, met als eerste rij de elementen van C te beginnen met $\bar{0}$ en met als $(i + 1)$de rij de elementen van $\bar{a}_i + C$ waarbij $\bar{z} \in C$ en $\bar{a}_i + \bar{z}$ zich in dezelfde kolom bevinden, $i = 1, 2, \ldots, s$. De eerste kolom bestaat dus uit de nevenklasseleiders $\bar{0}, \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s$. In de praktijk kan men als volgt te werk gaan :

Stap 1. De eerste rij bestaat uit de elementen van C, te beginnen met $\bar{0}$.

Stap 2. Kies een vector $\bar{a}_1 \notin C$ van minimum gewicht. Als tweede rij nemen wij dan $\bar{a}_1 + C$ waarbij $\bar{z} \in C$ en $\bar{a}_1 + \bar{z}$ zich in dezelfde kolom bevinden.

Stap 3. Kies een vector $\bar{a}_2 \notin C \cup (\bar{a}_1 + C)$ van minimum gewicht. Als derde rij nemen wij dan $\bar{a}_2 + C$ waarbij $\bar{z} \in C$ en $\bar{a}_2 + \bar{z}$ zich in dezelfde kolom bevinden.

Stap 4. Doe zo voort tot alle vectoren van $V(n, q)$ opgebruikt zijn.

In een standaard rooster is dus elk element de som van het codewoord in dezelfde kolom en de nevenklasseleider op de eerste plaats in de rij van dit element.

Voorbeeld 4.2.1
Beschouw de binaire $[4, 2]$-code voortgebracht door de matrix

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

Dan is $C = \{0000, 1011, 0110, 1101\}$. Een standaard rooster voor de code C is dan het volgende 4×4-rooster :
codewoorden :

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100.

De nevenklasseleiders zijn de vectoren 0000, 1000, 0100, 0001. Merk op dat er in de derde nevenklasse een andere keuze was voor nevenklasseleider, namelijk 0010.

Wij tonen nu aan hoe men decodeert met een standaard rooster. De vector $\bar{x} \in C$ werd verzonden en de vector $\bar{y}$ werd ontvangen, met $\bar{e} = \bar{y} - \bar{x}$. Bijgevolg behoren $\bar{y}$ en $\bar{e}$ tot een zelfde nevenklasse van C. Met dichtste gebuur decodering decodeert men $\bar{y}$ als een codewoord $\bar{x}'$ waarvoor $\bar{e}' = \bar{y} - \bar{x}'$ het kleinst mogelijke gewicht heeft, waarvoor dus $\bar{e}'$ een element is met het kleinste gewicht in de nevenklasse van $\bar{y}$. Voor $\bar{e}'$ nemen we dan de nevenklasseleider $\bar{a}_i$ in de rij van $\bar{y}$, m.a.w. we decoderen $\bar{y}$ als $\bar{x}' = \bar{y} - \bar{a}_i$, dus als het codewoord in dezelfde kolom als $\bar{y}$. De foutvectoren die verbeterd worden zijn dus juist de nevenklasseleiders.

Samengevat
De ontvangen vector $\bar{y}$ wordt gedecodeerd als het codewoord in dezelfde kolom als $\bar{y}$.

Voorbeeld 4.2.2
Wij hernemen Voorbeeld 4.2.1. Eén enkele fout zal verbeterd worden indien ze voorkomt in de eerste, tweede of vierde positie; ze zal niet verbeterd worden indien ze voorkomt in de derde positie

	Bericht	Codewoord	Kanaal	Ontvangen vector	Gedecodeerd woord	Ontvangen bericht
(a)	01	0110	0110	0111	0110	01
(b)	01	0110	0110	0100	0000	00

Perfecte codes
Onderstel dat $d(C) = 2t + 1$ of $2t + 2$, zodat C tot t fouten kan verbeteren. Onderstel dat $\bar{v}$ en $\bar{v}'$ verschillende vectoren van gewicht $\leq t$ zijn. Dan is $d(\bar{v}, \bar{v}') = w(\bar{v} - \bar{v}') \leq 2t$ zodat $\bar{v} - \bar{v}' \notin C$. Bijgevolg behoren $\bar{v}$ en $\bar{v}'$ tot verschillende nevenklassen van C. Hieruit volgt dat alle vectoren van gewicht $\leq t$ nevenklasseleiders zijn.

Onderstel nu dat C perfect is. Elke vector $\bar{y}$ behoort dan tot één enkele bol met straal t en met als middelpunt een codewoord $\bar{x}$. Bijgevolg behoort $\bar{y}$ tot een nevenklasse met als leider een vector met gewicht $\leq t$. Wij besluiten dat er geen andere nevenklasseleiders zijn dan alle vectoren met gewicht $\leq t$. In het geval van een perfecte code kunnen wij alle nevenklasseleiders dus onmiddellijk opschrijven.

Opmerkingen 4.2.3

(i) In de praktijk is het hierboven beschreven decodeer schema te traag voor grote codes en moeten teveel elementen opgeslagen worden. Dit kan vermeden worden door toepassing van "syndroom decodering"; zie volgend hoofdstuk.

(ii) In 4.2.2(b) werden de berichtsymbolen 01 niet gewijzigd door storingen, en nochtans werd, na decodering, een verkeerd bericht 00 ontvangen. Dit is een voorbeeld waarbij toevoegen van overtalligheid er de oorzaak van was dat een verkeerd bericht werd ontvangen. Om te besluiten hoe goed een code is moeten wij de waarschijnlijkheid berekenen dat een ontvangen vector gedecodeerd wordt als het codewoord dat werd verzonden.

4.3 Waarschijnlijkheid van foutverbetering

Eenvoudigheidshalve beperken wij ons hier tot binaire lineaire codes. Onderstel dat het kanaal binair symmetrisch is met symboolfout waarschijnlijkheid p. In 1.3 zagen we dat de waarschijnlijkheid dat de foutvector een gegeven vector van gewicht i is, gegeven wordt door $p^i(1-p)^{n-i}$.

Stelling 4.3.1
Beschouw een binaire $[n, k]$-code C en onderstel dat α_i het aantal nevenklasseleiders van gewicht i is, $i = 0, 1, 2, \ldots, n$. De waarschijnlijkheid $P_{corr}(C)$ dat bij standaard rooster decodering een ontvangen vector gedecodeerd wordt als het verzonden codewoord, is dan gelijk aan

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}.$$

Bewijs. $P_{\text{corr}}(C)$ = waarschijnlijkheid dat de foutvector $\bar{e}$ tot de verzameling $\{\bar{0}, \bar{a}_1, \bar{a}_2, \ldots\}$ der nevenklasseleiders behoort. Dus is

$$\begin{aligned} P_{\text{corr}}(C) &= \sum_{i=0}^{s} P(\bar{e} = \bar{a}_i), \text{ met } \bar{a}_0 = \bar{0} \text{ en } s = q^{n-k} - 1 \\ &= \sum_{i=0}^{s} p^{w(\bar{a}_i)}(1-p)^{n-w(\bar{a}_i)} \\ &= \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}. \end{aligned}$$

□

Voorbeeld 4.3.2
Wij hernemen Voorbeeld 4.2.1. Hier is $\alpha_0 = 1, \alpha_1 = 3, \alpha_2 = \alpha_3 = \alpha_4 = 0$. Dus is

$$P_{\text{corr}}(C) = (1-p)^4 + 3p(1-p)^3 = (1-p)^3(1+2p).$$

Voor $p = 0,01$ wordt dit

$$P_{\text{corr}}(C) = 0,9897.$$

De woordfout waarschijnlijkheid, dit is de waarschijnlijkheid op het maken van een foutieve decodering, is dus

$$P_{\text{err}}(C) = 1 - P_{\text{corr}}(C) = 0,0103.$$

Zonder coderen zou de waarschijnlijkheid op het ontvangen van een verkeerd bericht gelijk geweest zijn aan $1-(1-p)^2$; voor $p = 0,01$ is dit $0,0199$, dus ongeveer tweemaal $0,0103$.

Opmerking 4.3.3
Voor $0 \leq i \leq t$ is $\alpha_i = \binom{n}{i}$ (dit is het aantal vectoren met gewicht i; zie 4.2). Voor $i > t$ is het dikwijls zeer moeilijk om α_i te berekenen. In het geval van een perfecte code is $\alpha_i = 0$ voor $i > t$.

4.4 Waarschijnlijkheid van foutdetectie

Wij beperken ons opnieuw tot binaire lineaire codes. Het is duidelijk dat de ontvanger geen aanwezige fouten zal detecteren als en slechts als de ontvangen vector $\bar{y}$ een codewoord is verschillend van het codewoord $\bar{x}$ dat werd verzonden, dat is, als en slechts als $\bar{y} - \bar{x} = \bar{e}$ een codewoord verschillend van $\bar{0}$ is. De waarschijnlijkheid $P_{\text{undetec}}(C)$ dat een verkeerd codewoord ontvangen wordt, wordt dus gegeven door volgende stelling.

Stelling 4.4.1
Beschouw een binaire $[n,k]$-code C en onderstel dat A_i het aantal codewoorden van gewicht i is. De waarschijnlijkheid dat er een fout optreedt tijdens transmissie die niet gedetecteerd wordt, is dan

$$P_{undetec}(C) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}.$$

Bewijs. Volgt onmiddellijk uit het feit dat $P_{\text{undetec}}(C)$ de waarschijnlijkheid is dat de foutvector een codewoord verschillend van $\bar{0}$ is. □

Opmerking 4.4.2
De sommatie begint hier vanaf 1, terwijl in $P_{\text{corr}}(C)$ de sommatie vanaf 0 begint.

Voorbeeld 4.4.3
Wij hernemen opnieuw Voorbeeld 4.2.1. Hier is

$$P_{\text{undetec}}(C) = p^2(1-p)^2 + 2p^3(1-p) = p^2 - p^4.$$

Voor $p = 0,01$ wordt dit

$$P_{\text{undetec}}(C) = 0,00009999.$$

Dus bij ongeveer 1 op 10.000 verkeerde berichten gaan geen fouten gedetecteerd worden.

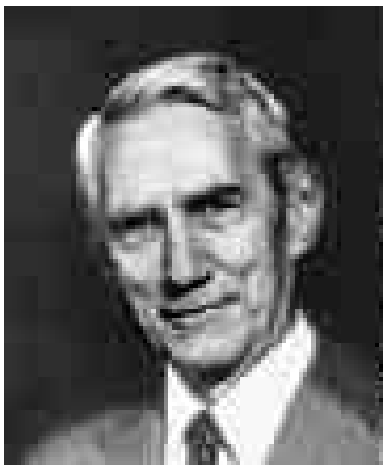
Wij zouden telkens om retransmissie kunnen vragen wanneer fouten gedetecteerd worden. Dit veroorzaakt vanzelfsprekend vertraging. De *retransmissie waarschijnlijkheid* van een $[n, k]$-code wordt gegeven door

$$P_{\text{retrans}}(C) = 1 - (1-p)^n - P_{\text{undetec}}(C)$$

(dit is de waarschijnlijkheid dat de ontvangen vector $\bar{y}$ geen codewoord is).

Voorbeeld 4.4.4
Wij hernemen opnieuw Voorbeeld 4.2.1. Met $p = 0,01$ is $P_{\text{retrans}}(C) \approx 0,04$. Dus ongeveer 4% van de berichten moeten opnieuw verzonden worden.

4.5 De stelling van Shannon



Figuur 4.1: Claude Elwood Shannon

Claude Elwood Shannon werd op 30 april 1916 in Gaylord, Michigan, Verenigde Staten, geboren.

Claude Elwood Shannon's vader had ook de naam Claude Elwood Shannon, en zijn moeder was Mabel Catherine Wolf. Shannon studeerde aan de Universiteit van Michigan, waar hij in 1936 afstudeerde als wiskundige en electrotechnisch ingenieur. Hij studeerde daarna aan het Massachusetts Institute of Technology (MIT) waar hij in 1940 de graad van master electrotechnisch ingenieur en zijn doctoraat in de wiskunde behaalde. Shannon schreef een master thesis, getiteld A symbolic Analysis of Relay and Switching Circuits*, over het gebruik van Boole-algebra om relais circuits te analyseren en te optimaliseren. Zijn doctoraatsproefschrift handelde over bevolkingsgenetica.*

Aan het Massachusetts Institute of Technology werkte hij aan de ontwikkeling van de differential analyzer*, een vroeg type mechanische computer, ontworpen door Vannevar Bush, voor het bekomen van numerieke oplossingen voor gewone differentiaalvergelijkingen. Shannon publiceerde in 1941* Mathematical theory of the differential analyzer*. In de inleiding van dit artikel schrijft hij:*

De belangrijkste resultaten, vooral gegeven in de vorm van stellingen met bewijs, handelen over voorwaarden voor het genereren van functies in één of meer variabelen, en voorwaarden voor het oplossen van gewone differentiaalvergelijkingen. Aandacht wordt ook besteed aan het benaderen van functies, die niet exact gegenereerd kunnen worden, benaderen van versnellingsverhoudingen en automatische snelheidscontrole.

Shannon ging in 1941 als onderzoekswiskundige voor AT&T Bell Telephones in New Jersey werken, en bleef verbonden aan Bell Laboratories tot 1972.

D. Slepian, een collega aan Bell Laboratories, schreef:

Velen onder ons brachten onze lunch mee naar het werk en speelden wiskundige bordspelletjes, maar Claude kwam zelden. Hij werkte meestal met zijn deur gesloten. Maar als je in zijn bureau binnen ging, dan was hij heel geduldig en hielp hij je verder. Hij kon een probleem onmiddellijk vatten. Hij was werkelijk een genie. Hij is de enige persoon voor wie ik dit woord gebruikt heb.

Samenwerkend met John Riordan, publiceerde Shannon in 1942 een artikel over het aantal twee-terminale reeks-parallele netwerken. Dit artikel breidde resultaten bekomen door MacMahon uit die zijn vroege bijdrage in 1892 in het tijdschrift the Electrician *gepubliceerd had.*

Shannon publiceerde in 1948 A Mathematical Theory of Communication *in* The Bell System Technical Journal*. Dit artikel lag aan de grondslag van informatietheorie en hij stelde een lineair schematisch model van een communicatiesysteem voor. Dit was een nieuw idee. Communicatie werd tot dan beschouwd als zijnde het doorsturen van electromagnetische golven door een draad. Het idee dat men foto's, woorden, geluiden, $\cdots$, kan verzenden door een reeks nullen en énen door een draad te sturen, iets wat heden zo vanzelfsprekend is voor ons, was fundamenteel nieuw.*

Shannon beschouwt een informatiebron die woorden genereert bestaande uit een eindig aantal symbolen. Deze worden verzonden door een kanaal, waarbij elk symbool een eindige tijd in het communicatiekanaal doorbrengt. Het probleem gebruikte statistiek door de onderstelling dat als x_n het n-de symbool is geproduceerd door de informatiebron, dan het genereren van x_n een stationair stochastisch proces is. Hij gaf een methode om een reeks fouttermen in een signaal te analyseren om hun inherente verscheidenheid te vinden, en om deze te vergelijken met de ontworpen ver-

scheidenheid van het controlesysteem. In A Mathematical Theory of Communication*, waarin het woord* bit *voor het eerst gebruikt werd, toonde Shannon aan dat het toevoegen van extra bits aan een signaal het mogelijk maakt om fouten te verbeteren die optreden tijdens transmissie. Slepian schrijft:*

Er is waarschijnlijk geen enkel werk in de 20ste eeuw dat meer de menselijke visie op communicatie veranderd heeft dan Shannon's artikel: *A Mathematical Theory of Communication*, eerst verschenen in 1948. De ideeën in Shannon's artikel werden heel vlug, over heel de wereld, overgenomen door communicatie ingenieurs en wiskundigen. Ze werden bestudeerd, uitgebreid, en aangevuld met nieuwe verwante ideeën. Het onderzoeksgebied bloeide en groeide uit tot een welafgerond en opwindend hoofdstuk in de annalen van de wetenschappen.

Shannon trouwde op 27 maart 1949 met Mary Elizabeth Moore. Zij hadden drie zonen en een dochter; Robert, James, Andrew Moore, en Margarita. Hij zette zijn werk verder door aan te tonen hoe Boole algebra gebruikt kon worden om relais circuits te realiseren en te vereenvoudigen. Hij bewees ook resultaten over het kleuren van de bogen (takken) in grafen zodat geen twee bogen (takken) met dezelfde kleur een top (knoop) gemeen hebben. Een ander belangrijk artikel, verschenen in 1949, is Communication theory of secrecy systems.

In 1952 ontwierp Shannon een experiment dat de mogelijkheden van telefoonverbindingen illustreerde. Hij had in 1956 een positie bekomen als gastprofessor communicatiewetenschappen en wiskunde aan het Massachusetts Institute of Technology, vanaf 1957 werd hij benoemd aan de Faculteit van het MIT, maar hij bleef een consulent voor Bell Telephones. Hij werd in 1958 Donner Professor in de Wetenschappen.

R.G. Gallager, een collega die werkte aan het MIT, schreef:

Shannon was de persoon die inzag dat de bit het fundamentele element in communicatie was. Dat was echt zijn ontdekking, en vanuit deze ontdekking is de volledige revolutie in communicatie voortgekomen.

In zijn latere werk bestudeerde hij artificiële intelligentie. Hij ontwierp schaak spelprogramma's en een electronische muis die labyrint problemen kon oplossen. Het schaak spelprogramma verscheen in het artikel Programming a computer for playing chess*, gepubliceerd in 1950. Dit voorstel leidde in 1956 tot het eerste spel gespeeld door de Los Alamos MANIAC computer. Dit was ook het jaar dat Shannon een artikel publiceerde waarin hij aantoonde dat een universele Turing machine geconstrueerd kan worden met precies twee toestanden.*

Later had hij het gevoel dat de revoluties in communicaties, waarin hij in de beginperiode een belangrijke rol gespeeld had, te ver gingen. Hij schreef:

Informatietheorie heeft misschien een belangrijkheid bereikt die groter is dan zijn werkelijke verwezenlijkheden.

Marvin Minsky beschreef Shannon op de volgende manier:

Welk probleem ook opdook, hij engageerde zich met plezier, en hij bestudeerde het met een verrassend iets dat zowel een nieuw soort technisch concept kon zijn, als een hamer en zaag met

enkele stukken hout. Voor hem, hoe moeilijker een probleem was, hoe groter de kans was om iets nieuws te vinden.

Shannon ontving heel veel waardering voor zijn werk. Onder de lange lijst onderscheidingen die hij kreeg, waren de Alfred Nobel American Institute of American Engineers onderscheiding in 1940, de National Medal of Science in 1966, en de Audio Engineering Society Gold Medal en de Kyoto Prize in 1985.

Hij leed op het einde van zijn leven aan de ziekte van Alzheimer en verbleef de laatste jaren van zijn leven in een verpleeghuis in Massachusetts.

Hij stierf op 24 februari 2001 in Medford, Massachusetts, Verenigde Staten.

(http://turnbull.mcs.st-and.ac.uk/∼history/Mathematicians/Shannon.html)

Eenvoudigheidshalve beperken wij ons opnieuw tot binaire lineaire codes.

Definitie 4.5.1
Beschouw een binaire lineaire $[n, k]$-code C. De *verhouding (rate)* van C is dan

$$R(C) = k/n.$$

Een goede code heeft een grote verhouding.

Voorbeeld 4.5.2
Wij hernemen Voorbeeld 1.3.1. Onderstel dat wij de route NNWNNWWZ
ZWW... wensen door te zenden, gebruik makend van een lineaire code met verhouding tenminste $1/2$. Het aantal overtallige symbolen mag dus ten hoogste k zijn. Wij onderstellen opnieuw dat het kanaal binair symmetrisch is met $p = 0,01$.

Gebruiken wij de $[4, 2]$-code uit Voorbeeld 4.2.1, dan is $P_{\text{err}}(C) = 0,0103$ (zie 4.3.2) en $R(C) = 1/2$.

Vervolgens identificeren wij N, W, O en Z met de berichtvectoren $00, 01, 10$ en 11 zodat de route nu de rij $00000100000010111110101\ldots$ wordt. Wij breken deze rij nu op in blokken van lengte 4 en coderen elke blok tot een codewoord van lengte 7 met de $[7, 4]$-code C' van Voorbeeld 2.3.8. Aangezien C' een perfecte $[7, 4, 3]$-code is, hebben wij $\alpha_0 = 1, \alpha_1 = 7$ en $\alpha_i = 0$ voor $i > 1$ (zie 4.2 en 4.3). Bijgevolg is $P_{\text{err}}(C') = 1 - (1-p)^7 - 7p(1-p)^6 \approx 0,002$ (voor $p = 0,01$). Hier is $R(C') = 4/7$.

Dus is $P_{\text{err}}(C') \approx P_{\text{err}}(C)/5$ en $R(C') > R(C) = 1/2$.

Breken wij nu de rij hierboven op in blokken van 12, dan kan men bij het coderen gebruik maken van een $[23, 12]$-code C'' met $P_{\text{err}}(C'') \approx 0,00008$. Hier is eveneens $R(C'') = 12/23 > 1/2$.

Het ziet er dus naar uit dat wij de woordfout waarschijnlijkheid zo klein kunnen maken als wij maar willen, door gebruik te maken van een code met voldoend grote lengte, maar steeds met een verhouding die tenminste $1/2$ is. Dit is een gevolg van een beroemde stelling van Shannon die wij nu geven zonder bewijs.

Definitie 4.5.3
De *capaciteit (capacity)* $\mathcal{C}(p)$ van een binair symmetrisch kanaal met symboolfout waarschijnlijkheid p is

$$\mathcal{C}(p) = 1 + p\log_2 p + (1-p)\log_2(1-p).$$

Stelling 4.5.4 (Stelling van Shannon)
Onderstel dat een kanaal binair symmetrisch is met symboolfout waarschijnlijkheid p, waarbij $p < \frac{1}{2}$. Onderstel verder dat R een reëel getal is dat voldoet aan $R < \mathcal{C}(p)$. Voor elk reëel getal $\varepsilon > 0$ bestaat er dan, voor voldoende grote n, een binaire lineaire $[n,k]$-code C met verhouding $k/n \geq R$ en $P_{err}(C) < \varepsilon$. □

Voorbeeld 4.5.5
Er geldt $\mathcal{C}(0,01) \approx 0,92$. Dus voor $p = 0,01$ bestaat, voor voldoende grote n (en k), een $[n,k]$-code C met verhouding tenminste $9/10$ en met $P_{\text{err}}(C)$ zo klein als we maar willen.

Opmerkingen 4.5.6

(i) De stelling van Shannon wordt bewezen met probabilistische methodes, en uit het bewijs volgt niet hoe de codes geconstrueerd worden. Ook merken wij op dat wij in de praktijk codes nodig hebben waarvoor coderen en decoderen gemakkelijk is, en meestal is dit niet het geval voor codes met grote lengte en met veel codewoorden.

(ii) De stelling van Shannon werd ook bewezen voor niet-binaire codes; een andere definitie voor capaciteit is dan nodig.

(iii) In 1948 schreef Claude Shannon van Bell Telephone Laboratories zijn beroemd artikel dat de aanleiding was tot de *informatietheorie* en de *codeertheorie*. In de informatietheorie wordt er hoofdzakelijk gesteund op ideeën en methodes uit de waarschijnlijkheidsrekening; in de codeertheorie wordt er hoofdzakelijk gebruik gemaakt van ideeën en methodes uit de zuivere wiskunde.

Hoofdstuk 5

Duale code, pariteit controlematrix, syndroom decodering en onvolledige decodering

5.1 Duale code en pariteit controlematrix

Het *inwendig* of *scalair product* $\bar{u}.\bar{v}$ van de vectoren $\bar{u} = u_1u_2\cdots u_n$ en $\bar{v} = v_1v_2\cdots v_n$ van $V(n,q)$ is het element

$$\bar{u}.\bar{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n$$

van GF(q). Is $\bar{u}.\bar{v} = 0$, dan zegt men dat $\bar{u}$ en $\bar{v}$ *orthogonaal* zijn.

Definitie 5.1.1
Is C een $[n,k]$-code over GF(q), dan is de *duale code* $C^\perp$ van C de verzameling van alle vectoren van $V(n,q)$ die orthogonaal zijn met elke vector van C, m.a.w.

$$C^\perp = \{\bar{v} \in V(n,q) \parallel \bar{v}.\bar{u} = 0 \text{ voor alle } \bar{u} \in C\}.$$

Is $C = C^\perp$, dan zegt men dat C *zelfduaal* is.

Lemma 5.1.2
Onderstel dat C een $[n,k]$-code is met voortbrengende matrix G. Dan behoort $\bar{v} \in V(n,q)$ tot $C^\perp$ a.s.a. $\bar{v}$ orthogonaal is met elke rij van G.

Bewijs. Behoort $\bar{v}$ tot $C^\perp$ dan staat $\bar{v}$ vanzelfsprekend loodrecht op alle rijen van G. Onderstel omgekeerd dat $\bar{v}$ loodrecht staat op alle rijen van G. Zijn $\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_k$ de rijen van G, dan is dus $\bar{v}.\bar{r}_i = 0$, met $i = 1, 2, \cdots, k$. Is $\bar{u}$ een willekeurig codewoord van C, dan is $\bar{u} = \sum_{i=1}^{k} \lambda_i\bar{r}_i$ met $\lambda_i \in$ GF(q), zodat

$$\bar{v}.\bar{u} = \sum_{i=1}^{k} \lambda_i(\bar{v}.\bar{r}_i) = \sum_{i=1}^{k} \lambda_i 0 = 0.$$

Bijgevolg staat $\bar{v}$ loodrecht op elke vector van C, zodat $\bar{v} \in C^{\perp}$. □

Stelling 5.1.3
Is C een lineaire $[n,k]$-code over GF(q)*, dan is $C^{\perp}$ een lineaire $[n, n-k]$-code over* GF(q).

Bewijs. Eerst en vooral bewijzen wij dat $C^{\perp}$ lineair is. Beschouw vectoren $\bar{v}_1, \bar{v}_2 \in C^{\perp}$ en elementen $\lambda, \mu \in$ GF(q). Dan is voor elke $\bar{u} \in C$ voldaan aan

$$(\lambda\bar{v}_1 + \mu\bar{v}_2).\bar{u} = \lambda(\bar{v}_1.\bar{u}) + \mu(\bar{v}_2.\bar{u}) = \lambda 0 + \mu 0 = 0.$$

Bijgevolg is $\lambda\bar{v}_1 + \mu\bar{v}_2 \in C^{\perp}$, zodat $C^{\perp}$ lineair is.

Wij bewijzen nu dat $C^{\perp}$ dimensie $n-k$ heeft. Beschouw een voortbrengende matrix $G = [g_{ij}]$ van C. Wegens Lemma 5.1.2. bestaat $C^{\perp}$ uit de vectoren $\bar{v} = v_1 v_2 \cdots v_n$ waarvoor

$$\sum_{j=1}^{n} g_{ij} v_j = 0, \quad i = 1, 2, \cdots, k.$$

De dimensie van $C^{\perp}$ is dus de dimensie van de oplossingenverzameling van een stelsel van k lineaire en homogene vergelijkingen in n onbekenden waarvan de rang gelijk is aan k, m.a.w. $n-k$. □

Voorbeelden 5.1.4
(i) Is $C = \{0000, 1100, 0011, 1111\}$, met C binair, dan is $C = C^{\perp}$, zodat C zelfduaal is.

(ii) Is $C = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$, met C binair, dan is $C^{\perp} = \{0000, 1111\}$ m.a.w. $C^{\perp}$ is de binaire herhalingscode van lengte 4.

Stelling 5.1.5
Voor elke $[n,k]$-code C is $(C^{\perp})^{\perp} = C$.

Bewijs. Aangezien elke vector van C loodrecht staat op elke vector van $C^{\perp}$ is $C \subseteq (C^{\perp})^{\perp}$. Nu is $\dim((C^{\perp})^{\perp}) = n - (n-k) = k = \dim C$. Bijgevolg is $C = (C^{\perp})^{\perp}$. □

Definitie 5.1.6
Een *pariteit controlematrix* (*parity-check matrix*) H van een $[n,k]$-code C is een voortbrengende matrix van $C^{\perp}$.

Bijgevolg is H een $(n-k) \times n$-matrix van rang $n-k$ waarvoor voldaan is aan $GH' = 0$, met G een voortbrengende matrix van C. Uit Lemma 5.1.2 en Stelling 5.1.5 volgt onmiddellijk dat

$$C = \{\bar{x} \in V(n,q) \parallel \bar{x}H' = 0\}.$$

Een lineaire code C is dus volledig bepaald door zijn pariteit controlematrix.

Definitie 5.1.7
Elke vector van $C^\perp$ noemt men een *pariteit controle* (*parity-check*) van C. Is $\bar{x} = x_1x_2\cdots x_n \in C^\perp - \{\bar{0}\}$, dan noemt men de vergelijking $x_1X_1 + x_2X_2 + \cdots + x_nX_n = 0$ een *pariteit controlevergelijking* (*parity-check equation*) van C; elke zulke vergelijking stelt een hypervlak voor van $V(n,q)$. De code C is de doorsnede van de $n-k$ hypervlakken bepaald door de $n-k$ pariteit controlevergelijkingen die met de rijen van H corresponderen.

Voorbeelden 5.1.8
(i) In Voorbeeld 5.1.4(i) is

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

(ii) In Voorbeeld 5.1.4(ii) is $H = [1111]$.

(iii) Herneem Voorbeeld 5.1.4(ii). De vector $\bar{x} = 1111$ is een pariteit controle voor C en C is het hypervlak bepaald door de pariteit controlevergelijking $X_1+X_2+X_3+X_4 = 0$.

Beschouw nu algemener de binaire code bepaald door de pariteit controlematrix $H = [11\cdots1]$, met H een $1 \times n$-matrix. Dan is C het hypervlak bepaald door de pariteit controlevergelijking $X_1 + X_2 + \cdots + X_n = 0$. De code C is een binaire $[n, n-1]$-code, en bestaat uit alle vectoren van $V(n,2)$ met even gewicht. Deze code C noemt men de *even gewicht code* van lengte n.

Stelling 5.1.9
Is $G = [I_k \;\; A]$ een voortbrengende matrix in standaard gedaante van de $[n,k]$-code C over GF(q)*, dan is $H = [-A' \;\; I_{n-k}]$ een pariteit controlematrix van C.*

Bewijs. Rang $H = n-k$ en

$$GH' = [\mathrm{I}_k \;\; A] \begin{bmatrix} -A \\ \mathrm{I}_{n-k} \end{bmatrix} = [-A + A] = 0.$$

Bijgevolg is H een pariteit controlematrix voor C. □

Definitie 5.1.10
Men zegt dat een pariteit controlematrix H van C in *standaard gedaante* is als

$$H = [B \;\; \mathrm{I}_{n-k}],$$

met B een $(n-k) \times k$-matrix over GF(q).

Op een volledig analoge manier als voor een voortbrengende matrix kan een pariteit controlematrix in standaardgedaante gebracht worden.

Voorbeeld 5.1.11
Herneem de voortbrengende matrix in standaardgedaante uit Voorbeeld 3.3.4(ii)

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

Een pariteit controlematrix in standaardgedaante voor deze binaire code is dan

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

5.2 Syndroom decodering

Onderstel dat H een pariteit controlematrix is van de $[n, k]$-code C. Voor elke vector $\bar{y} \in V(n, q)$ wordt de rijvector van type $1 \times (n - k)$

$$S(\bar{y}) = \bar{y}H'$$

het *syndroom* van $\bar{y}$ genoemd. Zijn $\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_{n-k}$ de rijen van H, dan is dus $S(\bar{y}) = (\bar{y}.\bar{r}_1, \bar{y}.\bar{r}_2, \cdots, \bar{y}.\bar{r}_{n-k})$. Verder is $S(\bar{y}) = \bar{0}$ a.s.a. $\bar{y} \in C$.

Lemma 5.2.1
Twee vectoren $\bar{u}$ en $\bar{v}$ bevinden zich in eenzelfde additieve nevenklasse van C a.s.a. ze eenzelfde syndroom hebben.

Bewijs. De vectoren $\bar{u}$ en $\bar{v}$ bevinden zich in eenzelfde additieve nevenklasse van C a.s.a. $\bar{u} + C = \bar{v} + C \Leftrightarrow \bar{u} - \bar{v} \in C \Leftrightarrow (\bar{u} - \bar{v})H' = \bar{0} \Leftrightarrow \bar{u}H' = \bar{v}H' \Leftrightarrow S(\bar{u}) = S(\bar{v})$. □

Gevolg 5.2.2
De afbeelding $\bar{u} + C \mapsto S(\bar{u})$ definieert een bijectie van de verzameling der nevenklassen op de verzameling der syndromen. □

Bij decoderen met een standaard rooster is er geen moeilijkheid om een ontvangen vector $\bar{y}$ te localiseren in het rooster als n klein is; indien n groot is en $V(n, q)$ dus veel vectoren telt is dit echter niet meer zo eenvoudig. Dit probleem kan opgelost worden door gebruik te maken van de syndromen.

