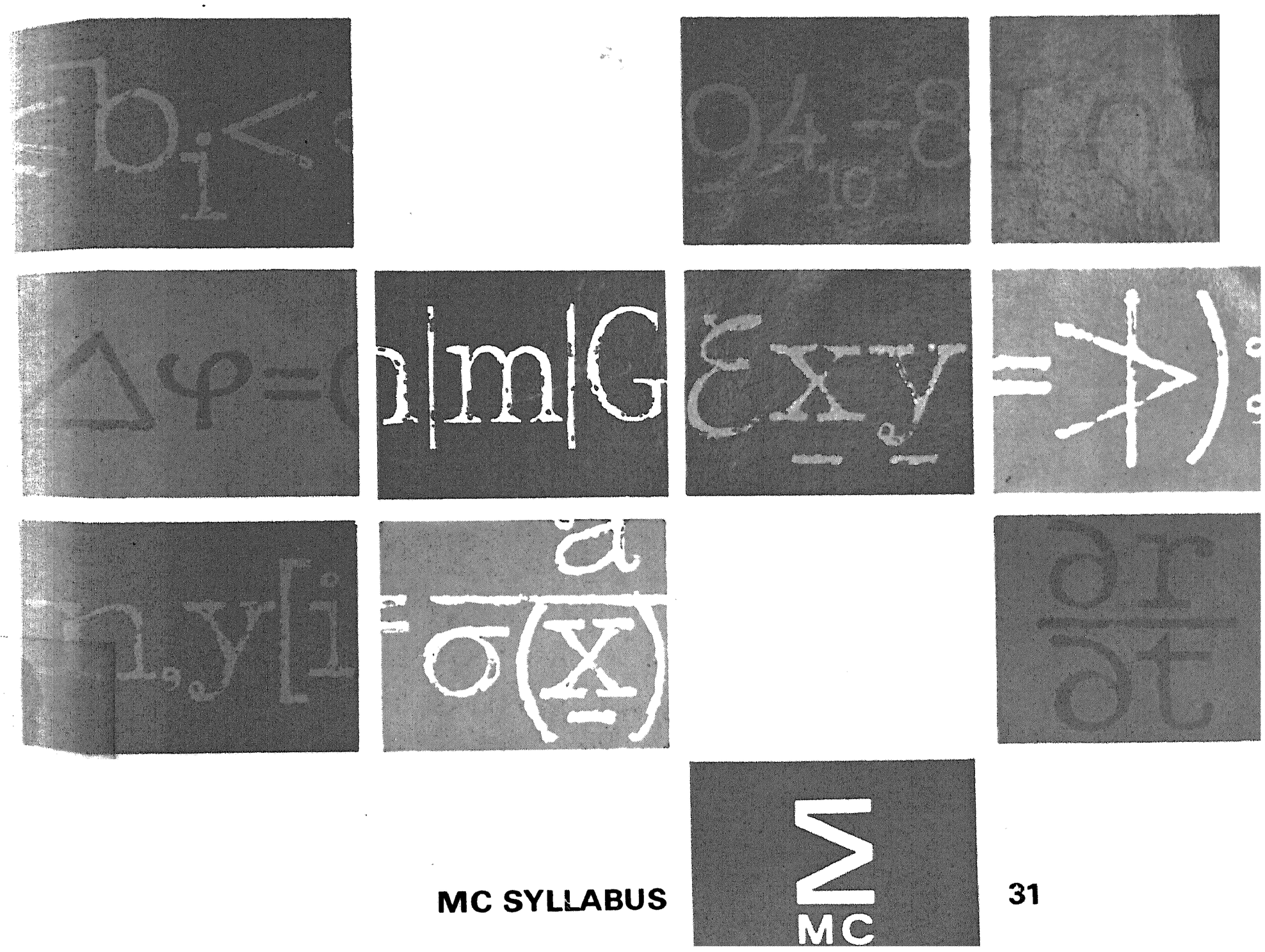
INLEIDING IN DE CODERINGSTHEORIE

J.H. VAN LINT (red.)



MC SYLLABUS 31

MC SYLLABUS 31

J.H. VAN LINT (red.)

INLEIDING IN DE CODERINGSTHEORIE

TWEEDE DRUK

MATHEMATISCH CENTRUM AMSTERDAM 1980

1980 Mathematics subject classification: 94A10

ISBN 90 6196 136 X

Eerste druk 1976
Tweede druk 1980

INHOUD

Inhoud v
Voorwoord ix
0. Voorbereidingen (J.H. van Lint)
0.1. Algebra 1
0.2. Getaltheorie 5
0.3. Combinatoriek 6
0.4. Waarschijnlijkheidsrekening 8

1. De stelling van Shannon (J.H. van LINT)
1.1. Inleiding 10
1.2. De stelling van Shannon 14
1.3. Commentaar 17

2. Voorbeelden van codes (J.H. van Lint)
2.1. De (7,4)-Hamming code 19
2.2. Hadamard codes en generalisaties 19
2.3. De binaire Golay code en afgeleiden 20
2.4. De ternaire Golay code 21
2.5. Combinatie van codes 22
2.6. Commentaar 23
2.7. Opgaven 23

3. Lineaire codes (T.M.V. Janssen, J.H. van Lint)
3.1. Blok codes 25
3.2. Lineaire codes 26
3.3. Foutenverbetering 27
3.4. Hamming codes 29
3.5. Drempel decodering 30
3.6. De weight enumerator en de McWilliams identiteit 32
3.7. Commentaar 35
3.8. Opgaven 36

4. Grenzen aan codes (M.R. Best)
4.1. Inleiding 38
4.2. Ondergrens 39
4.3. Bovengrenzen 42

I. De Singleton bound 42
II. De Plotkin bound en de Griesmer bound 43
III. De Hamming bound 45
IV. De Elias bound 46
V. De Johnson bound 49
VI. De linear-programming bound 52
4.4. Commentaar 57
4.5. Opgaven 58

5. Cyclische codes (A.E. Brouwer, A. Schrijver)
5.1. Cyclische codes 60
5.2. Generator matrix en check polynoom 61
5.3. Nulpunten van een cyclische code 63
5.4. De idempotent van een cyclische code 65
5.5. BCH-codes 65
5.6. Een procedure voor het corrigeren van fouten bij BCH-codes . . 69
5.7. Reed-Solomon codes 70
5.8. Kwadraatrest-codes 71
5.9. Commentaar 74
5.10. Opgaven 75

6. Reed-Muller codes en de stelling van Chevalley
(P. van Emde Boas, J.H. van Lint)
6.1. Voorbereidingen 77
6.2. Binaire Reed-Muller codes 81
6.3. Functies en polynomen over eindige lichamen 84
6.4. De stelling van Chevalley en generalisaties 86
6.5. De gegeneraliseerde Reed-Muller codes 88
6.6. Bewijs der Reed-Muller grens 91
6.7. Alternatieve beschrijving der Reed-Muller code 95
6.8. Dualiteit van Reed-Muller codes 99
6.9. Commentaar 100
6.10. Opgaven 100

7. Gelijkmatig verdeelde codes (J.H. van Lint, H.C.A. van Tilborg)
7.1. Inleiding 102
7.2. Krawtchouk polynomen 103
7.3. Het karakteristieke polynoom van een code 106

7.4. Gelijkmatig verdeelde codes 107
7.5. Voorbeelden 110
7.6. Nonexistentie stellingen 114

8. Goppa codes (A.E. Brouwer)
8.1. Motivatie 118
8.2. Goppa codes 119
8.3. Minimum afstand van Goppa codes 120
8.4. Asymptotisch gedrag van Goppa codes 122
8.5. Het Mattson-Solomon polynoom 123
8.6. Commentaar 126
8.7. Opgaven 127

9. Asymptotisch goede algebraische codes (J.H. van Lint)
9.1. Een eenvoudig niet-constructief bewijs 128
9.2. Justesen codes 129
9.3. Directe constructie 133
9.4. Commentaar 135
9.5. Opgaven 135

10. Arithmetische codes (H.W. Lenstra Jr.)
10.1. AN-codes 136
10.2. Perfecte cyclische AN-codes van orde 1 140
10.3. Berekening van het arithmetische en modulaire gewicht 144
10.4. Mandelbaum-Barrows codes 148
10.5. Chen-Chien-Liu codes 151
10.6. Opgaven 158

Literatuur 159

VOORWOORD

In augustus 1975 werd door de afdeling Zuivere Wiskunde van het Mathematisch Centrum een studieweek gehouden over Coderingstheorie. Uit de syllabus, die bij die gelegenheid aan de deelnemers werd uitgereikt, is dit boekje ontstaan.

De voorbereiders van de Studieweek stelden zich tot doel belangstellenden, die wel over enige wiskundige basiskennis beschikten, maar van wie niet werd verwacht dat zij al iets van codes afwisten, een degelijke kennis bij te brengen van een representatief deel van de algebraïsche codetheorie. Bij de nu voorliggende nadere uitwerking is meer in het bijzonder gedacht aan wiskunde-studenten als lezers en gebruikers. De schrijvers hopen dat dit boek een bruikbare handleiding zal blijken te zijn bij menig college over dit interessante en zich nog snel ontwikkelende onderwerp.

Vooral ten behoeve van student-lezers is in hoofdstuk 0 een korte opsomming bijeengebracht van benodigde voorkennis. Waarschijnlijk staat voor iedere lezer in die opsomming zowel te veel als te weinig; moge de gemiddelde lezer er toch baat bij vinden.

De belangstelling binnen het Mathematisch Centrum voor de Coderingstheorie is gewekt en aangewakkerd door onze adviseur J.H. van Lint. Onder zijn leiding hebben enige medewerkers van de afdeling Zuivere Wiskunde, tezamen met een groepje belangstellenden, afkomstig van diverse Universiteiten en Hogescholen, zich in dit vakgebied ingewerkt. Ook de leiding van de Studieweek 1975 berustte bij hem.

Wij waarderen het zeer dat Van Lint bereid was de syllabus van de Studieweek nog eens kritisch te bezien, hem te verbeteren en aan te vullen, en waar nodig (en 't was nog al eens nodig!) te herschrijven. Voor zover dit boekje eenheid toont, is die eenheid aan hem te danken.

Maar door de eenheid heen blijven de afzonderlijke bijdragen van de verschillende auteurs - docenten op de Studieweek - naar stijl en opzet herkenbaar. Zonder hun inzet en hun noeste vlijt was die Studieweek niet tot stand gekomen, en was dus ook dit boek niet verschenen. Aan die docenten, te weten J.H. van Lint en H.C.A. van Tilborg (THE), H.W. Lenstra, jr. (UvA), en M.R. Best, A.E. Brouwer, P. van Emde Boas, T.M.V. Janssen en A. Schrijver (MC), zij hierbij dank gebracht. Hun bijdragen zijn, min of meer gewijzigd, in verschillende hoofdstukken van deze verhandeling terug te vinden. Hoofdstuk 9 is na de Studieweek toegevoegd.

Dit is het eerste boek over Coderingstheorie in de Nederlandse taal. Dat heeft zijn consequenties voor de aard van het gebruikte Nederlands. Vele vaktechnische termen zijn niet uit het Engels vertaald, omdat nog geen gangbaar en geaccepteerd Nederlands aequivalent is aangewezen. Wij hopen dat velen dit boekje zullen gebruiken: dan zullen enerzijds steeds meer Nederlanders over Coderingstheorie praten, waarbij hopelijk goed-Nederlandse termen ingeburgerd zullen raken waar nu nog Engelse uitdrukkingen worden gebruikt; anderzijds zal dit boekje dan (vele?) herdrukken beleven, en in die herdrukken kunnen dan de nieuwe termen worden overgenomen. Met het oog op die mogelijke herdrukken worden de gebruikers vriendelijk verzocht ook andere verbeteringen of essentieel geachte aanvullingen te melden aan het Mathematisch Centrum, t.a.v. de afdeling Zuivere Wiskunde. Eén lezer, C. Roos (THD), heeft dat al gedaan: zijn lange lijst met correcties is verwerkt, hetgeen de kwaliteit van dit boekje duidelijk ten goede is gekomen.

Amsterdam, Augustus 1976

P.C. Baayen.

Bij de Tweede druk.

De voortdurende belangstelling voor deze "Inleiding in de Coderingstheorie" maakt een tweede druk noodzakelijk. Afgezien van enkele kleine correcties is deze druk identiek aan de vorige.

Amsterdam, December 1980

P.C. Baayen.

0. VOORBEREIDINGEN

In de in dit boek beschreven cursus wordt nogal wat voorkennis van de lezer vereist. De belangrijkste gebieden waar hij enigszins thuis moet zijn zijn algebra, combinatoriek, elementaire getaltheorie, waarschijnlijkheidsrekening. We geven in dit hoofdstuk een snel overzicht van veel gebruikte begrippen en stellingen. Voor de algemene theorie en voor bewijzen raadplege men een van de vele leerboeken over deze vakken. We gebruiken algemeen bebekende notaties. (Met $|C|$ geven we het aantal elementen van de verzameling C aan; $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$ en evenzo $\lceil x \rceil$ voor afronden naar boven.)

0.1. ALGEBRA

We zullen veel gebruik maken van lineaire algebra, o.a. begrippen als vectorruimte over een lichaam, lineaire deelruimte, lineaire afbeelding, inwendig product van vectoren (N.B. vectoren geven we aan door onderstreepte symbolen, het inwendig product met $\langle \underline{x}, \underline{y} \rangle$), matrixvermenigvuldiging, etc. worden allemaal bekend verondersteld.

(0.1.1) <u>DEFINITIE</u>. Een verzameling met productoperatie (G,) heet een *groep* als

() $\forall_{a \in G} \forall_{b \in G} [ab \in G]$,

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

(ii) $\exists_{e \in G} \forall_{a \in G} [ae = ea = a]$,
(er is dan precies één e met deze eigenschap),

(iii) $\forall_{a \in G} \exists_{b \in G} [ab = ba = e]$.

Als bovendien

(iv) $\forall_{a\in G} \forall_{b\in G} [ab = ba]$

dan heet de groep *abels* of *commutatief*.

Is (G,) een groep en $H\subset G$ en (H,) een groep, dan noemt men (H,) een *ondergroep* van (G,). Meestal schrijft men G i.p.v. (G,). Het aantal elementen van een eindige groep heet de *orde* van de groep. Is (G,) een groep en $a \in G$ dan heet de kleinste positieve n zó dat $a^n = e$ - indien deze bestaat - de *orde* van a. De elementen $e, a, a^2, \ldots, a^{n-1}$ vormen een zgn. *cyclische* groep met *voortbrenger* a. Als (G,) een abelse groep is en (H,) een ondergroep dan noemt men de verzamelingen $aH := \{ah \mid h\in H\}$ *nevenklassen* van H. Daar twee nevenklassen identiek of disjunct zijn vormen de nevenklassen een partitie van G. De nevenklassen kunnen we aangeven door uit elke klasse een zgn. *representant* te kiezen. Het is niet moeilijk in te zien dat de nevenklassen zelf een groep vormen als we definieren $(aH)(bH) := ab\,H$. Deze groep heet de *factorgroep* en wordt aangegeven met G/H.

(0.1.2) <u>DEFINITIE</u>. Een verzameling met twee bewerkingen (R,+,) heet een *ring* als:

(i) (R,+) is een abelse groep,

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

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

Als bovendien geldt

(iv) $\forall_{a\in R} \forall_{b\in R} [ab=ba]$

dan heet de ring *commutatief*.

(0.1.3) <u>DEFINITIE.</u> Is (R,+,) een ring en $\emptyset \neq S \subset R$ dan heet S een *ideaal* als:

(i) $\forall_{a\in S} \forall_{b\in S} [a-b \in S]$,

(ii) $\forall_{a\in S} \forall_{b\in R} [ab \in S \wedge ba \in S]$.

(0.1.4) <u>DEFINITIE</u>. Een *lichaam* is een ring (R,+,) waarvoor $(R\setminus\{0\},)$ een abelse groep is.

(0.1.5) <u>STELLING</u>. *Iedere eindige ring met tenminste twee elementen waarin geldt*

$$ab = 0 \Rightarrow (a=0 \vee b=0)$$

is een lichaam.

Is S een ideaal in de ring (R,+,) dan is (S,+) een ondergroep van (R,+). We kunnen de factorgroep vormen. De nevenklassen noemen we nu *restklassen mod* S. Hiervoor kunnen we ook vermenigvuldiging op voor de hand liggende manier definieren. We vinden dan een ring, de zgn. *restklassenring* R *mod* S (= R/S). Nemen we bijv. R:= $\mathbb{Z}$ en S het ideaal van alle p-vouden (p priem, notatie $p\mathbb{Z}$ of (p)) dan vinden we de ring van gehele getallen modulo p (= $\mathbb{Z}/p\mathbb{Z}$).

(0.1.6) STELLING. $\mathbb{Z}/p\mathbb{Z}$ *is een lichaam.*

Een ring die vaak gebruikt zal worden is de ring van alle polynomen $a_0 + a_1x + \ldots + a_nx^n$ met coefficienten a_i in een lichaam $\mathbb{F}$ en n = 0,1,... . Deze ring geven we aan met $\mathbb{F}[x]$. Is g(x) een polynoom dan vormen alle veelvouden van g(x) (d.w.z. alle polynomen a(x) g(x) met $a(x) \in \mathbb{F}[x]$) een ideaal in $\mathbb{F}[x]$ dat we aangeven met (g(x)). De restklassenring $\mathbb{F}[x]/(g(x))$ kunnen we dan representeren met de polynomen waarvan de graad kleiner is dan de graad van g(x). Optelling en vermenigvuldiging geschieden dan op de "gewone" manier, gevolgd door reductie modulo g(x) (dus: bepaal de rest bij deling door g(x)).

Is $\mathbb{F}$ een lichaam met n elementen dan geeft men $\mathbb{F}$ ook wel aan als $\mathbb{F}_n$ of GF(n) (Galois field). We gebruiken beide notaties regelmatig en door elkaar! Men kan bewijzen dat als $n = p^r$ (p priem, $r \geq 1$) er (op isomorfie na) één lichaam $\mathbb{F}_n$ is en anders geen. Een constructie van $GF(p^r)$ gaat als volgt. Laat g(x) een irreducibel polynoom zijn van de graad r in $\mathbb{F}_p[x]$. Zo'n polynoom is er (zie o.a. BERLEKAMP (1968)). De restklassenring $\mathbb{F}_p[x]/(g(x))$ is een lichaam.

(0.1.7) STELLING. *In* $(GF(p^r),+,\ )$ *is de groep* $(GF(p^r)\backslash\{0\},\ )$ *cyclisch. Een voortbrenger van deze groep heet primitief element van het lichaam.*

(0.1.8) VOORBEELD. Het polynoom $x^4 + x + 1$ is irreducibel over $\mathbb{F}_2$. De restklassenring $\mathbb{F}_2[x]/(x^4+x+1)$ bestaat uit

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

Hier is het polynoom x een voorbrenger van de multiplicatieve groep van GF(16). Dus x is een primitief element. Uit de constructie zien we verder dat $GF(p^r)$ een r-dimensionale vectorruimte over GF(p) is. Hierbij interesseert ons voornamelijk de additieve structuur van $GF(p^r)$.

Uit stelling (0.1.7) is eenvoudig in te zien dat $GF(p^r)$ een deellichaam is van $GF(p^s)$ als en alleen als r een deler van s is.

Verschillende eigenschappen van de polynoomring $\mathbb{F}[x]$ worden in dit boek vaak gebruikt.

(0.1.9) <u>STELLING</u>. $\mathbb{F}[x]$ *is een hoofdideaalring.*

Dit betekent dat als S een ideaal is in $\mathbb{F}[x]$ er een polynoom g(x) is zo dat S = (g(x)).

(0.1.10) <u>STELLING</u>. *Zij* $q = p^r$ *en* $0 \neq f(x) \in \mathbb{F}_q[x]$. *Dan geldt*

(i) *Het aantal nulpunten van* f(x) *in een lichaam* $\mathbb{F}_{q^k}$ *is ten hoogste gelijk aan de graad van* f(x);

(ii) *Is* α *een meervoudig nulpunt van* f(x) *in* $\mathbb{F}_{q^k}$ *dan is de formele afgeleide van* f(x) *ook* 0 *in* $x = \alpha$;

(iii) *Is* α *een nulpunt van* f(x) *in* $\mathbb{F}_{q^k}$ *dan is* α^q *ook een nulpunt van* f(x)..

(0.1.11) STELLING. *Als de grootste gemene deler* $(a(x),b(x))$ *van* $a(x)$ *en* $b(x)$ *het polynoom* 1 *is dan zijn er polynomen* $p(x)$ *en* $q(x)$ *zo dat*

$$a(x)\ p(x) + b(x)\ q(x) = 1.$$

Is $\alpha \in GF(p^r)$ en $\alpha^n = 1$ terwijl $\alpha^m \neq 1$ voor $0 < m < n$ dan noemen we α een *primitieve* n-*de eenheidswortel*. Zo is bijv. een primitief element van $GF(q)$ een primitieve $(q-1)$-de eenheidswortel.

0.2. GETALTHEORIE

Uit de elementaire getaltheorie hebben we slechts weinig nodig. Bekend is dat in $\mathbb{N}\setminus\{0\}$ ieder getal eenduidig (op volgorde na) is te ontbinden in priemfactoren. Als a een deler is van b geven we dit aan met $a|b$. Is p priem, $p^r|a$ en $p^{r+1}\nmid a$ dan schrijven we $p^r \| a$. Bij een $k \in \mathbb{N}$, $k > 1$, is een k-tallige schrijfwijze van het getal n een representatie

$$n = \sum_{i=0}^{\ell} n_i k^i$$

met $0 \leq n_i < k$ voor $0 \leq i \leq \ell$.

Het eenvoudigste voorbeeld van de in § 0.1 genoemde restklassenringen vinden we binnen $\mathbb{Z}$. De collectie $m\mathbb{Z}$ van veelvouden van m is een ideaal in $\mathbb{Z}$. De restklassenring $\mathbb{Z}/m\mathbb{Z}$ heet de ring van gehele getallen modulo m. Als representanten nemen we meestal $0,1,2,\ldots,m-1$. We schrijven $a \equiv b \pmod m$ als $a - b \in m\mathbb{Z}$.

De grootste gemene deler van a en b geven we aan met g.g.d. (a,b) of alleen (a,b).

(0.2.1) STELLING. *Als*

$$\phi(n) := |\ \{m|\ 1 \leq m \leq n,\ (m,n) = 1\}\ |$$

dan is

$$\phi(n) = n \prod_{p|n} (1-\frac{1}{p}).$$

ϕ heet de *functie van Euler*.

(0.2.2) STELLING. *Als* $(a,m) = 1$ *dan is* $a^{\phi(m)} \equiv 1 \pmod m$.
Dit heet de stelling van EULER-FERMAT.

De elementen van $\mathbb{Z}/p\mathbb{Z}$, p een oneven priemgetal, zijn te verdelen in drie klassen resp. bestaande uit 0, alle kwadraten $\neq 0$ en alle niet-kwadraten. Daar $x^2 = (-x)^2$ en de vergelijking $x^2 = a$ in $\mathbb{F}_p$ niet meer dan 2 oplossingen heeft, zien we dat er precies $\frac{1}{2}(p-1)$ kwadraten zijn. Daar deze modulo p gereduceerd zijn noemt men ze meestal *kwadraatresten* (= *quadratic residues*). Uit (0.1.6), (0.1.7) en (0.2.2) zien we dat x een kwadraatrest is als en alleen als $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$. In het bijzonder is in $\mathbb{F}_p$ het element -1 een kwadraat als en alleen als $p \equiv 1 \pmod 4$. Bovenstaande geldt voor ieder lichaam $\mathbb{F}_q$ met q oneven. In $\mathbb{F}_{2^r}$ is ieder element een kwadraat.

0.3. COMBINATORIEK

In diverse hoofdstukken maken we gebruik van allerlei begrippen uit de combinatoriek. Veel meer dan enkele definities zullen we hier niet noemen. Vrijwel alle theorie die de lezer wellicht nodig heeft is te vinden in het boek *Combinatorial Theory* van M. HALL (1967).

(0.3.1) <u>DEFINITIE</u>. Zij S een verzameling van v elementen en zij $\mathcal{B}$ een collectie deelverzamelingen van S (die we *blokken* noemen) zó dat:

(i) voor iedere $B \in \mathcal{B}$ geldt $|B| = k$,

(ii) voor iedere $T \subset S$ met $|T| = t$ zijn er precies λ blokken B zo dat $T \subset B$.

Dan heet $\mathcal{B}$ een t-*design* (ook wel aangegeven met $t-(v,k,\lambda)$). Is $\lambda = 1$ dan spreken we van een *Steiner system*.

Een design wordt vaak gerepresenteerd door een *incidentiematrix*. Deze matrix heeft $|\mathcal{B}|$ rijen en $|S|$ kolommen. De rijen zijn de karakteristieke functies van de blokken van $\mathcal{B}$.

(0.3.2) <u>DEFINITIE</u>. Een *block design* (= balanced incomplete block design) met parameters $(v,k;b,r,\lambda)$ is een 2-design $2-(v,k,\lambda)$ met $|\mathcal{B}| = b$. Bij elk element van S zijn er r blokken die dat element bevatten. Een *Steiner Triple System* is een block design met $k = 3$ en $\lambda = 1$. Een block design met $v = b$ heet *symmetrisch*.

(0.3.3) <u>DEFINITIE</u>. Een symmetrisch block design met $\lambda = 1$ heet een *projectief vlak*. De punten van S noemen we de *punten* van het vlak.

De blokken van $\mathcal{B}$ heten de *lijnen* van het vlak. Het is eenvoudig in te zien dat $|S| = n^2 + n + 1$. Men noemt n de *orde* van het vlak. Er geldt $k = r = n + 1$. Een projectief vlak van de orde n geven we aan met PG(2,n).

(0.3.4) DEFINITIE. De *affiene meetkunde* van dimensie m over het lichaam $\mathbb{F}_q$ is de vectorruimte $(\mathbb{F}_q)^m$ (Notatie AG(m,q)). Een affiene deelruimte is een nevenklasse van een lineaire deelruimte (opgevat als ondergroep). De groep van transformaties voortgebracht door translaties en lineaire afbeeldingen heet de groep van *affiene transformaties*.

(0.3.5) DEFINITIE. Een vierkante matrix H van de orde n met elementen +1 en −1 waarvoor $HH^T = nI$ heet een *Hadamard matrix*.

Hierin is I de eenheidsmatrix. In het vervolg geven we met I_k de eenheidsmatrix van de orde k aan; met J_k de matrix van de orde k met alle elementen gelijk aan 1; en verder met P_k de matrix van de orde k met $p_{ij} := 1$ als $j-i = 1 \pmod k$ en $p_{ij} := 0$ anders. Als geen verwarring mogelijk is laten we de index k weg.

(0.3.6) DEFINITIE. Een *conferentie-matrix* is een vierkante matrix C (van de orde n) met $c_{ii} = 0$ en $c_{ij} = \pm 1$ als $i \neq j$, zo dat $CC^T = (n-1)\, I$.

Eén van de bekendste methoden om Hadamard matrices en conferentie-matrices te construeren is de zgn. Paley-constructie (cf. HALL (1967) § 14.1). Zij q een macht van een oneven priemgetal. We definieren χ op GF(q) door $\chi(0) := 0$, $\chi(x) := 1$ als x een kwadraat is, $\chi(x) := -1$ anders. We nummeren de elementen van GF(q) als $a_0, a_1, \ldots, a_{q-1}$ met $a_0 = 0$.

(0.3.7) STELLING. *De Paley matrix* S *van de orde* q *gedefinieerd door* $s_{ij} := \chi(a_i - a_j)$ *heeft de eigenschappen*

(i) $SJ = JS = 0$, 7 $q=9$ kwadraten zijn 0,1,4,7

(ii) $SS^T = qI - J$,

(iii) $S^T = (-1)^{\frac{q-1}{2}} S$.

Het is nu eenvoudig om Hadamard matrices en conferentie-matrices te construeren.

(0.3.8) VOORBEELD. Pas (0.3.7) toe voor $q = 11$. Construeer dan H_{12} door

$$H_{12} := I_{12} + \begin{pmatrix} 0 & 1 & 1 & \cdots & \cdots \\ -1 & & & & \\ -1 & & & & \\ \vdots & & & S & \\ -1 & & & & \end{pmatrix}$$

Dan zijn alle elementen van H_n gelijk aan $+1$ of -1 en $HH^T = 12I$.

0.4. WAARSCHIJNLIJKHEIDSREKENING

Voor een stochastische variabele $\underline{x}$ met eindig veld geven we zoals gebruikelijk met p_i de kans aan dat $\underline{x} = x_i$, dat is $p_i = P(\underline{x}=x_i)$. Het *gemiddelde* $\mu = E\underline{x}$ is $\sum p_i x_i$. In het algemeen is voor een functie g het gemiddelde $Eg(x) = \sum p_i\, g(x_i)$. We gebruiken o.a. de eigenschap $E(a\underline{x}+b\underline{y}) = aE\underline{x} + bE\underline{y}$. De *spreiding* σ wordt gedefinieerd door $\sigma \geq 0$ en $\sigma^2 = \sum p_i x_i^2 - \mu^2 = E(\underline{x}-\mu)^2$. De grootheid σ^2 heet de *variantie*.

Ook enkele bekende feiten betreffende tweedimensionale verdelingen worden in hoofdstuk I gebruikt. We noemen de notaties $p_{ij} := P(\underline{x} = x_i \wedge \underline{y} = y_j)$, $p_{i\cdot} = P(\underline{x}=x_i) = \sum_j p_{ij}$, de voorwaardelijke kans $P(\underline{x}=x_i \mid \underline{y}=y_j) = p_{ij}/p_{\cdot j}$. We noemen $\underline{x}$ en $\underline{y}$ *onafhankelijk* als $p_{ij} = p_{i\cdot}\, p_{\cdot j}$ voor alle i en j. Dan is $E(\underline{xy}) = \sum_{i,j} p_{ij}\, x_i y_j = E(\underline{x})\, E(\underline{y})$.

(0.4.1) STELLING. (Bienaymé-Chebyshev). *Voor een stochastische variable met gemiddelde* μ *en spreiding* σ *geldt*

$$P(|\underline{x}-\mu| > k\sigma) < k^{-2}.$$

De kansverdeling die in het vervolg de grootste rol speelt is de *binominale verdeling*. Hierbij neemt $\underline{x}$ de waarden $0,1,\ldots,n$ aan en wel $P(\underline{x}=i) := \binom{n}{i} p^i q^{n-i}$, waarbij $0 \leq p \leq 1$ en $q := 1-p$. Voor deze verdeling geldt $\mu = np$ en $\sigma^2 = npq$.

(0.4.2) STELLING.

$$\log n! = n \log n - n + O(\log n) \quad \textit{voor} \quad n \to \infty.$$

(0.4.3) <u>LEMMA</u>.

