

# Experimentele nota's CODETHEORIE

Philippe CARA

6 juni 2011

# Inhoudsopgave

<b>1</b>	<b>Inleiding</b>	<b>1-1</b>
1.1	Codetheorie en cryptografie . . . . .	1-1
1.2	Enkele voorbeelden en definities . . . . .	1-1
1.3	Verbetering van fouten . . . . .	1-3
1.4	Een perfecte code . . . . .	1-6
<b>2</b>	<b>Eindige lichamen</b>	<b>2-1</b>
2.1	Algemeenheden . . . . .	2-1
2.2	Additieve structuur van een eindig lichaam . . . . .	2-3
2.3	Over het aantal irreduciebele veeltermen van graad $m$ in $\mathbb{F}[X]$ . . . . .	2-4
2.4	Multiplicatieve structuur van een eindig veld . . . . .	2-6
<b>3</b>	<b>Foutverbeterende codes</b>	<b>3-1</b>
3.1	Algemeen . . . . .	3-1
3.2	Lineaire codes . . . . .	3-3
3.3	Cyclische codes . . . . .	3-5
3.4	BCH codes . . . . .	3-7
<b>4</b>	<b>Perfekte codes</b>	<b>4-1</b>
4.1	Perfekte binaire codes die één fout verbeteren . . . . .	4-1
4.2	Perfekte binaire codes die drie fouten verbeteren . . . . .	4-2
4.3	De binaire Golay code . . . . .	4-3
4.4	Andere structuren in verband met de Golay code . . . . .	4-5
4.5	Uniciteit van de binaire Golay code . . . . .	4-8
4.6	De ternaire Golay code . . . . .	4-14
4.7	Zijn er nog perfecte codes? . . . . .	4-14
<b>5</b>	<b>Gewichtsverdelingen</b>	<b>5-1</b>
<b>6</b>	<b>Het hoofdprobleem van de lineaire codetheorie</b>	<b>6-1</b>
	<b>Bibliografie</b>	<b>6-5</b>

*INHOUDSOPGAVE*

2

**Index**

**6-6**

# Voorwoord

Dit zijn nota's die nuttig kunnen zijn bij het studeren van het vak "codetheorie". Dit vak wordt aan de VUB aangeboden als keuzevak voor 4 studiepunten (26u HOC). Er bestaat ook een variant van 5 SP. Voor het bijkomende studiepoint moet de student minstens één van de taken maken die in de tekst vermeld staan. Deze taak wordt afgegeven voor het laatste hoorcollege van de cursus.

De nota's zijn bondig opgesteld en bevatten enkel de hoofdideeën. Op het examen wordt vooral gepeild naar het begrip van de cursus en de wiskundige technieken die aan de basis liggen. Alle stellingen, lemma's, gevolgen, ... moeten gekend zijn, met bewijs. De bewijzen die niet in de cursus staan zou de gemiddelde licentiestudent wiskunde zelf moeten kunnen vinden of al in een andere cursus zijn tegengekomen. Er wordt dus verwacht dat deze bewijzen ook gekend zijn.

Philippe Cara  
6 juni 2011

# Hoofdstuk 1

## Inleiding

### 1.1 Codetheorie en cryptografie

Deze cursus handelt over *foutverbeterende codes*. Dit is een onderdeel van de tak van de wiskunde die *informatietheorie* wordt genoemd. Als je informatie wil overbrengen van een punt *A* naar een punt *B*, kunnen storingen optreden. Het gevolg hiervan is dat het bericht dat *B* ontvangt niet identiek hetzelfde is als dat door *A* verzonden. Om toch te verzekeren dat *B* de volledige informatie krijgt, gaat *A* een bericht maken dat meer bevat dan de gewone informatie. Deze bijkomende informatie zal *B* toelaten toch de volledige informatie te reconstrueren, ondanks de storingen.

Codetheorie mag niet verward worden met *cryptografie*. Dit is de kunst om in *A* de informatie zo te bewerken dat ze onleesbaar wordt voor iemand anders dan *B*. Cryptografie is dus een synoniem voor *geheimschrift* en de wiskundige studie ervan. De cryptografie is een tak van de wiskunde die minder ontwikkeld is dan de codetheorie. Er bestaat (nog) geen algemene theorie en vele methodes werken slechts in zeer speciale gevallen. De *cryptanalyse* is de tak van de wiskunde die probeert om een onderschept geheim bericht te ontcijferen. Het is dus het “breken van codes” dat je in vele oorlogsfilms en spionageromans ontmoet.

### 1.2 Enkele voorbeelden en definities

**Het telefoongesprek.** Indien je aan de telefoon iets niet goed begrijpt, vraag je je correspondent meestal om te herhalen wat hij gezegd heeft. Dit is mogelijk omdat we hier beschikken over *tweewegcommunicatie*. Soms verwacht je op voorhand al problemen met het goed verstaan van een naam bijvoorbeeld. Dan gaan vele mensen spontaan *spellen*. Als je de naam “VALENTIJN” wil doorbellen zeg je iets als “Victor, Albert, Leopold, Evarist, Norbert, Theofiel, Isidoor, Josef, Norbert”. In dit bericht bestaat de echte informatie uit de eerste letter van elk woord. De rest wordt toegevoegd en is eigenlijk overbodig maar helpt bij slechte communicatie de informatie te reconstrueren of misverstanden uit te sluiten. Deze bijkomende overbodige informatie noemt men **redundante informatie**. Een code zal dus aan bepaalde informatie redundante informatie toevoegen die toelaat fouten bij de ontvangst te verbeteren.

**De printer en de computer.** Je weet vast dat computers alle informatie opslaan in de vorm van *bytes* die elk bestaan uit acht *bits*. Deze bits zijn elk gelijk aan één van de binaire symbolen “0” of “1”. Als je print, wordt de informatie in groepjes van 8 bits door een kabel naar je printer gestuurd. De informatie bestaat eigenlijk uit 7 van die 8 bits. De laatste bit is een *controlebit*. Deze wordt door de computer zó berekend dat het aantal symbolen “1” in elke byte die naar de printer vertrekt *even* is. Indien onderweg naar de printer een “1” in een “0” verandert of omgekeerd, zal het aantal symbolen “1” niet meer even zijn. De printer zal dan weten dat er iets fout liep en de computer vragen om de laatste byte te herhalen.

We zien dus dat de printer een fout kan *detecteren* in wat hij ontvangt. Indien er twee fouten optreden zal dit niet opgemerkt worden. Ook kan de printer niet weten welke bit van waarde veranderde. Hij kan dus de fout niet zelf verbeteren maar moet om herhaling vragen. Dit is mogelijk omdat we hier ook in een tweewegsysteem werken waar computer en printer met elkaar in dialoog staan.

De code die hier werd getoond noemen we **(enkelvoudige) pariteitscontrole**.

**Je bankrekeningnummer.** Als je gebruik maakt van “phone banking” zal je het al wel eens voorgehad hebben dat een rekeningnummer geweigerd wordt omdat je het fout ingetoetst had. Is het zo dat de computer met dewelke je belt een lijst heeft van alle geldige bankrekeningnummers? Neen, de computer maakt gewoon een rekensommetje. Onze Belgische rekeningnummers zijn zo gemaakt dat het getal gevormd door de eerste 10 cijfers min het getal gevormd door de laatste twee cijfers steeds deelbaar is door 97. Voor het rekeningnummer

$$001 - 2155815 - 66$$

heb je dus dat

$$97 \mid (0012155815 - 66)$$

Als “phone banking” een foutboodschap geeft is dat dus omdat deze voorwaarde niet voldaan is. Merk op dat 97 het grootste priemgetal is kleiner dan 100 en dat de laatste twee cijfers van je rekeningnummer de rest geven bij deling door 97 van het getal gevormd door de eerste 10 cijfers.

**De ISBN code.** Bijna elk boek draagt een uniek International Standard Book Number (ISBN). Dit “nummer” bestaat uit 10 symbolen waarvan de eerste 9 de werkelijke informatie (eerste cijfer(s) geven taal waarin het boek geschreven is, daarna wordt de uitgeverij aangeduid, ...) bevatten over het boek. Het laatste symbool is zó gekozen dat een zekere lineaire combinatie van de symbolen steeds deelbaar is door 11. Meer precies geldt

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10} \in \text{ISBN} \iff 11 \mid \sum_{i=1}^{10} ia_i$$

De eerste 9 symbolen zijn gewoon cijfers en het symbool  $a_{10}$  kan een cijfer zijn van 0 tot 9 of het symbool “X” dat nodig is als  $\sum_{i=1}^9 ia_i$  rest 10 geeft bij deling door 11. Een voorbeeld is

$$0 - 201 - 11954 - 4$$

Indien één cijfer  $a_j$  verkeerd wordt ontvangen als  $x_j$ , geeft de som

$$\sum_{i=1}^{10} ia_i + j(x_j - a_j) \not\equiv 0 \pmod{11}$$

Stel je voor dat je een koffievlek maakt op de ISBN code van een boek zodanig dat één van de cijfers onleesbaar wordt:

$$0 - 201 - 1\blacksquare 954 - 4$$

Het voordeel is dat je de positie van het beschadigd cijfer kent. Laat ons de lineaire combinatie berekenen zonder  $a_6$ .

$$\sum_{i=1}^{10} ia_i - 6a_6 = 192 \equiv 5 \pmod{11}$$

Modulo 11 geldt dan  $6^{-1}5 = -a_6$ , zodat we  $a_6 = 1$  terugvinden.

Indien je geen vlek maakt, maar twee symbolen (op plaatsen  $j$  en  $k > j$ ) in een ISBN code verwisselt, krijg je ook

$$\sum_{i=1}^{10} ia_i + j(a_k - a_j) + k(a_j - a_k) = \sum_{i=1}^{10} ia_i + (k - j)(a_j - a_k) \not\equiv 0 \pmod{11}$$

De ISBN code laat dus toe één fout te detecteren, één fout te verbeteren als je weet waar ze is ontstaan. Bovendien is deze code in staat de verwisseling van twee symbolen te detecteren.

**Oefening.** Kijk na dat de code van de bankrekeningnummers ook een koffievlek kan verbeteren. Kan deze code steeds een verwisseling van twee cijfers detecteren?

**Enkele belangrijke parameters.** We zien dat in een codewoord meestal een stuk *informatie* zit waaraan een *redundant* stuk wordt toegevoegd. Dit redundant stuk is overbodig indien er geen storing optreedt maar laat in het andere geval (soms) toe te *detecteren* dat er een storing geweest is en soms zelfs om de fout te verbeteren. Als bij een bepaalde *code* alle woorden bestaan uit  $n$  symbolen, waarvan er steeds  $k$  informatie zijn en  $r$  redundant ( $k + r = n$ ), noemt men de verhouding  $I := \frac{k}{n}$  de **informatie-inhoud** van de code. Het redundante stuk noemt men soms de *controlebits*. De parameter  $n$  heet **lengte** van de code.

Het doel van de codetheorie is dus de informatie-inhoud zo groot mogelijk maken, met de garantie dat een zeker aantal fouten kan gedetecteerd en/of verbeterd worden. Hoeveel fouten je wil verbeteren hangt meestal af van de manier waarop de berichten worden verzonden. Voor een verbinding tussen printer en computer gebruik je een goed geleidende kabel die weinig onderhevig is aan storingen. Je hoeft dus geen sterke code. Detectie van een fout is meer dan voldoende. Voor snelheid is het wel belangrijk dat de informatieverhouding hoog is. Deze is in dit geval  $7/8$ . In het volgende voorbeeld is een sterke code geen luxe.

**Mariner 9.** In 1971 maakte de Amerikaanse ruimtesonde Mariner 9 meer dan 7500 prachtige foto's van het oppervlak van de planeet Mars. Een beeld is ongeveer 5 minuten onderweg tot aan de aarde. Indien er een fout optreedt, kan je niet aan de sonde vragen om het beeld opnieuw door te sturen. Ten eerste is de sonde dan al niet meer op de plaats waar de foto werd genomen. Ten tweede ben je dan weer 5 minuten kwijt waarop je beter een andere foto zou doorsturen. Daarom gebruikte men in 1971 een zogenaamde *Reed-Muller code* van lengte 32 met  $k = 6$  en  $r = 26$ . De informatieverhouding is  $\frac{6}{32} \approx 0.18$  en lijkt niet zo goed, maar de code is wel in staat om zeven fouten te verbeteren. Je mag dus in een woord van lengte 32 tot 7 bits veranderen en toch zal de code het oorspronkelijke bericht kunnen reconstrueren. By the way: de ISBN code is ook een Reed-Muller code, maar dan over  $\mathbb{F}_{11}$ .

**Repetitie codes.** Deze eenvoudige manier om te coderen bestaat er in om de informatie een vast aantal keer te herhalen. Als het bericht bijvoorbeeld "0" is, zal men "000" doorzenden. Als er niet teveel fouten optreden, kan men dit decoderen aan de hand van een *meerderheidsregel*: een groepje van drie bits interpreteert men als het symbool dat het meest voorkomt in dat groepje. Een groepje "110" wordt geïnterpreteerd als "1". Als er maar één fout is opgetreden, is dit correct. Indien er twee fouten zijn opgetreden, was dit bericht oorspronkelijk "000" en dus bedoeld als een "0". We decoderen in dat geval dus verkeerd. Om twee fouten te kunnen verbeteren zou je elke letter 5 maal moeten herhalen. Merk op dat deze repetitie codes in staat zijn vele fouten te verbeteren als je maar een groot aantal keer herhaalt. De informatie-inhoud is echter zeer klein: als je alles  $r$  keer herhaalt, krijg je  $I = \frac{1}{r+1}$ . Daarom is het nuttig betere foutverbeterende codes te verzinnen.

**De Compact Disc.** Dit is een pareltje van de codetheorie dat we allemaal in huis hebben... Een CD schijfje dat je nieuw in de winkel koopt bevat gemiddeld 500.000 fouten. Toch hoor je daar niets van bij het afspelen. Als je zeer voorzichtig bent met je CD zullen er na een tiental uur luisterplezier toch al gauw 5 miljoen fouten op staan. Nog steeds merk je niets... Bij de CD werken twee redelijk zwakke codes samen om een uiterst sterk duo te vormen. Het zijn *Reed-Solomon codes* met parameters  $(n, k)$  gelijk aan  $(32, 28)$  en  $(28, 24)$  die ons, samen met nog een paar wiskundige vindingen, toelaten dagelijks te genieten van perfecte digitale muziek.

### 1.3 Verbetering van fouten

Laat ons veronderstellen dat we een schip op de Noordzee tussen verschillende wrakken moeten loodsen. De enige richtlijnen die we kunnen geven is de vaarrichting die **Noord**, **Oost**, **Zuid** of **West** kan zijn. Jammer genoeg beschikt het schip niet over een telefoon. Wij moeten onze berichten doorseinen als *binair woorden*. Een voor de hand liggende vertaling gebruikt respectievelijk de volgende woorden van twee letters: 00, 01, 10 en 11. Deze codering laat natuurlijk geen enkele fout toe: als een symbool verandert, blijft het ontvangen tweeletterwoord zin hebben en is het gevaar voor milieurampen zeer groot. Deze code detecteert geen enkele fout.

We verbeteren de code met een pariteitscontrole. De vier woorden zijn dan

000, 011, 101, 110

Indien er nu een letter verandert, bekomen we een woord dat geen van deze vier is. We detecteren dus een fout en kunnen vragen om het bericht opnieuw door te zenden. Het kan ook zijn dat de zendinstallatie van het schip defect is zodat het niet kan vragen om herhaling. Dan moeten we de code nog verbeteren. . .

Nu maken we een code van lengte 5 met volgende vier woorden:

00000, 01101, 10110, 11011

Indien er nu bij het doorzenden van een woord één fout optreedt, kunnen we ze niet alleen detecteren, maar ook nog verbeteren. Veronderstel bijvoorbeeld dat we 00101 ontvangen. We vergelijken dit woord met de vier woorden van onze code en noteren het aantal plaatsen waarin ze van elkaar verschillen:

00000,	01101,	10110,	11011
2	1	3	4

Er is dus een uniek woord dat het minst verschilt van het ontvangen woord. We beslissen dus dat het verzonden bericht 01101 was en gaan naar het Oosten. Als er maar één fout was, is dit de juiste beslissing, anders. . .

Deze code van lengte 5 is dus in staat om één fout te verbeteren. (Ga na dat dit niet alleen in ons voorbeeld het geval is!)

We spraken hier over een uniek codewoord dat het minst verschilt van het ontvangen woord. We zouden dit codewoord ook het “dichtst bij” het ontvangen woord willen noemen. Hiervoor is een begrip *afstand* nodig.

**1 Definitie.** Zij  $A$  een eindige verzameling die we *alfabet* noemen. De elementen van  $A$  noemen we meestal *letters* of *symbolen*. Voor een positief geheel getal  $n$  heten de elementen van het Cartesisch product  $A^n$  *woorden* van *lengte*  $n$  over  $A$ . De *Hamming afstand*  $d(\mathbf{x}, \mathbf{y})$  tussen twee woorden  $\mathbf{x}, \mathbf{y} \in A^n$  is het aantal coördinaten waarin  $\mathbf{x}$  en  $\mathbf{y}$  verschillen. Formeel hebben we dus

$$d(\mathbf{x}, \mathbf{y}) = |\{i \mid i \in \{1, 2, \dots, n\} \text{ en } x_i \neq y_i\}|$$

Een woord  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  noteren we soms ook  $x_1 x_2 \dots x_n$ .

**2 Eigenschap.** De Hamming afstand is een metriek.

*Bewijs.* Enkel de driehoeksongelijkheid vraagt enkele seconden aandacht.

$$d(\mathbf{x}, \mathbf{z}) = |\{i \mid x_i \neq z_i\}| = |\{i \mid x_i \neq z_i \text{ en } x_i \neq y_i\} \cup \{i \mid x_i \neq z_i \text{ en } x_i = y_i\}| \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$$

□

**3 Definitie.** Een *code* van *lengte*  $n \in \mathbb{N}_0$  over een alfabet  $A$  is gewoon een verzameling  $C$  van woorden van lengte  $n$  over  $A$ . De elementen van  $C$  noemen we *codewoorden*.

Zij  $C \subseteq A^n$  een code. Bij het *decoderen* gaan we er steeds van uit dat er zo weinig mogelijk fouten zijn opgetreden. Als we dus een woord  $\mathbf{x} \in A^n$  ontvangen, gaan we op zoek naar een woord  $\mathbf{c} \in C$  zodanig dat de Hamming afstand  $d(\mathbf{x}, \mathbf{c})$  zo klein mogelijk wordt. Als we zulk een woord vinden, gaan we beslissen dat  $\mathbf{c}$  waarschijnlijk het woord was dat oorspronkelijk verzonden was. Indien er vele symbolen veranderd werden, vergissen wij ons. Soms vinden we ook meer dan één woord op minimale afstand van  $\mathbf{x}$ . Dan kunnen we niet beslissen. We kunnen wel zeggen dat er fouten geweest zijn.

**4 Definitie.** De *minimale afstand* van een code  $C \subseteq A^n$  is

$$d(C) := \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y} \in C\}$$

**5 Stelling.** Zij  $C \subseteq A^n$  een code. Indien  $d(C) \geq s + 1$ , kan  $C$  tot  $s$  fouten detecteren. Als  $d(C) \geq 2t + 1$ , kan  $C$  tot  $t$  fouten verbeteren.

*Bewijs.* Veronderstel dat een woord  $\mathbf{c} \in C$  verzonden wordt en er  $s$  (of minder) fouten optreden. Dan kan  $\mathbf{c}$  hierdoor nooit zo gewijzigd worden dat het een ander codewoord wordt. We kunnen dus vaststellen dat er fouten geweest zijn.

Onderstel nu dat  $t$  (of minder) fouten het verzonden codewoord  $\mathbf{c}$  wijzigen tot een woord  $\mathbf{x}$ . We hebben dan  $d(\mathbf{c}, \mathbf{x}) \leq t$ . Mocht er een codewoord  $\mathbf{c}'$  bestaan met  $d(\mathbf{x}, \mathbf{c}') \leq t$ , zou de driehoeksongelijkheid impliceren dat  $d(\mathbf{c}, \mathbf{c}') \leq 2t$ , wat onmogelijk is. We hebben dus dat elk codewoord  $\mathbf{c}' \neq \mathbf{c}$  verder ligt van  $\mathbf{x}$  dan  $\mathbf{c}$  zodat we  $\mathbf{x}$  decoderen als  $\mathbf{c}$ . □

**Notatie.** Een code van lengte  $n$  die  $M$  woorden bevat en minimale afstand  $d$  heeft, noteren we kort een  $[n, M, d]$ -code.

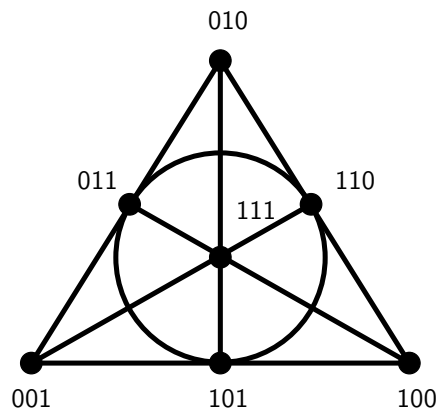


Je ziet dat de syndroomvector 010 gelijk is aan de zesde kolom van de matrix  $H$ . Dit toont ons dat de fout (waarschijnlijk) is opgetreden bij de zesde bit van het codewoord  $\mathbf{x}$ . Om  $\mathbf{x}$  terug te vinden uit  $\mathbf{y}$  veranderen we dus gewoon de zesde bit in  $\mathbf{y}$ . Doordat we binair werken, is er voor die wijziging slechts één keuze.

Hetzelfde syndroom had ook kunnen veroorzaakt worden door een foutvector  $\mathbf{e}' = 0110001$  (er treden drie fouten op). In dat geval is het ontvangen woord afkomstig van het codewoord 0011110 en maken wij dus een fout bij het decoderen.

We hebben hier een code van lengte 7 met 16 woorden over een alfabet met twee letters en minimale afstand 3 (verifieer!). Dit is een perfecte code.

Merk op dat de 7 kolommen van de matrix  $H$  juist de coördinaten zijn van de 7 punten van  $P^2(\mathbb{F}_2)$ , het kleinste projectief vlak.



## Hoofdstuk 2

# Eindige lichamen

**10 Definitie.** Zoals je al lang weet is een **lichaam** een ring met eenheid waarin elk niet-nul element een invers heeft voor de vermenigvuldiging. Een **veld** is een lichaam waarvan de vermenigvuldiging commutatief is.

**Opmerking.** Wij veronderstellen steeds dat  $0 \neq 1$  is in een lichaam. Bijgevolg heeft elk lichaam minstens twee elementen.

### 2.1 Algemeenheden

**11 Definitie.** Een element  $a \neq 0$  van een ring  $R$  heet een **nuldeler** indien er een  $b \in R \setminus \{0\}$  bestaat zodanig dat  $ab = 0$  of  $ba = 0$  in  $R$ .

**12 Lemma.** Een lichaam heeft geen nuldelers.

**13 Stelling.** De ring  $(\mathbb{Z}_m, +, \cdot)$  is een lichaam **als en slechts als**  $m$  een priemgetal is.

*Bewijs.* Een implicatie steunt op voorgaand lemma. Voor de andere implicatie nemen we  $a \in \mathbb{Z}_m \setminus \{0\}$  vast en tonen gemakkelijk aan dat alle elementen van de verzameling  $\{ax \mid x \in \mathbb{Z}_m\}$  verschillend zijn. Bijgevolg heeft  $a$  een invers.  $\square$

Voor een priemgetal  $p$  noteren we vanaf nu het lichaam  $(\mathbb{Z}_p, +, \cdot)$  kort  $\mathbb{F}_p$ . Merk op dat dit lichaam commutatief is. Volgende stelling toont dat dit geen toeval is.

**14 Stelling (Wedderburn).** Elk eindig lichaam is een veld.

Het bewijs van deze stelling geven we niet en hoort thuis in een cursus algebra. Dankzij dit resultaat mogen we in wat volgt wel steeds aannemen dat de vermenigvuldiging commutatief is.

**Taak.** Zoek het bewijs van de “Stelling van Wedderburn” op in [1] en werk het volledig uit.

In wat volgt zal het symbool  $\mathbb{F}$  steeds een veld voorstellen. Met  $\mathbb{F}$  kan je een **veeltermring**  $\mathbb{F}[X]$  construeren die ook commutatief is.

**15 Stelling.** Voor elke twee veeltermen  $A$  en  $B$  in  $\mathbb{F}[X]$ , met  $B \neq 0$ , bestaan unieke veeltermen  $Q$  en  $R$  in  $\mathbb{F}[X]$  die voldoen aan  $A = BQ + R$  en  $\deg R < \deg B$ .