Voor elke nevenklasseleider $\bar{e}$ berekenen wij het syndroom $S(\bar{e})$ en breiden het rooster uit met een extra kolom die de syndromen $S(\bar{e})$ bevat. Indien een vector $\bar{y}$ ontvangen wordt berekenen wij $S(\bar{y}) = \bar{y}H'$ en zoeken wij $S(\bar{y})$ op in de kolom der syndromen van het rooster. Aldus localizeren wij zeer vlug de rij waarin $\bar{y}$ zich bevindt. De vector $\bar{y}$ wordt dan gedecodeerd als het codewoord in de kolom van $\bar{y}$.

In feite hebben wij slechts twee kolommen nodig, namelijk de kolom der syndromen $\bar{s}$ en de kolom der nevenklasseleiders $\bar{s}^\sigma$; merk op dat σ een bijectie is van de verzameling der syndromen op de verzameling der nevenklasseleiders

$$\begin{array}{cc} \underline{\bar{s}} & \underline{\bar{s}^\sigma} \\ S(\bar{e}) & \bar{e} \\ \vdots & \vdots \end{array}$$

Deze kolommen vormen de zogenaamde *syndroom opzoekingstabel* (*syndrome look-up table*).

Decodeerprocedure die wij nu volgen:

Stap 1. Voor een ontvangen vector $\bar{y}$ berekenen wij $S(\bar{y}) = \bar{y}H'$.

Stap 2. Stel $\bar{s} = S(\bar{y})$ en zoek $\bar{s}$ op in de eerste kolom van de tabel.

Stap 3. Decodeer $\bar{y}$ als $\bar{y} - \bar{s}^\sigma$.

Voorbeelden 5.2.3
Wij hernemen Voorbeeld 4.2.1. Hier is

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

Wegens Stelling 5.1.9 is

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

Syndromen van de nevenklasseleiders:

$$\begin{aligned} &\mathrm{S}(0000) = 00, \\ &\mathrm{S}(1000) = 11, \\ &\mathrm{S}(0100) = 10, \\ &\mathrm{S}(0001) = 01. \end{aligned}$$

Het standaard rooster wordt nu uitgebreid met de kolom der syndromen:

	nevenklasse-leiders				syndromen
codewoorden:	0000	1011	0110	1101	00
	1000	0011	1110	0101	11
	0100	1111	0010	1001	10
	0001	1010	0111	1100	01

Onderstel dat $\bar{y} = 1110$ ontvangen wordt. Dan is $S(\bar{y}) = 11$, zodat $\bar{y}$ zich in de tweede rij moet bevinden. Inspectie van deze rij leert ons dat $\bar{y}$ zich onder het codewoord 0110 bevindt, zodat $\bar{y}$ gedecodeerd wordt als 0110.

Wij zullen nu decodering uitvoeren aan de hand van de syndroom opzoekingstabel.

Syndroom opzoekingstabel:

syndroom $\bar{s}$	nevenklasseleider $\bar{s}^\sigma$
00	0000
11	1000
10	0100
01	0001

Onderstel dat $\bar{y} = 1110$ ontvangen wordt. Dan is $S(\bar{y}) = 11 = \bar{s}$. De vector $\bar{y}$ wordt dan gedecodeerd als $\bar{y} - \bar{s}^\sigma = 1110 - 1000 = 0110$.

5.3 Onvolledige decodering

Onvolledige decodering is een combinatie van foutverbetering en foutdetectie. Onderstel dat $d(C) = 2t+1$ of $2t+2$. Wij volgen nu een schema waarbij verbetering van ten hoogste t fouten gegarandeerd is, en waarbij als d even is en er juist $t+1$ fouten gemaakt worden men detecteert dat er ten minste $t+1$ fouten zijn en alsdan om retransmissie vraagt.

Wij beschouwen opnieuw het standaard rooster, en verdelen het in een *bovendeel* (*top part*) en een *benedendeel (bottom part)*; in het bovendeel bevinden zich juist alle nevenklasseleiders met gewicht $\leq t$, in het benedendeel de andere nevenklasseleiders (merk op dat alle vectoren met gewicht $\leq t$ nevenklasseleider zijn).

Indien de ontvangen vector $\bar{y}$ in het bovendeel gelegen is, decoderen wij hem op de gebruikelijke manier (wij nemen dan aan dat er ten hoogste t fouten gemaakt werden); indien $\bar{y}$ in het benedendeel gelegen is vragen wij om retransmissie (in zulk geval weten wij dat tenminste $t+1$ fouten gemaakt werden).

Onderstel nu dat $d(C) = 2t+2$, en onderstel dat juist $t+1$ fouten gemaakt werden. Moest $\bar{y}$ in het bovendeel liggen, dan zou $\bar{y} = \bar{x}' + \bar{e}$ met $w(\bar{e}) \leq t$ en $\bar{x}' \in C$. Aangezien juist $t+1$ fouten gemaakt werden is $d(\bar{y}, \bar{x}) = t+1$, met $\bar{x}$ het verzonden codewoord. Bijgevolg zou $d(\bar{x}, \bar{x}') \leq d(\bar{x}, \bar{y}) + d(\bar{y}, \bar{x}') = t+1+w(\bar{y}-\bar{x}') = t+1+w(\bar{e}) \leq 2t+1$, een strijdigheid. Bijgevolg ligt $\bar{y}$ in het benedendeel, zodat wij zien dat tenminste $t+1$ fouten gemaakt werden; wij vragen dus om retransmissie.

Met gebruik van een syndroom opzoekingstabel wordt deze procedure, die *onvolledige decodering* (*incomplete decoding*) wordt genoemd, zeer eenvoudig. De nevenklasseleiders in het bovendeel zijn alle vectoren met gewicht $\leq t$ en daarvan berekenen wij de syndromen. Dit levert ons de syndroom opzoekingstabel die wij hier nodig hebben; met onvolledige decodering hebben wij het benedendeel van de syndroom opzoekingstabel uit 5.2. niet nodig.

Procedure die wij volgen (wij maken gebruik van de notaties uit 5.2):

Stap 1. Voor een ontvangen vector $\bar{y}$ berekenen wij $S(\bar{y}) = \bar{y}H'$.

Stap 2. Stel $\bar{s} = S(\bar{y})$ en zoek $\bar{s}$ op in de kolom van de syndromen (van de nevenklasseleiders met gewicht $\leq t$).

Stap 3. Komt $\bar{s}$ niet in deze kolom voor (dat is als $S(\bar{y})$ een syndroom is van een nevenklasseleider in het benedendeel), dan vragen wij om retransmissie; komt $\bar{s}$ wel in deze kolom voor, dan decoderen wij $\bar{y}$ als $\bar{y} - \bar{s}^{\sigma}$.

Voorbeeld 5.3.1
Beschouw de binaire code C met voortbrengende matrix

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

Een standaard rooster voor C is:

	nevenklasse-leiders			
codewoorden:	00000	10110	01101	11011
	10000	00110	11101	01011
	01000	11110	00101	10011
	00100	10010	01001	11111
	00010	10100	01111	11001
	00001	10111	01100	11010
	00011	10101	01110	11000
	01010	11100	00111	10001

bovendeel

benedendeel

Indien 01111 wordt ontvangen, decoderen wij als 01101. Indien 01110 wordt ontvangen vragen wij om retransmissie. Indien 01110 wordt ontvangen en indien we weten dat juist 2 fouten gemaakt werden, zou bij decoderen er een waarschijnlijkheid van 1/2 zijn dat na decodering het codewoord ook het verzonden codewoord is (indien we niet weten dat juist 2 fouten gemaakt werden zal deze waarschijnlijkheid kleiner dan 1/2 zijn).

Een pariteit controlematrix van C is

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

Syndroom opzoekingstabel:

syndrooom $\bar{s}$	nevenklasseleider $\bar{s}^{\sigma}$
000	00000
110	10000
101	01000
100	00100
010	00010
001	00001

Indien $\bar{y} = 01111$ ontvangen wordt berekenen wij eerst $S(\bar{y}) = \bar{y}H' = 010$. De vector $\bar{y}$ wordt dan gedecodeerd als $\bar{y} - \bar{s}^{\sigma} = 01111 - 00010 = 01101$. Indien $\bar{y} = 01110$ ontvangen wordt is $S(\bar{y}) = \bar{y}H' = 011$, zodat $S(\bar{y})$ niet in de opzoekingstabel voorkomt; hier vragen wij dus om retransmissie.

5.4 Een interessante decimale code

Beschouw de lineaire [10,8]-code C' over GF(11) met als pariteit controlematrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

Noem C de 10-aire code die uit C' ontstaat door alle codewoorden weg te laten die het element 10 bevatten, m.a.w. C bestaat uit alle decimale getallen $\bar{x} = x_1 x_2 \cdots x_{10}$ van lengte 10 waarvoor voldaan is aan de volgende pariteit controlevergelijkingen over GF(11) :

$$\sum_{i=1}^{10} X_i = 0 \text{ en } \sum_{i=1}^{10} iX_i = 0.$$

Het is niet moeilijk om aan te tonen dat $|C| = 82.644.629$.

Om alle codewoorden van C te vinden kunnen wij als volgt te werk gaan.
Eerst brengen wij H in standaard gedaante (rijen stellen wij voor door $\bar{r}_1$ en $\bar{r}_2$):

$$H \underset{\bar{r}_1 \to \bar{r}_1 + \bar{r}_2}{\longrightarrow} \begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}$$

$$\underset{\bar{r}_1 \to -\bar{r}_1, \bar{r}_2 \to -\bar{r}_2}{\longrightarrow} \begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

$$\underset{\bar{r}_2 \to \bar{r}_2 - 2\bar{r}_1}{\longrightarrow} \begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \end{bmatrix}.$$

Een voortbrengende matrix voor C' is dan

$$G = \begin{bmatrix} & 2 & 8 \\ & 3 & 7 \\ & 4 & 6 \\ I_8 & 5 & 5 \\ & 6 & 4 \\ & 7 & 3 \\ & 8 & 2 \\ & 9 & 1 \end{bmatrix}.$$

Dus is C de verzameling van de vectoren $(x_1, x_2, \cdots, x_8, 2x_1 + 3x_2 + 4x_3 + 5x_4 + 6x_5 + 7x_6 + 8x_7 + 9x_8, 8x_1 + 7x_2 + 6x_3 + 5x_4 + 4x_5 + 3x_6 + 2x_7 + x_8)$, waarbij $x_1, x_2, \cdots, x_8 \in \{0, 1, \cdots, 9\}$

en waarbij de vector geschrapt wordt indien één van de laatste twee coördinaten gelijk is aan 10.

Onderstel nu dat $\bar{x} = x_1x_2\cdots x_{10} \in C$ verzonden wordt en dat $\bar{y} = y_1y_2\cdots y_{10}$ ontvangen wordt; hierbij wordt verondersteld dat het transmissiesysteem zodanig is dat ook $y_1, y_2, \cdots, y_{10} \in \{0, 1, \cdots, 9\}$.
Bereken nu het syndroom

$$(A, B) = \bar{y}H' = (\sum_{i=1}^{10} y_i, \sum_{i=1}^{10} iy_i)$$

over GF(11).

Onderstel dat één enkele fout is opgetreden, zodat

$$(y_1, y_2, \cdots, y_{10}) = (x_1, \cdots, x_{j-1}, x_j + k, x_{j+1}, \cdots, x_{10})$$

met $k \neq 0$ (in GF(11)). Dan is

$$A = \sum_{i=1}^{10} y_i = (\sum_{i=1}^{10} x_i) + k = k,$$

$$B = \sum_{i=1}^{10} iy_i = (\sum_{i=1}^{10} ix_i) + jk = jk.$$

De grootte van de fout is dus A, terwijl de positie waar de fout zich bevindt gelijk is aan BA^{-1}.

Decodeerprocedure die wij zullen volgen:

- Wij berekenen het syndroom (A, B).
- Is $A = 0 = B$, dan is $\bar{y}$ een codewoord en onderstellen wij dat $\bar{y}$ verzonden werd.
- Is $A \neq 0 \neq B$ dan nemen wij aan dat er één enkele fout gemaakt werd, die wij verbeteren door A af te trekken van de BA^{-1}de coördinaat van $\bar{y}$. Bekomt men echter, na verbetering, voor de BA^{-1}de coördinaat van $\bar{y}$ het element 10, dan werden er ten minste twee fouten gemaakt en vragen wij om retransmissie.
- Is $A = 0$ of $B = 0$, maar niet beide, dan hebben wij tenminste twee fouten gedetecteerd en vragen wij om retransmissie. Dit geval doet zich steeds voor indien twee verschillende symbolen in het codewoord, in de resp. posities j en k, omgewisseld werden; in zulk geval is inderdaad $A = 0$ en $B = (k - j)(x_j - x_k) \neq 0$.

Opmerking 5.4.1

(i) Het decoderen gebeurt hier uiterst snel. Hier moet zelfs geen syndroom opzoekingstabel opgeslagen worden.

(ii) Aangezien wij in staat zijn één enkele fout te verbeteren is de minimum afstand van deze code tenminste 3.

Voorbeelden 5.4.2
Onderstel dat $\bar{y} = 1207845023$ ontvangen wordt. Dan is $A = 10$ en $B = 4$. Dus $BA^{-1} = 4.10 = 7$. Wij decoderen $\bar{y}$ als 1207846023 (het symbool op de 7de plaats wordt vervangen door 5–10=6).

Hoofdstuk 6

Gewichtspolynomen

Figuur 6.1: Florence Jessie MacWilliams

Florence Jessie Collinson MacWilliams werd in 1917 in Stoke-on-Trent, Engeland, geboren. Zij behaalde in 1938 de graad van Bachelor of Arts aan de Universiteit van Cambridge en in 1939 de graad van Master of Arts. In 1939 ontving zij een reisbeurs van Cambridge en bezocht de John Hopkins Universiteit, waar zij samenwerkte met Oscar Zariski. In 1940 ging zij samen met Zariski naar de Harvard Universiteit om daar een jaar te studeren. Zij trouwde in 1941 en verliet haar wiskundig werk enkele jaren om haar drie kinderen, een dochter en twee zonen, op te voeden.

In 1958 ging Florence Jessie MacWilliams als computerprogrammeur werken bij Bell Telephone Laboratories in Murray Hill, New Jersey, waar haar echtgenoot, Walter MacWilliams, na de oorlog aangeworven was als ingenieur. Zij geraakte geinteresseerd in codeertheorie toen R.C. Bose Bell Labs bezocht en een voordracht gaf over dit onderwerp. Florence Jessie wilde lid worden van de technische ploeg aan Bell Labs, een positie waarvoor een doctoraat vereist was. Daarom keerde zij in 1961 voor een jaar terug naar Harvard Universiteit, en behaalde de graad van doctor door, onder leiding van Andrew Gleason, onderzoek te verrichten op codeertheorie. (Haar dochter Ann, die ook een doctor in de wiskunde is, studeerde op hetzelfde ogenblik aan Harvard.) Volgens een in memoriam, geschreven door Vera Pless van de Universiteit van Illinois in Chicago, dat in november 1990 in SIAM NEWS *verscheen, bevatte haar doctoraatsthesis* Combinatorial Problems of Elementary Group Theory *één van de* meest performante stellingen in de codeertheorie.

Vera Pless schrijft:

De MacWilliams vergelijkingen leggen een verband tussen de gewichtsdistributie van een lineaire code en de gewichtsdistributie van zijn duale code. Als de lineaire code gelijk is aan zijn duale code, dan vertellen deze vergelijkingen heel veel over de gewichtsdistributie van zelf-duale codes. De vergelijkingen van MacWilliams worden frequent gebruikt door onderzoekers in codeertheorie, om zowel nieuwe theoretische informatie over foutenverbeterende codes te bekomen als om de gewichtsdistributie van specifieke codes te vinden.

De vergelijkingen van MacWilliams leiden ook tot belangrijke resultaten over combinatorische designs.

Florence Jessie werkte ook op cyclische codes, door deze klasse codes te veralgemenen tot abelse groep codes. Zij loste samen met H.B. Mann een moeilijk probleem betreffende zekere design matrices op. Zij is misschien het best gekend voor haar boek The Theory of Error-Correcting Codes*, North-Holland, 1977, dat zij schreef samen met N.J.A. Sloane van Bell Labs. In haar in memoriam merkt Vera Pless op dat dit boek, met bijna 1500 referenties, vele verschillende gebieden in de codeertheorie behandelt. Vera Pless schrijft ook:*

De vele onderzoeksproblemen verspreid doorheen dit boek hebben onderzoek gestimuleerd in vele gebieden binnen in de codeertheorie.

Florence Jessie MacWilliams ging in januari 1983 op pensioen bij Bell Labs, en wijdde zich aan haar kleinkinderen, haar thuis en haar tuin. Zij stierf in mei 1990.

(http://www.awm-math.org/noetherbrochure/MacWilliams80.html)

6.1 Gewichtspolynomen

Beschouw een code C met lengte n over $F_q = \{0, 1, \cdots, q-1\}$, en noem A_i, $i = 0, 1, \cdots, n$, het aantal codewoorden met gewicht i. Dan noemt men

$$A(X, Y) = \sum_{i=0}^{n} A_i X^i Y^{n-i} \in \mathbb{N}[X, Y]$$

de *gewichtspolynoom* (*weight enumerator*) van C. Merk op dat $\sum_{i=o}^{n} A_i = |C|$.

Het is eveneens duidelijk dat

$$A(X, Y) = \sum_{\bar{x} \in C} X^{w(\bar{x})} Y^{n-w(\bar{x})}.$$

Voorbeeld 6.1.1
Herneem de code uit Voorbeeld 5.3.1. Hier is

$$A(X, Y) = Y^5 + 2X^3Y^2 + X^4Y.$$

6.2 De stelling van MacWilliams

In deze sectie geven wij het verband tussen de gewichtspolynoom $A(X,Y)$ van een lineaire $[n,k]$-code C over GF(q) en de gewichtspolynoom $A^{\perp}(X,Y)$ van de duale code $C^{\perp}$.

De functie χ. Beschouw een irreduciebele polynoom $F(X) \in$ GF$(p)[X]$, p priem, van de graad r. Dan is voor $q = p^r$

$$\mathrm{GF}(q) = \{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda_{r-1}\alpha^{r-1} \parallel \lambda_i \in \mathrm{GF}(p)\},$$

waarbij optelling in GF(q) de gewone optelling is, en vermenigvuldiging modulo $F(\alpha)$ geschiedt.

Stel $\xi = e^{2\pi i/p} \in \mathbb{C}$. Dan is $\xi^p = 1$. Verder stellen wij

$$\chi : \ \mathrm{GF}(q) \longrightarrow \mathbb{C}_p, \lambda_0 + \lambda_1\alpha + \cdots + \lambda_{r-1}\alpha^{r-1} \longmapsto \xi^{\lambda_0},$$

waarbij $\mathbb{C}_p$ de verzameling is van de p complexe $p$de machtswortels uit 1, en waarbij in ξ^{λ_0} het element λ_0 beschouwd wordt als element van $\mathbb{Z}$. Dan is χ een epimorfisme van de additieve groep van GF(q) op de multiplicatieve groep $\mathbb{C}_p$.

Voor elke $\bar{v} \in F^n$, met $F =$GF(q), definiëren wij $\chi_{\bar{v}}$ als volgt:

$$\chi_{\bar{v}} : F^n \longrightarrow \mathbb{C}_p, \bar{u} \longmapsto \bar{u}^{\chi_{\bar{v}}} = (\bar{u}.\bar{v})^{\chi}.$$

Lemma 6.2.1
Is B een vectorruimte over $\mathbb{C}$, is φ een afbeelding van F^n in B, en wordt de afbeelding ψ van F^n in B gedefinieerd door

$$\bar{u}^{\psi} = \sum_{\bar{v}\in F^n} \bar{u}^{\chi_{\bar{v}}}\bar{v}^{\varphi},$$

dan geldt voor elke deelruimte V van F^n en de orthogonale deelruimte $V^{\perp}$

$$\sum_{\bar{u}\in V} \bar{u}^{\psi} = |V| \sum_{\bar{v}\in V^{\perp}} \bar{v}^{\varphi}.$$

Bewijs.

$$\begin{aligned}
\sum_{\bar{u}\in V} \bar{u}^{\psi} &= \sum_{\bar{u}\in V}\sum_{\bar{v}\in F^n} \bar{u}^{\chi_{\bar{v}}}\bar{v}^{\varphi} \\
&= \sum_{\bar{v}\in F^n}\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}}\bar{v}^{\varphi} \\
&= \sum_{\bar{v}\in F^n} (\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}})\bar{v}^{\varphi} \\
&= \sum_{\bar{v}\in V^{\perp}} (\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}})\bar{v}^{\varphi} + \sum_{\bar{v}\notin V^{\perp}} (\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}})\bar{v}^{\varphi} \\
&= \sum_{\bar{v}\in V^{\perp}} (\sum_{\bar{u}\in V} (\bar{u}\cdot\bar{v})^{\chi})\bar{v}^{\varphi} + \sum_{\bar{v}\notin V^{\perp}} (\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}})\bar{v}^{\varphi} \\
&= |V| \sum_{\bar{v}\in V^{\perp}} \bar{v}^{\varphi} + \sum_{\bar{v}\notin V^{\perp}} (\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}})\bar{v}^{\varphi},
\end{aligned}$$

aangezien $(\bar{u}.\bar{v})^\chi = 1$ voor $\bar{u} \in V$ en $\bar{v} \in V^\perp$. Het lemma is volledig bewezen indien wij kunnen aantonen dat

$$\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}} = 0, \text{ met } \bar{v} \notin V^\perp.$$

De afbeelding

$$\theta_{\bar{v}} : V \longrightarrow \text{GF}(q), \bar{u} \longmapsto \bar{u} \cdot \bar{v}, \text{ met } \bar{v} \notin V^\perp,$$

is een homomorfisme van de additieve groep van V in de additieve groep van $\text{GF}(q) = F$. Noem $\{\overline{u}_1, \overline{u}_2, \cdots, \overline{u}_s\}$ een basis van V. Aangezien $\bar{v} \notin V^\perp$ is voor tenminste één i voldaan aan $\bar{u}_i \cdot \bar{v} \neq 0$, bijvoorbeeld $\overline{u}_1 \cdot \bar{v} = a \neq 0$. Er geldt:

$$\theta_{\bar{v}} : \bar{u} = l_1\overline{u}_1 + l_2\overline{u}_2 + \cdots + l_s\overline{u}_s \longmapsto l_1 a + l_2(\overline{u}_2.\bar{v}) + \cdots + l_s(\overline{u}_s.\bar{v}).$$

Dus is $\{(l_1\overline{u}_1)^{\theta_{\bar{v}}} \parallel l_1 \in F\} = \{l_1 a \parallel l_1 \in F\} = F$. Bijgevolg is $\theta_{\bar{v}}$ een epimorfisme van de additieve groep van V op de additieve groep van $F = \text{GF}(q)$. Hieruit volgt dat

$$\sum_{\bar{u}\in V} \bar{u}^{\chi_{\bar{v}}} = \sum_{\bar{u}\in V} (\bar{u} \cdot \bar{v})^\chi = q^{s-1} \sum_{\beta\in F} \beta^\chi$$

(merk op dat $q^{s-1} = |\text{ Ker } \theta_{\bar{v}}|$). Het lemma is dus volledig bewezen indien wij kunnen aantonen dat

$$\sum_{\beta\in F} \beta^\chi = 0.$$

Aangezien χ een epimorfisme is van de additieve groep van F op de multiplicatieve groep van $\mathbb{C}_p$ is

$$\sum_{\beta\in F} \beta^\chi = p^{r-1}. \text{ (som van de elementen van } \mathbb{C}_p) = 0$$

(merk op dat $p^{r-1} = |\text{ Ker } \chi|$ en dat de som van de p complexe $p$de machtswortels uit 1 gelijk is aan nul). □

Stelling 6.2.2 (De stelling van MacWilliams)
Is $A(X, Y)$ de gewichtspolynoom van een lineaire $[n, k]$-code C over $\text{GF}(q)$ en is $A^\perp(X, Y)$ de gewichtspolynoom van de duale code $C^\perp$, dan is

$$A^\perp(X, Y) = q^{-k} A(Y - X, Y + (q - 1)X).$$

Bewijs. In Lemma 6.2.1 nemen wij voor B de vectorruimte $\mathbb{C}[X, Y]$ van alle polynomen in twee variabelen X, Y over $\mathbb{C}$. Verder stellen wij

$$\bar{v}^\varphi = X^{w(\bar{v})} Y^{n-w(\bar{v})}, \bar{v} \in F^n.$$

Ook voeren wij volgende notatie in: voor $a \in \mathrm{GF}(q)$ is $w(a) = 1$ als $a \neq 0$ en $w(0) = 0$.

Dan geldt, met de notaties van Lemma 6.2.1,

$$\begin{aligned}
\bar{u}^{\psi} &= \sum_{\bar{v}\in F^n} \bar{u}^{\chi_{\bar{v}}}\bar{v}^{\varphi} = \sum_{\bar{v}\in F^n} \bar{u}^{\chi_{\bar{v}}} X^{w(\bar{v})}Y^{n-w(\bar{v})} \\
&= \sum_{v_1\in F} \cdots \sum_{v_n\in F} (u_1v_1 + \cdots + u_nv_n)^{\chi} X^{w(v_1)+\cdots+w(v_n)}Y^{(1-w(v_1))+\cdots+(1-w(v_n))} \\
&= (\sum_{v\in F} (u_1v)^{\chi} X^{w(v)}Y^{1-w(v)}) \cdots (\sum_{v\in F} (u_nv)^{\chi} X^{w(v)}Y^{1-w(v)}) \\
&= \prod_{i=1}^{n} (\sum_{v\in F} (u_iv)^{\chi} X^{w(v)}Y^{1-w(v)}).
\end{aligned}$$

Nu is voor $u_i = 0$ voldaan aan

$$\sum_{v\in F} (u_iv)^{\chi} X^{w(v)}Y^{1-w(v)} = Y + (q-1)X,$$

en voor $u_i \neq 0$ aan

$$\begin{aligned}
\sum_{v\in F} (u_iv)^{\chi} X^{w(v)}Y^{1-w(v)} &= Y + (\sum_{\beta\in F-\{0\}} \beta^{\chi})X \\
&= Y - X \text{ (aangezien } \sum_{\beta\in F} \beta^{\chi} = 0).
\end{aligned}$$

Bijgevolg is

$$\bar{u}^{\psi} = (Y + (q-1)X)^{n-w(\bar{u})}(Y - X)^{w(\bar{u})}.$$

In Lemma 6.2.1 stellen wij nu $V = C$. Uit Lemma 6.2.1 volgt dan

$$\begin{aligned}
A^{\perp}(X, Y) &= \sum_{\bar{v}\in C^{\perp}} X^{w(\bar{v})}Y^{n-w(\bar{v})} \\
&= \sum_{\bar{v}\in C^{\perp}} \bar{v}^{\varphi} \\
&= q^{-k} \sum_{\bar{u}\in C} \bar{u}^{\psi} \\
&= q^{-k} \sum_{\bar{u}\in C} (Y - X)^{w(\bar{u})}(Y + (q-1)X)^{n-w(\bar{u})} \\
&= q^{-k} A(Y - X, Y + (q-1)X).
\end{aligned}$$

□

Gevolg 6.2.3
Is $A(X, Y)$ de gewichtspolynoom van een binaire lineaire $[n, k]$-code C en is $A^{\perp}(X, Y)$ de gewichtspolynoom van de duale code $C^{\perp}$, dan is

$$A^{\perp}(X, Y) = 2^{-k} A(Y - X, Y + X).$$

Bewijs. Onmiddellijk uit voorgaande stelling. □

Voorbeeld 6.2.4
Herneem Voorbeeld 6.1.1. Hier is

$$\begin{aligned} A^{\perp}(X,Y) &= 2^{-2}[(Y+X)^5 + 2(Y-X)^3(Y+X)^2 + (Y-X)^4(Y+X)] \\ &= Y^5 + 2X^2Y^3 + 4X^3Y^2 + X^4Y. \end{aligned}$$

Opmerkingen 6.2.5

(i) Onderstel dat wij de gewichtspolynoom moeten berekenen van een $[n,k]$-code over GF(q) met k groot. Het nagaan van de gewichten van de q^k codewoorden kan dan een enorm werk zijn. Indien $n-k=r$ klein is bevat $C^{\perp}$ echter q^r, dus een relatief klein aantal, codewoorden. Het is dan mogelijk dat de gewichtspolynoom van $C^{\perp}$ gemakkelijk te berekenen is. Stelling 6.2.3 geeft ons nu onmiddellijk de gewichtspolynoom van C.

(ii) Onderstel dat $C = C^{\perp}$, m.a.w. de lineaire code C is *zelfduaal*. Dan is

$$A(X,Y) = A^{\perp}(X,Y) = q^{-k}A(Y-X, Y+(q-1)X).$$

Deze gelijkheid van polynomen geeft ons een aantal betrekkingen tussen de coëfficiënten A_i. Wij bekomen dus een reeks sterke nodige voorwaarden waaraan de A_i's moeten voldoen opdat C zelfduaal zou zijn.

6.3 Waarschijnlijkheid van foutdetectie

Onderstel dat C een binaire lineaire code is, dat het kanaal binair symmetrisch is, en dat p de symboolfout waarschijnlijkheid is. In 4.4 zagen wij dat

$$P_{\text{undetec}}(C) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i},$$

met A_i het aantal codewoorden met gewicht i. Dus is

$$P_{\text{undetec}}(C) = A(p, 1-p) - (1-p)^n,$$

met $A(X,Y)$ de gewichtspolynoom van C.

Hoofdstuk 7

Hamming codes

In dit hoofdstuk bestuderen we de Hamming codes. Deze codes werden ontdekt door Hamming (1950) en Golay (1949).

Figuur 7.1: Richard Wesley Hamming

Richard Wesley Hamming werd op 11 februari 1915 in Chicago, Illinois, Verenigde Staten, geboren.

Hij studeerde aan de Universiteit van Chicago, en behaalde in 1937 de graad van bachelor of science. Dan ging hij aan de Universiteit van Nebraska studeren waar hij in 1939 de graad van master of arts behaalde. Daarna behaalde hij in 1942 de graad van doctor in de wiskunde aan de Universiteit van Illinois at Urbana-Champaign. Zijn doctoraatsproefschrift Some Problems in the Boundary Value Theory of Linear Differential Equations *schreef hij onder de leiding van Waldemar Trjitzinsky.*

In 1945 ging Richard Hamming voor het Manhattan Project werken, een onderzoeksproject van de regering van de Verenigde Staten om een atoombom te maken. Dit project werd het Manhattan Project genoemd omdat het eerste onderzoek verricht was aan Columbia University in Manhattan. Richard Hamming werkte echter in Los Alamos voor dit project.

Na het einde van de tweede wereldoorlog ging Hamming in 1946 voor Bell Telephone Laboratories werken. Daar kon hij samenwerken met Shannon en Tukey. Hij heeft tot 1976 voor Bell

Telephones gewerkt tot hij een leerstoel in de computerwetenschappen aanvaardde aan de Naval Postgraduate School in Monterey, Californië.

Hamming is het best gekend voor zijn werk over foutendetecterende en -verbeterende codes. Zijn fundamenteel artikel over dit onderwerp verscheen in 1950 en hij startte hiermee een nieuw onderwerp binnen de informatietheorie. Hamming codes zijn van fundamenteel belang in de codeertheorie en zijn van praktisch nut bij het ontwerpen van computers.

Onderzoek over codes staat in verband met packing problemen, en foutenverbeterende codes ontworpen door Hamming hebben geleid tot de oplossing van een packing probleem betreffende matrices over eindige velden.

In 1956 werkte Hamming aan het ontwerp van een vroege computer, de IBM 650. Zijn werk leidde tot de ontwikkeling van een programmeertaal die zich ontwikkeld heeft tot de hogere-orde programmeertalen die in de hedendaagse computers gebruikt worden.

Hamming werkte ook op numerieke analyse, en op de integratie van differentiaalvergelijkingen.

Zijn belangrijkste werken omvatten onder andere Numerical Methods for Scientists and Engineers *(1962),* Introduction to applied numerical analysis *(1971),* Digital filters *(1977),* Coding and information theory *(1980),* Methods of mathematics applied to calculus, probability, and statistics *(1985),* Introduction to applied numerical analysis *(1989),* The Art of Probability for Scientists and Engineers *(1991), en* The Art of Doing Science and Engineering: Learning to Learn *(1997).*

Hamming heeft veel onderscheidingen ontvangen voor zijn baanbrekend werk. In 1968 werd hij tot lid verkozen van het Institute of Electrical and Electronics Engineers, en kreeg hij de Turing prijs van de Association for Computing Machinery. The Institute of Electrical and Electronics Engineers kende Hamming in 1979 de Emanuel R. Piore prijs toe, en kende hem in 1988 een medaille toe For exceptional contributions to information sciences and systems.

Het IEEE hebben hun medaille de Hamming medaille *genoemd ter ere van hem.*

Verdere onderscheidingen zijn onder andere de verkiezing tot lid van de National Academy of Engineering in 1980, en de Harold Pender prijs van de Universiteit van Pennsylvania in 1981. Hij verkreeg in 1996 in Munchen de prestigieuze $130.000 Eduard Rheim Award for Achievement in Technology voor zijn werk op foutenverbeterende codes.