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

<u>BEWIJS</u>: $n^n = [m+(n-m)]^n \ge \binom{n}{m} m^m (n-m)^{n-m}$. □

(0.4.4) <u>DEFINITIE</u>. De *binaire entropie* functie H wordt gedefinieerd door

$$H(0) := 0,$$
$$H(x) := -x\ {}^2\log(x) - (1-x)\ {}^2\log(1-x), \quad (0<x\le\tfrac{1}{2}).$$

(0.4.5) <u>LEMMA.</u> *Zij* $0 \le \lambda \le \frac{1}{2}$. *Dan geldt*:

(i) $$\sum_{0\le i\le\lambda n} \binom{n}{i} \le 2^{nH(\lambda)},$$

(ii) $$\lim_{n\to\infty} n^{-1}\ {}^2\log \sum_{i\le\lambda n} \binom{n}{i} = H(\lambda).$$

<u>BEWIJS.</u>

(i) $$1 = \{\lambda+(1-\lambda)\}^n \ge \sum_{0\le i\le\lambda n} \binom{n}{i} \lambda^i (1-\lambda)^{n-i} \ge$$

$$\ge \sum_{0\le i\le\lambda n} \binom{n}{i} (1-\lambda)^n \left(\frac{\lambda}{1-\lambda}\right)^{\lambda n} = 2^{-nH(\lambda)} \sum_{0\le i\le\lambda n} \binom{n}{i}.$$

(ii) Schrijf $m = \lfloor\lambda n\rfloor$. Dan is $m = \lambda n + O(1)$, voor $n \to \infty$. Dus

$$n^{-1}\ {}^2\log \sum_{0\le i\le\lambda n} \binom{n}{i} \ge n^{-1}\ {}^2\log \binom{n}{m} =$$

$$= n^{-1}(n \log n - m \log m - (n-m) \log (n-m) + o(n)) =$$

$$= \log n - \lambda \log (\lambda n) - (1-\lambda) \log ((1-\lambda)n) + o(1) =$$

$$= H(\lambda) + o(1) \quad \text{voor} \quad n \to \infty.$$

Het gestelde volgt nu uit deel (i). □

Hoofdstuk I

DE STELLING VAN SHANNON

1.1. INLEIDING

De theorie van *fouten-verbeterende codes* wordt toegepast in de communicatie theorie in allerlei situaties waar een informatie leverende bron is verbonden met een ontvanger door middel van een zgn. *kanaal* dat deze informatie niet foutloos transporteert. Men denke bijv. aan een gestoorde telefoonlijn of een magneetband waarop door magnetische storingen fouten ontstaan. Het volgende is een typisch recent voorbeeld. De foto's die door de Mariner satellieten van Mars werden gemaakt werden naar de aarde geseind. Dit gebeurde door eerst op de foto een fijn rooster te plaatsen en van ieder hokje de zwartingsgraad te meten, in een schaal van 0 t/m 63. Achtereenvolgens werden deze getallen daarna (als electromagnetisch golven) naar een ontvangstation op aarde gestuurd. Het zeer zwakke signaal moest eerst door de ontvanger versterkt worden. Door thermische ruis in deze ontvanger wordt het signaal verminkt. Om er voor te zorgen dat het signaal desondanks goed wordt geinterpreteerd moest van te voren zgn. *redundantie* worden ingebouwd. Dit betekent dat elk signaal meer bevat dan de nodige informatie alleen. Een voorbeeld dat we allen goed kennen is onze taal. Als in gedrukte tekst fouten voorkomen (dus bijv. drukfouten) dan zien wij dit mits een verminkt woord niet is overgegaan in een ander woord dat wij kennen. Ook het volgende voorbeeld is bekend. Op ponsband voor rekenmachines wordt één redundant bit gebruikt om fouten te detecteren. Om 32 symbolen binair weer te geven zijn 5-tallen nullen en enen nodig. Aan ieder vijftal wordt een zesde bit toegevoegd (dat dus géén informatie meer verschaft) en wel zó dat het aantal enen in een 6-tal even is. Treedt nu door een storing één fout op in zo'n 6-tal dan is het aantal enen oneven geworden en dan wordt het 6-tal door de leesapparatuur niet aanvaard. De fout is ontdekt. We spreken in dit geval van een *single-error-detecting code*. Bij het eerdergenoemde voorbeeld van de Mariners kon men de zwartingsgraden weergeven met behulp van 64 zestallen nullen en enen, nl. de binaire representatie van de getallen 0 t/m 63. In plaats daarvan werden echter 64 verschillende 32-tallen gebruikt. De gebruikte code was zó geconstrueerd dat een ontvangen signaal met 7 fouten erin nog goed geinterpreteerd werd. De tol die men betaalde was het feit dat voor het overseinen van de informatie meer dan 5 keer zo veel tijd

nodig was als zonder de redundante symbolen.

Om een beter idee te krijgen van de oorsprong van de coderingstheorie beschouwen we een experiment. We bevinden ons in een vertrek waar een proefpersoon met vaste snelheid met een munt kruis (K) of munt (M) werpt. We beschikken over een communicatiekanaal met een ander vertrek (bijv. een seinsleutel + electrische verbinding). Over dit kanaal kunnen we twee soorten symbolen, die we 0 en 1 noemen, zenden. Door storing van het kanaal is er iedere keer dat we een 0 of 1 zenden een kans p dat het door de ontvanger juist als het andere symbool wordt geïnterpreteerd. Men noemt dit een *binair symmetrisch kanaal* (B.S.C. = binary symmetric channel).

Als we nu iedere keer dat kruis wordt geworpen een 1 zenden en bij munt een 0 dan zal na voldoende lange tijd een fractie p van de ontvangen informatie, betreffende de werper met de munt fout zijn. Laat nu verder gegeven zijn dat we precies even lang informatie over het kanaal mogen sturen als de duur van het experiment (niet noodzakelijk tegelijkertijd) maar dat we voor iedere worp met de munt *twee* symbolen over het kanaal kunnen sturen.

Als we niet aan de tijdsbepaling gebonden waren zouden we voor een overbrenging met willekeurig grote nauwkeurigheid kunnen zorgen en wel als volgt. Bij de worp kruis zenden we N keer een 1 over het kanaal, bij munt N keer een 0. De ontvanger vertaalt een serie van N signalen in kruis als meer dan de helft van de signalen 1 is. In dit geval gebruiken we de zgn. *repetitiecode* van de lengte N. Deze code bestaat uit twee "woorden", nl. $\underline{0} = (0,0,\ldots,0)$ en $\underline{1} = (1,1,\ldots,1)$. Neem nu als voorbeeld $p = 0.001$. De kans dat de ontvanger verkeerd decodeert is dan

$$(1.1.1) \qquad \sum_{k=0}^{N/2} \binom{N}{k} q^k p^{N-k} < (0.07)^N, \qquad (q=1-p),$$

en deze kans heeft limiet 0 voor $N \to \infty$ (zie (1.4.1)).

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

munt - munt → 0000
kruis - munt → 1001

munt - kruis → 0111
kruis - kruis → 1110.

Als een ander woord ontvangen wordt nemen we aan dat op één van de eerste drie plaatsen een fout is gemaakt. De kans op verkeerd overkomen van het resultaat van twee worpen is nu ongeveer 0.001 terwijl bij gewoon zenden deze kans 0.002 is. Nog groter nauwkeurigheid bereiken we door aan iedere serie van 3 worpen een signaal van 6 symbolen toe te voegen, bijv. als volgt: Als de drie worpen a_1, a_2, a_3 zijn dan zenden we

$$(a_1, a_2, a_3, a_2+a_3, a_1+a_3, a_1+a_2) = (a_1, \ldots, a_6)$$

waarbij optelling modulo 2 is. Dit achttal noemen we de gebruikte *code*. Als het ontvangen signaal $(b_1, \ldots, b_6)$ is, dan is $(b_1, \ldots, b_6) = (a_1, \ldots, a_6) + (e_1, \ldots, e_6)$ waarin $\underline{e}$ het zgn. *foutenpatroon* is; $e_i = 0$ als het symbool goed wordt ontvangen, $e_i = 1$ bij een foute ontvangst. Nu geldt

$$e_2 + e_3 + e_4 = b_2 + b_3 + b_4 = s_1$$

$$e_1 + e_3 + e_5 = b_1 + b_3 + b_5 = s_2$$

$$e_1 + e_2 + e_6 = b_1 + b_2 + b_6 = s_3$$

en hierin zijn de rechterleden aan de ontvanger bekend. Deze neemt aan dat onder alle mogelijke $\underline{e}$ die aan deze vergelijkingen voldoen de werkelijke een minimaal aantal 1'en heeft. Voor 7 van de 8 mogelijke waarden van (s_1, s_2, s_3) leidt dit tot een eenduidig bepaalde $\underline{e}$. Alleen bij (1,1,1) moet de ontvanger kiezen uit (1,0,0,1,0,0), (0,1,0,0,1,0) en (0,0,1,0,0,1). Alle foutenpatronen met 0 of 1 fout worden goed gedecodeerd + nog één met twee fouten. Dit betekent dat na decoderen de kans op alle 3 goed nu

$$q^6 + 6q^5p + q^4p^2$$

is. Het gemiddelde aantal goede symbolen na decoderen kan nog iets groter zijn. In ieder geval hebben we nu al de kans op verkeerd overkomen van één experiment verlaagd tot ongeveer 0.000014; een enorme verbetering!

Door deze inleiding moet de lezer al enigszins een gevoel gekregen hebben voor enkele belangrijke begrippen uit de informatietheorie.

(1.1.2) DEFINITIE. Gebruikt men voor communicatie een collectie C (de code) gekozen uit alle n-tallen nullen en enen dan heet

$$R := n^{-1}\ {}^{2}\log|C|$$

de informatie-inhoud (*information rate* of vaak *rate*) van C.

Het begrip rate heeft te maken met de eerder genoemde snelheid van overbrenging. Voor het ponsband voorbeeld van 32 woorden van 6 letters (0 of 1) is R = 5/6. Voor de code van de Mariner was R = 6/32 in overeenstemming met onze opmerking dat we meer dan 5 keer zo lang nodig hadden als zonder codering. In het net besproken voorbeeld is $|C| = 8$ en $n = 6$, dus $R = \frac{1}{2}$ hetgeen overeenkomt met de eis dat we niet meer dan twee nullen of enen per worp mogen seinen.

De reden waarom de door de Mariner gebruikte code C zelfs bij het optreden van 7 fouten nog tot een goede interpretatie leidde is het feit dat twee verschillende woorden van C steeds op tenminste 16 van de 32 plaatsen van elkaar verschillen. Na het veranderen van ten hoogste 7 symbolen lijkt het gewijzigde woord toch nog meer op het oorspronkelijke dan op één van de andere woorden. Vandaar de volgende definitie (zie 3.1.1).

(1.1.3) DEFINITIE. Zijn $\underline{x}$ en $\underline{y}$ twee n-tallen nullen en enen dan noemen we

$$d_H(\underline{x},\underline{y}) := |\{i \mid 1 \le i \le n,\ x_i \ne y_i\}|$$

de *Hamming-afstand* van $\underline{x}$ en $\underline{y}$.

In het boven gebruikte voorbeeld van een code C met 8 woorden waren de onderlinge afstanden van de woorden tenminste 3. Daardoor konden we ieder foutenpatroon met één fout verbeteren. De code is een *single-error-correcting* code.

Bij het decoderen gaan we er steeds van uit dat een ontvangen signaal zo weinig mogelijk fouten bevat. Dit doen we bij het lezen van gedrukte tekst ook; als een gedrukt woord niet in onze taal voorkomt zoeken we een woord dat er zo veel mogelijk op lijkt. Bij een ontvangen signaal $\underline{y}$ zoekt men dus een $\underline{x}$ uit de code zó dat de Hamming-afstand van $\underline{x}$ en $\underline{y}$ minimaal is. Dit noemt men *maximum-likelihood decoding*.

1.2. DE STELLING VAN SHANNON

We geven nu het bewijs van de stelling van Shannon voor het voorbeeld uit § 1.1. We stellen het probleem opnieuw. Gegeven is een *binair symmetrisch kanaal* met kans p ($0<p<\frac{1}{2}$; $q:=1-p$) op een fout. Stel dat we een code C hebben bestaande uit M vectoren uit $\{0,1\}^n$ met een of andere decodeerregel. Laat P_i de kans zijn dat er na decoderen een fout overblijft aangenomen dat $\underline{x}_i$ het gezonden signaal is. Daar we aannemen dat alle te zenden signalen dezelfde waarschijnlijkheid hebben geldt nu

(1.2.1) $\quad P_C :=$ de kans op een fout $= M^{-1} \sum_{i=1}^{N} P_i$. ?, N

Definieer nu

(1.2.2) $\quad P^*(M,n,p) =$ minimum van P_C over alle codes C met de gegeven parameters.

Dan is:

(1.2.3) <u>STELLING VAN SHANNON</u>. *Als* $0 < R < 1 + p \log p + q \log q$ *en* $M_n := 2^{[Rn]}$ *dan geldt* $P^*(M_n,n,p) \to 0$ *als* $n \to \infty$.

(In de stelling en bewijs hebben alle logarithmen het grondtal 2.)

Merk op dat in ons voorbeeld $1 + p \log p + q \log q$ bijna 1 is, d.w.z. dat met $\varepsilon > 0$ en n voldoende groot een code bestaat waarvoor $P_C < \varepsilon$ terwijl de rate van C meer dan $\frac{1}{2}$ is.

Voor we aan het bewijs beginnen behandelen we enkele technische details die we later gebruiken. Als een codewoord over het kanaal wordt gezonden, dan is de kans op een foutenpatroon met precies w fouten $p^w q^{n-w}$, d.w.z. dat deze kans alleen van het aantal fouten afhangt. We merken op dat de kans dat $\underline{y}$ wordt ontvangen als $\underline{x}$ is gezonden (aangegeven met $P(\underline{y}|\underline{x})$) gelijk is aan de kans op ontvangst van $\underline{x}$ bij signaal $\underline{y}$. Het aantal fouten in een ontvangen woord is een stochastische variabele met verwachtingswaarde np en variantie $np(1-p)$. Als $b := \left(\frac{np(1-p)}{\varepsilon/2}\right)^{\frac{1}{2}}$ dan is volgens Bienaymé-Chebyshev (0.4.1):

(1.2.4) $\quad P(w > np+b) \le \frac{1}{2}\varepsilon$.

Zij $p < \frac{1}{2}$. Zij $\rho := \lfloor np+b \rfloor$ en kies n zo groot dat $\rho < \frac{1}{2}n$. Het aantal woorden met Hamming-afstand $d_H \le \rho$ tot een vast woord $\underline{x}$ is

$$(1.2.5) \qquad |B_\rho(\underline{x})| = \sum_{w \le \rho} \binom{n}{w} < \tfrac{1}{2}n\binom{n}{\rho} \le \tfrac{1}{2}n\frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}},$$

(zie (0.4.3)).

We noemen de collectie $B_\rho(\underline{x})$ de *bol* met middelpunt $\underline{x}$ en straal ρ. Er geldt

$$(1.2.6) \qquad \frac{\rho}{n}\log\frac{\rho}{n} = \frac{1}{n}\lfloor np + b\rfloor \log\frac{\lfloor np+b\rfloor}{n} = p\log p + O(n^{-\frac{1}{2}})$$

en evenzo

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

We introduceren nu twee hulpfuncties. Als $\underline{u} \in \{0,1\}^n$ en $\underline{v} \in \{0,1\}^n$ dan definiëren we:

$$(1.2.7) \qquad f(\underline{u},\underline{v}) := \begin{cases} 0 & \text{als} \quad d_H(\underline{u},\underline{v}) > \rho, \\ 1 & \text{als} \quad d_H(\underline{u},\underline{v}) \le \rho. \end{cases}$$

Is $\underline{x}_i \in C$ en $\underline{y} \in \{0,1\}^n$ dan definiëren we:

$$(1.2.8) \qquad g_i(\underline{y}) := 1 - f(\underline{y},\underline{x}_i) + \sum_{j \ne i} f(\underline{y},\underline{x}_j).$$

Merk op dat $g_i(\underline{y}) = 0$ als $\underline{x}_i$ het enige codewoord is met afstand $\le \rho$ tot $\underline{y}$ en dat anders $g_i(\underline{y}) \ge 1$.

<u>BEWIJS VAN</u> (1.2.3).

De belangrijkste stap in het bewijs is de volgende redenering. Kies woorden $\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_M$ willekeurig uit $\{0,1\}^n$ en gebruik deze M woorden als code C. De ontvanger decodeert volgens de regel: wordt $\underline{y}$ ontvangen en is er één codewoord $\underline{x}_i$ met afstand $\le \rho$ tot $\underline{y}$ dan $\underline{y}$ decoderen als $\underline{x}_i$ en anders $\underline{y}$ decoderen als $\underline{x}_1$ (of $\underline{y}$ "fout" verklaren). Laat P_i weer de kans zijn dat $\underline{x}_i$ is uitgezonden en verkeerd gedecodeerd. Dan is

$$P_i \le \sum_{\underline{y}\in\{0,1\}^n} P(\underline{y}|\underline{x}_i)\ g_i(\underline{y}) =$$

$$= \sum_{\underline{y}} P(\underline{y}|\underline{x}_i)\ \{1 - f(\underline{y},\underline{x}_i)\} + \sum_{\underline{y}} \sum_{j\neq i} f(\underline{y},\underline{x}_j)\ P(\underline{y}|\underline{x}_i).$$

De eerste som rechts is de kans dat $\underline{y} \notin B_\rho(\underline{x}_i)$. Deze kans hangt alleen van ρ en niet van $\underline{x}_i$ af. Noem die kans α_ρ. Volgens (1.2.4) is $\alpha_\rho \le \frac{1}{2}\varepsilon$. Volgens (1.2.1) is

$$P_C \le \tfrac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_{\underline{y}} \sum_{j\neq i} P(\underline{y}|\underline{x}_i)\ f(\underline{y},\underline{x}_j).$$

We berekenen de verwachtingswaarde van het rechterlid over alle grepen $\underline{x}_1,\ldots,\underline{x}_M$ en merken op dat $P^*(M,n,p)$ niet groter kan zijn! Dus is

$$P^*(M,n,p) \le \tfrac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_{\underline{y}} \sum_{j\neq i} E(P(\underline{y}|\underline{x}_i))E(f(\underline{y},\underline{x}_j)) =$$

$$= \tfrac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_{\underline{y}} \sum_{j\neq i} E(P(\underline{y}|\underline{x}_i))\ \frac{|B_\rho|}{2^n} =$$

$$= \tfrac{1}{2}\varepsilon + (M-1)2^{-n}\ |B_\rho|.$$

Door de log te nemen, (1.2.5) en (1.2.6) te gebruiken en door n te delen, vinden we

$$n^{-1} \log(P^*(M,n,p) - \tfrac{\varepsilon}{2}) \le n^{-1} \log M - (1 + p \log p + q \log q) +$$

$$+ O(n^{-\frac{1}{2}}).$$

Uit de definitie van M_n volgt

$$n^{-1} \log M_n - (1 + p \log p + q \log q) + O\ (n^{-\frac{1}{2}}) < -\beta < 0$$

voor $n > n_0$, d.w.z. $P^*(M_n,n,p) < \frac{1}{2}\varepsilon + 2^{-\beta n}$ voor $n > n_0$, d.w.z. $P^*(M_n,n,p) < \varepsilon$ voor n voldoende groot.

Hiermee is de stelling bewezen. □

1.3. COMMENTAAR

De stelling van Shannon (zie C.E. SHANNON (1948)) markeert het begin van onderzoek in de coderingstheorie. Daar het bestaan van goede codes was aangetoond ging men proberen zulke codes te construeren. Daar deze codes gebruikt moesten worden met behulp van electronische apparatuur (vaak zéér klein, bijv. in satellieten) moesten de codes zo veel mogelijk regelmaat vertonen. Daardoor zou zowel codering als decodering en in het bijzonder de foutenverbetering met eenvoudige algoritmen kunnen geschieden. Uit de volgende hoofdstukken zal blijken dat het niet eenvoudig is deze regelmaat in te bouwen zonder datgene wat de stelling van Shannon belooft te verliezen. Men heeft er zelfs aan getwijfeld of dit wel mogelijk is (zie Hoofdstuk IX).

We merken nog op dat één van de belangrijke toepassingsgebieden van de coderingstheorie het telefoonverkeer is. Vele namen die in dit boek genoemd worden zijn namen van (vroegere) medewerkers van Bell Telephone Laboratories. Naast Shannon zelf noemen we Berlekamp, Gilbert, Hamming, Lloyd, MacWilliams, Slepian, Sloane. Het is dan ook niet verwonderlijk dat veel van de literatuur uit de begintijd van dit gebied is te vinden in Bell System Technical Journal.

De lezer die geïnteresseerd is in meer details over de Mariner '69 verwijzen we naar E.C. POSNER (1968).

1.4. OPGAVEN

(1.4.1) Bewijs (1.1.1).

(1.4.2) Om de 8 mogelijke drietallen (a_1,a_2,a_3) uit $\{0,1\}^3$ te zenden gebruiken we de code C gedefinieerd door $(a_1,a_2,a_3) \to (a_1,a_2,a_3,$ $a_1+a_2+a_3,a_1+a_2+a_3,a_1+a_2,a_1+a_2,a_1+a_3,a_1+a_3,a_1)$. Wat is nu de information-rate? Stel dat we een B.S.C. met foutenkans $p = 0.1$ gebruiken (een erg slecht kanaal!). Hoe groot is ongeveer de kans op een fout (per symbool) bij deze code en maximum-likelihood-decoding?

(1.4.3) Construeer 8 woorden uit $\{0,1\}^7$ zó dat de onderlinge afstanden tenminste 4 zijn.

(1.4.4) Een binair kanaal heeft een kans $q = 0.9$ dat een symbool goed aankomt en een kans $p = 0.1$ dat een onherkenbaar symbool (? = erasure) aankomt. We willen een code met rate $\frac{1}{2}$ gebruiken. Wordt de kans

op goede interpretatie groter als we gewoon ieder symbool herhalen? Hoe veel? Kunnen we een nog grotere kans op goede interpretatie maken. Bedenk een bruikbaar systeem met 6 woorden uit $\{0,1\}^5$. Hoe groot is de rate?

Hoofdstuk II

VOORBEELDEN VAN CODES

In dit hoofdstuk noemen we een code C met M woorden van de lengte n en onderlinge afstand $\geq$ d een [n,M,d]-code.

2.1. DE (7,4)-HAMMING CODE

Beschouw de 7 vectoren die ontstaan door cyclische permutatie van (1,1,0,1,0,0,0). Dit zijn de rijen van de incidentiematrix van PG(2,2), het projectieve vlak van de orde 2 (zie (0.3.3)). Hieruit (of door eenvoudige inspectie) volgt dat deze 7 woorden onderling afstand 4 hebben. We voegen nu toe $\underline{0}$ = (0,0,...,0) en de 8 woorden die ontstaan door in alle woorden overal 0 door 1 en 1 door 0 te vervangen. Zo hebben we 16 woorden uit $\{0,1\}^7$. Het is eenvoudig in te zien dat deze code H *minimum afstand* 3 heeft. H is dus een [7,16,3]-code. Als we H *verlengen* tot de code $\overline{H}$ door ieder woord een achtste letter te geven en wel zó dat ieder woord van $\overline{H}$ een even aantal enen heeft, dan vinden we een code met minimumafstand 4, een [8,16,4]-code. $\overline{H}$ heeft de eigenschap dat als $\underline{a} \in \overline{H}$ en $\underline{b} \in \overline{H}$ dan ook $\underline{a} + \underline{b} \in \overline{H}$ (optelling modulo 2). (Zie Hoofdstuk III).

2.2. HADAMARD CODES EN GENERALISATIES

Zij H_n een Hadamard matrix van de orde n (zie (0.3.5)). Vervang in H_n en $-H_n$ overal -1 door 0. Dan ontstaan 2n rijen van n symbolen met onderlinge afstand $\geq \frac{1}{2}n$. Een Hadamard code is een $[n,2n,\frac{1}{2}n]$-code. Voor n = 8 vinden we de code $\overline{H}$ uit § 2.1. Voor n = 32 vinden we de code gebruikt door de Mariner '69 die in § 1.1 is genoemd.

Zij S een Paley matrix van de orde n. Beschouw de rijen van de matrices $\frac{1}{2}(S+I+J)$ en $\frac{1}{2}(-S+I+J)$ en voeg ook nog $\underline{0}$ en $\underline{1}$ toe. Uit stelling (0.3.7) volgt dat we nu een $[n,2(n+1),\frac{1}{2}(n-1)]$-code geconstrueerd hebben. Voor n = 9 vinden we de code bestaande uit de rijen van de matrix

$$\begin{pmatrix} 0\,0\,0 & 0\,0\,0 & 0\,0\,0 \\ J & P^2 & P \\ P & J & P^2 \\ P^2 & P & J \\ I & J-P^2 & J-P \\ J-P & I & J-P^2 \\ J-P^2 & J-P & I \\ 1\,1\,1 & 1\,1\,1 & 1\,1\,1 \end{pmatrix}$$

waarin I, J, en **P** orde 3 hebben.

De methode van § 2.1 wil ook wel eens lukken in meer ingewikkelde situaties. Beschouw de code C van lengte 8 die bestaat uit $\underline{0}$, $\underline{1}$, en alle cyclische permutaties van (1,1,0,1,0,0,0,0), (1,1,1,0,0,1,0,0), (1,0,1,0,1,0,1,0). Men ga zelf na dat dit een [8,20,3]-code is. Zo'n code krijgen we ook als we in de [9,20,4]-code in elk woord de laatste letter weglaten.

2.3. DE BINAIRE GOLAY CODE EN AFGELEIDEN

Beschouw de (7,4)-Hamming code H uit § 2.1. We vormen H^* door de woorden van H achterstevoren te schrijven. Daarna vormen we weer $\overline{H}^*$. Dit is een [8,16,4]-code met $\overline{H} \cap \overline{H}^* = \{\underline{0},\underline{1}\}$. We vormen nu een code $\overline{C}$ met woordlengte 24 door te definieren:

$$\overline{C} := \{(\underline{a}+\underline{x},\underline{b}+\underline{x},\underline{a}+\underline{b}+\underline{x}) \mid \underline{a} \in \overline{H},\ \underline{b} \in \overline{H},\ \underline{x} \in \overline{H}^*\}$$

Hierbij zijn de optellingen modulo 2. De code $\overline{C}$ bestaat uit 2^{12} woorden. Voor $\overline{C}$ geldt, evenals voor $\overline{H}$ en $\overline{H}^*$, dat de som van twee code woorden weer een codewoord is. Om de minimum afstand van $\overline{C}$ te bepalen moeten we dus de woorden van $\overline{C}\backslash\{\underline{0}\}$ zoeken met zo weinig mogelijk enen. Voor $\underline{x} \in \overline{C}$ noemt men $d_H(\underline{x},\underline{0}) =: w(\underline{x})$ het *gewicht* van $\underline{x}$, (zie (3.1.1),(3.3.1)). Is $\underline{c} = (\underline{a}+\underline{x},\underline{b}+\underline{x},\underline{a}+\underline{b}+\underline{x})$ en is tenminste één van de vectoren $\underline{a}$, $\underline{b}$, $\underline{a}+\underline{b}$, en $\underline{x}$ gelijk aan $\underline{0}$ of $\underline{1}$ dan zien we dat $\underline{c} = \underline{0}$ of $w(\underline{c}) \geq 8$. Uit de eigenschappen van $\overline{H}$ en uit $\overline{H} \cap \overline{H}^* = \{\underline{0},\underline{1}\}$ volgt dat als $\underline{a}$, $\underline{b}$, $\underline{a}+\underline{b}$ en $\underline{x}$ niet $\underline{0}$ of $\underline{1}$ zijn elk van de woorden $\underline{a}+\underline{x}$, $\underline{b}+\underline{x}$ en $\underline{a}+\underline{b}+\underline{x}$ een positief en even gewicht heeft. Was nu $w(\underline{c}) = 6$ dan zou moeten gelden $w(\underline{a}+\underline{x}+\underline{b}+\underline{x}+\underline{a}+\underline{b}+\underline{x}) =$

$= w(\underline{x}) = 6$ (ga na!). Daar $w(\underline{x}) = 4$ hebben we nu bewezen dat $w(\underline{c}) = 6$ niet kan. Dus heeft $\overline{C}$ minimum afstand 8. Dus $\overline{C}$ is een $[24,2^{12},8]$-code.

Laat nu uit alle woorden van $\overline{C}$ de laatste letter weg. We vinden een $[23,2^{12},7]$-code C, genaamde de *binaire Golay code*.

(2.3.1) DEFINITIE. Een code C met woordlengte n en minimum afstand 2e+1 heet *perfect* (en wel e-perfect) als ieder woord (van n letters) afstand $\leq$ e heeft tot een codewoord. Uit deze definitie en uit $|B_e(\underline{c})| = \sum_{i=0}^{e} \binom{n}{i}$ volgt dat een $(n,|C|,2e+1)$-code C e-perfect is als en alleen als

(2.3.2) $$|C| \sum_{i=0}^{e} \binom{n}{i} = 2^n.$$

Hieruit zien we dat de code H uit § 2.1 perfect is (daar $16(1+7) = 2^7$). De binaire Golay code C is ook perfect: C is een 3-error-correcting code en

$$|C| \sum_{i=0}^{3} \binom{23}{i} = 2^{12}(1+23+253+1771) = 2^{23}.$$

Uit onze constructie van de Golay code kan men vrij eenvoudig inzien dat er 32 codewoorden $\underline{c} = (c_1,c_2,\ldots,c_{24})$ in $\overline{C}$ zijn die met 8 nullen beginnen. Kiezen we $c_8 = 1$ en precies één van de letters c_1 t/m c_7 ook 1 dan vinden we weer 32 woorden van $\overline{C}$. We hebben zo een collectie van 32(1+7) = 256 woorden uit $\overline{C}$ waarvan we nu de eerste 8 letters weglaten. De code N die op deze manier onstaat heet de *Nordstrom-Robinson code*. Het is een $[16,2^8,6]$-code.
Uit N construeren we door verder af te breken nog enkele interessante codes. Eerst merken we op dat in N precies 64 woorden op (0,0) eindigen. We nemen deze woorden en laten daarvan de laatste drie letters weg. Zo ontstaat een [13,64,5]-code Y. Als we uit alle woorden van Y die op een 0 eindigen deze 0 weglaten vinden we een [12,32,5]-code die de *Nadler code* wordt genoemd (zie (2.7.4)).

2.4. DE TERNAIRE GOLAY CODE

Zij S_5 de Paley matrix

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

Laat C bestaan uit alle lineaire combinaties, met coefficienten in $\mathbb{F}_3$, van de rijen van

$$G := \begin{pmatrix} I_6 & \begin{array}{c} 1\ 1\ 1\ 1\ 1 \\ \boxed{S_5} \end{array} \end{pmatrix}$$

Het is natuurlijk niet handig om alle 3^6 woorden (met letters 0,+1 of -1) die zo ontstaan op te schrijven en te vergelijken. In het volgende hoofdstuk leren we technieken die ons snel in staat stellen in te zien dat deze code minimum-afstand 5 heeft en dus perfect is (zie (3.8.14)). [Merk op dat vgl. (2.3.2) welke gold voor een alfabet van twee symbolen hier

$$|C| \sum_{i=0}^{2} \binom{11}{i} 2^i = 3^{11}$$

luidt.]

Het is wellicht nuttig voor de lezer om te proberen de eigenschappen van deze code nu af te leiden zonder te beschikken over de middelen van hoofdstuk III.

2.5. COMBINATIE VAN CODES

Een bekende manier om codes te construeren is het aan elkaar plakken van woorden uit verschillende codes zoals we ook in § 2.3 gedaan hebben. Beschouw bijv. de [12,24,6]-Hadamard code uit § 2.2. Hieruit nemen we 6 woorden die met (0,0) beginnen en vormen zo een [10,6,6]-code. We plakken nu twee zulke codes aan elkaar, d.w.z. achter ieder woord schrijven we hetzelfde woord nog een keer. Hierachter zetten we 6 woorden van de [7,8,4]-code die we krijgen door de woorden van even gewicht van de (7,4)-Hamming code code te beschouwen. Zo ontstaat een [27,6,16]-code. In hoofdstuk IV zullen we zien dat een [27,M,16]-code moet voldoen aan $M \leq 6$. Onze plak-techniek levert dus een optimaal resultaat!

We geven nog een voorbeeld. Laat C_1 een $[n,M_1,d_1]$-code zijn en C_2 een $[n,M_2,d_2]$-code. Definieer

$$C := \{(\underline{x}+\underline{y},\underline{y}) \mid \underline{x} \in C_1,\ \underline{y} \in C_2\}.$$

Dan is C een $[2n,M_1M_2,d]$-code met $d := \min\{d_1,2d_2\}$. Om dit in te zien beschouwen we $d((\underline{x}_1+\underline{y}_1,\underline{y}_1),(\underline{x}_2+\underline{y}_2,\underline{y}_2))$. Als $\underline{x}_1 = \underline{x}_2$ dan is deze afstand $2d(\underline{y}_1,\underline{y}_2)$. Is echter $x_{1i} \neq \underline{x}_{2i}$ dan kan de i-de letter van $\underline{x}_1 + \underline{y}_1$ alleen gelijk zijn aan de i-de letter van $\underline{x}_2 + \underline{y}_2$ als $\underline{y}_1$ en $\underline{y}_2$ ook verschillende i-de coordinaten hebben. Dan is dus $d((\underline{x}_1+\underline{y}_1,\underline{y}_1),(\underline{x}_2+\underline{y}_2,\underline{y}_2)) \geq d_1$. Nemen we bijvoorbeeld voor C_1 de $[8,20,3]$-code uit § 2.2 en voor C_2 de $[8,2^7,2]$-code bestaande uit alle woorden van even gewicht dan vinden we een $[16,5.2^9,3]$-code. Op het ogenblik is geen $[16,M,3]$-code bekend met $M > 5.2^9$.