*Bewijs.* Als  $B \mid A$ , nemen we gewoon  $R = 0$  en  $Q = \frac{A}{B}$ . In het andere geval beschouwen we de verzameling  $V := \{A - BC \mid C \in \mathbb{F}[X]\}$  en kiezen hierin  $R = A - BQ$  van minimale graad. Veronderstel dat  $d := \deg R \geq \deg B =: e$  en noteer de hoogste graadscoëfficiënt van  $R$  en  $B$  respectievelijk  $r$  en  $b$ . Dan geldt

$$R - \frac{r}{b}X^{d-e}B = A - B\left(Q + \frac{r}{b}X^{d-e}\right)$$

De graad van het linkerlid is hoogstens  $d - 1$  en in het rechterlid staat een element van  $V$ , in tegenspraak met de keuze van  $R$ . De uniciteit van  $Q$  en  $R$  bewijzen we ook uit het ongerijmde.  $\square$

Zoals gebruikelijk noemen we de veelterm  $Q$  van vorige stelling het **quotiënt** van de **deling** van  $A$  door  $B$ . De veelterm  $R$  is de **rest** van deze deling.

**16 Definitie.** Naar analogie met gehele getallen, noemen we twee veeltermen  $A$  en  $A'$  **congruent modulo een veelterm  $M$**  indien hun verschil  $A - A'$  deelbaar is door  $M$ . We noteren dit  $A \equiv A' \pmod{M}$ .

**17 Gevolg.** Zij  $A, A', M \in \mathbb{F}[X]$ , dan geldt  $A \equiv A' \pmod{M}$  als en slechts als  $A$  en  $A'$  dezelfde rest geven bij deling door  $M$ .

**18 Definitie.** Een veelterm waarvan de hoogstegraadscoëfficiënt 1 is, heet **monisch**.

Voor een veelterm  $M \in \mathbb{F}[X]$  kunnen we de quotiëntring  $\mathbb{F}[X]/(M)$  beschouwen waarbij  $(M)$  het ideaal is voortgebracht door  $M$ . De elementen van deze ring zijn de equivalentieclassen van de congruentie van veeltermen modulo  $M$ . We spreken af dat we als representant voor elke klasse de monische veelterm van minimale graad nemen.

Neem nu  $A, B \in \mathbb{F}[X]$  met  $B \neq 0$ . Toepassing van stelling (15) levert een quotiënt  $Q$  en een rest  $R_0$  met  $\deg R_0 < \deg B$ . We kunnen de stelling opnieuw toepassen op de deling van  $B$  door  $R_0$ . Dit levert een nieuw quotiënt  $Q_0$  en een rest  $R_1$  met  $\deg R_1 < \deg R_0 < \deg B$ . Daar de graad van de rest strikt dalend is, kunnen we dit niet oneindig lang blijven doen. We bekomen een opeenvolging van delingen waarbij de laatste rest nul is.

$$\begin{array}{rcl} A & = & BQ + R_0 & \deg R_0 < \deg B \\ B & = & R_0Q_0 + R_1 & \deg R_1 < \deg R_0 \\ & & \vdots & \vdots \\ R_{n-2} & = & R_{n-1}Q_{n-1} + R_n & \deg R_n < \deg R_{n-1} \\ R_{n-1} & = & R_nQ_n + 0 & \end{array}$$

Voor elke twee veeltermen  $A$  en  $B$  met  $0 \leq \deg B \leq \deg A$  kan je zulke rij van delingen opstellen. Dit procédé noemt men het **Euklidisch delingsalgoritme**.

**19 Stelling.** De laatste niet-nulle rest in het Euklidisch delingsalgoritme is een grootste gemene deler van de veeltermen  $A$  en  $B$ .

*Bewijs.* Zij  $C \in \mathbb{F}[X]$  een gemene deler van  $A$  en  $B$ . Bij inductie gaan we na dat  $C$  alle resten  $R_0, R_1, \dots, R_n$  deelt. Bovendien is  $R_n$  een gemene deler van  $A$  en  $B$  (ook bij inductie).  $\square$

Meestal hebben twee veeltermen meerdere grootste gemene delers omdat elk scalair veelvoud van een grootste gemene deler opnieuw een grootste gemene deler is. We spreken af dat we **de** grootste gemene deler van  $A$  en  $B$  steeds monisch kiezen. Deze veelterm noteren we  $\text{ggd}(A, B)$ .

**20 Stelling (Bezout).** Zij  $A, B \in \mathbb{F}[X]$ . Dan bestaan er veeltermen  $C, D \in \mathbb{F}[X]$  zodat  $AD - BC = \text{ggd}(A, B)$ .

*Bewijs.* Lees het Euklidisch algoritme achterstevoren!  $\square$

**21 Gevolg.**  $\text{ggd}(A, M) = 1 \implies \exists A' \in \mathbb{F}[X] : AA' \equiv 1 \pmod{M}$

**22 Definitie.** Een veelterm  $M \in \mathbb{F}[X]$  heet **irreduciebel** als  $M$  geen andere delers heeft dan de scalair (i.e. de constante veeltermen) en zichzelf.

**23 Stelling.**  $M \in \mathbb{F}[X]$  irreduciebel  $\implies \mathbb{F}[X]/(M)$  is een veld.

*Bewijs.* Je kan als representanten voor de de restklassen in  $\mathbb{F}[X]$  modulo  $M$  alle veeltermen met graad kleiner dan  $\deg M$  kiezen. Voor zo een representant  $A$  geldt, door de irreducibiliteit van  $M$ , dat  $\text{ggd}(A, M) = 1$ . Pas de stelling van Bezout toe om het invers van  $A$  te vinden (modulo  $M$ ).  $\square$

**Opmerking.** De omgekeerde implicatie in bovenstaande stelling geldt ook. Met de cursus “algebra 1” van tweede kandidatuur in de hand maak je gemakkelijk volgende redenering: vermits  $\mathbb{F}$  commutatief is, is  $\mathbb{F}[X]$  het ook. Bijgevolg is het ideaal  $(M)$  maximaal als en slechts als  $\mathbb{F}[X]/(M)$  een veld is. Bovendien is een maximaal ideaal steeds een priemideaal.

Als we nu  $\mathbb{F} = \mathbb{F}_p$  nemen voor een priemgetal  $p$ , levert bovenstaande constructie een veld op met  $p^h$  elementen op voorwaarde dat we een irreduciebele veelterm in  $\mathbb{F}_p[X]$  vinden met graad  $h$ . Sectie 2.3 gaat over de existentie van irreduciebele veeltermen.

## 2.2 Additieve structuur van een eindig lichaam

Zij  $\mathbb{F}$  een eindig veld met eenheidselement 1 en beschouw de sommen  $1, 1 + 1, 1 + 1 + 1, \dots$ . Doordat  $\mathbb{F}$  maar een eindig aantal elementen heeft, moeten er twee natuurlijke getallen  $r < s$  bestaan met

$$\sum_{i=1}^r 1 = \sum_{i=1}^s 1$$

Dit is equivalent met  $\sum_{i=1}^{s-r} 1 = 0$ .

**24 Definitie.** De *karakteristiek* van een eindig veld  $\mathbb{F}$  is het kleinste natuurlijk getal  $c > 0$  met  $\sum_{i=1}^c 1 = 0$ . We noteren dit getal  $\text{char } \mathbb{F}$ .

**25 Eigenschap.** De karakteristiek van een eindig veld is steeds een priemgetal.

*Bewijs.* Anders zouden er nuldelers zijn. □

**26 Eigenschap.**  $\text{char } \mathbb{F} = p \implies \forall a \in \mathbb{F} : pa = \underbrace{a + a + \dots + a}_{p \text{ keer}} = 0$ .

*Bewijs.* Herschrijf  $pa$  als som van enen. □

**27 Stelling.** Elk veld  $\mathbb{F}$  van karakteristiek  $p$  omvat een deelveld isomorf met  $\mathbb{F}_p$ .

*Bewijs.* Het deelveld bestaat uit de elementen  $1, 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p \text{ keer}} = 0$ . □

**28 Definitie.** Het deelveld uit vorige stelling noemt men het *priemveld* van  $\mathbb{F}$ .

**29 Gevolg.** Een veld  $\mathbb{F}$  waarvan het aantal elementen een priemgetal  $p$  is, is isomorf met  $\mathbb{F}_p$ .

*Bewijs.* Stel  $q := \text{char } \mathbb{F} > 1$ . Uit stelling (27) volgt dat de groep  $(\mathbb{F}, +)$  van orde  $p$  en deelgroep heeft van orde  $q$ . Vermits  $p$  priem is, volgt uit de stelling van Lagrange dat  $q = p$ . Het veld  $\mathbb{F}$  is dus gelijk aan zijn priemveld, dat isomorf is met  $\mathbb{F}_p$ . □

**30 Stelling.** Een eindig veld heeft steeds  $p^h$  elementen voor een zeker priemgetal  $p$  en een zeker natuurlijk getal  $h > 0$ .

*Bewijs.* Stel  $p := \text{char } \mathbb{F}$  en

$$S_1 := \{1, 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p \text{ keer}} = 0\}$$

Als  $S_1 = \mathbb{F}$  is het bewijs gedaan. Anders kiezen we  $a \in \mathbb{F} \setminus S_1$  en stellen we

$$S_2 = \{ma + n1 \mid 0 < m, n \leq p\}$$

Deze verzameling heeft hoogstens  $p^2$  elementen. Veronderstel  $m_1 a + n_1 1 = m_2 a + n_2 1$  met  $n_2 > n_1$ . Als  $m_1 = m_2$ , is  $(n_2 - n_1)1 = 0$ , in tegenspraak met  $\text{char } \mathbb{F} = p$ . Voor  $m_1 \neq m_2$ , nemen we  $k \in S_1$  zó dat  $k(m_1 - m_2) = 1$ . Dan geldt  $a = ak(m_1 - m_2) = k(n_2 - n_1)1 \in S_1$ , een  $\frac{1}{2}$ . Dus geldt  $|S_2| = p^2$ . Indien  $S_2 \neq \mathbb{F}$  definiëren we op analoge wijze  $S_3$  met  $p^3$  elementen enz. Dit stopt na een tijd vermits  $\mathbb{F}$  eindig is. □

**31 Gevolg.** De additieve groep van een eindig veld  $\mathbb{F}$  is isomorf met een direct product van isomorfe cyclische groepen van orde  $\text{char}\mathbb{F}$ .

*Bewijs.* Uit vorig bewijs halen we dat

$$\mathbb{F} = S_h = \left\{ \sum_{i=1}^h \lambda_i a_i \mid \lambda_i \in S_1 \right\}$$

met  $a_1 = 1$ . Vermits  $S_1$  isomorf is met de groep  $(\mathbb{Z}_p, +)$ , construeren we gemakkelijk een isomorfisme  $(\mathbb{F}, +) \longleftrightarrow (\mathbb{Z}_p)^h$ .  $\square$

**Notatie.** Voor een veelterm  $A = \sum_{i=0}^n \alpha_i X^i$  over  $\mathbb{F}$  en een element  $a \in \mathbb{F}$  stellen we  $A(a) := \sum_{i=0}^n \alpha_i a^i \in \mathbb{F}$ . We zeggen dat we de veelterm  $A$  evalueren in  $a$ .

**32 Lemma.** Zij  $a \in \mathbb{F}$  en  $A \in \mathbb{F}[X]$ . Dan is  $A$  deelbaar door  $X - a$  als en slechts als  $A(a) = 0$ .

**33 Gevolg.** Een veelterm van graad  $n > 0$  kan hoogstens  $n$  verschillende nulpunten bezitten.

**34 Lemma.** Zij  $P$  irreduciebel in  $\mathbb{F}[X]$  en  $G_1, G_2 \in \mathbb{F}[X]$ . Er geldt

$$P \mid G_1 G_2 \implies P \mid G_1 \text{ of } P \mid G_2$$

*Bewijs.* Als  $P$  de veelterm  $G_1$  niet deelt, impliceert de irreducibiliteit dat  $\text{ggd}(P, G_1) = 1$ . De stelling van Bezout levert veeltermen  $A$  en  $B$  met  $AP + BG_1 = 1$ . Hieruit volgt dat  $APG_2 + BG_1G_2 = G_2$ . Vermits  $P$  beide termen van deze som deelt, volgt de stelling.  $\square$

**35 Gevolg.** Een irreduciebele veelterm die een eindig product van veeltermen deelt, moet minstens één van de factoren delen.

**36 Stelling.** Iedere monische veelterm kan steeds op een (op volgorde na) unieke wijze geschreven worden als product van irreduciebele monische veeltermen.

*Bewijs.* Het is duidelijk dat er steeds minstens één ontbinding is. Voor de uniciteit werken we uit het ongerijmde. Veronderstel dat

$$A = \prod_{i=1}^r G_i = \prod_{j=1}^s H_j$$

De veelterm  $G_1$  is irreduciebel en deelt het product  $\prod_{j=1}^s H_j$ . Bijgevolg bestaat er een index  $j$  met  $G_1 \mid H_j$ . Maar  $H_j$  is ook irreduciebel zodat  $H_j = G_1$ . De factor  $G_2$  deelt nu het product  $H_1 H_2 \cdots \widehat{H}_j \cdots H_s$  zodat er een andere  $H_j$  wegvalt.  $\square$

## 2.3 Over het aantal irreduciebele veeltermen van graad $m$ in $\mathbb{F}[X]$

Zij  $\mathbb{F}$  een veld met  $q$  elementen (eindig dus). We noteren de verzameling van alle monische veeltermen in  $\mathbb{F}[X]$  met  $\mathcal{M}$  en stellen het aantal irreduciebele veeltermen van graad  $m$  in  $\mathcal{M}$  voor met  $i_m$ . We gaan bewijzen dat  $i_m > 0$  voor elke  $m \in \mathbb{N}$ . Voor  $m < 2$  is dat duidelijk.

**37 Stelling.**

$$\sum_{N \in \mathcal{M}} z^{\deg N} = \prod_{\substack{P \in \mathcal{M} \setminus \{1\} \\ P \text{ irreduciebel}}} \frac{1}{1 - z^{\deg P}} \quad \text{voor } 0 \leq z < \frac{1}{q}$$

*Bewijs.* In het linkerlid hebben we

$$\sum_{N \in \mathcal{M}} z^{\deg N} = \sum_{m=0}^{\infty} \sum_{\substack{N \in \mathcal{M} \\ \deg N = m}} z^m = \sum_{m=0}^{\infty} q^m z^m = \frac{1}{1 - qz}$$

Een algemene factor van het rechterlid is

$$\frac{1}{1 - z^{\deg P}} = \sum_{i=0}^{\infty} z^{i \deg P} = \sum_{i=0}^{\infty} z^{\deg P^i}$$

zodat het product van twee factoren gelijk is aan

$$\frac{1}{1 - z^{\deg P}} \cdot \frac{1}{1 - z^{\deg Q}} = \left( \sum_{i=0}^{\infty} z^{\deg P^i} \right) \cdot \left( \sum_{j=0}^{\infty} z^{\deg Q^j} \right) = \sum_{\substack{j=0 \\ i=0}}^{\infty} z^{\deg P^i Q^j}$$

Voor  $P$  en  $Q$  irreduciebel in  $\mathcal{M}$  loopt deze laatste som over monische veeltermen. Een product van  $k$  factoren in het rechterlid zal dus voldoen aan

$$\prod_{j=1}^k \frac{1}{1 - z^{\deg P_j}} = \sum_{\substack{j_1=0 \\ j_2=0 \\ \vdots \\ j_k=0}}^{\infty} z^{\deg P_1^{j_1} P_2^{j_2} \dots P_k^{j_k}} \leq \sum_{N \in \mathcal{M}} z^{\deg N} = \frac{1}{1 - qz}$$

Vermits elke veelterm in  $\mathcal{M}$  op unieke wijze te schrijven is als product van irreduciebele monische veeltermen, volgt de stelling. Merk op dat de monische veelterm 1 toch in het (partieel)product verschijnt op het moment dat alle exponenten  $j_i$  nul zijn.  $\square$

**38 Gevolg.** Voor  $0 \leq z < \frac{1}{q}$  geldt

$$\frac{1}{1 - qz} = \prod_{m=1}^{\infty} \left( \frac{1}{1 - z^m} \right)^{i_m}$$

**39 Stelling.**

$$\forall k \in \mathbb{N}_0 : q^k = \sum_{m|k} m i_m$$

*Bewijs.* Neem de logaritme in beide leden van gevolg (38):

$$-\log(1 - qz) = - \sum_{m=1}^{\infty} i_m \log(1 - z^m)$$

Zolang we binnen de convergentiestraal blijven, mogen we term per term afleiden en vermenigvuldigen met  $z$ . Dit geeft

$$\frac{qz}{1 - qz} = \sum_{m=1}^{\infty} i_m m \frac{z^m}{1 - z^m}$$

of

$$\sum_{k=1}^{\infty} (qz)^k = \sum_{m=1}^{\infty} i_m m \sum_{r=1}^{\infty} z^{mr} = \sum_{k=1}^{\infty} z^k \sum_{m|k} m i_m$$

waarbij  $k := mr$  in de laatste stap. Gelijkstelling van de coëfficiënten van  $z^k$  in beide leden geeft nu het gewenste resultaat.  $\square$

**40 Gevolg.** Voor elk veld  $\mathbb{F}$  met  $q$  elementen en voor elke graad  $m \in \mathbb{N}$  bevat  $\mathbb{F}[X]$  een irreduciebele veelterm van graad  $m$ .

*Bewijs.* Uit vorige stelling halen we dat voor elke  $k \in \mathbb{N}_0$  geldt

$$q^k - \sum_{r=1}^{k-1} r i_r = \sum_{m|k} m i_m - \sum_{r=1}^{k-1} r i_r \leq k i_k$$

maar ook dat  $k i_k \leq q^k$  zodat

$$\sum_{r=1}^{k-1} r i_r \leq \sum_{r=1}^{k-1} q^r = \frac{q^k - 1}{q - 1}$$

Nu volgt

$$ki_k \geq q^k - \frac{q^k - 1}{q - 1} = \frac{1}{q - 1} + q^k \left( 1 - \frac{1}{q - 1} \right) > 0$$

De laatste ongelijkheid volgt uit het feit dat  $q > 1$  moet zijn omdat  $\mathbb{F}$  een veld is. □

**Voorbeeld.** Nemen we  $\mathbb{F} = \mathbb{F}_2$  (of  $q = 2$ ), dan geldt  $i_1 = 2$  omdat beide veeltermen,  $X$  en  $X + 1$ , van graad 1 over  $\mathbb{F}$  irreduciebel zijn. Uit stelling (39) volgt dat

$$2^2 = 1i_1 + 2i_2 = 2 + 2i_2$$

zodat  $i_2 = 1$ . Inderdaad, de enige irreduciebele veelterm van graad 2 over  $\mathbb{F}_2$  is  $X^2 + X + 1$ . Voor  $i_3$  krijgen we de recurrentie

$$2^3 = 1i_1 + 3i_3 = 2 + 3i_3$$

zodat  $i_3 = 2$  enz.

## 2.4 Multiplicatieve structuur van een eindig veld

Bij definitie vormen de niet-nulle elementen van een lichaam  $\mathbb{F}$  een groep voor de vermenigvuldiging. We noteren deze groep in het algemeen  $\mathbb{F}^\times$  en bestuderen nu zijn structuur in het geval dat  $\mathbb{F}$  eindig is.

In een eindig veld  $\mathbb{F}$  kijken we naar de opeenvolgende machten  $a, a^2, a^3, \dots$  van een niet-nul element  $a$ . Doordat er slechts een eindig aantal elementen zijn in  $\mathbb{F}$ , moeten er exponenten  $r < s$  zijn met  $a^r = a^s$ , zodat  $a^{s-r} = 1$ .

**41 Definitie.** De *orde* van een niet-nul element  $a$  van een eindig veld  $\mathbb{F}$  is de kleinste macht  $n > 0$  zodanig dat  $a^n = 1$ . We noteren deze macht  $\text{ord}(a)$ .

**Opmerking.** Als  $\text{ord}(a) = n$ , zijn alle machten  $a, a^2, \dots, a^n = 1$  verschillend.

**42 Eigenschap.** Zij  $a$  en  $b$  elementen van respectievelijke orde  $m$  en  $n$ . Dan geldt

- (i)  $a^k = 1 \iff m \mid k$ ;
- (ii)  $\forall k \in \mathbb{N}_0 : \text{ord}(a^k) = \frac{m}{\text{ggd}(m,k)}$ ;
- (iii)  $\text{ggd}(m,n) = 1 \implies \text{ord}(ab) = mn$ .

*Bewijs.* 1. Eén implicatie is triviaal. Euklidische deling geeft  $k = qm + r$  met  $r < m$  zodat geldt  $a^{qm+r} = 1 \cdot a^r = 1$ . Dus moet  $r = 0$ .

2. Stel  $t := \text{ord}(a^k)$ . Dan is  $t$  de kleinste  $l > 0$  met  $(a^k)^l = a^{kl} = 1$ . We weten al  $m \mid kl$ . Stel  $g := \text{ggd}(m,k)$ . Dan geldt  $m = m'g$  en  $k = k'g$ , met  $\text{ggd}(m',k') = 1$ . Dus is  $t$  de kleinste  $l$  met  $m'g \mid k'gl$ . Dit impliceert  $m' \mid l$ . De minimaliteit van  $t$  garandeert nu  $l = m' = \frac{m}{g}$ .

3. Als  $(ab)^k = 1$ , geldt  $a^k = b^{-k}$ , zodat  $a^{nk} = b^{-nk} = 1$ . Hieruit volgt  $m \mid k$ . Analoog geldt  $n \mid k$ . □

**43 Stelling.** Zij  $a$  en  $b$  elementen van respectievelijke orde  $m$  en  $n$  in  $\mathbb{F}$ . Er bestaat een  $c \in \mathbb{F}$  met  $\text{ord}(c) = \text{kgv}(m,n)$ .

*Bewijs.* Zij  $p$  een priemfactor van  $m$  (of  $n$ ) en stel  $\alpha$  de hoogste macht van  $p$  die  $m$  deelt en  $\beta$  de hoogste macht van  $p$  die  $n$  deelt. Zonder de algemeenheid te schaden mogen we aannemen dat  $\alpha \geq \beta$ . Dan is  $p^\alpha$  de grootste macht van  $p$  die  $\text{kgv}(m,n)$  deelt. We hebben  $m = p^\alpha r$  met  $p \nmid r$ . Stel dan  $c_p := a^r$ . Dan is de orde van  $c_p$  gelijk aan  $\frac{m}{\text{ggd}(m,r)} = \frac{m}{r} = p^\alpha$ . Vermits  $\text{kgv}(m,n)$  te ontbinden is in priemfactoren  $\prod_{i=1}^k p_i^{\alpha_i}$ , volstaat het  $c := \prod_{i=1}^k c_{p_i}$  te nemen. □

**44 Definitie.** Een element  $a \in \mathbb{F}$  heet *primitief* indien  $\text{ord}(a) = |\mathbb{F}| - 1$ . Dit wil zeggen dat  $\forall b \in \mathbb{F} \setminus \{0\} : \exists k \in \mathbb{N} : a^k = b$ .

**45 Stelling.** Elk eindig veld bezit een primitief element.

*Bewijs.* Stel  $n := \max\{\text{ord}(a) \mid a \in \mathbb{F} \setminus \{0\}\}$  en zij  $a$  een element van orde  $n$ . Veronderstel nu dat  $n \neq q - 1$ . Dan bestaat er een  $b \in \mathbb{F} \setminus \{a, a^2, \dots, a^n, 0\}$  van orde  $m \leq n$ . Indien  $m \mid n$  dan is  $n = mk$ , zodat  $b^n = 1$ . Maar dan heeft de vergelijking  $X^n - 1 = 0$  meer dan  $n$  wortels. Dus moet  $m \nmid n$ . Maar dan is  $\text{kgv}(m, n) > n$  en geeft vorige stelling een element van orde groter dan  $n$ .  $\square$

**46 Gevolg.** De multiplicatieve groep van een eindig veld is cyclisch.

**47 Gevolg.** In een veld  $\mathbb{F}$  met  $q$  elementen geldt

$$\forall a \in \mathbb{F} : a^q - a = 0$$

**Opmerking.** Indien  $q = p$  voor een priemgetal  $p$ , hebben we  $\mathbb{F} = \mathbb{F}_p$  en staat er in vorig gevolg eigenlijk  $\forall x \in \mathbb{Z} : x^p \equiv x \pmod{p}$ . Dit is de zogenaamde ‘‘Kleine stelling van Fermat’’.

**Opmerking.** Vorige stelling toont wel dat er steeds primitieve elementen zijn, maar zegt niet hoe je die elementen kan vinden. Het vinden van primitieve elementen in een eindig veld is nog steeds een open probleem. Er is nog geen constructie gevonden die in elk eindig veld werkt en die snel en zeker leidt tot een primitief element. Ook een vraag zoals ‘‘voor hoeveel priemgetallen  $p$  is 10 een primitief element van  $\mathbb{F}_p$ ?’’ heeft nog geen antwoord.

**48 Eigenschap.** In een veld  $\mathbb{F}$  van karakteristiek  $p$  geldt

$$\forall a, b \in \mathbb{F} : (a + b)^p = a^p + b^p$$

*Bewijs.*

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$$

maar

$$\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{k!}$$

is steeds deelbaar door  $p$ , tenzij  $k = 0$  of  $k = p$ .  $\square$

**49 Gevolg.** In een veld  $\mathbb{F}$  van karakteristiek  $p$  is de afbeelding

$$\phi : \mathbb{F} \longrightarrow \mathbb{F} : x \longmapsto x^p$$

een lichaamsautomorfisme.