Naar aanleiding van de dood van Richard Hamming op 7 januari 1998 te Monterey, Californië, schreef Richard Franke van de Naval Postgraduate School in Monterey:

Hij zal heel lang herinnerd worden voor zijn diep inzicht in vele aspecten van wetenschap en computergebruik. Ik zal hem ook heel lang herinneren voor zijn rode tartan sportvest en zijn slechte moppen.

James F. Kaiser schreef in een kort in memoriam aan Hamming:

Wij zullen allen zijn inspirerende geest en zijn doorgrondend inzicht in wetenschappelijke zaken, ingenieurszaken en alledaagse zaken missen.

(http://turnbull.mcs.st-and.ac.uk/~history/Mathematicians/Hamming.html)

7.1 Binaire Hamming codes

Belangrijk voor de praktijk zijn de Hamming codes. Wij definiëren deze codes eerst over GF(2), daarna over GF(q).

Definitie 7.1.1
Onderstel dat $r \in \mathbb{N} - \{0, 1\}$ en dat H de $r \times (2^r - 1)$-matrix is met als kolommen alle vectoren van $V(r, 2) - \{\bar{0}\}$. De binaire code met H als pariteit controlematrix noemt men een *binaire Hamming code*; deze code wordt voorgesteld door $\mathrm{Ham}(r, 2)$.

$\mathrm{Ham}(r, 2)$ heeft lengte $n = 2^r - 1$ en dimensie $k = n - r$. Bijgevolg is $r = n - k$ de overtalligheid van de code. Aangezien de orde waarin de kolommen van H genomen worden niet bepaald is, is voor gegeven r $\mathrm{Ham}(r, 2)$ bepaald op gelijkwaardigheid na.

Voorbeelden 7.1.2
(i) $r = 2$. Hier is

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

Dus is $G = [1\,1\,1]$, zodat $\mathrm{Ham}(2, 2)$ de binaire herhalingscode van lengte 3 is.

(ii) $r = 3$. Hier is

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

De orde van de kolommen is hier zodanig dat de $i$de kolom de binaire voorstelling is van $i \in \mathbb{N}, i = 1, 2, \ldots, 7$. Een pariteit controlematrix van $\mathrm{Ham}(3, 2)$ in standaardvorm is

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

De corresponderende voortbrengende matrix in standaardvorm is

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Uit 3.3.4(ii) volgt nu onmiddellijk dat $\mathrm{Ham}(3, 2)$ gelijkwaardig is met de perfecte $[7, 4, 3]$-code van Voorbeeld 2.3.8.

Stelling 7.1.3
De binaire Hamming code Ham$(r, 2), r \geq 2$, is een perfecte $[2^r - 1, 2^r - 1 - r, 3]$-code.

Bewijs. Ham$(r,2)$ heeft lengte $n = 2^r - 1$ en dimensie $k = n - r = 2^r - 1 - r$. Stel Ham$(r,2) = C$. Er geldt $d(C) = w(C)$. Is $w(\bar{x}) = 1$, met $\bar{x} \in C - \{\bar{0}\}$, dan volgt uit $\bar{x}H' = 0$ dat $(00\ldots0)'$ een kolom is van H, een strijdigheid. Onderstel nu dat $w(\bar{x}) = 2, \bar{x} \in C - \{\bar{0}\}$, waarbij de $i$de coördinaat en de $j$de coördinaat $(i \neq j)$ van $\bar{x}$ niet nul zijn. Dan volgt uit $\bar{x}H' = 0$ dat de $i$de en de $j$de kolom van H gelijk zijn, een strijdigheid. Dus is $w(C) \geq 3$. In H komen de kolommen $(1\,0\ldots0)', (0\,1\,0\ldots0)', (1\,1\,0\ldots0)'$ voor, bijvoorbeeld op de resp. $i$de, $j$de, $k$de plaats. Stel dan $\bar{x} = 0\ldots010\ldots010\ldots010\ldots0$, met de drie elementen 1 op de $i$de, $j$de, $k$de plaats. Dan is $\bar{x}H' = 0$, zodat $\bar{x} \in C$. Uit $w(\bar{x}) = 3$ volgt nu onmiddellijk dat $w(C) = 3$, zodat $d(C) = 3$.

Ten slotte tonen wij aan dat Ham$(r,2)$ perfect is. Het eerste lid in de bolpakkingsongelijkheid (zie Stelling 2.3.5) is

$$2^{n-r}\left(1 + \binom{n}{1}\right) = 2^{n-r}(1+n) = 2^n,$$

terwijl het tweede lid eveneens gelijk is aan 2^n. Aangezien wij gelijkheid hebben in de bolpakkingsformule is Ham$(r,2)$ perfect. □

7.2 Decoderen bij binaire Hamming codes

Aangezien Ham$(r,2)$ een perfecte één-foutverbeterende code is zijn de nevenklasseleiders juist alle $2^r = n+1$ vectoren van $V(n,2)$ met gewicht ≤ 1 (zie 4.2).

Het syndroom van de nevenklasseleider $0\ldots010\ldots0$, met 1 in de $j$de positie, is het getransponeerde van de $j$de kolom van H. Indien nu de $j$de kolom van H de binaire representatie van het natuurlijk getal j is, dan hebben wij volgend decodeeralgoritme.

Stap 1. Voor de ontvangen vector $\bar{y}$ berekenen wij het syndroom $S(\bar{y}) = \bar{y}H'$.

Stap 2. Is $S(\bar{y}) = \bar{0}$, dan decoderen wij $\bar{y}$ als $\bar{y}$.

Stap 3. Is $S(\bar{y}) \neq \bar{0}$, dan nemen wij aan dat er één fout gemaakt is, met name in de positie met binaire representatie $S(\bar{y})$.

Voorbeeld 7.2.1
Beschouw Ham$(3,2)$ met H zoals in Voorbeeld 7.1.2(ii).
Onvangen wij $\bar{y} = 0\,1\,0\,1\,0\,1\,1$, dan is $S(\bar{y}) = 111$, dit is de binaire voorstelling van 7, zodat $\bar{y}$ gedecodeerd wordt als $\bar{x} = 0\,1\,0\,1\,0\,1\,0$.

7.3 Uitgebreide binaire Hamming codes

De uitgebreide Hamming code $\widehat{\text{Ham}}(r,2)$ is de code die men uit Ham$(r,2)$ verkrijgt door het toevoegen van een pariteit controlesymbool (zie bewijs van Stelling 2.2.10). Men toont gemakkelijk aan dat de uitgebreide code $\hat{C}$ van een lineaire binaire code C opnieuw lineair

is. Uit het bewijs van Stelling 2.2.10 volgt dan dat $\widehat{\mathrm{Ham}}(r,2)$ een binaire $[2^r, 2^r-1-r, 4]$-code is. Aangezien de minimum afstand van $\widehat{\mathrm{Ham}}(r,2)$ even is, is $\widehat{\mathrm{Ham}}(r,2)$ zeer geschikt voor toepassen van onvolledige decodering (worden er 2 fouten gemaakt, dan komt de ontvangen vector $\bar{y}$ terecht in het benedendeel van het standaard rooster, en vragen wij om retransmissie; zie 5.3).

Onderstel dat H een pariteit controlematrix van $\mathrm{Ham}(r,2)$ is. Stel dan

$$\hat{H} = \begin{bmatrix} & & & & 0 \\ & & H & & 0 \\ & & & & \vdots \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix}.$$

De matrix $\hat{H}$ is een $(r+1) \times 2^r$-matrix, met rang $\hat{H} = r+1$. Bovendien is $\hat{\bar{x}}\hat{H}' = 0$ voor elke vector van $\widehat{\mathrm{Ham}}(r,2)$. Hieruit volgt dat $\hat{H}$ een pariteit controlematrix van $\widehat{\mathrm{Ham}}(r,2)$ is.

Is de $j$de kolom van H de binaire representatie van het natuurlijk getal j, dan hebben wij het volgende decodeeralgoritme wat betreft $\widehat{\mathrm{Ham}}(r,2)$. Merk hierbij op dat het syndroom van de nevenklasseleider $00\dots010\dots0$, met de 1 op de $j$de plaats, het getransponeerde is van de $j$de kolom van $\hat{H}$.

(i) Voor de ontvangen vector $\bar{y}$ berekenen wij het syndroom $S(\bar{y}) = \bar{y}\hat{H}' = s_1 s_2 \dots s_{r+1}$.

(ii) Is $s_1 s_2 \dots s_{r+1} = \bar{0}$, dan decoderen wij $\bar{y}$ als $\bar{y}$.

(iii) Is $s_{r+1} = 0$ en $s_1 s_2 \dots s_r \neq \bar{0}$, dan bevindt $\bar{y}$ zich in het benedendeel van het standaard rooster, zodat wij om retransmissie vragen.

(iv) Is $s_{r+1} = 1$ en $s_1 s_2 \dots s_r = \bar{0}$, dan nemen wij aan dat er juist één fout gemaakt werd, met name in de laatste positie.

(v) Is $s_{r+1} = 1$ en $s_1 s_2 \dots s_r \neq \bar{0}$, dan nemen wij aan dat er juist één fout gemaakt werd, met name in positie j waarbij $s_1 s_2 \dots s_r$ de binaire representatie van j is.

Voorbeeld 7.3.1
Beschouw $\widehat{\mathrm{Ham}}(3,2)$ met H zoals in Voorbeeld 7.1.2(ii).

Ontvangen wij $\bar{y} = 01010110$, dan is $S(\bar{y}) = 1110$, zodat wij om retransmissie vragen.

Ontvangen wij $\bar{y} = 01010111$, dan is $S(\bar{y}) = 1111$ en nemen wij aan dat er juist één fout gemaakt werd, namelijk in positie 7. De vector $\bar{y}$ wordt dus gedecodeerd als $\hat{\bar{x}} = 01010101$.

Ontvangen wij $\bar{y} = 01010100$, dan is $S(\bar{y}) = 0001$ en nemen wij aan dat er juist één fout gemaakt werd, namelijk in positie 8. De vector $\bar{y}$ wordt dus gedecodeerd als $\hat{\bar{x}} = 01010101$.

7.4 Minimum afstand en pariteit controlematrix

Alvorens Hamming codes over GF(q) te definiëren, tonen wij aan hoe de minimum afstand van een lineaire code kan afgeleid worden uit een pariteit controlematrix van de code.

Stelling 7.4.1
Onderstel dat C een lineaire $[n,k]$-code is over GF(q) *met pariteit controlematrix H. Dan is de minimum afstand van C gelijk aan d als en slechts als elke $d-1$ kolommen van H lineair onafhankelijk zijn en er tenminste één stel van d lineair afhankelijke kolommen is.*

Bewijs. Onderstel dat $d(C) = d$. Dan is ook $w(C) = d$. De kolommen van H noteren wij $\bar{h}_1, \ldots, \bar{h}_n$. Neem aan dat de kolommen $\bar{h}_{j_1}, \bar{h}_{j_2}, ..., \bar{h}_{j_{d-1}}$ lineair afhankelijk zijn. Dan bestaan elementen $x_{j_1}, x_{j_2}, \ldots, x_{j_{d-1}}$, niet allen nul, waarvoor

$$x_{j_1}\bar{h}_{j_1} + x_{j_2}\bar{h}_{j_2} + \ldots + x_{j_{d-1}}\bar{h}_{j_{d-1}} = 0.$$

Onderstel om de gedachten te vestigen dat $j_1 < j_2 < \ldots < j_{d-1}$. Is

$$\bar{x} = 0\ldots0x_{j_1}0\ldots0x_{j_2}0\ldots0x_{j_{d-1}}0\ldots0,$$

dan is $\bar{x}H' = 0$, zodat $\bar{x} \in C$. Maar $w(\bar{x}) \leq d-1$, een strijdigheid aangezien $w(C) = d$. Elke $d-1$ kolommen van H zijn dus lineair onafhankelijk. Aangezien $w(C) = d$ bestaat een codewoord $\bar{z}$ waarvoor $w(\bar{z}) = d$. Onderstel dat

$$\bar{z} = 0\ldots0z_{i_1}0\ldots0z_{i_2}0\ldots0z_{i_d}0\ldots0,$$

met $z_{i_1}z_{i_2}\ldots z_{i_d} \neq 0$. Uit $\bar{z}H' = 0$ volgt dat

$$z_{i_1}\bar{h}_{i_1} + z_{i_2}\bar{h}_{i_2} + \ldots + z_{i_d}\bar{h}_{i_d} = 0,$$

zodat de kolommen $\bar{h}_{i_1}, \bar{h}_{i_2}, \ldots, \bar{h}_{i_d}$ van H lineair afhankelijk zijn.

Omgekeerd onderstellen wij nu dat elke $d-1$ kolommen van H lineair onafhankelijk zijn, en dat H tenminste één stel van d lineair afhankelijke kolommen bezit. Stel $d(C) = w(C) = d'$. Is $d' > d$, dan volgt uit het eerste deel van het bewijs dat elke $d'-1\,(\geq d)$ kolommen van H lineair onafhankelijk zijn. Dus zijn ook elke d kolommen lineair onafhankelijk, een strijdigheid. Is $d' < d$, dan bezit H tenminste één stel van d' lineair afhankelijke kolommen. Elk stel van $d-1\,(\geq d')$ kolommen dat deze d' kolommen bevat bestaat dus uit $d-1$ lineair afhankelijke kolommen, een strijdigheid. Bijgevolg is $d' = d$, zodat $d(C) = d$. □

7.5 q-aire Hamming codes

Wij zoeken nu naar een q-aire lineaire code C met minimum afstand 3, gegeven overtalligheid $r\,(\geq 2)$ en maximale lengte n. Uit Stelling 7.4.1 volgt dan dat geen kolom van een pariteit controlematrix H van C uitsluitend uit nullen bestaat en dat elke twee kolommen van H lineair onafhankelijk zijn. Is $\bar{h}_i = (x_1^i, x_2^i, \ldots, x_r^i)'$ de $i$de kolom van H, dan stellen

$p_1(x_1^1, x_2^1, \ldots, x_r^1), \ldots, p_n(x_1^n, x_2^n, \ldots, x_r^n)$ dus n verschillende punten voor van de $(r-1)$-dimensionale projectieve ruimte $\mathrm{PG}(r-1,q)$ over $\mathrm{GF}(q)$. Aangezien $(q^r-1)/(q-1)$ het aantal punten van $\mathrm{PG}(r-1,q)$ is hebben wij $n \leq (q^r-1)/(q-1)$.
Onderstel nu dat H een $r \times n$-matrix is, waarbij $n = (q^r-1)/(q-1)$, en waarvoor de n kolommen stellen coördinaten bepalen van de $(q^r-1)/(q-1) = n$ punten van $\mathrm{PG}(r-1,q)$. De q-aire code met pariteit controlematrix H noemen wij een *q-aire Hamming code*, en stellen wij voor door $\mathrm{Ham}(r,q)$. Het is duidelijk dat $\mathrm{Ham}(r,2)$ de binaire Hamming code is die gedefinieerd werd in 7.1.1. Aangezien H ondubbelzinnig bepaald is op een permutatie van de kolommen na en op evenredigheidsfactoren ($\neq 0$) van de respectievelijke kolommen na, is $\mathrm{Ham}(r,q)$ ondubbelzinnig bepaald, op gelijkwaardigheid na, door de parameters r en q.

Stelling 7.5.1
De Hamming code $Ham(r,q), r \geq 2$, is een perfecte $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]$-code over $\mathrm{GF}(q)$.

Bewijs. Uit de constructie volgt onmiddellijk dat $n = (q^r-1)/(q-1)$ de lengte van $\mathrm{Ham}(r,q)$ is en dat $k = n - r = [(q^r-1)/(q-1)] - r$ de dimensie van $\mathrm{Ham}(r,q)$ is. Uit de constructie volgt eveneens dat elke twee kolommen van H lineair onafhankelijk zijn. De matrix H heeft 3 kolommen van de gedaante $(a,0,\ldots,0)', (0,b,0,\ldots,0)', (c,d,0,\ldots,0)'$ met $abcd \neq 0$. Het is duidelijk dat deze 3 kolommen lineair afhankelijk zijn. Uit Stelling 7.4.1 volgt nu onmiddellijk dat de minimum afstand van $\mathrm{Ham}(r,q)$ gelijk is aan 3. Wij tonen ten slotte aan dat $\mathrm{Ham}(r,q)$ perfect is.

Het eerste lid in de bolpakkingsongelijkheid (zie Stelling 2.3.5) is

$$q^{n-r}[1 + (q-1)\binom{n}{1}] = q^{n-r}(1 + q^r - 1) = q^n,$$

terwijl het tweede lid eveneens gelijk is aan q^n. Aangezien wij gelijkheid hebben in de bolpakkingsformule is $\mathrm{Ham}(r,q)$ perfect. □

Voorbeelden 7.5.2
Een eenvoudige manier om een pariteit controlematrix H voor $\mathrm{Ham}(r,q)$ neer te schrijven is er voor te zorgen dat in elke kolom de eerste cöordinaat verschillend van nul gelijk is aan 1 (dit is mogelijk aangezien elke kolom maar op een evenredigheidsfactor ($\neq 0$) na bepaald is).

(i) Een pariteit controlematrix voor $\mathrm{Ham}(2,5)$ is

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

(ii) Een pariteit controlematrix voor Ham$(3,3)$ is

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}.$$

(iii) Een pariteit controlematrix voor Ham$(2,4)$ is

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \text{x} & \text{x+1} \end{bmatrix},$$

met GF$(4) = \{0, 1, x, x+1\}$ en $x^2 + x + 1 = 0$.

7.6 Decoderen bij q-aire Hamming codes

Aangezien Ham(r, q) een perfecte één-foutverbeterende code is zijn de nevenklasseleiders juist alle $1 + n(q-1) = q^r$ vectoren van $V(n, q)$ met gewicht ≤ 1 (zie 4.2).

Het syndroom van de nevenklasseleider $0 \ldots 0b0 \ldots 0, b \neq 0$, met b in de $j$de positie, is het product van b met het getransponeerde van de $j$de kolom van H. Wij hebben dus volgend decodeeralgoritme.

Voor de ontvangen vector $\bar{y}$ berekenen wij het syndroom $S(\bar{y}) = \bar{y}H'$. Is $S(\bar{y}) = \bar{0}$, dan decoderen wij $\bar{y}$ als $\bar{y}$. Is $S(\bar{y}) \neq \bar{0}$, dan is $S(\bar{y}) = b\bar{h}'_j, b \neq 0$, voor een bepaalde kolom $\bar{h}_j$ van H. In zulk geval nemen wij aan dat er één fout gemaakt is en decoderen wij $\bar{y}$ door b af te trekken in de $j$de positie.

Voorbeeld 7.6.1
Beschouw Ham$(2,4)$ met pariteit controlematrix zoals in Voorbeeld 7.5.2(iii). Onderstel dat $\bar{y} = (1, x, x+1, x, 1)$ ontvangen wordt. Dan is $S(\bar{y}) = (x, x) = x(1, 1)$. De vector $\bar{y}$ wordt dus gedecodeerd als het codewoord $\bar{x} = \bar{y} - x(0, 0, 1, 0, 0) = (1, x, 1, x, 1)$.

7.7 Gewichtspolynomen van de Hamming en de duale Hamming codes

Wij zullen eerst aantonen dat de gewichtspolynomen van de q-aire duale Hamming codes bijzonder eenvoudig zijn.

Stelling 7.7.1
Elk codewoord $\bar{x} \neq \bar{0}$ van de duale Hamming code Ham$(r, q)^\perp$ heeft gewicht q^{r-1}.

Bewijs. Onderstel dat

$$H = \begin{bmatrix} \bar{y}_1 \\ \bar{y}_2 \\ \vdots \\ \bar{y}_r \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rn} \end{bmatrix}$$

een pariteit controlematrix is van $\mathrm{Ham}(r,q) = C$. Elk codewoord $\bar{x} \neq \bar{0}$ van $C^\perp$ is dan van de gedaante $\bar{x} = \lambda_1\bar{y}_1 + \lambda_2\bar{y}_2 + \ldots + \lambda_r\bar{y}_r$ met $(\lambda_1, \lambda_2, \ldots, \lambda_r) \neq (0, 0, \ldots, 0)$. Is $n_0(\bar{x})$ het aantal coördinaten van $\bar{x}$ gelijk aan nul, dan geldt $w(\bar{x}) = n - n_0(\bar{x})$. De $j$de coördinaat van $\bar{x}$ is nul a.s.a. $\lambda_1 a_{1j} + \lambda_2 a_{2j} + \ldots + \lambda_r a_{rj} = 0$, dit is a.s.a. $\lambda_1 z_1 + \lambda_2 z_2 + \ldots + \lambda_r z_r = 0$, met $[z_1 z_2 \ldots z_r]'$ de $j$de kolom van H. Aangezien de kolommen van H alle punten van $\mathrm{PG}(r-1,q)$ voorstellen, is het aantal kolommen van H waarvoor voldaan is aan de vergelijking $\lambda_1 X_1 + \lambda_2 X_2 + \ldots + \lambda_r X_r = 0$ gelijk aan het aantal punten van $\mathrm{PG}(r-1,q)$ in het hypervlak $\lambda_1 X_1 + \lambda_2 X_2 + \ldots + \lambda_r X_r = 0$ van $\mathrm{PG}(r-1,q)$; dit aantal kolommen is dus gelijk aan $(q^{r-1}-1)/(q-1)$. Bijgevolg is $n_0(\bar{x}) = (q^{r-1}-1)/(q-1)$, zodat $w(\bar{x}) = n - (q^{r-1}-1)/(q-1) = [(q^r-1)/(q-1)] - [(q^{r-1}-1)/(q-1)] = q^{r-1}$. □

Gevolg 7.7.2
De gewichtspolynoom van Ham$(r,q)^\perp$ is

$$A^\perp(X,Y) = Y^n + (q^r-1)X^{q^{r-1}}Y^{n-q^{r-1}}.$$

In het binaire geval wordt dit

$$A^\perp(X,Y) = Y^n + nX^{(n+1)/2}Y^{(n-1)/2}.$$

De gewichtspolynoom van Ham(r,q) is

$$A(X,Y) = q^{-r}[(Y+(q-1)X)^n + (q^r-1)(Y-X)^{q^{r-1}}(Y+(q-1)X)^{n-q^{r-1}}].$$

In het binaire geval wordt dit

$$A(X,Y) = 2^{-r}[(Y+X)^n + n(Y-X)^{(n+1)/2}(Y+X)^{(n-1)/2}].$$

Bewijs. Dit is een onmiddellijk gevolg van Stellingen 7.7.1 en 6.2.2. □

Voorbeeld 7.7.3
Beschouw $\mathrm{Ham}(3,3)$. Dan is

$$A^\perp(X,Y) = Y^{13} + 26X^9Y^4,$$

en

$$\begin{aligned} A(X,Y) &= 3^{-3}[(Y+2X)^{13} + 26(Y-X)^9(Y+2X)^4] \\ &= 288X^{13} + 2080X^{12}Y + 5616X^{11}Y^2 + 11232X^{10}Y^3 \\ &+ 13442X^9Y^4 + 11934X^8Y^5 + 8424X^7Y^6 + 4056X^6Y^7 \\ &+ 1404X^5Y^8 + 468X^4Y^9 + 104X^3Y^{10} + Y^{13}. \end{aligned}$$

Hoofdstuk 8

Designs

8.1 Inleiding tot de theorie van de designs

Een $t-(v,k,\lambda)$ *design* of kortweg een *t-design*, met $t,v,k,\lambda \in \mathbb{N}$ en $v > k > 1, k \geq t \geq 1, \lambda > 0$, is een geordend drietal $\mathcal{D} = (P, B, \mathrm{I})$ bestaande uit disjuncte eindige verzamelingen P, B en een incidentierelatie $\mathrm{I} \subseteq P \times B$ waarvoor voldaan is aan :

(i) $|P| = v$ en elk element $L \in B$ is incident met juist k elementen van P (dit is, voor elk element $L \in B$ bestaan er juist k elementen $p \in P$ waarvoor $(p, L) \in \mathrm{I}$);

(ii) elke t verschillende elementen van P zijn incident met juist λ elementen van B (dit is, zijn $p_1, p_2, \ldots, p_t$ t verschillende elementen van P, dan bestaan er juist λ elementen $L_1, L_2, \ldots, L_\lambda$ in B waarvoor $(p_i, L_j) \in \mathrm{I}, i = 1, 2, \ldots, t$ en $j = 1, 2, \ldots, \lambda$).

De elementen van P worden de *punten (points)* van de design genoemd; de elementen van B worden de *blokken (blocks)* van de design genoemd. Is $(p, L) \in \mathrm{I}$, m.a.w. $p\,\mathrm{I}\,L$, dan zegt men dat het punt p incident is met de blok L, dat de blok L incident is met het punt p, dat p op de blok L ligt, dat L door het punt p gaat, dat L het punt p bevat, enz.

Een *isomorfisme* van een design $\mathcal{D} = (P, B, \mathrm{I})$ op een design $\mathcal{D}' = (P', B', \mathrm{I}')$ is een bijectie α van $P \cup B$ op $P' \cup B'$ waarvoor $P^\alpha = P', B^\alpha = B', x\,\mathrm{I}\,L \iff x^\alpha\,\mathrm{I}'\,L^\alpha$ met $x \in P$ en $L \in B$. Bestaat er een isomorfisme van de design $\mathcal{D}$ op de design $\mathcal{D}'$, dan noemen wij $\mathcal{D}$ en $\mathcal{D}'$ *isomorf* en schrijven wij $\mathcal{D} \cong \mathcal{D}'$. Is $\mathcal{D}$ een $t-(v,k,\lambda)$ design en is $\mathcal{D}$ isomorf met de design $\mathcal{D}'$, dan is $\mathcal{D}'$ eveneens een $t-(v,k,\lambda)$ design. Is $\mathcal{D} = \mathcal{D}'$, dan spreken wij van een *automorfisme* in plaats van een isomorfisme. De groep van alle automorfismen van de design $\mathcal{D}$ noteren wij Aut $\mathcal{D}$.

Beschouw een $t-(v,k,\lambda)$ design $\mathcal{D} = (P, B, \mathrm{I})$. De verzameling van alle punten incident met de blok $L \in B$ noteren wij L_P. Impliceert $L \neq M$ dat $L_P \neq M_P$ dan definieert $L \mapsto L_P$ een bijectie van B op de verzameling B_P der elementen L_P, en noemt men $\mathcal{D}$ een design zonder *repeterende blokken*. In zulk geval is $\mathcal{D} \cong \mathcal{D}_P$ met $\mathcal{D}_P = (P, B_P, \mathrm{I}_P)$ en

$p \, \mathrm{I}_P \, L_P \Longleftrightarrow p \in L_P$. Hier kunnen wij dus gerust werken met de design $\mathcal{D}_P$ waarvoor de blokken puntenverzamelingen zijn en waarvoor de incidentierelatie de relatie "$\in$" is.

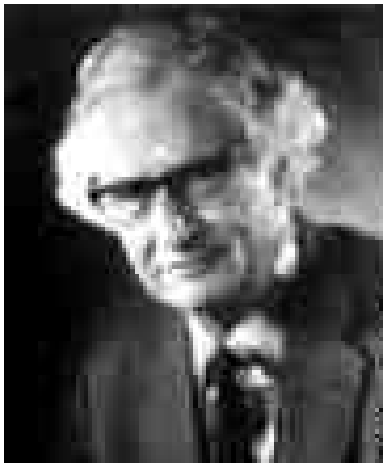
Beschouw de verzameling B van alle deelverzamelingen van de orde k van een verzameling P van de orde $v\,(v > k > 1)$. Is I de relatie "behoort tot", dan is $\mathcal{D} = (P, B, \mathrm{I})$ een $k-(v,k,1)$ design. Omgekeerd beschouwen wij nu een willekeurige $k-(v,k,1)$ design $\mathcal{D} = (P, B, \mathrm{I})$. Dan heeft $\mathcal{D}$ geen repeterende blokken (moest $L_P = M_P$, met $L \neq M$, dan zouden de k punten van de blok L incident zijn met tenminste twee blokken L, M, een strijdigheid), en is $\mathcal{D}_P$ een design van het hierboven beschreven type. Een $k-(v,k,1)$ design $\mathcal{D}$ noemen wij een *complete design*.

Een t-design $\mathcal{D}$ waarvoor $\lambda = 1$ wordt een *Steiner systeem (Steiner system)* genoemd. Een Steiner systeem heeft geen repeterende blokken (moest $L_P = M_P$ met $L \neq M$, dan zouden t punten van de blok L incident zijn met tenminste twee blokken L, M, een strijdigheid). De blokken van een Steiner systeem met $t = 2$ worden ook dikwijls *rechten* genoemd.

Een *balanced incomplete block design (BIBD)* is een 2-design die niet compleet is.

Opmerking 8.1.1
Het begrip design werd ingevoerd in 1939 door de statisticus F. Yates in een voordracht die gehouden werd voor de Royal Statistical Society in Londen. Een andere pionier in de theorie van de designs is de statisticus R.A. Fisher (1890-1962). Steiner systemen met $k = 3$ en $t = 2$ werden reeds bestudeerd door Steiner in 1853.

We geven hierna de biografieën van F. Yates en R.A. Fisher.



Figuur 8.1: Frank Yates

Frank Yates werd op 12 mei 1902 in Manchester, Engeland, geboren. Hij studeerde aan Wadham House, een private school waar de wiskundeleraar een uitstekende wiskundige en leraar was die Frank beinvloedde in de richting van wiskunde. Hij bekwam in 1916 een beurs voor Clifton College. Vier jaar later kreeg hij een beurs om te gaan studeren aan Saint John's College in Cambridge. Hij studeerde in 1924 cum laude af na heel goede studies aan de Universiteit

van Cambridge, maar hij leek in die tijd nooit op de uitstekende geleerde die hij uiteindelijk zou worden.

Na twee jaar wiskundelessen gegeven te hebben, besloot hij het lesgeven te verlaten, en trad toe tot de Gold Coast Survey als wiskundig adviseur. Omwille van een slechte gezondheid besloot hij te proberen een positie in Engeland te bekomen, en, na het postuleren bij R.A. Fisher, werd hij in 1931 benoemd tot assistent statistiek aan het Rothamsted Experimental Station.

Toen Fisher in 1933 een leerstoel kreeg aan University College in London, werd Yates benoemd tot hoofd statistiek in Rothamsted. Hij bleef hoofd statistiek tot zijn pensioen in 1968.

Frank Yates werkte op het ontwerp van experimenten, vaak samenwerkend met Fisher. Tijdens wereldoorlog II bestudeerde hij voedselvoorzieningen en toepassingen van meststoffen om gewassen te verbeteren. Hij paste zijn technieken voor het ontwerpen van experimenten toe op een grote variëteit aan problemen, zoals bijvoorbeeld de controle van plagen. Hij bleef na 1945 zijn statistische methoden toepassen op problemen betreffende de menselijke voeding.

Yates werd benoemd aan de United Nations Commission on Statistical Sampling, en publiceerde in 1949 Sampling Methods for Censuses and Surveys. *Hij was een enthousiast gebruiker van computers:*

· · · als je een goede theoretische statisticus wil zijn, dan moet je ook programmeren, en moet je daarom de beste computerhulpmiddelen hebben.

Hij was één van de personen die heel veel invloed hadden in het oprichten van de British Computer Society, en hij was de voorzitter van deze vereniging in 1960-1961.

Yates was een heel goed departementshoofd. In een toespraak op zijn herdenkingsdienst werd gezegd:

Frank Yates zijn manier om het departement te besturen was een opmerkelijke manier, in dat opzicht dat het een volledig onzichtbare manier was. Er waren praktisch geen reglementen, behalve het reglement waarin hij eiste dat geen enkel wetenschappelijk artikel het departement mocht verlaten zonder gelezen te worden, en gewoonlijk sterk verbeterd te worden, door hem.

Na zijn pensionering werd hij onderzoekslid aan Imperial College, London. Daar heeft hij voor de eerste keer in zijn leven gedoceerd, zonder echter veel succes te hebben. Zijn manier van doceren werd in een artikel beschreven als:

Hij was geen ideale lesgever, daar het hem ontbrak aan begrijpbare formele presentatie en daar hij verkoos te spreken over algemene ideeën.

De Royal Society van London kende hem in 1966 hun Royal Medal toe als:

· · · erkenning voor zijn fundamentele en ver-rijkende bijdragen aan de statistische methoden voor experimentele biologie.

Hij stierf op 17 juni 1994 in Harpenden, Engeland.

(http://turnbull.mcs.st-and.ac.uk/∼history/Mathematicians/Yates.html)

Figuur 8.2: Sir Ronald Aylmer Fisher

Sir Ronald Aylmer Fisher werd op 17 februari 1890 in London geboren.

R.A. Fisher zijn ouders waren Katie Heath, de dochter van een rechterlijk ambtenaar, en George Fisher, vennoot van Robinson and Fisher, een veilingmeestershuis in King Street, St. James, London. Katie en George hadden zeven kinderen, vier jongens en drie meisjes. Na de geboorte van Geoffrey in 1876 en van Evelyn in 1877 noemden zij hun derde kind, geboren in 1878, Alan. Hij stierf heel jong en Katie, die bijgelovig was, besloot dat al hun volgende kinderen de letter "y" in hun naam zouden hebben. Ronald Aylmer Fisher was de jongste van een tweeling, maar de oudste van de tweeling was doodgeboren.