2.6. COMMENTAAR

Om didactische redenen hebben we dit hoofdstuk vóór het volgende geplaatst. Het is aan te nemen dat vele van bovenstaande voorbeelden duidelijker worden na lezing van Hoofdstuk III. We raden de lezer aan Hoofdstuk II na Hoofdstuk III te herlezen.

De Hamming code uit § 2.1 is een speciaal geval van de serie uit § 3.5. Hadamard codes komen terug in hoofdstuk VI als 1^e orde RM-codes. De beide Golay codes komen terug in de hoofdstukken V en VII. Deze codes zijn in 1949 geconstrueerd door M.J.E. Golay (zie GOLAY (1949)).

Perfecte codes behandelen we in hoofdstuk VII. De Nordstrom-Robinson code is een speciaal geval van de Preparata codes uit hoofdstuk VII. Veel meer over de Golay codes vindt men in CAMERON & VAN LINT (1975), GOETHALS (1971) en VAN LINT (1971). Over het onderwerp van § 2.5 raadplege men vooral SLOANE, REDDY & CHEN (1972) en SLOANE & WHITEHEAD (1970).

2.7. OPGAVEN

(2.7.1) Zij A_i het aantal woorden van gewicht i uit de binaire Golay code. Bewijs dat uit het feit dat deze code perfect is (met e = 3) volgt dat: $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$, en alle andere $A_i = 0$. De woorden van gewicht 7 vormen een Steiner systeem met $\nu = 23$, $k = 7$, $t = 4$, $\lambda = 1$. Bewijs dit.

(2.7.2) Zij S een Paley matrix van de orde 11. Beschouw de matrix A = $= \frac{1}{2}(S+I+J)$. De 11 rijen van A en alle sommen (mod 2) van twee verschillende rijen van A vormen een verzameling van 66 woorden van de lengte 11. Hieraan voegen we toe alle woorden die we krijgen door alle nullen in enen te veranderen en omgekeerd. Bewijs dat dit een [11,132,3]-code C is. Nu voegen we aan ieder woord C een letter toe zó dat de nieuwe code $\overline{C}$ alleen even gewichten heeft. Permuteer de letters zo dat (111 111 000 000) een codewoord is. Voeg nu toe (1,1,0,0,...,0), (0,0,1,1,0,0,...,0), ...,(0,0,...,0,1,1), en de zes woorden die hieruit ontstaan door weer 0 en 1 te verwisselen. Bewijs dat de nieuwe code een [12,144,4]-code is. Deze code bevat 38 woorden $\underline{c}$ met $c_{10} = 0$, $c_{12} = 1$. Deze 38 woorden vormen (na weglating van de genoemde coordinaten) een [10,38,4]-code. Bewijs dit. De beste code met n = 10 en d = 4 heeft 40 woorden.

(2.7.3) Bewijs dat met een Paley matrix een [17,36,8]-code is te construeren.

(2.7.4) Beschouw I, J en P van de orde 3. Definieer

$$A = \begin{pmatrix} J-I & I & I & I \\ I & J-I & I & I \\ I & I & J-I & I \\ I & I & I & J-I \end{pmatrix}, \quad B = \begin{pmatrix} J & P & I & P^2 \\ P & J & P^2 & I \\ I & P^2 & J & P \\ P^2 & I & P & J \end{pmatrix},$$

$$C = (J-I \quad J-I \quad J-I \quad J-I), \qquad D = \begin{pmatrix} 000 & 111 & 111 & 111 \\ 111 & 000 & 111 & 111 \\ 111 & 111 & 000 & 111 \\ 111 & 111 & 111 & 000 \end{pmatrix}$$

Bewijs dat $\underline{0}$ en de rijen van A, B, C en D een [12,32,5]-code vormen.

Hoofdstuk III

LINEAIRE CODES

3.1. BLOK CODES

We nemen nu aan dat informatie wordt gecodeerd met behulp van een *alfabet* Q van q verschillende symbolen. Een code heet een *blok code* als de gecodeerde informatie verdeeld kan worden in rijtjes symbolen van vaste lengte die onafhankelijk van elkaar gedecodeerd kunnen worden. Deze blokken noemen we *codewoorden*; de lengte heet *blok lengte* of *woord lengte*. Alle voorbeelden in hoofdstuk II zijn blok codes. De symbolen van een woord noemen we weer de *letters* of ook wel coordinaten (zie § 3.2). Merk op dat de woorden in de nederlandse taal ook blokken zijn maar niet met vaste lengte. Een voor de practijk zeer belangrijke manier van coderen die we in dit boek helemaal niet beschouwen is een zgn. *convolutiecode*. Daarbij wordt een (evtl. oneindige) informatierij $i_0, i_1, i_2, \ldots$ gecodeerd (bij rate $\frac{1}{2}$) als $i_0, i_0', i_1, i_1', i_2, i_2', \ldots$ waarbij i_n' berekend wordt (m.b.v. een vooraf gegeven voorschrift) uit $i_0, i_1, \ldots, i_n$. Bij deze code is van blokken geen sprake.

Als generalisatie van (1.1.3) definieren we voor woorden $\underline{x}$ en $\underline{y}$ van n letters uit een alfabet Q met q letters:

(3.1.1) <u>DEFINITIE</u>. De *Hamming-afstand* $d_H(\underline{x},\underline{y})$ van $\underline{x}$ en $\underline{y}$ is

$$d_H(\underline{x},\underline{y}) := |\{i \mid 1 \le i \le n,\ x_i \ne y_i\}|.$$

Het *gewicht* $w(\underline{x})$ van $\underline{x}$ is $d_H(\underline{x},\underline{0})$, waarbij $\underline{0} = (0,0,\ldots,0)$, (= de *oorsprong*).

Hamming-afstand is een geschikt afstandsbegrip indien bij een fout in het i-de symbool alle mogelijke fouten op die positie even waarschijnlijk zijn en de fout in de i-de positie geen gevolgen heeft voor de andere posities. In hoofdstuk X leren we een ander afstandsbegrip kennen.

Een (blok-)code C met woordlengte n is een niet-lege deelverzameling van Q^n. We noemen C *triviaal* als $|C| = 1$. De code heet *binair* (zie hoofdstuk II) als $q = 2$, *ternair* als $q = 3$, etc. De volgende begrippen spelen

een centrale rol zoals uit de voorbeelden van hoofdstuk II duidelijk moet zijn:

(3.1.2) DEFINITIE. De *minimale afstand* van een niet-triviale code C is $\min\{d_H(\underline{x},\underline{y}) \mid \underline{x} \in C, \underline{y} \in C, \underline{x} \neq \underline{y}\}$. Het *minimale gewicht* van C is $\min\{w(\underline{x}) \mid \underline{x} \in C, \underline{x} \neq \underline{0}\}$.

We generaliseren (1.1.2) nu ook.

(3.1.3) DEFINITIE. Is $|Q| = q$ en $C \subset Q^n$ dan heet

$$R := n^{-1}\, {}^q\log|C|$$

de (*information-*) *rate* van C.

3.2. LINEAIRE CODES

We willen nu codes construeren met een algebraïsche structuur. Als het alfabet Q een groep is en de code C is een ondergroep van Q^n dan heet C een *groepcode*. In deze paragraaf eisen we nog iets meer. Laat Q het lichaam GF(q) zijn waarbij $q = p^f$ (p priem). De collectie Q^n is een n-dimensionale vectorruimte die we ook met $R^{(n)}$ aangeven.

(3.2.1) DEFINITIE. Een *lineaire code* V is een lineaire deelruimte van $R^{(n)}$. Als V dimensie k heeft wordt V een (n,k)-code over GF(q) genoemd. (N.B. niet verwarren met de notatie uit hoofdstuk II).

(3.2.2) DEFINITIE. Een *generator matrix* G (kort: generator) voor een lineaire code V is een matrix G waarvan de rijen een stelsel basisvectoren van V vormen.

Voor een (n,k)-code over GF(q) is een generator G een matrix met afmetingen $k \times n$. De code bestaat uit alle vectoren $\underline{a}G$ met $\underline{a} \in R^{(k)}$. We zullen zeggen dat G de *standaardvorm* heeft als $G = (I_k, P)$, waarbij P een $k \times (n-k)$ matrix is. De in § 1.1 behandelde (6,3)-code over GF(2) had generator $G = (I, J-I)$, dus in standaardvorm. Merk op dat als G de standaardvorm heeft elk codewoord begint met k symbolen die willekeurig gekozen mogen worden (*informatiesymbolen*) gevolgd door n-k redundante symbolen die *parity-check symbolen* worden genoemd. Deze naam is afkomstig van het in hoofdstuk I genoemde voorbeeld van ponsband waar $G = (I_5 \underline{j}^T)$. Het zesde symbool van ieder woord controleert de pariteit.

(3.2.3) DEFINITIE. Twee codes C_1 en C_2 heten *equivalent* als er een permutatie π van $\{1,2,\ldots,n\}$ is zo dat

$$C_2 = \{c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)}) \mid \underline{c} \in C_1\}.$$

Vaak wordt het equivalentie-begrip nog uitgebreid door ook nog toe te staan dat op elke plaats een permutatie van Q optreedt.

(3.2.4) STELLING. Bij iedere lineaire code is er een equivalente code die een generator in standaardvorm heeft.

BEWIJS. Dit is een bekende stelling uit de lineaire algebra. □

I.h.a. wordt een code *systematisch* genoemd als een aantal symbolen van elk woord vrij gekozen mag worden (weer: informatiesymbolen) en de andere symbolen dan bepaald zijn. In (3.2.4) staat dus dat iedere lineaire code (equivalent met) een systematische code is. Zoals we mochten verwachten is volgens (3.1.2) de rate van een (n,k)-code $\frac{k}{n}$ omdat de code q^k woorden bevat.

3.3. FOUTENVERBETERING

Bij het interpreteren van ontvangen signalen (bij gebruik van lineaire codes) passen we weer maximum-likelihood decoding toe. Als voor de code V de minimum afstand 2e + 1 is dan kunnen we foutenpatronen met $\leq$ e fouten corrigeren. Is de minimum afstand 2e dan wordt een foutenpatroon met e fouten wel ontdekt maar het is soms niet te verbeteren (e-*error-detecting code*).

(3.3.1) STELLING. *Voor een lineaire code* V *is de minimum-afstand gelijk aan het minimum gewicht.*

BEWIJS. $d_H(\underline{x},\underline{y}) = w(\underline{x}-\underline{y})$ en als $\underline{x} \in V$ en $\underline{y} \in V$ is ook $\underline{x}-\underline{y} \in V$. □

Uit deze stelling zien we dat de controle van de kwaliteit van een lineaire code aanzienlijk minder werk vergt dan voor een niet lineaire code waar men $d_H(\underline{x},\underline{y})$ voor alle paren $(\underline{x},\underline{y})$ moet uitrekenen.

(3.2.2) DEFINITIE. Is V een (n,k)-code over GF(q) dan is de *duale code* $V^{\perp}$ een (n,n-k)-code gedefinieerd door

$$V^{\perp} := \{\underline{y} \in R^{(n)} \mid \forall_{x \in V}[<\underline{x},\underline{y}>=0]\}.$$

Hierin is $< \underline{x},\underline{y} >$ het inwendig product over GF(q), d.i. $x_1y_1 + \ldots + x_ny_n$. Merk op dat het feit dat $V^{\perp}$ een (n-k)-dimensionale lineaire deelruimte van $R^{(n)}$ is weer een bekende stelling uit de lineaire algebra is. We moeten wel bedenken dat over GF(q) i.h.a. niet geldt dat iedere $\underline{z}$ is te schrijven als $\underline{x} + \underline{y}$ met $\underline{x} \in V^{\perp}$ zoals we uit de lineaire algebra in Euclidische ruimten gewend zijn.

Is $G = (I_k, P)$ een generator van V in standaardvorm dan is $H = (-P^T, I_{n-k})$ een generator van $V^{\perp}$. Immers: H heeft de juiste afmetingen, de rang van H is n-k en $GH^T = 0$. Daar ieder codewoord $\underline{x} \in V$ de vorm $\underline{x} = \underline{a}\, G$ heeft kunnen we V ook beschrijven door

(3.3.3) $\quad \underline{x} \in V \Longleftrightarrow \underline{x}\, H^T = \underline{0}.$

Dit is een stelsel van n-k lineaire vergelijkingen die V bepalen. Deze vergelijkingen heten *parity-check* vergelijkingen en H heet een *parity-check matrix* voor V. I.h.a. is voor iedere $\underline{y} \in V^{\perp}$ de vergelijking $< \underline{x},\underline{y} > = 0$ een parity-check vergelijking voor V. Voor de code uit § 1.1 zijn de vergelijkingen $a_4 = a_2 + a_3$, etc. waarmee de code werd gedefinieerd drie parity-check vergelijkingen, overeenkomend met H = (J-I, I).

(3.3.4) <u>DEFINITIE</u>. Is V een lineaire code met parity-check matrix H, dan noemen we voor iedere $\underline{x} \in R^{(n)}$ de vector $\underline{x}H^T$ het *syndroom* van $\underline{x}$.

De code V bestaat uit alle vectoren met syndroom $\underline{0}$. Daar V een ondergroep is van $R^{(n)}$ kunnen we $R^{(n)}$ splitsen in nevenklassen van V. Het is duidelijk dat twee vectoren $\underline{x}$ en $\underline{y}$ in dezelfde nevenklasse zitten als en alleen als ze hetzelfde syndroom hebben (immers $\underline{x}H^T = \underline{y}H^T \Longleftrightarrow \underline{x}-\underline{y} \in V$). Hieruit zien we dat een ontvangen signaal $\underline{x}$ een foutenpatroon $\underline{e}$ uit dezelfde nevenklasse moet hebben (want $\underline{x}-\underline{e} \in V$). Om te decoderen moeten we dus een keuze doen uit de elementen van de nevenklasse van $\underline{x}$ die minimaal gewicht hebben. In de practijk gaat dit als volgt. We maken een lijstje van alle syndroomwaarden. Bij ieder daarvan behoort een nevenklasse. Uit deze nevenklasse kiezen we een representant (*coset-leader*) met minimaal gewicht. Wordt nu $\underline{x}$ ontvangen dan zoeken we bij $\underline{x}H^T$ de representant op en trekken deze van $\underline{x}$ af. De lezer kan nu zelf nagaan dat dit precies is wat we in § 1.1 hebben

gedaan met de binaire (6,3)-code. Voor 7 nevenklassen was de representant eenduidig bepaald; voor de laatste moesten we er één kiezen uit drie met hetzelfde gewicht. Het is duidelijk dat als V minimum afstand $d = 2e+1$ heeft twee vectoren met gewicht $\leq e$ niet in dezelfde nevenklasse kunnen zitten. In dat geval zijn deze vectoren dus allemaal representanten van verschillende nevenklassen.

Ook over een alfabet van q symbolen geldt (2.3.1). Bij een perfecte code zijn er geen andere representanten van nevenklassen dan de vectoren met gewicht $\leq e$. (Dit zijn er $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$). Een code (zoals ons voorbeeld uit § 1.1) waarvan de minimum afstand $d = 2e+1$ is en alle representanten van nevenklassen een gewicht $\leq e+1$ hebben heet *quasiperfect*.

3.4. HAMMING CODES

(3.4.1) STELLING. *Een lineaire code* V *over* GF(q) *heeft minimum afstand* ≥ 3 *als en alleen als de kolommen van de parity-check matrix* H *niet* $\underline{0}$ *zijn en paarsgewijs lineair onafhankelijk.*

BEWIJS. (i) Stel dat H de genoemde eigenschap heeft. De vergelijking $\underline{x}H^T = \underline{0}$ betekent dat de kolommen behorende bij coordinaten $x_i \neq 0$ lineair afhankelijk zijn. Is dus $\underline{x} \neq \underline{0}$ en $\underline{x}H^T = \underline{0}$ dan is $w(\underline{x}) \geq 3$.

(ii) Heeft H de genoemde eigenschap niet dan zien we op precies dezelfde manier dat er een $\underline{x}$ is met $1 \leq w(\underline{x}) \leq 2$ zó dat $\underline{x}H^T = \underline{0}$. □

Beschouw nu de r-dimensionale ruimte over GF(q). Bij iedere $\underline{x} \neq \underline{0}$ zijn er q-1 vectoren die veelvouden van $\underline{x}$ zijn. Er zijn dus $(q^r-1)/(q-1)$ paarsgewijs lineair onafhankelijke vectoren $\neq \underline{0}$. Noem dit aantal n. Kiezen we zo'n stelsel van n vectoren als kolommen van een r bij n matrix H dan heet de code met deze parity-check matrix een *Hamming code* en wel een (n,n-r)-*Hamming code* over GF(q). Is q = 2 dan **bestaat** H uit alle mogelijke kolommen $\neq \underline{0}$. Decoderen is dan heel eenvoudig. Orden de kolommen van H zo dat de i-de kolom de binaire schrijfwijze van het getal i is. Wordt $\underline{x}$ ontvangen en is het syndroom niet $\underline{0}$ dan is het syndroom de binaire schrijfwijze van een getal i. Vervang dan x_i door $x_i + 1$. Er ontstaat een codewoord. Hieruit zien we dat een binaire Hamming code perfect is. Dit geldt voor alle Hamming codes.

(3.4.2) STELLING. *De Hamming codes over* GF(q) *zijn perfect.*

BEWIJS. Zij $n := (q^r-1)/(q-1)$ en V een (n,n-r)-Hamming code. Is $\underline{v} \in V$ dan is $|B_1(\underline{v})| = 1 + n(q-1) = q^r$. De q^{n-r} disjuncte bollen $B_1(\underline{v})$ met $\underline{v} \in V$ bevatten dus q^n punten, d.w.z. dat ze $R^{(n)}$ overdekken. □

In § 2.1 hebben we gezien hoe uit de (7,4)-Hamming code door verlenging een code met woordlengte 8 en minimum afstand 4 kon worden gemaakt. Dit is een voorbeeld van een algemeen principe.

(3.4.3) DEFINITIE. Is C een code in $R^{(n)}$ dan wordt de *verlengde code* $\overline{C}$ (= *extended code*) in $R^{(n+1)}$ gedefinieerd door

$$(c_1,c_2,\ldots,c_{n+1}) \in \overline{C} \Longleftrightarrow ((c_1,c_2,\ldots,c_n) \in C \wedge \sum_{i=1}^{n+1} c_i = 0).$$

Voor het geval dat C een lineaire code in $R^{(n)}$ is met generator G en parity-check matrix H vinden we voor $\overline{C}$ de matrices G^* en H^* door aan G een kolom toe te voegen zó dat de kolommen samen $\underline{0}$ zijn en dan

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

(Vaak wordt de nieuwe letter van de verlengde code voorop geschreven).
Voor het binaire geval zien we dat in $\overline{C}$ alle woorden even gewicht hebben en dat $\overline{C}$ dus even minimum afstand heeft. Als dus C een oneven minimum afstand d heeft dan heeft $\overline{C}$ minimum afstand d + 1.

3.5. DREMPEL DECODERING

We geven nu een korte schets van een decodeermethode die voor vele lineaire codes wordt gebruikt. De methode heeft als voordeel de eenvoud en het feit dat vaak meer fouten worden verbeterd dan men verwacht op grond van de minimum afstand.

(3.5.1) <u>DEFINITIE</u>. Een stelsel parity-check vergelijkingen $< \underline{x}, \underline{y}^{(\nu)} > = 0$, $(1 \le \nu \le r)$ heet *orthogonaal* op positie i voor de code V als

(i) $y_i^{(\nu)} = 1 \quad (1 \le \nu \le r)$,

(ii) als $j \ne i$ dan is $y_j^{\nu} \ne 0$ voor ten hoogste één waarde van ν.

Laat $\underline{x}$ een woord zijn dat t fouten bevat waarbij $t \le \frac{1}{2} r$. Dan is

$$< \underline{x}, \underline{y}^{(\nu)} > \ne 0 \text{ voor } \begin{cases} \le t \text{ waarden van } \nu \text{ als } x_i \text{ goed is,} \\ \ge r-(t-1) \text{ waarden van } \nu \text{ als } x_i \text{ fout is.} \end{cases}$$

Daar $r-(t-1) > t$ beslist de meerderheid van de waarden van $< \underline{x}, \underline{y}^{(\nu)} >$ (nl. 0 of niet 0) of x_i goed is of fout. Bij een binaire code kan direct daarop x_i verbeterd worden. In de practijk gebruikt men een teller die zodra een bepaalde drempelwaarde wordt overschreden x_i verandert. Daarom noemt men dit procédé *"threshold decoding"*. Men moet wel voor iedere i over zo'n orthogonaal stelsel parity-checks beschikken.

We geven een voorbeeld. Zij V de duale code van de (7,4)-Hamming code. Deze code heeft generator

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

De parity-check vergelijkingen

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 + x_4 + x_5 &= 0 \\ x_1 + x_6 + x_7 &= 0 \end{aligned}$$

zijn orthogonaal op de 1ste positie. Als het woord $\underline{x}$ precies één fout bevat dan geven de drie vergelijkingen als uitkomst of drie keer 1 (als x_1 fout is) of één keer 1 (als x_1 goed is). Er zijn 6 even waarschijnlijke foutenpatronen van gewicht 2 die bij de drie vergelijkingen het resultaat 0,1,1 leveren. Slechts twee daarvan hebben een fout op de 1ste plaats. Hier blijkt dus dat we als drempel $2\frac{1}{2}$ moeten kiezen omdat alleen de uitkomst 1,1,1 verandering van x_1 rechtvaardigt. We kunnen de zaak ook enigszins anders bekijken. Stel dat we het woord $\underline{y} = \underline{x} + \underline{e}$ ontvangen. Dan is blijkbaar

$$y_1 = x_1 + e_1$$
$$y_2 + y_3 = x_1 + e_2 + e_3$$
$$y_4 + y_5 = x_1 + e_4 + e_5$$
$$y_6 + y_7 = x_1 + e_6 + e_7.$$

De ontvanger kent de linkerleden. De meerderheid van de waarden is de waarde die we aan x_1 moeten toekennen. Bij staken van de stemmen nemen we $x_1 = y_1$ zoals boven is uitgelegd. Deze zienswijse verklaart de naam *majority-decoding* die ook wel voor dit procédé wordt gebruikt. In ons voorbeeld heeft V minimum afstand 4. We verwachten 1 fout te kunnen verbeteren.

3.6. DE WEIGHT ENUMERATOR EN DE MACWILLIAMS IDENTITEIT

Hoewel het minimum gewicht d van een lineaire code iets zegt over het aantal fouten dat we kunnen verbeteren is het mogelijk dat deze minimum afstand zelden optreedt. Dan zullen vele fouten patronen van gewicht $> \frac{1}{2}$ d ook nog goed gedecodeerd worden. Meer informatie over een code wordt gegeven door de zgn. "*weight enumerator*".

(3.6.1) <u>DEFINITIE</u>. Is A_i het aantal woorden van gewicht i in een code met woordlengte n dan heet

$$A(z) := \sum_{i=0}^{n} A_i z^i$$

de *weight enumerator* van de code. De rij $(A_i)_{i=0}^{n}$ wordt de *weight distribution* van de code genoemd.

Een voorbeeld van berekening van A(z) is gegeven in (2.7.1).

Is de code klein genoeg dan kunnen we de getallen A_i door inspectie bepalen.

We berekenen de weight enumerator van de binaire Hamming codes. Beschouw i-1 kolommen van de parity check matrix H. Er zijn 3 mogelijkheden:

1) de som van deze kolommen is $\underline{0}$,
2) de som van deze kolommen is een van de gekozen kolommen,
3) de som van deze kolommen is gelijk aan een van de andere kolommen.

Het totale aantal manieren om i-1 kolommen te kiezen is $\binom{n}{i-1}$. Mogelijkheid 1) kan op A_{i-1} manieren optreden, mogelijkheid 2) op $(n-(i-2))A_{i-2}$ manieren,

en 3) op iA_i manieren. Dus

$$iA_i = \binom{n}{i-1} - A_{i-1} - (n-i+2)A_{i-2}.$$

Deze formule hebben we bewezen voor $1 \le i \le n+1$. Als $i > n$ dan is $A_i = 0$, dus voor $i = n + 1$ levert deze formule $0 = 1 - A_n - A_{n-1}$. Dit klopt, want de code is 1-perfect. We vermenigvuldigen beide leden met z^{i-1} en sommeren over $i = 1,\ldots,n+1$

$$\sum_{i=1}^{n+1} iA_i z^{i-1} = \sum_{i=1}^{n+1} \left\{\binom{n}{i-1} z^{i-1} - A_{i-1} z^{i-1} - nz^{i-1} A_{i-2} + (i-2) z^{i-1} A_{i-2}\right\}$$

dus

$$A'(z) = (1+z)^n - A(z) - nzA(z) + z^2 A'(z)$$

daar $A(0) = 1$ is de oplossing

(3.6.2) $$A(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}.$$

We willen nu uit de weight enumerator van een code de weight enumerator van de duale code afleiden. Om het verband tussen beide op te sporen gebruiken we als hulpmiddel karakters.

Zij $(G,+)$ een groep en T de groep van de complexe getallen met modulus gelijk aan 1 en met vermenigvuldiging als operatie. Een *karakter* χ is een homomorfisme $\chi: G \to T$. Dus

$$\chi(g_1+g_2) = \chi(g_1) \cdot \chi(g_2)$$

en

$$\chi(-g_1) = (\chi(g_1))^{-1}.$$

(3.6.3) <u>LEMMA</u>. *Zij* 0 *het eenheidselement in* $(G,+)$. *Dan is* $\chi(0) = 1$.

Een karakter χ heet het *hoofdkarakter* als $\forall g \in G\ [\chi(g) = 1]$.

(3.6.4) <u>LEMMA</u>. *Als* χ *het hoofdkarakter is, dan is* $\sum_{g\in G} \chi(g) = |G|$. *Als* χ *niet het hoofdkarakter is, dan is* $\sum_{g\in G} \chi(g) = 0$.

BEWIJS.

$$\chi(h) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(h+g) = \sum_{k\in G} \chi(k)$$

dus

$$(\chi(h) - 1) \sum_{g\in G} \chi(g) = 0.$$

Als er een h is met $\chi(h) \neq 1$ dan $\sum_{g\in G} \chi(g) = 0$, anders $\sum_{g\in G} \chi(g) = \sum_{g\in G} 1 = |G|$. □

(3.6.5) STELLING. (MacWilliams identiteit). *Zij* V *een* (n,k)-*code over* GF(q), *zij* A(z) *de weight enumerator van* V, *en* B(z) *die van* $V^{\perp}$. *Dan geldt*

$$q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right) = B(z).$$

(3.6.6) LEMMA. *Definieer* $g(\underline{u}) = \sum_{\underline{v}\in R} \chi(\langle \underline{u},\underline{v}\rangle)\, z^{w(\underline{v})}$ *waarin* $w(\underline{v})$ *het gewicht van* $\underline{v}$ *is, en* χ *een willekeurig niet-hoofdkarakter; dan is* $B(z) = \frac{1}{|V|} \sum_{\underline{u}\in V} g(\underline{u})$.

BEWIJS. Zij R de n-dimensionale vectorruimte over GF(q).

$$\sum_{\underline{u}\in V} g(\underline{u}) = \sum_{\underline{u}\in V} \sum_{\underline{v}\in R} \chi(\langle \underline{u},\underline{v}\rangle)\, z^{w(\underline{v})} = \sum_{\underline{v}\in R} z^{w(\underline{v})} \sum_{\underline{u}\in V} \chi(\langle \underline{u},\underline{v}\rangle)$$

$$= \sum_{\underline{v}\in V^{\perp}} z^{w(\underline{v})}\, |V| = |V|\, B(z)$$

want de afbeelding $\underline{u} \mapsto \chi(\langle \underline{u},\underline{v}\rangle)$ is een karakter op de additieve groep van de vectorruimte R en wel het hoofdkarakter als en slechts als $\underline{v} \in V^{\perp}$. □

BEWIJS VAN STELLING (3.6.5)

Zij g gedefinieerd als in het lemma, zij $\underline{u} = u_1u_2\ldots u_n$ en breid w uit tot GF(q) door

$$w(v) = \begin{cases} 0 & \text{als } v = 0 \\ 1 & \text{anders,} \end{cases} \quad \text{voor } v \in GF(q).$$

Dan geldt

$$g(\underline{u}) = \sum_{\underline{v} \in R} \chi(\langle \underline{u}, \underline{v} \rangle)\, z^{w(\underline{v})} =$$

$$= \sum_{v_1 \ldots v_n \in R} z^{w(v_1)+\ldots+w(v_n)} \chi(u_1 v_1 + \ldots u_n v_n) =$$

$$= \sum_{v_1 \ldots v_n} z^{w(v_1)} \chi(u_1 v_1) \ldots z^{w(v_n)} \chi(u_n v_n) =$$

$$= \prod_{i=1}^{n} \sum_{v \in GF(q)} z^{w(v)} \chi(u_i v).$$

Als $u_i = 0$ dan is de som gelijk aan $1 + (q-1)z$,
als $u_i \neq 0$ dan is de som gelijk aan $1 + z \sum_{\substack{\alpha \in GF(q) \\ \alpha \neq 0}} \chi(\alpha) = 1 - z$.

Dus

$$g(\underline{u}) = (1-z)^{w(\underline{u})} (1+(q-1)z)^{n-w(\underline{u})} = (1+(q-1)z)^n \left(\frac{1-z}{1+(q-1)z}\right)^{w(\underline{u})}$$

Nu is

$$B(z) = \frac{1}{|V|} \sum_{\underline{u} \in V} g(\underline{u}) = q^{-k}(1+(q-1)z)^n \sum_{\underline{u} \in V} \left(\frac{1-z}{1+(q-1)z}\right)^{w(\underline{u})}$$

$$= q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right). \quad \square$$

3.7. COMMENTAAR

Een van de baanbrekers in de theorie van groep codes was D. Slepian. Zijn artikelen (1956 en later) geven nu, door de snelle groei van het vak, weinig informatie meer maar ze hebben grote invloed gehad.

De lezer die meer wil weten over drempel decodering raadplege MASSEY (1963).

Een generalisatie van de weight enumerator en de identiteit van MacWilliams vinden we in hoofdstuk VII.

In VAN LINT (1971) wordt met behulp van (3.6.2) aangetoond dat het gemiddelde aantal fouten per blok in een Hamming code na het decoderen groter kan zijn dan ervoor! Het hangt dus van het kanaal af of het wel of niet zinvol is om een Hamming code te gebruiken.

3.8. OPGAVEN

(3.8.1) Beschouw een code over een alfabet van 3 symbolen met woordlengte n. Hoeveel woorden zijn er met Hamming-afstand maximaal 3 tot een gegeven codewoord?

(3.8.2) Beschouw de vectorruimte $\{0,1\}^6$ met Hamming-afstand (= blokken nullen en enen, blok lengte 6). Wat is het aantal punten in een bol met straal 1? Is het mogelijk 9 vectoren (woorden) te vinden zo dat voor ieder paar $\underline{x},\underline{y}$ geldt $\underline{x}\neq\underline{y} \Rightarrow d_H(\underline{x},\underline{y}) \geq 3$?

(3.8.3) Als een (n,k) code over GF(q) een generator G heeft waarin geen kolom met alleen nullen voorkomt, dan is de som van de gewichten van de codewoorden $n(q-1)q^{k-1}$. Bewijs dit.