*Bewijs.* Neem vorige eigenschap samen met het feit dat  $(ab)^p = a^p b^p$ , voor elke  $a, b \in \mathbb{F}$ . Nu blijft te tonen dat  $\phi$  bijectief is. Vermits  $\mathbb{F}$  eindig is, volstaat het te tonen dat  $\phi$  injectief is. Zij  $x, y \in \mathbb{F}$  met  $x^p = y^p$ . Dan geldt wegens vorige eigenschap dat  $(x - y)^p = 0$ . Vermits  $\mathbb{F}$  geen nuldelers heeft, kan dit alleen als  $x - y = 0$ .  $\square$

**50 Definitie.** De afbeelding  $\phi$  van bovenstaand gevolg noemt men het **Frobenius automorfisme** van het lichaam  $\mathbb{F}$ .

**51 Gevolg.** In een veld  $\mathbb{F}$  van karakteristiek  $p$  geldt voor willekeurige elementen  $w_1, w_2, \dots, w_k \in \mathbb{F}$  en willekeurige  $n \in \mathbb{N}$  steeds

$$\left( \sum_{i=1}^k w_i \right)^{p^n} = \sum_{i=1}^k w_i^{p^n}$$

*Bewijs.* Twee keer per inductie uit eigenschap (48).  $\square$

**52 Gevolg.** De karakteristiek  $p$  van een eindig veld deelt nooit de orde van een niet-nul element.

*Bewijs.* Anders geldt  $\text{ord}(a) = kp$ , zodat  $a^{kp} = 1$ . Maar dan is  $a^{kp} - 1 = (a^k - 1)^p = 0$ , zodanig dat  $a^k = 1$ , een  $\downarrow$ .  $\square$

**53 Eigenschap.** Zij  $\mathbb{F}_p$  het priemveld van een eindig veld  $\mathbb{F}$ . Dan geldt voor elk element  $a$  van  $\mathbb{F}$

$$a \in \mathbb{F}_p \iff a^p = a$$

*Bewijs.* Eén implicatie is reeds hoger bewezen. Voor de andere merken we op dat de veelterm  $X^p - X$  hoogstens  $p$  wortels heeft.  $\square$

**54 Gevolg.** Het priemveld van een eindig lichaam is juist het dekpuntenlichaam van het Frobenius automorfisme. Dit wil zeggen dat het Frobenius automorfisme de identieke afbeelding induceert op het priemveld en geen andere elementen fixeert.

## Hoofdstuk 3

# Foutverbeterende codes

**55 Definitie.** Zij  $A$  een verzameling met  $q$  elementen,  $n$  een positief natuurlijk getal en  $C \subset A^n$  met  $|C| = M > 1$ . Stel  $d := \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y} \in C\}$ . Dan heet  $C$  een  $q$ -aire  $[n, M, d]$ -code. Voor  $q = 2$  spreken we van een **binaire** code en voor  $q = 3$  van een **ternaire**. De verzameling  $A$  noemt men het **alfabet** van  $C$  en de elementen van  $A^n$  zijn **woorden** van **lengte**  $n$  over  $A$ . De elementen van  $A$  noemen we **letters** of **symbolen**. Elk element van  $C$  is een **codewoord** en  $n$  is de **lengte** van de code  $C$ . De parameter  $d$  heet **minimale afstand** van  $C$ .

**Opmerking.** We veronderstellen steeds dat een code minstens twee woorden bevat. Een code met slechts één woord zou niet erg nuttig zijn vermits je hiermee slechts één boodschap kan versturen. Hiermee kan je geen informatie overbrengen, tenzij tonen dat de zender werkt.

Bestaan er voor elke keuze van getallen  $q, n, M$  en  $d$  steeds  $q$ -aire  $[n, M, d]$ -codes? Een goede code zal veel codewoorden bevatten en toch een kleine lengte en grote minimale afstand realiseren (zie hoofdstuk 1).

**Notatie.** Een  $q$ -aire  $[n, M, d]$ -code noteren we ook een  $[n, M, d]_q$ -code. Gegeven  $q, n$  en  $d$ , noteren we met  $A_q(n, d)$  het grootste getal  $M$  waarvoor een  $[n, M, d]_q$ -code bestaat.

Het is gemakkelijk te zien dat steeds geldt  $A_q(n, 1) = q^n$  vermits twee verschillende woorden in  $A^n$  steeds op afstand  $\geq 1$  liggen van elkaar. Als we echter op zoek gaan naar een code waarvan twee woorden op afstand minstens  $n$  van elkaar liggen, moeten alle woorden in alle letters van elkaar verschillen. Kijken we bijvoorbeeld naar de eerste letter van elk codewoord, zien we dat er ten hoogste  $q$  woorden zijn in zulke code. De code  $\Delta_n(A) = \{(a, a, \dots, a) \in A^n \mid a \in A\}$  heeft juist  $q = |A|$  woorden en minimale afstand  $n$ . We hebben dus bewezen dat  $A_q(n, n) = q$ . De code  $\Delta_n(A)$  heet **repetitiecode** van lengte  $n$  over  $A$ .

Laat ons eens een moeilijker geval bekijken. . . We gaan op zoek naar  $A_2(5, 3)$ . De code  $C_3 = \{00000, 01101, 10110, 11011\}$  over  $A = \{0, 1\}$  heeft minimale afstand 3 zodat  $A_2(5, 3) \geq 4$ . Nu zouden we met een computer alle mogelijke deelverzamelingen van  $A^5$  kunnen bekijken en op zoek gaan naar een  $[5, 5, 3]$ -code. Ondanks de kleine parameters is dit nogal veel werk. Daarom zullen we onze theoretische kennis over foutverbeterende codes een beetje uitbreiden.

**Taak.** Schrijf een computerprogramma om te zoeken naar een  $[5, 5, 3]$ -code over  $\mathbb{F}_2$ . Je mag hiervoor gebruik maken van de programmeertaal GAP[5] en eventueel het pakket guava.

### 3.1 Algemeen

**56 Definitie.** Twee codes  $C_1$  en  $C_2$  van zelfde lengte  $n$  over  $A$  heten **equivalent in brede zin** indien er permutaties  $\sigma_i \in \text{Sym}(A)$  ( $i = 1, 2, \dots, n$ ) en  $\pi \in S_n$  bestaan zodanig dat

$$C_2 = \{(\sigma_1(a_{\pi(1)}), \sigma_2(a_{\pi(2)}), \dots, \sigma_n(a_{\pi(n)})) \mid (a_1, a_2, \dots, a_n) \in C_1\}$$

**57 Lemma.** Equivalent zijn in brede zin is een equivalentierelatie.

**58 Lemma.** *In brede zin equivalente codes hebben dezelfde parameters.*

**59 Lemma.** *Elke  $q$ -aire  $[n, M, d]$ -code over een alfabet  $A$  dat een bijzonder element  $0 \in A$  bevat, is equivalent in brede zin met een  $[n, M, d]$ -code die het woord  $(0, 0, \dots, 0) \in A^n$  bevat.*

We herhalen de Hamming grens die bewezen werd in hoofdstuk 1.

**60 Stelling.** *Voor een  $q$ -aire  $[n, M, 2t + 1]$ -code geldt*

$$M \cdot \sum_{i=0}^t \binom{n}{i} (q-1)^i \leq q^n$$

Er is echter nog een belangrijke grens op het aantal woorden in een foutverbeterende code.

**61 Stelling (Singleton grens).** *Een  $q$ -aire  $[n, M, d]$ -code voldoet aan*

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

*Bewijs.* Bekijk de  $n - d + 1$  eerste letters van elk codewoord. Deze woorden van lengte  $n - d + 1$  moeten alle verschillend zijn aangezien de afstand tussen elke twee codewoorden minstens  $d$  bedraagt. Bijgevolg kunnen er hoogstens  $q^{n-d+1}$  codewoorden zijn.  $\square$

De codes die de de **Singleton grens** bereiken, heten **maximum distance separating codes** of kortweg **MDS codes**.

De Hamming grens levert  $A_2(5, 3) \leq 5$  en de Singleton grens geeft  $A_2(5, 3) \leq 8$ . We moeten dus enkel nog onderzoeken of er een  $[5, 5, 3]$ -code bestaat over  $A = \{0, 1\}$ .

Zij  $C$  een  $[5, M, 3]$ -code met  $M \geq 4$ . Door lemma (59) mogen we veronderstellen dat  $00000 \in C$ . Doordat de minimale afstand 3 moet zijn, impliceert dit dat elk niet-nul codewoord minstens drie enen zal hebben. Daar de minimale afstand 3 moet zijn, weten we ook dat er ten hoogste één codewoord met minstens vier enen kan zijn. De afstand tussen om het even welke twee verschillende woorden met vier enen is immers 2. We hebben dus ten minste twee codewoorden met juist drie enen. Door permutatie van de coördinaten zien we dat  $C$  equivalent is in brede zin met een code die de woorden  $00000$ ,  $11100$  en  $00111$  bevat. Door wat te proberen zie je gemakkelijk dat deze drie woorden enkel nog kunnen aangevuld worden met het woord  $11011$ . We hebben zo bewezen dat  $A_2(5, 3) = 4$  en dat er, op equivalentie in brede zin na, slechts één code deze grens bereikt. Zo zien we ook dat de Hamming grens niet steeds bereikt wordt. In een later hoofdstuk zullen we aantonen dat perfecte codes inderdaad zeer zeldzaam zijn.

Het bereikte resultaat kunnen we gebruiken om ook  $A_2(6, 4) = 4$  te bewijzen. Hiervoor gebruiken we volgende stelling.

**62 Stelling.** *Als  $d$  oneven is, bestaat er een binaire  $[n, M, d]$ -code **als en slechts als** er een binaire  $[n + 1, M, d + 1]$ -code bestaat.*

*Bewijs.* Vertrek met een binaire  $[n, M, d]$ -code  $C$  over  $A = \{0, 1\}$ . We voegen nu aan elk woord van  $C$  een letter toe zodanig dat het aantal symbolen “1” in elk verlengd woord even is (enkelvoudige pariteitscontrole). Doordat elk woord van de nieuwe code een even aantal symbolen “1” heeft, is de afstand tussen twee woorden (en dus ook de minimale afstand) even. Vermits  $d$  oneven is en de minimale afstand van de verlengde code minstens  $d$  is, moet hij  $d + 1$  zijn.

Neem twee codewoorden op minimale afstand in een  $[n + 1, M, d + 1]$ -code. Kies een plaats  $i$  waar deze twee woorden verschillen en schrap in elk woord de  $i$ -de letter. Je krijgt een  $[n, M, d]$ -code.  $\square$

**63 Gevolg.** *Als  $d$  oneven is, dan geldt  $A_2(n + 1, d + 1) = A_2(n, d)$ . Als  $d$  even is, dan geldt  $A_2(n - 1, d - 1) = A_2(n, d)$ .*

De unieke  $[5, 4, 3]$ -code  $C$  die we hoger construeerden kan beschouwd worden over het alfabet  $\mathbb{F}_2 = \{0, 1\}$ . Dan zien we dat deze code eigenlijk een *deelruimte* is van  $\mathbb{F}_2^5$ . Inderdaad:  $C = \text{vect}\{(1, 1, 1, 0, 0), (0, 0, 1, 1, 1)\}$ . We hebben hier een voorbeeld van de zeer belangrijke klasse der lineaire codes.

### 3.2 Lineaire codes

Als we veronderstellen dat het alfabet  $A$  van een code een lichaam  $\mathbb{F}_q$  is, dan heeft  $A^n$  de structuur van een  $n$ -dimensionale vectorruimte over  $\mathbb{F}_q$ . Bijgevolg kunnen we al onze kennis van de vectorruimten (zie cursus “meetkunde en lineaire algebra”) aanwenden bij de studie van zulke codes. Aangezien er enkel eindige lichamen bestaan waarvan het aantal elementen een priemmacht  $p^h$  is, lijkt deze veronderstelling een beperking. Ervaring leert daarentegen dat de meeste “goede” codes in een vectorruimte leven of eruit kunnen afgeleid worden.

**64 Definitie.** Een **lineaire**  $q$ -aire  $[n, k]$ -code  $C$  is een niet-nulle  $k$ -dimensionale deelruimte van  $\mathbb{F}_q^n$ . Soms noteert men ook  $[n, k, d]$ -code als de minimale afstand  $d$  van  $C$  gekend is. Een **genererende matrix** van  $C$  is een  $(n \times k)$ -matrix waarvan de kolommen een basis vormen van  $C$ .

De equivalentie in brede zin, zoals gedefinieerd in (56), bewaart de lineariteit niet. Daarom voeren we een meer beperkt begrip van equivalentie in.

**65 Definitie.** Twee lineaire codes van zelfde lengte over  $\mathbb{F}_q$  zijn **equivalent** indien ze equivalent zijn in brede zin en alle permutaties  $\sigma_i$  van de vorm  $x \mapsto \lambda_i x$  voor een zekere  $\lambda_i \in \mathbb{F}_q \setminus \{0\}$  zijn.

Door over te gaan op een equivalente code en de basis van  $\mathbb{F}_q^n$  goed te kiezen kunnen we er altijd voor zorgen dat de genererende matrix van een code de volgende **standaardvorm** aanneemt:

$$G = \left( \begin{array}{c} I_k \\ A \end{array} \right)$$

Een genererende matrix van een  $[n, k]$ -code is dus steeds een matrix van rang  $k$ .

Het **coderen** van informatie kan voor een lineaire code  $C$  eenvoudig gebeuren door vermenigvuldiging van matrices. Zij  $\mathbf{x} \in \mathbb{F}_q^k$  een informatievektor (i.e. een woord van  $k$  letters geschreven als kolom) en  $G$  een genererende matrix voor  $C$ . Dan is (bij afspraak) het codewoord dat overeenkomt met de informatie  $\mathbf{x}$  juist  $G\mathbf{x} \in \mathbb{F}_q^n$ . Als  $G$  bovendien de standaardvorm

$\left( \begin{array}{c} I_k \\ A \end{array} \right)$  heeft, staat de informatie steeds op de eerste  $k$  plaatsen van een codewoord. Dit helpt bij het decoderen.

Op de vectorruimte  $\mathbb{F}_q^n$  plaatsen we het gewone inproduct

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i \in \mathbb{F}_q$$

**66 Definitie.** Zij  $C \leq \mathbb{F}_q^n$  een code. De **duale code**  $C^\perp$  is de verzameling  $\{\mathbf{v} \in \mathbb{F}_q^n \mid \forall \mathbf{u} \in C : \mathbf{v} \cdot \mathbf{u} = 0\}$ .

**67 Lemma.** Zij  $G$  een genererende matrix van een  $[n, k]$ -code  $C$ , dan geldt  $\mathbf{v} \in C^\perp \iff {}^t G \mathbf{v} = \mathbf{0}$ .

*Bewijs.* Een vector staat loodrecht op alle vectoren van de deelruimte  $C$  als en slechts als hij loodrecht staat op alle vectoren van een voortbrengend deel van  $C$ . De kolommen van  $G$  geven juist zo een voortbrengend deel.  $\square$

**68 Lemma.** De duale van een lineaire  $[n, k]$ -code  $C$  is een  $[n, n - k]$ -code.

*Bewijs.* Vorige stelling leert dat  $C^\perp$  juist de kern is van de lineaire afbeelding

$$L_G: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^k: \mathbf{x} \longmapsto {}^t G \mathbf{x}$$

Bijgevolg is  $C^\perp$  een lineaire code en beëindigt de dimensiestelling voor lineaire afbeeldingen het bewijs.  $\square$

**69 Lemma.** Voor een lineaire code  $C$  geldt  $(C^\perp)^\perp = C$ .

*Bewijs.* Eén inclusie is triviaal en de andere volgt uit een dimensie-argument gebaseerd op vorig lemma.  $\square$

**70 Definitie.** Een genererende matrix voor de duale van een lineaire code  $C$  heet een **pariteitsmatrix** van  $C$ .

**71 Eigenschap.** Een genererende matrix  $G$  en een pariteitsmatrix  $H$  van een  $[n, k]$ -code  $C$  voldoen steeds aan

$${}^tGH = O_{k, n-k} \quad \text{en} \quad {}^tHG = O_{n-k, k}$$

*Bewijs.* Triviaal vermits alle kolommen van  $G$  loodrecht staan op alle kolommen van  $H$ . □

**72 Stelling.** Als  $G = \begin{pmatrix} I_k \\ A \end{pmatrix}$  de standaard genererende matrix van de  $[n, k]$ -code  $C$  is, dan is  $H = \begin{pmatrix} -{}^tA \\ I_{n-k} \end{pmatrix}$  een pariteitsmatrix voor  $C$ .

*Bewijs.* Het is gemakkelijk na te gaan dat  ${}^tGH = O_{k, n-k}$ , zodat de deelruimte opgespannen door de kolommen van  $H$  binnen  $C^\perp$  ligt. Maar bovendien is de rang van de matrix  $H$  gelijk aan  $n - k$ , de dimensie van  $C^\perp$ . □

**73 Definitie.** Het **gewicht**  $w(\mathbf{x})$  van een codewoord  $\mathbf{x} \in \mathbb{F}_q^n$  is de Hamming afstand  $d(\mathbf{0}, \mathbf{x})$ . Dit is het aantal niet-nulle coördinaten van  $\mathbf{x}$ .

**74 Lemma.** Voor de minimale afstand  $d$  van een lineaire code  $C$  geldt

$$d = \min \{w(\mathbf{x}) \mid \mathbf{x} \in C \setminus \{\mathbf{0}\}\}$$

**Taak.** Naast de grenzen van Hamming en Singleton bestaan er nog vele grenzen op de verschillende parameters van een (lineaire) code. Er is bijvoorbeeld nog de Plotkin grens, de Griesmer grens, de Gilbert-Varshamov grens, ... Zoek deze grenzen op en bewijs ze. Vergelijk ze met elkaar en pas ze toe op enkele voorbeelden.

**75 Stelling.** Zij  $C$  een lineaire code met pariteitsmatrix  $H$ . De minimale afstand van  $C$  is juist het minimaal aantal lineair afhankelijke rijen in  $H$ .

*Bewijs.* Schrijf de rijen van  $H = [h_{ij}]$  als vectoren  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n$ . Nu geldt

$$\begin{aligned} \mathbf{c} \in C &\iff {}^tH\mathbf{c} = \mathbf{0} \\ &\iff \forall i \in \{1, 2, \dots, n-k\} : \sum_{j=1}^n h_{ji}c_j = 0 \\ &\iff c_1\mathbf{h}_1 + c_2\mathbf{h}_2 + \dots + c_n\mathbf{h}_n = \mathbf{0} \end{aligned}$$

We zien dus dat de niet-nulle woorden van  $C$  aanleiding geven tot niet-nulle lineaire combinaties van de rijen van  $H$  die gelijk zijn aan de nulvector. Het minimaal aantal niet-nulle coëfficiënten in zulk een lineaire combinatie is juist het minimaal gewicht van een niet-nulle vector in  $C$ . □

**Opmerking.** Een andere formulering van de stelling luidt: de minimale afstand van  $C$  is  $\geq \delta$  **als en slechts als** elke  $\delta - 1$  rijen van  $H$  lineair onafhankelijk zijn.

**Oefening.** De ISBN code die we in hoofdstuk 1 leerden kennen is lineair. Bepaal zijn minimale afstand.

In de volgende paragrafen bestuderen we enkele bijzondere families lineaire codes.

### 3.3 Cyclische codes

**76 Definitie.** Een *cyclische code* is een lineaire code waar voor elk codewoord  $(c_0, c_1, \dots, c_{n-1})$  geldt dat  $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$  ook een codewoord is.

**Notatie.** Voor een vector  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$  noteren we de **rechtse shift**  $(a_{n-1}, a_0, a_1, \dots, a_{n-2})$  als  $\vec{\mathbf{a}}$ . We hebben dus  $\vec{a}_i = a_{i-1}$ , waarbij we de indices modulo  $n$  nemen.

Met een codewoord  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$  associëren we de veelterm  $a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in \mathbb{F}_q[X]$  die we  $\mathbf{a}(X)$  noteren. De shift naar rechts komt dan overeen met de vermenigvuldiging met  $X$ . We hebben inderdaad  $\vec{\mathbf{a}}(X) = X\mathbf{a}(X)$ , modulo  $X^n - 1$ . De algebraïsche behandeling van cyclische codes zal zich dus afspelen in de ring  $\mathbb{F}_q[X]/(X^n - 1)$ . Merk op dat  $X^n - 1$  reducibel is van zolang  $n > 1$ .

Voor een cyclische code  $C$  noteren we  $C(X)$  voor de verzameling van alle veeltermen geassocieerd met codewoorden van  $C$ .

**77 Lemma.** Voor een cyclische code  $C$  is  $C(X)$  een ideaal in  $\mathbb{F}_q[X]/(X^n - 1)$ .

*Bewijs.* Vermits  $C$  lineair is, zal de som van twee codewoorden  $\mathbf{a}$  en  $\mathbf{b}$  terug een codewoord zijn. Bijgevolg geldt  $\mathbf{a}(X) + \mathbf{b}(X) = (\mathbf{a} + \mathbf{b})(X) \in C(X)$ . De lineariteit geeft ook dat  $\lambda(\mathbf{a}(X)) \in C(X)$  voor elk codewoord  $\mathbf{a}$  en elke  $\lambda \in \mathbb{F}_q$ . Bovendien geldt  $X\mathbf{a}(X) \in C(X)$  daar  $C$  cyclisch is. Dit toont aan dat voor elke veelterm  $P \in \mathbb{F}_q[X]$  geldt dat  $P\mathbf{a}(X) \in C(X)$ , modulo  $X^n - 1$ .  $\square$

**78 Stelling.** Er bestaat een bijectie tussen de verzameling van cyclische codes van lengte  $n$  over  $\mathbb{F}_q$  en de verzameling van alle idealen van  $\mathbb{F}_q[X]/(X^n - 1)$ .

*Bewijs.* We hoeven enkel nog op te merken dat een ideaal aanleiding geeft tot een cyclische code.  $\square$

De studie van cyclische codes is dus equivalent met de studie van idealen in  $\mathbb{F}_q[X]/(X^n - 1)$ . De algebra leert ons dat deze idealen goed onder controle zijn.

**79 Lemma.** Elk ideaal in  $\mathbb{F}_q[X]/(X^n - 1)$  is een hoofdideaal.

*Bewijs.* Zij  $I$  een niet-nul ideaal in  $\mathbb{F}_q[X]/(X^n - 1)$  en zij  $G$  een veelterm in  $I$  met laagste graad. Voor elke  $F \in I$  geeft de Euklidische deling ons  $F = QG + R$  met  $\deg R < \deg G$ . Hieruit volgt  $R = F - QG \in I$ , waaruit volgt  $R = 0$ .  $\square$

**Opmerking.** De veelterm  $G$  van vorig lemma is niet uniek, maar er is wel een unieke *monische* veelterm die  $(G)$  voortbrengt. Veronderstel inderdaad dat  $G_1$  en  $G_2$  beide monisch zijn en dat  $(G_1) = (G_2)$ . Bovendien eisen we dat  $G_1$  en  $G_2$  de laagste graad hebben in  $(G_1) = (G_2)$ . Dus hebben beide veeltermen dezelfde graad  $k$  en dezelfde hoogstegraadscoëfficiënt gelijk aan 1. Hieruit volgt dat  $\deg(G_2 - G_1) < k$ . Maar dit verschil behoort tot het ideaal  $(G_1)$  waarin geen enkel element een graad lager dan  $k$  kan hebben.

**80 Definitie.** Voor een hoofdideaal  $I = (G)$  heet  $G$  een **generator** van  $I$ . Voor een cyclische code  $C$  zullen we een generator van  $C(X)$  ook een **generator van de code**  $C$  noemen. We nemen bij afspraak steeds een monische generator die we dan de generator noemen.

**81 Stelling.** De generator  $G$  van een ideaal in  $\mathbb{F}_q[X]/(X^n - 1)$  is een deler van  $X^n - 1$ .

*Bewijs.* De Euklidische deling geeft  $X^n - 1 = QG + R$  met  $\deg R < \deg G$ . Maar dan geldt  $R \equiv -QG \pmod{X^n - 1}$  zodat  $R \in (G)$ . Dit is een tegenspraak, tenzij  $R = 0$ .  $\square$

We noteren het quotiënt  $\frac{X^n - 1}{G}$  met  $H \in \mathbb{F}_q[X]/(X^n - 1)$  en kunnen (voor een zekere  $k$ ) schrijven

$$\begin{aligned} G &= g_0 + g_1X + \dots + g_{n-k}X^{n-k} \\ H &= h_0 + h_1X + \dots + h_kX^k \end{aligned}$$

Vermits we  $G$  monisch nemen en vermits  $GH = X^n - 1$ , geldt dat  $g_{n-k} = h_k = 1$  en dat  $g_0h_0 = -1$ . Bovendien hebben we ook

$$\begin{aligned} g_0h_1 + g_1h_0 &= 0 \\ g_0h_2 + g_1h_1 + g_2h_0 &= 0 \\ &\vdots \end{aligned}$$

Aangezien  $(G)$  een cyclische code  $C$  voorstelt, is  $\mathbf{g}_0 := (g_0, g_1, \dots, g_{n-k}, 0, \dots, 0)$  een codewoord (van lengte  $n$ ). Ook alle shifts  $\mathbf{g}_i := \vec{\mathbf{g}}_{i-1}$  voor  $i \in \{1, 2, \dots, k-1\}$  zijn codewoorden. Bovendien zijn deze lineair onafhankelijk door de nullen achteraan. We tonen nu dat alle codewoorden lineaire combinaties zijn van  $\mathbf{g}_0$  en deze  $k-1$  shifts.