In 1904 ging Ronald naar Harrow naar school, maar dit was een moeilijke tijd voor de veertienjarige jongen, daar zijn moeder dat jaar stierf aan acute buikvliesontsteking. Ondanks dit overlijden van zijn moeder blonk hij uit aan Harrow door in 1906 de Neeld medaille te winnen in een competitie, open voor de ganse school, voor wiskundeverhandelingen. Hij won een beurs van £80 voor Caius and Gonville College, Cambridge, die hij nodig had om zijn studies te financieren daar zijn vader zijn fortuin verloren had. Hij schreef zich in 1909 in Cambridge in.

Hoewel hij wiskunde en sterrenkunde studeerde in Cambridge, was hij ook geinteresseerd in biologie. In zijn tweede jaar begon hij te informeren bij hogere leden van de universiteit over de mogelijkheid om een Cambridge University Eugenics (rasveredeling) Society te vormen. Hij studeerde in 1912 met onderscheiding af. Zijn leraar vond echter dat hij nog beter kon, en schreef:

⋯ als hij zich volledig ingezet had, dan zou hij een eerste klas wiskundige geworden zijn, maar hij heeft het niet gedaan.

Na het bekomen van een beurs voor Wollaston bleef hij in Cambridge, onder leiding van Stratton, verder studeren over foutentheorie door Airy's handboek The Theory of Errors *te bestuderen. Het was Fisher's interesse in de foutentheorie die hem uiteindelijk leidde tot het onderzoeken van statistische problemen.*

Na het verlaten van Cambridge had Fisher geen financiële inkomsten meer, en hij werkte daardoor enkele maanden op een boerderij in Canada. Hij keerde naar London terug, en nam een

positie aan als statisticus aan de Mercantile and General Investment Company. Toen wereldoorlog I uitbrak in 1914 wilde hij zich enthousiast inschrijven in het leger, nadat hij reeds in Cambridge verbleven had aan het Officer's Training Corps. Zijn medische testen waren op alle vlakken heel goed, behalve voor zijn ogen, en hij werd geweigerd. Hij was van 1915 tot 1919 een wiskunde en fysica leraar in Rugby en in andere gelijkaardige scholen.

Zijn interesse voor rasveredeling en zijn ervaringen van zijn werk in een canadese boerderij leidden hem er toe om zelf een boerderij te beginnen. Hij werd in deze plannen gesteund door Gudruna, de echtgenote van een schoolvriend, en dit leidde hem tot een ontmoeting met Ruth Eileen Gratton Guinness, Gudruna's jongere zus. Dr. Henry Gratton Guinness, de vader van Ruth Eileen en Gudruna, was gestorven toen zij beiden heel jong waren, en Ruth Eileen, toen zestien jaar oud, wist dat haar moeder nooit zou toestemmen dat zij zo jong huwde. Bijgevolg huwde Fisher op 26 april 1917, tijdens een geheime huwelijksplechtigheid en slechts enkele dagen na Ruth Eileen's zeventiende verjaardag, met Ruth Eileen, zonder dat haar moeder het wist. Zij hadden twee zonen en zeven dochters, maar één van de kinderen stierf tijdens zijn kleutertijd.

Fisher stopte in 1919 met wiskundeleraar te zijn toen hij gelijktijdig twee posities aangeboden kreeg. Karl Pearson bood hem de positie van hoofdstatisticus bij Galton laboratories aan, en hij kreeg ook het aanbod om statisticus te worden bij het Rothamsted Agricultural Experiment Station. Dit laatste was het oudste agrarisch onderzoekscentrum in het Verenigd Koninkrijk. Dit onderzoekscentrum was in 1837 opgericht om de effecten van voeding en grondtypes op de fertiliteit van planten te bestuderen, en het sprak Fisher's interesse in landbouw aan. Hij nam de positie in Rothamsted aan waar hij vele bijdragen aan zowel statistiek, in bijzonder het ontwerp en analyseren van experimenten, als aan genetica leverde.

Daar bestudeerde hij het ontwerp van experimenten door het begrip van willekeurigheid en de variantie analyse in te voeren; methoden die nu gebruikt worden over gans de wereld. Fisher's idee was om een experiment te verdelen in een verzameling deelexperimenten die van elkaar verschillen in één of meerdere factoren of behandelingen die op hen toegepast worden. De deelexperimenten worden zo opgesteld dat verschillen in hun uitkomsten door middel van statistische analyse toegeschreven kunnen worden aan verschillende factoren of combinaties van factoren. Dit was een belangrijke vooruitgang in vergelijking met de toen bestaande benadering die enkel één factor per keer varieerde in een experiment, wat een relatief inefficiënte methode is.

In 1921 introduceerde hij het begrip waarschijnlijkheid. *In 1922 gaf hij een nieuwe definitie van statistiek. Zijn bedoeling was, zoals hij stelde, het verminderen van gegevens, en hij identificeerde drie fundamentele problemen. Deze drie problemen zijn:*

i. het specifiëren van het type populatie waaruit de data komt,

ii. schatting, en

iii. distributie.

Fisher publiceerde een aantal belangrijke teksten; in het bijzonder verscheen Statistical Methods for Research Workers *(1925) voortdurend in nieuwe edities. Het was een handboek over methoden voor het ontwerp en de analyse van experimenten die hij had ontwikkeld in Rothamsted. De bijdragen die Fisher geleverd heeft, omvatten de ontwikkeling van methoden geschikt voor kleine steekproeven, zoals deze van Gosset, en de ontdekking van de exacte distributies van vele types verdelingen. Fisher publiceerde* The design of experiments *(1935) en* Statistical tables

(1947). Zijn boeken:

· · · waren een revolutie in agrarisch onderzoek; daar zij de methoden beschreven, die nu wereldwijd gebruikt worden, om de resultaten van kleine steekproeven te evalueren en op die manier onze experimentele methoden op te stellen om de storingen te minimaliseren die te wijten zijn aan de verscheidenheid van de bodems en aan de onvermijdbare irregulariteit van biologisch materiaal.

Tijdens zijn verblijf aan het Agricultural Experiment Station had hij kweekexperimenten met muizen, slakken en gevogelte verricht, en de resultaten die hij bekwam hebben geleid tot theorieën over de dominantie van genen en fitheid, die hij publiceerde in The Genetical Theory of Natural Selection *(1930).*

Zijn werk over de natuurlijke selectie leidde Fisher tot het in vraag stellen hoe in ontwikkelde maatschappijen zwakke en relatief onvruchtbare mensen voordelen bekwamen over sterke gezonde individuen. Hij voelde dat de natuurlijke overleving van de beste methode om het menselijk ras te verbeteren artificieel aan het veranderen was door factoren die specifiek de minder goeden bevoordeelden. Als een sterke verdediger van maatregelen om deze trend tegen te gaan, stelde hij voor dat gezinsuitkeringen evenredig zouden zijn met het inkomen om de goed aangepaste gezonde leden uit de gemeenschap te steunen. Zoals verwacht kon worden, was deze opvatting heel onpopulair en hij vond heel weinig aanhangers voor deze theorie.

In 1933 ging Karl Pearson op pensioen als Professor rasveredeling aan University College, en Fisher werd benoemd tot zijn opvolger. Feitelijk werd deze positie opgesplitst in twee, daar Karl Pearson's zoon Egon Pearson ook benoemd werd. Fisher behield deze positie gedurende tien jaar, waarna hij in 1943 benoemd werd tot Arthur Balfour professor genetica aan de Universiteit van Cambridge. Eerder was hij verhuisd uit London toen de oorlog in 1939 uitbrak, en hij vond een tijdelijk verblijf in Harpenden. Hij ging in 1957 op pensioen in Cambridge, maar hij bleef zijn taken gedurende nog twee jaren verder vervullen tot een opvolger benoemd kon worden. Hij verhuisde dan naar de Universiteit van Adelaide waar hij zijn onderzoek verder zette gedurende de laatste drie jaar van zijn leven.

Er lag een zekere ironie in het feit dat Fisher Pearson in 1933 opvolgde daar beiden al lang een lopend dispuut hadden. Het dispuut begon in 1917 toen Pearson een artikel publiceerde waarin hij stelde dat Fisher er niet in geslaagd was om waarschijnlijkheid te onderscheiden van inverse probabiliteit in een artikel uit 1915. Hoewel Fisher toen nog maar pas op het begin van zijn carriere was, was hij kwaad dat Pearson een artikel gepubliceerd had waarin hij kritisch was over zijn eigen resultaten, zonder hem dit op voorhand te vertellen. Meer zelfs, hij aanvaardde de kritiek van Pearson niet, omdat hij vond dat hij correct was.

In feite waren de redenen voor de vete helemaal niet zo eenvoudig als ze gewoonlijk voorgesteld worden. De standaard verklaring is dat Fisher verbitterd geworden was omdat hij groot onrecht aangedaan was omdat zijn artikels geweigerd werden door wiskundigen die biologie niet begrepen, en door biologen die wiskunde niet begrepen. We beschouwen een voorbeeld om aan te tonen dat dit een vereenvoudiging van het probleem is. Fisher diende in 1918 zijn heel belangrijk artikel On the correlation between relatives on the supposition of Mendelian inheritance *in bij de Royal Society. Twee referenten, R.C. Punnett en Pearson, werden aangesteld voor dit artikel en brachten verslag uit over dit artikel. Geen van hen beiden weigerde het artikel, maar zij waren gereserveerd in hun oordeel en stelden duidelijk dat er aspecten aan het artikel waren waarvoor zij niet competent genoeg waren om deze te beoordelen. Daaropvolgend trok Fisher zijn artikel terug, en diende het*

in bij Transactions of the Royal Society of Edinburgh *waar het aanvaard werd voor publicatie. Het is niet verrassend dat Fisher's innoverende ideeën tijd nodig hadden om aanvaard te worden.*

De vete werd bitterder toen Pearson zijn positie als editor van Biometrika *gebruikte om Fisher's gebruik van de chi-kwadraat test in een artikel uit 1922 aan te vallen. Pearson ging veel verder, en beweerde dat Fisher statistiek een slechte dienst bewezen had door wereldwijd foutieve resultaten te publiceren. De Royal Statistical Society weigerde daarop de resultaten van Fisher te publiceren en daaropvolgend nam hij uit protest ontslag uit deze vereniging. Natuurlijk greep Fisher elke kans om Pearson aan te vallen, en het is gerechtvaardigd te zeggen dat ze elkaar haatten. Zelfs na de dood van Pearson in 1936 ging Fisher verder met zijn aanvallen op Pearson, wat de relatie in University College met Pearson's zoon, Egon Pearson die daar ook een leerstoel had, heel moeilijk maakte.*

Fisher werd in 1929 verkozen tot lid van de Royal Society, kreeg in 1938 de Royal Medal van deze Society, en kreeg in 1948 de Darwin Medal van deze Society.

In 1955 kreeg hij de Copley Medal van de Royal Society.

Hij werd in 1934 verkozen tot lid van de American Academy of Arts and Sciences, in 1941 tot lid van de American Philosophical Society, in 1948 tot lid van de International Society of Haematology en tot lid van de National Academy of Sciences of the United States, en in 1960 tot lid van de Kaiserlich Deutsche Akademie der Naturfoscher. Verschillende onderzoeksinstellingen kenden hem een eredoctoraat toe, zoals de Harvard University (1936), University of Calcutta (1938), University of London (1946), University of Glasgow (1947), University of Adelaide (1959), University of Leeds (1961), en het Indian Statistical Institute (1962). Hij werd geridderd in 1952.

Fisher's karakter wordt als volgt omschreven:

Hij was in staat om heel veel charme en warmte in vriendschap te tonen. Maar hij was ook het slachtoffer, zoals hij zelf erkende, van een oncontroleerbaar humeur; en vanwege zijn toewijding aan de wetenschappelijke waarheid die hij letterlijk passioneel zag, was hij een genadeloze vijand van allen die hij schuldig achtte aan het verkondigen van fouten.

Hij had ook andere sterktes en zwakheden:

Fisher sprong eruit als een doordringend denker; maar zijn publicaties waren voor vele lezers moeilijk. Sommige van zijn stellingen zijn effectief beter meegedeeld in de boeken van anderen die deze ideeën konden vereenvoudigen. Ook als docent was Fisher te moeilijk voor de gemiddelde student; zijn studenten vielen heel vlug af tot er nog twee of drie overbleven die het tempo van lesgeven aankonden. Hij was ook niet bijzonder succesvol in administratie; misschien slaagde hij er niet in de beperkingen van de gemiddelde mens te aanvaarden. Maar met zijn brede interessesfeer en doordringende geest was hij een heel stimulerende en gezellige prater.

Hij stierf op 29 juli 1962 in Adelaide, Australië.

(http://turnbull.mcs.st-and.ac.uk/∼history/Mathematicians/Fisher.html)

Voorbeelden 8.1.2

(a) Beschouw de m-dimensionale projectieve ruimte $\mathrm{PG}(m, q), m \geq 2$, over het Galois veld $\mathrm{GF}(q)$. Stel

P (punten) : verzameling van de punten van $\mathrm{PG}(m,q)$,

B (blokken) : verzameling van de rechten van $\mathrm{PG}(m,q)$,

I (incidentie) : natuurlijke incidentierelatie (een punt p is incident met een rechte L a.s.a. $p \subset L$).

Dan is $|P| = (q^{m+1}-1)/(q-1)$, het aantal punten incident met een blok is $q+1$, en door 2 verschillende punten gaat juist één blok. Bijgevolg is $\mathcal{D} = (P, B, \mathrm{I})$ een

$$2-(\frac{q^{m+1}-1}{q-1}, q+1, 1) \text{ design.}$$

Is $m = 2$, dan hebben wij een

$$2-(q^2+q+1, q+1, 1) \text{ design.}$$

(b) Een *(axiomatisch) projectief vlak ((axiomatic) projective plane)* is een geordend drietal $\mathcal{P} = (P, B, \mathrm{I})$ bestaande uit disjuncte verzamelingen P, B en een incidentierelatie $\mathrm{I} \subseteq P \times B$ waarvoor voldaan is aan :

(i) elke twee verschillende elementen van P zijn incident met juist één element van B;

(ii) elke twee verschillende elementen van B zijn incident met juist één element van P;

(iii) in P bestaan 4 elementen waarvan geen 3 incident zijn met een zelfde element van B.

De elementen van P worden de *punten* van het projectief vlak genoemd; de elementen van B worden de *rechten* van het projectief vlak genoemd. Is $(p, L) \in \mathrm{I}$, m.a.w. $p\,\mathrm{I}\,L$, dan zegt men dat het punt p incident is met de rechte L, dat de rechte L incident is met het punt p, dat p op de rechte L ligt, dat L door het punt p gaat, dat L het punt p bevat, enz. Isomorfismen tussen projectieve vlakken worden op analoge manier gedefinieerd als voor designs.

Is P en/of B eindig, dan zegt men dat $\mathcal{P}$ *eindig* is. In zulk geval bestaat een getal $n \in \mathbb{N} - \{0, 1\}$, de *orde (order)* van het projectief vlak genoemd, waarvoor $|P| = |B| = n^2+n+1$, waarvoor elke rechte $n+1$ punten bevat, en waarvoor door elk punt $n+1$ rechten gaan.

Een projectief vlak van de orde $n\,(\geq 2)$ is dus een $2-(n^2+n+1, n+1, 1)$ design. Omgekeerd toont men gemakkelijk aan dat elke $2-(n^2+n+1, n+1, 1)$ design met $n \geq 2$ een projectief vlak van de orde n is.

Men bewijst dat er (op een isomorfisme na) juist één projectief vlak van de orde $n \in \{2, 3, 4, 5, 7, 8\}$ bestaat, dat er geen projectief vlak van de orde 6 bestaat, dat er (op een isomorfisme na) juist 4 projectieve vlakken van de orde 9 bestaan, en dat er geen projectief vlak van de orde 10 bestaat; het niet-bestaan van een vlak van de orde 10 is een historisch resultaat dat met behulp van een computer (meer dan 10.000 uren) werd aangetoond door Lam, Thiel en Swiercz (1989). Uit (a) volgt dat een projectief vlak van de orde $q = p^h, p$ priem en $h \geq 1$, bestaat.

(c) Beschouw het projectieve vlak $\mathrm{PG}(2, q^2)$ over het Galois veld $\mathrm{GF}(q^2)$. In $\mathrm{PG}(2, q^2)$ beschouwen wij een niet-singuliere hermitische kromme H (ten opzichte van een behoorlijk gekozen basis kan H voorgesteld worden door de vergelijking $X_0^{q+1} + X_1^{q+1} + X_2^{q+1} = 0$). Dan is $|H| = q^3 + 1$ en elke rechte van $\mathrm{PG}(2, q^2)$ bevat 1 of $q + 1$ punten van H.

Definieer nu $\mathcal{D} = (P, B, \mathrm{I})$ met

$P = H$,

B: verzameling der rechten die $q + 1$ punten van H bevatten,

I: natuurlijke incidentierelatie (een punt p is incident met een rechte L a.s.a. $p \subset L$).

Dan is $|P| = q^3 + 1$, het aantal punten incident met een blok is $q + 1$, en door 2 verschillende elementen van P gaat juist één blok. Bijgevolg is $\mathcal{D} = (P, B, \mathrm{I})$ een

$$2 - (q^3 + 1, q + 1, 1) \text{ design.}$$

(d) Beschouw de m-dimensionale affiene ruimte $\mathrm{AG}(m, q), m \geq 2$, over het Galois veld $\mathrm{GF}(q)$. Stel

P: verzameling van de punten van $\mathrm{AG}(m, q)$,

B: verzameling van de rechten van $\mathrm{AG}(m, q)$,

I: natuurlijke incidentierelatie.

Dan is $|P| = q^m$, het aantal punten incident met een blok is q, en door twee verschillende punten gaat juist één rechte. Bijgevolg is $\mathcal{D} = (P, B, \mathrm{I})$ een

$$2 - (q^m, q, 1) \text{ design.}$$

Is $m = 2$, dan hebben wij een

$$2 - (q^2, q, 1) \text{ design.}$$

(e) Een *(axiomatisch) affien vlak ((axiomatic) affine plane)* is een geordend drietal $\mathcal{A} = (P, B, \mathrm{I})$ bestaande uit disjuncte verzamelingen P, B, resp. de verzameling der punten en de verzameling der rechten genoemd, en een incidentierelatie $\mathrm{I} \subseteq P \times B$ waarvoor, met de gebruikelijke terminologie, voldaan is aan :

(i) door elke twee verschillende punten gaat juist één rechte;

(ii) ligt het punt p niet op de rechte L, dan gaat door p juist één rechte die met L geen enkel punt gemeen heeft;

(iii) er bestaan 3 punten die niet op een gemeenschappelijke rechte gelegen zijn.

Is P en/of B eindig, dan zegt men dat $\mathcal{A}$ eindig is. In zulk geval bestaat er een getal $n \in \mathbb{N} - \{0, 1\}$, de *orde (order)* van het affien vlak $\mathcal{A}$ genoemd, waarvoor $|P| = n^2, |B| = n^2 + n$, waarvoor elke rechte n punten bevat, en waarvoor door elk punt $n + 1$ rechten gaan.

Een affien vlak van de orde n is dus een $2 - (n^2, n, 1)$ design. Omgekeerd toont men gemakkelijk aan dat elke $2 - (n^2, n, 1)$ design een affien vlak van de orde n is.

Beschouw een projectief vlak $\mathcal{P} = (P, B, \mathrm{I})$ en kies een rechte L. Stel $\mathcal{P}^L = (P^L, B^L, \mathrm{I}^L)$ met $P^L = \{x \in P \parallel x \not\mathrm{I}\, L\}, B^L = B - \{L\}, \mathrm{I}^L = \mathrm{I} \cap (P^L \times B^L)$. Dan toont men gemakkelijk aan dat $\mathcal{P}^L$ een affien vlak is. Is $\mathcal{P}$ eindig, dan is ook $\mathcal{P}^L$ eindig, en hebben $\mathcal{P}$ en $\mathcal{P}^L$ dezelfde orde n. Omgekeerd, is $\mathcal{A}$ een affien vlak dan bewijst men dat er altijd een projectief vlak $\mathcal{P}$ en een rechte L van $\mathcal{P}$ bestaan zodanig dat $\mathcal{A} = \mathcal{P}^L$; is $\mathcal{A}$ eindig, dan is vanzelfsprekend eveneens $\mathcal{P}$ eindig met dezelfde orde n als $\mathcal{A}$. Een projectief vlak van de orde n bestaat dus a.s.a. een affien vlak van de orde n bestaat.

(f) Beschouw de m-dimensionale affiene ruimte $\mathrm{AG}(m, 2), m \geq 3$, over het veld $\mathrm{GF}(2)$. Stel

P: verzameling van de punten van $\mathrm{AG}(m, 2)$,

B: verzameling van de vlakken van $\mathrm{AG}(m, 2)$,

I: natuurlijke incidentierelatie.

Dan is $|P| = 2^m$ en elke blok is incident met 4 punten. Aangezien geen 3 punten van $\mathrm{AG}(m, 2)$ collineair zijn (een affiene rechte $\mathrm{AG}(1, 2)$ over $\mathrm{GF}(2)$ bezit slechts 2 punten), zijn elke 3 punten van P incident met juist één blok. Bijgevolg is $\mathcal{D} = (P, B, \mathrm{I})$ een

$$3 - (2^m, 4, 1) \text{ design .}$$

Is $m = 3$, dan hebben wij een

$$3 - (8, 4, 1) \text{ design .}$$

Stelling 8.1.3
Is $\mathcal{D} = (P, B, \mathrm{I})$ een $t-(v,k,\lambda)$ design met $t > 1$, dan is voor elke $t' \in \mathbb{N}$ met $1 \leq t' < t$ $\mathcal{D}$ ook een $t'-(v,k,\lambda')$ design met

$$\lambda' = \lambda.\frac{(v-t')(v-t'-1)\dots(v-t+1)}{(k-t')(k-t'-1)\dots(k-t+1)}.$$

Bewijs. Beschouw $t' \in \mathbb{N}$ met $1 \leq t' < t$. Kies t' verschillende punten $p_1, p_2, \dots, p_{t'}$ in P. Noem U de verzameling van alle deelverzamelingen van de orde t van P die $p_1, p_2, \dots, p_{t'}$ bevatten, en noem V de verzameling van alle blokken van $\mathcal{D}$ die incident zijn met $p_1, p_2, \dots, p_{t'}$. Verder stellen wij $S = \{(T, L) \in U \times V \parallel$ de t elementen van T zijn incident met de blok $L\}$. Wij tellen nu het aantal elementen van S op twee verschillende manieren :

$$\begin{aligned} |S| &= \frac{(k-t')(k-t'-1)\dots(k-t+1)}{(t-t')!}|V| \\ &= \lambda|U| = \lambda\frac{(v-t')(v-t'-1)\dots(v-t+1)}{(t-t')!}. \end{aligned}$$

Dus is

$$|V| = \lambda\frac{(v-t')(v-t'-1)\dots(v-t+1)}{(k-t')(k-t'-1)\dots(k-t+1)}.$$

Bijgevolg is $\mathcal{D}$ een $t'-(v,k,\lambda')$ design met

$$\lambda' = \lambda\frac{(v-t')(v-t'-1)\dots(v-t+1)}{(k-t')(k-t'-1)\dots(k-t+1)}.$$

□

Gevolgen 8.1.4
(i) Is $\mathcal{D}$ een $t-(v,k,\lambda)$ design met $t > 1$, dan is voor elke t' met $1 \leq t' < t$ voldaan aan

$$(k-t')(k-t'-1)\dots(k-t+1) \text{ deelt } \lambda(v-t')(v-t'-1)\dots(v-t+1).$$

(ii) Is $\mathcal{D}$ een $t-(v,k,\lambda)$ design, dan is $\mathcal{D}$ ook een $1-(v,k,r)$ design, waarbij r het aantal blokken door een punt is. Voor $t > 1$ geldt

$$r = \lambda\frac{(v-1)(v-2)\dots(v-t+1)}{(k-1)(k-2)\dots(k-t+1)}.$$

Bewijs. Onmiddellijk gevolg van Stelling 8.1.3. □

Stelling 8.1.5
Is $\mathcal{D} = (P, B, \mathrm{I})$ een $t-(v,k,\lambda)$ design met $|B| = b$ en is r het aantal blokken incident met een punt, dan geldt

$$vr = bk.$$

Bewijs. Stel $S = \{(p, L) \in P \times B \,\|\, p \,\mathrm{I}\, L\}$. Wij tellen nu het aantal elementen van S op twee verschillende manieren :

$$|S| = r|P| = k|B| \text{ waaruit } rv = kb.$$

□

Stelling 8.1.6
Is $\mathcal{D} = (P, B, \mathrm{I})$ een $2-(v, k, \lambda)$ design, dan geldt

$$\begin{cases} vr = bk, \\ r(k-1) = \lambda(v-1). \end{cases}$$

Bewijs. In Stelling 8.1.5 hebben wij reeds bewezen dat $vr = bk$. Toepassing van Gevolg 8.1.4(ii) geeft

$$r = \lambda\frac{(v-1)}{(k-1)} \text{ waaruit } r(k-1) = \lambda(v-1).$$

□

Opmerkingen 8.1.7

(i) Is $\mathcal{D}$ een $t-(v, k, \lambda)$ design met $t \geq 2$, dan is $\mathcal{D}$ eveneens een $2-(v, k, \lambda')$ design zodat $r(k-1) = \lambda'(v-1)$.

(ii) Is $\mathcal{D}$ een $2-(v, k, \lambda)$ design, dan zijn b en r ondubbelzinnig bepaald door v, k, λ.

Definitie 8.1.8
Beschouw een $t-(v, k, \lambda)$ design $\mathcal{D} = (P, B, \mathrm{I})$ met $P = \{p_1, p_2, \ldots, p_v\}$ en $B = \{L_1, L_2, \ldots, L_b\}$. Een *incidentiematrix* van $\mathcal{D}$ is dan de $v \times b$-matrix $A = [a_{ij}]$ over $\mathbb{Q}$ waarvoor

$$a_{ij} = \begin{cases} 1 \text{ als } p_i \,\mathrm{I}\, L_j, \\ 0 \text{ als } p_i \not\mathrm{I}\, L_j. \end{cases}$$

Een andere indexering van punten en blokken geeft een incidentiematrix C die uit A kan verkregen worden na een permutatie van de rijen en kolommen. De matrix A is dus ondubbelzinnig bepaald door $\mathcal{D}$ op een permutatie van rijen en kolommen na.

De matrix in Voorbeeld 2.3.8 die gebruikt werd om een perfecte binaire (7,16,3)-code te construeren is een incidentiematrix van de design der punten en rechten van het projectieve vlak $\mathrm{PG}(2, 2)$.

Stelling 8.1.9
Is A een incidentiematrix van de $2-(v, k, \lambda)$ design $\mathcal{D} = (P, B, \mathrm{I})$, is I_v de eenheidsmatrix van de orde v en is J_v de $v \times v$-matrix waarvan alle elementen 1 zijn, dan geldt (over $\mathbb{Q}$) :

$$AA' = (r-\lambda)I_v + \lambda J_v.$$

Bewijs. Stel $P = \{p_1, p_2, \ldots, p_v\}, B = \{L_1, L_2, \ldots, L_b\}, A = [a_{ij}]$ en $AA' = [c_{ij}]$. Dan is $c_{ij} = \sum_{l=1}^{b} a_{il}a_{jl}$ = aantal indices l waarvoor a_{il} en a_{jl} tzt 1 zijn = aantal blokken L_l incident met p_i en p_j. Bijgevolg is $c_{ii} = r$, en $c_{ij} = \lambda$ voor $i \neq j$. Hieruit volgt dat

$$AA' = \begin{bmatrix} r & \lambda & \lambda & \ldots & \lambda \\ \lambda & r & \lambda & \ldots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \ldots & r \end{bmatrix} = (r-\lambda)I_v + \lambda J_v.$$

□

Stelling 8.1.10
Is $\mathcal{D}$ een $2-(v,k,\lambda)$ design met incidentiematrix A, dan geldt

$$det(AA') = (r-\lambda)^{v-1}rk.$$

Bewijs. Wegens Stelling 8.1.9 is

$$AA' = \begin{bmatrix} r & \lambda & \lambda & \ldots & \lambda \\ \lambda & r & \lambda & \ldots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \ldots & r \end{bmatrix}.$$

Wij trekken de eerste kolom van AA' van elke andere kolom af, en daarna tellen wij bij de eerste rij elke andere rij op. Dan bekomen wij de matrix

$$\begin{bmatrix} r+(v-1)\lambda & 0 & 0 & \ldots & 0 \\ \lambda & r-\lambda & 0 & \ldots & 0 \\ \lambda & 0 & r-\lambda & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & 0 & 0 & \ldots & r-\lambda \end{bmatrix}.$$

Bijgevolg is $\det(AA') = (r+(v-1)\lambda)(r-\lambda)^{v-1}$. Uit Stelling 8.1.6 volgt dat $r+\lambda(v-1) = rk$ zodat $\det(AA') = rk(r-\lambda)^{v-1}$. □

Stelling 8.1.11 (De ongelijkheid van Fisher)
Voor elke t-design met $t \geq 2$ geldt de ongelijkheid

$$b \geq v.$$

Bewijs. Beschouw een t-design $\mathcal{D}$ met $t \geq 2$. Dan is $\mathcal{D}$ ook een $2-(v,k,\lambda)$ design. Wegens Stelling 8.1.10 is $\det(AA') = rk(r-\lambda)^{v-1}$, met A een incidentiematrix van $\mathcal{D}$. Dus is $\det(AA') \neq 0$ ($k > 1, r > 0$ omdat $B \neq \emptyset$, uit $r = \lambda$ zou wegens Stelling 8.1.6 volgen dat $v = k$ wat onmogelijk is). Bijgevolg is $\text{rang}(AA') = v$. Aangezien A een $v \times b$-matrix is, is

rang $A \leq b$. Is D een willekeurige $f \times g$-matrix over $\mathbb{C}$ en is C een willekeurige $g \times h$-matrix over $\mathbb{C}$, dan is steeds rang $D \geq$rang(DC). Toepassing van deze bekende ongelijkheid uit de lineaire algebra geeft

$$b \geq \text{ rang } A \geq \text{ rang}(AA') = v.$$

□

8.2 Symmetrische designs

Een $2-(v,k,\lambda)$ design, die geen $(v-1)-(v,v-1,1)$ design is, wordt symmetrisch genoemd als $b = v$. Uit Stelling 8.1.6 volgt dan dat $r = k$ en $\lambda(v-1) = k(k-1)$.

Voorbeelden 8.2.1

(i) Beschouw een symmetrische $2-(v,k,1)$ design $\mathcal{D}$. Dan is $v = k^2 - k + 1$. Stel nu $k = n+1$ zodat $v = n^2+n+1$. Dus is $\mathcal{D}$ een $2-(n^2+n+1, n+1, 1)$ design. Aangezien $\mathcal{D}$ geen $(v-1)-(v,v-1,1)$ design is, is noodzakelijk $n \geq 2$. De symmetrische designs met $\lambda = 1$ zijn dus niets anders dan de eindige projectieve vlakken.

(ii) Beschouw de projectieve ruimte $\text{PG}(m,q), m \geq 2$. Stel

P: verzameling van alle punten van $\text{PG}(m,q)$,

B: verzameling van alle hypervlakken van $\text{PG}(m,q)$,

I: natuurlijke incidentierelatie (een punt p is incident met een hypervlak L a.s.a. $p \subset L$).

Dan is $|P| = |B| = (q^{m+1}-1)/(q-1)$ en het aantal punten incident met een blok is $(q^m-1)/(q-1)$. Het aantal blokken incident met de punten p_1 en $p_2, p_1 \neq p_2$, is gelijk aan het aantal hypervlakken door de rechte p_1p_2, is dus wegens dualiteit gelijk aan het aantal punten van een $\text{PG}(m-2,q)$, is dus gelijk aan $(q^{m-1}-1)/(q-1)$. Het is duidelijk dat (P,B,I) geen $(v-1)-(v,v-1,1)$ design is. Bijgevolg is (P,B,I) een symmetrische

$$2-\left(\frac{q^{m+1}-1}{q-1}, \frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}\right) \text{ design .}$$

Voor $m = 2$ is dit een symmetrische $2-(q^2+q+1, q+1, 1)$ design.

Stelling 8.2.2

Is $\mathcal{D}$ een symmetrische $2-(v,k,\lambda)$ design met incidentiematrix A, dan geldt

$$AA' = A'A = (k-\lambda)I_v + \lambda J_v.$$

Bewijs. Wegens Stelling 8.1.9 is $AA' = (r-\lambda)I_v + \lambda J_v$. Wegens $r = k$ is dus $AA' = (k-\lambda)I_v + \lambda J_v$.