(3.8.4) Als V een binaire (n,k)-code is, dan hebben alle woorden even gewicht, of de codewoorden van even gewicht vormen een (n,k-1) code. Bewijs dit.

(3.8.5) Zij C een binaire code met generator matrix.

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

Decodeer a) 1 1 0 1 0 1 1,
b) 0 1 1 0 1 1 1,
c) 0 1 1 1 0 0 0.

(3.8.6) De parity check matrix van een binaire code is

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

Decodeer a) 1 1 1 1 0 1 0 0 0,
b) 1 1 0 1 0 1 0 1 1,
c) 0 1 0 0 1 0 0 1 0.

(3.8.7) Zij p priem. Bestaat er een zelfduale (8,4)-code over GF(p)?

(3.8.8) Hoe gedraagt de rate van een (n,k)-Hamming code zich voor grote k?

(3.8.9) U speelt mee in de voetbaltoto en wilt zeker zijn van de 1e of 2e prijs. Hoeveel rijtjes moet U invullen om er zeker van te zijn dat ieder rijtje van 13 keer een 1, 2 of 3 in hoogstens één positie verschilt van een door U ingevuld rijtje?

(3.8.10) Beschouw de code van § 3.5. Decodeer met drempeldecodering het woord (0,0,1,1,0,0,1).

(3.8.11) Wat is de weight enumerator van de (8,4)-verlengde binaire Hamming code?

(3.8.12) Zij C een binaire code met weight enumerator A(z). Druk de weight enumerator van $\overline{C}$ uit in A(z).

(3.8.13) Zij C de $(2^k-1, 2^k-k-1)$-binaire Hamming code. Bepaal de weight enumerator van $\overline{C}^{\perp}$. Wat is het verband met § 2.2?

(3.8.14) Beschouw de code C van § 2.4. Bewijs dat uit de eigenschappen van S_5 volgt dat $\overline{C} = \overline{C}^{\perp}$ en dat daaruit volgt dat de gewichten van de woorden van $\overline{C}$ door 3 deelbaar zijn. Toon aan dat een lineaire combinatie van minder dan vier rijen van de generator een gewicht ≥ 5 heeft. Bepaal dan de weight enumerator van C.

Hoofdstuk IV

GRENZEN AAN CODES

4.1. INLEIDING

In dit hoofdstuk trekken we ons niets aan van de bruikbaarheid van een code (codering, decodering, etc.).

Het gaat ons slechts om aan te geven hoeveel woorden van gegeven lengte en onderlinge afstand er in een code kunnen zitten, en wat niet meer mogelijk is. Met het volgende probleem, nl. uit de zo gevonden klasse van "goede" codes diegene te kiezen die in de practijk nuttig blijken, d.w.z. een mooie structuur bezitten, houden we ons hier niet bezig.

Alvorens verder te gaan en ons probleem exact te formuleren voeren we enige notatie in:

We werken over een *alfabet* Q met $|Q| = q \geq 2$ en $0 \in Q$ (bijv. $Q = \{0,1,\ldots,q-1\}$). Ter afkorting voeren we in: $\theta = (q-1)/q$.

We gebruiken de Hamming-afstand d_H en het begrip gewicht uit (3.1.1). De information rate R van een code is gedefinieerd in (3.1.2).

Een $[n,d]$-code is een triviale code met lengte n of een niet-triviale code met lengte n en minimale afstand tenminste d. Dit is dezelfde notatie als in hoofdstuk II waarbij we nu het aantal woorden weglaten. Een $[n,d]$-code heet *maximaal* als hij niet echt bevat is in een andere $[n,d]$-code.

We kiezen nu n en d vast, en vragen ons af hoe groot het aantal woorden M van een $[n,d]$-code kan zijn. Gezien kennelijk $M \leq q^n$, kunnen we definiëren:

(4.1.1) <u>DEFINITIE</u>. $A(n,d) := \max\{M \mid \text{er is een } [n,M,d]\text{-code}\}$. Een code C met $|C| = A(n,d)$ heet *optimaal*.

Daarnaast kunnen we ons afvragen hoe de functie $A(n,d)$ zich gedraagt voor grote codes met gegeven waarde van d/n. Gezien $A(n,d) \leq q^n$, mogen we definiëren:

(4.1.2) <u>DEFINITIE</u>. $\alpha(\delta) := \limsup_{n\to\infty} n^{-1}\, {}^q\log A(n,\delta n)$.

Op de betekenis hiervan gaan we even in. Als we codes beschouwen met steeds grotere woordlengte n en een vast kanaal met foutenkans p gebruiken zal het gemiddelde aantal fouten per ontvangen woord als np stijgen. Willen

de codes bruikbaar zijn dan zal d tenminste als 2np moeten stijgen, d.w.z. $\delta \geq 2p$. Ons interesseert de maximale waarde van de rate bij gegeven δ en $n\to\infty$, hetgeen $\alpha(\delta)$ is. Vaak neemt men het standpunt van hoofdstuk I in en geeft de waarde van R. De vraag is dan hoe groot d/n kan zijn als $n\to\infty$. Dan is dus de functie $\alpha^{\leftarrow}$ van belang. (Zie hoofdstuk IX).

Hoewel de functies A noch α tot op heden exact bekend zijn, bestaan er verscheidene resultaten die bruikbare schattingen geven.

In (3.4.3) hebben we het begrip verlengde code leren kennen. We zagen toen al dat de minimum afstand van een binaire verlengde code even is. Bij diverse voorbeelden uit hoofdstuk II werden twee verkortingstechnieken gebruikt:

(i) Schrap van alle codewoorden de laatste letter. Dit is de omkering van verlenging. Uit een [n,M,d]-code ontstaat dan een [n-1,M,d-1]-code.

(ii) Neem uit de code C alle woorden met dezelfde laatste letter en laat dan die letter weg. Uit een [n,M,d]-code over Q kan men zo een [n-1,M',d]-code maken met $M' \geq q^{-1} M$.

(4.1.3) <u>STELLING</u>. *Voor binaire codes geldt*

$$A(n,2\ell-1) = A(n+1,2\ell).$$

BEWIJS: Dit volgt door verlenging en verkorting. □

4.2. ONDERGRENS

Om een ondergrens aan te geven voor A(n,d) is het voldoende een [n,d]-code aan te geven die deze grens haalt. We nemen hiervoor een willekeurige maximale [n,d]-code. Deze op het eerste gezicht van weinig inventiviteit getuigende keuze geeft - zeker asymptotisch - een redelijk scherp resultaat.

Een maximale [n,d]-code heeft de eigenschap dat er geen woord met afstand tenminste d tot de code bestaat, m.a.w. de bollen met straal d - 1 om de codewoorden overdekken Q^n.

(4.2.1) <u>LEMMA</u>. *Het volume (= cardinaliteit) van een bol* $B_r(\underline{x}) = \{\underline{y} \mid \underline{y} \in Q^n \wedge d_H(\underline{x},\underline{y}) \leq r\}$ *met straal* r *om een punt* $\underline{x} \in Q^n$ *is gelijk aan*

$$V(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Dus voor een maximale [n,d]-code met M woorden geldt:

$$M.V(n,d-1) \geq q^n.$$

Anderzijds geldt:

(4.2.2) STELLING. [*Gilbert bound*]. *Als* $n \in \mathbb{N}$, $d \in \mathbb{N}$, $d \geq 1$, *dan is*

$$A(n,d) \geq q^n/V(n,d-1).$$

BEWIJS. Ga uit van een triviale [n,d]-code. Als deze niet maximaal is, dan kunnen we een codewoord toevoegen met behoud van de minimale afstand d. Dit kunnen we net zo lang doen tot dat de code maximaal is. Als de code dan M woorden bevat, dan is $M.V(n,d-1) \geq q^n$. Dus dit is de gevraagde [n,d]-code. □

Een bezwaar van deze constructie is dat de gevormde code geen enkele structuur behoeft te hebben. Er geldt echter iets sterkers:

(4.2.3) STELLING. [*Gilbert bound voor lineaire codes*]. *Als* $n \in \mathbb{N}$, $d \in \mathbb{N}$, $d \geq 1$ *en* $k \in \mathbb{N}$ *voldoen aan* $V(n,d-1) < q^{n-k+1}$, *dan bestaat er een lineaire* [n,d]-*code van dimensie* k.

BEWIJS. Voor k = 0 triviaal. Stel er bestaat een [n,d]-code C_{k-1} van dimensie k - 1. Gezien $q^{k-1}.V(n,d-1) < q^n$ is deze code niet maximaal. Dus er is een $\underline{x} \in Q^n$ met $d_H(\underline{x},C_{k-1}) \geq d$. Zij nu C_k het lineair opspansel van $C_{k-1} \cup \{\underline{x}\}$. Dan is C_k een lineaire [n,d]-code van dimensie k, want als $\underline{z} \in C_k$, dan is $\underline{z} = a\underline{x} + \underline{y}$ met $a \in Q$, $y \in C_{k-1}$, dus

$$w(\underline{z}) = w(a^{-1}\underline{z}) = w(\underline{x}+a^{-1}\underline{y}) = d_H(\underline{x},-a^{-1}\underline{y}) \geq d \qquad \text{als } a \neq 0$$

en

$$w(\underline{z}) = w(\underline{y}) \geq d \qquad \text{als } a = 0. \quad \square$$

VOORBEELD. q = 2, n = 13, d = 5.
Dan is

$$V(13,4) = 1 + 13 + 78 + 286 + 715 = 1093.$$

Dus

$$A(13,5) \geq \left\lceil \frac{8192}{1093} \right\rceil = 8.$$

De bijbehorende code mag dan zelfs lineair gekozen worden. Het resultaat is niet overweldigend, gezien het bestaan van een [13,5]-code met 64 codewoorden (de code $\mathbf{Y}$ uit § 2.3), en van een lineaire [13,5]-code van dimensie 5, dus met 32 codewoorden (de verkorte eerste orde Reed-Muller-code met lengte 16 (zie Hfdst. VI)).

We gaan nu over naar het asymptotische geval. Eerst definiëren we de functie $H_q: [0,\theta] \to \mathbb{R}$ door

$$H_q(0) = 0 \text{ en}$$
$$H_q(x) = x\ {}^q\log\,(q-1) - x\ {}^q\log\,x - (1-x)\ {}^q\log\,(1-x) \text{ als } 0 < x \leq \theta.$$

H_q heet de *entropiefunctie* (vgl. (0.4.4)).
Merk op dat H_q monotoon stijgend is.

4.2.4) <u>LEMMA</u>. *Zij* $0 \leq \lambda \leq \theta$, $q \geq 2$. *Dan is*

$$\lim_{n\to\infty} n^{-1}\ {}^q\log\,V_q(n,\lambda n) = H_q(\lambda).$$

<u>BEWIJS</u>. Daar in de som $\sum_{i\leq\lambda n} \binom{n}{i}(q-1)^i$ de laatste term de grootste is geldt

$$\binom{n}{\lfloor\lambda n\rfloor}(q-1)^{\lfloor\lambda n\rfloor} \leq V_q(n,\lfloor\lambda n\rfloor) \leq (1+\lfloor\lambda n\rfloor)\binom{n}{\lfloor\lambda n\rfloor}(q-1)^{\lfloor\lambda n\rfloor}$$

Door nu de ${}^q\log$ te nemen, door n te delen en precies als in het bewijs van Lemma (0.4.5) weer (0.4.2) toe te passen volgt het gestelde. □

We weten nu dus volgens stelling (4.2.2) dat $A(n,d) \geq q^n/V(n,d-1)$. Neem nu $d = \delta n$. Dan is

$$\alpha(\delta) = \limsup_{n\to\infty} n^{-1}\ {}^q\log\,A(n,\delta n) \geq \lim_{n\to\infty} (1 - n^{-1}\ {}^q\log\,V_q(n,\delta n)) =$$

$$= 1 - H_q(\delta).$$

Hiermede is bewezen:

(4.2.5) STELLING. [*Asymptotische Gilbert bound*].

$$\alpha(\delta) \geq 1 - H_q(\delta) \qquad \textit{als } 0 \leq \delta \leq \theta.$$

4.3. BOVENGRENZEN

We zullen achtereenvolgens een aantal bovengrenzen voor A(n,d) behandelen, die asymptotisch steeds scherper worden.

I. DE SINGLETON BOUND

Als men één van de in § 4.1 besproken verkortingstechnieken herhaald toepast ontstaat uit een [n,d]-code met M woorden bijv. een [n-d+1,1]-code met M woorden. Hiervoor geldt vanzelfsprekend: $M \leq q^{n-d+1}$. Dus

(4.3.1) STELLING. [*Singleton bound*]. *Als* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$; *dan is*

$$A(n,d) \leq q^{n-d+1}.$$

Voor lineaire codes levert dit:

(4.3.2) STELLING. [*Singleton bound voor lineaire codes*]. *Voor iedere lineaire* [n,d]-*code van dimensie* k *geldt:*

$$k \leq n - d + 1.$$

VOORBEELD. $q = 2$, $n = 13$, $d = 5$.
Dan is

$$A(13,5) \leq 2^{13-5+1} = 512.$$

Asymptotisch leidt de Singleton bound tot

(4.3.3) STELLING. [*Asymptotische Singleton bound*].

$$\alpha(\delta) \leq 1 - \delta \qquad \textit{als } 0 \leq \delta \leq 1.$$

II. DE PLOTKIN BOUND EN DE GRIESMER BOUND

Beschouw een [n,d]-code met M woorden. Schrijf al deze woorden als rijen van een $M \times n$ - matrix. We berekenen de som van de afstanden van alle geordende paren verschillende codewoorden. Stel in een zekere kolom komt m_j keer het cijfer j voor. De bijdrage tot de bedoelde som door deze kolom is nu:

$$\sum_{j\in Q} m_j(M-m_j).$$

Aangezien $\sum_{j\in Q} m_j = M$, is volgens Cauchy-Schwarz:

$$\sum_{j\in Q} m_j(M-m_j) = M^2 - \sum_{j\in Q} m_j^2 \le M^2 - q^{-1}\Big(\sum_{j\in Q} m_j\Big)^2 = \theta M^2.$$

Aangezien er M(M-1) paren zijn, en iedere kolom ten hoogste θM^2 tot de totale afstand bijdraagt, is

$$M(M-1)d \le n\theta M^2.$$

Hieruit volgt:

$$M \le \frac{d}{d-\theta n} \qquad \text{als } d > \theta n.$$

Als $d \le \theta n$, dan geeft deze methode geen enkel resultaat, maar we kunnen eerst de tweede verkortingstechniek toepassen.

We construeren uitgaande van de [n,d]-code met M woorden, een [n',d]-code met ten minste $Mq^{-n+n'}$ woorden. Passen we nu de bovenstaande ongelijkheid toe, dan is

$$Mq^{-n+n'} \le \frac{d}{d-\theta n'}.$$

Kiezen we nu $n' = \lceil (d-1)/\theta \rceil$ dan vinden we:

$$M \le \left\lfloor \frac{d}{d-\theta\lceil (d-1)/\theta\rceil}\right\rfloor q^{n-\lceil (d-1)/\theta\rceil} \le d\, q^{n-(d-1)/\theta}$$

(Ga na!!). Hiermee is bewezen:

(4.3.4) STELLING. [*Plotkin bound*]. *Als* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$ *en* $\theta = 1 - q^{-1}$, *dan is*

$$A(n,d) \leq \frac{d}{d - \theta n} \qquad \textit{als } d \geq \lfloor \theta n \rfloor + 1$$

$$A(n,d) \leq dq^{n-(d-1)/\theta} \qquad \textit{als } d < \lfloor \theta n \rfloor.$$

VOORBEELD. $q = 2$, $n = 13$, $d = 5$, $\theta = \frac{1}{2}$.
Dan is

$$A(13,5) \leq 5 \,.\, 2^{13-8} = 160.$$

Een scherper resultaat verkrijgt men door de verlengde code te bekijken:

$$A(13,5) = A(14,6) \leq 6.2^{14-10} = 96.$$

Asymptotisch levert de Plotkin bound:

(4.3.5) STELLING. [*Asymptotische Plotkin bound*].

$$\alpha(\delta) \leq 1 - \delta/\theta \qquad \textit{als } 0 \leq \delta < \theta,$$

$$\alpha(\delta) = 0 \qquad \textit{als } \theta \leq \delta \leq 1.$$

Voor *lineaire* codes vond Griesmer een grens, die asymptotisch gelijk is aan de Plotkin bound, maar in speciale gevallen scherper is. Schrijf de generatormatrix op van de $[n,d]$-code met dimensie k. We mogen aannemen dat in de eerste rij minimaal d enen staan. Onder deze d enen komen in de tweede rij ten minste $\lceil d/q \rceil$ gelijken voor. Dit proces voortzettend, concluderen we dat er $\lceil d/q^{k-1} \rceil$ gelijke kolommen voorkomen. Dus ieder codewoord heeft op deze plaatsen steeds hetzelfde cijfer staan. De codewoorden met een nul op deze plaatsen vormen - na weglaten van deze nullen - een $[n- \lceil d/q^{k-1} \rceil, d]$-code met dimensie $k - 1$. Dit proces voortzettend, vinden we een (triviale) $[n - \sum_{i=0}^{k-1} \lceil d/q^i \rceil, d]$-code van dimensie 0. Dus $n - \sum_{i=0}^{k-1} \lceil d/q^i \rceil \geq 0$, ofwel:

(4.3.6) STELLING. [*Griesmer bound*]. *Voor iedere lineaire* [n,d]-*code van dimensie* k *is*

$$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

Deze stelling geldt niet voor niet-lineaire codes: er is een binaire code met 16 woorden ter lengte 18 met minimale afstand 9, en toch geldt niet: $18 \geq 9 + 5 + 3 + 2$. (Deze code kan men verkrijgen uit de Hadamard-matrix van orde 20 door twee kolommen (waarbij één constante) en vier rijen weg te laten, zie § 2.2).

VOORBEELD. $q = 2$, $n = 13$, $d = 5$.
Daar

$$13 \leq 5 + 3 + 2 + 1 + 1 + 1,$$

is $k \leq 6$, dus een lineaire binaire [13,5]-code bevat ten hoogste 64 woorden.

III. DE HAMMING BOUND

Bij een [n,M,d]-code met $d = 2e + 1$ ($e \in \mathbb{N}$) zijn de bollen met straal e om de codewoorden disjunct, dus $M.V(n,e) \leq q^n$.

(4.3.7) STELLING. [*Hamming bound*]. *Als* $q,n,e \in \mathbb{N}$, $q \geq 2$, $d = 2e + 1$, *dan is*

$$A(n,d) \leq q^n/V(n,e).$$

VOORBEELD. $q = 2$, $n = 13$, $d = 5$.
Dan is

$$V(13,2) = 1 + 13 + 78 = 92.$$

Dus

$$A(13,5) \leq \left\lfloor \frac{8192}{92} \right\rfloor = 89.$$

Nemen we nu $d = \delta n$, dan is

$$A(n,\delta n) = A(n,\lceil \delta n \rceil) \le A(n,2\lceil \tfrac{1}{2}\delta n\rceil -1) \le$$

$$\le q^n/V(n,\lceil \tfrac{1}{2}\delta n\rceil -1)$$

en

$$\lim_{n\to\infty} n^{-1}\, {}^q\log V(n,\lceil \tfrac{1}{2}\delta n\rceil -1) = H_q(\tfrac{1}{2}\delta),$$

dus

(4.3.8) <u>STELLING</u>. [*Asymptotische Hamming bound*].

$$\alpha(\delta) \le 1 - H_q(\tfrac{1}{2}\delta).$$

IV. <u>DE ELIAS BOUND</u>

De Plotkin bound is gebaseerd op het feit dat de minimale afstand ten hoogste gelijk is aan de gemiddelde afstand. Als de afstanden elkaar niet veel ontlopen, dus bij codes met weinig woorden, is dit redelijk. Als de code groter wordt, geeft deze methode geen resultaat meer, en moet eerst een geschikte deelcode worden beschouwd. Het idee van Elias is om bij zo'n "grote" code een andere geschikte deelcode te beschouwen, en wel alle codewoorden binnen een zekere bol.

(4.3.9) <u>LEMMA</u>. *Zij* $A,C \subseteq Q^n$. *Dan is er een* $\underline{x} \in Q^n$ *zodat*

$$\frac{|(\underline{x}+A) \cap C|}{|A|} \ge \frac{|C|}{q^n}.$$

<u>BEWIJS</u>. Kies $\underline{x}$ zó dat $|(\underline{x}+A) \cap C|$ maximaal is.

$$q^n|(\underline{x}+A) \cap C| \ge \sum_{\underline{x}\in Q^n} |(\underline{x}+A) \cap C| = \sum_{\underline{x}\in Q^n} \sum_{\underline{a}\in A} \sum_{\underline{c}\in C} |\{\underline{x}+\underline{a}\} \cap \{\underline{c}\}| =$$

$$= \sum_{\underline{a}\in A} \sum_{\underline{c}\in C} 1 = |A|\ |C|. \qquad \square$$

We nemen nu voor A de bol $B_r(\underline{0})$, met straal r om $\underline{0}$, en voor C de beschouwde [n,d]-code met M woorden. Zonder verlies van algemeenheid mogen we aannemen dat $\underline{x} = \underline{0}$. Dus

$$K = |B_r(\underline{0}) \cap C| \geq MV_q(n,r)/q^n.$$

We berekenen nu weer de som van alle afstanden van geordende paren verschillende codewoorden in $B_r(\underline{0})$. We schrijven deze codewoorden als rijen van een $K \times n$ - matrix. Stel in de i^{de} kolom komt m_{ij} keer het cijfer j voor. De bijdrage tot de bedoelde som door deze kolom is nu:

$$\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}).$$

Aangezien

$$\sum_{j=0}^{q-1} m_{ij} = K \qquad \text{en} \qquad \sum_{i=1}^{n} m_{i0} = S \geq K(n-r),$$

is

$$\sum_{j=1}^{q-1} m_{ij}^2 \geq (q-1)^{-1}\left(\sum_{j=1}^{q-1} m_{ij}\right)^2 = (q-1)^{-1}(K-m_{i0})^2$$

en

$$\sum_{i=1}^{n} m_{i0}^2 \geq n^{-1}\left(\sum_{i=1}^{n} m_{i0}\right)^2 = n^{-1}S^2.$$

Dus de totale som is:

$$\sum_{i=1}^{n}\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}) = nK^2 - \sum_{i=1}^{n}\left(m_{i0}^2 + \sum_{j=1}^{q-1} m_{ij}^2\right) \leq$$

$$\leq nK^2 - (q-1)^{-1}\sum_{i=1}^{n}(qm_{i0}^2 + K^2 - 2Km_{i0}) =$$

$$= nK^2 - (q-1)^{-1}\left(nK^2 - 2KS + q\sum_{i=1}^{n} m_{i0}^2\right) \leq$$

$$\leq nK^2 - (q-1)^{-1}n^{-1}(n^2K^2 - 2nKS + qS^2).$$

Veronderstel nu $r \leq \theta n$. Dan is $S \geq K(n-r) \geq q^{-1}nK$, dus de totale som is

$$\leq nK^2 - (q-1)^{-1}n^{-1}(n^2K^2 - 2nK^2(n-r) + qK^2(n-r)^2) =$$

$$= nK^2 - (q-1)^{-1}n^{-1}K^2((q-1)n^2 - 2(q-1)nr + qr^2) =$$

$$= K^2r\left(2 - \frac{r}{\theta n}\right).$$

Aangezien er $K(K-1)$ paren zijn, is

$$K(K-1)d \leq K^2r(2 - \theta^{-1}n^{-1}r).$$

Hiermee is het volgende lemma bewezen.

(4.3.10) <u>LEMMA</u>. *Als* K *woorden ter lengte* n *binnen een bol met straal* $r \leq \theta n$ *een onderlinge afstand minimaal* d *hebben, dan is*

$$d \leq \frac{Kr}{K-1}\left(2 - \frac{r}{\theta n}\right)$$

ofwel

$$K \leq \frac{\theta nd}{\theta nd - 2\theta nr + r^2} \qquad \textit{als } \theta nd - 2\theta nr + r^2 > 0.$$

Combinatie van de gevonden resultaten levert:

(4.3.11) <u>STELLING</u>. [*Elias bound*]. *Zij* $q,n,d,r \in \mathbb{N}$, $q \geq 2$, $d \geq 1$, $\theta = 1 - q^{-1}$, $r \leq \theta n$, $\theta nd - 2\theta nr + r^2 > 0$, *dan is*

$$A(n,d) \leq \frac{\theta nd}{\theta nd - 2\theta nr + r^2} \cdot \frac{q^n}{V_q(n,r)}.$$

<u>BEWIJS</u>.

$$\frac{MV_q(n,r)}{q^n} \leq K \leq \frac{\theta nd}{\theta nd - 2\theta nr + r^2}. \qquad \square$$

VOORBEELD. $q = 2$, $n = 13$, $d = 5$, $\theta = \frac{1}{2}$.
We kunnen hier weer beter overgaan op de verlengde code. Dus

$$A(13,5) = A(14,6) \le \frac{42}{42-14r+r^2} \cdot \frac{2^{14}}{\sum_{i\le r}\binom{14}{i}} .$$

Met $r = 3$ volgt $A(13,5) \le 162$.
Asymptotisch levert de Elias bound een grens die uniform beter is dan zowel de Plotkin als de Hamming bound:

(4.3.12) STELLING. [*Asymptotische Elias bound*].

$$\alpha(\delta) \le 1 - H_q(\theta - \sqrt{\theta(\theta-\delta)}\ ) \qquad \textit{als } 0 \le \delta \le \theta,$$

$$\alpha(\delta) = 0 \qquad \textit{als } \theta \le \delta \le 1.$$

BEWIJS. Zij $0 < \delta \le \theta$, $0 \le \lambda < \theta - \sqrt{\theta(\theta-\delta)}$, en $r = \lfloor \lambda n \rfloor$. Dan is $\theta\delta - 2\theta\lambda + \lambda^2 > 0$, dus

$$n^{-1}\ {}^q\log A(n,\delta n) \le n^{-1}\ {}^q\log\left(\frac{\theta n\lceil \delta n\rceil}{\theta n\lceil \delta n\rceil - 2\theta n\lfloor \lambda n\rfloor + \lfloor \lambda n\rfloor^2}\ \frac{q^n}{V_q(n,\lfloor \lambda n\rfloor)}\right) \sim$$

$$\sim n^{-1}\left({}^q\log\left(\frac{\theta\delta}{\theta\delta - 2\theta\lambda + \lambda^2}\right) + n - nH_q(\lambda)\right) \sim$$

$$\sim 1 - H_q(\lambda).$$

Dus

$$\alpha(\delta) \le 1 - H_q(\lambda).$$

Dit geldt voor iedere $\lambda \in [0, \theta-\sqrt{\theta(\theta-\delta)})$, dus

$$\alpha(\delta) \le 1 - H_q(\theta - \sqrt{\theta(\theta-\delta)}\ ). \qquad \square$$

V. DE JOHNSON BOUND

Johnson verscherpte de Hamming bound door ook te kijken naar wat er

zich buiten de bollen met straal e afspeelt. Stel we hebben een [n,M,d]-code C. We definiëren C^i als de verzameling woorden met afstand i tot C. Dus $C^0 = C$ en $\sum_{i=0}^{\infty} |C^i| = q^n$.

Definiëer $M_r(\underline{x})$ als het aantal woorden in C^r die op afstand r liggen van het codewoord $\underline{x}$, en $M(\underline{y})$ als het aantal codewoorden dat minimale afstand heeft tot het woord $\underline{y}$. Dan is

$$\sum_{\underline{x}\in C} M_r(\underline{x}) = \sum_{\underline{y}\in C^r} M(\underline{y}).$$

Definiëren we verder

$$M_r^0 = \min_{\underline{x}\in C} M_r(\underline{x})$$

en

$$M_0^r = \max_{y\in C^r} M(\underline{y}).$$

dan is

$$|C|M_r^0 \le \sum_{\underline{x}\in C} M_r(\underline{x}) = \sum_{\underline{y}\in C^r} M_0(\underline{y}) \le |C^r|M_0^r,$$

dus

$$|C^r| \ge M\, M_r^0/M_0^r.$$

We vinden zo:

$$M \sum_{r=0}^{\infty} (M_r^0/M_0^r) \le q^n,$$

dus

$$M \le q^n / \sum_{r=0}^{\infty} (M_r^0/M_0^r).$$

Als $r < d/2$, dan is $M_r^0 = \binom{n}{r}(q-1)^r$ en $M_0^r = 1$. We moeten nu een onderschatting geven voor M_r^0 en een bovenschatting voor M_0^r voor $r \ge d/2$.

Als we M_r^0 met 0 schatten, dan volgt de Hamming bound. We geven hier

voor $q = 2$ en $d = 2e + 1$ één van de bekende schattingen voor M^0_{e+1} en M^{e+1}_0, en schatten M^0_r voor $r \geq e + 2$ met 0.

Zij $A(n,d,w)$ het maximale aantal woorden in $\{0,1\}^n$ met gewicht w en onderlinge afstand $\geq d$.

(4.3.13) LEMMA.

$$A(n,2k-1,w) = A(n,2k,w) \leq \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \right\lfloor \ldots \left\lfloor \frac{n-w+k}{k} \right\rfloor \ldots \right\rfloor \right\rfloor.$$

BEWIJS.

Daar woorden met hetzelfde gewicht altijd een even afstand hebben, geldt $A(n,2k-1,w) = A(n,2k,w)$.

Stel er is een verzameling van K woorden in $\{0,1\}^n$ met gewicht w en onderlinge afstand $\geq 2k$. Schrijf deze woorden als rijen van een $K \times n$-matrix. In iedere kolom van deze matrix staan ten hoogste $A(n-1, 2k,w-1)$ enen. Het totaal aantal enen is Kw.

Dus geldt

$$Kw \leq n\, A(n-1,2k,w-1).$$

en dus

$$A(n,2k,w) \leq \left\lfloor \frac{n}{w} A(n-1,2k,w-1) \right\rfloor.$$

Daar verder geldt

$$A(n,2k,k-1) = 1,$$

vinden we door inductie het gestelde. □

(4.3.14) LEMMA. *Zij* C *een binaire* $[n,d]$*-code met* $d = 2e + 1$. *Dan is*

$$M^0_{e+1} \geq \binom{n}{e+1} - \binom{d}{e} A\,(n,d,d).$$

BEWIJS. Zij $\underline{x} \in C$. We mogen aannemen dat $\underline{x} = \underline{0}$.

Het aantal codewoorden van gewicht d is ten hoogste $A(n,d,d)$. Het aantal woorden van gewicht $e + 1$ met afstand e tot de code is dus ten hoogste $\binom{d}{e+1} A(n,d,d)$. Hieruit volgt het gestelde daar er

$\binom{n}{e+1}$ woorden zijn met afstand e + 1 tot $\underline{0}$. □

(4.3.15) LEMMA. *Voor een binaire* [n,d]-*code* C *met* d = 2e + 1 *geldt*

$$M_0^{e+1} \le \left\lfloor \frac{n}{e+1} \right\rfloor .$$

BEWIJS. Zij $\underline{y} \in C^{e+1}$. We mogen aannemen dat $\underline{y} = \underline{0}$. Dan is $M(\underline{y})$ het aantal codewoorden met gewicht e + 1. Dit aantal is ten hoogste A(n,d,e+1) waaruit het gestelde volgt. □

We hebben zo gevonden:

(4.3.16) STELLING. [*Johnson bound*]. *Zij* q = 2, n,e ∈ ℕ, d = 2e + 1. *Dan is*

$$A(n,d) \le \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i} + \dfrac{\binom{n}{e+1} - \binom{d}{e} A(n,d,d)}{\left\lfloor \dfrac{n}{e+1} \right\rfloor}}$$

waarin

$$A(n,d,d) \le \left\lfloor \frac{n}{d} \left\lfloor \frac{n-1}{d-1} \right\rfloor \cdots \left\lfloor \frac{n-e}{d-e} \right\rfloor \cdots \right\rfloor \right\rfloor .$$

VOORBEELD. q = 2, n = 13, d = 5, e = 2.
Dan is

$$A(13,5,5) \le \left\lfloor \frac{13}{5} \left\lfloor \frac{12}{4} \left\lfloor \frac{11}{3} \right\rfloor \right\rfloor \right\rfloor = 23,$$

$$A(13,5) \le \left\lfloor \frac{8192}{1 + 13 + 78 + \dfrac{286 - 10.23}{4}} \right\rfloor = \left\lfloor \frac{8192}{106} \right\rfloor = 77.$$

VI. DE LINEAR-PROGRAMMING BOUND.

Deze laatste grens, die door P. Delsarte is ontwikkeld, geeft vaak zeer scherpe resultaten, maar vergt in elk geval afzonderlijk zeer veel rekenwerk. Hij berust op een ongelijkheid, die in nauw verband staat met de MacWilliams identiteit voor duale (lineaire) codes (zie (3.6.5)).