Zij  $\mathbf{a} \in C$ . Door (het bewijs van) stelling (78) weten we dat  $\mathbf{a}(X) \in (G)$ , zodat

$$\begin{aligned} \mathbf{a}(X) &= QG = (q_0 + q_1X + \dots + q_{k-1}X^{k-1})(g_0 + g_1X + \dots + g_{n-k}X^{n-k}) \\ &= q_0G + q_1(XG) + \dots + q_{k-1}(X^{k-1}G) \end{aligned}$$

Dus geldt  $\mathbf{a} = q_0\mathbf{g}_0 + q_1\mathbf{g}_1 + \dots + q_{k-1}\mathbf{g}_{k-1}$ .

Nu zien we dat de notatie  $n-k$  voor de graad van  $G$  goed gekozen was. We hebben nu immers dat  $\dim C = k$ , onze gewoonlijke notatie.

We hebben net bewezen dat

$$\begin{pmatrix} g_0 & 0 & 0 & \dots & \dots & 0 \\ g_1 & g_0 & 0 & \dots & \dots & 0 \\ g_2 & g_1 & g_0 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ g_{n-k} & g_{n-k-1} & g_{n-k-2} & \ddots & \ddots & \vdots \\ 0 & g_{n-k} & g_{n-k-1} & \ddots & \ddots & \vdots \\ 0 & 0 & g_{n-k} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \dots & g_{n-k} \end{pmatrix}$$

een genererende matrix is voor de cyclische code  $C$  gegenereerd door de veelterm  $G = g_0 + g_1X + \dots + g_{n-k}X^{n-k}$ .

**82 Stelling.** Als  $X^n - 1 = GH$ , dan is

$$\begin{pmatrix} h_k & 0 & 0 & \dots & \dots & 0 \\ h_{k-1} & h_k & 0 & \dots & \dots & 0 \\ h_{k-2} & h_{k-1} & h_k & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ h_0 & h_1 & h_2 & \ddots & \ddots & \vdots \\ 0 & h_0 & h_1 & \ddots & \ddots & \vdots \\ 0 & 0 & h_0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \dots & h_0 \end{pmatrix}$$

een pariteitsmatrix van de code die overeenkomt met het ideaal  $(G)$ .

*Bewijs.* De afmetingen van de matrix kloppen. Ook zijn de kolommen van de matrix lineair onafhankelijk zodat zij een deelruimte van dimensie  $n-k$  voortbrengen. Er blijft na te kijken dat de kolommen  $\mathbf{h}_j$  (met  $0 \leq j < n-k$ , ja nu nummeren we kolommen vanaf nul) van deze matrix loodrecht staan op de vectoren  $\mathbf{g}_i$  (met  $0 \leq i < k$ ). Voor het gemak stellen we

$g_{n-k+1} = g_{n-k+2} = \dots = g_{n-1} = 0$  en  $h_{k+1} = h_{k+2} = \dots = h_{n-1} = 0$  en interpreteren we de indices nu even modulo  $n$ . Dan geldt

$$\mathbf{g}_i \cdot \mathbf{h}_j = \sum_{l=0}^{n-1} g_{l-i} h_{k+j-l} = \sum_{\substack{r,s \in \{0, \dots, n-1\} \\ r+s=k-i+j}} g_r h_s$$

Maar deze laatste som is de coëfficiënt van  $X^{k-i+j}$  in het product  $GH$ . Deze is steeds nul, tenzij  $k-i+j = n$  of  $k-i+j = 0$ .  $\square$

**Voorbeeld.** Geef alle binaire cyclische codes van lengte 7?

Het volstaat  $X^7 - 1$  te factoriseren:

$$X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

We zien dus dat  $X^7 - 1$  acht delers heeft, waarvan zes niet-triviaal. Deze bepalen eenduidig de acht cyclische codes van lengte 7 over  $\mathbb{F}_2$ .

De code die overeenkomt met de triviale veelterm 1 is de deelruimte voortgebracht door het woord 1000000 en zijn rechtse shifts. Het is dus de volledige vectorruimte  $\mathbb{F}_2^7$ .

De veelterm  $X + 1$  geeft de code voortgebracht door 1100000 en de shifts ervan. Deze code bestaat uit alle woorden van even gewicht. Hij heeft dimensie 6 en minimale afstand 2.

Geassocieerd met de veelterm  $X^3 + X + 1$  vinden we de code die bestaat uit het nulle woord, het woord 1101000 en zijn shifts, samen met alle woorden die men bekomt door in de bestaande woorden "0" en "1" te verwisselen. Deze 16 woorden vormen een code van dimensie 4 en minimale afstand 3. We merken op dat deze code equivalent is met de perfecte code van sectie 1.4.

De code bepaald door het ideaal  $(X^3 + X^2 + 1)$  wordt bekomen uit de vorige code door de woorden achterstevoren op te schrijven. Hij is dus equivalent met deze code.

Voor  $(X + 1)(X^3 + X + 1)$  krijgen we de woorden van even gewicht in de code van  $X^3 + X + 1$ . Deze code heeft minimaal gewicht 4.

Achterstevoren opschrijven van de woorden van vorige code geeft de code van  $(X + 1)(X^3 + X^2 + 1)$ .

Het ideaal  $(X^6 + X^5 + \dots + X + 1)$  geeft aanleiding tot de repetitiecode voortgebracht door het woord 1111111.

Voor  $X^7 - 1$  vinden we geen echte code omdat de overeenkomstige deelruimte enkel de nulvector bevat.

### 3.4 BCH codes

In vorige paragraaf zagen we een handige manier om lineaire codes te maken van gegeven lengte. Hun dimensie (en dus informatieverhouding) was gemakkelijk te bepalen. De minimale afstand vinden is daarentegen veel moeilijker. Nu geven we een constructie om een gegeven minimale afstand te bereiken. Bovendien krijgen we een bovengrens op de dimensie van deze codes.

BCH is een afkorting voor de namen van de drie auteurs die betrokken zijn bij de ontwikkeling van deze codes: Bose, Ray-Chaudhuri en Hocquenghem. De BCH codes werden onafhankelijk ingevoerd door BOSE en RAY-CHAUDHURI<sup>1</sup> en door HOCQUENGHEM<sup>2</sup>.

Eerst geven we nog enkele nuttige eigenschappen van eindige lichamen.

**83 Definitie.** Zij  $n$  en  $q$  getallen die relatief priem zijn. De **orde** van  $q$  modulo  $n$  is het kleinste niet-nul getal  $e$  zodanig dat  $q^e \equiv 1 \pmod{n}$ .

**Opmerking.** Doordat  $n$  en  $q$  relatief priem zijn, is  $q$  geen nuldeeler in  $\mathbb{Z}/n\mathbb{Z}$ . De orde is dus gewoon de orde van  $q$  in de eenhedengroep van de ring  $\mathbb{Z}/n\mathbb{Z}$ .

**84 Definitie.** Zij  $n \in \mathbb{N}_0$ . Een **primitieve  $n$ -de eenheidswortel** in een veld  $\mathbb{F}$  is een element  $a$  van  $\mathbb{F}$  van multiplicatieve orde  $n$ . Er geldt dus  $a^n = 1$  maar  $a^m \neq 1$  voor  $0 < m < n$ .

<sup>1</sup>R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.

<sup>2</sup>A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

**85 Lemma.** *Zij  $q = p^h$  een priemmacht en stel  $e$  gelijk aan de orde van  $q$  modulo een natuurlijk getal  $n$ . Het kleinste lichaam dat  $\mathbb{F}_q$  omvat en een primitieve  $n$ -de eenheidswortel bevat, is  $\mathbb{F}_{q^e}$ .*

*Bewijs.* Merk eerst op dat elk lichaam dat  $\mathbb{F}_q$  omvat isomorf moet zijn met  $\mathbb{F}_{q^m}$  voor een zekere  $m \in \mathbb{N}_0$ . Indien  $\mathbb{F}_{q^m}$  bovendien een primitieve  $n$ -de eenheidswortel bevat, omvat  $\mathbb{F}_{q^m}^\times$  een deelgroep van orde  $n$ . Dit impliceert dat  $n \mid q^m - 1$ .

Omgekeerd, als  $n \mid q^m - 1$ , dan omvat  $\mathbb{F}_{q^m}^\times$  een deelgroep van orde  $n$ , zodat er een primitieve  $n$ -de eenheidswortel is.  $\square$

Kies nu  $q = p^h$  een priemmacht,  $n$  een natuurlijk getal met  $\text{ggd}(n, q) = 1$ . Stel  $e$  gelijk aan de orde van  $q$  modulo  $n$  en zij  $a$  een primitieve  $n$ -de eenheidswortel in  $\mathbb{F}_{q^e}$ . Verder nemen we nog een natuurlijk getal  $\delta \leq n$ . We zagen in hoofdstuk 2 dat  $\mathbb{F}_q \cong \mathbb{F}_p[X]/(F)$  waarbij  $F$  een irreduciebele veelterm is van graad  $h$  over  $\mathbb{F}_p$ . Er is natuurlijk een analoge constructie voor  $\mathbb{F}_{q^e}$  met een irreduciebele veelterm  $G$  van graad  $e$  over  $\mathbb{F}_q$ . We hebben  $\mathbb{F}_{q^e} \cong \mathbb{F}_q[X]/(G)$ . Op deze manier kunnen we  $\mathbb{F}_{q^e}$  zien als een  $e$ -dimensionale vectorruimte over  $\mathbb{F}_q$ .

Stel nu

$$H := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a & a^2 & a^3 & \cdots & a^{\delta-1} \\ a^2 & a^4 & a^6 & \cdots & a^{2(\delta-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ a^{n-1} & a^{2(n-1)} & a^{3(n-1)} & \cdots & a^{(\delta-1)(n-1)} \end{pmatrix} \in M_{n, \delta-1}(\mathbb{F}_{q^e})$$

We kunnen deze matrix  $H$  beschouwen over  $\mathbb{F}_q$  door zijn elementen voor te stellen als vectoren van  $\mathbb{F}_{q^e}$ . We stellen de vector die overeenkomt met  $x \in \mathbb{F}_{q^e}$  voor door  $[x]$ . Als het element  $a \in \mathbb{F}_{q^e}$  bijvoorbeeld overeenkomt met  $[a] = (a_1, a_2, \dots, a_e) \in \mathbb{F}_q^e$ , zullen we in de matrix in de tweede rij beginnen met  $a_1 \ a_2 \ \cdots \ a_e$  in plaats van  $a$ . Doen we dit voor alle elementen, krijgen we uiteindelijk een  $(n \times e(\delta - 1))$ -matrix  $\bar{H}$  over  $\mathbb{F}_q$  die kan beschouwd worden als pariteitsmatrix voor een code van lengte  $n$ .

$$\bar{H} = \begin{pmatrix} [1] & [1] & [1] & \cdots & [1] \\ [a] & [a^2] & [a^3] & \cdots & [a^{\delta-1}] \\ [a^2] & [a^4] & [a^6] & \cdots & [a^{2(\delta-1)}] \\ \vdots & \vdots & \vdots & & \vdots \\ [a^{n-1}] & [a^{2(n-1)}] & [a^{3(n-1)}] & \cdots & [a^{(\delta-1)(n-1)}] \end{pmatrix} \in M_{n, e(\delta-1)}(\mathbb{F}_q)$$

**86 Definitie.** *De BCH code van lengte  $n$  en parameter  $\delta$  is de code  $\ker L_{\bar{H}}$ .*

We herhalen een beroemd resultaat uit de theorie der determinanten (zie cursus “meetkunde en lineaire algebra”).

**87 Lemma** (“Vandermonde determinanten”). *Zij  $\lambda_1, \lambda_2, \dots, \lambda_n$  twee aan twee verschillende elementen van een veld  $\mathbb{F}$ . Dan geldt*

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\ \vdots & \vdots & & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_n^{n-1} \end{pmatrix} \neq 0$$

**Een beetje geschiedenis** Alexandre Théophile Vandermonde werd geboren te Parijs in 1735 en stierf aldaar in 1796. Zijn wiskundige publicaties verschenen alle in de jaren 1771–72 en in geen enkele wordt verwezen naar ‘zijn determinanten’. Het is wel zeer normaal dat een determinant(formule) zijn naam draagt aangezien één van zijn artikels kan beschouwd worden als de eerste volledige uiteenzetting van de theorie der determinanten (die ouder is dan de matrixtheorie). In zijn later leven speelde Vandermonde een belangrijke rol in de Franse Revolutie.

**88 Stelling.** *De BCH code van lengte  $n$  en parameter  $\delta$  over  $\mathbb{F}_q$  heeft minstens  $\delta$  als minimale afstand en heeft minstens dimensie  $n - e(\delta - 1)$ .*

*Bewijs.* Volgens stelling (75) moeten we eerst aantonen dat elke  $\delta - 1$  rijen van de matrix  $\bar{H}$  lineair onafhankelijk zijn. Zijn rijen  $m_1, m_2, \dots, m_{\delta-1}$  lineair afhankelijk, dan bestaan er coëfficiënten  $\lambda_1, \lambda_2, \dots, \lambda_{\delta-1} \in \mathbb{F}_q$ , niet allemaal nul, zodat

$$\lambda_1 \bar{\mathbf{h}}_{m_1} + \lambda_2 \bar{\mathbf{h}}_{m_2} + \dots + \lambda_{\delta-1} \bar{\mathbf{h}}_{m_{\delta-1}} = \mathbf{0}$$

Nu bestaat een rij van  $\bar{H}$  uit  $\delta - 1$  groepjes van  $e$  elementen van  $\mathbb{F}_q$  die elementen van  $\mathbb{F}_{q^e}$  voorstellen. Als gevolg van het isomorfisme  $\mathbb{F}_q^e \cong \mathbb{F}_{q^e}$  moet dan ook gelden dat dezelfde lineaire combinatie van de overeenkomstige rijen in  $H$  de nulvector is. We hebben dus

$$\lambda_1 \mathbf{h}_{m_1} + \lambda_2 \mathbf{h}_{m_2} + \dots + \lambda_{\delta-1} \mathbf{h}_{m_{\delta-1}} = \mathbf{0}$$

zodat die rijen lineair afhankelijk zijn in  $\mathbb{F}_{q^e}^{\delta-1}$ , omdat de coëfficiënten, die in  $\mathbb{F}_q$  zitten, ook kunnen beschouwd worden als elementen van  $\mathbb{F}_{q^e}$ . Dit alles zou tot gevolg hebben dat de determinant

$$\det \begin{pmatrix} a^{m_1} & a^{2m_1} & \dots & a^{(\delta-1)m_1} \\ a^{m_2} & a^{2m_2} & \dots & a^{(\delta-1)m_2} \\ \vdots & \vdots & \ddots & \vdots \\ a^{m_{\delta-1}} & a^{2m_{\delta-1}} & \dots & a^{(\delta-1)m_{\delta-1}} \end{pmatrix}$$

nul moet zijn, in tegenspraak met vorig lemma.

De dimensie van de code  $\ker L_{\bar{H}}$  is  $n - \text{rang}(\bar{H})$  en de rang van  $\bar{H}$  is ten hoogste het aantal kolommen  $e(\delta - 1)$ .  $\square$

Even een algebraïsch intermezzo... We weten al sinds lemma (32) dat een veelterm  $F \in \mathbb{F}[X]$  nul wordt in  $a \in \mathbb{F}$  als en slechts als  $(X - a) \mid F$ . Nu is  $X - a$  de veelterm met laagste graad die nul wordt in  $a$ . Als nu  $a \notin \mathbb{F}$ , is  $X - a \notin \mathbb{F}[X]$ . Onderstel dat  $a$  wel behoort tot een lichaamsuitbreiding van  $\mathbb{F}$ , bestaan er dan veeltermen in  $\mathbb{F}[X]$  die nul worden in  $a$ ? Een klassiek voorbeeld is  $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$  dat nulpunt is van  $X^2 - 2 \in \mathbb{Q}[X]$ . Ook  $i \in \mathbb{C} \setminus \mathbb{R}$  is een wortel van de bekende veelterm  $X^2 + 1 \in \mathbb{R}[X]$  (of  $\mathbb{Q}[X]$ ). In beide gevallen hebben de gegeven veeltermen de laagst mogelijke graad voor de gevraagde eigenschap.

**89 Definitie.** Zij  $\mathbb{F}_1 \leq \mathbb{F}_2$  twee velden en  $a \in \mathbb{F}_2$ . We zeggen dat  $a$  **algebraïsch** is over  $\mathbb{F}_1$  als er een veelterm  $F \in \mathbb{F}_1[X]$  bestaat met  $F(a) = 0$ . Anders heet  $a$  **transcendent** over  $\mathbb{F}_1$ .

In een cursus algebra heb je zeker al bewezen dat  $\pi$  en  $e$  transcendent zijn over  $\mathbb{Q}$ . Indien dat niet het geval is, kan je hierover een leuk taakje maken.

**Taak.** Bewijs de transcendentie van  $\pi$  of  $e$  over  $\mathbb{Q}$ . Inspireer je bijvoorbeeld van [11].

In het eindige geval is de situatie veel aangenamer. Uit gevolg (47) volgt onmiddellijk volgende stelling.

**90 Stelling.** Zij  $\mathbb{F}$  een eindig lichaam van karakteristiek  $p$ . Elk element van  $\mathbb{F}$  is algebraïsch over  $\mathbb{F}_p$ .

**91 Definitie.** Zij  $a$  algebraïsch over  $\mathbb{F}$ . De monische veelterm met laagste graad in  $\mathbb{F}[X]$  die nul wordt in  $a$  heet **minimale veelterm** van  $a$ . We noteren deze veelterm  $M_a$ .

**Opmerking.** Uit lemma (32) volgt onmiddellijk dat een minimale veelterm over een lichaam  $\mathbb{F}$  irreduciebel moet zijn over  $\mathbb{F}$ .

Terug naar de codes ! De definitie toont het niet, maar toch geldt volgende stelling.

**92 Stelling.** BCH codes zijn cyclisch.

*Bewijs.* Zoals in vorige paragraaf noteren we de veelterm geassocieerd met een codewoord  $\mathbf{c} = c_0 c_1 \dots c_{n-1}$  met  $\mathbf{c}(X)$ . De voorwaarden om tot de code te behoren lezen we af uit de matrix  ${}^t \bar{H}$  en zijn van de vorm

$$\mathbf{c}(a^i) = c_0 + c_1 a^i + \dots + c_{n-1} a^{i(n-1)} = 0$$

voor  $i \in \{1, 2, \dots, \delta - 1\}$ . Stel  $G$  gelijk aan het kleinste gemeen veelvoud van de minimale veeltermen over  $\mathbb{F}_q$  van de machten  $a, a^2, \dots, a^{\delta-1}$ . Dan behoort  $\mathbf{c}$  tot de BCH code  $\ker L_{\bar{H}}$  als en slechts als  $\mathbf{c}(X)$  deelbaar is door  $G$ . Bovendien zijn de wortels van  $G$  juist  $n$ -de eenheidswortels, zodat  $G \mid X^n - 1$ . De beschouwde BCH code is dus cyclisch met generator  $G$ .  $\square$

**Taak.** Vermits de BCH codes cyclisch zijn, hebben ze generatoren. Kan je deze vinden? Je mag de literatuur raadplegen en moet een bewijs geven.

Het bewijs van vorige stelling kan ons helpen bij het verbeteren van de ondergrens van stelling (88) op de dimensie van een BCH code. Het aantal voorwaarden op de codewoorden bepalen de dimensie van de code. Een woord  $\mathbf{c} = c_0c_1 \cdots c_{n-1}$  behoort tot de beschouwde BCH code als en slechts als de machten  $a^i$  voor  $i \in \{1, 2, \dots, \delta - 1\}$  alle wortel zijn van de veelterm  $\mathbf{c}(X)$ . Deze  $\delta - 1$  voorwaarden zijn misschien niet alle onafhankelijk.

**Opmerking.** Eigenlijk zijn er  $e(\delta - 1)$  voorwaarden op de letters  $c_0, c_1, \dots, c_{n-1}$  van een codewoord. Door weer in  $\mathbb{F}_{q^e} \geq \mathbb{F}_q$  te werken kunnen we dit korter schrijven als  $\delta - 1$  voorwaarden over  $\mathbb{F}_{q^e}$ .

Volgend lemma is nuttig.

**93 Lemma.** *Zij  $F$  een veelterm met coëfficiënten in  $\mathbb{F}_q$ . Indien  $w$  een wortel is van  $F$ , beschouwd als veelterm over een uitbreiding  $\mathbb{F}_{q^r}$  van  $\mathbb{F}_q$ , dan is  $w^q$  ook een wortel van  $F$ .*

*Bewijs.* Zij  $q = p^h$  met  $p$  een priemgetal. Dan is de afbeelding  $x \mapsto x^q$  de  $h$ -de macht van het Frobenius automorfisme  $\phi$  in  $\mathbb{F}_{q^r}$ . Als  $F = \sum_{i=0}^n a_i X^i$  met alle  $a_i \in \mathbb{F}_q$ , hebben we  $F(w) = \sum_{i=0}^n a_i w^i = 0$ , waarop we  $\phi^h$  kunnen toepassen zodat we krijgen  $\sum_{i=0}^n a_i (w^q)^i = 0$ . Maar door gevolg (47) hebben we voor elke  $i \in \{0, 1, \dots, n\}$  dat  $a_i^q = a_i$ . We zien dus dat  $\sum_{i=0}^n a_i (w^q)^i = 0$ , zodat ook  $w^q$  een wortel is van  $F$ .  $\square$

Als we dus twee getallen  $i$  en  $j$  vinden met  $j \equiv iq^m \pmod{n}$  voor een zekere  $m$ , dan kunnen we uit vorig lemma afleiden dat indien  $a^i$  een wortel is van de veelterm  $\mathbf{c}(X)$ , dan automatisch ook  $a^j = (a^i)^{q^m}$ . Dus zal de voorwaarde  $\mathbf{c}(a^j) = 0$  geen bijkomende beperking zijn op de keuze van  $\mathbf{c}$ . Bijgevolg is de  $j$ -de kolom van de matrix  $H$  overbodig om de code  $C = \ker L_{\bar{H}}$  te bepalen. De rang van  $\bar{H}$  wordt dus kleiner, zodat de (ondergrens op de) dimensie van  $C$  groter wordt.

**Voorbeeld.** Beschouw de binaire BCH code  $C$  van lengte 15 en parameter 5. Dan corresponderen de codewoorden met de veeltermen die nul worden in  $a, a^2, a^3$  en  $a^4$ , waarbij  $a$  een primitieve 15-de eenheidswortel is in  $\mathbb{F}_{2^4}$  (omdat de orde van 2 modulo 15 gelijk is aan 4). Deze code heeft minimaal gewicht 5 en kan dus twee fouten verbeteren. De ondergrens van stelling (88) geeft  $\dim C \geq 15 - 4 \cdot 4 = -1$ , wat natuurlijk waardeloos is!

Uit lemma (93) leren we echter dat zodra  $a \in \mathbb{F}_{16}$  wortel is van een veelterm in  $\mathbb{F}_2[X]$ , de elementen  $a^2$  en  $a^4$  ook wortel zijn. Bijgevolg verdwijnen twee kolommen in de matrix die  $C$  definieert over  $\mathbb{F}_{16}$ . Dit betekent dat er in de pariteitsmatrix van  $C$  over  $\mathbb{F}_2$  acht kolommen verdwijnen, zodat zijn rang hoogstens 8 kan zijn. Het gevolg is dat  $\dim C \geq 15 - 8 = 7$ . We zien dus dat  $C$  minstens 128 woorden bevat.

Het bewijs van stelling (92) toont dat het kleinste gemeen veelvoud van de minimale veeltermen van  $a$  en  $a^3$  een generator van  $C$  oplevert. De ontbinding van  $X^{15} - 1$  over  $\mathbb{F}_2$  levert een irreduciebele factor  $X^4 + X + 1$  (controleer dit!). Deze veelterm kan gebruikt worden om de uitbreiding  $\mathbb{F}_{2^4}$  te construeren, waarin een wortel  $a$  van deze veelterm een primitieve 15-de eenheidswortel is. Dan is  $a^3$  een 5-de eenheidswortel zodat deze macht van  $a$  een wortel is van de (over  $\mathbb{F}_2$ ) irreduciebele veelterm  $X^4 + X^3 + X^2 + X + 1$ . De irreducibiliteit van deze twee veeltermen leert ons dat het kleinste gemeen veelvoud van de minimale veeltermen van  $a$  en  $a^3$  juist het product  $(X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$  moet zijn. Dus heeft  $C$  een generator van graad 8. Op bladzijde 3-6 merkten we op dat de graad van de generator  $n - k$  bedraagt, met  $n$  de lengte en  $k$  de dimensie van de cyclische code. Bijgevolg is de dimensie van  $C$  juist  $15 - 8 = 7$ . Onze ondergrens is bereikt!