Aangezien door elk punt $r = k$ blokken gaan is $AJ_v = kJ_v$, en aangezien elke blok incident is met k punten is $J_v A = kJ_v$. In het bewijs van Stelling 8.1.11 hebben wij gezien dat $\det(AA') \neq 0$. Hier is $\det(AA') = (\det A)^2$, zodat $\det A \neq 0$. Bijgevolg bestaat A^{-1}. Nu is $A' = A^{-1}AA' = (k-\lambda)A^{-1} + \lambda A^{-1}J_v$. Uit $AJ_v = kJ_v$ volgt dat $k^{-1}J_v = A^{-1}J_v$, zodat $A' = (k-\lambda)A^{-1} + \lambda k^{-1}J_v$. Bijgevolg is $A'A = (k-\lambda)I_v + \lambda k^{-1}J_v A$. Uit $J_v A = kJ_v$ volgt nu dat $A'A = (k-\lambda)I_v + \lambda J_v$. □

Stelling 8.2.3
Is $\mathcal{D} = (P, B, \mathrm{I})$ een symmetrische $2-(v,k,\lambda)$ design, dan hebben elke twee verschillende blokken juist λ punten gemeen. Hieruit volgt dat $\mathcal{D}^* = (B, P, \mathrm{I}^{-1})$ eveneens een symmetrische $2-(v,k,\lambda)$ design is.

Bewijs. Onderstel dat $\mathcal{D} = (P, B, \mathrm{I})$ een symmetrische $2-(v,k,\lambda)$ design is. Stel $P = \{p_1, p_2, \ldots, p_v\}, B = \{L_1, L_2, \ldots, L_v\}$ en noem A de corresponderende incidentiematrix van $\mathcal{D}$. Is $A = [a_{ij}]$ dan volgt uit $A'A = (k-\lambda)I_v + \lambda J_v$ dat voor $i \neq j$ $\lambda = \sum_{l=1}^{v} a_{li}a_{lj}$ = aantal indices l waarvoor a_{li} en a_{lj} tzt 1 zijn = aantal punten p_l incident met L_i en L_j. Voor $i \neq j$ hebben L_i en L_j dus juist λ punten gemeen.

Het is nu onmiddellijk duidelijk dat $\mathcal{D}^* = (B, P, \mathrm{I}^{-1})$ eveneens een $2-(v,k,\lambda)$ design is met evenveel punten als blokken. Ook is het gemakkelijk om aan te tonen dat $\mathcal{D}^*$ een $(v-1)-(v,v-1,1)$ design is a.s.a. $\mathcal{D}$ een $(v-1)-(v,v-1,1)$ design is. Aangezien $\mathcal{D}$ symmetrisch is, en dus geen $(v-1)-(v,v-1,1)$ design is, is $\mathcal{D}^*$ ook geen $(v-1)-(v,v-1,1)$ design. Zo besluiten wij dat $\mathcal{D}^*$ een symmetrische design is met dezelfde parameters als $\mathcal{D}$. □

Stelling 8.2.4 (Schützenberger (1949),Chowla en Ryser (1950))
Is $\mathcal{D}$ een symmetrische $2-(v,k,\lambda)$ design en is v even, dan is $k-\lambda$ het kwadraat van een natuurlijk getal.

Bewijs. Is A een incidentiematrix van $\mathcal{D}$, dan geldt $(\det A)^2 = (k-\lambda)^{v-1}k^2$ (zie Stelling 8.1.10). Bijgevolg is $(k-\lambda)^{v-1}$ het kwadraat van een geheel getal. Uit v even, dus $v-1$ oneven, volgt nu onmiddellijk dat $k-\lambda$ het kwadraat is van een geheel getal. □

Voorbeeld 8.2.5
Onderstel dat een $2-(46,10,2)$ design $\mathcal{D}$ bestaat. Dan is $b = v = 46$ en is $\mathcal{D}$ geen $(v-1)-(v,v-1,1)$ design. Bijgevolg is $\mathcal{D}$ symmetrisch. Aangezien v even is, is $k-\lambda = 8$ het kwadraat van een geheel getal, een strijdigheid. Een $2-(46,10,2)$ design bestaat dus niet.

Stelling 8.2.6 (Chowla en Ryser (1950),Shrikhande (1950))
Is $\mathcal{D}$ een symmetrische $2-(v,k,\lambda)$ design en is v oneven, dan bestaan er steeds drie gehele getallen x, y, z, die niet allen nul zijn, waarvoor

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2 \text{ met } n = k-\lambda.$$

Bewijs. Zonder bewijs. □

Het geval $\lambda = 1$
Beschouw een symmetrische design met $\lambda = 1$, m.a.w. een projectief vlak van de orde n (merk op dat $n = k - 1 = k - \lambda$). Dan is $v = n^2 + n + 1$, zodat v oneven is. Dus bestaan drie gehele getallen x, y, z niet allen nul, waarvoor

$$x^2 = ny^2 + (-1)^{(n^2+n)/2} z^2. \tag{8.1}$$

Is $n \equiv 0$ of $3 \pmod 4$, dan is $n^2 + n \equiv 0 \pmod 4$, zodat $(-1)^{(n^2+n)/2} = 1$. Dan wordt (8.1)

$$x^2 = ny^2 + z^2.$$

Aan (8.1) is dus voldaan voor $x = z = 1, y = 0$. Stelling 8.2.6 levert ons dus niets op.

Onderstel nu dat $n \equiv 1$ of $2 \pmod 4$. Dan is $n^2 + n \equiv 2 \pmod 4$, zodat $(-1)^{(n^2+n)/2} = -1$. Dan wordt (8.1)

$$x^2 + z^2 = ny^2 \text{ of } \left(\frac{x}{y}\right)^2 + \left(\frac{z}{y}\right)^2 = n.$$

Bijgevolg is n de som van de kwadraten van twee rationale getallen. Men kan aantonen dat n dan ook de som is van de kwadraten van twee natuurlijke getallen.

Stelling 8.2.7 (Bruck en Ryser (1949))
Bestaat een projectief vlak van de orde n, waarbij $n \equiv 1$ of $2 \pmod 4$, dan is $n = a^2 + b^2$ met $a, b \in \mathbb{N}$.

Voorbeeld 8.2.8
Er bestaat geen projectief vlak van de orde 6 en 14.

Opmerking 8.2.9
De eer voor Stelling 8.2.6 komt in grote mate toe aan Bruck en Ryser aangezien Stelling 8.2.6 bekomen werd door uitbreiding van het bewijs van Stelling 8.2.7 tot willekeurige λ.

8.3 Afleidingen en uitbreidingen van designs

Het ligt hier in onze bedoeling om vertrekkende van een gegeven design nieuwe designs te construeren.

Stelling 8.3.1
Beschouw een $t - (v, k, \lambda)$ design $\mathcal{D} = (P, B, \mathrm{I})$ met $t \geq 2$ en $k > 2$. Is $p \in P$, $P_p = P - \{p\}, B_p = \{L \in B \parallel p \,\mathrm{I}\, L\}, \mathrm{I}_p = \mathrm{I} \cap (P_p \times B_p)$, dan is $\mathcal{D}_p = (P_p, B_p, \mathrm{I}_p)$ een $(t-1) - (v-1, k-1, \lambda)$ design.

Bewijs. Onmiddellijk. □

Definitie 8.3.2
De design $\mathcal{D}_p$ noemt men de *afgeleide design* van $\mathcal{D}$ met betrekking tot het punt p.

Definitie 8.3.3
De design $\mathcal{D}_1 = (P_1, B_1, \mathrm{I}_1)$ wordt een *uitbreiding* van de design $\mathcal{D} = (P, B, \mathrm{I})$ genoemd als een element $p \in P_1$ kan gevonden worden waarvoor $\mathcal{D} \cong (\mathcal{D}_1)_p$, m.a.w. waarvoor $\mathcal{D}$ isomorf is met de afgeleide design van $\mathcal{D}_1$ met betrekking tot p. Bezit $\mathcal{D}$ een uitbreiding, dan zegt men dat $\mathcal{D}$ *uitbreidbaar* is. Is $\mathcal{D}$ een $t-(v,k,\lambda)$ design, dan is elke uitbreiding een $(t+1)-(v+1,k+1,\lambda)$ design.

Stelling 8.3.4
Is de $t-(v,k,\lambda)$ design $\mathcal{D}$ uitbreidbaar, dan is $k+1$ een deler van $b(v+1)$.

Bewijs. Onderstel dat $\mathcal{D}_1 = (P_1, B_1, \mathrm{I}_1)$ een uitbreiding is van de $t-(v,k,\lambda)$ design $\mathcal{D} = (P, B, \mathrm{I})$. Dan is $|P_1| = v+1$ en is b het aantal blokken van B_1 door een punt van P_1. Als $|B_1| = b_1$, dan geeft toepassing van Stelling 8.1.5 op $\mathcal{D}_1$: $b_1(k+1) = (v+1)b$. Bijgevolg is $k+1$ een deler van $b(v+1)$. □

Stelling 8.3.5
Een projectief vlak van de orde $n \notin \{2, 4, 10\}$ is niet uitbreidbaar.

Bewijs. Onderstel dat het projectief vlak $\mathcal{P}$ van de orde n uitbreidbaar is. Wegens Stelling 8.3.4 is $n+2$ een deler van $(n^2+n+1)(n^2+n+2)$, dus een deler van $((n+2)(n-1)+3)((n+2)(n-1)+4)$, dus een deler van 12. Aangezien $n \geq 2$ is dan noodzakelijk $n \in \{2, 4, 10\}$.□

Uitbreidingen van projectieve vlakken

(a) $\underline{n=2}$. Beschouw de design uit 8.1.2(f) met $m = 3$. Dit is een $3-(8,4,1)$ design $\mathcal{D}$. Is p een punt van $\mathcal{D}$, dan is $\mathcal{D}_p$ een $2-(7,3,1)$ design, m.a.w. het unieke (op een isomorfisme na) projectief vlak van de orde 2. Het projectief vlak van de orde 2 is dus uitbreidbaar. Men kan aantonen dat er op een isomorfisme na slechts één $3-(8,4,1)$ design bestaat, m.a.w. op een isomorfisme na bezit het projectief vlak van de orde 2 slechts één uitbreiding. Is de design $\mathcal{D}$ uitbreidbaar, dan is wegens Stelling 8.3.4 5 een deler van 14.9, een strijdigheid. De design $\mathcal{D}$ is dus niet uitbreidbaar.

(b) $\underline{n=4}$. Beschouw het unieke (op een isomorfisme na) projectief vlak $\mathcal{P}$ van de orde 4. Dit is een $2-(21,5,1)$ design. Men kan aantonen dat $\mathcal{P}$ uitbreidbaar is tot een $3-(22,6,1)$ design W_{22} en dat er op een isomorfisme na slechts één design met zulke parameters bestaat. Men kan aantonen dat W_{22} uitbreidbaar is tot een $4-(23,7,1)$ design W_{23} en dat er op een isomorfisme na slechts één design met zulke parameters bestaat. Men kan aantonen dat W_{23} uitbreidbaar is tot een $5-(24,8,1)$ design W_{24} en dat er op een isomorfisme na slechts één design met zulke parameters bestaat. Uit Stelling 8.3.4 volgt gemakkelijk dat de design W_{24} niet uitbreidbaar is. De designs W_{22}, W_{23}, W_{24} werden in 1938 door Witt ontdekt.

De design W_{22} bezit een automorfismengroep M_{22} die enkelvoudig is en 3-transitief werkt op de puntenverzameling van W_{22} (M_{22} is een normale deelgroep van index 2 in Aut W_{22}). Aut $W_{23} = M_{23}$ is een enkelvoudige groep die 4-transitief werkt op de puntenverzameling van W_{23}. Aut $W_{24} = M_{24}$ is een enkelvoudige groep

die 5-transitief werkt op de puntenverzameling van W_{24}. De enkelvoudige groepen M_{22}, M_{23}, M_{24} werden in 1873 door Mathieu ontdekt.

(c) n=10. Lam, Swiercz en Thiel (1989) bewezen met de computer dat een projectief vlak van de orde 10 niet bestaat.

Hierna geven we de biografieën van Ernst Witt en Emile Léonard Mathieu.

Figuur 8.3: Ernst Witt

Ernst Witt werd op 26 juni 1911 op het baltisch eiland Alsen geboren. Dit eiland was in 1864, net als de rest van Noord-Schleeswijk, een deel van Duitsland geworden. Het eiland werd na een referendum in 1920 teruggegeven aan Denemarken, negen jaar na de geboorte van Witt, en is nu gekend onder de naam Als. *Het eiland wordt gescheiden van het Sundeved schiereiland van Zuid-Jutland door een nauw stuk water, gekend onder de naam* Als zee-engte.

Kort na zijn geboorte verhuisde Witt naar China waar hij opgroeide. Hij keerde terug naar Europa toen hij negen jaar oud was.

Witt studeerde aan de universiteiten van Freiburg en Göttingen. Hij behaalde zijn doctoraat aan de universiteit van Göttingen onder de leiding van Emmy Noether. Zij had hem een onderwerp voorgesteld dat in verband stond met de Riemann-Roch stelling, en hij heeft effectief zijn doctoraat over dit onderwerp geschreven.

In Göttingen nam Witt deel aan Helmut Hasse's seminaries over congruentie functievelden en p-adische getallen. Oswald Teichmüller en Ludwig Schmid namen ook deel aan die seminaries, en Schmid werkte met Witt samen op resultaten die geleid hebben tot de Witt vector calculus.

Emil Artin was niet joods, maar zijn vrouw was joods. Toen nazi wetten uit 1937 gevolgen hadden voor mensen die gehuwd waren met iemand van joodse afkomst, werd Artin uit zijn leerstoel aan de universiteit van Hamburg gezet, en verliet Artin Duitsland voor de Verenigde Staten. Witt volgde Artin in Hamburg op, en bleef daar tot zijn pensioen in 1979.

Witt's werk ging vooral over kwadratische vormen en vele verwante gebieden, zoals algebraische functievelden, Witt vectoren, Lie ringen en Mathieu groepen. Hij is vooral gekend voor het invoeren van Witt vectoren in een artikel uit J. Reine Angew. Math. *uit 1936.*

Hij stierf op 3 juli 1991.

(http://turnbull.mcs.st-and.ac.uk/∼history/Mathematicians/Witt.html)

Emile Léonard Mathieu wordt vooral herinnerd voor zijn ontdekking in 1860 en 1873 van vijf sporadische enkelvoudige groepen, die naar hem genoemd zijn. Deze groepen werden bestudeerd in zijn thesis over transitieve functies.

Mathieu werd op 15 mei 1835 in Metz, Frankrijk, geboren. Hij groeide in Metz op, en ging naar school in deze stad. Hij blonk uit op school, eerst in klassieke studies waar hij opmerkelijke talenten in grieks en latijn vertoonde. Nadat hij echter in zijn tienerjaren met wiskunde in contact kwam, werd dit het enige onderwerp waarin hij verder wilde werken. Na zijn intrede in de Ecole Polytechnique in Parijs was zijn vooruitgang in wiskundige kennis bijna onvoorstelbaar. Mathieu had maar 18 maanden nodig om de volledige opleiding te voltooien, en hij studeerde daar verder om een doctoraat voor te bereiden. Tegen 1859 was hij Doctor in de Wetenschappen na het verdedigen van een doctoraatsthesis over transitieve functies; thesis die leidde tot zijn ontdekking van sporadische enkelvoudige groepen.

Zijn bijna onvoorstelbare vooruitgang in wiskundige kennis zou normaal gezien hem in de ideale positie geplaatst hebben om een universitaire benoeming te bekomen, maar dit was niet zo. Hij aanvaardde werk als privé leraar wiskunde en hij deed dit werk gedurende 10 jaar. Hij leed in 1866 aan een eerder zware ziekte, en dit zou hem datzelfde jaar doen afzien hebben van het overnemen van Lamé's opleidingsonderdelen aan de Sorbonne. Hij werd in 1869 tot professor wiskunde benoemd in Besançon, en vijf jaar later, verhuisde Mathieu naar Nancy om de leerstoel wiskunde daar op te nemen.

Mathieu was na zijn oorspronkelijk werk in zuivere wiskunde vooral werkzaam in wiskundige natuurkunde, hoewel hij ook belangrijk werk over hypergeometrische functies deed. Zo schrijft Grattan-Guinness:

Hoewel Mathieu veelbelovend was in zijn eerste jaren als onderzoeker, kreeg hij nooit de normale tekenen van erkentelijkheid zoals een parijse leerstoel of verkiezing tot lid van de Académie des Sciences. Vanaf zijn eind-twintiger jaren waren zijn inspanningen gewijd aan de, in die tijd weinig populaire, verderzetting van de grote franse traditie in wiskundige natuurkunde, en hij breidde grondig het opstellen en het oplossen van partiële differentiaalvergelijkingen voor een grote reeks fysische problemen uit.

Misschien, moest Mathieu zijn opmerkelijke ontdekkingen in groepentheorie verder gezet hebben, was hij beroemder geweest en had hij betere leerstoelen gehad.

Een gedeelte van zijn vroegste werk in wiskundige natuurkunde stond in verband met zijn studie van het licht, en hij bestudeerde de vibratie oppervlakken komende van Fresnel golven. Hij werkte ook op de polarisatie van licht, en vestigde de aandacht op enkele zwakheden in Cauchy's resultaten over dit onderwerp.

Hij werkte ook op potentiaaltheorie, toegepast op elasticiteit, en warmte verspreiding. Mathieu bestudeerde vloeistoffen, in het bijzonder capillaire krachten. Hij bestudeerde ook magnetische inductie, en het drie lichamen probleem, dat hij toepaste in zijn onderzoek op de perturbatie van de banen van Jupiter en Saturnus.

Mathieu wordt naast zijn onderzoek over de Mathieu groepen ook herinnerd voor de Mathieu functies. Hij ontdekte deze functies, die bijzondere hypergeometrische functies zijn, toen hij de golfvergelijking oploste van een elliptisch membraan bewegend door een vloeistof.

Grattan-Guinness beschrijft Mathieu als:

... schuchter en teruggetrokken wat misschien in zekere mate het gebrek aan succes in zijn leven en carriere tot gevolg gehad heeft; maar onder collega's kreeg hij altijd vriendschap en respect.

Hij stierf op 19 oktober 1890 in Nancy, Frankrijk.

(http://turnbull.mcs.st-and.ac.uk/∼history/Mathematicians/Mathieu_Emile.html)

Uitbreidingen van affiene vlakken

Beschouw een affien vlak $\mathcal{A}$ van de orde n, dit is een $2-(n^2,n,1)$ design. De nodige voorwaarde 8.3.4 voor uitbreidbaarheid zegt dat $n+1$ een deler moet zijn van $(n^2+n)(n^2+1)$, hetgeen geen beperking oplegt. Een uitbreiding van $\mathcal{A}$ is een $3-(n^2+1,n+1,1)$ design.Een $3-(n^2+1,n+1,1)$ design noemt men een *inversief vlak van de orde* n. De blokken van een inversief vlak noemt men gewoonlijk *cirkels*.

Een *ovoïde* O van $\mathrm{PG}(3,q), q>2$, is een verzameling van q^2+1 punten van $\mathrm{PG}(3,q)$ waarvan geen drie collineair zijn; een ovoïde O van $\mathrm{PG}(3,2)$ is bij definitie een elliptische kwadriek, dit is een niet-singuliere kwadriek van $\mathrm{PG}(3,2)$ waarop geen rechten gelegen zijn. Elk vlak π van $\mathrm{PG}(3,q)$ bezit 1 of $q+1$ punten van de ovoïde O. Bezit π juist 1 punt x van O, dan zegt men dat π de ovoïde O *raakt* in x; door elk punt $x\in O$ gaat juist één raakvlak van O.
Is O een ovoïde van $\mathrm{PG}(3,q)$, dan stellen wij :

$P=O$;

B : verzameling van de doorsneden van O met de vlakken die O niet raken;

$\mathrm{I}:\in$.

Dan is $\mathcal{I}=(P,B,\mathrm{I})$ een $3-(q^2+1,q+1,1)$ design, dus een inversief vlak van de orde q. Dergelijk inversief vlak noemen wij een *eivormig* inversief vlak.

Elke elliptische kwadriek O van $\mathrm{PG}(3,q)$ is een ovoïde. Is O een elliptische kwadriek dan noemt men het corresponderend inversief vlak *klassiek* of *miqueliaans*.

Is $\mathcal{I}=(P,B,\mathrm{I})$ een eivormig inversief vlak en is x een willekeurig punt van P, dan is de afgeleide design $\mathcal{I}_x$ isomorf met de design gevormd door de punten en rechten van $\mathrm{AG}(2,q)$. De design der punten en rechten van $\mathrm{AG}(2,q)$ is dus steeds uitbreidbaar.

Er bestaat juist één inversief vlak van de orde $n\in\{2,3,4,5,7,16\}$ en juist 2 inversieve vlakken van de orde $n\in\{8,32\}$ (op een isomorfisme na).

Barlotti (1955) en Panella (1955) bewezen dat elke ovoïde van $\mathrm{PG}(3,q)$, met q oneven, een elliptische kwadriek is, m.a.w. dat elk eivormig inversief vlak van oneven orde miqueliaans is. Buiten de miqueliaanse inversieve vlakken zijn geen andere inversieve vlakken van oneven orde gekend. Dembowski (1963) bewees dat elk inversief vlak van even orde n eivormig is, zodat $n = 2^h$. Tits (1962) bewees dat er voor elke $n = 2^{2h+1}, h \geq 1$, een inversief vlak van de orde n bestaat dat niet miqueliaans is. Buiten de miqueliaanse inversieve vlakken en de inversieve vlakken van Tits, zijn geen andere inversieve vlakken van even orde gekend.

Thas (1994) bewees dat voor q oneven het miqueliaans inversief vlak de enige (op een isomorfisme na) uitbreiding is van de design der punten en rechten van $\mathrm{AG}(2,q)$. Hieruit volgt gemakkelijk dat er juist één inversief vlak is van de orde $n \in \{3,5,7\}$, hetgeen het eerste computer-vrij bewijs levert van de uniciteit van het inversief vlak van de orde 7.

Is het inversief vlak $\mathcal{I}$ van de orde n uitbreidbaar dan volgt uit Stelling 8.3.4 dat $n \in \{2,3,4,8,10,13,18,28,58\}$. Is n even dan weten wij dat $n = 2^h$, zodat noodzakelijk $n \in \{2,3,4,8,13\}$. Kantor (1974) bewees verder dat $n \in \{2,3,13\}$.

(a) $\underline{n = 2}$. De complete $3-(5,3,1)$ design is uitbreidbaar tot de complete $4-(6,4,1)$ design, die uitbreidbaar is tot de complete $5-(7,5,1)$ design, die uitbreidbaar is tot de complete $6-(8,6,1)$ design, ...

(b) $\underline{n = 3}$. Beschouw het unieke (op een isomorfisme na) inversief vlak $\mathcal{I}$ van de orde 3. Dit is een $3-(10,4,1)$ design. Men kan aantonen dat $\mathcal{I}$ uitbreidbaar is tot een $4-(11,5,1)$ design W_{11} en dat er op een isomorfisme na slechts één design met zulke parameters bestaat. Men kan aantonen dat W_{11} uitbreidbaar is tot een $5-(12,6,1)$ design W_{12} en dat er op een isomorfisme na slechts één design met zulke parameters bestaat. Uit Stelling 8.3.4 volgt gemakkelijk dat de design W_{12} niet uitbreidbaar is. De designs W_{11} en W_{12} werden door Witt in 1938 ontdekt.

Aut $W_{11} = M_{11}$ is een enkelvoudige groep die 4-transitief werkt op de puntenverzameling van W_{11}. Aut $W_{12} = M_{12}$ is een enkelvoudige groep die 5-transitief werkt op de puntenverzameling van W_{12}. De enkelvoudige groepen M_{11} en M_{12} werden in 1861 door Mathieu ontdekt.

(c) $\underline{n = 13}$. Een uitbreiding van een inversief vlak van de orde 13 werd nog niet gevonden en bestaat waarschijnlijk niet.

Hoofdstuk 9

Perfecte codes

9.1 Perfecte codes

Wordt voor een code C de bolpakkingsgrens bereikt, dan noemt men C een perfecte code. Is $|C| = 1$, dan noemt men C bij definitie perfect. De triviale perfecte codes zijn de singletons,de gehele verzameling $(F_q)^n$ (hier is $t = 0$), en de binaire herhalingscodes met oneven lengte n.

Hamming codes zijn perfect (zie Hoofdstuk 7). $\mathrm{Ham}(r, q), r \geq 2$ en q een priemmacht, is een perfecte

$$\left[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3\right] \text{-code}$$

over GF(q). Uit de constructie van $\mathrm{Ham}(r, q)$ volgt dat elke lineaire code met de parameters van $\mathrm{Ham}(r, q)$ noodzakelijk $\mathrm{Ham}(r, q)$ is.

9.2 De ternaire Golay code

Onderstel dat het alfabet GF(3) is. Noem S_5 de circulant met eerste rij
$\begin{bmatrix} 0 & 1 & -1 & -1 & 1 \end{bmatrix}$, d.w.z.

$$S_5 = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{bmatrix}.$$

Merk op dat S_5 symmetrisch is. De *ternaire Golay code* G_{11} is dan de $[11,6]$-code over GF(3) voortgebracht door de matrix

$$G = \left[\begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \\ 0 & & & & I_5 & & & & S_5 & & \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \end{array}\right].$$

Een pariteit controlematrix van G_{11} is dan de matrix

$$H = \left[\begin{array}{cccccc|c} -1 & 0 & -1 & 1 & 1 & -1 & \\ -1 & -1 & 0 & -1 & 1 & 1 & \\ -1 & 1 & -1 & 0 & -1 & 1 & I_5 \\ -1 & 1 & 1 & -1 & 0 & -1 & \\ -1 & -1 & 1 & 1 & -1 & 0 & \end{array}\right].$$

Stelling 9.2.1
De ternaire Golay code G_{11} is een perfecte 2-foutverbeterende lineaire $[11,6]$-code.

Bewijs. Er geldt :

$$GG' = \left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & -J_5 & & \\ 0 & & & & & \\ 0 & & & & & \end{array}\right].$$

Is $\bar{u} = u_1 u_2 \dots u_6$, dan is $\bar{u}G$ een codewoord van G_{11}. Nu is

$$\begin{aligned} ([u_1\ u_2\ \dots\ u_6]G)([u_1\ u_2\ \dots\ u_6]G)' &= [u_1\ u_2\ \dots\ u_6]GG'[u_1\ u_2\ \dots\ u_6]' \\ &= \left[-\left(\sum_{i=2}^{6} u_i\right)^2\right]. \end{aligned}$$

Bijgevolg is $(\bar{u}G).(\bar{u}G) \neq 1$, waaruit volgt dat $w(\bar{u}G) \not\equiv 1 \pmod 3$. Is $\bar{x} \in G_{11}$ dan is dus $w(\bar{x}) \notin \{1,4,7,10\}$.

De rijen $\bar{r}_1, \bar{r}_2, \dots, \bar{r}_6$ van G hebben gewicht 5 of 6. Beschouw nu een codewoord $\bar{x}$ van de gedaante $a\bar{r}_i + b\bar{r}_j$, met $ab \neq 0$ en $i \neq j$. De $i$de en $j$de coördinaat van $\bar{x}$ zijn verschillend van nul. Is $i > 1$ en $j > 1$, dan zijn eveneens de $(i+5)$de en $(j+5)$de coördinaat verschillend van nul, zodat $w(\bar{x}) \geq 4$ en dus $w(\bar{x}) \geq 5$. Is bijvoorbeeld $i = 1$ en $j = 2$, dan is de zevende coördinaat van $\bar{x}$ niet nul, en is bovendien

$$\text{rang} \left[\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{array}\right] = 2,$$

zodat opnieuw $w(\bar{x}) \geq 4$ en dus $w(\bar{x}) \geq 5$. De andere gevallen zijn analoog.

Beschouw nu een codewoord $\bar{x}$ van de gedaante $a\bar{r}_i + b\bar{r}_j + c\bar{r}_l$, met $abc \neq 0$ en i, j, l verschillend. De $i$de, $j$de, $l$de coördinaat van $\bar{x}$ zijn dan verschillend van nul. Aangezien verder elke 3 rijen van de matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ & & S_5 & & \end{bmatrix}$$

lineair onafhankelijk zijn, is $w(\bar{x}) \geq 4$ en dus ook $w(\bar{x}) \geq 5$.

Beschouw tenslotte een codewoord $\bar{x}$ van de gedaante $a_{i_1}\bar{r}_{i_1} + a_{i_2}\bar{r}_{i_2} + \ldots + a_{i_s}\bar{r}_{i_s}$, met $s \geq 4$, $a_{i_1}a_{i_2}\ldots a_{i_s} \neq 0$ en $i_1, i_2, \ldots, i_s$ allen verschillend. Dan zijn de $i_1$de, $i_2$de, $\ldots$, $i_s$de coördinaat van $\bar{x}$ verschillend van nul, zodat $w(\bar{x}) \geq s \geq 4$, en dus ook $w(\bar{x}) \geq 5$.

Uit dit alles volgt dat $w(G_{11}) = 5$, zodat ook $d(G_{11}) = 5$. Bijgevolg is G_{11} 2-foutverbeterend.

Nu is $|G_{11}| = 3^6$ en $3^6(1 + 2\binom{11}{1} + 4\binom{11}{2}) = 3^{11} = |V(11,3)|$.
Voor de code G_{11} wordt dus de bolpakkingsgrens bereikt, zodat G_{11} perfect is. □

Gewichtspolynoom van G_{11}. Men toont aan dat voor G_{11}

$$A(X,Y) = Y^{11} + 132X^5Y^6 + 132X^6Y^5 + 330X^8Y^3 + 110X^9Y^2 + 24X^{11}.$$

9.3 De uitgebreide ternaire Golay code

Beschouw een willekeurige lineaire $[n,k]$-code C over GF(q). Wij definiëren nu als volgt de *uitgebreide code* $\hat{C}$ van C : is $\bar{x} = x_1x_2\ldots x_n \in C$, dan is $\hat{\bar{x}} = x_1x_2\ldots x_nx_{n+1}$ met $\sum_{i=1}^{n+1} x_i = 0$ een codewoord van $\hat{C}$. Men toont gemakkelijk aan dat $\hat{C}$ een lineaire $[n+1,k]$-code over GF(q) is.

Beschouw nu de uitgebreide code $G_{12} = \hat{G}_{11}$ van de ternaire Golay code. Dan is G_{12} een lineaire $[12,6]$-code over GF(3). Een voortbrengende matrix van G_{12} is dan

$$\hat{G} = \begin{bmatrix} & & 0 \\ & & -1 \\ & G & -1 \\ & & -1 \\ & & -1 \\ & & -1 \end{bmatrix}.$$

Stelling 9.3.1
De code G_{12} is een zelfduale code over GF(3)*, met gewichtspolynoom*

$$\hat{A}(X,Y) = Y^{12} + 264X^6Y^6 + 440X^9Y^3 + 24X^{12}.$$

Bewijs. Er geldt

$$\hat{G}\hat{G}' = \begin{bmatrix} & & 0 \\ & & -1 \\ & G & -1 \\ & & -1 \\ & & -1 \\ & & -1 \end{bmatrix} \begin{bmatrix} & & G' & & & \\ 0 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

$$= GG' + \begin{bmatrix} 0 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \begin{bmatrix} 0 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

$$= GG' + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & J_5 & & \\ 0 & & & & & \\ 0 & & & & & \end{bmatrix} = 0 \text{ (zie begin bewijs van Stelling 9.2.1).}$$

Bijgevolg is $\hat{H} = \hat{G}$, zodat $G_{12}^{\perp} = G_{12}$; m.a.w. G_{12} is zelfduaal.

Onderstel dat $\bar{x} \in G_{11}$ en $w(\bar{x}) = 5$. Dan is $w(\hat{\bar{x}}) = 5$ of 6. Uit $\hat{\bar{x}}.\hat{\bar{x}} = 0$ volgt dat $w(\hat{\bar{x}}) = 6$. Onderstel vervolgens dat $\bar{x} \in G_{11}$ en $w(\bar{x}) = 6$. Dan is $w(\hat{\bar{x}}) = 6$ of 7. Uit $\hat{\bar{x}}.\hat{\bar{x}} = 0$ volgt dat $w(\hat{\bar{x}}) = 6$.

Analoog volgt uit $\bar{x} \in G_{11}$ met $w(\bar{x}) = 8$, dat $w(\hat{\bar{x}}) = 9$; uit $\bar{x} \in G_{11}$ met $w(\bar{x}) = 9$, volgt dat $w(\hat{\bar{x}}) = 9$. Ten slotte volgt uit $w(\bar{x}) = 11, \bar{x} \in G_{11}$, dat $w(\hat{\bar{x}}) = 12$.

Bijgevolg heeft G_{12} gewichtspolynoom $\hat{A}(X, Y)$, met

$$\hat{A}(X, Y) = Y^{12} + 264X^6Y^6 + 440X^9Y^3 + 24X^{12}.$$

□

Definitie 9.3.2
Beschouw een willekeurige lineaire code C met lengte n, en stel

$$P = \{1, 2, 3, \ldots, n\}.$$

Is $\bar{x} = x_1x_2 \ldots x_n \in C$ en zijn $x_{i_1}, x_{i_2}, \ldots, x_{i_s}$ de coördinaten van $\bar{x}$ die niet nul zijn, dan zeggen wij dat de verzameling $\{i_1, i_2, \ldots, i_s\} \subseteq P$ de *ondersteuning (support)* is van $\bar{x}$. Merk op dat het aantal elementen van de ondersteuning van $\bar{x}$ gelijk is aan $w(\bar{x})$.