Voor vaste q en n definiëren we eerst:

$$K_k(i) = \sum_j \binom{i}{j}\binom{n-i}{k-j}(-1)^j(q-1)^{k-j}.$$

Voor vaste q, n en k is K_k een polynoom, het z.g. Krawtchouk-polynoom (vgl. § 7.2).

De getallen $K_k(i)$ voldoen aan een eenvoudige recurrente betrekking:

$$K_k(i) = K_k(i-1) - (q-1)K_{k-1}(i) - K_{k-1}(i-1),$$

met $K_0(i) = 1$, $K_k(0) = \binom{n}{k}(q-1)^k$.

Als we voor het alfabet Q de restklassenring modulo q nemen, en we definiëren $\langle \underline{x},\underline{y}\rangle = \sum_{i=1}^{n} x_i y_i$, dan geldt:

(4.3.17) <u>LEMMA</u>. *Zij* ω *een primitieve* q*-de eenheidswortel, en* $\underline{x} \in Q^n$ *een vast woord van gewicht* i. *Dan is*

$$\sum_{\substack{\underline{y}\in Q^n \\ w(\underline{y})=k}} \omega^{\langle \underline{x},\underline{y}\rangle} = K_k(i)$$

<u>BEWIJS</u>. We mogen aannemen dat $\underline{x} = (x_1,\ldots,x_i,0,\ldots,0)$ met $x_h \neq 0$ voor $0 < h \leq i$.

Zij nu $0 < h_1 < \ldots < h_j \leq i < h_{j+1} < \ldots < h_k \leq n$ en zij D de verzameling van alle woorden (van gewicht k) in Q^n die juist in de posities $h_1,\ldots,h_k$ ongelijk 0 zijn. Dan geldt:

$$\sum_{\underline{y}\in D} \omega^{\langle \underline{x},\underline{y}\rangle} = \sum_{y_{h_1},\ldots,y_{h_k}\in Q\setminus\{0\}} \omega^{x_{h_1}y_{h_1}+\ldots+x_{h_j}y_{h_j}} =$$

$$= (q-1)^{k-j} \prod_{\ell=1}^{j} \sum_{y\in Q\setminus\{0\}} \omega^{x_{h_\ell}y} = (-1)^j (q-1)^{k-j}.$$

Dus

$$\sum_{\substack{\underline{y}\in Q^n \\ w(\underline{y})=k}} \omega^{\langle \underline{x},\underline{y}\rangle} = \sum_j \binom{i}{j}\binom{n-i}{k-j}(-1)^j (q-1)^{k-j} = K_k(i). \qquad \square$$

We definiëren nu

(4.3.18) <u>DEFINITIE</u>: Zij $C \subseteq Q^n$ een code met M woorden en gemiddeld A_i woorden op afstand i van een vast codewoord, dus

$$A_i = M^{-1} \left|\{(\underline{x},\underline{y}) \mid \underline{x},\underline{y} \in C \wedge d_H(\underline{x},\underline{y}) = i\}\right|.$$

Dan heet de rij $(A_i)_{i=0}^n$ de *distance distribution* of *inner distribution* van C.

Merk op dat voor een lineaire code de distance distribution gelijk is aan de weight distribution (zie (3.6.1)).

(4.3.19) <u>LEMMA</u>. *Zij* $(A_i)_{i=0}^n$ *de distance distribution van een code. Dan is*

$$\sum_{i=0}^{n} A_i K_k(i) \geq 0$$

voor iedere $k \in \{0,1,\ldots,n\}$.

<u>BEWIJS</u>.

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \sum_{\substack{\underline{x},\underline{y}\in C \\ d_H(\underline{x},\underline{y})=i}} \sum_{\substack{\underline{z}\in Q^n \\ w(\underline{z})=k}} \omega^{\langle \underline{x}-\underline{y},\underline{z}\rangle} =$$

$$= \sum_{\substack{\underline{z}\in Q^n \\ w(\underline{z})=k}} \left| \sum_{\underline{x}\in C} \omega^{\langle \underline{x},\underline{z}\rangle} \right|^2 \geq 0. \qquad \square$$

(4.3.20) <u>STELLING</u>. *Zij* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$. *Dan is*

$$A(n,d) \leq \max \left\{ \sum_{i=0}^{n} A_i \;\middle|\; A_0 = 1,\ A_i = 0 \quad \textit{voor } 1 \leq i < d,\ A_i \geq 0,\ \sum_{i=0}^{n} A_i K_k(i) \geq 0 \quad \textit{voor } k \in \{1,\ldots,n\} \right\}.$$

Als $q = 2$, d *even, dan mogen we bovendien aannemen dat* $A_i = 0$ *als* i *oneven.*

De laatste bewering volgt uit het feit dat we door eerst te verkorten en dan weer te verlengen een [n,M,d]-code met d even kunnen omzetten in een [n,M,d]-code met alleen even gewichten, en dus even afstanden.

VOORBEELD. We beschouwen weer een [13,5]-code met q = 2. Door toevoeging van één extra parity check bit verkrijgen we een [14,6]-code met hetzelfde aantal woorden. Bovendien hebben alle woorden even gewicht. We weten dus a priori:

$$A_0 = 1,\ A_1 = A_2 = A_3 = A_4 = A_5 = A_7 = A_9 = A_{11} = A_{13} = 0,$$

$$A_6 \geq 0,\ A_8 \geq 0,\ A_{10} \geq 0,\ A_{12} \geq 0,\ A_{14} \geq 0.$$

De stelling geeft de ongelijkheden:

$$14 + 2A_6 - 2A_8 - 6A_{10} - 10A_{12} - 14A_{14} \geq 0$$
$$91 - 5A_6 - 5A_8 + 11A_{10} + 43A_{12} + 91A_{14} \geq 0$$
$$364 - 12A_6 + 12A_8 + 4A_{10} - 100A_{12} - 364A_{14} \geq 0$$
$$1001 + 9A_6 + 9A_8 - 39A_{10} + 121A_{12} + 1001A_{14} \geq 0$$
$$2002 + 30A_6 - 30A_8 + 38A_{10} - 22A_{12} - 2002A_{14} \geq 0$$
$$3003 - 5A_6 - 5A_8 + 27A_{10} - 165A_{12} + 3003A_{14} \geq 0$$
$$3432 - 40A_6 + 40A_8 - 72A_{10} + 264A_{12} - 3432A_{14} \geq 0$$

We moeten nu $M = 1 + A_6 + A_8 + A_{10} + A_{12} + A_{14}$ naar boven begrenzen. Dit lineair programmeringsprobleem blijkt een unieke maximale oplossing te bezitten:

$$A_6 = 42,\ A_8 = 7,\ A_{10} = 14,\ A_{12} = A_{14} = 0.$$

Dus

$$M \leq 64.$$

Dus

$$A(13,5) \leq 64.$$

Zoals we gezien hebben, bestaat er een [13,5]-code met 64 woorden, dus deze grens is scherp, d.w.z. de code Y uit § 2.3 is optimaal.

OPMERKING. In de lemma's (4.3.17) en (4.3.19) wordt gebruik gemaakt van een ringstructuur (de restklassenring), van een inwendig product, en van een primitieve eenheidswortel. In wezen is dit volstrekt arbitrair. Men kan de theorie veel abstracter opbouwen.

We voorzien Q van een willekeurige abelse groepsstructuur. We geven de karaktergroep van Q aan met $\hat{Q}$ en die van Q^n met $\hat{Q}^n$. Ieder karakter $\chi \in \hat{Q}^n$ definieert ondubbelzinnig karakters $\chi_1,\ldots,\chi_n \in \hat{Q}$ zodat

$$\chi(x_1,\ldots,x_n) = \chi_1(x_1)\ldots\chi_n(x_n).$$

Het aantal niet-hoofdkarakters onder $\chi_1,\ldots\chi_n$ noemen we het *gewicht* van χ, notatie: $w(\chi)$. Nu geldt:

(4.3.21) LEMMA. *Zij* $\underline{x} \in Q^n$ *een woord van gewicht* i. *Dan is*

$$\sum_{\substack{\chi\in\hat{Q}^n \\ w(\chi)=k}} \chi(\underline{x}) = K_k(i).$$

BEWIJS. Zoals (4.3.17). □

We kunnen nu lemma (4.3.19) nogmaals bewijzen.

BEWIJS van (4.3.19).

$$M \sum_{i=0}^{n} A_i\, K_k(i) = \sum_{i=0}^{n} \sum_{\substack{\underline{x},\underline{y}\in C \\ d_H(\underline{x},\underline{y})=i}} \sum_{\substack{\chi\in\hat{Q}^n \\ w(\chi)=k}} \chi(\underline{x}-\underline{y}) =$$

$$= \sum_{\substack{\chi\in\hat{Q}^n \\ w(\chi)=k}} \left|\sum_{\underline{x}\in C} \chi(\underline{x})\right|^2 \geq 0. \qquad \square$$

Als C een abelse groepcode is, waarbij Q dus voorzien is van abelse groepsstructuur, dan is

$$\sum_{\underline{x}\in C} \chi(\underline{x}) = 0 \quad \text{als} \quad C \not\subseteq \operatorname{Ker} \chi,$$
$$= M \quad \text{als} \quad C \subseteq \operatorname{Ker} \chi.$$

Definiëren we C^* als de verzameling van alle karakters $\chi \in \hat{Q}^n$ met $\operatorname{Ker} \chi \supseteq C$, dan is C^* een groepcode over $\hat{Q}$. Als $(B_k)_{k=0}^n$ de weight distribution van C^* is, dan is

$$(4.3.22) \qquad B_k = \sum_{\substack{\chi\in C^* \\ w(\chi)=k}} 1 = M^{-1} \sum_{i=0} A_i K_k(i) \qquad (k=0,1,\ldots,n).$$

Als tenslotte C een lineaire code is, waarbij Q dus voorzien is van een lichaamsstructuur, dan is $C^\perp$ equivalent met C^* onder het isomorfisme ϕ: $Q^n \to \hat{Q}^n$ gedefiniëerd door

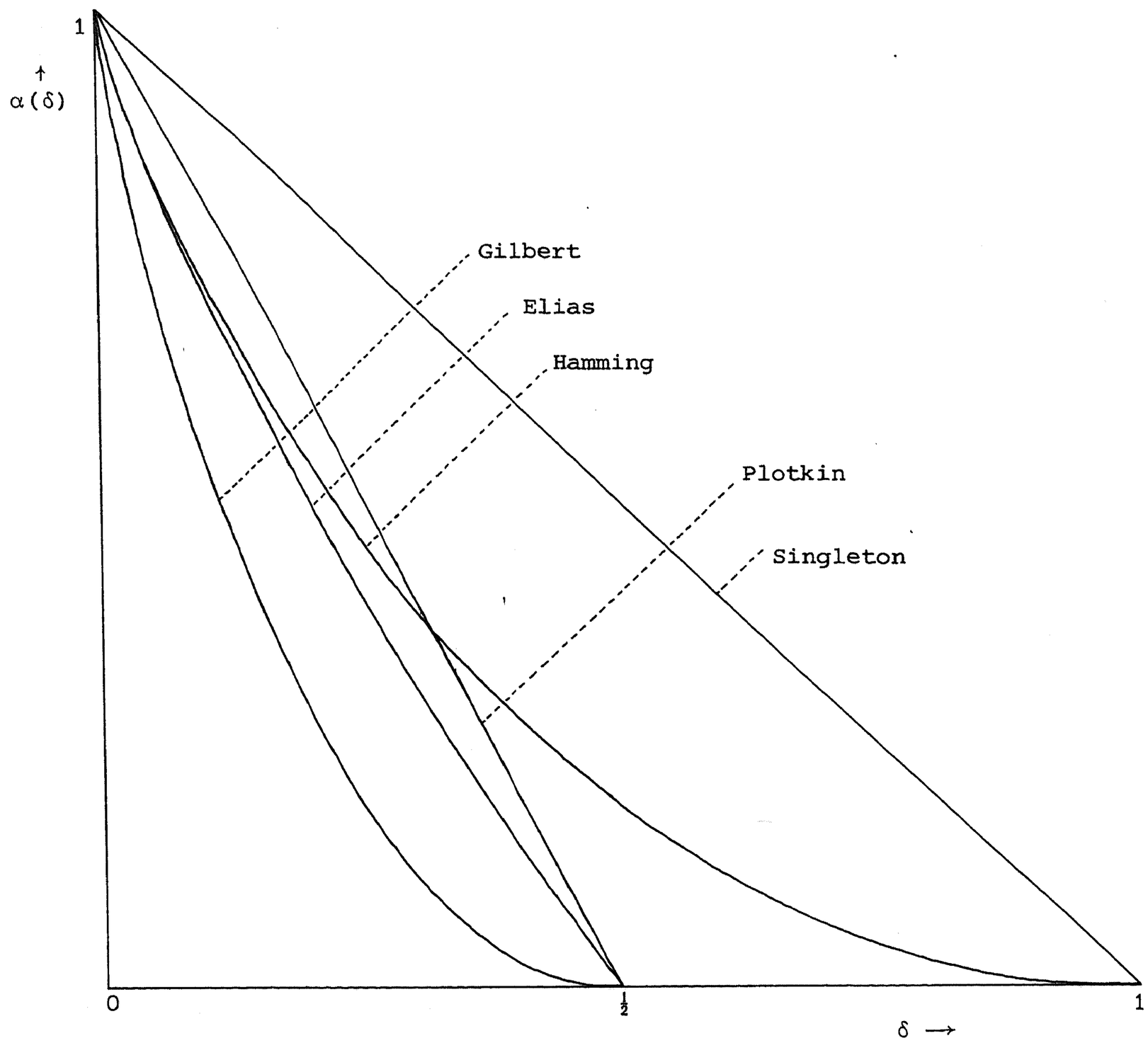
$$\phi(\underline{y}) = \chi_1(<.,\underline{y}>),$$

waarbij χ_1 een of ander niet-hoofdkarakter is. Dus $(B_k)_{k=0}^n$ is de weight distribution van de duale code. De relaties (4.3.22) zijn de MacWilliams relaties welke in (3.6.5) in de vorm van een relatie tussen de weight enumerators werden gegeven.

4.4. COMMENTAAR

De verschillende grenzen die in dit hoofdstuk zijn behandeld vindt men in de literatuur onder de bij de stellingen genoemde namen. We verwijzen verder naar BERLEKAMP (1968), HELGERT & STINAFF (1973), SLOANE (1972). Recente verscherpingen vindt men in LEVENSHTEIN (1975), SIDELNIKOV (1975), BEST & BROUWER (1975), McELIECE e.a. (1976), BEST e.a. (1976).

Onderstaande grafiek geeft voor q = 2 de verschillende asymptotische grenzen.



4.5. OPGAVEN

(4.5.1) Bepaal A(10,5) voor q = 2.

(4.5.2) Bewijs dat als q = 2 en de rechterkant van de Plotkin Bound (4.3.4) een oneven geheel getal is deze grens met 1 verminderd kan worden.

(4.5.3) Als in (4.3.13) de buitenste t entierhaken door ronde haken vervangen kunnen worden en gelijkheid optreedt dan vormen de woorden van een [n,A(n,2k,w),2k]-code met woorden van gewicht w een t-design. Bewijs dit.

(4.5.4) Bepaal grenzen voor A(17,8).

(4.5.5) Wanneer is de Plotkin bound scherp? Ga na dat de [27,6,16]-code uit § 2.5 optimaal is.

(4.5.6) Bewijs dat door inkorten van een binaire Hamming code een optimale code ontstaat.

(4.5.7) Bewijs dat $A(n,d,w) \leq \left[\frac{n}{w} A(n-1,d,w-1)\right]$

en $A(n,d,w) \leq \left[\frac{n}{n-w} A(n-1,d,w)\right]$.

Geef een voorbeeld met $w \leq \frac{1}{2}n$ waarbij de tweede ongelijkheid scherper is dan de eerste.

(4.5.8) Bewijs dat de Plotkin bound voor $d > \theta n$ volgt uit de linear programming bound.

(4.5.9) [GREY bound] Zij C een binaire [n,M,d]-code zo dat als $\underline{x} \in C$ dan ook $\underline{x} + \underline{j} \in C$. Als $n - \sqrt{n} < 2d \leq n$ dan geldt

$$M \leq \frac{8d(n-d)}{n-(n-2d)^2} .$$

(Aanwijzing (E. WATTEL): gebruik de tweede Delsarte ongelijkheid d.w.z. (4.3.19) met k = 2.)

(4.5.10) Bewijs de MacWilliams identiteit (3.6.5) uitgaande van (4.3.22).

(4.5.11) Bewijs dat de [8,20,3]-code uit § 2.2 optimaal is (moeilijk!).

Hoofdstuk V

CYCLISCHE CODES

5.1. CYCLISCHE CODES

Een lineaire code V (ter lengte n over een eindig lichaam $\mathbb{F}$) werd gedefinieerd als een deelruimte van de n-dimensionale vectorruimte over $\mathbb{F}$, d.w.z. als $(a_0,\ldots,a_{n-1}) \in V$ en $(b_0,\ldots,b_{n-1}) \in V$, dan ook $(a_0+b_0,\ldots,a_{n-1}+b_{n-1}) \in V$, en als $(a_0,\ldots,a_{n-1}) \in V$ en $\lambda \in F$, dan $(\lambda a_0,\ldots,\lambda a_{n-1}) \in V$. Een lineaire code V heet een *cyclische code* als daarnaast ook geldt: als $(a_0,\ldots,a_{n-1}) \in V$ dan $(a_{n-1}, a_0,\ldots,a_{n-2}) \in V$.

Een triviaal voorbeeld van een cyclische code is de code V ter lengte 2k met: $(a_0,\ldots,a_{2k-1}) \in V \Longleftrightarrow a_0=a_k,\ a_1=a_{k+1},\ldots,a_{k-1}=a_{2k-1}$. Zij $\mathcal{R}^{(n)}$ de n-dimensionale vectorruimte over $\mathbb{F}$. Door $(a_0,\ldots,a_{n-1})$ te schrijven als $a_0+a_1x+\ldots a_{n-1}x^{n-1}$, is het mogelijk een vector uit $\mathcal{R}^{(n)}$ voor te stellen als een element van (een volledig representantensysteem van) de restklassenring $\mathbb{F}[x]/(x^n-1)$. Het is duidelijk dat deze relatie een 1-1-correspondentie geeft tussen elementen van $\mathcal{R}^{(n)}$ en elementen van $\mathbb{F}[x]/(x^n-1)$, en daarom maken we in het vervolg geen onderscheid meer tussen deze twee verzamelingen; beide noteren we met $\mathcal{R}^{(n)}$ of $\mathcal{R}$.

(5.1.1) <u>STELLING</u>. *Een lineaire code* V *in* $\mathcal{R}^{(n)}$ *is cyclisch als en alleen als* V *een ideaal in* $\mathbb{F}[x]/(x^n-1)$ *is.*

<u>BEWIJS</u>. (i) Zij V cyclisch. Is $a(x) = a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ een codewoord dan $a_{n-1}+a_0x+a_1x^2+\ldots+a_{n-2}x^{n-1} = xa(x)$ ook. Daar V lineair is volgt hieruit dat voor ieder polynoom f(x) geldt dat $f(x)\,a(x) \in V$. Dus V is een ideaal.

(ii) Is omgekeerd V een ideaal dan is met a(x) ook xa(x) in V. Dus is V cyclisch. □

Zij $q := |\mathbb{F}|$. We beperken ons in het vervolg tot de gevallen waarin $(n,q) = 1$. Verder zullen wij schrijven: $R := \mathbb{F}[x]$, $S := (x^n-1)$ (het ideaal in R voortgebracht door x^n-1) en $\mathcal{R}\,g(x)$:= het ideaal in $\mathcal{R}$ voortgebracht door g(x). Dus $\mathcal{R} = R/S$. Omdat R een hoofdideaalring is, is ook ieder ideaal in $\mathcal{R}$ een hoofdideaal, en ieder ideaal V in $\mathcal{R}$ wordt voortgebracht door een monisch polynoom g(x) met de laagste graad in V. Dit uniek bepaalde poly-

noom heet de *generator* van V. Steeds is deze $g(x)$ een deler (in R) van x^n-1. Anders zou de g.g.d. (in R) van $g(x)$ en x^n-1 een polynoom in V zijn met lagere graad dan $g(x)$.

Zij $x^n-1 = f_1(x).\ \ldots\ .f_t(x)$ de ontbinding (in R) van x^n-1 in irreducibele polynomen. Een generator $g(x)$ zal dan het product van een aantal faktoren f_i zijn. Omdat we hebben aangenomen dat $(n,q) = 1$, zijn $f_1,\ldots,f_t$ alle verschillend. Als een ideaal V als generator een der faktoren f_i heeft, d.w.z. $V = Rf_i(x)$, dan is V een maximaal ideaal in R en V heet dan een *maximale cyclische code*.

5.2. GENERATOR MATRIX EN CHECK POLYNOOM

Zij $g(x)$ de generator van een cyclische code V in R met graad n-k. Dan vormen:

$$g(x), x.g(x), \ldots, x^{k-1}.g(x)$$

een basis voor V. Dus een woord $(b_0,\ldots,b_{k-1})$ kan gecodeerd worden als:

$$b_0.g(x) + b_1.x.g(x) + \ldots + b_{k-1}.x^{k-1}.g(x);$$

d.w.z. als $b(x).g(x)$, waarbij:

$$b(x) = b_0 + b_1x + \ldots + b_{k-1}x^{k-1}.$$

Zij $b(x)g(x) = v(x) = v_0 + v_1x + \ldots\ v_{n-1}x^{n-1}$.

Dan

$$(b_0,\ldots,b_{k-1})\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & \cdot & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & \cdot\ \cdot & & & \cdot\ \cdot & & \cdot \\ \cdot & \cdot & \cdot\ \cdot\ \cdot & & & & \cdot\ \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot & \cdot & & & \cdot\ \cdot & \cdot \\ \cdot & \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot & & \cdot & 0 \\ 0 & 0 & \cdots & 0 & g_0\ g_1 & \cdots & \cdot & g_{n-k} \end{pmatrix} = (v_0,\ldots,v_{n-1}).$$

Dus de bovenstaande matrix G is een generator matrix voor V.

Een parity-check matrix voor V kan als volgt worden verkregen. Omdat $g(x) \mid x^n-1$ bestaat er een $h(x)$ zo dat $g(x)h(x) = x^n-1$ (in R). Omdat $g(x)$ de graad n-k heeft, zal $h(x)$ de graad k hebben. Dus:

$$h(x) = h_0 + h_1x + \ldots + h_kx^k.$$

Omdat in R geldt: $g(x)h(x) = 0$, weten we:

$$\begin{array}{lllll}
g_0h_{n-1} & + g_1h_{n-2} & + \ldots\ldots\ldots\ldots & + g_{n-2}h_1 & + g_{n-1}h_0 & = 0, \\
g_0h_{n-2} & + g_1h_{n-3} & + \ldots\ldots\ldots\ldots & + g_{n-2}h_0 & + g_{n-1}h_{n-1} & = 0, \\
\cdot & \cdot & & \cdot & \cdot & \cdot \\
\cdot & \cdot & & \cdot & \cdot & \cdot \\
\cdot & \cdot & & \cdot & \cdot & \cdot \\
g_0h_0 & + g_1h_{n-1} & + \ldots\ldots\ldots\ldots & + g_{n-2}h_2 & + g_{n-1}h_1 & = 0.
\end{array}$$

Als nu:

$$H = \begin{pmatrix}
0 & \cdot & \cdot & \cdot & \cdot & 0 & h_k & \cdot & \cdot & \cdot & h_1 & h_0 \\
0 & \cdot & \cdot & \cdot & 0 & h_k & \cdot & \cdot & \cdot & \cdot & h_0 & 0 \\
\cdot & & & \cdot & \cdot & & & & \cdot & \cdot & 0 & 0 \\
\cdot & & \cdot & \cdot & & & & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & & & & \cdot & \cdot & \cdot & & \cdot & \cdot \\
0 & \cdot & & & & \cdot & \cdot & \cdot & & & \cdot & \cdot \\
h_k & \cdot & \cdot & \cdot & h_1 & h_0 & 0 & \cdot & \cdot & \cdot & 0 & 0
\end{pmatrix}$$

dan geldt dus $G.H^T = 0$ (omdat $h_{k+1} = \ldots = h_{n-1} = 0$), d.w.z. H is de parity-check matrix van de code. Hieruit volgt ook dat de code $Rh(x)$ equivalent is met de duale code van $Rg(x)$. Het polynoom $h(x)$ heet het *check polynoom* van de code V. $v(x)$ zit in deze code als en slechts als $v(x)h(x) = 0$ (in R).

Wij geven nu een voorbeeld van een cyclische code.

Zij $\mathbb{F} = \mathbb{F}_2$ en $n = 7$. De ontbinding van x^n-1 in irreducibele faktoren is:

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

Als $g(x) = x^3+x+1$, dan

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

Nu is $h(x) = (x+1)(x^3+x^2+1) = x^4 + x^2 + x + 1$, dus:

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

d.w.z. $\mathcal{R}g(x)$ is equivalent met de (7,4)-Hamming-code.

De duale code van de maximale cyclische code $\mathcal{R}f_i(x)$ heeft $f_i(x)$ als check polynoom. Deze code heet een *minimale* cyclische code of *irreducibele* cyclische code. Een minimale cyclische code is een lichaam. Om dit in te zien is het voldoende om te bewijzen dat twee codewoorden $a(x)$ en $b(x)$ alleen product 0 kunnen hebben als een factor 0 is (zie (0.1.5)). Maar $a(x)b(x) = 0$ in $\mathcal{R}$ betekent dat in $\mathcal{R}$ een van de factoren bijv. $a(x)$ door $f_i(x)$ deelbaar is. Daar ieder codewoord deelbaar is door $(x^n-1)/f_i(x)$ is $a(x) = 0$. Als eenvoudigste voorbeeld kiezen we $n = 2^k-1$ en nemen voor $f(x)$ een primitief polynoom van de graad k. Laat $x^n-1 = g(x)f(x)$. De code $\mathcal{R}g(x)$ heeft dimensie k en bestaat dus uit 2^k woorden. Daarbij zijn $\underline{0}$ en de n cyclische permutaties van $g(x)$ en dus blijkbaar geen andere woorden. Dit betekent dat ieder tweetal cyclische permutaties van $g(x)$ als verschil weer een cyclische permutatie heeft! Deze code heeft dus de eigenaardige eigenschap dat ieder tweetal woorden dezelfde afstand heeft. Zo'n code heet *equidistant*. In het geval van ons voorbeeld moet de afstand dan 2^{k-1} zijn (zie § 2.2).

5.3. NULPUNTEN VAN EEN CYCLISCHE CODE

Zij β_i een nulpunt van f_i in een uitbreidingslichaam van $\mathbb{F}$. Dan is:

$$\mathcal{R}f_i(x) = \{v(x) \mid v(\beta_i) = 0\}$$

(want f_i is het minimaalpolynoom van β_i).
Algemeen kan een cyclische code V gespecifieerd worden door een aantal nulpunten voor te schrijven:

$$V = \{v(x) \mid v(\beta_1) = v(\beta_2) = \ldots = v(\beta_\ell) = 0\}$$

waarbij $\beta_1,\beta_2,\ldots,\beta_\ell$ n-de eenheidswortels zijn. De generator van V is nu het k.g.v. van de minimaalpolynomen van de β_j's. Omgekeerd, als $g(x)$ de generator is van een cyclische code V en $g(x) = \prod_{i\in J} f_i(x)$ $(J \subset \{1,\ldots,t\})$ en β_i is een nulpunt van $f_i(x)$ $(i\in J)$, dan is $V = \{v(x) \mid v(\beta_i) = 0$ voor iedere $i \in J\}$.

Als we β uit het uitbreidingslichaam $GF(q^m)$ kiezen, dan kan β opgevat worden als kolomvector $\underline{\beta}$ ter hoogte m over $GF(q)$ (uitgeschreven op een willekeurige basis). De eis $v(\beta) = 0$ wordt nu: $vH^T = 0$, met $H = (\underline{1}\ \underline{\beta}\ \underline{\beta}^2 \ldots \underline{\beta}^{n-1})$. Bij meer β's, krijgen we meer rijen in H. Deze hoeven overigens niet lineair onafhankelijk te zijn.

Als voorbeeld van een toepassing geven we de volgende stelling.

(5.3.1) <u>STELLING</u>. *Zij* $n = \frac{q^m-1}{q-1}$ *en zij* β *een primitieve* n-*de eenheidswortel in een uitbreidingslichaam van* $GF(q)$. *Dan is de cyclische code* $V = \{v(x) \mid v(\beta) = 0\}$ *(equivalent met) de* $(n,n-m)$-*Hamming-code over* $GF(q)$ *als en slechts als* $(m,q-1) = 1$.

<u>GEVOLG</u>. *Iedere binaire Hamming-code is (equivalent met) een cyclische code.*

<u>BEWIJS VAN DE STELLING</u>

Als $\beta^1,\beta^2,\ldots,\beta^{n-1} \notin GF(q)$ (opgevat als deellichaam van $GF(q^m)$) dan zijn alle kolommen van $H = (\underline{1}\ \underline{\beta}\ \underline{\beta}^2 \ldots \underline{\beta}^{n-1})$ paarsgewijs lineair onafhankelijk en is H dus een parity-check-matrix voor een Hamming-code. Omgekeerd, als H een parity-check-matrix is voor een $(n,n-m)$-Hamming-code, dan zijn de kolommen van H paarsgewijs lineair onafhankelijk (want de code bevat geen woorden van gewicht 2) en dan:

$$\beta^1,\beta^2,\ldots,\beta^{n-1} \notin GF(q).$$

Nu geldt: $\beta^1,\beta^2,\ldots,\beta^{n-1} \notin GF(q) \Longleftrightarrow (m,q-1) = 1$.
Immers, $(m,q-1) = (n,q-1)$, want:

$$n = \frac{q^m-1}{q-1} = q^{m-1}+q^{m-2}+\ldots+1 = (q-1)(q^{m-2}+2q^{m-3}+\ldots+(m-1)) + m.$$

Verder zijn de volgende beweringen equivalent.

$\forall\ i \in \{1,\ldots,n-1\}$: $\beta^i \notin GF(q)$.

$\forall\ i \in \{1,\ldots,n-1\}$: $\beta^{i(q-1)} \neq 1$,

$\forall\ i \in \{1,\ldots,n-1\}$: $n \nmid i(q-1)$,

$(n,q-1) = (m,q-1) = 1$. □

5.4. DE IDEMPOTENT VAN EEN CYCLISCHE CODE

(5.4.1) STELLING. *Zij* V *een cyclische code. Dan bevat* V *een (uniek bepaald) codewoord* $c(x)$ *dat een eenheidselement is voor* V, *d.w.z. als* $v(x) \in V$, *dan* $c(x)v(x) = v(x)$.

BEWIJS. Zij $g(x)$ de generator en $h(x)$ het check-polynoom voor V (d.w.z. $g(x)h(x) = x^n-1$). Omdat x^n-1 geen meervoudige wortels heeft geldt $(g(x),h(x)) = 1$. Dus zijn er polynomen $a(x)$ en $b(x)$ zo dat $a(x)g(x) + b(x)h(x) = 1$. Definieer nu: $c(x) := a(x)g(x) = 1 - b(x)h(x)$. Als $v(x) = k(x)g(x)$ een codewoord in V is dan volgt:

$$c(x)v(x) = k(x)g(x) - k(x)g(x)b(x)h(x) = k(x)g(x) = v(x) \text{ in } R.$$

Dus $c(x)$ is inderdaad een eenheidselement in V en daarom uniek bepaald. □

In het bijzonder geldt: $c^2(x) = c(x)$; daarom heet $c(x)$ de *idempotent* van V. Ook geldt dat $c(x)$ de code genereert, omdat iedere $v(x) \in V$ een veelvoud van $c(x)$ is (want $v(x) = v(x)c(x)$).