We merken even op dat de Hamming grens voor een binaire code van lengte 15 die twee fouten verbetert ons leert dat  $|C| \leq 2^{15} / (1 + 15 + \binom{15}{2}) \approx 270.81$ . Aangezien  $C$  een lineaire code is, moet het aantal codewoorden een macht van twee zijn zodat we krijgen  $|C| \leq 256 = 2^8$ . Dus scheelt de dimensie van onze BCH code slechts weinig van de best mogelijke.

Een belangrijke klasse van BCH codes zijn de zogenaamde **Reed-Solomon codes**. Deze werden eerder ontdekt en komen overeen met het geval dat  $n = q - 1$ . In dat geval is de orde van  $q$  modulo  $n$  duidelijk gelijk aan 1. Dan levert de grens van stelling (88) dat de dimensie van een Reed-Solomon code  $C$  minstens  $n - \delta + 1$  bedraagt, waarbij  $\delta$  de parameter is. Als we de minimale afstand van  $C$  met  $d$  noteren, weten we dat  $d \geq \delta$ . De Singleton grens van stelling (61) levert  $|C| \leq q^{n-d+1}$ , zodat  $\dim C \leq n - d + 1$ . We krijgen dus

$$n - d + 1 \leq n - \delta + 1 \leq \dim C \leq n - d + 1$$

waaruit we afleiden dat  $d = \delta$  en  $\dim C = n - d + 1$ . Bijgevolg zijn de Reed-Solomon codes voorbeelden van MDS codes.

# Hoofdstuk 4

## Perfecte codes

Nu concentreren we ons op codes die de Hamming grens bereiken.

### 4.1 Perfecte binaire codes die één fout verbeteren

**94 Definitie.** De elementen  $\mathbf{c}$  van  $\mathbb{F}_2^n$  kunnen we interpreteren als karakteristieke vectoren van deelverzamelingen van een verzameling van  $n$  elementen. Deze deelverzameling noemen we de **drager** van  $\mathbf{c}$  en noteren we  $\text{supp}(\mathbf{c})$ . Als verzameling van  $n$  elementen nemen we dikwijls  $\Omega_n := \{1, 2, \dots, n\}$ . Dan is  $\text{supp}(\mathbf{c}) = \{i \in \Omega_n \mid c_i \neq 0\}$ .

**95 Lemma.** De drager laat toe vectoriële bewerkingen te vertalen naar verzamelingen.

(i)  $\forall \mathbf{x} \in \mathbb{F}_2^n: w(\mathbf{x}) = |\text{supp}(\mathbf{x})|$

(ii)  $\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n: \langle \mathbf{x}, \mathbf{y} \rangle = |\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})|$  en  $\mathbf{x} \cdot \mathbf{y} = |\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})| \pmod{2}$

(iii)  $\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n: w(\mathbf{x} + \mathbf{y}) = |\text{supp}(\mathbf{x}) \Delta \text{supp}(\mathbf{y})| = w(\mathbf{x}) + w(\mathbf{y}) - 2|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})| = w(\mathbf{x}) + w(\mathbf{y}) - 2\langle \mathbf{x}, \mathbf{y} \rangle$

**Opmerking.** In deze cursus gebruiken we (meestal op  $\mathbb{F}_2^n$ ) twee inproducten door elkaar. Er geldt op  $\mathbb{F}_2^n$  dat  $\mathbf{x} \cdot \mathbf{y} = \langle \mathbf{x}, \mathbf{y} \rangle \pmod{2}$  en we hebben  $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$  als we de coördinaten  $x_i$  en  $y_i$  beschouwen als gehele (of reële) getallen.

**96 Lemma.** Een lineaire binaire perfecte code  $C$  is voortgebracht door zijn woorden van minimaal gewicht.

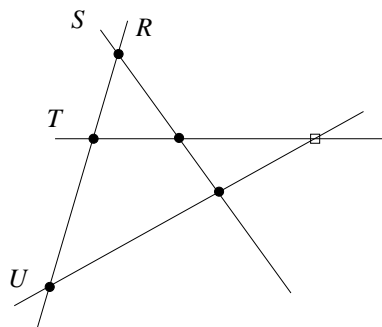
*Bewijs.* Neem  $\mathbf{c} \in C$ . Als  $w(\mathbf{c}) = 2e + 1$ , het minimaal gewicht van  $C$ , is er niets te bewijzen. Als  $w(\mathbf{c}) > 2e + 1$ , kiezen we  $e + 1$  elementen in de drager  $\text{supp}(\mathbf{c})$  en stellen we  $\mathbf{e}$  gelijk aan de karakteristieke vector van die  $e + 1$  elementen. Vermits  $C$  perfect is, bestaat er een uniek codewoord  $\mathbf{x}$  op afstand  $\leq e$  van  $\mathbf{e}$ . Dit codewoord is niet de nulvector zodat  $w(\mathbf{x}) \geq 2e + 1$ . Maar dan moet  $|\text{supp}(\mathbf{e}) \cap \text{supp}(\mathbf{x})| \leq e + 1$  zodat  $\mathbf{x}$  op ten minste  $e$  plaatsen buiten  $\text{supp}(\mathbf{e})$  een 1 moet hebben. Bijgevolg hebben we  $d(\mathbf{e}, \mathbf{x}) \geq e$  zodat  $d(\mathbf{e}, \mathbf{x}) = e$ . Dus heeft  $\mathbf{x}$  op juist  $e$  plaatsen buiten  $\text{supp}(\mathbf{e})$  een 1 en ook juist op de plaatsen van  $\text{supp}(\mathbf{e})$  een 1. Het gewicht van  $\mathbf{x}$  is dus  $2e + 1$  en er geldt  $\text{supp}(\mathbf{e}) \subset \text{supp}(\mathbf{x})$ .

Nu bekijken we  $w(\mathbf{c} + \mathbf{x}) = w(\mathbf{c}) + w(\mathbf{x}) - 2|\text{supp}(\mathbf{c}) \cap \text{supp}(\mathbf{x})|$  en merken op dat  $|\text{supp}(\mathbf{c}) \cap \text{supp}(\mathbf{x})| \geq e + 1$ . Hieruit volgt dat  $w(\mathbf{c} + \mathbf{x}) \leq w(\mathbf{c}) + (2e + 1) - 2(e + 1) = w(\mathbf{c}) - 1 < w(\mathbf{c})$ . Dus is  $\mathbf{c} + \mathbf{x}$  een codewoord dat lichter is dan  $\mathbf{c}$ . We kunnen zo verder gaan en woorden van minimaal gewicht blijven aftrekken tot het resultaat een woord van minimaal gewicht is.  $\square$

We herhalen de axiomatische definitie van een projectieve ruimte en een paar andere begrippen (zie cursus “Affiene en projectieve meetkunde”).

**97 Definitie.** Een **axiomatische projectieve ruimte** bestaat uit een niet-lege verzameling  $\mathcal{P}$  van **punten** en een niet-lege verzameling  $\mathcal{L}$  van deelverzamelingen van  $\mathcal{P}$  die men **rechten** noemt. Bovendien zijn volgende axioma's voldaan.

- (PR1) Twee punten bepalen steeds een rechte;
- (PR2) Twee verschillende rechten hebben hoogstens één gemeenschappelijk punt;
- (PR3) Zij  $R, S, T, U$  verschillende rechten zodanig dat  $R$  en  $S$  snijden,  $T$  en  $U$  allebei zowel  $R$  als  $S$  snijden in verschillende punten (zie figuur), dan snijden  $T$  en  $U$  ook;
- (PR4) Elke rechte bevat minstens drie punten;
- (PR5) Er zijn minstens drie niet-collineaire punten.



**98 Definitie.** In een axiomatische projectieve ruimte  $(\mathcal{P}, \mathcal{L})$  heet een deelverzameling  $\mathcal{P}'$  van  $\mathcal{P}$  **projectief gesloten** indien voor alle  $x \neq y \in \mathcal{P}'$  geldt dat de rechte door  $x$  en  $y$  omvat is door  $\mathcal{P}'$ . De kleinste projectief gesloten verzameling die een gegeven deel  $D \subset \mathcal{P}$  omvat heet de **projectieve sluiting** van  $D$  en noteren we  $\text{proj} D$ .

Een verzameling punten  $S = \{p_1, p_2, \dots, p_n\}$  in een projectieve ruimte heet **projectief onafhankelijk** indien voor elke  $i \in \{1, 2, \dots, n\}$  geldt  $p_i \notin \text{proj}(S \setminus \{p_i\})$ .

**99 Lemma.** In een projectieve ruimte hebben alle maximale projectief onafhankelijke verzamelingen evenveel elementen.

**100 Definitie.** De cardinaliteit van een maximale projectief onafhankelijke verzameling in een projectieve ruimte heet **dimensie** van die ruimte.

Het bewijs van volgende stelling hoort thuis in een cursus projectieve meetkunde maar kan als taakje gemaakt worden.

**101 Stelling (Veblen).** Een axiomatische projectieve ruimte van dimensie  $d > 2$  is steeds Desarguisch en bijgevolg isomorf met een  $P^d(\mathbb{F})$  voor een zeker veld  $\mathbb{F}$ . Een axiomatische projectieve ruimte met drie punten per rechte is steeds een  $P^d(\mathbb{F}_2)$ .

**Taak.** Bewijs vorige stelling.

**102 Stelling.** Een lineaire binaire perfecte 1-foutverbeterende code heeft steeds lengte  $2^d - 1$  voor een zekere  $d > 1$ . Voor elke  $d > 1$  bestaat er juist één zulke code.

*Bewijs.* Zij  $C \subseteq \mathbb{F}_2^n$  een code die één fout verbetert. Dan heeft elk niet-nul codewoord gewicht  $\geq 3$ . Als er maar één woord  $\mathbf{c}$  van gewicht 3 is, gebruiken we lemma (96) om te zien dat  $C = \text{vect}\{\mathbf{c}\} = \{\mathbf{0}, \mathbf{c}\}$ . Hieruit volgt dat  $n = 3 = 2^2 - 1$ .

Onderstel nu dat er meerdere codewoorden van gewicht drie zijn en stel  $\mathcal{P} := \Omega_n$  en  $\mathcal{L} := \{\text{supp}(\mathbf{c}) \mid \mathbf{c} \in C \text{ en } w(\mathbf{c}) = 3\}$ . We tonen aan dat  $(\mathcal{P}, \mathcal{L})$  een projectieve ruimte is. Het is duidelijk dat elke rechte (juist) drie punten bevat. Zij  $x, y \in \mathcal{P}$  en neem  $\mathbf{e}$  gelijk aan de karakteristieke vector van  $\{x, y\} \subset \Omega_n$ . Doordat  $C$  perfect is, bestaat er juist één codewoord  $\mathbf{c}$  met  $d(\mathbf{c}, \mathbf{e}) = 1$ . Vermits  $w(\mathbf{c}) \geq 3$ , moet  $\{x, y\} \subset \text{supp}(\mathbf{c}) \in \mathcal{L}$ .

Doordat de rechten maar 3 punten hebben, moeten (elke) drie van de rechten die in aanmerking komen voor axioma (PR3) de vorm  $\text{supp}(\mathbf{u}) = \{x, y, r\}$ ,  $\text{supp}(\mathbf{v}) = \{x, z, q\}$  en  $\text{supp}(\mathbf{w}) = \{y, z, p\}$  hebben voor zekere codewoorden  $\mathbf{u}, \mathbf{v}$  en  $\mathbf{w}$ . Maar  $C$  is lineair zodat  $\mathbf{u} + \mathbf{v} + \mathbf{w} \in C$ . Bovendien is  $\text{supp}(\mathbf{u} + \mathbf{v} + \mathbf{w}) = \{r, q, p\}$  zodat dit de unieke rechte is door  $r$  en  $q$ . We zien dat  $p$  een gemeenschappelijk punt is van  $\text{supp}(\mathbf{w})$  en  $\text{supp}(\mathbf{u} + \mathbf{v} + \mathbf{w})$ .

Dus is  $(\mathcal{P}, \mathcal{L})$  een axiomatische projectieve ruimte met drie punten per rechte. Volgens stelling (101) is deze structuur isomorf met  $P^{d-1}(\mathbb{F}_2)$  voor  $d > 2$ . Bijgevolg geldt  $n = |\Omega_n| = |\mathcal{P}| = 2^d - 1$ .

Bovendien verzekert lemma (96) dat  $C$  volledig bepaald is door zijn woorden van minimaal gewicht. Vermits de projectieve ruimten  $P^d(\mathbb{F}_2)$  voor elke  $d > 1$  bestaan en uniek zijn op isomorfisme na, is de stelling bewezen.  $\square$

## 4.2 Perfecte binaire codes die drie fouten verbeteren

Perfecte binaire codes die drie fouten verbeteren bestaan niet voor elke lengte. De lengte  $n$  moet immers zo zijn dat de som

$$\sum_{i=0}^3 \binom{n}{i}$$

een macht van 2 moet zijn. We krijgen dus voor een zekere  $l$

$$\begin{aligned} 1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} &= 2^l \\ \iff 6 + 6n + 3n^2 - 3n + n^3 - 3n^2 + 2n &= 3 \cdot 2^{l+1} \\ \iff n^3 + 5n + 6 &= 3 \cdot 2^{l+1} \\ \iff (n+1)(n^2 - n + 6) &= 3 \cdot 2^{l+1} \end{aligned}$$

Als  $n+1$  een veelvoud is van 3, bestaat er een natuurlijk getal  $\lambda$  met  $n = 3 \cdot 2^\lambda - 1$ . Hieruit volgt

$$n^2 - n + 6 = 3^2 \cdot 2^{2\lambda} - 3 \cdot 2^{\lambda+1} - 3 \cdot 2^\lambda + 8$$

De laatste uitdrukking moet een macht van 2 zijn. Voor  $\lambda \in \{0, 1, 2, 3\}$  kan je met de hand nagaan dat dit enkel het geval is voor 0 en 3. Voor  $\lambda > 3$  kan je een factor 8 afzonderen en zien dat wat overblijft oneven is. Bijgevolg kan de uitdrukking  $n^2 - n + 6$  geen macht van 2 zijn voor andere waarden van  $n$  dan 2 en 23. Bovendien heeft een code van lengte 2 geen zin als je 3 fouten wil verbeteren.

Veronderstel nu dat 3 geen deler is van  $n+1$ . Dan is er een  $\lambda$  met  $n = 2^\lambda - 1$ . We krijgen

$$n^2 - n + 6 = 2^{2\lambda} - 2^{\lambda+1} - 2^\lambda + 8$$

dat juist één keer deelbaar moet zijn door drie en verder enkel door 2. We merken op dat even machten van 2 steeds een rest 1 opleveren bij deling door 3 en oneven machten altijd 2. Dus geldt  $n^2 - n + 6 \equiv 1 - 2 - 1 + 2 \equiv 0 \pmod{3}$ , zodat deze uitdrukking *steeds* een veelvoud is van 3. Weer doen we de kleine voorbeelden met de hand. Dit levert mogelijke lengtes 0, 1, 3 en 7 op. We zien gemakkelijk dat de waarde van  $n^2 - n + 6$  voor  $\lambda > 3$  groter wordt dan  $48 = 3 \cdot 16$ . Als we de rest van  $n^2 - n + 6$  modulo 16 bekijken zien we echter dat die vanaf  $\lambda = 4$  steeds 8 bedraagt, zodat de uitdrukking niet meer deelbaar is door 16 en niet kan in aanmerking komen voor het bereiken van de Hamming grens.

De lengtes  $n = 0$  of 1 zijn natuurlijk zinloos voor een code die drie fouten verbetert. Voor  $n = 3$  hebben we slechts één codewoord. Dat is ook flauw en wordt niet beschouwd als een code. Voor  $n = 7$  toont de Hamming grens dat er twee codewoorden zijn. We hebben hier de repetitiecode  $\Delta_7(\mathbb{F}_2)$ .

### 4.3 De binaire Golay code

Er bestaan juist vijf Platonische lichamen. Eén daarvan is de **icosaëder** of twintigvlak. Deze polyeder heeft twaalf toppen, dertig ribben en twintig driehoekige zijvlakken. Elke top ligt op vijf ribben en is zo ‘verbonden’ met vijf andere toppen. We definiëren nu een  $12 \times 12$  binaire matrix  $A$  door de 12 toppen van de icosaëder te nummeren van 1 tot en met 12. We zetten op plaats  $(i, j)$  in  $A$  een 1 als en slechts als toppen  $i$  en  $j$  geen ribbe vormen. Merk op dat de diagonaalelementen van  $A$  gelijk zijn aan 1 en elke rij en elke kolom van  $A$  juist zeven keer 1 en vijf keer 0 bevat. De vijf nullen komen overeen met de vijf toppen die verbonden zijn met de top die door de gegeven rij (of kolom)  $i$  wordt voorgesteld. De zeven enen geven dus de toppen die niet verbonden zijn met  $i$  en  $i$  zelf. Deze verzameling van zeven toppen noemen we de **anti-vijfhoek** van  $i$  en noteren we  $AV(i)$ .

**103 Eigenschap.** *Elke twee rijen (of kolommen) van de matrix  $A \in M_{12}(\mathbb{F}_2)$  zijn orthogonaal.*

*Bewijs.* De icosaëder leert ons dat twee anti-vijfhoeken elkaar steeds 2 of 4 toppen gemeenschappelijk hebben. Het inproduct van twee kolommen telt juist het aantal gemeenschappelijke enen modulo 2.  $\square$

Zij  $C$  de lineaire binaire code met als genererende matrix

$$G := \begin{pmatrix} I_{12} \\ A \end{pmatrix}$$

Door de eenheidsdeelmatrix heeft  $G$  rang 12 en krijgen we dus een lineaire code van lengte 24 en dimensie 12. Een woord  $\mathbf{x} \in \mathbb{F}_2^{12}$  wordt gecodeerd door vermenigvuldiging met  $G$ . Het resultaat is een kolom  $\begin{pmatrix} \mathbf{x} \\ A\mathbf{x} \end{pmatrix}$ .

**104 Lemma.**  $C^\perp = C$

*Bewijs.* Neem twee codewoorden  $\begin{pmatrix} \mathbf{x} \\ A\mathbf{x} \end{pmatrix}$  en  $\begin{pmatrix} \mathbf{y} \\ A\mathbf{y} \end{pmatrix}$ . Dan geldt  $\begin{pmatrix} \mathbf{x} \\ A\mathbf{x} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{y} \\ A\mathbf{y} \end{pmatrix} = \mathbf{x} \cdot \mathbf{y} + A\mathbf{x} \cdot A\mathbf{y}$ . Maar vermits  $A$  orthogonaal is zijn de twee termen van deze som gelijk, zodat we modulo 2 nul krijgen. We hebben nu  $C \subseteq C^\perp$ , maar  $C^\perp$  heeft wegens lemma (68) dimensie 12.  $\square$

**105 Gevolg.** Voor elke twee codewoorden  $\mathbf{x}$  en  $\mathbf{y}$  is  $|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})|$  even.

*Bewijs.* Omdat  $|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})| = \langle \mathbf{x}, \mathbf{y} \rangle$ .  $\square$

**Notatie.** We zullen de karakteristieke vector van  $\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})$  soms kort  $\mathbf{x} \cap \mathbf{y}$  noteren.

**106 Eigenschap.** De gewichten van de woorden van  $C$  zijn veelvouden van 4.

*Bewijs.* Uit  $G$  lezen we af dat de woorden die  $C$  voortbrengen gewicht 8 hebben, een veelvoud van 4. Neem nu  $\mathbf{x}$  en  $\mathbf{y}$  codewoorden met  $w(\mathbf{x}) = 4k$  en  $w(\mathbf{y}) = 4l$  voor zekere  $k$  en  $l$ . Dan is  $w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y})$  wegens vorig gevolg ook een veelvoud van 4. Zo deelt 4 de gewichten van alle lineaire combinaties van voortbrengers van  $C$ .  $\square$

**107 Eigenschap.** Het éénwoord  $\mathbf{1} = 111 \cdots 1 \in \mathbb{F}_2^{24}$  behoort tot  $C$ .

*Bewijs.* Stel  $\mathbf{x} := {}^t(1, 1, \dots, 1) \in \mathbb{F}_2^{12}$ , dan bevat de kolomvector  $A\mathbf{x}$  de gewichten van de rijen van  $A$  modulo 2. Aangezien deze rijen elk gewicht 7 hebben, is  $A\mathbf{x} = \mathbf{x}$ .  $\square$

**108 Eigenschap.** Voor alle  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{12}$  geldt  $\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \in C \implies \begin{pmatrix} \mathbf{y} \\ \mathbf{x} \end{pmatrix} \in C$ .

*Bewijs.* We hebben dus eigenlijk  $\mathbf{y} = A\mathbf{x}$ . Merk op dat  $A$  symmetrisch en orthogonaal is. Hieruit volgt  $A^2 = A^t A = I_{12}$ . Nu zien we dat  $\begin{pmatrix} \mathbf{y} \\ \mathbf{x} \end{pmatrix} = \begin{pmatrix} A\mathbf{x} \\ \mathbf{x} \end{pmatrix} \in C$ .  $\square$

**109 Eigenschap.** De code  $C$  heeft geen woorden van gewicht 4.

*Bewijs.* Zij  $\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \in C$  van gewicht 4. Dan zijn de mogelijke gewichtscombinaties  $(w(\mathbf{x}), w(\mathbf{y}))$  die kunnen optreden  $(0, 4)$ ,  $(1, 3)$ ,  $(2, 2)$ ,  $(3, 1)$  en  $(4, 0)$ . De eerste en laatste zijn onmogelijk omdat  $\mathbf{x} = \mathbf{0} \implies A\mathbf{x} = \mathbf{0}$ . Als  $w(\mathbf{x}) = 1$ , is  $\mathbf{x}$  in feite een basisvector  $\mathbf{e}_i \in \mathbb{F}_2^{12}$ . Maar dan is  $A\mathbf{x}$  de  $i$ -de kolom van  $A$  en deze heeft gewicht 7,  $\nmid 4$ . Wegens vorige eigenschap is ook de combinatie  $(3, 1)$  onmogelijk. Veronderstel nu dat  $w(\mathbf{x}) = 2$ . Dan is  $\mathbf{x}$  de som van twee verschillende basisvectoren  $\mathbf{e}_i$  en  $\mathbf{e}_j$  zodat  $A\mathbf{x}$  de som van twee kolommen van  $A$  is. Aangezien deze kolommen elk gewicht 7 hebben en twee kolommen steeds 2 of 4 énen gemeenschappelijk hebben, krijgen we weer een  $\nmid 4$ .  $\square$

**110 Gevolg.** Het minimaal gewicht van  $C$  bedraagt 8.

**111 Gevolg.** De gewichten van de woorden in  $C$  behoren tot de verzameling  $\{0, 8, 12, 16, 24\}$ .

**112 Definitie.** Kies een getal  $i$  tussen 1 en 24. De code  $\mathcal{G}_i$  wordt uit  $C$  geconstrueerd door in alle woorden de  $i$ -de letter te schrappen. We noemen de codes  $\mathcal{G}_i$  **Golay codes**.

**113 Eigenschap.** De codes  $\mathcal{G}_i$  zijn perfecte  $[23, 2^{12}, 7]$ -codes.

*Bewijs.* Zulke code heeft duidelijk lengte 23. Hij heeft  $2^{12}$  woorden omdat het schrappen van één enkele letter in elk woord nooit twee keer hetzelfde woord kan opleveren. Ook kan de minimale afstand slechts met één eenheid afnemen. Deze parameters impliceren dat de code  $\mathcal{G}_i$  perfect is.  $\square$

In sectie 4.5 zullen we aantonen dat er, op equivalentie na, slechts één binaire Golay code bestaat zodat alle  $\mathcal{G}_i$  eigenlijk dezelfde code voorstellen, *de* Golay code.

**Een beetje geschiedenis.** Marcel Golay (1902–1989) publiceerde in 1949 een artikel van één bladzijde<sup>1</sup> waarin hij twee matrices gaf en beweerde dat dit pariteitsmatrices waren van twee perfecte codes (een binaire en een ternaire). Het waren inderdaad de twee Golay codes. Hij gaf geen details over hoe hij de matrices vond. De ternaire Golay code kan gebruikt worden om met de Toto te spelen. Indien je de uitkomst (ploeg A wint, verliest of gelijk spel) van 11 voetbalwedstrijden moet voorspellen met ten hoogste twee fouten, ben je op zoek naar een verzameling vectoren van  $\mathbb{F}_3^{11}$  die op afstand ten hoogste twee van om het even welke vector van deze ruimte is. De ternaire Golay code is een  $[11, 6, 5]$ -code. We kunnen dus winnen door  $3^6$  formulieren in te vullen. Golay was Zwitser, studeerde toegepaste wetenschappen aan de ETH Zürich en emigreerde in 1924 naar de VS. Hij<sup>2</sup> veralgemeende ook de perfecte Hamming code van sectie (1.4) tot alle eindige lichamen.