Stelling 9.3.3
Is $P = \{1, 2, \ldots, 12\}$ en is B de verzameling van de ondersteuningen van de codewoorden van gewicht 6 van G_{12}, dan is $(P, B, \in)$ een $5 - (12, 6, 1)$ design, m.a.w. de Witt design W_{12}.

Bewijs. Beschouw codewoorden $\bar{x}, \bar{y} \in G_{12}$, met $w(\bar{x}) = w(\bar{y}) = 6$. Is $\bar{y} = \pm\bar{x}$, dan is vanzelfsprekend de ondersteuning van $\bar{x}$ ook de ondersteuning van $\bar{y}$. Noem l het aantal posities waarin $\bar{x}$ en $\bar{y}$ beiden verschillend van nul zijn, noem l_1 (resp. l_2) het aantal posities waarin $\bar{x}$ (resp. $\bar{y}$) de coördinaat 1 en $\bar{y}$ (resp. $\bar{x}$) de coördinaat –1 heeft, en noem l_3 (resp. l_4) het aantal posities waarin $\bar{x}$ en $\bar{y}$ beiden de coördinaat 1 (resp. –1) hebben. Dan is $l_1 + l_2 + l_3 + l_4 = l, w(\bar{x} + \bar{y}) = 12 - 2l + l_3 + l_4, w(\bar{x} - \bar{y}) = 12 - 2l + l_1 + l_2$. Bijgevolg is $w(\bar{x} + \bar{y}) \leq 12 - 2l + \frac{l}{2}$ of $w(\bar{x} - \bar{y}) \leq 12 - 2l + \frac{l}{2}$.

Onderstel nu dat $\bar{y} \neq \pm\bar{x}$. Dan is $w(\bar{x} + \bar{y}) \geq 6$ en $w(\bar{x} - \bar{y}) \geq 6$, zodat $6 \leq 12 - 2l + \frac{l}{2}$ en dus $l \leq 4$. Hieruit volgt dat ondersteuningen van codewoorden $\bar{x}, \bar{y} \in G_{12}$ van gewicht 6 samenvallen a.s.a. $\bar{y} = \pm\bar{x}$. Bijgevolg is $|B| = 132$.

Het aantal verschillende deelverzamelingen van de orde 5 bevat in elementen van B is gelijk aan $132 \times 6 = 792$ (hierbij houden wij rekening met $l \leq 4$). Het totaal aantal deelverzamelingen van de orde 5 van P is $\binom{12}{5} = 792$. Elke deelverzameling van de orde 5 van P is dus bevat in een element van B, en bovendien in juist één (opnieuw wegens $l \leq 4$) element van B.

Bijgevolg is $(P, B, \in)$ een $5 - (12, 6, 1)$ design, m.a.w. de Witt design W_{12} ingevoerd in 8.3. □

9.4 De binaire Golay code

De *binaire Golay code* G_{23} wordt voortgebracht door de 12×23-matrix G over GF(2) met als $i$de rij, $i = 1, 2, \ldots, 12$,

$$[0_{1\times(i-1)} \quad \bar{g} \quad 0_{1\times(12-i)}]$$

met $0_{i\times j}$ de nulmatrix van het type $i \times j$ en $\bar{g} = [1\,1\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1]$. Men toont aan dat deze $[23, 12]$-code over GF(2) 3-foutverbeterend en perfect is.

Beschouw vervolgens de uitbreiding $\hat{G}_{23} = G_{24}$. Deze code is een lineaire $[24, 12]$-code over GF(2). De code G_{24} is zelfduaal en $0, 8, 12, 16, 24$ zijn de enige gewichten die in G_{24} voorkomen.

Stelling 9.4.1
Is $P = \{1, 2, \ldots, 24\}$ en is B de verzameling van de ondersteuningen van de codewoorden van gewicht 8 van G_{24}, dan is $(P, B, \in)$ een $5 - (24, 8, 1)$ design, m.a.w. de Witt design W_{24}.

9.5 Fundamentele stellingen

De Golay codes werden in 1949 door Golay ingevoerd.

Stelling 9.5.1 (van Lint-Tietäväinen ('73-'75), Zinoviev-Leontiev ('73))
Iedere niet-triviale perfecte code over F_q, met q een priemmacht, heeft de parameters van een Hamming of een Golay code.

Bewijs. Zonder bewijs. □

In 1975 bewezen Delsarte en Goethals dat elke code met de parameters van een Golay code, gelijkwaardig met een Golay code is (gedeelten van dit resultaat werden reeds bewezen door Pless (1968) en Snover (1973)). Bijgevolg hebben wij volgende stelling.

Stelling 9.5.2
Iedere niet-triviale perfecte code over F_q, met q een priemmacht, heeft de parameters van een Hamming code of is gelijkwaardig met een Golay code.

Uit 9.1 volgt dan

Stelling 9.5.3
Iedere niet-triviale lineaire perfecte code is gelijkwaardig met een Hamming code of een Golay code.

Verder merken wij op dat er perfecte niet-lineaire codes met de parameters van Hamming codes bestaan, die niet gelijkwaardig zijn met Hamming codes (dergelijke codes werden bijvoorbeeld door Schönheim (1968) en Lindström (1969) geconstrueerd). Tenslotte is het een open vraagstuk of er al dan niet niet-triviale perfecte codes over F_q, met q geen priemmacht, bestaan.

Hoofdstuk 10

Codes en latijnse vierkanten

10.1 Latijnse vierkanten

Een *latijns vierkant* (*Latin square*) over de verzameling F_q, met $|F_q| = q$, is een $q \times q$-rooster A, waarbij in elke rij en elke kolom elk element van F_q juist eenmaal optreedt. In zulk geval zegt men dat het latijns vierkant A de *orde* q heeft.

Voorbeelden 10.1.1

(i) Stel $F_q = \{a, b, c\}$. Dan is

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

een latijns vierkant van de orde 3.

(ii) De geneesmiddelen 1,2,3 tegen hoofdpijn worden getest op patiënten P_1, P_2, P_3 op drie opeenvolgende dagen M, D, W. Hierbij willen wij een idee hebben over de invloed van de dagen op het effect van de geneesmiddelen. Hiertoe zullen wij er voor zorgen dat elk geneesmiddel op elk van de dagen M, D, W ingenomen wordt, m.a.w. het testschema wordt gegeven door een latijns vierkant, bijvoorbeeld

	M	D	W
P_1	1	2	3
P_2	2	3	1
P_3	3	1	2

.

Stelling 10.1.2

Voor elke $q \in \mathbb{N}_0$ bestaat een latijns vierkant van de orde q.

Bewijs. Stel $F_q = \{1, 2, \cdots, q\}$ en stel

$$A = \begin{bmatrix} 1 & 2 & 3 & \dots & q-2 & q-1 & q \\ 2 & 3 & 4 & \dots & q-1 & q & 1 \\ 3 & 4 & 5 & \dots & q & 1 & 2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ q & 1 & 2 & \dots & q-3 & q-2 & q-1 \end{bmatrix}.$$

□

10.2 Onderling orthogonale latijnse vierkanten

Beschouw $t, t \geq 2$, latijnse vierkanten $A_k = [a_{ij}^{(k)}], k = 1, 2, \cdots, t$, van de orde q over F_q. Men zegt dat $A_1, A_2, \cdots, A_t$ *onderling orthogonale latijnse vierkanten* (*mutually orthogonal Latin squares*), afgekort *MOLS*, zijn als voor elke $k \neq l$ alle koppels $(a_{ij}^{(k)}, a_{ij}^{(l)})$, met $i, j = 1, 2, \cdots, q$, verschillend zijn, met andere woorden als $\{(a_{ij}^{(k)}, a_{ij}^{(l)}) \parallel i, j = 1, 2, \cdots, q\} = F_q \times F_q$.

Voorbeelden 10.2.1

(i) $F_1 = \{0\}$

$[0], [0], [0], \cdots$ zijn MOLS van de orde 1.

(ii) $F_2 = \{0, 1\}$

Er bestaan geen 2 MOLS over F_2.

(iii) $F_3 = \{1, 2, 3\}$

$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$ en $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$ zijn MOLS van de orde 3.

(iv) De geneesmiddelen 1,2,3 tegen hoofdpijn en de geneesmiddelen 1,2,3 tegen koorts worden getest op patiënten P_1, P_2, P_3 op drie opeenvolgende dagen M, D, W. Zoals in Voorbeeld 10.1.1 (ii) zullen wij wat het testschema betreft voor het geneesmiddel tegen hoofdpijn gebruik maken van een latijns vierkant van de orde 3, en zullen wij wat het testschema betreft voor het geneesmiddel tegen koorts eveneens gebruik maken van een latijns vierkant van de orde 3. Aangezien elke patiënt elke dag een geneesmiddel tegen hoofdpijn en een geneesmiddel tegen koorts gebruikt, kunnen wij hun gecombineerd effect onderzoeken. Is het mogelijk om elk van de 9 mogelijkheden voor (geneesmiddel hoofdpijn, geneesmiddel koorts) juist eenmaal uit te proberen? Ja, door elk element uit het eerste latijns vierkant uit Voorbeeld (iii) te vervangen door het corresponderend koppel overeenkomstige elementen uit het eerste en het tweede vierkant:

	M	D	W
P_1	$(1,1)$	$(2,2)$	$(3,3)$
P_2	$(2,3)$	$(3,1)$	$(1,2)$.
P_3	$(3,2)$	$(1,3)$	$(2,1)$

Stelling 10.2.2
Is q een priemmacht, dan bestaan $q-1$ MOLS van de orde q.

Bewijs. Onderstel dat $\mathrm{GF}(q) = \{\lambda_0, \lambda_1, \cdots, \lambda_{q-1}\}$, met $\lambda_0 = 0$. Is $\mu \in \mathrm{GF}(q) - \{0\}$, dan stellen wij

$$A_\mu = [a_{ij}^{(\mu)}], \text{ met } a_{ij}^{(\mu)} = \lambda_j + \mu\lambda_i \text{ en } i, j = 0, 1, \cdots, q-1.$$

Eerst en vooral tonen wij aan dat A_μ latijns is, met $\mu = \lambda_1, \lambda_2, \cdots, \lambda_{q-1}$.
Als twee elementen uit kolom j van A_μ gelijk zijn, dan is

$$\lambda_j + \mu\lambda_i = \lambda_j + \mu\lambda_{i'}, \text{ met } i \neq i'.$$

Dus is $\mu(\lambda_i - \lambda_{i'}) = 0$, een strijdigheid aangezien $\mu \neq 0$ en $\lambda_i \neq \lambda_{i'}$. Als twee elementen uit rij i van A_μ gelijk zijn, dan is

$$\lambda_j + \mu\lambda_i = \lambda_{j'} + \mu\lambda_i, \text{ met } j \neq j'.$$

Dus is $\lambda_j = \lambda_{j'}$, een strijdigheid. Bijgevolg is A_μ latijns, $\mu = \lambda_1, \lambda_2, \cdots, \lambda_{q-1}$.

Vervolgens tonen wij aan dat A_μ en $A_{\mu'}$, $\mu \neq 0 \neq \mu'$ en $\mu \neq \mu'$, onderling orthogonaal zijn. Onderstel dat

$$(a_{ij}^{(\mu)}, a_{ij}^{(\mu')}) = (a_{i'j'}^{(\mu)}, a_{i'j'}^{(\mu')}).$$

Dan is

$$\begin{aligned} \lambda_j + \mu\lambda_i &= \lambda_{j'} + \mu\lambda_{i'}, \\ \lambda_j + \mu'\lambda_i &= \lambda_{j'} + \mu'\lambda_{i'}. \end{aligned}$$

Door aftrekken van de overeenkomstige leden bekomen wij

$$(\mu - \mu')\lambda_i = (\mu - \mu')\lambda_{i'}.$$

Uit $\mu \neq \mu'$ volgt dan dat $\lambda_i = \lambda_{i'}$, zodat $i = i'$. Uit $\lambda_j + \mu\lambda_i = \lambda_{j'} + \mu\lambda_i$ volgt nu dat $\lambda_j = \lambda_{j'}$, m.a.w. $j = j'$. Zo besluiten wij dat $A_{\lambda_1}, A_{\lambda_2}, \cdots, A_{\lambda_{q-1}}$ $q-1$ MOLS van de orde q zijn . □

Voorbeeld 10.2.3
Beschouw $\mathrm{GF}(5) = \{0, 1, 2, 3, 4\}$. Dan zijn

$$A_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix} \quad A_4 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

4 MOLS van de orde 5.

Opmerkingen 10.2.4
Is A een latijns vierkant en verkrijgen wij B uit A door een permutatie van rijen en kolommen, dan is B ook een latijns vierkant. Zijn de latijnse vierkanten A_1 en A_2 onderling orthogonaal en verkrijgen wij B_1 uit A_1 en B_2 uit A_2 door een zelfde permutatie van rijen en kolommen, dan zijn ook B_1 en B_2 orthogonaal. Is $A = [a_{ij}]$ een latijns vierkant over F_q en is σ een permutatie van F_q, dan is ook $A^\sigma = [a_{ij}^\sigma]$ een latijns vierkant over F_q.

Stelling 10.2.5
Onderstel dat $A = [a_{ij}]$ en $B = [b_{ij}]$ onderling orthogonale latijnse vierkanten over F_q zijn. Zijn σ_1 en σ_2 permutaties van F_q, dan zijn ook $A^{\sigma_1} = [a_{ij}^{\sigma_1}]$ en $B^{\sigma_2} = [b_{ij}^{\sigma_2}]$ onderling orthogonale latijnse vierkanten over F_q.

Bewijs. Onderstel dat

$$(a_{ij}^{\sigma_1}, b_{ij}^{\sigma_2}) = (a_{i'j'}^{\sigma_1}, b_{i'j'}^{\sigma_2}).$$

Dan is

$$a_{ij}^{\sigma_1} = a_{i'j'}^{\sigma_1}, b_{ij}^{\sigma_2} = b_{i'j'}^{\sigma_2}.$$

Bijgevolg is

$$a_{ij} = a_{i'j'}, b_{ij} = b_{i'j'},$$

zodat

$$(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'}).$$

Aangezien A en B onderling orthogonaal zijn volgt hieruit dat $i = i'$ en $j = j'$. Zo besluiten wij dat ook A^{σ_1} en B^{σ_2} onderling orthogonaal zijn. □

Definitie 10.2.6
Beschouw t MOLS $A_1, A_2, \cdots, A_t$ van de orde q over F_q. Onderstel dat B_i uit A_i ontstaat als gevolg van een permutatie σ_i van F_q, $i = 1, 2, \cdots, t$, en dat C_1 uit B_1, C_2 uit $B_2, \cdots, C_t$ uit B_t ontstaan als gevolg van een zelfde permutatie van rijen en kolommen. Dan zijn ook $C_1, C_2, \cdots, C_t$ MOLS over F_q. Men zegt dat de geordende t-tallen MOLS $(A_1, A_2, \cdots, A_t)$ en $(C_1, C_2, \cdots, C_t)$ *equivalent* zijn. Is $F_q = \{0, 1, \cdots, q-1\}$ dan is het geordend t-tal MOLS $(A_1, A_2, \cdots, A_t)$ over F_q equivalent met een geordend t-tal MOLS $(C_1, C_2, \cdots, C_t)$ over F_q, waarbij $[0\ 1\ 2\ \cdots\ q-1]$ de eerste rij is van C_i, $i = 1, 2, \cdots, t$, en $[0\ 1\ 2\ \cdots\ q-1]'$ de eerste kolom is van C_1.

Stelling 10.2.7
Zijn $A_1, A_2, \cdots, A_t$ MOLS van de orde $q, q > 1$, dan is $t \leq q - 1$.

Bewijs. Onderstel dat $A_1, A_2, \cdots, A_t$ MOLS van de orde q, $q > 1$, over $F_q = \{0, 1, 2, \cdots, q-1\}$ zijn. Dan is $(A_1, A_2, \cdots, A_t)$ equivalent met een geordend t-tal MOLS $(C_1, C_2, \cdots, C_t)$ over F_q, waarbij $[0\ 1\ 2\ \cdots\ q-1]$ de eerste rij is van $C_i, i = 1, 2, \cdots, t$. Stel $C_k = [c_{ij}^{(k)}]$, $k = 1, 2, \cdots, t$. Onderstel dat $c_{21}^{(k)} = c_{21}^{(l)} = s, k \neq l$. Dan zou $(c_{21}^{(k)}, c_{21}^{(l)}) = (s, s) = (c_{1,s+1}^{(k)}, c_{1,s+1}^{(l)})$, een strijdigheid aangezien C_k en C_l MOLS zijn. Dus zijn $c_{21}^{(1)}, c_{21}^{(2)}, \cdots, c_{21}^{(t)}$ t verschillende elementen van F_q. Verder is $c_{21}^{(k)} \neq 0$, $k = 1, 2, \cdots, t$, omdat in de eerste kolom van C_k geen twee nullen voorkomen. Bijgevolg zijn $c_{21}^{(1)}, c_{21}^{(2)}, \cdots, c_{21}^{(t)}$ t verschillende elementen van $F_q - \{0\}$. Dus is $t \leq |F_q - \{0\}| = q - 1$. □

Opmerking 10.2.8
Voor $q = 1$ is Stelling 10.2.7 vanzelfsprekend niet geldig.

Definitie 10.2.9
Zijn $A_1, A_2, \cdots, A_{q-1}$ MOLS van de orde $q, q > 1$, dan zegt men dat $\{A_1, A_2, \cdots, A_{q-1}\}$ een *complete verzameling MOLS* (*complete set of MOLS*) van de orde q is.

Stelling 10.2.10
Er bestaat een complete verzameling MOLS van de orde q, $q > 1$, a.s.a. een projectief vlak van de orde q bestaat.

Bewijs. Zonder bewijs. □

Opmerking 10.2.11
Om het niet-bestaan van een projectief vlak van de orde 10 aan te tonen is het dus voldoende om het niet-bestaan van een complete verzameling MOLS van de orde 10 aan te tonen. Tot hiertoe weet men echter niet of er al dan niet 3 MOLS van de orde 10 bestaan.

10.3 Het vraagstuk van Euler

In 10.3 zullen wij onder andere het beroemde "vraagstuk van de 36 officieren" van Euler bespreken.

Stelling 10.3.1
Bestaan t MOLS van de orde q en bestaan t MOLS van de orde q', dan bestaan t MOLS van de orde qq'.

Bewijs. Onderstel dat $A_1, A_2, \cdots, A_t$, met $A_k = [a_{ij}^{(k)}]$, t MOLS van de orde q over F_q zijn, en dat $B_1, B_2, \cdots, B_t$, met $B_k = [b_{ij}^{(k)}]$, t MOLS van de orde q' over $F_{q'}$ zijn. Stel $I = \{1, 2, \cdots, q\}$, $J = \{1, 2, \cdots, q'\}$, $K = \{1, 2, \cdots, qq'\}$. Beschouw nu een willekeurige bijectie

$$\sigma : I \times J \to K, (a, b) \mapsto (a, b)^{\sigma}.$$

Stel nu

$$C_k = [c_{uv}^{(k)}], u, v = 1, 2, \cdots, qq' \text{ en } k = 1, 2, \cdots, t,$$

waarbij

$$c_{uv}^{(k)} = (a_{ij}^{(k)}, b_{rs}^{(k)}) \text{ met } (i,r)^\sigma = u, (j,s)^\sigma = v.$$

Wij tonen nu aan dat C_k een latijns vierkant is over $F_q \times F_{q'}$. Onderstel dat $c_{uv}^{(k)} = c_{uv'}^{(k)}$. Dan is $(a_{ij}^{(k)}, b_{rs}^{(k)}) = (a_{ij'}^{(k)}, b_{rs'}^{(k)})$, met $(i,r)^\sigma = u$, $(j,s)^\sigma = v, (j',s')^\sigma = v'$. Dus is $a_{ij}^{(k)} = a_{ij'}^{(k)}$ en $b_{rs}^{(k)} = b_{rs'}^{(k)}$. Aangezien A_k en B_k latijns zijn gelden $j = j'$ en $s = s'$. Bijgevolg is $v = v'$. Analoog volgt uit $c_{uv}^{(k)} = c_{u'v}^{(k)}$ dat $u = u'$. Wij besluiten dat C_k een latijns vierkant is, $k = 1, 2, \cdots, t$.

Nu tonen wij aan dat C_k en C_l, $k \neq l$, orthogonaal zijn. Onderstel dat $(c_{uv}^{(k)}, c_{uv}^{(l)}) = (c_{u'v'}^{(k)}, c_{u'v'}^{(l)})$. Dan is $c_{uv}^{(k)} = c_{u'v'}^{(k)}$ en $c_{uv}^{(l)} = c_{u'v'}^{(l)}$. Dus geldt $(a_{ij}^{(k)}, b_{rs}^{(k)}) = (a_{i'j'}^{(k)}, b_{r's'}^{(k)})$ en $(a_{ij}^{(l)}, b_{rs}^{(l)}) = (a_{i'j'}^{(l)}, b_{r's'}^{(l)})$, met $(i,r)^\sigma = u, (j,s)^\sigma = v, (i',r')^\sigma = u', (j',s')^\sigma = v'$. Hieruit volgt dat $a_{ij}^{(k)} = a_{i'j'}^{(k)}, b_{rs}^{(k)} = b_{r's'}^{(k)}$, $a_{ij}^{(l)} = a_{i'j'}^{(l)}, b_{rs}^{(l)} = b_{r's'}^{(l)}$, m.a.w. $(a_{ij}^{(k)}, a_{ij}^{(l)}) = (a_{i'j'}^{(k)}, a_{i'j'}^{(l)})$ en $(b_{rs}^{(k)}, b_{rs}^{(l)}) = (b_{r's'}^{(k)}, b_{r's'}^{(l)})$. Aangezien A_k en A_l, resp. B_k en B_l, onderling orthogonaal zijn is noodzakelijk $i = i'$, $j = j'$, resp. $r = r'$, $s = s'$. Dus is $u = u'$ en $v = v'$. Zo besluiten wij dat C_k en C_l, $k \neq l$ en $k, l = 1, 2, \cdots, t$, onderling orthogonaal zijn. □

Voorbeeld 10.3.2
Wegens Stelling 10.2.2 bestaan 8 MOLS van de orde 9 en 7 MOLS van de orde 8. Wegens Stelling 10.3.1 bestaan dus 7 MOLS van de orde 72.

Stelling 10.3.3
Is $q = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, met $q \in \mathbb{N} - \{0,1\}, a_1, a_2, \cdots, a_k \in \mathbb{N}_0$ en $p_1, p_2, \cdots, p_k$ verschillende priemgetallen, en is $t = min\ \{p_1^{a_1} - 1, p_2^{a_2} - 1, \cdots, p_k^{a_k} - 1\}$, dan bestaan t MOLS van de orde q.

Bewijs. Wegens Stelling 10.2.2 bestaan $p_i^{a_i} - 1$ MOLS van de orde $p_i^{a_i}$, $i = 1, 2, \cdots, k$. Er bestaan dus zeker t MOLS van de orde $p_i^{a_i}$, $i = 1, 2, \cdots, k$. Door herhaalde toepassing van Stelling 10.3.1 bestaan dus t MOLS van de orde $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q$. □

Stelling 10.3.4
Is $q \not\equiv 2$ (mod 4), $q \in \mathbb{N} - \{0,1\}$, dan bestaan er steeds twee onderling orthogonale latijnse vierkanten van de orde q.

Bewijs. Onderstel dat $q = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, met $a_1, a_2, \cdots, a_k \in \mathbb{N}_0$ en $p_1, p_2, \cdots, p_k$ verschillende priemgetallen. Stel t= min $\{p_1^{a_1} - 1, p_2^{a_2} - 1, \cdots, p_k^{a_k} - 1\}$. Moest $t = 1$, dan zou er een $i \in \{1, 2, \cdots, k\}$ zijn waarvoor $1 = p_i^{a_i} - 1$, zodat $p_i = 2$ en $a_i = 1$. Dus zou $q = 2q'$, met q' oneven, zodat $q \equiv 2$ (mod 4), een strijdigheid. Bijgevolg is $t \geq 2$. Uit Stelling 10.3.3 volgt dat er t MOLS van de orde q bestaan, zodat er ook twee MOLS van de orde q bestaan. □

Euler, Tarry, Bose, Shrikhande en Parker

Euler zocht naar een oplossing van het volgende vraagstuk. Er zijn 36 officieren waarvan 6 behoren tot regiment 1, 6 tot regiment 2, $\cdots$, 6 tot regiment 6, waarvan 6 graad 1 hebben,

6 graad 2, $\cdots$, 6 graad 6, en waarbij geen twee officieren terzelfdertijd dezelfde graad hebben en tot een zelfde regiment behoren. Is het nu mogelijk om met die 36 officieren een vierkante formatie te vormen, zodanig dat in elke rij en elke kolom juist één officier van elke graad en elk regiment voorkomt? Onderstel dat wij een oplossing van het vraagstuk hebben. Bezit een officier graad i en behoort hij tot regiment j, dan noteren we hem (i, j). Vervang nu in de formatie elke officier (i, j) door het element i, resp. j. Dan ontstaat een 6×6-rooster A, resp. B, over $F_6 = \{1, 2, \cdots, 6\}$. Het is duidelijk dat A en B twee MOLS van de orde 6 zijn. Omgekeerd correspondeert met twee MOLS van de orde 6 een oplossing van het vraagstuk van Euler. Euler vond geen oplossing voor het vraagstuk. Aangezien geen twee MOLS van de orde 2 bestaan, en aangezien hij geen twee MOLS van de orde 6 vond, sprak Euler in 1782 het volgende vermoeden uit: voor $q \equiv 2 \pmod 4$ bestaan geen twee MOLS van de orde q. De volgende twee stellingen sloten het probleem af.

Stelling 10.3.5 (Tarry(1900))
Er bestaan geen twee MOLS van de orde 6.

Bewijs. Zonder bewijs (in het zeer lange bewijs gaat Tarry alle mogelijkheden na). □

Stelling 10.3.6 (Bose, Shrikhande en Parker (1960))
Voor $q \equiv 2$ (mod 4), $q \in \mathbb{N}_0 - \{2, 6\}$, bestaan steeds 2 MOLS van de orde q.

Bewijs. Zonder bewijs (het bewijs van deze stelling is constructief). □

10.4 Optimale één-foutverbeterende codes van lengte 4

In deze paragraaf zullen wij het hoofdprobleem van de codeertheorie voor codes van lengte 4 en minimum afstand 3 onderzoeken, dat is, wij zullen zoeken naar $A_q(4, 3)$. In 10.4 onderstellen wij steeds dat $q \neq 1$.

Stelling 10.4.1
Voor elke q is $A_q(4, 3) \leq q^2$.

Bewijs. Onderstel dat C een q-aire $(4, M, 3)$-code is en beschouw verschillende codewoorden $\bar{x} = x_1x_2x_3x_4$ en $\bar{y} = y_1y_2y_3y_4$ van C. Aangezien $d(C) = 3$ is noodzakelijk $(x_1, x_2) \neq (y_1, y_2)$. Bijgevolg is $M = |C| \leq |F_q \times F_q| = q^2$. □

Voorbeeld 10.4.2
Aangezien Ham(2,3) een $(4, 9, 3)$-code over GF(3) is, volgt uit Stelling 10.4.1 dat $A_3(4, 3) = 9$.

Opmerking 10.4.3
De Hamming grens (zie 2.3.6) geeft $A_q(4, 3) \leq q^4/(4q - 3)$. Voor $q > 3$ is de ongelijkheid uit Stelling 10.4.1 veel sterker. Voor $q = 3$ geven beide grenzen $A_3(4, 3) \leq 9$; voor $q = 2$ geeft de Hamming grens $A_2(4, 3) \leq 3$.

Stelling 10.4.4
Er bestaat een q-aire $(4, q^2, 3)$-code a.s.a. een paar MOLS van de orde q bestaat.

Bewijs. Onderstel dat C een $(4, q^2, 3)$-code is over $F_q = \{1, 2, \cdots, q\}$. Dan is $(x_1, x_2) \neq (y_1, y_2)$ voor elke twee codewoorden $\bar{x} = x_1x_2x_3x_4$, $\bar{y} = y_1y_2y_3y_4$ van C, en $\{(x_1, x_2) \parallel \bar{x} = x_1x_2x_3x_4 \in C\} = (F_q)^2$. Bijgevolg is

$$C = \{ija_{ij}b_{ij} \parallel (i, j) \in (F_q)^2\}.$$

Aangezien $d(C) = 3$ is $(j, a_{ij}) \neq (j, a_{i'j}), i \neq i'$, en $(i, a_{ij}) \neq (i, a_{ij'}), j \neq j'$. Bijgevolg is $A = [a_{ij}]$ een latijns vierkant over F_q. Analoog is $B = [b_{ij}]$ een latijns vierkant over F_q. Verder is $(a_{ij}, b_{ij}) \neq (a_{i'j'}, b_{i'j'})$ voor $(i, j) \neq (i', j')$. Hieruit volgt dat A en B onderling orthogonaal zijn.

Omgekeerd, beschouw onderling orthogonale latijnse vierkanten $A = [a_{ij}]$ en $B = [b_{ij}]$ over $F_q = \{1, 2, \cdots, q\}$. Stel nu

$$C = \{ija_{ij}b_{ij} \parallel (i, j) \in (F_q)^2\}.$$

Dan is C een q-aire code van lengte 4 met q^2 codewoorden. Onderstel dat $d(C) \leq 2$. Dan zouden voor ten minste twee verschillende codewoorden $ija_{ij}b_{ij}$ en $i'j'a_{i'j'}b_{i'j'}$ $((i, j) \neq (i', j'))$ de coördinaten in ten minste twee posities gelijk zijn. Moest $(i, a_{ij}) = (i', a_{i'j'})$ of $(j, a_{ij}) = (j', a_{i'j'})$, dan zou A geen latijns vierkant zijn; moest $(i, b_{ij}) = (i', b_{i'j'})$ of $(j, b_{ij}) = (j', b_{i'j'})$, dan zou B geen latijns vierkant zijn; moest $(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'})$, dan zouden A en B niet orthogonaal zijn. Uit deze strijdigheden volgt dat $d(C) \geq 3$. Moest $d(C) = 4$, dan zouden elke twee verschillende codewoorden in de eerste positie verschillen zodat $|C| \leq q$, een strijdigheid. Zo besluiten wij dat $d(C) = 3$ en zodoende is C een q-aire $(4, q^2, 3)$-code. □

Stelling 10.4.5
Voor alle $q \in \mathbb{N}_0 - \{2, 6\}$ is $A_q(4, 3) = q^2$.

Bewijs. Dit is een gevolg van Stellingen 10.4.1, 10.4.4, 10.3.4 en 10.3.6. □

Nu blijft er ons nog slechts over $A_2(4, 3)$ en $A_6(4, 3)$ te bepalen.

Stelling 10.4.6
$A_2(4, 3) = 2$ *en* $A_6(4, 3) = 34$.

Bewijs. Onderstel eerst en vooral dat $F_2 = \{0, 1\}$. Is C een $(4, M, 3)$-code over F_2, dan is voor elke twee verschillende codewoorden $\bar{x} = x_1x_2x_3x_4$ en $\bar{y} = y_1y_2y_3y_4$ voldaan aan $(x_i, x_j) \neq (y_i, y_j)$ voor $i \neq j$. Uit Lemma 2.2.5 volgt dat wij mogen onderstellen dat $\bar{0} = 0000 \in C$. Onderstel eerst dat $\bar{y} = 1111$ een codewoord is. Dan is $d(\bar{0}, \bar{y}) = 4$. Voor elk ander woord $\bar{z}$ is dan $d(\bar{0}, \bar{z}) \leq 2$ of $d(\bar{y}, \bar{z}) \leq 2$, zodat $\bar{z} \notin C$ en dus $d(C) = 4$, een strijdigheid. Is $\bar{y} \neq \bar{0}$ een codewoord, dan zal $\bar{y}$ dus juist één nul als coördinaat hebben. Onderstel bijvoorbeeld dat $\bar{y} = 0111$. Is $\bar{z}$ een derde codewoord, dan bezit $\bar{z}$ juist één nul in de 2de, 3de of 4de positie. Maar dan zou $d(\bar{z}, \bar{y}) = 2$, een strijdigheid. Uit dit alles volgt dat $A_2(4, 3) = 2$.

Onderstel vervolgens dat $F_6 = \{1, 2, \cdots, 6\}$. Beschouw de latijnse vierkanten

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 4 & 6 & 5 & 1 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 1 & 2 & 3 & 4 \end{bmatrix} \text{ en } B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 6 & 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ 5 & 6 & 2 & 1 & 3 & 4 \end{bmatrix}.$$

Stelt men $A = [a_{ij}]$ en $B = [b_{ij}]$, dan zijn de 34 koppels (a_{ij}, b_{ij}) met $(i, j) \neq (6, 5), (6, 6)$ verschillend. Zoals in het bewijs van Stelling 10.4.4 toont men dan aan dat

$$C = \{ija_{ij}b_{ij} \parallel (i, j) \in (F_6)^2, \text{ met } (i, j) \neq (6, 5), (6, 6)\}$$

een $(4, 34, 3)$-code over F_6 is. Onderstel nu dat er een $(4, 35, 3)$-code C' over F_6 bestaat. Dan is C' van de gedaante

$$C' = \{ija'_{ij}b'_{ij} \parallel (i, j) \in (F_6)^2, \text{ met } (i, j) \neq (i_0, j_0)\}$$

voor een zeker koppel (i_0, j_0). Beschouw nu de partiële 6×6-roosters $A_1 = [a'_{ij}]$ en $B_1 = [b'_{ij}]$, waarbij in A_1 en B_1 het element op de $i_0$de rij en $j_0$de kolom ontbreekt. Merk op dat alle koppels $(a'_{ij}, b'_{ij}), (i, j) \neq (i_0, j_0)$, verschillend zijn.