5.5. BCH-CODES

Een klasse van cyclische codes vormen de zgn. BCH-codes, ontdekt door BOSE & RAY-CHAUDHURI en HOCQUENGHEM.

Zij $R = R^{(n)} = \mathbb{F}[x]/(x^n-1)$ en laat $(n,q) = 1$ en $\mathbb{F} = \mathbb{F}_q$. Zij m het kleinste positieve gehele getal zo dat $n \mid q^m-1$ en zij β een primitieve n-de eenheidswortel in $GF(q^m)$ (dit is het kleinste uitbreidingslichaam van $GF(q)$ met een primitieve n-de eenheidswortel). Zij $g(x)$ het k.g.v. van de

minimale polynomen van $\beta,\beta^2,\ldots,\beta^{d-1}$. Dan heet de cyclische code $R\,g(x)$ een *BCH-code* met *ontwerp-afstand* d. Dit is dus de code:

$$\{v(x) \mid v(\beta) = v(\beta^2) = \ldots = v(\beta^{d-1}) = 0\} \text{ (zoals in § 5.3).}$$

Als $n = q^m-1$ dan heet de code een *primitieve BCH-code*.

De minimum afstand van een BCH-code behoeft niet gelijk te zijn aan de ontwerp-afstand, maar kan niet kleiner zijn:

(5.5.1) STELLING. *De minimum afstand van een* BCH-*code met ontwerp-afstand* d *is ten minste* d.

BEWIJS. Definieer de $m(d-1) \times n$-matrix H als volgt:

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

Iedere β^i hierin stelt een kolom ter hoogte m voor als beschreven in § 5.3. Dan is $\underline{v} = (v_0,\ldots,v_{n-1})$ in de code als en alleen als $\underline{v}H^T = \underline{0}$. We bewijzen nu dat iedere d-1 kolommen lineair onafhankelijk zijn; dan heeft ieder codewoord $\underline{v} \neq \underline{0}$ een gewicht groter dan d-1.
Neem de kolommen met bovenaan resp. $\xi_1,\ldots,\xi_{d-1}$ (onderling verschillend).
Dan is de submatrix bestaande uit deze kolommen:

$$\begin{pmatrix} \xi_1 & \ldots & \xi_{d-1} \\ \xi_1^2 & \ldots & \xi_{d-1}^2 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \xi_1^{d-1} & \ldots & \xi_{d-1}^{d-1} \end{pmatrix}$$

Beschouwd als matrix over $GF(q^m)$ heeft deze Vandermonde-matrix als determinant:

$$\xi_1 \cdot \ldots \cdot \xi_{d-1} \cdot \prod_{i<j} (\xi_i - \xi_j) \neq 0.$$

Dus deze kolommen zijn lineair onafhankelijk als kolommen over $GF(q^m)$, dus ook als kolommen over $GF(q)$. $\square$

In het algemeen is het vinden van de feitelijke minimum afstand een moeilijk probleem. Niet altijd is de minimum afstand gelijk aan de ontwerp-afstand. Zij bijvoorbeeld $n = 31$, $m = 5$ $q = 2$ en $d = 8$. Zij β een primitieve n-de eenheidswortel in $GF(2^5)$. Dan hebben β, β^2, β^4, β^8 en β^{16} hetzelfde minimale polynoom. Evenzo hebben β^5, β^{10}, β^{20}, β^9, β^{18} hetzelfde minimale polynoom. Zij $g(x)$ het kleinste gemene veelvoud van de minimale polynomen van β, β^2, β^3, β^4, β^5, β^6, β^7. Dan is $\mathcal{R}g(x)$ de BCH-code met ontwerp-afstand 8. Maar ook is $g(x)$ het produkt (zonder faktor-herhaling) van de minimale polynomen van β, β^2, β^3, β^4, β^5, β^6, β^7, β^8, β^9, β^{10}; dus $\mathcal{R}g(x)$ is ook de BCH-code met ontwerp-afstand 11. D.w.z. de minimale afstand van de code is ten minste 11.

Men noemt (5.5.1) ook wel de BCH-*grens* voor de minimum afstand van een cyclische code. De stelling geldt onveranderd als de d-1 opeenvolgende machten van β niet bij β^1 beginnen. De volgende stelling van HARTMANN en TZENG (1972) is een uitbreiding.

(5.5.2) STELLING. *Zij* C *een cyclische code met woordlengte* n *over* $\mathbb{F}_q$ *en voortbrenger* $g(x)$. *Zij* β *een primitieve* n-*de eenheidswortel in* $GF(q^m)$. *Als* $(n,c_1) = (n,c_2) = 1$ *en* $g(\beta^{\ell+i_1c_1+i_2c_2}) = 0$ $(i_1 = 0,1,\ldots,d_0-2;\ i_2 = 0,1,\ldots,s)$ *dan geldt voor de minimum afstand* d *van* C

$$d \geq d_0 + s.$$

BEWIJS. Volgens de BCH-grens is $d \geq d_0$. Zij $d_0 \leq w < d_0 + s$. Neem aan dat

$$v(x) := 1 + \sum_{i=1}^{w-1} Y_i\, x^{a_i}$$

een codewoord van gewicht w is $(Y_i \in \mathbb{F}_q\backslash\{0\},\ 1 \leq a_1 < a_2 < \ldots < n)$.
Zij $X_i := \beta^{a_i}$, $S_j := \sum_{i=1}^{w-1} Y_i X_i^j = -1 + v(\beta^j)$.

We definieren

$$\sigma_1(x) := \prod_{i_1=1}^{d_0-2} (x-X_{i_1}^{c_1}) = \sigma_0^{(1)} x^{d_0-2} + \sigma_1^{(1)} x^{d_0-3} + \ldots + \sigma_{d_0-3}^{(1)} x + \sigma_{d_0-2}^{(1)}$$

(met $\sigma_0^{(1)} = 1$), en

$$\sigma_2(x) := \prod_{i_2=d_0-1}^{w-1} (x-X_{i_2}^{c_2}) = \sigma_0^{(2)} x^{w-d_0+1} + \sigma_1^{(2)} x^{w-d_0} + \ldots + \sigma_{w-d_0}^{(2)} x + \sigma_{w-d_0+1}^{(2)}$$

(met $\sigma_0^{(2)} = 1$), en verder

$$\sigma(x) := \sigma_1(x)\sigma_2(x).$$

Daar $a_i \neq 0$, $(n,c_1) = (n,c_2) = 1$, is $X_i \neq 1$, $X_{i_1}^{c_1} \neq 1$ $(i_1=1,2,\ldots,d_0-2)$, $X_{i_2}^{c_2} \neq 1$ $(i_2=d_0-1,\ldots,w-1)$. Dus is $\sigma(1) \neq 0$. Nu is

$$(5.5.3) \qquad \sum_{j=0}^{w-d_0+1} \sigma_j^{(2)} \sum_{k=0}^{d_0-2} \sigma_k^{(1)} S_{\ell+(d_0-2-k)c_1+(w-d_0+1-j)c_2} = \sum_{i=1}^{w-1} Y_i X_i^{\ell} \sigma_1(X_i^{c_1})\sigma_2(X_i^{c_2}) = 0.$$

Uit de definitie van S_j en het gegeven volgt echter dat $S_{\ell+i_1c_1+i_2c_2} = -1$ voor $i_1 = 0,1,\ldots,d_0-2$ en $i_2 = 0,1,\ldots,s$. Dan staat in (5.5.3) echter $\sigma(1) = 0$, een tegenspraak. De aanname was dus onjuist. □

<u>VOORBEELD</u>. Zij $n = 51$, $g(x) := m_1(x)m_9(x)$. De nulpunten β^i van $g(x)$ hebben resp. $i = 1,2,4,8,16,32,13,26$ en $9,18,36,21,42,33,15,30$. De dimensie van de code is 35. Volgens (5.5.1) is $d \geq 3$. Volgens (5.5.2) is echter $d \geq 5$ omdat we met $i = 1,2,8,9,15,16$ blijkbaar $\ell = 1$, $c_1 = 1$, $c_2 = 7$ kunnen nemen in stelling (5.5.2).

5.6. EEN PROCEDURE VOOR HET CORRIGEREN VAN FOUTEN BIJ BCH-CODES

Stel dat een codewoord $C(x)$ van een BCH-code (met ontwerp-afstand $d \geq 2t + 1$, ter lengte n, over het lichaam $GF(q)$, en m en β als in § 5.5) wordt verzonden en een woord: $R(x) = R_0 + R_1x + \ldots + R_{n-1}x^{n-1}$ wordt ontvangen. Zij $E(x) = R(x) - C(x) = E_0 + E_1x + \ldots + E_{n-1}x^{n-1}$ het foutenpatroon. Definieer voorts:

$M := \{i \mid E_i \neq 0\}$, de verzameling posities waar een fout is gemaakt;

$e := |M|$, het aantal fouten;

$\sigma(z) := \prod_{i \in M} (1-\beta^i z)$; dit polynoom heet het "error-locator polynomial";

$$\omega(z) := \sum_{i \in M} E_i \beta^i z \prod_{j \in M \setminus i} (1-\beta^j z).$$

Kennelijk is kennis van $\sigma(z)$ en $\omega(z)$ voldoende om fouten te verbeteren:

als $\sigma(\beta^{-i}) \neq 0$, dan is op de i-plaats geen fout gemaakt;

als $\sigma(\beta^{-i}) = 0$, dan is de fout $E_i = \dfrac{-\omega(\beta^{-i})}{\sigma'(\beta^{-i})} \cdot \beta^i$.

Natuurlijk kunnen we alleen voor $e \leq t$ verwachten dat $E(x)$ bepaald kan worden (en daarmee $C(x)$). Neem dus aan dat $e \leq t$, dan zal blijken hoe $E(x)$ gevonden kan worden m.b.v. relatief eenvoudige operaties (het oplossen van een stelsel lineaire vergelijkingen over $GF(q)$).

We berekenen hiertoe:

$$\frac{\omega(z)}{\sigma(z)} = \sum_{i \in M} \frac{E_i \beta^i z}{1-\beta^i z} = \sum_{i \in M} E_i \sum_{\ell=1}^{\infty} (\beta^i z)^\ell = \sum_{\ell=1}^{\infty} z^\ell \sum_{i \in M} E_i \beta^{\ell i} =$$

$$= \sum_{\ell=1}^{\infty} z^\ell E(\beta^\ell).$$

Voor $1 \leq \ell \leq 2t$ is $E(\beta^\ell) = R(\beta^\ell)$, dus aan de ontvanger van het codewoord bekend. D.w.z. $\frac{\omega(z)}{\sigma(z)}$ is bekend modulo z^{2t+1}. De kunst is nu om polynomen $\sigma(z)$ en $\omega(z)$ met graad $\omega(z) \leq$ graad $\sigma(z)$ en graad $\sigma(z)$ minimaal te vinden, zó dat:

$$\frac{\omega(z)}{\sigma(z)} = \sum_{\ell=1}^{2t} z^\ell R(\beta^\ell) \pmod{z^{2t+1}}.$$

Zij $S_\ell = E(\beta^\ell) = R(\beta^\ell)$ voor $\ell = 1,\ldots,2t$, en zij $\sigma(z) = \sum_{i=0}^{e} \sigma_i z^i$. Dan is:

$$\omega(z) = (\sum_{\ell=1}^{2t} z^\ell S_\ell)(\sum_{i=0}^{e} \sigma_i z^i) = \sum_k z^k (\sum_{i+\ell=k} S_\ell \sigma_i) \qquad (\mathrm{mod}\ z^{2t+1}).$$

Daar $\omega(z)$ de graad e heeft, volgt:
$\sum_{i+\ell=k} S_\ell \sigma_i = 0$ voor $e + 1 \le k \le 2t$. Dit zijn 2t-e vergelijkingen voor de e onbekenden $\sigma_1,\ldots,\sigma_e$ (want $\sigma_0 = 1$ is bekend). Als $e \le t$ dan heeft dit stelsel hooguit één oplossing: stel $\tilde{\sigma}(z) = \sum_{i=0}^{e} \tilde{\sigma}_i z^i$ is een oplossing (met $\tilde{\sigma}_0 = 1$); dan volgt voor $e + 1 \le k \le 2t$:

$$0 = \sum_\ell S_{k-\ell}\tilde{\sigma}_\ell = \sum_{i\in M} \sum_\ell E_i\ \beta^{i(k-\ell)}\tilde{\sigma}_\ell = \sum_{i\in M} E_i \beta^{ik}\tilde{\sigma}(\beta^{-i}).$$

Dit zijn 2t-e vergelijkingen voor de e onbekenden $E_i\tilde{\sigma}(\beta^{-i})$. Vanwege Vandermonde is de oplossing uniek, d.w.z. $\forall\ i \in M$ geldt: $E_i\tilde{\sigma}(\beta^{-i}) = 0$. Nu is $E_i \neq 0$, d.w.z. $\tilde{\sigma}(x)$ heeft als nulpunten: $\beta^{-i}(i\in M)$; dus $\tilde{\tilde{\sigma}} = \sigma$.
Dus als we polynomen $\omega(z)$ en $\sigma(z)$ van zo laag mogelijke graad gevonden hebben, dan zijn dit de gevraagde $\omega(z)$ en $\sigma(z)$.

5.7. REED-SOLOMON CODES

Een *Reed-Solomon code* of *RS-code* is een primitieve BCH-code waarbij $m = 1$, $n = q-1$. De code wordt voortgebracht door het polynoom $g(x) = \prod_{i=1}^{d-1} (x-\alpha^i)$ uit $GF(q)[x]$. Op grond van (5.5.1) is de minimum afstand van de code ten minste d. De code heeft dimensie $k = n-d+1$ en dus op grond van (4.3.2) een minimum afstand ten hoogste d. We zien dus dat d de minimum afstand is en dat de code optimaal is (vgl. (4.1.1)).

De RS-codes worden o.a. gebruikt voor de verbetering van zgn. "burst-errors", dat zijn intervallen uit de ontvangen rij symbolen met veel fouten er in (veroorzaakt door een storing op het kanaal). Een RS-code met $q = 2^r$ kunnen we opvatten als binaire code met woordlengte $r(2^r-1)$ en dimensie rk. Als een burst-error fouten veroorzaakt op een traject ter lengte $b \le ([d/2]-1)r + 1$ dan worden van de oorspronkelijke RS-code niet meer dan $[d/2]$ symbolen veranderd. De fout kan dus gecorrigeerd worden. Dezelfde gedachte is de basis van de zgn. *concatenated codes* (cf. Hfdst. IX).

5.8. KWADRAATREST-CODES

Zij n een oneven priemgetal, zódat q een kwadraatrest modulo n is, d.w.z. $\exists x: x^2 \equiv q \pmod{n}$. Dit is hetzelfde als: $q^{\frac{1}{2}(n-1)} \equiv 1 \pmod{n}$ (zie § 0.2). Zij α een primitieve n-de eenheidswortel in een uitbreidingslichaam van GF(q). Zij R_0 de verzameling van alle kwadraatresten modulo n:

$$R_0 = \{x^2 | x \in GF(n)\setminus\{0\}\},$$

en R_1 de verzameling van alle niet-kwadraatresten modulo n:

$$R_1 = GF(n)\setminus\{0\}\setminus R_0.$$

Definieer verder:

$$g_0(x) := \prod_{r \in R_0} (x-\alpha^r) \text{ en } g_1(x) := \prod_{r \in R_1} (x-\alpha^r).$$

Dan geldt:

$$x^n-1 = (x-1)g_0(x)g_1(x), \text{ en } g_0(x),\ g_1(x) \in GF(q)[x].$$

Merk op dat de eis dat q een kwadraatrest modulo n is equivalent is met de eis dat g_0 en g_1 polynomen over GF(q) zijn.

(5.8.1) <u>DEFINITIE</u>. De cyclische codes van lengte n over GF(q) met generatoren $g_0(x)$ en $(x-1)g_0(x)$ heten *kwadraatrest-codes* of *QR-codes*. De verlengde *QR-code* van lengte n+1 over GF(q) wordt verkregen door aan de code met generator $g_0(x)$ een extra parity-check symbool toe te voegen (zie (3.4.3)).

De code met generator $(x-1)g_0(x)$ bestaat uit alle woorden $(v_0,\ldots,v_{n-1})$ uit de code met generator $g_0(x)$ waarvoor geldt: $v_0+\ldots+v_{n-1} = 0$.
Door in de definitie g_0 door g_1 te vervangen krijgen we codes equivalent met de oorspronkelijke. Want zij j een niet-kwadraatrest modulo n. Dan definieert:

$$\pi_j(\ell) := j\ell \pmod{n},\ 0 \le \pi_j(\ell) < n,$$

een permutatie op $\{0,\ldots,n-1\} = GF(n)$, en dus ook een permutatie op de posities van de codewoorden in $R^{(n)}$. Laat $\pi_j c(x)$ het codewoord zijn dat door deze permutatie uit $c(x)$ ontstaat. Aangezien:

$$c(\alpha^r) = \sum_{i=0}^{n-1} c_i \alpha^{ri} = \sum_{i=0}^{n-1} c_{\pi_j(i)} \alpha^{r\pi_j(i)} = \sum_{i=0}^{n-1} c_{\pi_j(i)} \alpha^{rji} = \pi_j^{-1} c(\alpha^{rj}),$$

en: $R_0 = jR_1$, zijn de volgende beweringen equivalent:

$$c(x) \in Rg_0(x);\ \forall r \in R_0 : c(\alpha^r) = 0;\ \forall r \in R_0 : \pi_j c(\alpha^{rj}) = 0;$$

$$\forall r \in R_1 : \pi_j c(\alpha^r) = 0;\ \pi_j c(x) \in Rg_1(x).$$

Evenzo:

$$c(x) \in R(x-1)g_0(x) \Leftrightarrow \pi_j c(x) \in R(x-1)g_1(x).$$

Over de gewichten van de woorden kan het volgende gezegd worden.

(5.8.2) <u>STELLING</u>. *Zij* $c(x)$ *een codewoord van* $Rg_0(x)$, *zo dat* $c(x) \notin R\cdot(x-1)g_0(x)$. *Zij* d *het gewicht van* $c(x)$. *Dan:*

(i) $d^2 \geq n$;

(ii) *als* $n \equiv -1 \pmod 4$, *dan* $d^2-d+1 \geq n$;

(iii) *als* $n \equiv -1 \pmod 8$, *en* $q = 2$, *dan* $d \equiv 3 \pmod 4$.

<u>BEWIJS</u>.

(i) Omdat $c(x) \in R\, g_0(x) \backslash R\, (x-1)g_0(x)$, geldt ook:

$$\pi_j c(x) \in R\, g_1(x) \backslash R\, (x-1)g_1(x).$$

Dan:

$$g_0(x)g_1(x) \mid c(x)\pi_j c(x), \text{ en } (x-1) \nmid c(x)\pi_j c(x).$$

Dus:

$$c(x)\cdot\pi_j c(x) = m(1+x+\ldots+x^{n-1}) \pmod{x^n-1} \text{ voor zekere } m \in GF(q).$$

Maar dan:

$$d^2 = (w(c(x)))^2 = w(c(x))\cdot w(\pi_j c(x)) \geq w(c(x)\pi_j c(x)) = n.$$

(ii) als $n \equiv -1 \pmod 4$ dan is -1 een niet-kwadraatrest, dus dan kunnen we $j = -1$ nemen. Maar dan dragen in het produkt $c(x)\pi_j c(x)$ de termen x en x^{-1}, resp. x^2 en x^{-2},..., resp. x^{n-1} en x^{-n+1}, alle bij tot dezelfde term. Dus dan:

$$w(c(x)\pi_j c(x)) \leq w(c(x))\cdot w(\pi_{-1} c(x)) - d+1.$$

(iii) Zij $c(x) = \sum_{i=1}^{d} x^{e_i}$. Dan
$c(x)\pi_{-1}c(x) = d + \sum_{i\neq j} x^{e_i-e_j}$. Als $e_i-e_j = e_k-e_\ell$ dan vallen de twee termen $x^{e_i-e_j}$ en $x^{e_k-e_\ell}$ tegen elkaar weg. Maar dan vallen ook $x^{e_j-e_i}$ en $x^{e_\ell-e_k}$ tegen elkaar weg. Dus het aantal wegvallende termen is een viervoud, zeg 4b.

Dan:

$d^2-d+1-4b = n$, of: $d \equiv 3 \pmod 4$ (d is oneven, omdat $c(x) \notin R\,(x-1)g_0(x)$). □

Het kan bewezen worden dat elke verlengde binaire QR-code met woordlengte $n + 1$ en posities geindiceerd met $PG(1,n) = \mathbb{F}_n \cup \{\infty\}$ invariant is onder de werking op de posities van de 2-voudig transitieve groep $PSL(2,n) := \{x \mapsto \frac{ax+b}{cx+d} \mid ad-bc = 1\}$ (zie VAN LINT 1971)). Hieruit volgt eenvoudig dat een binaire QR-code oneven minimum gewicht heeft, zodat de bovenstaande stelling gebruikt kan worden om ondergrenzen voor de minimum afstand van een QR-code te vinden.

<u>VOORBEELDEN</u>

(5.8.3) Neem $q = 2$, $n = 7$ en generator $g_0(x)$ (zodat $k = 4$). Stelling (5.8.2) levert $d \geq 3$ maar $(1+7)\cdot 2^4 = 2^7$ dus de QR-code met deze parameters is 1-perfect. (In feite is het natuurlijk de (7,4)-Hamming code, zie § 2.1 en § 2.4).

In dit voorbeeld was $g(x) = x + x^2 + x^4$ en $h(x) = 1 + x + x^2 + x^4 = 1 + g(x)$. Dit verschijnsel is algemeen in het binaire geval:

Bekijk $g(x) = \sum_{r\in R_0} x^2$. Er geldt $g(x^i) = g(x) \pmod{x^n-1}$ als $i \in R_0$, en in het bijzonder $g(x)^2 = g(x) \pmod{x^n-1}$. Voorts is voor $j \in R_1$: $g(x^j) + g(x) = \sum_{r=1}^{n-1} x^r \pmod{x^n-1}$. Als dus α een primitieve n-de eenheidswortel is (in een uitbreidingslichaam van GF(2)) dan is $g(\alpha^i) \in GF(2)$ en de afbeelding $i \mapsto g(\alpha^i)$ is constant op R_0 en op R_1 d.w.z. òf $g_0(x)|g(x)$ òf $g_1(x)|g(x)$. Bij passende keuze van α volgt $g_0(x)|g(x)$ zodat $g(x)$ een idempotent van de code $\mathcal{R}g_0(x)$ is. Aangezien $x^n-1 = (x-1)g_0(x)g_1(x)$ en $(g_1(x),g(x)) = 1$ is de cyclische code met generator $g(x)$ òf $\mathcal{R}g_0(x)$ òf $\mathcal{R}g_0(x)(x-1)$. Nu is $g(1) = \frac{n-1}{2}$ dus het eerste geval treedt op als $n \equiv -1 \pmod 8$ en het tweede als $n \equiv 1 \pmod 8$. [Merk op dat de eis dat 2 een kwadraatrest mod n is impliceert dat $n \equiv \pm 1 \pmod 8$.] Tenslotte volgt $g(x)\cdot(1+g(x)) = 0 \pmod{x^n-1}$ zodat $h(x) = 1 + g(x)$.

(5.8.4) Neem $q = 2$, $n = 23$ en generator $g_0(x)$ (zodat $k = 12$). Stelling (5.8.2) levert tezamen met de wetenschap dat d oneven is dat $d \geq 7$. Echter $(1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3})\cdot 2^{12} = 2^{23}$ dus de QR-code met deze parameters is 3-perfect. (In feite is het natuurlijk de (23,12)-binaire Golay code, zie § 2.3.)

(5.8.5) Neem $q = 3$, $n = 11$ en generator $g_0(x)$ (zodat $k = 6$). Nu vinden we de 2-perfecte (11,6)-ternaire Golay code (zie § 2.4).

Deze voorbeelden zouden de indruk kunnen wekken dat alle QR-codes perfect zijn, maar dat is natuurlijk geenszins het geval (zie opgave (5.10.5)); algemeen geldt dat QR-codes vaak goed zijn, maar moeilijk te decoderen.

5.9. COMMENTAAR

Het idee van cyclische codes kan gegeneraliseerd worden. Men kan bijvoorbeeld bij vaste ξ eisen dat met $(a_0,a_1,\ldots,a_{n-1})$ uit C ook $(\xi a_{n-1},a_0,a_1,\ldots,a_{n-2})$ in de code zit. Men noemt zo'n code *constacyclisch* (als $\xi = -1$ ook wel *negacyclisch*). De theorie is geheel analoog (zie BERLEKAMP (1968)). Voor een toepassing van idempotenten verwijzen we naar VAN LINT (1971) § 3.3. De procedure uit § 5.6 is een generalisatie van een door BERLEKAMP bedacht algorithme dat reeds practische toepassing vindt.

Voor meer theorie over QR-codes en diverse toepassingen in de combi-

natoriek verwijzen we naar CAMERON & VAN LINT (1975) en de twee hierboven genoemde boeken.

5.10. OPGAVEN

(5.10.1) Construeer een ternaire BCH-code met lengte 26 en ontwerp-afstand 5.

(5.10.2) Bepaal de idempotent van de (15,11)-Hamming code.

(5.10.3) Zij α een primitief element van $GF(2^5)$ met $\alpha^5 = \alpha^2 + 1$. Bij gebruik van een BCH-code met ontwerp afstand 5 ontvangen we

$$(1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1)$$

Bepaal met de algorithme van 5.6 het verzonden codewoord.

(5.10.4) Bepaal de ternaire QR-code met lengte 11 en toon aan dat dit een perfecte code is! Laat zien dat deze code equivalent is met de in § 2.4 geconstrueerde.

(5.10.5) Behalve de onder (5.8.3) - (5.8.5) genoemde QR-codes is er nog een perfecte QR-code. Welke?

(5.10.6) Zij $n = 4$, $q = 5$, $d = 3$. Kies $\alpha = 2$ als primitief element van $GF(5)$. Construeer de RS-code C met minimum afstand d voor deze parameters. Bewijs dat de matrices A en B gedefinieerd door $(i,j,a_{ij},b_{ij}) \in C$ orthogonale latijnse vierkanten zijn.

(5.10.7) Generaliseer de resultaten uit § 5.8 zoveel mogelijk tot e-de graads resten; de voorwaarden worden nu: n priem, $e|n-1$, $q^{\frac{n-1}{e}} \equiv 1 \pmod{n}$.

(a) Bewijs als generalisatie van (5.8.2) (i) dat $d^e > n$.

(b) Bepaal de generator en de minimum afstand van de binaire kubische rest code voor $n = 31$.

(5.10.8) Bepaal de minimum afstand van de binaire kwadraatrest code met $n = 47$.

(5.10.9) Zij m oneven, $n = 2^m-1$, α primitief element van $GF(2^m)$. Zij $g(x)$ een deler van x^n-1 en $g(\alpha) = g(\alpha^5) = 0$. Bewijs dat de cyclische

code voortgebracht door $g(x)$ minimum afstand ≥ 4 heeft en wel

(a) door aan te tonen dat $1 + \xi + \eta = 0$ en $1 + \xi^5 + \eta^5 = 0$ met ξ en η in $GF(2^m)$ niet mogelijk is.

(b) door toepassing van een stelling.

(5.10.10) Zij C een BCH-code met ontwerpafstand d. Bewijs dat de minimum afstand van de verlengde code $\overline{C}$ tenminste $d + 1$ is.

Hoofdstuk VI

REED-MULLER CODES EN DE STELLING VAN CHEVALLEY

In dit hoofdstuk beschrijven we een klasse van codes die zowel practisch als theoretisch van belang zijn. Als introductie beschouwen we binaire *Reed-Muller codes* (= RM-codes), welke zich o.a. zeer goed met behulp van eindige affiene meetkunde laten beschrijven. De decodering van deze codes is een mooi voorbeeld van threshold decoding. Daarna zullen we aantonen dat de bepaling van het minimale gewicht van algemene RM-codes leidt tot een nieuw bewijs voor de bekende stelling van CHEVALLEY (1936) over nulpunten van polynomen en tot generalisaties van deze stelling.

6.1. VOORBEREIDINGEN

We zullen bij de beschrijving van RM-codes gebruik maken van de volgende stelling van LUCAS (1878), (zie DICKSON (1952)).

(6.1.1) STELLING. *Zij* p *een priemgetal. Laten*

$$n = \sum_{i=0}^{\ell} n_i p^i \quad \textit{en} \quad k = \sum_{i=0}^{\ell} k_i p^i$$

p-tallige representaties van n *en* k *zijn.*
Dan is

$$\binom{n}{k} \equiv \prod_{i=0}^{\ell} \binom{n_i}{k_i} \pmod{p}.$$

BEWIJS: Zoals bekend is

$$(1+x)^p \equiv 1 + x^p \pmod{p}.$$

Dus is, met $0 \le r < p$,

$$(1+x)^{ap+r} \equiv (1+x^p)^a (1+x)^r. \pmod{p}.$$

Bepalen we in beide leden de coefficient van x^{bp+s} waarbij $0 \le s < p$, dan vinden we

$$\binom{ap+r}{bp+s} \equiv \binom{a}{b}\binom{r}{s} \pmod{p}.$$

Hieruit volgt het gestelde met volledige inductie. □

Zij $q = 2^r$. We beschouwen $GF(q)[x]$. Is $P(x)$ een polynoom uit deze ring dan definieren we het Hamming gewicht $w(P(x))$ van dit polynoom als het aantal coefficienten $\neq 0$ in de ontwikkeling van $P(x)$. Zij $c \in GF(q)$, $c \neq 0$. De polynomen $(x+c)^i$, $i \geq 0$, vormen een basis van $GF(q)[x]$.

(6.1.2) <u>STELLING</u>. (MASSEY et al (1973)). *Zij* $P(x) = \sum_{i=0}^{\ell} b_i (x+c)^i$ *waarbij* $b_\ell \neq 0$ *en laat* i_0 *de kleinste index* i *zijn waarvoor* $b_i \neq 0$. *Dan is*

$$w(P(x)) \geq w((x+c)^{i_0}).$$

<u>BEWIJS</u>: Voor $\ell = 0$ is het gestelde eenvoudig te controleren. We gebruiken volledige inductie. Laat de stelling juist zijn voor $\ell < 2^n$. Neem nu aan dat $2^n \leq \ell < 2^{n+1}$. Dan is

$$P(x) = \sum_{i=0}^{2^n-1} b_i (x+c)^i + \sum_{i=2^n}^{\ell} b_i (x+c)^i =$$

$$= P_1(x) + (x+c)^{2^n} P_2(x)$$

$$= (P_1(x) + c^{2^n} P_2(x)) + x^{2^n} P_2(x);$$

waarbij $P_1(x)$ en $P_2(x)$ polynomen zijn waarvoor de stelling geldt. We onderscheiden 2 gevallen.

(i) Als $P_1(x) = 0$ dan is

$$w(P(x)) = w((x^{2^n}+c^{2^n})P_2(x)) = 2\, w(P_2(x))$$

en evenzo daar $i_0 \geq 2^n$

$$w((x+c)^{i_0}) = w((x^{2^n}+c^{2^n})(x+c)^{i_0-2^n}) = 2\, w((x+c)^{i_0-2^n})$$

waaruit het gestelde volgt.