**Taak.** De manier die wij gebruiken om de Golay code in te voeren via de icosaeëder is niet gebruikelijk. Er bestaan vele equivalente definities van de Golay code. In een artikel<sup>3</sup> vind je enkele alternatieve definities. Neem er drie en toon de equivalentie met onze definitie.

**Taak.** De Golay code bevat 4096 woorden. Het decoderen van deze code houdt in principe in dat een ontvangen woord vergeleken moet worden met alle 4096 woorden van de code. Zo vindt men dan het unieke woord van de code dat het dichtst bij het ontvangen woord ligt. Er bestaan echter efficiëntere algoritmen om de Golay code te decoderen. Zo een methode vind je in [10]. Bestudeer deze methode en leg uit waarom ze werkt.

## 4.4 Andere structuren in verband met de Golay code

De Golay code laat toe vele verschillende takken van de wiskunde te verbinden. Het is werkelijk een uitzonderlijk object met unieke eigenschappen.

**114 Definitie.** We beschouwen de code  $C$  van vorige sectie en bekijken de dragers van de woorden op de verzameling  $X = \{1, 2, \dots, 24\}$ . De dragers van de woorden van gewicht 8 worden **blokken** genoemd. De verzameling van alle blokken noteren we  $\mathcal{B}$ . De elementen van  $X$  zullen we **punten** noemen.

**115 Eigenschap.** Kiezen we 5 punten in  $X$ , dan is er hoogstens één blok die deze 5 punten bevat.

*Bewijs.* Zij  $B_1, B_2 \in \mathcal{B}$  met  $|B_1 \cap B_2| \geq 5$ . Dan zijn er codewoorden  $\mathbf{c}_1, \mathbf{c}_2 \in C$  met  $\text{supp}(\mathbf{c}_1) = B_1$  en  $\text{supp}(\mathbf{c}_2) = B_2$  zodat  $w(\mathbf{c}_1 + \mathbf{c}_2) = 8 + 8 - 2|B_1 \cap B_2| \leq 6$ . Aangezien de enige vector met gewicht  $\leq 6$  in  $C$  het nulwoord is, besluiten we dat  $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{0}$  zodat  $B_1 = B_2$ .  $\square$

**116 Eigenschap.** De code  $C$  heeft ten hoogste 759 woorden van gewicht 8.

*Bewijs.* Wegens vorige eigenschap bepaalt elke deelverzameling van 5 elementen van  $X$  hoogstens één codewoord van gewicht 8. Bovendien zijn er in elke blok  $\binom{8}{5}$  deelverzamelingen van 5 elementen te vinden. Noteren we het aantal woorden van gewicht 8 met  $N_8$  hebben we dus

$$\binom{24}{5} \geq N_8 \binom{8}{5}$$

of

$$N_8 \leq \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20}{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4} = 23 \cdot 11 \cdot 3 = 759$$

$\square$

Nu tellen we exact het aantal woorden van gewicht 8 in  $C$ . Van vorige sectie weten we dat een woord  $\begin{pmatrix} \mathbf{x} \\ A\mathbf{x} \end{pmatrix}$  in  $C$  bestaat uit twee delen. We splitsen de woorden van gewicht 8 op in 9 groepjes, naargelang het gewicht van het eerste stuk  $\mathbf{x}$ :

$$N_{8,i} := \left| \left\{ \begin{pmatrix} \mathbf{x} \\ A\mathbf{x} \end{pmatrix} \in C \mid w(\mathbf{x}) = i \text{ en } w(A\mathbf{x}) = 8 - i \right\} \right|$$

<sup>1</sup>M.J.E. Golay. Notes on Digital Coding. *Proc. I.R.E.*, vol. 37, p. 657, 1949

<sup>2</sup>M.J.E. Golay. Notes on the Penny-Weighing Problem, Lossless Symbol Coding with Nonprimes, etc. *I.R.E. Trans. Inform. Theory*, IT-4, 103–109, 1958.

<sup>3</sup>R. Chapman. Constructions of the Golay Codes: A Survey. Unpublished.

Uit eigenschap (108) volgt  $N_{8,i} = N_{8,8-i}$  zodat

$$N_8 = 2N_{8,0} + 2N_{8,1} + 2N_{8,2} + 2N_{8,3} + N_{8,4}$$

Het is duidelijk dat  $N_{8,0} = 0$  omdat  $A\mathbf{0} = \mathbf{0}$ . Als het gewicht van het eerste stuk woord  $\mathbf{x}$  juist 1 bedraagt, is  $\mathbf{x}$  één van de twaalf basisvectoren  $\mathbf{e}_i$  met overal nullen behalve op plaats  $i$ . We hebben dus  $N_{8,1} = 12$ .

De woorden van gewicht 8 waarvan het eerste stuk gewicht twee heeft, zijn van de vorm  $\begin{pmatrix} \mathbf{e}_i + \mathbf{e}_j \\ A\mathbf{e}_i + A\mathbf{e}_j \end{pmatrix}$  voor zekere  $i \neq j$  in  $\{1, 2, \dots, 12\}$ . Maar hier moeten we opletten omdat niet alle keuzes van  $i$  en  $j$  aanleiding geven tot een woord van gewicht 8. Inderdaad:  $w(A\mathbf{e}_i + A\mathbf{e}_j) = w(A\mathbf{e}_i) + w(A\mathbf{e}_j) - 2|\text{supp}(A\mathbf{e}_i) \cap \text{supp}(A\mathbf{e}_j)|$  is het gewicht van de som van kolommen  $i$  en  $j$  van de matrix  $A$ . In het bewijs van eigenschap (103) merkten we op dat twee kolommen op 2 of 4 gemeenschappelijke plaatsen een 1 hebben. Het geval met twee 1-en komt overeen het antipodaal zijn van de toppen  $i$  en  $j$  in de icosaeëder. Enkel de andere gevallen leveren een woord van gewicht 8 zodat we krijgen  $N_{8,2} = \frac{12 \cdot 10}{2}$ .

Voor  $N_{8,3}$  gaan we op zoek naar verzamelingen  $\{i, j, k\}$  van toppen van de icosaeëder zodanig dat de som van de overeenkomstige kolommen van  $A$  gewicht 5 heeft. We onderzoeken dit best op een tekening, waar we de anti-vijfhoeken van de drie toppen in verschillende kleuren op aanduiden en dan de toppen te tellen die in één of drie kleuren geschilderd zijn. Er zijn verschillende gevallen die we één voor één onderzoeken en tellen. Na een beetje kleurwerk vinden we volgend lemma.

**117 Lemma.**  $N_{8,3} \geq 180$

Voor  $N_{8,4}$  doen we hetzelfde voor verzamelingen  $\{i, j, k, l\}$  van vier toppen op de icosaeëder.

**118 Lemma.**  $N_{8,4} \geq 255$

**119 Gevolg.**  $N_8 \geq 0 + 2 \cdot 12 + 2 \cdot 60 + 2 \cdot 180 + 255 = 759$

Samen met eigenschap (116) hebben we dus

**120 Stelling.** De code  $C$  bevat juist 759 woorden van gewicht 8.

Samen met eigenschap (115) krijgen we dan

**121 Gevolg.** Elke verzameling van 5 punten in  $X$  bepaalt juist één blok.

De code  $C$  geeft aanleiding tot een voorbeeld van een zeer belangrijke combinatorische structuur.

**122 Definitie.** Zij  $X$  een verzameling van cardinaliteit  $v$  en  $\mathcal{B}$  een verzameling delen van  $X$  met elk  $k$  elementen. Voor een natuurlijk getal  $t \leq k$  zegt men dat de structuur  $(X, \mathcal{B})$  een **Steiner systeem**  $S(t, k, v)$  is indien voor elk deel  $D$  van  $X$  met  $t$  elementen er juist één  $B \in \mathcal{B}$  bestaat met  $D \subset B$ . De elementen van  $X$  noemen we **punten** van het Steiner systeem en de elementen van  $\mathcal{B}$  zijn **blokken**.

**Voorbeeld.** Een (axiomatisch) projectief vlak van orde  $n$  is een  $S(2, n+1, n^2+n+1)$  als je de rechten blokken noemt.

**Oefening.** Toon aan dat elke  $S(2, n+1, n^2+n+1)$  een projectief vlak is.

**Voorbeeld.** Een (axiomatisch) affien vlak van orde  $n$  is een  $S(2, n, n^2)$ . Er bestaan  $S(2, n, n^2)$  die geen affiene vlakken zijn.

**123 Stelling.** De woorden van gewicht 8 van de code  $C$  geven aanleiding tot een  $S(5, 8, 24)$ .

**124 Definitie.** Zij  $(X, \mathcal{B})$  een  $S(t, k, v)$  en kies  $x \in X$ . Stel  $X' := X \setminus \{x\}$  en  $\mathcal{B}' := \{B \setminus \{x\} \mid x \in B \in \mathcal{B}\}$ . Dan is  $(X', \mathcal{B}')$  een  $S(t-1, k-1, v-1)$  dat we **afgeleid Steiner systeem** noemen.

Het herhaaldelijk afleiden van ons Steiner systeem geeft ons een rij van Steiner systemen  $S(5, 8, 24)$ ,  $S(4, 7, 23)$ ,  $S(3, 6, 22)$  en  $S(2, 5, 21) \cong P^2(\mathbb{F}_4)$ , het uniek projectief vlak van orde 4.

**125 Definitie.** Een *automorfisme* van een Steiner systeem  $(X, \mathcal{B})$  is een permutatie van  $X$  die blokken op blokken afbeeldt. De verzameling van alle automorfismen van een Steiner systeem vormt een groep voor de samenstelling die we  $\text{Aut}(X, \mathcal{B})$  noteren.

De automorfismengroepen van de rij Steiner systemen geassocieerd met de code  $C$  zijn ook zeer bijzonder. Volgende stelling wordt niet bewezen, maar is zeer aaneembaar en kan als taakje bewezen worden.

**126 Stelling.** De automorfismengroep van het  $S(5, 8, 24)$  Steiner systeem  $(X, \mathcal{B})$  is 5-transitief op de punten.

Noteren we de automorfismengroepen van de Steiner systemen op  $v \in \{21, 22, 23, 24\}$  punten als  $M_v$ , krijgen we dus volgend gevolg.

**127 Gevolg.**  $M_v$  is  $(v - 19)$ -transitief op het Steiner systeem met  $v$  punten.

*Bewijs.* We merken gewoon op dat de automorfismengroep van het Steiner systeem met  $v \in \{23, 22, 21\}$  punten steeds de stabilisator is van een punt in  $M_{v+1}$ .  $\square$

Aangezien  $S(2, 5, 21)$  isomorf is met een projectief vlak, kennen we de automorfismengroep  $M_{21}$  zeer goed. De cursus “Affiene en projectieve meetkunde” leert ons dat dit  $\text{PSL}_3(4)$  is. Hiermee kunnen we de orden van de groepen  $M_v$  bepalen.

**128 Stelling.** De orde van  $M_{21}$  is  $21 \cdot 20 \cdot 48$ . Voor  $v \in \{22, 23, 24\}$  geldt  $|M_v| = v \cdot |M_{v-1}|$ .

*Bewijs.* Voor  $M_{21}$  hoeven we gewoon de orde van  $\text{PSL}_3(4) = \text{SL}_3(4)/Z(\text{SL}_3(4))$  uit te rekenen. We weten dat  $|\text{GL}_3(4)|$  gelijk is aan het aantal basissen in de ruimte  $\mathbb{F}_4^3$ . Dat is dus  $(4^3 - 1)(4^3 - 4)(4^3 - 4^2)$ . Elke matrix  $M$  van  $\text{GL}_3(4)$  geeft aanleiding tot een matrix van  $\text{SL}_3(4)$  door de eerste kolom te delen door de (niet-nulle) determinant van  $M$ . Omgekeerd kan je met een matrix  $A$  van  $\text{SL}_3(4)$  drie matrices van  $\text{GL}_3(4)$  maken waarvan de eerste kolom een veelvoud is van de eerste kolom van  $A$ . We kunnen inderdaad de eerste kolom van  $A$  vermenigvuldigen met elk van de drie niet-nulle elementen van  $\mathbb{F}_4$ . Via dubbeltelling krijgen we dus  $|\text{SL}_3(4)| = \frac{1}{3}|\text{GL}_3(4)| = 21 \cdot 60 \cdot 48 = 60480$ . Hieruit volgt  $|\text{PSL}_3(4)| = \frac{1}{3}|\text{SL}_3(4)| = 21 \cdot 20 \cdot 48$  omdat  $Z(\text{PSL}_3(4))$  juist de drie niet-nulle scalaire matrices van  $\text{GL}_3(4)$  bevat. Het is inderdaad zo dat elk niet-nul element van  $\mathbb{F}_4$  een derdemachtswortel van 1 is.

De andere ordes volgen uit de beroemde “orbit-stabilizer stelling”.  $\square$

We kunnen nog groepen maken met onze code  $C$ .

**129 Definitie.** Zij  $D$  de drager van een woord van gewicht 12 in  $C$ . Dan snijdt elke blok van  $(X, \mathcal{B})$  de verzameling  $D$  in 2, 4 of 6 punten. Stel  $\mathcal{D} := \{B \cap D \mid B \in \mathcal{B} \text{ en } |B \cap D| = 6\}$ . Dan is  $(D, \mathcal{D})$  een  $S(5, 6, 12)$  met 132 blokken (verifieer dit!).

Weer kunnen we  $(D, \mathcal{D})$  afleiden zodat we een rij krijgen  $S(5, 6, 12), S(4, 5, 11), S(3, 4, 10)$  en  $S(2, 3, 9)$ . Het laatste Steiner systeem is het affiene vlak met 9 punten (en 12 rechten). De automorfismengroep van het Steiner systeem  $S(5, 6, 12)$  wordt  $M_{12}$  genoteerd. De stabilisator van een punt van  $S(5, 6, 12)$  in  $M_{12}$  is  $M_{11}$ . Als we twee, resp. drie punten fixeren, krijgen we  $M_{10}$  resp.  $M_9$ . De orde van  $M_9$  is  $8 \cdot 9$ . Het is een 2-transitieve normale deelgroep van de volledige automorfismengroep van het affiene vlak met 9 punten ( $\text{AGL}_2(3)$ , met 432 elementen). De grootste van deze vier groepen is opnieuw 5-transitief op 12 punten zodat we de orden van alle groepen in de rij kennen.

De groepen  $M_{24}, M_{23}, M_{22}, M_{12}$  en  $M_{11}$  werden rond 1873 ontdekt door de Franse wiskundige Emile Mathieu. We noemen ze nu **Mathieu groepen**.

Een stelling van TITS toont dat er weinig 5-transitieve groepen zijn.

**130 Stelling (Tits).** Een 5-transitieve eindige permutatiegroep is isomorf met één van volgende groepen:

- (i) de symmetrische groepen  $S_n$  of  $A_{n+2}$  voor  $n \geq 5$ ;
- (ii) de Mathieugroepen  $M_{24}$  of  $M_{12}$ .

Het wordt dus duidelijk dat de Mathieugroepen een bijzondere plaats verdienen binnen de groepentheorie.

Nog een stelling zonder bewijs. . .

**131 Stelling.** De Mathieugroepen  $M_{24}, M_{23}, M_{22}, M_{12}$  en  $M_{11}$  zijn enkelvoudig.

Enkelvoudige groepen zijn van groot belang omdat alle groepen eigenlijk opgebouwd zijn uit zulke groepen. Zij  $G$  een eindige groep. Indien hij niet enkelvoudig is, heeft hij een niet-triviale normale deelgroep  $N_1$ . Nu kan je kijken naar het quotiënt  $G/N_1$ . Indien  $N_1$  niet enkelvoudig is, is er een niet-triviale normale deelgroep  $N_2 \triangleleft N_1$ . Je kan zo verder gaan tot je een enkelvoudige groep  $N_k$  hebt zodat je volgende rij kan schrijven.

$$G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots \triangleright N_k \triangleright 1$$

Deze rij heeft lengte  $k + 1$ . Het is mogelijk dat deze rij langer kan gemaakt worden. Daarvoor beschouwen we de quotiënten  $N_i/N_{i+1}$ . Als er een  $i$  bestaat waarvoor  $N_i/N_{i+1}$  niet enkelvoudig is, bestaat er een deelgroep  $K$  van  $N_i$  die  $N_{i+1}$  strikt omvat zodanig dat  $K/N_{i+1} \triangleleft N_i/N_{i+1}$ . Maar natuurlijk geldt dan dat  $N_{i+1} \neq K \triangleleft N_i$ , zodat we in onze rij  $K$  kunnen zetten tussen  $N_i$  en  $N_{i+1}$ . Dit alles geldt natuurlijk omdat je uit de algebracursus van eerste kandidatuur weet dat er een bijjectie bestaat tussen de deelgroepen van  $N_i$  die  $N_{i+1}$  omvatten en de deelgroepen van  $N_i/N_{i+1}$ . Je weet ook dat deze bijjectie normale deelgroepen afbeeldt op normale deelgroepen. Zodoende wordt de rij langer tot alle quotiënten  $N_i/N_{i+1}$  enkelvoudig zijn. Zo een rij van normale deelgroepen die je niet langer kan maken heet een **compositierij** van  $G$  en de enkelvoudige quotiënten  $N_i/N_{i+1}$  heten **compositiefactoren**. Je kan je natuurlijk afvragen of de rij die we bekomen niet afhangt van de keuze van de normale deelgroep  $N_{i+1}$  in  $N_i$  bij elke stap. Een stelling die je bewijst in de cursus “Groepen- en Galoistheorie” gaat als volgt.

**132 Stelling** (Jordan–Hölder). *Elke compositierij van een gegeven groep is even lang. Bovendien zijn de compositiefactoren van twee compositierijen voor eenzelfde groep op volgorde na dezelfde.*

We zien hier dus een situatie analoog aan de ontbinding in priemfactoren van een geheel getal. Als een getal niet priem is, kan je het delen door een niet-triviale deler. Zo krijg je een dalende rij getallen tot je stopt in een priemgetal. Indien het quotiënt van twee opeenvolgende getallen in de rij geen priemgetal is, kan de rij langer gemaakt worden. Uiteindelijk zijn alle quotiënten van opeenvolgende getallen in de rij priemgetallen en kan de rij niet langer gemaakt worden. Op volgorde na is de ontbinding in priemfactoren van een getal uniek. Enkelvoudige groepen spelen dus dezelfde rol als priemgetallen. Het zijn de bouwstenen van alle groepen. Daarom is het zo belangrijk de enkelvoudige groepen goed te kennen.

De eindige enkelvoudige groepen werden vorige eeuw geclassificeerd. Het gaat om een stelling waarvan het bewijs ongeveer 10.000 bladzijden lang is en waar een 100-tal wiskundige van de hele wereld gedurende ongeveer 30 jaar aan werkten.

We geven uiteraard geen bewijs!

**133 Stelling** (Classificatie der eindige enkelvoudige groepen). *Een eindige enkelvoudige groep behoort tot juist één van volgende families:*

- (i) *De cyclische groepen van priemorde;*
- (ii) *De alternerende groepen van graad  $\geq 5$ ;*
- (iii) *De groepen van Lie-type;*
- (iv) *De 26 sporadische groepen.*

De eerste drie families bevatten elk oneindig veel groepen, maar er zijn slechts 26 sporadische enkelvoudige groepen (daarom heten ze ook “sporadisch”). De familie groepen van Lie-type bevat onder andere de groepen  $\mathbf{PSL}_n(q)$ . Dit zijn groepen die meestal kunnen begrepen worden als automorfismengroep van een zekere meetkundige structuur zoals een projectieve ruimte. De sporadische groepen zijn zeer mysterieus en nog niet volledig begrepen. Zij duiken in zeer veel takken van de wiskunde op.

De vijf Mathieugroepen zijn de oudste sporadische enkelvoudige groepen. De overige sporadische groepen werden pas lang (bijna 100 jaar) na Mathieu ontdekt. Je krijgt in bijlage een overzicht van de (sporadische) enkelvoudige groepen.

**Taak.** Geef een beschrijving voor enkele families groepen van Lie-type en leg uit met welke meetkundige structuren ze in verband staan.

## 4.5 Uniciteit van de binaire Golay code

We weten uit vorige sectie exact hoeveel woorden van elk gewicht in de code  $C$  zitten. Een Golay code bekomt men door in  $C$  een coördinaat te schrappen. Daarom noemt men  $C$  soms ook de **uitgebreide Golay code**. Nu tellen we het aantal

woorden van elk gewicht in een perfecte Golay code  $\mathcal{G}_i$ . We zullen zien dat dit niet moeilijk is juist doordat de code perfect is.

We herhalen dat  $\mathcal{G}_i$  een binaire lineaire perfecte code is van lengte 23, dimensie 12 en minimale afstand 7. Met  $A_j$  noteren we de woorden van gewicht  $j \in \{0, 1, \dots, 23\}$ . Aangezien de minimale afstand 7 bedraagt, hebben we  $A_0 = 1$  en  $A_1 = A_2 = A_3 = A_4 = A_5 = A_6 = 0$ .

Beschouw nu de koppels  $(\mathbf{x}, \mathbf{c}) \in \mathbb{F}_2^{23} \times \mathcal{G}_i$  met  $w(\mathbf{x}) = 4$  en  $d(\mathbf{x}, \mathbf{c}) \leq 3$ . Doordat  $\mathcal{G}_i$  perfect is, is er voor elke keuze van  $\mathbf{x}$  een *uniek* codewoord  $\mathbf{c}$  op afstand  $\leq 3$ . De minimale afstand impliceert dat  $w(\mathbf{c}) = 7$  en  $d(\mathbf{x}, \mathbf{c}) = 3$ . Als we de koppels  $(\mathbf{x}, \mathbf{c})$  op twee manieren tellen, krijgen we volgende vergelijking.

$$\binom{23}{4} = A_7 \cdot \binom{7}{3}$$

Hieruit volgt  $A_7 = 23 \cdot 11 = 253$ .

Nemen we nu koppels  $(\mathbf{x}, \mathbf{c})$  waar  $w(\mathbf{x}) = 5$ , kan een codewoord op afstand  $\leq 3$  gewicht 7 of 8 hebben. We krijgen een vergelijking.

$$\binom{23}{5} = A_7 \cdot \binom{7}{2} + A_8 \cdot \binom{8}{3}$$

Als we de gekende waarde voor  $A_7$  substitueren, vinden we  $A_8 = 506$ .

Een vergelijking voor  $A_9$  krijgen we door koppels  $(\mathbf{x}, \mathbf{c})$  met  $w(\mathbf{x}) = 6$  te tellen. Een woord van gewicht 6 heeft twee soorten codewoorden van gewicht 7 op afstand  $\leq 3$ . Je kan namelijk op afstand 1 zijn van een codewoord (door juist een "0" van  $\mathbf{x}$  te veranderen in een "1") of op afstand 3 (door twee keer een "0" te veranderen in een "1" en dan een andere "1" in een "0" te veranderen). We krijgen een vergelijking

$$\binom{23}{6} = A_7 \cdot \binom{7}{1} + A_7 \cdot \binom{7}{2} \cdot 16 + A_8 \binom{8}{2} + A_9 \binom{9}{3},$$

waaruit volgt dat  $A_9 = 0$ .

Analoog vinden we  $A_{10} = 0, A_{11} = 1288, A_{12} = 1288, \dots$

We zien dat bovenstaande redenering kan gebruikt worden bij elke perfecte code.

**134 Stelling.** *Voor een perfecte code die het nulwoord bevat, kan men steeds het aantal woorden van elk gewicht bepalen.*

Nu gaan we bewijzen dat er eigenlijk maar één Golay code bestaat. Dit gebeurt in verschillende stappen.