Stel $(F_6)^2 - \{(a'_{ij}, b'_{ij}) \parallel (i, j) \in (F_6)^2, (i, j) \neq (i_0, j_0)\} = (a'_{i_0j_0}, b'_{i_0j_0})$. Dan is $\{(a'_{ij}, b'_{ij}) \parallel (i, j) \in (F_6)^2\} = (F_6)^2$. Onderstel dat $a'_{i_0j_0} = a'_{i_0j} = k$ met $j_0 \neq j$. Aangezien k in de $i$de rij van A_1, $i \neq i_0$, juist éénmaal voorkomt zijn er 7 verschillende koppels van de gedaante $(k = a'_{ij}, b'_{ij})$, een strijdigheid. Vervolledigen wij A_1, resp. B_1, tot een 6×6-rooster A_2, resp. B_2, door toevoegen van het element $a'_{i_0j_0}$, resp. $b'_{i_0j_0}$, dan zijn alle elementen van de $i_0$de rij van A_2 verschillend; analoog zijn alle elementen van de $j_0$de kolom van A_2 verschillend. Bijgevolg is A_2 een latijns vierkant over F_6; analoog is B_2 een latijns vierkant over F_6. Bovendien zijn A_2 en B_2 onderling orthogonaal. Dit is in strijd met Stelling 10.3.5. Bijgevolg bestaat er geen $(4, 35, 3)$-code over F_6. Zo besluiten wij dus dat $A_6(4, 3) = 34$. □

10.5 q-aire $(n, q^2, n-1)$-codes en MOLS

In deze paragraaf onderzoeken wij het verband tussen q-aire $(n, q^2, n-1)$-codes en MOLS van de orde q. Merk op dat wij voor $n = 4$ opnieuw q-aire $(4, q^2, 3)$-codes hebben. In 10.5 onderstellen wij steeds dat $q \neq 1$.

Stelling 10.5.1
Voor elke q is $A_q(n, n-1) \leq q^2$.

Bewijs. Onderstel dat C een q-aire $(n, M, n-1)$-code is en beschouw verschillende codewoorden $\bar{x} = x_1x_2\cdots x_n$ en $\bar{y} = y_1y_2\cdots y_n$ van C. Aangezien $d(C) = n-1$ is noodzakelijk $(x_1, x_2) \neq (y_1, y_2)$. Bijgevolg is $M = |C| \leq |F_q \times F_q| = q^2$. □

Stelling 10.5.2
Een q-aire $(n, q^2, n-1)$-code bestaat a.s.a. $n-2$ MOLS van de orde q bestaan.

Bewijs. Onderstel dat C een $(n, q^2, n-1)$-code is over $F_q = \{1, 2, \cdots, q\}$. Dan is $(x_1, x_2) \neq (y_1, y_2)$ voor elke twee codewoorden $\bar{x} = x_1 x_2 \cdots x_n, \bar{y} = y_1 y_2 \cdots y_n$ van C en $\{(x_1, x_2) \parallel \bar{x} = x_1 x_2 \cdots x_n \in C\} = (F_q)^2$. Bijgevolg is

$$C = \{ij a_{ij}^{(1)} a_{ij}^{(2)} \cdots a_{ij}^{(n-2)} \parallel (i,j) \in (F_q)^2\}.$$

Aangezien $d(C) = n-1$ is $(j, a_{ij}^{(k)}) \neq (j, a_{i'j}^{(k)}), i \neq i'$, en $(i, a_{ij}^{(k)}) \neq (i, a_{ij'}^{(k)}), j \neq j'$. Bijgevolg is $A_k = [a_{ij}^{(k)}]$ een latijns vierkant over $F_q, k = 1, 2, \cdots, n-2$. Verder is $(a_{ij}^{(k)}, a_{ij}^{(l)}) \neq (a_{i'j'}^{(k)}, a_{i'j'}^{(l)})$ voor $k \neq l$ en $(i,j) \neq (i', j')$. Hieruit volgt dat A_k en A_l onderling orthogonaal zijn voor elke $k \neq l$. Dus zijn $A_1, A_2, \cdots, A_{n-2}$ $n-2$ MOLS van de orde q.

Omgekeerd beschouwen wij nu $n-2$ MOLS $A_k = [a_{ij}^{(k)}], k = 1, 2, \cdots, n-2$, over $F_q = \{1, 2, \cdots, q\}$. Stel nu

$$C = \{ij a_{ij}^{(1)} a_{ij}^{(2)} \cdots a_{ij}^{(n-2)} \parallel (i,j) \in (F_q)^2\}.$$

Dan is C een q-aire code van lengte n met q^2 codewoorden. Onderstel dat $d(C) < n-1$. Dan zouden voor ten minste twee verschillende codewoorden $ij a_{ij}^{(1)} a_{ij}^{(2)} \cdots a_{ij}^{(n-2)}$ en $i'j' a_{i'j'}^{(1)} a_{i'j'}^{(2)} \cdots a_{i'j'}^{(n-2)}$ $((i,j) \neq (i',j'))$ de coördinaten in ten minste twee posities gelijk zijn. Moest $(i, a_{ij}^{(k)}) = (i', a_{i'j'}^{(k)})$ of $(j, a_{ij}^{(k)}) = (j', a_{i'j'}^{(k)})$, $k \in \{1, 2, \cdots, n-2\}$, dan zou A_k geen latijns vierkant zijn; moest $(a_{ij}^{(k)}, a_{ij}^{(l)}) = (a_{i'j'}^{(k)}, a_{i'j'}^{(l)}), k \neq l$, dan zouden A_k en A_l niet onderling orthogonaal zijn. Uit deze strijdigheden volgt dat $d(C) \geq n-1$. Moest $d(C) = n$, dan zouden elke twee verschillende codewoorden in de eerste positie verschillen zodat $|C| \leq q$ een strijdigheid. Zo besluiten wij dat $d(C) = n-1$ en zodoende is C een q-aire $(n, q^2, n-1)$-code. □

Stelling 10.5.3

(i) $A_q(3,2) = q^2$ *voor alle* q*;*

(ii) $A_q(n, n-1) = q^2$ *voor* q *een priemmacht en* $n \leq q+1$*;*

(iii) $A_q(n, n-1) < q^2$ *voor alle* $n > q+1$.

Bewijs.

(i) Voor elke $q \in \mathbb{N}_0$ bestaat een latijns vierkant van de orde q. Uit Stelling 10.5.2 volgt dan dat $A_q(3,2) = q^2$.

(ii) Is q een priemmacht en $n-2 \leq q-1$, dan bestaan wegens Stelling 10.2.2 $n-2$ MOLS van de orde q.

(iii) Onderstel dat $n > q+1$. Wegens Stelling 10.2.7 bestaan geen $n-2$ MOLS van de orde q, zodat wegens Stelling 10.5.2 $A_q(n, n-1) \neq q^2$. Uit Stelling 10.5.1 volgt dan dat $A_q(n, n-1) < q^2$. □

Hoofdstuk 11

Grenzen op codes

11.1 De bolpakkingsgrens of de Hamming grens

In Stelling 2.3.5 hebben wij gezien dat elke q-aire (n, M, d)-code, met $d = 2t+1$ of $d = 2t+2$, voldoet aan

$$M\left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right] \leq q^n.$$

Bijgevolg is

$$A_q(n,d) \leq q^n / \left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right]. \tag{11.1}$$

In het bijzonder is

$$A_2(n,d) \leq 2^n / \left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right].$$

Hebben wij gelijkheid in (11.1), dan is de code perfect.

Aangezien $\mathrm{Ham}(r,q), r \geq 2$ en q een priemmacht, een perfecte q-aire

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right] - \text{code}$$

is (zie Hoofdstuk 7), geldt

$$A_q\left(\frac{q^r-1}{q-1}, 3\right) = q^{n-r}, \text{ met } n = \frac{q^r-1}{q-1}. \tag{11.2}$$

Uit de theorie van de Golay codes (zie Hoofdstuk 9) volgt verder dat

$$A_3(11,5) = 3^6 \text{ en } A_2(23,7) = 2^{12}. \tag{11.3}$$

Ten slotte volgt uit Stelling 9.5.1 dat voor q een priemmacht en niet-triviale codes, gelijkheid in (11.1) slechts geldt voor de parameters in (11.2) en (11.3).

11.2 Verkorten van een code

Beschouw een q-aire (n, M, d)-code C over F_q. Verder beschouwen wij de verzameling U van alle codewoorden met een gegeven element $\lambda \in F_q$ in positie j. In de elementen van U laten wij nu positie j weg. Dan vinden wij een q-aire $(n-1, M', d')$-code over F_q, met $M' \leq M$ en $d' \geq d$ (over het algemeen is $d' = d$). Deze procedure noemen wij het *verkorten* (*shortening*) van C.

Onderstel in het bijzonder dat C een lineaire $[n, k, d]$-code is over GF(q), en dat $\lambda = 0$. Men toont dan gemakkelijk aan dat de verkorte code C' eveneens lineair is. Is $\bar{x} = x_1 x_2 \cdots x_n \in C$, dan behoort $\bar{x}' = x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_n$ tot C' a.s.a. $x_j = 0$, dus a.s.a. $\bar{x}$ behoort tot het hypervlak π_j met vergelijking $X_j = 0$ van $V(n, q)$. Is $C \subseteq \pi_j$, dan is C' een q-aire $[n-1, k, d]$-code. Is $C \not\subseteq \pi_j$, dan is $C \cap \pi_j$ een $(k-1)$-dimensionale deelruimte van π_j zodat C' een q-aire $[n-1, k-1, d']$-code is met $d' \geq d$. Onderstel nu dat H een pariteit controlematrix is van C; dus H is een $(n-k) \times n$-matrix met rang $H = n - k$. Onderstel eerst dat $C \subseteq \pi_j$. Noem H_1 de $(n-k) \times (n-1)$-matrix die uit H ontstaat door de $j$de kolom weg te laten. Dan is rang $H_1 = n - k - 1$ en alle rijen van H_1 zijn orthogonaal met alle vectoren van C'. Een $(n-k-1) \times (n-1)$-deelmatrix H^* van H_1 waarvoor rang $H^* = n - k - 1$ is dan een pariteit controlematrix van C'. Onderstel vervolgens dat $C \not\subseteq \pi_j$. Is H^* de matrix die uit H ontstaat door de $j$de kolom weg te laten, dan is H^* een $(n-k) \times (n-1)$-matrix met rang $H^* = n - k$ en waarbij alle rijen van H^* orthogonaal zijn met alle vectoren van C'. Bijgevolg is H^* een pariteit controlematrix van C'.

Voorbeeld 11.2.1
Wij hernemen de lineaire $[10, 8]$-code C' over GF(11) uit 5.4, die gedefinieerd werd door de pariteit controlematrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

Aangezien elke twee kolommen van H lineair onafhankelijk zijn en elke drie kolommen van H lineair afhankelijk zijn, is $d(C') = 3$. Nu is

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}$$

een pariteit controlematrix voor Ham$(2, 11)$. Verkorten wij nu Ham$(2, 11)$ met betrekking tot de eerste positie, en verkorten wij daarna deze nieuwe code opnieuw met betrekking tot de eerste positie, dan ontstaat een lineaire $[10, 8]$-code over GF(11) met pariteit controlematrix H, m.a.w. dan vinden wij C'. Men kan aantonen dat C' optimaal is, m.a.w. $A_{11}(10, 3) = 11^8$.

Stelling 11.2.2 ((Best en Brouwer (1977))
Elke binaire lineaire code die verkregen wordt door de Hamming code Ham$(r, 2)$, $r \geq 2$, u maal, met $u = 1, 2, 3$, te verkorten is een optimale code met minimum afstand 3, m.a.w.

$$A_2(2^r - s, 3) = 2^{2^r - r - s}, r \geq 2 \text{ en } s = 1, 2, 3, 4.$$

Bewijs. Zonder bewijs. □

Opmerking 11.2.3
De stelling is niet meer juist indien wij $\mathrm{Ham}(r, 2)$ viermaal verkorten.

11.3 De Singleton grens

De volgende grens werd door Singleton in 1964 ontdekt.

Stelling 11.3.1
Er geldt

$$A_q(n, d) \leq q^{n-d+1}. \tag{11.4}$$

Is in het bijzonder C een lineaire $[n, k]$-code over $\mathrm{GF}(q)$*, dan is*

$$k \leq n - d + 1. \tag{11.5}$$

Bewijs. Onderstel dat C een q-aire (n, M, d)-code is. Beschouw verschillende codewoorden $\bar{x} = x_1x_2 \cdots x_n$ en $\bar{y} = y_1y_2 \cdots y_n$, en onderstel dat $(x_1, x_2, \cdots, x_{n-d+1}) = (y_1, y_2, \cdots, y_{n-d+1})$. Dan zou $d(\bar{x}, \bar{y}) \leq d - 1$, een strijdigheid. Voor verschillende codewoorden $\bar{x}$ en $\bar{y}$ is dus $(x_1, x_2, \cdots, x_{n-d+1}) \neq (y_1, y_2, \cdots, y_{n-d+1})$. Bijgevolg is $|C| = M \leq q^{n-d+1}$.

Is C een lineaire $[n, k, d]$-code over $\mathrm{GF}(q)$, dan is dus $|C| = q^k \leq q^{n-d+1}$, zodat $k \leq n - d + 1$.

In het lineaire geval kunnen wij ook als volgt te werk gaan. Noem $G = [I_k \quad A]$ een voortbrengende matrix in standaard gedaante. Dan is $d(C) = w(C) \leq$ gewicht van de rijen van $G \leq n - k + 1$. Dus is $d \leq n - k + 1$. □

Opmerkingen 11.3.2

(i) Zowel het tweede lid van (11.4) als het tweede lid van (11.5) noemt men de Singleton grens.

(ii) Stelling 10.4.1 en Stellling 10.5.1 zijn bijzondere gevallen van Stelling 11.3.1.

(iii) Wegens Stelling 10.4.5 en Stelling 10.5.3 wordt de Singleton grens bereikt in volgende gevallen

  (a) voor alle $q \in \mathbb{N}_0 - \{2, 6\}$ is $A_q(4, 3) = q^2$,

  (b) voor alle q is $A_q(3, 2) = q^2$,

  (c) voor q een priemmacht en $n \leq q + 1$ is $A_q(n, n - 1) = q^2$.

(iv) In Stelling 10.5.1 hebben wij gezien dat $A_q(n, n - 1) = q^2$ a.s.a. er $n - 2$ MOLS van de orde q bestaan.

Definitie 11.3.3
Wordt de gelijkheid bereikt in (11.4), dan spreekt men van een *Maximum Distance Separable code* (M.D.S. code).

Onderstel dat C een M.D.S. code is, m.a.w. C is een (n, q^k, d)-code met $k = n - d + 1$.

Fundamenteel probleem. Wat is de maximum lengte voor gegeven q en d, en welke is de structuur van C in het optimale geval?

Geval $k = 1$. Dan is $d = n$ en $|C| = q$. Men toont gemakkelijk aan dat elke code met deze parameters gelijkwaardig is met de q-aire herhalingscode van lengte n (zie Voorbeeld 2.2.3 (ii)).

Geval $k = 2$. Dan is $d = n - 1$ en $|C| = q^2$. In Stelling 10.5.2 hebben wij gezien dat dergelijke M.D.S. code bestaat a.s.a. $n - 2$ MOLS van de orde q bestaan. Uit Stelling 10.5.3 volgt dat voor elke zulke code met $q \neq 1$ noodzakelijk voldaan is aan $n \leq q + 1$, en dat voor q een priemmacht de bovengrens $n = q + 1$ bereikt wordt.

Geval $k > 2$. Is C een M.D.S. code met $q \neq 1$, dan kunnen wij uit het Geval $k = 2$ met inductie bewijzen dat voldaan is aan $n \leq q + k - 1$.

Geval $k = 3$. Hier is dus $n \leq q + 2$. Men kan bewijzen dat een dergelijke M.D.S. code met $n = q + 2$ bestaat als $q = 2^r$, $r \geq 1$.

Geval $k = 4$. Hier is $n \leq q + 3$. Men kan bewijzen dat een dergelijke M.D.S. code met $n = q + 3$ bestaat als $q = 2$. Bovendien bewezen Bruen en Silverman (1983) dat voor elke q-aire $(q + 3, q^4, q)$-code C, $q \neq 1$, voldaan is aan $q = 2$ of $36|q$.

Veel meer is er niet gekend wat betreft de bovengrens van n bij M.D.S. codes als er niet gevraagd wordt dat C lineair moet zijn.

We beschouwen nu het lineaire geval. De $[n, k, d]$-code C over GF(q) is dus een M.D.S. code a.s.a. $k = n - d + 1$. Stel dat C een $[n, k, d]$-code is over GF(q) met $k = n - d + 1$, $k < n - 1$, en onderstel dat H een pariteit controlematrix is van C. Aangezien $d = n - k + 1 = r + 1$ zijn elke r kolommen van H lineair onafhankelijk en bestaan er $r + 1$ kolommen die lineair afhankelijk zijn (dit laatste is triviaal aangezien H een $r \times n$-matrix is). Elke kolom van H kan opgevat worden als een stel coördinaten van een punt in de projectieve ruimte PG$(r - 1, q)$ t.o.v. een gegeven coördinatensysteem. Op die manier vinden wij n punten in PG$(r - 1, q)$ waarvan geen r in een zelfde hypervlak gelegen zijn. Omgekeerd, met elke n punten in PG$(r-1, q)$, $r \geq 2$, waarvan geen r in een zelfde hypervlak gelegen zijn correspondeert een pariteit controlematrix van een lineaire M.D.S. code.

Merk op dat de gevallen $k = n$ en $k = n-1$ triviaal zijn (een $[n, n-1]$-code C over GF(q) is een M.D.S. code a.s.a. C een hypervlak is van de gedaante $a_1X_1 + a_2X_2 + \ldots + a_nX_n = 0$ met $a_1a_2 \ldots a_n \neq 0$).

In 1955 voerde de Italiaanse wiskundige B. Segre volgende definitie in, en dit zonder het verband met codes, dat trouwens veel later werd ontdekt, te kennen: een *l-boog (l-arc)* van PG$(m, q), l \geq m + 1$ en $m \geq 1$, is elke verzameling van l punten in PG(m, q) waarvan

geen $m+1$ in een zelfde hypervlak gelegen zijn. Uit hetgeen voorafgaat hebben wij dan volgende stelling.

Stelling 11.3.4
De theorie van de lineaire M.D.S. *codes, met* $k < n-1$*, is gelijkwaardig met de theorie van de* l*-bogen in* $\mathrm{PG}(m,q), l \geq m+2$.

In 1955 stelde Segre de volgende drie problemen betreffende l-bogen in $\mathrm{PG}(m,q)$, $m > 1$:

(i) Wat is voor gegeven m en q de maximale waarde van l waarvoor een l-boog in $\mathrm{PG}(m,q)$ bestaat?

(ii) Wat zijn de waarden van q en m, $q > m+1$, waarvoor elke $(q+1)$-boog van $\mathrm{PG}(m,q)$ een *rationale normaalkromme* (*normal rational curve*) is? (Een rationale normaalkromme van $\mathrm{PG}(m,q)$ is elke verzameling punten die na een behoorlijke keuze van het coördinatensysteem voorgesteld kan worden door

$$\{(0,0,\cdots,0,1)\} \cup \{(1,t,t^2,\cdots,t^m) \parallel t \in \mathrm{GF}(q)\}.$$

Voor $m=2$ bijvoorbeeld zijn de rationale normaalkrommen de niet-singuliere kegelsneden. Merk op dat elke rationale normaalkromme van $\mathrm{PG}(m,q)$, met $q \geq m$, een $(q+1)$-boog is).

(iii) Voor gegeven m en q, met $q > m+1$, welke zijn de waarden van l waarvoor elke l-boog van $\mathrm{PG}(m,q)$ bevat is in een $(q+1)$-boog van deze ruimte?

Belangrijkste resultaten in verband met de problemen (i), (ii) en (iii).

1947: Bose bewijst dat $l \leq q+1$ voor $m=2$ en q oneven (het is gemakkelijk om aan te tonen dat $l \leq q+2$; voor q even bestaat steeds een $(q+2)$-boog in $\mathrm{PG}(2,q)$).

1955: Segre bewijst dat voor q oneven elke $(q+1)$-boog van $\mathrm{PG}(2,q)$ een kegelsnede is. Segre lost (i) en (ii) op voor $m=3$ en q oneven, en lost (i) op voor $m=4$ en q oneven.

1967: Segre toont aan dat (iii) geldt voor $m=2$ en l voldoende groot t.o.v. q.

1968: Voor q oneven lost Thas (i), (ii) en (iii) op voor de meeste waarden van de parameters.

1969: Thas bewijst dat de duale code van een lineaire M.D.S. code opnieuw een lineaire M.D.S. code is (het bewijs is in termen van l-bogen).

1969: Casse lost (i) op voor $m=3,4$ en q even.

1982: Casse en Glynn bepalen alle $(q+1)$-bogen voor q even en $m=3$.

1984: Casse en Glynn bepalen alle $(q+1)$-bogen voor q even en $m=4$.

1987: Thas verbetert voor q oneven de resultaten van Segre uit 1967.

1988: Voor q even lossen Bruen, Thas en Blokhuis (i), (ii), (iii) op voor de meeste waarden van de parameters.

1990-1991: Voloch verbetert de meeste voorgaande resultaten ingeval q geen kwadraat is.

1993: Storme en Thas verbeteren voor q even de resultaten van Bruen, Thas en Blokhuis.

1995: Voor q oneven verbeteren Hirschfeld en Korchmáros de meeste voorgaande resultaten.

Een lineaire code C over GF(q) wordt een *veralgemeende Reed-Solomon code* (*generalized Reed-Solomon* (GRS) *code*) genoemd als hij voortgebracht wordt door een matrix van de gedaante

$$G = [g_{ij}] \text{ met } g_{ij} = \nu_j t_j^{i-1}, 1 \leq i \leq k, 1 \leq j \leq n.$$

Hier zijn $t_1, t_2, \cdots, t_n$ verschillende elementen van GF(q); $\nu_1, \nu_2, \cdots, \nu_n$ zijn (niet noodzakelijk verschillende) elementen van GF(q) $- \{0\}$. In deze context definiëren wij $0^0 = 1$. Voegen wij een extra kolom aan G toe van de gedaante $(0 \;\; 0 \;\; \cdots \;\; \nu)'$, met $\nu \neq 0$, dan wordt de corresponderende lineaire code een *veralgemeende dubbel uitgebreide Reed-Solomon code (generalized doubly extended Reed-Solomon* (GDRS) *code)* genoemd. GRS codes en GDRS codes zijn lineaire M.D.S. codes. Uit de vorm van de voortbrengende matrices volgt onmiddellijk dat de n-boog die met de duale code correspondeert een deelverzameling is van een rationale normaalkromme; ook toont men aan dat de n-boog die met C zelf correspondeert eveneens deelverzameling is van een rationale normaalkromme. Het is een combinatie van twee dergelijke codes (over GF(2^8)) die gebruikt wordt voor de foutverbetering bij compact discspelers.

11.4 De Gilbert-Varshamov grens

De volgende grenzen werden onafhankelijk ontdekt door Gilbert (1952) en Varshamov (1957).

Stelling 11.4.1
Is q een priemmacht, dan bestaat een lineaire $[n, k, d]$-code over GF(q) *als voldaan is aan*

$$\sum_{i=0}^{d-2} (q-1)^i \begin{pmatrix} n-1 \\ i \end{pmatrix} < q^{n-k}. \tag{11.6}$$

Bijgevolg is

$A_q(n, d) \geq q^k$ *met k het grootste geheel getal waarvoor*

$$q^k < q^n / \left[\sum_{i=0}^{d-2} (q-1)^i \begin{pmatrix} n-1 \\ i \end{pmatrix} \right]. \tag{11.7}$$

Bewijs. Wij construeren een pariteit controlematrix H voor dergelijke code C. Voor de eerste r kolommen, met $r = n-k$, van H kiezen wij de kolommen van I_r; voor de $(r+1)$de kolom van H kiezen wij $(1\ 1\ 1\ \cdots\ 1\ 0\ 0\ \cdots\ 0)'$, waarbij er juist $d-1$ 1's voorkomen. Voor zulke H zal zeker rang $H = r$, en zullen d kolommen van H lineair afhankelijk zijn. Voor de $i$de kolom van H, met $i = r+2, r+3, \cdots$, kiezen wij nu een kolom die lineair onafhankelijk is van elke $d-2$ voorgaande kolommen. Hieraan is voldaan als wij voor de $i$de kolom niet $(0\ 0\ \cdots\ 0)'$ kiezen, noch een kolom evenredig, met evenredigheidsfactor niet nul, met een voorgaande kolom, noch een kolom die een lineaire combinatie is van twee voorgaande kolommen met beide scalairen verschillend van nul, $\cdots$, noch een kolom die een lineaire combinatie is van $d-2$ voorgaande kolommen met alle $d-2$ scalairen verschillend van nul. Het aantal uitgesloten kolommen is dus ten hoogste

$$N(i) = 1 + \begin{pmatrix} i-1 \\ 1 \end{pmatrix}(q-1) + \begin{pmatrix} i-1 \\ 2 \end{pmatrix}(q-1)^2 + \cdots + \begin{pmatrix} i-1 \\ d-2 \end{pmatrix}(q-1)^{d-2}$$

(merk op dat sommige van de lineaire combinaties een zelfde kolom zouden kunnen opleveren, zodat $N(i)$ inderdaad een bovengrens is voor het aantal uitgesloten kolommen). De $i$de kolom kan dus zeker zo gekozen worden indien $N(i) < |V(r,q)| = q^r$. Uit

$$N(r+2) < N(r+3) < \cdots < N(n) < q^r = q^{n-k}$$

volgt nu onmiddellijk dat wij tot en met de $n$de kolom op dergelijke manier kunnen kiezen. Voor zulke $r \times n$-matrix H is rang $H = r$, zijn elke $d-1$ kolommen lineair onafhankelijk en bestaat een stel van d lineair afhankelijke kolommen. Bijgevolg is H pariteit controlematrix van een lineaire $[n,k,d]$-code over GF(q). □

Opmerking 11.4.2
In tegenstelling met de voorgaande paragrafen vinden wij hier een benedengrens voor $A_q(n,d)$.

Stelling 11.4.3
Voor elke $q \neq 1$ is voldaan aan

$$A_q(n,d) \geq q^n / \left[\sum_{i=0}^{d-1} (q-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \right]. \tag{11.8}$$

Bewijs. Zonder bewijs. □

Opmerking 11.4.4
De ongelijkheid (11.8) is algemener dan (11.7) wat q betreft, maar is voor priemmachten q veel zwakker dan (11.7).

11.5 De Plotkin grens

In deze paragraaf zullen wij het over grenzen hebben die door Plotkin in 1960 werden afgeleid voor binaire codes.

Lemma 11.5.1
$A_q(n,d) \leq A_q(n,d')$ *voor* $n \geq d \geq d' > 0$.

Bewijs. Beschouw een q-aire (n,M,d)-code C, en neem twee codewoorden $\bar{x}, \bar{y}$ waarvoor $d(\bar{x},\bar{y}) = d$. Wijzig nu in $\bar{x}$ $d-d'$ posities op een zodanige manier dat voor het nieuwe woord $\bar{x}'$ voldaan is aan $d(\bar{x}',\bar{y}) = d'$. Voor elke $\bar{z} \in C - \{\bar{x},\bar{y}\}$ is dan voldaan aan $d(\bar{x}',\bar{z}) \geq d'$. Bijgevolg is $C' = (C - \{\bar{x}\}) \cup \{\bar{x}'\}$ een q-aire (n,M,d')-code, zodat $A_q(n,d') \geq A_q(n,d)$. □

Stelling 11.5.2
$A_2(n,d) \leq 2A_2(n-1,d)$.

Bewijs. Beschouw een binaire (n,M,d)-code C. Wij verdelen de codewoorden nu in twee klassen: de klasse C' van de codewoorden met een 0 in de eerste positie, de klasse C'' van de codewoorden met een 1 in de eerste positie. Laten wij de eerste coördinaat weg, dan is elke klasse een binaire code met lengte $n-1$ en minimum afstand ten minste d. Er geldt $|C'| \geq M/2$ of $|C''| \geq M/2$, bijvoorbeeld $|C'| \geq M/2$. Bijgevolg is C' een binaire $(n-1,M',d')$-code met $M' \geq M/2$ en $d' \geq d$. Uit het bewijs van Lemma 11.5.1 volgt nu dat een binaire $(n-1,M',d)$-code bestaat. Zo is dus $A_2(n-1,d) \geq A_2(n,d)/2$. □

Stelling 11.5.3 (De Plotkin grenzen (1960))
(i) Is $2d > n$, *dan geldt*

$$A_2(n,d) \leq 2\left[\frac{d}{2d-n}\right], \tag{11.9}$$

en

$$A_2(2d,d) \leq 4d. \tag{11.10}$$

(ii) Is d *oneven en* $2d+1 > n$, *dan geldt*

$$A_2(n,d) \leq 2\left[\frac{d+1}{2d+1-n}\right], \tag{11.11}$$

en

$$A_2(2d+1,d) \leq 4d+4. \tag{11.12}$$

(Hierbij is $[x]$ *het grootste geheel getal kleiner dan of gelijk aan* x*).*

Bewijs. Beschouw een binaire (n,M,d)-code C, met $2d > n$. Stel

$$S = \sum_{\bar{x}\in C}\sum_{\bar{y}\in C} d(\bar{x},\bar{y}).$$

Aangezien $d(\bar{x}, \bar{y}) \geq d$ voor alle $\bar{x} \neq \bar{y}$ en $d(\bar{x}, \bar{x}) = 0$ voor alle $\bar{x}$, is

$$S \geq M(M-1)d. \tag{11.13}$$

Beschouw nu de $M \times n$-matrix A met als rijen de codewoorden. Onderstel dat de $i$de kolom van A juist m_i nullen bevat en $M - m_i$ eentjes. Deze kolom draagt dan $2m_i(M - m_i)$ bij tot S. Bijgevolg is

$$S = \sum_{i=1}^{n} 2m_i(M - m_i). \tag{11.14}$$

Beschouw nu $y = x(M - x), x \in \mathbb{N}$. Voor M even wordt de grootste waarde voor y bereikt als $x = M/2$, namelijk $y = M^2/4$; voor M oneven wordt de grootste waarde voor y bereikt als $x = (M-1)/2$ of $x = (M+1)/2$, namelijk $y = (M^2-1)/4$.

Voor M even volgt dan uit (11.14) dat

$$S \leq nM^2/2, \tag{11.15}$$

zodat wegens (11.13) en (11.15)

$$M(M-1)d \leq S \leq nM^2/2.$$

Bijgevolg is

$$\frac{M}{2} \leq \frac{d}{2d-n},$$

zodat

$$\left[\frac{M}{2}\right] \leq \left[\frac{d}{2d-n}\right].$$

Omdat M even is, geldt $\frac{M}{2} = \left[\frac{M}{2}\right]$, zodat

$$\frac{M}{2} \leq \left[\frac{d}{2d-n}\right],$$

of

$$M \leq 2\left[\frac{d}{2d-n}\right].$$

Voor M oneven volgt uit (11.14) dat

$$S \leq n(M^2-1)/2, \tag{11.16}$$

zodat wegens (11.13) en (11.16)

$$M(M-1)d \leq S \leq n(M^2-1)/2.$$

Bijgevolg is

$$M \leq \frac{n}{2d-n} = \frac{2d}{2d-n} - 1. \tag{11.17}$$

Onderstel dat $x \in \mathbb{R}^+$, met $x = r + \varepsilon$, $r \in \mathbb{N}$ en $0 \leq \varepsilon < 1$; dus $[x] = r$. Dan is $[2x] = [2r + 2\varepsilon] \in \{2r, 2r+1\} = \{2[x], 2[x]+1\}$.

Uit (11.17) volgt dan dat

$$M \leq \left[\frac{2d}{2d-n}\right] - 1 \leq \left(2\left[\frac{d}{2d-n}\right] + 1\right) - 1 = 2\left[\frac{d}{2d-n}\right].$$

Voor elke binaire (n, M, d)-code is dus

$$M \leq 2\left[\frac{d}{2d-n}\right],$$

m.a.w.

$$A_2(n,d) \leq 2\left[\frac{d}{2d-n}\right]. \tag{11.18}$$

Wegens Stelling 11.5.2 is $A_2(2d,d) \leq 2A_2(2d-1,d)$. Uit (11.18) volgt dan dat

$$A_2(2d,d) \leq 4\left[\frac{d}{2d-(2d-1)}\right] = 4d. \tag{11.19}$$

Onderstel nu dat d oneven is en $2d+1 > n$. Wegens Stelling 2.2.10 is $A_2(n,d) = A_2(n+1,d+1)$. Uit (11.18) volgt dan

$$A_2(n,d) = A_2(n+1,d+1) \leq 2\left[\frac{d+1}{2d+1-n}\right]. \tag{11.20}$$

Uit (11.19) volgt

$$A_2(2d+1,d) = A_2(2d+2,d+1) \leq 4(d+1).$$

□

Opmerking 11.5.4
De ongelijkheden (11.9) en (11.10) gelden voor even en oneven d. Voor d oneven echter is (11.11) beter.