(ii) Als $P_1(x) \neq 0$ dan staat tegenover iedere term uit $c^{2^n} P_2(x)$ die tegen een term van $P_1(x)$ wegvalt een term uit $x^{2^n} P_2(x)$ die niet wegvalt. Dus is $w(P(x)) \geq w(P_1(x))$ en dan volgt het gestelde uit de inductieonderstelling. □

We beschouwen nu de m-dimensionale affiene ruimte over GF(2) (notatie: AG(m,2)). De punten van deze ruimte geven we aan als kolomvectoren. De standaardbasis noemen we $\underline{u}_0,\ldots,\underline{u}_{m-1}$. Zij $j = \sum_{i=0}^{m-1} \xi_{ij}\, 2^i$ de 2-tallige schrijfwijze van j, $\underline{x}_j := \sum_{i=0}^{m-1} \xi_{ij}\, \underline{u}_i$, en laat E de matrix zijn met als kolommen $\underline{x}_j$ $(j=0,1,\ldots,2^m-1)$. Zij $n := 2^m$. Dan is de m bij n matrix E een lijst van de punten van AG(m,2).

(6.1.3) <u>DEFINITIES:</u>

(i) $A_i := \{\underline{x}_j \in AG(m,2) \mid \xi_{ij}=1\}$, dat is een (m-1)-dimensionale affiene deelruimte $(i=0,1,\ldots,m-1)$;

(ii) $\underline{v}_i :=$ de i-de rij van E, dat is de karakteristieke functie van A_i $(i=0,\ldots,m-1)$;
$\underline{1} := (1,1,\ldots,1)$, de karakteristieke functie van AG(m,2).

(iii) Als $\underline{a} = (a_0,a_1,\ldots,a_{n-1})$ en $\underline{b} = (b_0,b_1,\ldots,b_{n-1})$ dan $\underline{a}\,\underline{b} := (a_0b_0,a_1b_1,\ldots,a_{n-1}b_{n-1})$.

(iv) Is $S \subset \{0,1,\ldots,m-1\}$ dan definieren we

$$C(S) := \{j = \sum_{i=0}^{m-1} \xi_{ij}\, 2^i \mid i \notin S \Rightarrow \xi_{ij} = 0 \ (0 \leq i \leq m-1)\}.$$

(6.1.4) <u>LEMMA</u>: *Zij* $\ell = \sum_{i=0}^{m-1} \xi_{i\ell}\, 2^i$ *en laten* $i_1,\ldots,i_s$ *de waarden van* i *zijn waarvoor* $\xi_{i\ell} = 0$. *Als*

$$\underline{v}_{i_1}\, \underline{v}_{i_2} \cdots \underline{v}_{i_s} = (a_{\ell,0}, a_{\ell,1}, \ldots, a_{\ell,n-1})$$

dan is

$$(x+1)^{\ell} = \sum_{j=0}^{n-1} a_{\ell,j}\, x^{n-1-j}.$$

(waarbij een leeg product (s=0) zoals gebruikelijk gelezen moet worden als $\underline{1}$).

BEWIJS. Volgens Stelling (6.1.1) is $\binom{\ell}{n-1-j} = 1$ dan en slechts dan als voor iedere i met $\xi_{i\ell} = 0$ geldt $\xi_{ij} = 1$. Volgens (6.1.3) (i), (ii), (iii) is ook $a_{\ell,j} = 1$ dan en slechts dan als $\xi_{ij} = 1$ voor $i = i_1,\ldots,i_s$. □

We maken nog enkele opmerkingen over de meetkundige betekenis van de producten der vectoren $\underline{v}_i$ in de vorm van een lemma.

(6.1.5) LEMMA: *Als* $i_1,\ldots,i_s$ *verschillend zijn dan is*

(i) $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ *de karakteristieke functie van de affiene deelruimte* $A_{i_1} \cap A_{i_2} \cap\ldots\cap A_{i_s}$,

(ii) *het gewicht* $w(\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s})$ *van de vector* $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ *uit de n-dimensionale ruimte* $R^{(n)}$ *over* GF(2) *is* 2^{m-s},

(iii) *de karakteristieke functie van* $\{\underline{x}_j\}$ *is de j-de basisvector* $\underline{e}_j$ *van* $R^{(n)}$, *en*

$$\underline{e}_j = \prod_{i=0}^{m-1} \{\underline{v}_i + (1+\xi_{ij})\underline{1}\},$$

(iv) *alle producten* $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ $(0 \le s \le m)$ *vormen een basis van* $R^{(n)}$.

BEWIJS:

(i) direct gevolg van (6.1.3) (i) t/m (iii).

(ii) $A_{i_1} \cap A_{i_2} \cap\ldots\cap A_{i_s}$ is een (m-s)-dimensionale affiene deelruimte van AG(m,2) en bevat dus 2^{m-s} punten.

(iii) Beschouw de matrix E. Als $\xi_{ij} = 0$ vervangen we de i-de rij (dus $\underline{v}_i$) door de complementaire rij $\underline{1} + \underline{v}_i$. Vermenigvuldigen we daarna alle rijen dan heeft de productvector een 1 op plaats j en verder nergens.

(iv) volgt uit (iii) daar er precies n producten $\underline{v}_{i_1}\ldots\underline{v}_{i_s}$ zijn. Het volgt ook uit Lemma (6.1.4) daar de polynomen $(x+1)^{\ell}$ onafhankelijk zijn. □

De volgende tabel voor m = 4, n = 16 illustreert het bovenstaande.

$\underline{v}_{i_1}\ \underline{v}_{i_2}\cdots\underline{v}_{i_s}$	Coordinaten = coeff. van $(x+1)^{\ell}$	$\ell = n-1-\sum 2^{i_s}$
$\underline{1}$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	15 = 1111
$\underline{v}_0$	0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1	14 = 1110
$\underline{v}_1$	0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1	13 = 1101
$\underline{v}_2$	0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1	11 = 1011
$\underline{v}_3$	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1	7 = 0111
$\underline{v}_0\ \underline{v}_1$	0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1	12 = 1100
$\underline{v}_0\ \underline{v}_2$	0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1	10 = 1010
$\underline{v}_0\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1	6 = 0110
$\underline{v}_1\ \underline{v}_2$	0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 1	9 = 1001
$\underline{v}_1\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1	5 = 0101
$\underline{v}_2\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1	3 = 0011
$\underline{v}_0\ \underline{v}_1\ \underline{v}_2$	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1	8 = 1000
$\underline{v}_0\ \underline{v}_1\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1	4 = 0100
$\underline{v}_0\ \underline{v}_2\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1	2 = 0010
$\underline{v}_1\ \underline{v}_2\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1	1 = 0001
$\underline{v}_0\ \underline{v}_1\ \underline{v}_2\ \underline{v}_3$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	0 = 0000

Zo komt $\underline{v}_0\underline{v}_2$ volgens Lemma 6.1.4 overeen met $\ell = 15 - 2^0-2^2 = 10$ en $(x+1)^{10} = x^{10} + x^8 + x^2 + 1$.

6.2. BINAIRE REED-MULLER CODES

(6.2.1) <u>DEFINITIE</u>: Zij $0 \le r \le m-1$. De lineaire code met woordlengte $n = 2^m$ en als basisvectoren alle producten $\underline{v}_{i_1}\underline{v}_{i_2}\cdots\underline{v}_{i_s}$ met $0 \le s \le r$ en $0 \le i_j < m$ voor $j = 1,\ldots,s$ heet de RM-code van lengte 2^m en <u>orde</u> r.

In het bijzonder is de RM-code van orde 0 de repetitiecode met als basis $\underline{1}$.

(6.2.2) STELLING: *De* RM *code van lengte* 2^m *en orde* r *heeft minimum afstand* 2^{m-r}.

<u>BEWIJS</u>: Uit (6.2.1) en (6.1.5) (ii) volgt dat de minimum afstand ten hoogste 2^{m-r} is. Uit (6.1.4) en (6.1.2) volgt dan dat de minimum afstand ook niet minder is. □

(6.2.3) STELLING: *De duale code van de* RM-*code van lengte* 2^m *en orde* r *is de* RM-*code van lengte* 2^m *en orde* m-r-1.

BEWIJS: (a) De dimensie van de RM-code van lengte 2^m en orde r is $k = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$. De dimensie van de RM-code van lengte 2^m en orde m-r-1 is dan n - k.

(b) Als $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ en $\underline{v}_{j_1}\underline{v}_{j_2}\ldots\underline{v}_{j_t}$ basisvectoren van deze twee codes zijn is $s + t \leq m - 1$. Het product van deze twee basisvectoren heeft dus volgens (6.1.5) (ii) even gewicht. Dit betekent dat de vectoren $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ en $\underline{v}_{j_1}\underline{v}_{j_2}\ldots\underline{v}_{j_t}$ inproduct 0 hebben.

Uit (a) en (b) volgt het gestelde. □

GEVOLG: *De* (n,n-m-1) *verlengde Hamming code is de* RM-*code van lengte* 2^m *en orde* m-2.

(6.2.4) STELLING: *Zij* C *de* RM-*code van lengte* 2^m *en orde* m-ℓ. *Zij* A *een* ℓ-*dimensionale affiene deelruimte van* AG(m,2). *Dan is de karakteristieke functie van* A *een codewoord van* C.

BEWIJS: Zij $\underline{f} = \sum_{j=0}^{n-1} f_j\,\underline{e}_j$ de karakteristieke functie van A. Volgens (6.1.3) (iv) en (6.1.5) (iii) is

$$\underline{e}_j = \sum_{s=0}^{m} \sum_{\substack{(i_1,\ldots,i_s) \\ j\in C(i_1,\ldots i_s)}} \underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$$

zodat

$$\underline{f} = \sum_{s=0}^{m} \sum_{(i_1,i_2,\ldots,i_s)} \left(\sum_{j\in C(i_1,\ldots,i_s)} f_j\right) \underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}.$$

De binnenste som telt het aantal punten uit de doorsnede van A met de s-dimensionale affiene deelruimte

$$L := \{\underline{x}_j \in AG(m,2) \mid j \in C(i_1,\ldots,i_s)\}.$$

Voor $s > m-\ell$ is $L \cap A$ leeg of een affiene deelruimte van positieve dimensie. In beide gevallen is $|L \cap A|$ even, d.w.z. de coefficient van $\underline{v}_{i_1}\underline{v}_{i_2}\ldots\underline{v}_{i_s}$ is 0. □

(6.2.5) STELLING: *Binaire* RM-*codes zijn equivalent met verlengde cyclische codes.*

BEWIJS: Laat uit E de 0-de kolom weg. De overige kolommen zijn op te vatten als de elementen $\neq 0$ uit $GF(2^m)$. Dit is t.a.v. vermenigvuldiging een cyclische groep met voortbrenger ξ, een primitief element van $GF(2^m)$. De afbeelding $\alpha : GF(2^m) \to GF(2^m)$ gedefinieerd door $\alpha(x) = \xi x$ is kennelijk een niet-singuliere lineaire afbeelding van AG(m,2) in zichzelf. Verder is α, opgevat als permutatie van $AG(m,2)\setminus\{\underline{0}\}$ van de orde n-1. Iedere affiene deelruimte van AG(m,2) wordt door α afgebeeld op een affiene deelruimte van dezelfde dimensie. Het gestelde volgt nu uit (6.1.5) (i), (6.2.1) en (6.2.4). □

(6.2.6) STELLING: *De groep* G *van affiene transformaties van* AG(m,2) *is een groep van automorfismen van elke* RM-*code van lengte* 2^m.

BEWIJS. De transformaties van AG(m,2) komen overeen met permutaties van de symbolen van codewoorden. Evenals in (6.2.5) volgt het gestelde onmiddelijk uit het feit dat $(a_0,a_1,\ldots,a_{n-1})$ dan en slechts dan een codewoord van een RM-code van lengte 2^m en orde r is als het een lineaire combinatie is van karakteristieke functies van affiene deelruimten van dimensie $\geq m-r$. Deze zijn invariant onder G. □

We merken nog op dat G een drievoudig transitieve groep is; dat wil zeggen, dat ieder drietal punten in ieder ander drietal punten wordt overgevoerd door een element van G [omdat over een lichaam van karakteristiek 2 twee vectoren lineair onafhankelijk zijn zodra ze verschillend en ongelijk nul zijn].

We gaan nog kort in op een decodeerprocedure die voor deze codes gebruikt wordt. Beschouw een RM-code C van lengte 2^m en orde r. Volgens (6.2.3) en (6.2.4) is de karakteristieke functie van een (r+1)-dimensionale affiene deelruimte van AG(m,2) een parity-check vector voor C. Voor iedere r-dimensionale affiene deelruimte A van AG(m,2) zijn er $2^{m-r}-1$ verschillende (r+1)-dimensionale affiene deelruimten van AG(m,2) die A bevatten. Ieder punt niet in A ligt in precies één van deze deelruimten. Elk van deze (r+1)-dimensionale deelruimten bestaat uit de $|A|$ punten van A en evenveel andere

punten. Is a de som van de coordinaten van een codewoord op de plaatsen van A dan is de som van de coordinaten op het andere $|A|$-tal plaatsen blijkbaar ook a. We berekenen nu de uitkomsten van de $2^{m-r}-1$ parity check vergelijkingen. Stel dat het aantal fouten in een ontvangen woord $\leq 2^{m-r-1}-1$ is. Stel nu dat t van de parity-check vergelijkingen een 1 geven.
Er zijn 2 verklaringen te geven:

(i) dat dit is veroorzaakt door een oneven aantal fouten op de plaatsen van A en $2^{m-r}-1-t$ keer gecompenseerd wordt door een oneven aantal fouten op de andere $|A|$ plaatsen van zo'n parity check vergelijking.

(ii) dat op de plaatsen van A geen fout (of een even aantal) is gemaakt maar dat in t van de parity check vergelijkingen op de andere helft een oneven aantal fouten is gemaakt. In geval (i) is het aantal fouten $\geq 2^{m-r}-t$ en in geval (ii) is het $\geq t$. Precies als bij de eerder behandelde drempeldecodering (§ 3.5) is de waarde van t bepalend voor de keuze tussen (i) en (ii). Op deze manier is voor iedere r-dimensionale affiene deelruimte A uit te maken of het ontvangen woord een oneven aantal fouten op de plaatsen van A bevat. Door een soort inductie procédé kunnen we in een aantal analoge stappen de fouten lokaliseren. Dit proces heet *"multistep majority decoding"*.

6.3. FUNCTIES EN POLYNOMEN OVER EINDIGE LICHAMEN

In het vervolg van dit hoofdstuk zullen we ons bezig houden met de generalisatie van de hiervoor voor $q = 2$ beschouwde Reed-Muller codes voor willekeurige q. Hierbij zullen we een tweetal beschrijvingen van de gegeneraliseerde Reed-Muller codes tegenkomen. De eerste beschrijving sluit aan op de meetkundige behandeling van het geval $q = 2$ in § 6.2. Bij de tweede beschrijving staat het feit dat de codes verlengde cyclische codes zijn centraal. Verder zal blijken dat de bepaling van het minimale gewicht van de gegeneraliseerde Reed-Muller codes ons in staat stelt een klassieke stelling uit de algebra nl. de stelling van CHEVALLEY (1936) en een verscherping: de stelling van WARNING (1936) als gevolg mee te nemen.

Voor een eindig lichaam k kan een polynoom f in $k[X]$ alle elementen van k als nulpunt hebben zonder dat alle coefficienten van f ook 0 zijn; zo geldt voor iedere $x \in \mathbb{F}_q$ dat $x^q-x = 0$ hetgeen impliceert dat het polynoom $X^q-X \in \mathbb{F}_q[X]$ een voorbeeld van zo'n polynoom is. We houden ons in deze paragraaf bezig met een generalisatie van deze situatie voor polynomen in

meer veranderlijken.

Zij V een m-dimensionale vectorruimte over $k = \mathbb{F}_q$ zodat $V \cong (k)^m$. Polynomen in $k[X_1,\ldots,X_m]$ laten zich op natuurlijke wijze opvatten als functies van V in k; bovendien is deze voor de hand liggende afbeelding E: $k[X_1,\ldots,X_m] \to k^V$ een homomorfisme van ringen. De kern J van deze afbeelding is een ideaal in $k[X_1,\ldots,X_m]$. Kennelijk geldt $f \in J$ als en alleen als E(f) identiek nul op V is.

Voorbeelden van functies in J zijn de polynomen $X_i^q - X_i$ $(i=1,\ldots,m)$. Deze functies brengen een ideaal voort dat we met I zullen aanduiden. Het is duidelijk dat modulo I ieder polynoom f in $k[X_1,\ldots,X_m]$ zich laat schrijven als een polynoom f^* dat de eigenschap heeft dat voor iedere i en ieder in f^* optredend monoom $X_1^{d_1}\ldots X_m^{d_m}$ de graad $d_i \leq q - 1$ is. Een dergelijk polynoom zullen we gereduceerd noemen en de verzameling gereduceerde polynomen duiden we aan met R.

(6.3.1) <u>STELLING</u>. $J \cap R = \{0\}$ *en* $I = J$. *Verder geldt* $R/J = k[X_1,\ldots,X_m]/J$.

<u>BEWIJS</u>: De bewering $J \cap R = \{0\}$ wordt bewezen met inductie naar m. Voor $m = 1$ is het duidelijk (een polynoom heeft niet meer nulpunten dan zijn graad). Voor het bewijs van de inductiestap ontwikkelen we een polynoom $f \in J \cap R$ naar machten van X_m:

$$f = f_0 + f_1X_m + f_2X_m^2 + \ldots + f_{q-1}X_m^{q-1},$$

waarbij de $f_i \in k[X_1,\ldots,X_{m-1}]$ gereduceerd zijn.

Voor vaste elementen $\alpha_1,\ldots,\alpha_{m-1} \in k$ geldt dat $f(\alpha_1,\ldots,\alpha_{m-1},X_m) \in$ $\in k[X_m]$ een gereduceerd polynoom is dat overal nul is. Dientengevolge geldt $f_j(\alpha_1,\ldots,\alpha_{m-1}) = 0$ voor $j = 0,\ldots,q-1$. Aangezien $\alpha_1,\ldots,\alpha_{m-1}$ willekeurig waren gekozen volgt nu met inductie dat alle f_j identiek nul zijn.

Het is duidelijk dat $I \subset J$. Beschouw derhalve het quotient J/I. Iedere restklasse in dit quotient bezit een gereduceerde representant maar dat kan alleen maar het nul polynoom zijn daar $J \cap R = \{0\}$. De derde bewering in de stelling volgt nu rechtstreeks. □

(6.3.2) <u>GEVOLG</u>: *De rij* $0 \to J \hookrightarrow k[X_1,\ldots,X_m] \xrightarrow{E} k^V \to 0$ *is exact (hetgeen wil zeggen dat* E *surjectief is en* J *als kern heeft).*

<u>BEWIJS 1</u>: (dimensies tellen). $k[X_1,\ldots,X_m]/J \cong R$. Het aantal verschillende gereduceerde monomen met coefficient 1 bedraagt q^m en dit is tevens de

dimensie van k^V. Omdat E als kern J heeft moet E dus wel surjectief zijn.

<u>BEWIJS 2</u>: (interpolatie). Zij $a_i \in k$. Dan heeft het polynoom

$$f_{a_i} = -\prod_{\substack{b\in k\\ b\neq a_i}} (X_i - b)$$

de eigenschap dat

$$f_{a_i}(a) = \begin{cases} 1 & \text{als } a = a_i, \\ 0 & \text{anders,} \end{cases}$$

(gebruik hierbij dat het product van alle elementen in $\mathbb{F}_q^*$ gelijk -1 is).
Voor $\underline{a} = (a_1,\ldots,a_m) \in V$ definiëren we

$$f_{\underline{a}} = \prod_{j=1}^{m} \left(-\prod_{\substack{b\in k\\ b\neq a_j}} (X_j - b)\right).$$

Kennelijk geldt

$$f_{\underline{a}}(\underline{b}) = \begin{cases} 1 & \text{als } \underline{a} = \underline{b}, \\ 0 & \text{anders.} \end{cases}$$

Het is bovendien duidelijk dat $f_{\underline{a}} \in R$. Schrijven we nu voor willekeurige $f \in k^V$ het polynoom

$$g = \sum_{\underline{a}\in V} f(\underline{a}).f_{\underline{a}} \in R$$

dan volgt direct dat $E(g) = f$ waarmee is aangetoond dat E surjectief is. □

(6.3.3) <u>CONCLUSIES</u>: We hoeven alleen maar naar gereduceerde polynomen te kijken en alle functies in k^V worden door een gereduceerde polynoom gerepresenteerd.

6.4. DE STELLING VAN CHEVALLEY EN GENERALISATIES

Aangezien iedere functie beschreven wordt door een polynoom is in het

algemeen niets te zeggen over het aantal nulpunten van een polynoom. Kijken we naar gereduceerde polynomen zonder constante term dan weten we dat de oorsprong van V een nulpunt is. We vragen ons af of dit nulpunt uniek is.

(6.4.1) <u>STELLING</u> [CHEVALLEY]: *Zij* $f_1,\ldots,f_s$ *een stelsel gereduceerde polynomen in* $k[X_1,\ldots,X_m]$ *met constante term* 0. *Zij* d_i *de graad van* f_i. *Als* $d = \sum_{i\leq s} d_i < m$ *dan bezit het stelsel* $f_1,\ldots,f_s$ *een gemeenschappelijk niet triviaal nulpunt in* V *(i.e.* $\exists \underline{a} \in V$, $\underline{a} \neq \underline{0}$ *en* $f_1(\underline{a}) = \ldots = f_s(\underline{a}) = 0$*).*

Er geldt in feite nog meer: het aantal gemeenschappelijke nulpunten is deelbaar door p (de karakteristiek van k). Deze laatste verscherping volgt rechtstreeks uit het bewijs.

<u>BEWIJS</u>: Zij $W = \{\underline{a} \in V \mid f_1(\underline{a}) = \ldots = f_s(\underline{a}) = 0\}$. Beschouw de volgende twee polynomen:

$$G := \prod_{i\leq s} (1-f_i^{q-1}),$$

$$H := \sum_{\underline{a}\in W} f_{\underline{a}}.$$

Het is makkelijk in te zien dat zowel E(G) als E(H) de waarde 1 aannemen in de punten van W en 0 daarbuiten. Derhalve geldt $G \equiv H \bmod J$. Nu is H gereduceerd. Indien we G reduceren (mod I) tot G^* geldt graad $(G^*) \leq$ graad $(G) = (q-1).d$. Maar volgens (6.3.1) is $G^* = H$ zodat graad $(H) \leq (q-1).d$. Merk nu op dat de hoogste graadsterm van $f_{\underline{a}}$, zijnde $(-1)^m X_1^{q-1} \ldots X_m^{q-1}$, van graad $m(q-1)$ is en niet van $\underline{a}$ afhangt. Wil in H geen term van deze graad voorkomen dan moet het aantal polynomen $f_{\underline{a}}$ dat wordt opgeteld om H te vormen een veelvoud van p zijn, i.e. $|W| \equiv 0 \pmod p$. □

(6.4.2) GENERALISATIE [WARNING]: Onder de bovengenoemde aannamen en met gebruikmaking der notaties uit het bewijs geldt $|W| \geq q^{m-d}$.

Deze generalisatie zal bewezen worden als gevolg van de grens voor het minimale gewicht voor de nog in te voeren gegeneraliseerde Reed-Muller codes.

Een generalisatie die zich uitspreekt over de deelbaarheids eigenschappen van het aantal nulpunten is de volgende stelling van AX (1964).

(6.4.3) STELLING [AX]: *Zij* f *een polynoom in* $k[X_1,\ldots,X_m]$ *van de graad* $d < m$. *Stel* $b = [m/d]$ *en zij* W *de verz. nulpunten van* f *in* k^m. *Dan geldt* $|W| \equiv 0 \pmod{q^b}$.

Van deze generalisatie zullen we in dit hoofdstuk geen bewijs geven.

6.5. DE GEGENERALISEERDE REED-MULLER CODES

Zij $V \simeq (k^m)$, $k = \mathbb{F}_q$. Bij een gegeven functie $f \in k^V$ kunnen we de tabel van waarden van f vormen, onder weglating der argumenten die wij op een of andere vaste wijze geënumereerd achten te zijn. Dit levert een afbeelding $S: k^V \to (k)^{q^m}$.

(6.5.1) DEFINITIE: De (gegeneraliseerde) *Reed-Muller code* RM(m,v,q) is het beeld onder de afbeelding $S \circ E$ van de verz. van polynomen

$$\{f \in k[X_1,\ldots,X_m] \mid \text{graad } (f) \leq v\} \text{ waarbij } k = \mathbb{F}_q.$$

Om deze definitie goed te praten moeten we laten zien dat de code niet afhangt van de (impliciete) basiskeuzen gemaakt in de definities van E en S. Wat betreft S is het duidelijk dat een omnummering van de elementen van V leidt tot een equivalente code in de zin als beschreven in (3.2.3). Minder duidelijk is het wat de invloed is van de keuze van de basis die ten grondslag ligt aan de isomorfie $V \cong k^m$. Immers een andere keuze van een basis impliceert dat de monomen $X_1,\ldots,X_m$ worden afgebeeld op andere functies in k^V. De *graad* van een polynoom wordt hierdoor echter niet beinvloed:

(6.5.2) LEMMA. *Zij* $\sigma: V \to V$ *een automorfisme en zij* $\underline{a} \in V$ *een vast element. Beschouw de affiene afbeelding* $\tau = \sigma + \underline{a}: V \to V$ *gedefiniëerd door* $\tau(\underline{x}) = \sigma(\underline{x}) + \underline{a}$. *Deze induceert een isomorfisme* $\tau^*: k^V \to k^V$ *door* $\tau^*(h) = h \circ \tau$. *Dan geldt dat het isomorfisme* $\tau^{**}: R \to R$ *gedefiniëerd door* $\tau^{**} = E^{-1} \circ \tau^* \circ E$ *de graad respecteert.*

BEWIJS: Uitschrijven leert dat τ^{**} de vorm heeft:

$$f(X_1,\ldots,X_m) \longrightarrow f(\Sigma\sigma_{i_1} X_i + a_1,\ldots,\Sigma\sigma_{i_m} X_i + a_m)$$

en onder deze transformatie stijgt de graad niet. De graad kan ook niet dalen want τ^{**} is een isomorfisme. □

(6.5.3) GEVOLG: *De groep van affiene transformaties van* V *die we hierboven hebben ingevoerd, werkende op de posities van de code* RM(m,v,q) *(opgevat als punten in* V*) voert deze code in zich zelve over.*

Een lineaire code is equivalent met een verlengde cyclische code als hij invariant is onder een permutatie van de plaatsen die een plaats vast laat, en de overige posities cyclisch verwisselt, terwijl bovendien alle woorden in de code de eigenschap hebben dat de som der coëfficienten gelijk nul is.

(6.5.4) STELLING: *Als* $v < m(q-1)$ *dan is de code* RM(m,v,q) *equivalent met een verlengde cyclische code.*

BEWIJS: Zij α een primitieve wortel van $\mathbb{F}_{q^m} \supset \mathbb{F}_q$. $\mathbb{F}_{q^m}$ is als $\mathbb{F}_q$-lineaire ruimte isomorf met $(\mathbb{F}_q)^m$. Bovendien is vermenigvuldigen met α een $\mathbb{F}_q$-lineair automorfisme van $\mathbb{F}_{q^m}$. Onder dit automorfisme blijft het element 0 op zijn plaats terwijl de elementen van $\mathbb{F}_{q^m}^*$ cyclisch worden verwisseld. Dit laat zien dat er een affiene transformatie van V bestaat met de gewenste vorm van de banen.

Om de tweede voorwaarde te controleren moeten we de som bepalen van de coordinaten in S(E(f)). Deze som $\sum$ is:

$$\sum = \sum_{\underline{a}\in(k)^m} f(\underline{a}) = \sum_{\substack{g \text{ monoom in } f}} \text{coeff. van } g. \left(\sum_{\underline{a}\in(k)^m} g(\underline{a})\right).$$

Schrijf een term g als:

$$g = \alpha_g X_1^{d_{1g}} \cdot \ldots \cdot X_m^{d_{mg}}. \text{ Dan vinden we}$$

$$\sum = \sum_g \alpha_g \prod_{i\le m} \sum_{a\in k} a^{d_{ig}} \qquad \text{waarbij} \qquad \sum_{i\le m} d_{ig} \le v \text{ voor ieder monoom } g.$$

Om $\sum_{i\le m} d_{ig} < m(q-1)$ is er ten minste één i waarvoor $d_{ig} < q-1$. Nu geldt voor een eindig lichaam:

$$\sum_{x\in\mathbb{F}_q} x^j = \begin{cases} -1 & \text{als} \quad j > 0 \text{ en } j \equiv 0 \pmod{q-1}, \\ 0 & \text{anders,} \end{cases}$$

hetgeen laat zien dat $\sum_{\underline{a}\in(k)^m} f(a) = 0$. □

(6.5.5) OPMERKING. Voor $v = 0$ is $R(m,v,q)$ de repetitie code van lengte q^m. Voor $v = 1$ bestaat $R(m,v,q)$ uit de "tabellen" van alle affiene functies op V. Omdat een niet identiek nul zijnde affiene functie ten hoogste q^{m-1} nulpunten heeft bedraagt het minimale gewicht in dit geval $(q-1)q^{m-1}$. Voor $v = (q-1)m$ beslaat $R(m,v,q)$ de gehele ruimte $(k)^{q^m}$.
Voor willekeurige $v < (q-1)m$ kunnen we schrijven

$$v = r.(q-1) + s \qquad\qquad 0 \le s \le q-1.$$

Beschouw vervolgens het polynoom

$$f = (1-X_1^{q-1})\dots(1-X_r^{q-1}) \prod_{0<i\le s} (X_{r+1} - \alpha_i)$$

(waarbij de α_i verschillende elementen van $\mathbb{F}_q$ zijn). Dan zien we dat dit polynoom graad v heeft. Een niet-nulpunt van f heeft de vorm

$$\underline{a} = (a_1,\dots,a_m) \quad \text{waarbij} \quad a_1 = a_2 = \dots = a_r = 0$$

$$\text{en} \quad a_{r+1} \ne \alpha_i \quad \text{voor } 0 < i \le s.$$

Het aantal niet-nulpunten van f is derhalve

$$q^{m-r-1} \cdot (q-s).$$

Dit getal is dus een bovengrens voor het minimale gewicht in $RM(m,v,q)$. De oplettende lezer zal wellicht opmerken dat deze grens exact is voor $v = 0,1$ en $v = m(q-1)$. Dat dit geen toeval is blijkt uit de volgende stelling (zie ook (6.2.2)).

(6.5.6) STELLING. (= Reed-Muller grens). *Het minimale gewicht van* $RM(m,v,q)$ *is* $q^{m-r-1}(q-s)$.

We zullen deze stelling in § 6.6 bewijzen. Om enig inzicht te krijgen

in de algebraïsche achtergronden beschouwen we het geval $q = 2$. Omdat $q - 1 = 1$ zijn de gereduceerde monomen lineair in iedere optredende variabele. De Reed-Muller grens voor $R(m,v,2)$ levert 2^{m-v}. Bij een polynoom f beschouwen we het polynoom $g = 1 + f$ dat nul is waar f geen nulpunt heeft en omgekeerd. Derhalve is het gewicht van $S(f)$ gelijk aan het aantal nulpunten van g. Bovendien hebben f en g dezelfde graad.

Volgens de stelling van Warning is het aantal nulpunten van g ten minste 2^{m-v}. Kennelijk is de stelling van Warning voor $q = 2$ equivalent met de Reed-Muller grens.