**135 Stelling.** *Zij  $C \subset \mathbb{F}_2^{24}$  met  $|C| = 2^{12}$  en  $\min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y} \in C\} = 8$ . Als bovendien nog  $\mathbf{0} \in C$ , dan is  $C$  een deelruimte van  $\mathbb{F}_2^{24}$  (m.a.w. de code  $C$  is lineair).*

*Bewijs.* Voor  $i \in \{1, 2, \dots, 24\}$  definiëren we

$$C_i := \{(c_1, c_2, \dots, c_{i-1}, c_{i+1}, \dots, c_{24}) \mid \mathbf{c} \in C\}$$

We schrappen dus de  $i$ -de coördinaat, zoals in de constructie van  $\mathcal{G}_i$ . We zien gemakkelijk dat  $|C_i| = 2^{12}$  en dat de minimale afstand in  $C_i$  moet gelijk zijn aan 7. We hebben dus dat  $C_i$  een perfecte binaire code is van lengte 23, met  $2^{12}$  woorden en minimale afstand 7. Wegens vorige stelling kennen we het aantal woorden van elk gewicht in  $C_i$ . Voor een perfecte code met die parameters hebben we die woorden eerder geteld zodat we nu weten dat  $C_i$  enkel woorden heeft wiens gewicht tot de verzameling  $\{0, 7, 8, 11, 12, 15, 16, 23\}$  behoort. Voor een woord  $\mathbf{c} \in C$  noteren we het overeenkomstige woord in  $C_i$  met  $\tilde{\mathbf{c}}$ . Er geldt  $\forall \mathbf{c} \in C : w(\mathbf{c}) = w(\tilde{\mathbf{c}})$  of  $w(\mathbf{c}) = w(\tilde{\mathbf{c}}) + 1$ . De woorden van gewicht 7 en 8 in  $C_i$  moeten dus afkomstig zijn van woorden van gewicht 7, 8 of 9 in  $C$ . Het minimaal gewicht van  $C$  sluit de eerste mogelijkheid uit. Mocht  $w(\mathbf{c}) = 9$  zijn voor een  $\mathbf{c} \in C$ , kunnen we een  $i$  kiezen buiten de drager van  $\mathbf{c}$ . De constructie van  $C_i$  voor deze bijzondere  $i$  geeft natuurlijk ook een perfecte code, maar nu geldt  $w(\tilde{\mathbf{c}}) = 9, \frac{1}{2}$ . Deze redenering leidt uiteindelijk tot het feit dat  $C$  enkel woorden heeft met gewicht in  $\{0, 8, 12, 16, 24\}$ .

Kies een codewoord  $\mathbf{c} \in C$ , dan heeft de verzameling  $C + \mathbf{c}$  nog steeds  $2^{12}$  elementen en bevat het nulwoord  $\mathbf{0} = \mathbf{c} + \mathbf{c}$ . Bovendien impliceert  $d(\mathbf{x} + \mathbf{c}, \mathbf{y} + \mathbf{c}) = d(\mathbf{x}, \mathbf{y})$  dat de minimale afstand in  $C + \mathbf{c}$  ook 8 bedraagt. Bijgevolg heeft  $C + \mathbf{c}$  ook enkel woorden met gewicht in  $\{0, 8, 12, 16, 24\}$ . Hieruit volgt dat  $\forall \mathbf{x}, \mathbf{c} \in C$  geldt  $w(\mathbf{x} + \mathbf{c}) = w(\mathbf{x} - \mathbf{c}) = d(\mathbf{x}, \mathbf{c}) \in$

$\{0, 8, 12, 16, 24\}$ , zodat  $\forall \mathbf{x}, \mathbf{y} \in C: w(\mathbf{x}) \equiv 0 \pmod{4}$  en  $w(\mathbf{x} + \mathbf{y}) \equiv 0 \pmod{4}$ . Hieruit volgt onmiddellijk dat  $\langle \mathbf{x}, \mathbf{y} \rangle$  even moet zijn en dus  $\mathbf{x} \cdot \mathbf{y} = 0$ .

Stellen we  $\bar{C} := \text{vect} C$ , hebben we  $C \subseteq \bar{C} \leq \bar{C}^\perp$ . Hieruit volgt dat

$$12 \leq \dim \bar{C} \leq \dim \bar{C}^\perp = 24 - \dim \bar{C} \leq 12$$

zodat  $|\bar{C}| = 2^{12} = |C|$ . Hieruit volgt  $C = \bar{C}$ . □

Nu hebben we een andere interessante combinatorische structuur nodig.

## Intermezzo over designs

**136 Definitie.** Zij  $X$  een verzameling met  $v$  elementen en  $\mathcal{B}$  een verzameling deelverzamelingen van  $X$  met elk  $k$  elementen. De structuur  $(X, \mathcal{B})$  heet een  $t - (v, k, \lambda)$ -**design** voor gehele getallen  $t$  en  $\lambda$  indien elke deelverzameling van  $X$  met  $t$  elementen omvat is door juist  $\lambda$  elementen van  $\mathcal{B}$ . De elementen van  $X$  noemen we **punten** en die van  $\mathcal{B}$  heten **blokken**. De parameter  $t$  heet **sterkte** van de design.

**Opmerking.** Designs zijn dus veralgemeningen van Steiner systemen. Elk Steiner systeem  $S(t, k, v)$  is een  $t - (v, k, 1)$ -design.

**Opmerking.** Het is duidelijk dat definitie (136) enkel zin heeft indien  $t \leq k \leq v$ .

**137 Stelling.** Een  $t - (v, k, \lambda)$  design  $(X, \mathcal{B})$  is ook een  $s - (v, k, \lambda_s)$ -design voor elke  $s \in \{1, 2, \dots, t\}$ . Hierbij is

$$\lambda_s = \lambda \cdot \frac{(v-s)(v-s-1) \cdots (v-t+1)}{(k-s)(k-s-1) \cdots (k-t+1)}$$

*Bewijs.* Bij inductie op  $t - s$ . Als  $t - s = 0$  is het in orde.

Veronderstel dat de stelling waar is voor  $s = i + 1$ . Dan moeten wij bewijzen dat ze geldt voor  $s = i$ . Zij  $I$  een verzameling van  $i$  punten. We tellen de koppels in de verzameling

$$\{(x, B) \in X \times \mathcal{B} \mid x \in X \setminus I \text{ en } (I \cup \{x\}) \subset B\}$$

Eenzijds hebben we  $v - i$  keuzes voor  $x$  en voor elke  $x$  zijn er  $\lambda_{i+1}$  blokken die  $I \cup \{x\}$  omvatten. Anderzijds kunnen we het aantal blokken dat  $I$  omvat even noteren met  $\lambda_I$  zodat we krijgen

$$(v - i)\lambda_{i+1} = \lambda_I(k - i)$$

We zien dat  $\lambda_I$  niet afhangt van de keuze van  $I$  maar volledig bepaald is door  $\lambda_{i+1}$ ,  $v$  en  $k$ . Dus hebben we wel echt een  $i - (v, k, \lambda_i)$ -design, waarbij

$$\lambda_i = \lambda_{i+1} \frac{v - i}{k - i}$$

□

**Opmerking.** Vorige stelling geldt ook voor  $s = 0$ . De parameter  $\lambda_0$  is dan het aantal blokken dat de lege verzameling omvat. Dit is gewoon  $|\mathcal{B}|$ , het totaal aantal blokken.

**Notatie.** In vorige stelling stelt de parameter  $\lambda_1$  het aantal blokken voor dat door een punt gaat. Dit noteren we gewoonlijk  $r$ . Het aantal blokken in een design noteren we  $b$ . We hebben dus dat in elke design van sterkte  $\geq 1$  geldt

$$rv = bk$$

Stelling (137) legt zware bestaansvoorwaarden op aan designs. De getallen  $\lambda_s$  moeten inderdaad geheel zijn.

**138 Gevolg.** Een design met parameters  $t - (v, k, \lambda)$  kan enkel bestaan indien

$$\forall i \in \{1, 2, \dots, t-1\}: (k-i)(k-i-1) \cdots (k-t+1) \mid \lambda(v-i)(v-i-1) \cdots (v-t+1)$$

**Voorbeeld.** Er bestaat geen  $3 - (11, 4, 1)$ -design omdat  $2 \nmid 1 \cdot 9$ .

Designs bestaan reeds sinds de jaren 30 en werden door BOSE<sup>4</sup> ingevoerd voor het ontwerpen (“to design”) van (statistische) proeven in de landbouw. Lang waren de sterkste gekende designs 6-designs en was het bestaan van  $t$ -designs voor willekeurige  $t$  een open probleem. In 1987 loste TEIRLINCK<sup>5</sup> dit probleem op: er bestaan  $t$ -designs voor elke  $t$ . Luc Teirlinck studeerde aan de VUB en werkt nu in de Verenigde Staten (Auburn University).

**139 Definitie.** We kunnen de punten en blokken van een  $t - (v, k, \lambda)$ -design  $(X, \mathcal{B})$  (willekeurig) nummeren zodat  $X = \{x_1, x_2, \dots, x_v\}$  en  $\mathcal{B} = \{B_1, B_2, \dots, B_b\}$ . De **incidentiematrix** van  $(X, \mathcal{B})$  is een  $(v \times b)$ -matrix  $N$  met

$$N_{ij} := \begin{cases} 1 & \text{indien } x_i \in B_j, \\ 0 & \text{indien } x_i \notin B_j. \end{cases}$$

De designs die we het best kennen zijn de projectieve en affiene vlakken. Hun sterkte is 2 omdat door twee punten steeds een unieke rechte gaat. Designs van sterkte 2 zullen verder ook de belangrijkste rol spelen.

**140 Eigenschap.** De matrix  $N$  van een design van sterkte 2 voldoet aan

$$N^t N = (r - \lambda)I_v + \lambda J_v$$

De matrix  $J_v$  is de vierkante matrix van orde  $v$  met overal 1.

*Bewijs.* Op plaats  $(i, j)$  in het product  $N^t N$  staat het inproduct  $\langle \mathbf{n}_i, \mathbf{n}_j \rangle$  van de  $i$ -de en de  $j$ -de rij van  $N$ . Dit inproduct telt juist het aantal blokken dat de punten  $x_i$  en  $x_j$  bevat. Als  $i \neq j$ , is dat  $\lambda$ , anders is het  $r$ .  $\square$

**141 Eigenschap.** De matrix  $N$  van een design van sterkte 2 voldoet aan

$$\det(N^t N) = rk(r - \lambda)^{v-1}$$

*Bewijs.* We weten  $N^t N = (r - \lambda)I_v + \lambda J_v$  en trekken de eerste kolom af van alle andere. Dan elke rij optellen bij de eerste en je hebt een onderdriehoeksmatrix. Merk op dat stelling (137) voor  $t = 2$  een voorwaarde  $(v - 1)\lambda = (k - 1)r$  oplevert.  $\square$

**142 Stelling.** Een niet-triviale  $2 - (v, k, \lambda)$ -design heeft minstens evenveel blokken als punten.

*Bewijs.* Uit vorige eigenschap halen we dat  $\det(N^t N) = 0$  enkel mogelijk is indien  $r = \lambda$ . Maar dit impliceert (via  $(v - 1)\lambda = (k - 1)r$ ) dat  $v = k$ . Hieruit volgt dat de design slechts één blok heeft die gans  $X$  is. Zulk een design is triviaal. We mogen veronderstellen dat  $\det(N^t N) \neq 0$ . Maar dan is  $N^t N$  inverteerbaar zodat zijn rang  $v$  is. Nu geldt

$$b \geq \text{rang} N \geq \text{rang}(N^t N) = v$$

$\square$

**143 Gevolg** (Stelling van Fisher<sup>6</sup>). Elke design van sterkte  $\geq 2$  heeft minstens evenveel blokken als punten.

*Bewijs.* Door stelling (137) is zulk een design ook een 2-design zodat vorige stelling van toepassing is.  $\square$

Onze vrienden de projectieve vlakken zijn designs van sterkte 2 waar bovendien het aantal blokken (=rechten) gelijk is aan het aantal punten. We veralgemenen dit.

<sup>4</sup>R. C. Bose. On the construction of balanced incomplete block designs. *Ann. Eugenics*, 9:353–399, 1939.

<sup>5</sup>Luc Teirlinck. Nontrivial  $t$ -designs without repeated blocks exist for all  $t$ . *Discrete Math.*, 65(3):301–311, 1987.

<sup>6</sup>Ronald A. Fisher (1890–1962), een prominent statisticus die zijn wetenschap toepaste in de landbouw en het ontwerpen van experimenten. De letter  $v$  staat voor “varieties” en  $r$  voor “replication number”.

**144 Definitie.** Een design  $(X, \mathcal{B})$  van sterkte  $t$  heet **symmetrisch** indien hij evenveel blokken als punten heeft. Een eenvoudige manier om een symmetrische  $t - (v, k, \lambda)$ -design te maken is te stellen  $\mathcal{B} = \binom{X}{v-1}$ . In dit geval spreken we ook van een **triviale symmetrische design**.

**145 Stelling.** Een (niet-triviale) symmetrische design heeft steeds sterkte 2.

*Bewijs.* Zij  $(X, \mathcal{B})$  een symmetrische  $t - (v, k, \lambda)$ -design van sterkte  $t \geq 3$ . Door stelling (137) is  $(X, \mathcal{B})$  dan zeker ook een  $3 - (v, k, \lambda_3)$ -design. We kunnen een “afgeleide design” construeren door een punt  $x \in X$  te kiezen en  $X' := X \setminus \{x\}$  te nemen, met  $\mathcal{B}' := \{B \setminus \{x\} \mid B \in \mathcal{B} \text{ en } x \in B\}$  (vergelijk met het afgeleid Steiner systeem van definitie (124)). Dit is inderdaad een design met parameters  $2 - (v-1, k-1, \lambda')$  voor een zekere  $\lambda'$ . Het aantal blokken van deze afgeleide design is gelijk aan het aantal blokken door het punt  $x$  in de oorspronkelijke design. Dit noteren we traditiegetrouw met  $r$ . De stelling van Fisher levert  $r \geq v-1$  maar doordat de design symmetrisch is, geldt ook  $r = k$  zodat  $k \geq v-1$ . Er zijn dus twee mogelijkheden: ofwel  $k = v$  ofwel  $k = v-1$ . In het eerste geval hebben we dus maar één blok en krijgen we uit  $b = v$  dat  $v = 1$ . Dit is een triviale design. In het tweede geval hebben we een triviale symmetrische design.  $\square$

**146 Lemma.** Zij  $N$  de incidentiematrix van een symmetrische  $2 - (v, k, \lambda)$ -design. Dan geldt ook

$${}^tNN = (k - \lambda)I_v + \lambda J_v$$

*Bewijs.* Elk punt behoort tot  $r = k$  blokken zodat  $NJ_v = kJ_v$ . Bovendien geldt in elke design  $J_vN = kJ_b$ . Zoals in het bewijs van stelling (142) hebben we  $\det(N^tN) \neq 0$ . Maar doordat  $N$  vierkant is, volgt hieruit dat  $\det N \neq 0$  zodat  $N$  inverteerbaar is.

Nu geldt  ${}^tN = N^{-1}N^tN = (k - \lambda)N^{-1} + \lambda N^{-1}J_v$  wegens eigenschap (140). Maar we weten ook  $N^{-1}J_v = N^{-1}(\frac{1}{k}NJ_v) = \frac{1}{k}J_v$  zodat uiteindelijk

$${}^tNN = (k - \lambda)I_v + \frac{\lambda}{k}J_vN = (k - \lambda)I_v + \lambda J_v$$

$\square$

**147 Stelling.** Twee verschillende blokken van een symmetrische  $2 - (v, k, \lambda)$ -design hebben steeds juist  $\lambda$  punten gemeenschappelijk.

*Bewijs.* Merk op dat het element op plaats  $(i, j)$  in de matrix  ${}^tNN$  juist gelijk is aan het aantal punten in de doorsnede van de blokken  $B_i$  en  $B_j$ . Gebruik nu vorig lemma.  $\square$

**148 Stelling.** Er is op isomorfisme na slechts één  $2 - (11, 5, 2)$ -design.

*Bewijs.* In een 2-design geldt steeds  $vr = bk$  en  $r(k-1) = \lambda(v-1)$ . Hieruit volgt dat een  $2 - (11, 5, 2)$ -design symmetrisch is zodat we vorige stelling kunnen toepassen. Om de existentie van zulk een design aan te tonen, gaan we zijn matrix opstellen. We zijn dus op zoek naar een  $(11 \times 11)$ -matrix met nullen en enen zodat in elke rij en elke kolom juist 5 enen staan en bovendien moet het inproduct van twee verschillende rijen of kolommen gelijk zijn aan 2. Isomorfismen van designs komen overeen met permutaties van rijen en kolommen van hun incidentiematrices. We kunnen dus veronderstellen dat de eerste rij gelijk is aan  $1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0$  en dat de eerste vijf plaatsen van de volgende tien rijen overeenkomen met de tien mogelijke combinaties van twee enen en drie nullen. Als we rekening houden met alle voorwaarden op de matrix, kunnen we nu elke rij aanvullen. Dit kan op het eerste zicht op verschillende manieren, maar je kan isomorfismen vinden tussen deze manieren.  $\square$

**149 Gevolg.** Er is op isomorfisme na slechts één  $2 - (11, 6, 3)$ -design.

*Bewijs.* Zij  $(X, \mathcal{B})$  zulk een design. Dan is deze symmetrisch. De design waarvan de blokken de complementen zijn van de blokken in  $(X, \mathcal{B})$  is een  $2 - (11, 5, 2)$ -design. Gebruik nu vorige stelling.  $\square$

**150 Stelling.** Zij  $C \subset \mathbb{F}_2^{24}$  met  $|C| = 2^{12}$  en  $\min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y} \in C\} = 8$ . Als bovendien nog  $\mathbf{0} \in C$ , is de structuur van  $C$ , op equivalentie na, uniek bepaald.





We hebben dus uiteindelijk volgende stelling.

**155 Stelling** (Tietäväinen en van Lint). *Elke niet-triviale perfecte code over een alfabet met  $p^h$  letters ( $p$  een priemgetal) heeft dezelfde parameters als één van de Golay of Hamming codes.*

Er is nog een algemenere stelling die werkt over elk alfabet.

**156 Stelling** (Best, Hong). *Voor  $t \geq 3$  is de enige niet-triviale perfecte  $t$ -foutverbeterende code (over om het even welk alfabet) de binaire Golay code.*

**Taak.** Schrijf een computerprogramma om op zoek te gaan naar mogelijke parameters van perfecte codes die niet zijn uitgesloten door de stelling van Lloyd. Verifieer dat de enige mogelijke parameters die nog geen aanleiding geven tot een gekende code juist  $[90, 2^{78}, 5]$  zijn.

## Hoofdstuk 5

# Gewichtsverdelingen

Ziehier een kort hoofdstuk over gewichtsverdelingen. We tonen het verband tussen de gewichtsverdeling van een lineaire code en zijn duale. Toepassing hiervan laat toe de gewichtsverdeling van een Hamming code in het algemeen te bepalen. Onze bewijzen zijn voor het binaire geval maar kunnen veralgemeend worden (zie bijvoorbeeld [8]).

We gebruikten de gewichtsverdeling al bij de studie van de binaire Golay code.

**157 Definitie.** Zij  $C$  een code van lengte  $n$  die  $A_i$  woorden van gewicht  $i$  heeft voor  $0 \leq i \leq n$ . De **gewichtsverdeling**  $W_C$  van  $C$  is de veelterm

$$W_C(z) := \sum_{i=0}^n A_i z^i = \sum_{\mathbf{c} \in C} z^{w(\mathbf{c})}$$

**Voorbeeld.** Voor de Golay code  $\mathcal{G}$  hebben we  $W_{\mathcal{G}} = 1 + 253z^7 + 506z^8 + 1288z^{11} + 1288z^{12} + 506z^{15} + 253z^{16} + z^{23}$ .

We beginnen met een paar technische lemma's.

**158 Lemma.** Zij  $C$  een binaire lineaire code en  $\mathbf{y}$  een vector die niet behoort tot  $C^\perp$ . Dan is juist de helft van de codewoorden orthogonaal met  $\mathbf{y}$ .

*Bewijs.* We stellen

$$A := \{\mathbf{c} \in C \mid \mathbf{c} \cdot \mathbf{y} = 0\} \quad \text{en} \quad B := \{\mathbf{c} \in C \mid \mathbf{c} \cdot \mathbf{y} = 1\}$$

Vermits  $\mathbf{y} \notin C^\perp$ , is  $B$  niet leeg zodat we  $\mathbf{b} \in B$  kunnen kiezen. Zij  $\mathbf{a} \in A$ , dan geldt  $(\mathbf{b} + \mathbf{a}) \cdot \mathbf{y} = \mathbf{b} \cdot \mathbf{y} + \mathbf{a} \cdot \mathbf{y} = 1$ , zodat  $\mathbf{b} + A \subseteq B$ . Anderzijds geldt ook voor elke  $\mathbf{b}' \in B$  dat  $(\mathbf{b} + \mathbf{b}') \cdot \mathbf{y} = \mathbf{b} \cdot \mathbf{y} + \mathbf{b}' \cdot \mathbf{y} = 1 + 1 = 0$ , zodat  $\mathbf{b} + B \subseteq A$ . Aangezien  $|\mathbf{b} + A| = |A|$  en  $|\mathbf{b} + B| = |B|$ , is het bewijs gedaan.  $\square$

**159 Gevolg.** Zij  $C$  een binaire lineaire  $[n, k, d]$ -code en  $\mathbf{y}$  een vector. Dan geldt

$$\sum_{\mathbf{c} \in C} (-1)^{\mathbf{c} \cdot \mathbf{y}} = \begin{cases} 2^k & \text{indien } \mathbf{y} \in C^\perp \\ 0 & \text{indien } \mathbf{y} \notin C^\perp \end{cases}$$

**160 Lemma.** Zij  $\mathbf{x} \in \mathbb{F}_2^n$  een vaste vector. Dan geldt in  $\mathbb{F}_2[z]$  dat

$$\sum_{\mathbf{y} \in \mathbb{F}_2^n} z^{w(\mathbf{y})} (-1)^{\mathbf{x} \cdot \mathbf{y}} = (1 - z)^{w(\mathbf{x})} (1 + z)^{n - w(\mathbf{x})}$$

*Bewijs.* Het linkerlid uitschrijven geeft

$$\begin{aligned} \sum_{\mathbf{y} \in \mathbb{F}_2^n} z^{w(\mathbf{y})} (-1)^{\mathbf{x} \cdot \mathbf{y}} &= \sum_{y_1=0}^1 \sum_{y_2=0}^1 \dots \sum_{y_n=0}^1 z^{y_1+y_2+\dots+y_n} (-1)^{x_1y_1+x_2y_2+\dots+x_ny_n} \\ &= \sum_{y_1=0}^1 \sum_{y_2=0}^1 \dots \sum_{y_n=0}^1 \left( \prod_{i=1}^n z^{y_i} (-1)^{x_i y_i} \right) \\ &= \prod_{i=1}^n \left( \sum_{j=0}^1 z^j (-1)^{x_i j} \right) \\ &= (1-z)^{w(\mathbf{x})} (1+z)^{n-w(\mathbf{x})} \end{aligned}$$

□

**161 Stelling (MacWilliams).** Zij  $C$  een binaire  $[n, k, d]$ -code. Dan geldt

$$W_{C^\perp}(z) = \frac{1}{2^k} (1+z)^n W_C\left(\frac{1-z}{1+z}\right)$$

*Bewijs.* Stel

$$f(z) := \sum_{\mathbf{c} \in C} \left( \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{c} \cdot \mathbf{y}} z^{w(\mathbf{y})} \right)$$

Vorig lemma impliceert

$$f(z) = \sum_{\mathbf{c} \in C} (1-z)^{w(\mathbf{c})} (1+z)^{n-w(\mathbf{c})} = (1+z)^n \sum_{\mathbf{c} \in C} \left( \frac{1-z}{1+z} \right)^{w(\mathbf{c})} = (1+z)^n W_C\left(\frac{1-z}{1+z}\right)$$

Anderzijds hebben we

$$f(z) = \sum_{\mathbf{y} \in \mathbb{F}_2^n} \left( \sum_{\mathbf{c} \in C} (-1)^{\mathbf{c} \cdot \mathbf{y}} z^{w(\mathbf{y})} \right) = \sum_{\mathbf{y} \in C^\perp} 2^k z^{w(\mathbf{y})} = 2^k W_{C^\perp}(z)$$

□

Met wat meer geavanceerde algebraïsche technieken kan je de algemene stelling van MacWilliams bewijzen.

**162 Stelling.** Zij  $C$  een lineaire  $[n, k, d]$ -code over  $\mathbb{F}_q$  dan geldt

$$W_{C^\perp}(z) = \frac{1}{q^k} (1+(q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right)$$

**Taak.** Bewijs de stelling van MacWilliams in het algemene geval.

**Opmerking.** Vermits voor een code  $C$  geldt  $C^{\perp\perp} = C$  hebben we

$$W_C = \frac{1}{2^{n-k}} (1+z)^n W_{C^\perp}\left(\frac{1-z}{1+z}\right).$$

Dit is nuttig indien  $k$  groot is. Dan is  $n-k$  inderdaad klein, zodat de duale code minder woorden heeft dan de code. Dan kunnen we gemakkelijker de gewichtsverdeling van de duale code bepalen. De formule van MacWilliams geeft dan de gewichtsverdeling van de code.

**Voorbeeld.** De Hamming code  $C$  van sectie 1.4 heeft als pariteitsmatrix

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

De duale code  $C^\perp$  heeft dus dimensie 3, wat kleiner is dan  $\dim C = 4$ . Je ziet gemakkelijk dat alle niet-nulle combinaties van de kolommen van  $H$  gewicht 4 hebben. Bijgevolg is  $W_{C^\perp} = 1 + 7z^4$ .

De formule van MacWilliams geeft na enig rekenwerk  $W_C = 1 + 7z^3 + 7z^4 + z^7$ . Hier lezen we onmiddellijk uit af dat de minimale afstand 3 bedraagt.

Het is tijd voor een precieze en algemene definitie van ‘‘Hamming code’’.

**163 Definitie.** De *binaire Hamming code met redundantie  $r$*  is de code  $\text{Ham}(r, 2)$  van lengte  $2^r - 1$  waarvoor in de rijen van de pariteitsmatrix alle niet-nulle vectoren van  $\mathbb{F}_2^r$  staan.