Een *Hadamard matrix* is een $n \times n$-matrix over $\mathbb{Q}$ waarvan alle elementen $+1$ of -1 zijn, en waarvoor

$$HH' = nI.$$

Is $H = [h_{ij}]$ een $n \times n$-matrix over $\mathbb{R}$ waarvoor $|h_{ij}| \leq 1$, dan toont men aan dat $|\det H| \leq n^{n/2}$. Hadamard bewees in 1893 dat $|\det H| = n^{n/2}$ a.s.a. H een Hadamard matrix is. Is H een Hadamard matrix van de orde $n \notin \{1, 2\}$, dan bewijst men dat n een viervoud is. Men vermoedt dat voor elke $n = 4t$, $t \in \mathbb{N}_0$, er een Hadamard matrix van de orde n bestaat; het eerste open geval is $n = 668$. Veel oneindige klassen van Hadamard matrices zijn gekend.

Beschouw een $m \times m$-matrix $A = [a_{ij}]$ over het veld K en beschouw een $n \times n$-matrix $B = [b_{ij}]$ over het veld K. Het Kronecker product van de matrix A met de matrix B is dan de volgende matrix $A \times B$ van de orde mn over K:

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}.$$

Zijn A en B Hadamard matrices, dan toont men aan dat het Kronecker product $A \times B$ eveneens een Hadamard matrix is.

Voorbeeld 11.5.5
De matrix

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

is een Hadamard matrix. Bijgevolg is

$$H \times H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

een Hadamard matrix. Bijgevolg is ook

$$H \times (H \times H) = \left[\begin{array}{rrrrrrrr} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]$$

een Hadamard matrix. Zo voortgaande ziet men dat er voor elke $k \in \mathbb{N}$ er een Hadamard matrix van de orde 2^k bestaat (merk op dat [1] eveneens een Hadamard matrix is).

Gebruik makende van Hadamard matrices construeert men codes waarvoor de gelijkheid geldt in (11.9)–(11.12).

Stelling 11.5.6 (Levenstein (1961))
Bestaat er een Hadamard matrix voor elke $m = 4t, t \in \mathbb{N}_0$, dan geldt voor elke toelaatbare n en d de gelijkheid in de Plotkin grenzen, waarbij voor d oneven de tweede grens uit Stelling 11.5.3 *genomen wordt.*

Voorbeeld 11.5.7
Beschouw een Hadamard matrix H van de orde $4t, t \in \mathbb{N}_0$. Beschouw nu de matrix

$$\left[\begin{array}{r} H \\ -H \end{array}\right]$$

en vervang overal –1 door 0. Dan toont men gemakkelijk aan dat de rijen van de nieuwe matrix de codewoorden zijn van een binaire $(4t, 8t, 2t)$-code. Bijgevolg is $A_2(4t, 2t) = 8t$.

Uit Voorbeeld 11.5.5 volgt dus dat er een binaire $(2^k, 2^{k+1}, 2^{k-1})$-code bestaat, $k \geq 2$. Voor $k = 5$ wordt dit een binaire $(32, 64, 16)$-code C. Het is deze code C die gebruikt werd voor de foutverbetering bij de transmissie van foto's van Mars door de Mariners (zie 1.4(i)).

Hadamard matrices zijn ook zeer belangrijk voor de constructie van designs, en omgekeerd kan men uit het bestaan van bepaalde designs het bestaan van zekere Hadamard matrices afleiden.

Stelling 11.5.8
Een Hadamard matrix van de orde $4t$, met $t > 1$, bestaat a.s.a. een (symmetrische) $2 - (4t - 1, 2t - 1, t - 1)$ design bestaat; een design met dergelijke parameters noemt men een Hadamard 2-design. Een Hadamard matrix van de orde $4t$, met $t > 1$, bestaat a.s.a. een $3 - (4t, 2t, t - 1)$ design bestaat; een design met dergelijke parameters noemt men een Hadamard 3-design.

Bewijs. Zonder bewijs. □

Voorbeeld 11.5.9
Aangezien Hadamard matrices van de orde $2^k, k \geq 3$, bestaan, bestaan ook (symmetrische) $2-(2^k-1, 2^{k-1}-1, 2^{k-2}-1)$ designs en $3-(2^k, 2^{k-1}, 2^{k-2}-1)$ designs. Symmetrische $2-(2^k-1, 2^{k-1}-1, 2^{k-2}-1)$ designs ontmoetten wij reeds in Voorbeeld 8.2.1 (ii) (stel hierin $q=2$).

11.6 Slotbemerking

Een andere zeer belangrijke grens is de *lineaire programmeergrens (linear programming bound)*.

Hoofdstuk 12

Een 2-foutverbeterende decimale code en een inleiding tot de BCH codes

12.1 Inleiding

In 1.4 (ii) zagen we de ISBN code, die een één-foutdetecterende code van lengte 10 over GF(11) is; wij herinneren eraan dat de eerste 9 symbolen van elk codewoord hier tot $\{0, 1, \cdots, 9\}$ behoren. Verder construeerden wij in 5.4 een één-foutverbeterende decimale code van lengte 10, als deelverzameling van een lineaire code over GF(11). Hier zullen wij een 2-foutverbeterende decimale code van lengte 10 construeren, opnieuw als deelverzameling van een lineaire code over GF(11). Ook zullen wij een efficiënt decodeeralgoritme bepalen.

Deze constructie van de lineaire code over GF(11) zullen wij daarna uitbreiden tot de constructie van een lineaire $\left[\frac{d-1}{2}\right]$-foutverbeterende code van lengte n over GF(q), waarbij d en n willekeurige natuurlijke getallen zijn waarvoor $3 \leq d \leq n < q$. Deze codes zijn bijzondere BCH codes (BCH codes werden onafhankelijk ontdekt door Hocquenghem (1959) en door Bose en Ray-Chaudhuri (1960)) en worden Reed-Solomon codes genoemd (zie 11.3).

Het decoderen van deze codes is afhankelijk van het oplossen van een zeker stelsel niet-lineaire vergelijkingen. Zulk stelsel vergelijkingen werd het eerst opgelost door Ramanujan in 1912, en het is deze oplossingsmethode die we zullen volgen. Hier hebben wij tevens een schitterend tegenvoorbeeld op Hardy's visie (1940) dat getallentheorie geen enkele nuttige toepassing zou hebben. Het is juist een resultaat van Hardy's grote protégé, de geniale Ramanujan, dat wij hier zullen toepassen op codes die effectief in de practijk gebruikt worden.

12.2 Een 2-foutverbeterende BCH code over GF(11)

Beschouw de lineaire $[10, 6]$-code C over GF(11) $= \{0, 1, 2, \cdots, 10\}$ bepaald door de pariteit controlematrix

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 10 \\ 1 & 2^2 & \cdots & 10^2 \\ 1 & 2^3 & \cdots & 10^3 \end{bmatrix}.$$

Merk op dat C een lineaire deelruimte is van de lineaire $[10, 8]$-code over GF(11) uit 5.4. Noem D de decimale code die uit C ontstaat door alle codewoorden weg te laten die het symbool 10 bevatten:

$$D = \{x_1 x_2 \cdots x_{10} \in (F_{10})^{10} \parallel \textstyle\sum_{i=1}^{10} x_i = \sum_{i=1}^{10} i x_i = \sum_{i=1}^{10} i^2 x_i = \sum_{i=1}^{10} i^3 x_i = 0 \text{ over GF(11)}\}$$

met $F_{10} = \{0, 1, 2, \cdots, 9\}$.

Uit de theorie van de Vandermonde matrices volgt onmiddellijk dat elke vier kolommen van H lineair onafhankelijk zijn over GF(11). Bijgevolg is $d = 5 = n - k + 1$, zodat wegens 11.3 C een lineaire M.D.S. code is. De code C is dus 2-foutverbeterend. Vanzelfsprekend is $d(D) \geq d(C) = 5$. Steunend op exclusie-inclusie principe weten wij dat $|D| = 11^6 - \binom{10}{1}11^5 + \binom{10}{2}11^4 - \binom{10}{3}11^3 + \binom{10}{4}11^2 - \binom{10}{5}11 + \binom{10}{6} = 683.024$. Moest $d(D) \geq 6$, dan zou wegens de Singleton grens $|D| \leq 10^{10-6+1} = 100.000$, een strijdigheid. Dus is $d(D) = 5$. Merk eveneens op dat D geen M.D.S. code is.

We zullen nu een syndroom decodeerschema opstellen dat alle dubbele en enkele fouten zal verbeteren wat betreft de code C. Onderstel dat codewoord $\bar{x} = x_1 x_2 \cdots x_{10}$ verzonden wordt, en dat het woord $\bar{y} = y_1 y_2 \cdots y_{10}$ ontvangen wordt. Wij berekenen nu het syndroom van de vector $\bar{y}$:

$$(S_1, S_2, S_3, S_4) = S(\bar{y}) = \bar{y}H' = (\sum_{i=1}^{10} y_i, \sum_{i=1}^{10} i y_i, \sum_{i=1}^{10} i^2 y_i, \sum_{i=1}^{10} i^3 y_i).$$

Onderstel nu dat er twee fouten in de posities i en j opgetreden zijn, met resp. grootten a en b. Dus is $y_i = x_i + a, y_j = x_j + b, i \neq j$, en $y_l = x_l$ voor $l \neq i, j$. Bijgevolg is

$$S_1 = a + b, \tag{12.1}$$

$$S_2 = ai + bj, \tag{12.2}$$

$$S_3 = ai^2 + bj^2, \tag{12.3}$$

$$S_4 = ai^3 + bj^3. \tag{12.4}$$

Wij moeten nu het stelsel (12.1)-(12.4) oplossen naar de onbekenden a, b, i, j. Wij elimineren nu a, b, j als volgt:

$$(i \times (12.1)) - (12.2) \text{ geeft } iS_1 - S_2 = b(i - j), \tag{12.5}$$

$$(i \times (12.2)) - (12.3) \text{ geeft } iS_2 - S_3 = bj(i - j), \tag{12.6}$$

$$(i \times (12.3)) - (12.4) \text{ geeft } iS_3 - S_4 = bj^2(i - j). \tag{12.7}$$

Uit (12.5) , (12.6), (12.7) volgt dat

$$(iS_2 - S_3)^2 = (iS_1 - S_2)(iS_3 - S_4),$$

zodat

$$(S_2^2 - S_1S_3)i^2 + (S_1S_4 - S_2S_3)i + S_3^2 - S_2S_4 = 0. \tag{12.8}$$

Elimineren wij a, b, i op analoge manier, dan bekomen wij

$$(S_2^2 - S_1S_3)j^2 + (S_1S_4 - S_2S_3)j + S_3^2 - S_2S_4 = 0. \tag{12.9}$$

Bijgevolg zijn i en j de wortels van de vierkantsvergelijking

$$(S_2^2 - S_1S_3)X^2 + (S_1S_4 - S_2S_3)X + S_3^2 - S_2S_4 = 0. \tag{12.10}$$

Stel

$$P = S_2^2 - S_1S_3, Q = S_1S_4 - S_2S_3, R = S_3^2 - S_2S_4.$$

Moest $P = 0$, dan zou $(ai + bj)^2 - (a + b)(ai^2 + bj^2) = -ab(i - j)^2 = 0$, een strijdigheid; moest $R = 0$, dan zou $(ai^2+bj^2)^2-(ai+bj)(ai^3+bj^3) = -abij(i-j)^2 = 0$, een strijdigheid. Bijgevolg is $P \neq 0 \neq R$. Zijn er juist twee fouten, dan heeft de vergelijking (12.10) juist twee verschillende oplossingen zodat $Q^2 - 4PR$ een kwadraat verschillend van nul is.

Onderstel nu dat $P \neq 0 \neq R$ en dat $Q^2 - 4PR$ een kwadraat verschillend van nul is. Zijn i en j de oplossingen van (12.10) en worden a en b bepaald uit (12.1) en (12.2), dan tonen wij nog juist aan dat $i \neq 0 \neq j$, dat $a \neq 0 \neq b$ en dat ook voldaan is aan (12.3) en (12.4). Moest $i = 0$ of $j = 0$, dan zou $S_3^2 - S_2S_4 = R = 0$, een strijdigheid. Onderstel nu dat $a = 0$. Dan is $S_2 = S_1j$, zodat $S_1 \neq 0$ (anders zou $P = 0$). Uit $(12.9)\cdot S_1^2$ volgt dan dat

$$(S_2^2 - S_1S_3)S_2^2 + (S_1S_4 - S_2S_3)S_2S_1 + (S_3^2 - S_2S_4)S_1^2 = 0,$$

m.a.w.

$$(S_2^2 - S_1S_3)^2 = 0,$$

zodat $P = 0$, een strijdigheid. Bijgevolg is $a \neq 0$, en analoog $b \neq 0$.
Stel nu

$$ai^2 + bj^2 = u,$$
$$ai^3 + bj^3 = v.$$

Dan zijn i en j eveneens de wortels van de vierkantsvergelijking

$$(S_2^2 - S_1u)X^2 + (S_1v - S_2u)X + u^2 - S_2v = 0. \tag{12.11}$$

Opnieuw is $S_2^2 - S_1u \neq 0 \neq u^2 - S_2v$. Uit (12.10) en (12.11) volgt dat voor een $l \in \mathrm{GF}(11) - \{0\}$ voldaan is aan

$$l(S_2^2 - S_1S_3) = S_2^2 - S_1u, \tag{12.12}$$

$$l(S_1S_4 - S_2S_3) = S_1v - S_2u, \tag{12.13}$$

$$l(S_3^2 - S_2S_4) = u^2 - S_2v. \tag{12.14}$$

Eliminatie van u uit (12.12) en (12.13) geeft

$$S_1^2v = l(S_1^2S_4 - S_2^3) + S_2^3,$$

terwijl na eliminatie van u en v uit (12.12), (12.13), (12.14)

$$l(S_3^2 - S_2S_4)S_1^2 = [S_2^2 - l(S_2^2 - S_1S_3)]^2 - S_2[l(S_1^2S_4 - S_2^3) + S_2^3].$$

Hieruit volgt nu gemakkelijk dat $l = 1$. Uit (12.12), (12.13) en (12.14) halen wij nu $u = S_3$ en $v = S_4$. Bijgevolg is voor i, j, a, b ook voldaan aan (12.3) en (12.4).

Onderstel vervolgens dat er juist één fout opgetreden is, met grootte a in positie i. Dus is $y_i = x_i + a$ en $y_s = x_s$ voor $s \neq i$. Bijgevolg is

$$S_1 = a, \tag{12.15}$$

$$S_2 = ai, \tag{12.16}$$

$$S_3 = ai^2, \tag{12.17}$$

$$S_4 = ai^3. \tag{12.18}$$

Hier is dus $S_1 \neq 0$, $S_2 \neq 0$, $S_3 \neq 0$, $S_4 \neq 0$, $P = S_2^2 - S_1S_3 = 0$, $Q = S_1S_4 - S_2S_3 = 0$, $R = S_3^2 - S_2S_4 = 0$.

Bereken het syndroom, en onderstel dat $P = Q = R = 0$, $S_1S_2S_3S_4 \neq 0$. Uit (12.15) en (12.16) halen wij dan a en i (merk op dat $a \neq 0 \neq i$). Aangezien $ai^2 = S_1S_2^2/S_1^2 = S_3$ en $ai^3 = S_1S_2^3/S_1^3 = S_3^2/S_2 = S_4$, is voor zulke a en i ook aan (12.17) en (12.18) voldaan.

Het decodeeralgoritme ziet er dus als volgt uit.

(i) Voor de ontvangen vector $\bar{y}$ berekenen wij het syndroom $S(\bar{y}) = \bar{y}H' = (S_1, S_2, S_3, S_4)$.

(ii) Is $S(\bar{y}) = \bar{0}$, dan is $\bar{y}$ een codewoord en onderstellen wij dat $\bar{y}$ verzonden werd.

(iii) Is $S(\bar{y}) \neq \bar{0}$, is $P = Q = R = 0$ en is $S_1S_2S_3S_4 \neq 0$, dan onderstellen wij dat er juist één fout is met grootte S_1 in positie S_2/S_1.

(iv) Is $S(\bar{y}) \neq \bar{0}$, is $P.R \neq 0$ en is $Q^2 - 4PR$ een kwadraat verschillend van nul, dan onderstellen wij dat er juist twee fouten zijn, in de posities i en j en met resp. grootten a en b waarbij

$$i = \frac{-Q + \sqrt{Q^2 - 4PR}}{2P},$$

$$j = \frac{-Q - \sqrt{Q^2 - 4PR}}{2P},$$

$$a = (jS_1 - S_2)/(j - i),$$

$$b = S_1 - a.$$

Met $\sqrt{Q^2 - 4PR}$ bedoelen wij een willekeurig gekozen element waarvan het kwadraat $Q^2 - 4PR$ is.

(v) In alle andere gevallen weten wij dat er ten minste drie fouten gemaakt werden.

Wat de decimale code D betreft kan eveneens de voorgaande decodeerprocedure gebruikt worden, met het enig verschil dat als in (iii) of (iv) de verbeterde vector een 10 bevat wij eveneens weten dat er ten minste drie fouten gemaakt werden (hierbij wordt verondersteld dat de ontvangen vector nooit het symbool 10 kan bevatten).

Tabellen die wij bij het decoderen nodig hebben zijn

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

en

x	1	3	4	5	9
$\sqrt{x}$	1	5	2	4	3

.

12.3 Een klasse BCH codes

Wij zullen nu de code uit 12.2 veralgemenen tot een lineaire code met lengte n en minimum afstand d over GF(q), met

$$3 \leq d \leq n \leq q-1.$$

Deze codes zijn bijzondere BCH *codes* die *Reed-Solomon codes* (zie 11.3) worden genoemd, maar de decodeerprocedure die wij zullen opstellen draagt de essentiële ingrediënten van de decodeerprocedure voor algemene BCH codes.

Beschouw de lineaire code C over GF(q) met pariteit controlematrix

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ t_1 & t_2 & \cdots & t_n \\ t_1^2 & t_2^2 & \cdots & t_n^2 \\ \vdots & \vdots & & \vdots \\ t_1^{d-2} & t_2^{d-2} & \cdots & t_n^{d-2} \end{bmatrix},$$

met $3 \leq d \leq n \leq q-1$ en met $t_1, t_2, \cdots, t_n$ verschillende elementen van GF(q) $-\{0\}$. M.a.w.

$$C = \{x_1 x_2 \cdots x_n \in V(n,q) \parallel \sum_{i=1}^{n} t_i^j x_i = 0 \text{ voor } j = 0, 1, \cdots, d-2\}.$$

Elke $d-1$ kolommen van de $(d-1) \times n$-matrix H zijn lineair onafhankelijk zodat $d(C) = d$. Bijgevolg is C een lineaire (n, q^{n-d+1}, d)-code over GF(q). Uit 11.3 volgt dat C een lineaire M.D.S. code is. Dus hebben wij volgende stelling.

Stelling 12.3.1
Is $3 \leq d \leq n \leq q-1$, *met* q *een priemmacht, dan is*

$$A_q(n,d) = q^{n-d+1}.$$

(*Deze stelling is eveneens geldig voor* $d \in \{1,2\}$ of $n \in \{q, q+1\}$.)

Onderstel dat het codewoord $\bar{x} = x_1 x_2 \cdots x_n$ werd verzonden en dat de vector $\bar{y} = y_1 y_2 \cdots y_n$ wordt ontvangen, waarbij wij aannemen dat ten hoogste t fouten werden gemaakt met $d = 2t+1$ of $d = 2t+2$. Onderstel dat de fouten voorkomen in posities $s_1, s_2, \cdots, s_e$ met resp. grootten $m_1, m_2, \cdots, m_e$; wij stellen $t_{s_i} = X_i, i = 1, 2, \cdots, e$. Bereken nu het syndroom

$$S(\bar{y}) = \bar{y}H' = (S_1, S_2, \cdots, S_{d-1}),$$

m.a.w.

$$S_j = \sum_{i=1}^{n} y_i t_i^{j-1} = \sum_{i=1}^{e} m_i X_i^{j-1},$$

met $j = 1, 2, \cdots, d-1$.

Om de fouten te vinden moeten wij dus volgend stelsel vergelijkingen naar de X_i en m_i oplossen:

$$\begin{aligned} S_1 &= m_1 + m_2 + \cdots + m_e, \\ S_2 &= m_1X_1 + m_2X_2 + \cdots + m_eX_e, \\ S_3 &= m_1X_1^2 + m_2X_2^2 + \cdots + m_eX_e^2, \\ &\vdots \\ S_{d-1} &= m_1X_1^{d-2} + m_2X_2^{d-2} + \cdots + m_eX_e^{d-2}. \end{aligned} \tag{12.19}$$

Dit is het stelsel vergelijkingen dat Ramanujan in 1912 beschouwde en hier zullen wij zijn oplossingsmethode volgen.

Beschouw volgend element van het veld $\mathrm{GF}(q)(\theta) \subset \mathrm{GF}(q)((\theta))$:

$$\phi(\theta) = \frac{m_1}{1 - X_1\theta} + \frac{m_2}{1 - X_2\theta} + \cdots + \frac{m_e}{1 - X_e\theta}. \tag{12.20}$$

Nu is

$$\frac{m_j}{1 - X_j\theta} = m_j(1 + X_j\theta + X_j^2\theta^2 + \cdots) \in \mathrm{GF}(q)((\theta)),$$

zodat

$$\begin{aligned} \phi(\theta) = (m_1 + m_2 + \cdots + m_e) + (m_1X_1 + m_2X_2 + \cdots + m_eX_e)\theta \\ +(m_1X_1^2 + m_2X_2^2 + \cdots + m_eX_e^2)\theta^2 + \cdots. \end{aligned}$$

Uit (12.19) volgt dan

$$\phi(\theta) = S_1 + S_2\theta + S_3\theta^2 + \cdots + S_{d-1}\theta^{d-2} + \cdots \tag{12.21}$$

Door in (12.20) alles op een gemeenschappelijke noemer te plaatsen vinden wij

$$\phi(\theta) = \frac{A_1 + A_2\theta + A_3\theta^2 + \cdots + A_e\theta^{e-1}}{1 + B_1\theta + B_2\theta^2 + \cdots + B_e\theta^e}. \tag{12.22}$$

Bijgevolg is

$$\begin{aligned} &(S_1 + S_2\theta + S_3\theta^2 + \cdots + S_{d-1}\theta^{d-2} + \cdots)(1 + B_1\theta + B_2\theta^2 + \cdots + B_e\theta^e) \\ &= A_1 + A_2\theta + A_3\theta^2 + \cdots + A_e\theta^{e-1}. \end{aligned} \tag{12.23}$$

Door gelijkstelling van de coëfficiënten van gelijke machten van θ in beide leden van (12.23) bekomen wij

$$\begin{cases} A_1 = S_1, \\ A_2 = S_2 + S_1B_1, \\ A_3 = S_3 + S_2B_1 + S_1B_2, \\ \vdots \\ A_e = S_e + S_{e-1}B_1 + S_{e-2}B_2 + \cdots + S_1B_{e-1}, \end{cases} \tag{12.24}$$

$$\begin{cases} 0 = S_{e+1} + S_eB_1 + S_{e-1}B_2 + \cdots + S_1B_e, \\ 0 = S_{e+2} + S_{e+1}B_1 + S_eB_2 + \cdots + S_2B_e, \\ \vdots \\ 0 = S_{2e} + S_{2e-1}B_1 + S_{2e-2}B_2 + \cdots + S_eB_e. \end{cases} \tag{12.25}$$

Er geldt

$$\sum(t) = \begin{bmatrix} S_1 & S_2 & \cdots & S_t \\ S_2 & S_3 & \cdots & S_{t+1} \\ \vdots & \vdots & & \vdots \\ S_t & S_{t+1} & \cdots & S_{2t-1} \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_t \\ \vdots & \vdots & & \vdots \\ X_1^{t-1} & X_2^{t-1} & \cdots & X_t^{t-1} \end{bmatrix} \begin{bmatrix} m_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & m_2 & & \vdots & \vdots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & & \cdots & m_e & \cdots & \cdots & \cdots \\ 0 & & \cdots & \cdots & 0 & \cdots & \cdots \\ \vdots & & & \cdots & \cdots & \ddots & \cdots \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{bmatrix} 1 & X_1 & \cdots & X_1^{t-1} \\ 1 & X_2 & \cdots & X_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & X_t & \cdots & X_t^{t-1} \end{bmatrix},$$

met $X_{e+1}, X_{e+2}, \cdots, X_t$ verschillende elementen van $\mathrm{GF}(q) - \{X_1, X_2, \cdots, X_e\}$.
Bijgevolg is

$$\text{rang } \sum(t) = e.$$

De rang van de matrix $\sum(t)$ bepaalt dus het aantal fouten.

Nadat e bepaald werd beschouwen wij het stelsel (12.25) in $B_1, B_2, \cdots, B_e$. De matrix van dit stelsel lineaire vergelijkingen is

$$\sum(e) = \begin{bmatrix} S_1 & S_2 & \cdots & S_e \\ S_2 & S_3 & \cdots & S_{e+1} \\ \vdots & \vdots & & \vdots \\ S_e & S_{e+1} & \cdots & S_{2e-1} \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_e \\ \vdots & \vdots & & \vdots \\ X_1^{e-1} & X_2^{e-1} & \cdots & X_e^{e-1} \end{bmatrix} \begin{bmatrix} m_1 & 0 & \cdots & 0 \\ 0 & m_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ & & & 0 \\ 0 & 0 & \cdots 0 & m_e \end{bmatrix} \begin{bmatrix} 1 & X_1 & \cdots & X_1^{e-1} \\ 1 & X_2 & \cdots & X_2^{e-1} \\ \vdots & \vdots & & \vdots \\ 1 & X_e & \cdots & X_e^{e-1} \end{bmatrix}.$$

Bijgevolg is rang $\sum(e) = e$. Het stelsel (12.25) heeft dus juist één oplossing in $B_1, B_2, \cdots, B_e$. Daarna halen wij $A_1, A_2, \cdots, A_e$ uit stelsel (12.24). Vervolgens splitsen wij de rationale functie (12.22) in partieelbreuken:

$$\phi(\theta) = \frac{p_1}{1 - q_1\theta} + \frac{p_2}{1 - q_2\theta} + \cdots + \frac{p_e}{1 - q_e\theta}. \tag{12.26}$$

Vergelijken wij (12.20) met (12.26), dan zien wij dat

$$m_1 = p_1, m_2 = p_2, \cdots, m_e = p_e,$$

$$t_{s_1} = X_1 = q_1, t_{s_2} = X_2 = q_2, \cdots, t_{s_e} = X_e = q_e.$$

De polynoom $\sigma(\theta) = 1 + B_1\theta + B_2\theta^2 + \cdots + B_e\theta^e$ wordt de *foutplaatsbepalende polynoom (error-locator polynomial)* genoemd. De nulpunten van deze polynoom bepalen de posities waar de fouten voorkomen; het aantal verschillende nulpunten bedraagt e. De polynoom $\omega(\theta) = A_1 + A_2\theta + \cdots + A_e\theta^{e-1}$ noemt men de *foutevaluerende polynoom (error-evaluator polynomial)*. Eens de elementen $X_1, X_2, \cdots, X_e$ bepaald zijn, gebruikt men $\omega(\theta)$ om de grootten van de fouten te bepalen.
Merk op dat

$$m_j = \frac{\omega(X_j^{-1})}{\Pi_{i=1, i\neq j}^{e}(1 - X_i X_j^{-1})}, j = 1, 2, \cdots, e. \tag{12.27}$$

Onderstel dat $\bar{x} = x_1 x_2 \cdots x_n \in C$ verzonden werd, en dat $\bar{y} = y_1 y_2 \cdots y_n$, met $\bar{x} \neq \bar{y}$, ontvangen werd. Wij maken geen onderstellingen betreffende het aantal fouten. Bereken dan $S_1, S_2, \cdots, S_{d-1}$, en noem e de rang van de matrix $\sum(t)$; is de matrix $\sum(e)$ singulier, dan besluiten wij dat er meer dan t fouten zijn. Onderstel nu dat $\sum(e)$ niet-singulier is. Uit de stelsels (12.24) en (12.25) halen wij nu $A_1, A_2, \cdots, A_e, B_1, B_2, \cdots, B_e$. Heeft de polynoom $\sigma(\theta)$ geen e verschillende nulpunten, dan besluiten wij dat er meer dan t fouten zijn; heeft $\sigma(\theta)$ e verschillende nulpunten, maar zijn niet alle nulpunten van de gedaante t_j^{-1}, dan zijn er eveneens meer dan t fouten. Onderstel nu dat $\sigma(\theta)$ juist e verschillende nulpunten $X_1^{-1} = t_{s_1}^{-1}, X_2^{-1} = t_{s_2}^{-1}, \cdots, X_e^{-1} = t_{s_e}^{-1}$ heeft. Wij berekenen dan

$$m_j = \frac{\omega(t_{s_j}^{-1})}{\Pi_{i=1, i\neq j}^{e}(1 - t_{s_i} t_{s_j}^{-1})}. \tag{12.28}$$

Is er voor $X_1, X_2, \cdots, X_e, m_1, m_2, \cdots, m_e$ niet voldaan aan alle vergelijkingen van (12.19), dan zijn er meer dan t fouten. Onderstel nu dat voor $X_1, X_2, \cdots, X_e, m_1, m_2, \cdots, m_e$ voldaan is aan alle vergelijkingen van (12.19). In zulk geval nemen wij aan dat er juist e fouten zijn in de posities $s_1, s_2, \cdots, s_e$ en met resp. grootten $m_1, m_2, \cdots, m_e$. In het ander geval weten wij dat er meer dan t fouten zijn.

Het decodeeralgoritme ziet er dus als volgt uit.

(i) Voor de ontvangen vector $\bar{y}$ berekenen wij het syndroom $S(\bar{y}) = \bar{y}H' = (S_1, S_2, \cdots, S_{d-1})$.

(ii) Is $S(\bar{y}) = \bar{0}$, dan is $\bar{y}$ een codewoord en onderstellen wij dat $\bar{y}$ verzonden werd.

(iii) Bereken de rang e van de matrix $\sum(t)$.

(iv) Is $\sum(e)$ singulier, dan zijn er meer dan t fouten.

(v) Onderstel nu dat $\sum(e)$ niet-singulier is. Uit de stelsels (12.24) en (12.25) berekenen wij $A_1, A_2, \cdots, A_e, B_1, B_2, \cdots, B_e$, zodat de polynomen $\omega(\theta)$ en $\sigma(\theta)$ nu gekend zijn.

(vi) Heeft de polynoom $\sigma(\theta)$ geen e verschillende nulpunten, dan besluiten wij dat er meer dan t fouten zijn; heeft de polynoom $\sigma(\theta)$ juist e verschillende nulpunten, maar zijn niet alle nulpunten van de gedaante t_j^{-1}, dan zijn er eveneens meer dan t fouten.

(vii) Onderstel nu dat $\sigma(\theta)$ juist e verschillende nulpunten $X_1^{-1} = t_{s_1}^{-1}, X_2^{-1} = t_{s_2}^{-1}, \cdots, X_e^{-1} = t_{s_e}^{-1}$ heeft. Stel

$$m_j = \frac{\omega(t_{s_j}^{-1})}{\Pi_{i=1, i\neq j}^{e}(1 - t_{s_i} t_{s_j}^{-1})}, \text{ met } j = 1, 2, \cdots, e.$$

(viii) Is er voor de bekomen $X_1, X_2, \cdots, X_e, m_1, m_2, \cdots, m_e$ niet voldaan aan de laatste $d - 2e - 1$ vergelijkingen van (12.19), dan weten wij dat er meer dan t fouten zijn.

(ix) Onderstel ten slotte dat aan alle vergelijkingen van (12.19) voldaan is.
Dan nemen wij aan dat er juist e fouten zijn in de posities $s_1, s_2, \cdots, s_e$ en met resp. grootten $m_1, m_2, \cdots, m_e$.

Opmerking 12.3.2
Door de zeer bijzondere gedaante van de matrix $\sum(e)$ slaagden Berlekamp (1968) en Massey (1969) erin om het oplossen van het stelsel (12.25) zeer sterk te vereenvoudigen. Merk hierbij op dat het oplossen van het stelsel (12.25) de meest omslachtige berekeningen vergen in de gehele decodeerprocedure.

Bibliografie

[1] P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and Their Links*, Cambridge University Press, Cambridge, 1991.

[2] R. Hill, *A First Course in Coding Theory*, Oxford University Press, Oxford, 1986.

[3] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[4] D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, *Coding Theory*, Marcel Dekker, New York, 1991.

[5] J.A. Thas, *Inleiding tot de Theorie van de Designs*, Cursus licentie wiskunde.

[6] V.D. Tonchev, *Combinatorial Configurations*, Wiley, New York, 1988.

[7] J.H. van Lint, *Introduction to Coding Theory*, Springer, New York, 1982.

[8] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.