**164 Eigenschap.** Zij  $C = \text{Ham}(r, 2)$ , dan heeft elke niet-nulle vector van de duale code  $C^\perp$  gewicht  $2^{r-1}$ .

*Bewijs.* Zij  $\mathbf{y} \in C^\perp \setminus \{\mathbf{0}\}$ , dan is  $\mathbf{y}$  een lineaire combinatie  $\sum_{j=1}^r \lambda_j \mathbf{h}_j$  van de kolommen van de pariteitsmatrix  $H = [h_{ij}]$  van  $C$ . De  $i$ -de coördinaat  $y_i$  van  $\mathbf{y}$  is dan gelijk aan  $\sum_{j=1}^r \lambda_j h_{ij}$ . Het aantal nullen in  $\mathbf{y}$  is dus gelijk aan het aantal elementen in de verzameling

$$N_{\mathbf{y}} := \{i \in \{1, 2, \dots, 2^r - 1\} \mid \sum_{j=1}^r \lambda_j h_{ij} = 0\}$$

Maar deze verzameling kunnen we anders schrijven:

$$\begin{aligned} N_{\mathbf{y}} &= \{(h_{i1}, h_{i2}, \dots, h_{ir}) \text{ rij van } H \mid \sum_{j=1}^r \lambda_j h_{ij} = 0\} \\ &= \{(x_1, x_2, \dots, x_r) \in \mathbb{F}_2^r \setminus \{\mathbf{0}\} \mid \sum_{j=1}^r \lambda_j x_j = 0\} \end{aligned}$$

Deze laatste schrijfwijze toont dat  $N_{\mathbf{y}}$  eigenlijk bestaat uit de niet-nulle vectoren van het hypervlak met vergelijking  $\sum_{j=1}^r \lambda_j x_j = 0$ . Hieruit volgt  $N_{\mathbf{y}} = 2^{r-1} - 1$ .  $\square$

**165 Gevolg.**

$$W_{\text{Ham}(r, 2)}(z) = \frac{1}{2^r} \left( (1+z)^n + n(1+z)^{\frac{n-1}{2}} (1-z)^{\frac{n+1}{2}} \right)$$

waarbij  $n = 2^r - 1$ .

*Bewijs.* Dit is een oefening in het zorgvuldig rekenen.  $\square$

## Hoofdstuk 6

# Het hoofdprobleem van de lineaire codetheorie

**Notatie.** Naar analogie met de notatie  $A_q(n, d)$  van bladzijde 3-1 noteren we voor gegeven getallen  $q, n$  en  $d$  de grootste  $M$  zodat er een lineaire  $[n, M, d]$ -code bestaat met  $B_q(n, d)$ . Merk op dat  $B_q(n, d) \leq A_q(n, d)$ .

Het hoofdprobleem van de lineaire codeertheorie is dus eigenlijk om voor elke  $q, n$  en  $d$  een geheel getal  $k$  te vinden zodat  $B_q(n, d) = q^k$ . We kunnen dit ook formuleren met de redundantie  $r = n - k$ : vind de grootste  $n$  waarvoor er een lineaire  $[n, n - r, d]$ -code bestaat over  $\mathbb{F}_q$ . Dit voelt ietwat natuurlijker aan.

Stelling (75) inspireert volgende definitie.

**166 Definitie.** Gegeven zijn  $q$  een priemmacht,  $n, s$  en  $r$  gehele getallen. Een  $(n, s)$ -verzameling in  $\mathbb{F}_q^r$  is een verzameling van  $n$  vectoren zodat elke  $s$  van hen lineair onafhankelijk zijn. We noteren  $\max_s(r, q)$  de grootste  $n$  waarvoor er een  $(n, s)$ -verzameling bestaat. Een **optimale**  $(n, s)$ -verzameling is één waarvoor  $n = \max_s(r, q)$ .

Uit stelling (75) weten we dat de rijen van de pariteitsmatrix van een  $[n, k, d]$ -code steeds een  $(n, d - 1)$ -verzameling vormen. Ook een  $(n, d - 1)$ -verzameling in  $\mathbb{F}_q^r$  geeft aanleiding tot een  $[n, n - r, d]$ -code als je haar vectoren gebruikt als rijen van een pariteitsmatrix.

**167 Gevolg.** Er bestaat een bijectie tussen de  $[n, n - r, d]$ -codes over  $\mathbb{F}_q$  en de  $(n, d - 1)$ -verzamelingen van  $\mathbb{F}_q^r$ . Voor gegeven  $q, d$  en  $r$  is de grootste  $n$  waarvoor een  $[n, n - r, d]$ -code bestaat juist  $\max_{d-1}(r, q)$ .

**168 Definitie.** Een code waarvan de pariteitsmatrix bestaat uit een optimale verzameling heet **optimaal**.

**169 Stelling.** Als  $r$  zó gekozen is dat  $\max_{d-1}(r - 1, q) < n \leq \max_{d-1}(r, q)$ , dan geldt  $B_q(n, d) = q^{n-r}$ .

*Bewijs.* Onderstel dat  $n \leq \max_{d-1}(r, q)$ . Dan bestaat er zeker een  $[n, n - r, d]$ -code zodat  $B_q(n, d) \geq q^{n-r}$ .

Indien  $B_q(n, d) > q^{n-r}$  zou zijn, zou er zeker een  $[n, n - r + 1, d]$ -code bestaan. Maar dan geldt  $n \leq \max_{d-1}(r - 1, q)$ ,  $\uparrow$ .  $\square$

We zullen nu voor enkele speciale waarden van parameters  $\max_{d-1}(r, q)$  bepalen.

**170 Stelling.** Gegeven  $q, d$  en  $r$ , geldt

$$\max_2(r, q) = \frac{q^r - 1}{q - 1}$$

*Bewijs.* Je zoekt zo groot mogelijke  $(n, 2)$ -verzamelingen in  $\mathbb{F}_q^r$ . In zulke verzameling zijn alle vectoren twee aan twee lineair onafhankelijk. Dit komt erop neer dat je nooit twee vectoren in eenzelfde één-dimensionale deelruimte mag kiezen. Een optimale verzameling bekom je door in elke één-dimensionale deelruimte juist één (niet-nulle) vector te kiezen. Zo zijn er juist  $\frac{q^r - 1}{q - 1}$ .  $\square$

De codes die overeenkomen met de optimale verzamelingen uit vorige stelling zijn juist de Hammingcodes  $\text{Ham}(r, q)$ . Deze zijn niet alleen optimaal maar ook perfect.

**171 Gevolg.** Als je voor gegeven  $q$  en  $n$  een geheel getal  $r$  zodanig kiest dat  $\frac{q^{r-1}-1}{q-1} < n \leq \frac{q^r-1}{q-1}$ , dan geldt  $B_q(n, 3) = q^{n-r}$ .

**Oefening.** Bewijs dat  $B_q(n, 3) = q^{\lfloor n - \log_q(nq - n + 1) \rfloor}$ .

We merkten vroeger reeds op dat de rijen van de pariteitsmatrix van een Hamming code overeenkomen met (homogene) coördinaten van de punten van een projectief vlak. De interpretatie van een  $(n, s)$ -verzameling in een projectieve ruimte zal later van pas komen.

**172 Definitie.** Een  $(n, s)$ -**verzameling** in een projectieve ruimte  $P^{r-1}(\mathbb{F}_q)$  is een verzameling van  $n$  punten zodat elke  $s$  van hen projectief onafhankelijk zijn.

Voor  $d = 4$  (één fout verbeteren, twee detecteren) gaan we dus op zoek naar  $(n, 3)$ -verzamelingen. Deze komen overeen met verzamelingen van punten in een projectieve ruimte waarvan geen drie collineair zijn.

**173 Definitie.** Een verzameling punten van de projectieve ruimte  $P^{r-1}(\mathbb{F}_q)$  waarin geen drie punten collineair zijn, heet een **hoog** als  $r = 3$  en een **kap** voor  $r > 3$ .

**174 Stelling.** Als  $d$  oneven is, bestaat er een binaire lineaire  $[n, k, d]$ -code **als en slechts als** er een binaire lineaire  $[n+1, k, d+1]$ -code bestaat.

*Bewijs.* We bewezen dit reeds in stelling (62). Je hoeft enkel te verifiëren dat de lineariteit bewaard blijft. □

**175 Gevolg.** Onderstel dat  $d$  even is. Dan gelden

- (i)  $B_2(n, d) = B_2(n-1, d-1)$  en
- (ii)  $\max_{d-1}(r, 2) = \max_{d-2}(r-1, 2) + 1$

*Bewijs.* De eerste bewering volgt direct uit vorige stelling.

Als  $n \leq \max_{d-1}(r, 2)$  weten we dat er een binaire  $[n, n-r, d]$ -code bestaat. Vorige stelling geeft dan onmiddellijk een  $[n-1, n-r, d-1]$ -code zodat  $n-1 \leq \max_{d-2}(r-1, 2)$ . □

**176 Gevolg.** Er geldt  $\max_3(r, 2) = 2^{r-1}$ .

*Bewijs.* We weten uit stelling (170) dat  $\max_2(r-1, 2) = 2^{r-1} - 1$  zodat toepassing van vorig gevolg het resultaat geeft. □

We zien dat de optimale binaire codes met  $d = 4$  de *uitgebreide Hamming codes* zijn. Dit zijn de gewone Hamming codes  $\text{Ham}(r, 2)$  met een pariteitscontrole toegevoegd (volgens het bewijs van stelling (174)).

**Oefening.** De rijen van de pariteitsmatrix van zulk een uitgebreide Hamming code vormen een kap in  $P^{r-1}(\mathbb{F}_2)$  die bestaat uit alle punten buiten een hypervlak.

Nu construeren we grote bogen in projectieve vlakken.

**177 Stelling.** Zij  $a_1, a_2, \dots, a_{q-1}$  de niet-nulle elementen van een eindig lichaam  $\mathbb{F}_q$  en beschouw de matrices

$$H = \begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ \vdots & \vdots & \vdots \\ 1 & a_{q-1} & a_{q-1}^2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{en} \quad H' = \begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ \vdots & \vdots & \vdots \\ 1 & a_{q-1} & a_{q-1}^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

De rijen van  $H$  vormen een boog in  $P^2(\mathbb{F}_q)$  en als  $q$  even is vormen de rijen van  $H'$  ook een boog in  $P^2(\mathbb{F}_q)$ .

*Bewijs.* Merk op dat vele deelmatrices van  $H$  “Vandermondematrices” zijn. Het is duidelijk dat de rang van  $H$  drie bedraagt.

In het even geval moeten we enkel nog de deelmatrices bekijken die de bijkomende rij  $(0, 1, 0)$  bevatten. We berekenen

$$\det \begin{pmatrix} 1 & a_i & a_i^2 \\ 1 & a_j & a_j^2 \\ 0 & 1 & 0 \end{pmatrix} = a_i^2 - a_j^2 = (a_i - a_j)^2 \neq 0$$

□

**178 Gevolg.**

$$\max_3(3, q) \geq \begin{cases} q+1 & \text{voor } q \text{ oneven} \\ q+2 & \text{voor } q \text{ even} \end{cases}$$

**Opmerking.** De boog met  $q+1$  punten van vorige stelling is eigenlijk de projectieve *kegelsnede*  $\{(x, y, z) \in P^2(\mathbb{F}_q) \mid xz = y^2\}$ .

De geconstrueerde bogen zijn ook optimaal.

**179 Stelling.** Voor elke priemmacht  $q$  geldt  $\max_3(3, q) \leq q+2$ . Als  $q$  oneven is, geldt bovendien  $\max_3(3, q) \leq q+1$ .

*Bewijs.* Zijn  $\mathcal{K}$  een optimale boog in  $P^2(\mathbb{F}_q)$ . Er geldt dus  $|\mathcal{K}| = \max_3(3, q)$ . Kiezen we een punt  $p \in \mathcal{K}$ , dan zijn er door  $p$  juist  $q+1$  rechten in  $P^2(\mathbb{F}_q)$ . Natuurlijk kan een rechte door  $p$  ten hoogste één bijkomend punt van de boog  $\mathcal{K}$  bevatten. Hieruit volgt  $|\mathcal{K}| \leq (q+1) + 1 = q+2$ .

Onderstel nu dat  $q$  oneven is en dat  $|\mathcal{K}| = q+2$ . Dan *moet* elke rechte door een punt  $p \in \mathcal{K}$  een tweede punt van  $\mathcal{K}$  bevatten. Bijgevolg zal elke rechte van  $P^2(\mathbb{F}_q)$  de boog  $\mathcal{K}$  ontmoeten in nul of twee punten. Nemen we een punt  $r$  buiten  $\mathcal{K}$ , dan zullen er bijvoorbeeld  $t$  rechten door  $r$  de boog snijden in twee punten. Dit toont aan dat  $|\mathcal{K}| = 2t$ , maar we hadden dat  $|\mathcal{K}| = q+2$ , een oneven getal,  $\frac{1}{2}$ . □

**Opmerking.** Er bestaat ook een algebraïsch bewijs van vorige stelling. Maar het is veel langer.

We hebben dus volgende stelling aangetoond.

**180 Stelling.**

$$\max_3(3, q) = \begin{cases} q+1 & \text{voor } q \text{ oneven} \\ q+2 & \text{voor } q \text{ even} \end{cases}$$

In 1954 bewees SEGRE dat elke boog met  $q+1$  punten in een projectief vlak  $P^2(\mathbb{F}_q)$  met  $q$  oneven een kegelsnede is. Bijgevolg zijn alle optimale bogen in dit geval projectief equivalent. Er is dus ook een unieke optimale code.

In het even geval bestaan er optimale bogen die geen kegelsneden zijn. Nog niet alle optimale bogen zijn gekend in projectieve vlakken van even orde.

**181 Stelling.** Voor  $q$  een oneven priemmacht geldt  $\max_3(4, q) \leq q^2 + 1$ .

*Bewijs.* Zij  $\mathcal{K}$  een optimale kap in  $P^3(\mathbb{F}_q)$  en kies twee punten  $p_1$  en  $p_2$  op  $\mathcal{K}$ . We noteren de rechte door  $p_1$  en  $p_2$  met  $L$  en merken op dat  $L \cap \mathcal{K} = \{p_1, p_2\}$ . Onze ervaring met projectieve ruimten leert ons dat er juist  $q+1$  vlakken zijn die  $L$  omvatten. Elk vlak door  $L$  dat  $\mathcal{K}$  snijdt in meer dan alleen  $p_1$  en  $p_2$  moet  $\mathcal{K}$  snijden in een boog. Dus bevat elk vlak door  $L$  ten hoogste  $q+1$  punten van  $\mathcal{K}$ . Hieruit volgt  $|\mathcal{K}| \leq (q+1)(q-1) + 2 = q^2 + 1$ . □

We tonen nu dat er wel degelijk een kap met  $q^2 + 1$  punten bestaat in  $P^3(\mathbb{F}_q)$ , met  $q$  oneven.

**182 Stelling.** Zij  $q$  een oneven priemmacht en  $b$  geen kwadraat in  $\mathbb{F}_q$ . Dan is de verzameling

$$\mathcal{Q} := \{(x, y, z, t) \in P^3(\mathbb{F}_q) \mid tz = x^2 - by^2\}$$

een kap met  $q^2 + 1$  punten.

*Bewijs.* Stel eerst even  $z = 0$ . Dan zie je dat de punten van  $\mathcal{Q}$  met nulle  $z$ -coördinaat voldoen aan  $x^2 = by^2$ . Als  $y \neq 0$  vinden we  $b = \left(\frac{x}{y}\right)^2$ ,  $\frac{x}{y}$ . Dus is het enige punt met nulle  $z$ -coördinaat in  $\mathcal{Q}$  noodzakelijk  $(0, 0, 0, 1)$ . Voor alle andere punten kunnen we  $z = 1$  nemen. We krijgen dus

$$\mathcal{Q} = \{(0, 0, 0, 1)\} \cup \{(x, y, 1, x^2 - by^2) \mid x, y \in \mathbb{F}_q\}$$

Hieruit volgt  $|\mathcal{Q}| = q^2 + 1$ .

Nu nog tonen dat  $\mathcal{Q}$  geen drie collineaire punten bevat. Als één van die drie  $(0, 0, 0, 1)$  is, moeten er dan  $\lambda, \mu, r, s \in \mathbb{F}_q$  bestaan met  $\lambda(x, y, 1, x^2 - by^2) + \mu(0, 0, 0, 1) = (r, s, 1, r^2 - bs^2)$ . Hiervoor moet zeker  $\lambda = 1$  zijn, waaruit volgt  $r = x$  en  $s = y$ .

Neem nu een rechte door twee punten  $(x, y, 1, x^2 - by^2)$  en  $(r, s, 1, r^2 - bs^2)$  van  $\mathcal{Q}$ , verschillend van  $(0, 0, 0, 1)$ . Dan moeten de coördinaten van een zekere lineaire combinatie hiervan voldoen aan de vergelijking die  $\mathcal{Q}$  bepaalt. We mogen een coëfficiënt van de combinatie gelijk nemen aan 1 zodat we bekomen dat  $(1 + \lambda)(x^2 - by^2 + \lambda r^2 - \lambda bs^2) = (x + \lambda r)^2 - b(y + \lambda s)^2$ , voor een niet-nulle  $\lambda$ . Hieruit volgt na vereenvoudiging dat  $\left(\frac{x+r}{y+s}\right)^2 = b$ , een tegenspraak tenzij  $y = s$  en  $x = r$ . □

**183 Gevolg.** Voor  $q$  oneven geldt  $\max_3(4, q) = q^2 + 1$ .

**Voorbeeld.** Nemen we in vorige stelling  $q = 3$  en  $b = -1$ , dan bekomen we een kap met tien punten. De pariteitsmatrix van de optimale  $[10, 6, 4]$ -code over  $\mathbb{F}_3$  is

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

**Opmerking.** De verzameling  $\mathcal{Q}$  van stelling (182) is eigenlijk een projectieve kwadriek. Deze kwadriek omvat geen rechten en wordt daarom een *elliptische kwadriek* genoemd (lijkt meer op een ellipsoïde dan op een hyperboloïde die wel rechten omvat).

In 1965 bewees BARLOTTI dat elke kap met  $q^2 + 1$  punten in  $P^3(\mathbb{F}_q)$  voor  $q$  oneven een elliptische kwadriek is. Alle elliptische kwadrieken zijn projectief equivalent zodat ook hier de optimale kappen en codes op equivalentie na uniek zijn.

Voor  $q > 2$  even geldt ook dat  $\max_3(4, q) = q^2 + 1$ . Het bewijs is een beetje moeilijker dan dat van stelling (182) en werd voor het eerst gegeven door QVIST in 1952. In het even geval is nog geen “stelling van Barlotti” gekend. De beste benadering is een stelling van BROWN. Zij  $\mathcal{K}$  een kap met  $q^2 + 1$  punten in  $P^3(\mathbb{F}_q)$  met  $q$  even. In 1997 bewees BROWN dat indien er minstens één vlak  $V$  bestaat waarvoor  $V \cap \mathcal{K}$  een kegelsnede is, de kap  $\mathcal{K}$  een elliptische kwadriek moet zijn.

**Taak.** Bewijs de gelijkheid  $\max_3(4, q) = q^2 + 1$  voor  $q$  even.

Met wat we weten over  $\max_3(r, q)$  voor  $r = 2$  of  $3$ , kunnen we gemakkelijk volgende stelling bewijzen.

**184 Stelling.** Zij  $q$  een priemmacht.

- (i) Indien  $q$  oneven is, geldt  $B_q(n, 4) = \begin{cases} q^{n-3} & \text{voor } 4 \leq n \leq q + 1 \\ q^{n-4} & \text{voor } q + 2 \leq n \leq q^2 + 1 \end{cases}$
- (ii) Indien  $q$  even is, geldt  $B_q(n, 4) = \begin{cases} q^{n-3} & \text{voor } 4 \leq n \leq q + 2 \\ q^{n-4} & \text{voor } q + 3 \leq n \leq q^2 + 1 \end{cases}$

Het bepalen van  $\max_3(r, q)$  voor  $r > 4$  is veel moeilijker. In 1970 vond PELLEGRINO kappen met 20 punten in  $P^4(\mathbb{F}_3)$ . Na een tijd kon hij ook bewijzen dat  $\max_3(5, 3) = 20$ . Voor de volgende dimensie was het daarentegen gemakkelijk te tonen dat  $\max_3(6, 3) \leq 56$  maar het was pas in 1973 dat HILL echt een kap met 56 punten kon construeren.

In 6 dimensies weet men enkel

$$112 \leq \max_3(7, 3) \leq 137.$$

Kappen en bogen zijn een zeer belangrijk onderzoeksgebied van de eindige meetkunde. Een overzicht van het recent onderzoek op dat gebied vind je in een artikel<sup>1</sup> van HIRSCHFELD en STORME, twee wereldexperts.

---

<sup>1</sup>J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. <http://cage.ugent.be/~ls/max2000finalprocfilejames.ps>

# Bibliografie

- [1] Martin Aigner and Günter M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin, 1999.
- [2] Norman Biggs. *Discrete Mathematics*. Clarendon Press, Oxford, revised edition, 1989.
- [3] P. J. Cameron and J. H. van Lint. *Designs, graphs, codes and their links*. Cambridge University Press, Cambridge, 1991.
- [4] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.
- [5] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.2*, 1999. (<http://www-gap.dcs.st-and.ac.uk/~gap>).
- [6] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics, an Applied Introduction*. Addison-Wesley, New York, second edition, 1989.
- [7] Raymond Hill. *A First Course in Coding Theory*. Oxford University Press, Oxford, 1988.
- [8] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.
- [9] Oliver Pretzel. *Error-Correcting Codes and Finite Fields*. Oxford University Press, Oxford, 1996.
- [10] Steven Roman. *Coding and Information Theory*. Springer-Verlag, New York, 1992.
- [11] Ian Stewart. *Galois Theory*. Chapman and Hall, London, second edition, 1989.
- [12] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, Cambridge, second edition, 2001.

# Index

- $(n, s)$ -verzameling, 6-1, 6-2
- $t - (v, k, \lambda)$ -design, 4-10
- (enkelvoudige) pariteitscontrole, 1-2
  
- afgeleid Steiner systeem, 4-6
- alfabet, 1-4, 3-1
- algebraïsch, 3-9
- anti-vijfhoek, 4-3
- automorfisme van een Steiner systeem, 4-7
- axiomatische projectieve ruimte, 4-1
  
- BCH code, 3-8
- binaire, 3-1
- binaire Hamming code, 5-3
- blok, 4-5
- blokken, 4-6, 4-10
- bol, 1-6
- boog, 6-2
  
- code, 1-4
- coderen, 3-3
- codewoord, 3-1
- codewoorden, 1-4
- compositiefactoren, 4-8
- compositierij, 4-8
- congruent, 2-2
- cyclische code, 3-5
  
- deling, 2-2
- dimensie, 4-2
- drager, 4-1
- duale code, 3-3
  
- equivalent, 3-3
- equivalent in brede zin, 3-1
- Euklidisch delingsalgoritme, 2-2
  
- Frobenius automorfisme, 2-7
  
- generator, 3-5
- generator van de code, 3-5
- genererende matrix, 3-3
- gewicht, 3-4
- gewichtsverdeling, 5-1
- Golay codes, 4-4
  
- Hamming afstand, 1-4
  
- icosaëder, 4-3
- incidentiematrix, 4-11
- informatie-inhoud, 1-3
- irreduciebel, 2-2
  
- kap, 6-2
- karacteristiek, 2-3
  
- lengte, 1-3, 1-4, 3-1
- letters, 1-4, 3-1
- lichaam, 2-1
- lineaire, 3-3
  
- Mathieu groepen, 4-7
- maximum distance separating codes, 3-2
- MDS codes, 3-2
- minimale afstand, 1-4, 3-1
- minimale veelterm, 3-9
- monisch, 2-2
  
- nuldeler, 2-1
  
- optimale, 6-1
- optimale code, 6-1
- orde, 2-6, 3-7
  
- pariteitsmatrix, 3-4
- perfect, 1-6
- priemveld, 2-3
- primitief, 2-6
- primitieve  $n$ -de eenheidswortel, 3-7
- projectief gesloten, 4-2
- projectief onafhankelijk, 4-2
- projectieve sluiting, 4-2
- punt, 4-5
- punten, 4-1, 4-6, 4-10
  
- quotiënt, 2-2
  
- rechten, 4-1
- rechtse shift, 3-5
- redundante informatie, 1-1
- Reed-Solomon codes, 3-10
- repetitiecode, 3-1
- rest, 2-2
  
- Singleton grens, 3-2

standaardvorm, 3-3  
Steiner systeem, 4-6  
sterkte, 4-10  
symbolen, 1-4, 3-1  
symmetrisch, 4-12  
syndroomvector, 1-6

ternaire, 3-1  
transcendent, 3-9  
triviale symmetrische design, 4-12

uitgebreide Golay code, 4-8

veeltermring, 2-1  
veld, 2-1

woorden, 1-4, 3-1