Algemeen geldt:

(6.5.7) STELLING. *De stelling van Warning is een direct gevolg van de Reed-Muller grens.*

BEWIJS: Zij $g_1,\ldots,g_s$ een stelsel gereduceerde polynomen met graden d_i waarbij $\Sigma d_i = d < m$. Beschouw het polynoom f^* dat ontstaat door het product $f = \prod_{i=1}^{s} (g_i^{q-1}-1)$ te reduceren. Dan geldt

$$\deg(f^*) \leq \deg(f) = (q-1)d < m(q-1).$$

Bovendien geldt

$$(f(\underline{x}) \neq 0) \Leftrightarrow (g_1(\underline{x}) = g_2(\underline{x}) = \ldots = g_s(\underline{x}) = 0).$$

Aannemende dat de g_i ten minste één gemeenschappelijk nulpunt bezitten leiden we af dat f niet identiek 0 is. Volgens de Reed-Muller grens bedraagt het gewicht van het woord $w := S(E(f))$ (N.B. $w \neq \underline{0}$) dat bevat is in $RM(m,d(q-1),q)$ ten minste q^{m-d}. Dit is de gevraagde ondergrens voor het aantal gemeenschappelijke nulpunten der g_i. □

6.6. BEWIJS DER REED-MULLER GRENS

Het bewijs van de Reed-Muller grens is triviaal indien $m = 1$. De polynomen zijn in dit geval polynomen in één veranderlijke zodat het aantal nulpunten begrensd wordt door de graad van het polynoom. Het aantal niet-nulpunten van een niet-nul polynoom van de graad $\leq v \leq q - 1$ is ten minste $q - v$ hetgeen precies is wat de Reed-Muller grens verlangt.

Het algemene geval berust op de volgende truc. Omdat $(\mathbb{F}_q)^m$ en $\mathbb{F}_{q^m}$

als $\mathbb{F}_q$-vectorruimte isomorf zijn kunnen we de functies in $\mathbb{F}_q^{(\mathbb{F}_q)^m}$ opvatten als functies in $\mathbb{F}_q^{\mathbb{F}_{q^m}}$ die zich laten weergeven door polynomen in één variabele en dan functies beschrijven in $\mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$. We moeten nauwkeurig nagaan wat er met het begrip graad gebeurt; indien we de graad van de te genereren polynomen in $\mathbb{F}_{q^m}[X]$ "laag" kunnen houden levert dit een ondergrens op voor het minimale gewicht. Zie ook het volgende diagram:

$$\begin{tikzcd}
V \arrow[r, "f"] & \mathbb{F}_q & & f \in \mathbb{F}_q[X_1,\ldots,X_m] \\
\wr\| \arrow[ur] & \cap & & \\
\mathbb{F}_{q^m} \arrow[r, "f^*"'] & \mathbb{F}_{q^m} & & f^* \in \mathbb{F}_{q^m}[X]
\end{tikzcd}$$

of het hiermee samenhangende diagram:

$$\begin{array}{ccc}
E^{-1}(S^{-1}(RM(m,v,q))) & \xrightarrow{*} & A = \{f^* \mid f \in B\} \\
\| & & \\
B := \{f \in \mathbb{F}_q[X_1,\ldots,X_m] \mid \text{graad } (f) \le v\} & & \cap \\
\cap & & \\
\mathbb{F}_q[X_1,\ldots,X_m] & \xrightarrow{*} & \mathbb{F}_{q^m}[X].
\end{array}$$

Om de $\mathbb{F}_q$-lineaire deelruimte A in $\mathbb{F}_{q^m}[X]$ te bepalen gebruiken we de volgende strategie. Eerst bepalen we welke elementen in $\mathbb{F}_{q^m}[X]$ optreden als beeld van een $\mathbb{F}_q$-lineaire functie. Daarna vormen we producten van deze functies opgebouwd uit ten hoogste v termen. Lineaire combinaties daarvan vormen de verzameling A.

Tijdens het bewijs zal blijken dat het voor het bepalen van de maximale graad van een element in A niet nodig is gebruik te maken van het feit dat functies $f^* \in \mathbb{F}_{q^m}[X]$ die afkomstig zijn van $\mathbb{F}_q[X_1,\ldots,X_m]$ bij substitutie van elementen in $\mathbb{F}_{q^m}$ alleen maar waarden in $\mathbb{F}_q$ aannemen.

(6.6.1) <u>STAP 1</u>: *Bepaling van $\mathbb{F}_q$-lineaire functies in $\mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$ (zonder constante term).*

Deze functies laten zich beschrijven door $m \times m$ matrices met elementen in $\mathbb{F}_q$ (vat $\mathbb{F}_{q^m}$ op als $(\mathbb{F}_q)^m$). Het aantal van deze functies bedraagt dus $q^{(m^2)}$.

We kunnen deze verzameling dus karakteriseren door een even grote verzameling van $\mathbb{F}_q$-lineaire functies te verzinnen.

Zij $\underline{\beta} = (\beta_0,\ldots,\beta_{m-1}) \in (\mathbb{F}_{q^m})^m$ en beschouw de functie $f_{\underline{\beta}}$ gedefinieerd door $\alpha \to \sum_{i=0}^{m-1} \beta_i \cdot \alpha^{q^i}$ (waarbij α een primitief element van $\mathbb{F}_{q^m}$ is). Men verifieert eenvoudig dat $f_{\underline{\beta}}$ $\mathbb{F}_q$-lineair is. Bovendien geldt op grond van het feit dat de $f_{\underline{\beta}}$ gereduceerd zijn (als polynomen in $\mathbb{F}_{q^m}[X]$) dat $f_{\underline{\beta}} = f_{\underline{\beta}'}$ d.e.s.d. als $\underline{\beta} = \underline{\beta}'$. Tellen van dimensies leert dat hiermede alle $\mathbb{F}_q$-lineaire functies gevonden zijn. □

(6.6.2) <u>OPMERKING</u>: Opdat $f_{\underline{\beta}}$ waarden in $\mathbb{F}_q$ aanneme is het voldoende te eisen dat $f_{\underline{\beta}} = (f_{\underline{\beta}})^q$ i.e. $\beta_i^q = \beta_{i+1}$ voor $0 \le i \le m-2$ en $\beta_{m-1}^q = \beta_0$.

(6.6.3) <u>LEMMA</u>. *Zij* $c_q(n)$ *de som van de cijfers van* n *bij ontwikkeling van* n *in het* q*-tallig stelsel. Dan geldt*

(i) $c_q(n) + c_q(m) \ge c_q(n+m)$ $\quad n,m \ge 0$

(ii) $c_q(n) + c_q(m) \equiv c_q(n+m) \pmod{q-1}$ $\quad n,m \ge 0$

(iii) *indien* $n \equiv m \bmod (q^t-1)$ *en* $0 \le n < q^t - 1 \le m$ *dan geldt*

$c_q(n) \le c_q(m)$ *en* $c_q(n) \equiv c_q(m) \bmod (q-1)$.

<u>BEWIJS</u>: (i) is vanzelfsprekend en (ii) drukt uit dat het verwerken van een overdracht (carry) de cijfersom met $(q-1)$ doet dalen. Omdat het reduceren van m modulo (q^t-1) neerkomt op het herhaald optellen van blokken van t opeenvolgende cijfers in het q-tallig stelsel is (iii) een rechtstreeks gevolg van (i) en (ii). □

(6.6.4) <u>STAP 2</u>: *Bepaling van* A.

De $\mathbb{F}_q$-lineaire polynomen in $\mathbb{F}_{q^m}[X]$ hebben de eigenschap dat ieder optredend monoom een exponent heeft met cijfersom ≤ 1. Vormen we van deze polynomen een v-voudig product dan heeft de exponent van ieder in dit product optredend monoom cijfersom $\le v$. Omgekeerd kan ieder zodanig monoom op deze wijze gevormd worden.

(6.6.5) <u>GEVOLG</u>:

$$A = \{f \mid f = \sum_{\substack{i<q^m \\ c_q(i)\le v}} \beta_i X^i \quad en \quad f^q \equiv f \pmod{X^{q^m}-X}\}.$$

(6.6.6) STAP 3: *Bepaling van de maximale graad van een element in* A.

Op grond van het voorafgaande hoeven we alleen maar de maximale exponent met cijfersom $\leq v$ te bepalen. Schrijven we als tevoren $v = r.(q-1) + s$, $0 \leq s \leq q-1$, dan zien we gemakkelijk in dat deze exponent zich laat schrijven als

$$\overbrace{\underline{q-1} \quad \underline{q-1} \quad \ldots \quad \underline{q-1}}^{r} \quad s \quad \overbrace{0 \quad 0 \quad \ldots \quad 0}^{m-1-r} \qquad \text{(q-tallig)}$$

en dus als waarde heeft $q^n - (q-s).q^{m-r-1}$.

(6.6.7) GEVOLG 1 [*Reed-Muller grens*]. (Notaties als boven.)

Zij graad $(f) \leq v$ dan geldt graad $(f^*) \leq q^n - (q-s).q^{m-r-1}$. Dientengevolge heeft f^* hoogstens $q^n - (q-s).q^{m-r-1}$ nulpunten en tan minste $(q-s).q^{m-r-1}$ niet-nulpunten. Gezien de aanwezigheid van woorden met precies dit gewicht is de Reed-Muller grens hiermee bewezen. □

(6.6.8) GEVOLG 2 [*dimensie Reed-Muller code*]. Uit de bovenstaande beschrijving blijkt direct dat de volledige verzameling

$$A^* = \{f \mid f = \sum_{\substack{i<q^m \\ c_q(i)\leq v}} \beta_i X^i\}$$

over $\mathbb{F}_{q^m}$ de dimensie $u := |\{j \mid 0 \leq j < q^m \text{ en } c_q(j) \leq v\}|$ heeft. In feite zijn we geinteresseerd in de dimensie van A over $\mathbb{F}_q$. Deze twee dimensies zijn echter gelijk. Dit kan men ondermeer controleren door na te gaan hoe de eis $f^q \equiv f \pmod{X^q - X}$ de keuzevrijheid der β_i beperkt: gebruikmakende van de conditie $\beta_i^q = \beta_{iq}$ en rekening houdende met het mogelijk optreden van tussenlichamen tussen $\mathbb{F}_q$ en $\mathbb{F}_{q^m}$ ingeval $iq^\ell \equiv i$ voor $\ell < m$ (er is niet gegeven dat $(m, q^m-1) = 1$) leidt men af dat deze congruentie-eis de multiplicatieve factor m precies opheft. Ook kan men gebruik maken van het (niet hier bewezen) feit dat

$$A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = A^*.$$

Tenslotte kan men rechtstreeks (door de exponenten in een monoom

$x_1^{e_1} \cdot \ldots \cdot x_m^{e_m}$ te lezen als een q-tallig getal) tot hetzelfde inzicht komen.

(6.6.9) OPMERKING: Men kan zich afvragen of de aangegeven woorden van minimaal gewicht (modulo symmetrie onder de werking van $Gl(\mathbb{F}_q,m)$) de enige woorden van minimaal gewicht zijn. Dit is inderdaad het geval zoals bewezen door DELSARTE, GOETHALS & MacWILLIAMS (1970). Het door hun aangegeven bewijs is te uitgebreid om op deze plaats te worden behandeld. Voor het speciale geval dat $s = 0$ is het resultaat door Peterson bewezen onder gebruikmaking van genererende functies. Het ziet er niet naar uit dat het bewijs van Delsarte c.s., dat wezenlijk gebruik maakt van de affien-meetkundige structuur van $(\mathbb{F}_q)^m$ zich laat vereenvoudigen door de hierboven beschreven methode berustende op de identificatie van $(\mathbb{F}_q)^m$ en $\mathbb{F}_{q^m}$.

6.7. ALTERNATIEVE BESCHRIJVING DER REED-MULLER CODE

We beschouwen als tevoren de code $RM(m,v,q)$ met $v < m(q-1)$. Zij α een element van $\mathbb{F}_{q^m}$. Zoals we eerder zagen gedraagt de functie $f_\alpha = 1 - (X-\alpha)^{q^m-1}$ zich als de karakteristieke functie van het element α. Voor willekeurige functies $f \in \mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$ kunnen we dus schrijven

$$f = \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha).f_\alpha = \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha).(1-(X-\alpha)^{q^m-1}).$$

Deze som laat zich als volgt uitwerken:

$$(X-\alpha)^{q^m-1} = \frac{X^{q^m} - \alpha^{q^m}}{X - \alpha} = \sum_{j=0}^{q^m-1} X^j \alpha^{q^m-1-j}.$$

Zodat

$$f = \sum_{j=0}^{q^m-1} \left(\sum_{\alpha\in\mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j + \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha) =$$

$$= \sum_{j=1}^{q^m-1} \left(\sum_{\alpha\in\mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j - \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha)(\alpha^{q^m-1} - 1) =$$

$$= \sum_{j=1}^{q^m-1} \left(\sum_{\alpha \in \mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j + f(0).$$

Stel nu dat $f \in A$, d.w.z. de exponenten van in f optredende monomen hebben som $\leq v$. Dan geldt

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^{q^m-1-j} = 0 \qquad \text{als } c_q(j) > v,\ 0 < j \leq q^{n-1}.$$

Omdat $q^m - 1$ uitgeschreven in het q-tallig stelsel er als volgt uit ziet:

$$\underbrace{\underline{q-1} \quad \underline{q-1} \quad \ldots \quad \underline{q-1}}_{m}$$

controleert men eenvoudig dat voor $0 \leq j \leq q^{m-1}$ geldt

$$c_q(j) > v \Longleftrightarrow c_q(q^m-1-j) < m(q-1) - v,$$

We vinden dus

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^j = 0 \qquad \text{voor } 0 \leq j < q^m - 1 \text{ en } c_q(j) < m(q-1) - v.$$

Als bijzonder geval geeft dit:

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) = 0,$$

wat we reeds hebben opgemerkt bij het bewijs dat RM(m,v,q) equivalent is met een verlengde cyclische code (6.5.4).

Willen we een code in $\mathbb{F}_q^{\mathbb{F}_q^m}$ beschrijven als verlengde cyclische code dan moeten we een plaats identificeren met het parity-check symbool en de overige q^m-1 plaatsen opvatten als coefficienten van polynomen in $\mathbb{F}_q[X]/(X^{q^m-1}-1)$. Merk op dat $(q^m-1,q) = 1$ zodat een cyclische code geheel bepaald is door zijn nulpunten. In het concrete geval van de code RM(m,v,q) ziet deze beschrijving er als volgt uit. Zij γ een primitief element van

$\mathbb{F}_{q^m}$. Voor iedere $f \in \mathbb{F}_q^{\mathbb{F}_{q^m}}$ geldt nu:

$$f = \sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot f_\alpha = \sum_{\alpha \in \mathbb{F}_{q^m}^*} f(\alpha) \cdot f_\alpha + f(0) \cdot f_0 =$$

$$= \sum_{j=0}^{q^m-2} f(\gamma^j) f_{\gamma^j} + f(0) \cdot f_0.$$

We identificeren nu f_{γ^j} met x^j en vatten de waarden $f(\gamma^j)$ als coëfficienten op. Let op dat dit geen isomorfisme van ringen is aangezien in het algemeen $f_{\gamma^i} f_{\gamma^j} \neq f_{\gamma^{i+j}}$. De coëfficient van f_0 vatten we op als parity-check symbool.
We verkrijgen zo

$$RM(m,v,q) \cong \left\{ \left(\sum_{j=0}^{q^m-2} f(\gamma^j) \cdot x^j,\ f(0) \right) \mid f \in A \right\}$$

waarbij het rechterlid nog steeds een verlengde cyclische code is.

Zij L de verzameling optredende polynomen $\sum_{j=0}^{q^m-2} f(\gamma^j) x^j$. Dan is L een ideaal in $\mathbb{F}_q[X]/(X^{q^m-1}-1)$ en we mogen dus vragen naar de gemeenschappelijke nulpunten van L. Van deze nulpunten is een aantal reeds bekend.

Zij als hiervoor γ een primitief element. Voor $f \in RM(m,v,q)$ en $0 < j < q^m - 1$ en $c_q(j) < m(q-1) - v$ geldt:

$$0 = \sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^j = \sum_{\alpha \in \mathbb{F}_{q^m}^*} f(\alpha) \cdot \alpha^j = \sum_{i=0}^{q^m-2} f(\gamma^i) \gamma^{ij} =$$

$$= \sum_{i=0}^{q^m-2} f(\gamma^i) (\gamma^j)^i.$$

Kennelijk zijn de punten γ^j met $0 < j < q^m - 1$ en $c_q(j) < m(q-1) - v$ gemeenschappelijke nulpunten van de elementen van L.

Dat de polynomen in L niet meer gemeenschappelijke nulpunten kunnen hebben zien we als volgt in. Zij L^* het ideaal in $\mathbb{F}_q[X]/(X^{q^m-1})$ bestaande uit de polynomen die de punten γ^j voor $c_q(j) < m(q-1) - v$ tot nulpunt

hebben. Uit het voorafgaande volgt $L^* \supset L$. Omdat $\mathbb{F}_q[X]$ een hoofdideaal ring is wordt L^* als ideaal voortgebracht door het minimale polynoom dat alle punten γ^j met $c_q(j) < m(q-1) - v$ tot nulpunt heeft. Dit is het polynoom

$$\prod_{\substack{0\le j<q^m-1 \\ c_q(j)<m(q-1)-v}} (X-\gamma^j)$$

(ga na dat dit een polynoom in $\mathbb{F}_q[X]$ is!). De graad van dit polynoom is gelijk aan

$$d = |\{j \mid 0 < j < q^m - 1,\ c_q(j) < m(q-1) - v\}|$$

en de dimensie over $\mathbb{F}_q$ van het ideaal L^* is dus $q^m - 1 - d$.

Anderzijds is de dimensie van het ideaal L gelijk aan de dimensie van de code RM(m,v,q). In de voorafgaande paragraaf hebben we deze dimensie uitgerekend waarbij de uitkomst was

$$f = |\{j \mid 0 \le j \le q^m - 1 \text{ en } c_q(j) \le v\}|.$$

Aangezien we hebben aangenomen dat $v < (q-1)m$ geldt

$$f = |\{j \mid 0 \le j < q^m - 1 \text{ en } c_q(j) \le v\}|.$$

Gebruiken we nu opnieuw dat voor $0 \le j \le q^m - 1$

$$c_q(j) < v \iff c_q(q^m-1-j) > m(q-1) - v$$

dan zien we direct in dat

$$d + f = |\{j \mid (0<j<q^m-1 \text{ en } c_q(j)\le v) \text{ of } (0<j\le q^m-1 \text{ en } c_q(j)>v)\} =$$

$$= q^m - 1.$$

Hieruit volgt $f = q^m - 1 - d$, dus $L = L^*$, zodat het bewijs voltooid is.

(6.7.1) <u>CONCLUSIE</u>. Voor $v < m(q-1)$ is de code RM(m,v,q) een verlengde cyclische code, waarvoor de bijbehorende cyclische code afkomstig is van het ideaal $L \subset \mathbb{F}_q[X]/(X^{q^m-1}-1)$ dat voor een vaste primi-

tieve wortel $\gamma \in \mathbb{F}_{q^m}$ alle machten γ^j met $0 < j < q^m - 1$ en cijfersom $c_q(j)$ kleiner dan $m(q-1) - v$ als gemeenschappelijke nulpunten heeft.

<u>OPMERKING</u>: Het feit dat de polynomen in L de punten γ^j voor $1 \le j \le q^m - 1$ en $c_q(j) < n(q-1) - v$ als nulpunten hebben levert ons met behulp van de BCH-grens (5.5.1) een nieuw bewijs voor de Reed-Muller grens. Aangezien het kleinste getal j met $c_q(j) = m(q-1) - v$ ontstaat door grote cijfers zo ver mogelijk naar rechts te schuiven laat dit getal zich makkelijk berekenen. Stel $v = r(q-1) + s$, $0 \le s \le q - 1$. Dan geldt $m(q-1) - v = (m-r-1)(q-1) + (q-1-s)$ zodat het minimale getal met cijfersom $m(q-1) - v$ er uitziet als:

$$0, \quad 0, \quad \ldots \quad 0, \quad \underline{q-1-s}, \underbrace{\underline{q-1}, \quad \ldots, \quad \underline{q-1}}_{m-r-1} = (q-s).q^{m-r-1} - 1.$$

De BCH-grens levert derhalve een minimaal gewicht van $(q-s)q^{m-r-1} - 2 + 2 = (q-s)q^{m-r-1}$ evenals in (6.5.6) [zie (5.10.10)]. Merk op dat de Reed-Muller code een deelcode is van de verlengde BCH-code met ontwerpafstand $(q-s)q^{m-r-1}$. Daar dit het minimale gewicht van RM(m,v,q) is hebben we hier voorbeelden van BCH-codes waarvoor de minimale afstand gelijk is aan de ontwerpafstand.

6.8. DUALITEIT VAN REED-MULLER CODES

(6.8.1) <u>STELLING</u>. *De code* C = RM(m,v,q) *is de duale van de code* C' = RM(m,m(q-1)-v-1,q).

<u>BEWIJS</u>. Merk allereerst op dat de som van de twee dimensies klopt: volgens het voorafgaande is deze som gelijk aan

$$|\{j \mid 0 \le j \le q^m-1 \text{ en } c^q(j) \le v\}| +$$

$$+ |\{j \mid 0 \le j \le q^m-1 \text{ en } c_q(j) < m(q-1) - v\} =$$

$$= |\{j \mid 0 \le j \le q^m-1 \text{ en } (c_q(j) \le v \text{ of } c_q(j) > v)\}| = q^m.$$

Het is derhalve voldoende om te controleren dat ieder paar elementen $\underline{x},\underline{x}'$ uit C resp. C' inproduct nul hebben.

Stel

$\underline{x} = S(E(f))$ met graad $(f) \leq v$ en
$\underline{x}' = S(E(f'))$ met graad $(f') \leq m(q-1) - v - 1$

dan volgt

$$\langle \underline{x},\underline{x}' \rangle = \sum_{a \in (\mathbb{F}_q)^m} f(a) \,.\, f'(a) = \sum_{a \in (\mathbb{F}_q)^m} (f.f')(a)$$

nu is $S(E(f.f'))$ een element van $RM(m,m(q-1)-1,q)$ dus de som der coëfficienten van $S(E(f.f'))$ is gelijk nul. Hieruit volgt $\langle \underline{x},\underline{x}' \rangle = 0$. □

6.9. COMMENTAAR

Voor gedeeltelijk andere maar in wezen equivalente beschrijvingen van RM-codes verwijzen we naar BERLEKAMP (1968), VAN LINT (1971), CAMERON & VAN LINT (1975). Hier treft men o.a. een bewijs aan dat de beschrijvingen van gegeneraliseerde RM-codes equivalent zijn. Het hier weergegeven bewijs is in deze vorm afkomstig van H.W. Lenstra, Jr. Voor meer informatie over de stellingen van Chevalley, Warning en Ax verwijzen we naar JOLY (1973).

6.10. OPGAVEN

(6.10.1) Zij $Tr : \mathbb{F}_{2m} \longrightarrow \mathbb{F}_2$ het spoor gedefiniëerd door

$$Tr(\xi) := \xi + \xi^2 + \xi^4 + \ldots + \xi^{2^{m-1}}.$$

Als we $\mathbb{F}_{2m}$ opvatten als m-dimensionale vectorruimte V over $\mathbb{F}_2$ is door

$$L_\eta(\xi) := Tr(\xi\eta)$$

een lineaire afbeelding L_η gegeven. Zij $n = 2^m-1$. Zij ω een primitieve n-de eenheidswortel in $\mathbb{F}_{2m}$.
Beschouw

$$C := \{u(x) = u_0 + u_1 x + \ldots + u_{n-1}x^{n-1} \mid u_i = L_\eta(\omega^i),$$

$$0 \le i \le n-1,\ \eta \in V\}.$$

Bewijs dat C bestaat uit de woorden van even gewicht in de 1^e orde RM-code.

(6.10.2) Bij gebruik van de 2^e orde RM-code van lengte 32 ontvangen we

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

Wat was het codewoord?

(6.10.3) Beschouw de 2^e orde binaire RM-code van lengte 2^m. Welke gewichten kunnen voorkomen? M.a.w. bepaal de coefficienten van de weight-enumerator die 0 zijn.

Hoofdstuk VII

GELIJKMATIG VERDEELDE CODES

7.1. INLEIDING

In dit hoofdstuk beperken we ons tot binaire codes. Om inzicht te krijgen in resultaten en bewijsmethoden van dit deel van Coding Theory is dit voldoende. Vrijwel alles gaat (met iets meer werk) precies zo voor codes over een alfabet van meer dan twee symbolen.

Om de codes die ons nu interesseren te definiëren en te bestuderen is een omvangrijk formeel apparaat nodig. We zullen hiervan een deel beschrijven. Zij X de n-dimensionale vectorruimte over GF(2) en zij $C \subset X$ een code. De Hamming afstand in X geven we weer aan met d. De "*inner distribution*" $\underline{a} := (a_0, a_1, \ldots, a_n)$ en het bijbehorende afstandspolynoom $A_C(z)$ definiëren we door

$$(7.1.1) \qquad A_C(z) := \sum_{i=0}^{n} a_i z^i := |C|^{-1} \sum_{\underline{u}\in C, \underline{v}\in C} z^{d(\underline{u},\underline{v})}.$$

Meer informatie over de afstanden kunnen we beschrijven met de zgn. "*outer distribution*" matrix B waarvan de rijen worden genummerd met de vectoren $\underline{x} \in X$ en de kolommen met $0,1,\ldots,n$, en wel

$$(7.1.2) \qquad B(\underline{x},i) := \text{aantal elementen van } C \text{ met afstand } i \text{ tot } \underline{x}.$$

Met $B(\underline{x})$ geven we de rij van B met nummer $\underline{x}$ aan. Merk op dat

$$(7.1.3) \qquad \underline{a} = |C|^{-1} \sum_{\underline{x}\in C} B(\underline{x}).$$

$$(7.1.4) \qquad B(\underline{x},0) = 1 \iff \underline{x} \in C.$$

Als alle rijen van B die met 1 beginnen hetzelfde zijn noemt men C een *reguliere* code. De code C heet *volledig regulier* als

$$(7.1.5) \qquad \forall_{\underline{x}\in X} \forall_{\underline{y}\in X} [(\rho(\underline{x},C) = \rho(\underline{y},C)) \Rightarrow (B(\underline{x}) = B(\underline{y}))],$$

waarbij $\rho(\underline{x},C)$ de afstand van $\underline{x}$ tot C is. Als C regulier is, $\underline{0} \in C$, dan is de *weight enumerator* $W_C(z) := \sum_{\underline{x}\in C} z^{w(\underline{u})}$ gelijk aan $A_C(z)$. (zie o.a. DELSARTE (1973)).

Zij $(A, \oplus, *)$ de groepsalgebra van X over $\mathbb{C}$, d.w.z. de vectorruimte over $\mathbb{C}$ met de elementen van $\underline{x}$ als basisvectoren voorzien van een vermenigvuldiging $*$, gedefinieerd door

$$(7.1.6) \qquad \bigoplus_{\underline{x}\in X} \alpha(\underline{x})\underline{x} * \bigoplus_{\underline{y}\in X} \beta(\underline{y})\underline{y} := \bigoplus_{\underline{z}\in X} \Big(\sum_{\underline{x}+\underline{y}=\underline{z}} \alpha(\underline{x})\beta(\underline{y})\Big)\underline{z}.$$

Aan een deelverzameling Y van X voegen we toe het element $\bigoplus_{\underline{y}\in Y} \underline{y}$ uit A. We geven dit element van A ook met Y aan. Van bijzonder belang zijn de verzamelingen van woorden van vast gewicht en de bollen om $\underline{0}$, d.w.z.

$$(7.1.7) \qquad Y_i := \{\underline{x} \in X \mid w(\underline{x}) = i\},$$

$$(7.1.8) \qquad S_j := \{\underline{x} \in X \mid w(\underline{x}) \le j\}.$$

Nu geldt voor een code C met outer distribution B

$$(7.1.9) \qquad Y_i * C = \bigoplus_{\underline{x}\in X} B(\underline{x},i)\underline{x}.$$

Zij $D(\underline{x},j)$ het aantal codewoorden met afstand $\le j$ tot $\underline{x}$, d.w.z. $D(\underline{x},j) = \sum_{i\le j} B(\underline{x},i)$. Dan is volgens (7.1.8) en (7.1.9)

$$(7.1.10) \qquad S_j * C = \sum D(\underline{x},j)\underline{x}.$$

(zie o.a. VAN LINT (1971)).

7.2. KRAWTCHOUK POLYNOMEN

Zij χ het karakter van GF(2) met $\chi(1) = -1$. We definiëren nu voor iedere $\underline{u} \in X$ de afbeelding $\chi_{\underline{u}}: X \to \mathbb{C}$ door

$$(7.2.1) \qquad \forall_{\underline{v}\in X}[\chi_{\underline{u}}(\underline{v}) := \chi((\underline{u},\underline{v})) = (-1)^{(\underline{u},\underline{v})}],$$

d.w.z. $\chi_{\underline{u}}(\underline{v}) = 1$ als $\underline{u} \perp \underline{v}$ en anders $\chi_{\underline{u}}(\underline{v}) = -1$. We breiden dit uit tot een lineaire functionaal op $\mathcal{A}$ door

(7.2.2) $$\chi_{\underline{u}}(\sum \alpha(\underline{x})\underline{x}) = \sum \alpha(\underline{x})\chi_{\underline{u}}(\underline{x}).$$

De volgende twee beweringen volgen eenvoudig uit de definities. We laten het bewijs als oefening aan de lezer over.

(7.2.3) $$\forall_{\underline{u}\in X} \forall_{A\in\mathcal{A}} \forall_{B\in\mathcal{A}} [\chi_{\underline{u}}(A*B) = \chi_{\underline{u}}(A)\chi_{\underline{u}}(B)]$$

(7.2.4) S_n is het enige element van $\mathcal{A}$ waarvoor geldt:
(i) $\chi_{\underline{0}}(S_n) = 2^n$ en
(ii) $\forall_{\underline{u}\neq\underline{0}} [\chi_{\underline{u}}(S_n) = 0]$.

Beschouw nu een woord $\underline{u}$ met $w(\underline{u}) = w$. Dan is

$$\chi_{\underline{u}}(Y_k) = \sum_{\underline{v}\in X, w(\underline{v})=k} \chi((\underline{u},\underline{v})) = \sum_{i=0}^{k} \binom{w}{i}\binom{n-w}{k-i}(-1)^i.$$

Bij vaste n definiëren we de *KRAWTCHOUK polynomen* $K_k(n,x)$ voor $k = 0,1,\ldots$ door

(7.2.5) $$K_k(n,x) := \sum_{i=0}^{k} (-1)^i\binom{x}{i}\binom{n-x}{k-i},$$

waarin $\binom{x}{a} := x(x-1)\ldots(x-a+1)/a!$.

We hebben dan aangetoond dat

(7.2.6) $$\chi_{\underline{u}}(Y_k) = K_k(n,w(\underline{u})).$$

De Krawtchouk polynomen zijn bekend uit de theorie van orthogonale polynomen op een discrete verzameling (cf. SZEGÖ(1959) *Orthogonal Polynomials* § 2.8). We noemen een aantal eigenschappen welke de lezer eenvoudig kan verifiëren of uit de algemene theorie halen.

(7.2.7) $$\sum_{k=0}^{\infty} K_k(n,x)z^k = (1+z)^{n-x}(1-z)^x,$$

$$(7.2.8)\qquad K_k(n,x) = \sum_{j=0}^{k} (-2)^j \binom{n-j}{k-j}\binom{x}{j},$$

dus K_k is een polynoom van de graad k in x.

$$(7.2.9)\qquad \sum_{m=0}^{n} \binom{n}{m} K_k(n,m)K_\ell(n,m) = \delta_{k,\ell}\binom{n}{k}2^n.$$

Voor een recurrente betrekking van de polynomen en voor de Sturm-Stieltjes scheidingsstellingen over de nulpunten verwijzen we de lezer naar Szegö, loc. cit.

Is F(x) een polynoom van graad $\le t$, dan is F(x) éénduidig te schrijven als lineaire combinatie van de $K_k(n,x)$, $0 \le k \le t$:

$$(7.2.10)\qquad F(x) = \sum_{k=0}^{t} \alpha_k K_k(n,x);$$

we noemen dit de Krawtchouk-ontwikkeling van F(x).

Uit (7.2.6) volgt via een eenvoudige berekening dat als $w(\underline{u}) = x$,

$$(7.2.11)\qquad \chi_{\underline{u}}(S_j) = K_j(n-1,x-1) =: \Psi_j(x).$$

Uit (7.2.8) kan men eenvoudig de coëfficienten van x^e, x^{e-1}, x^{e-2} en x^0 in $\Psi_e(x)$ berekenen. Hieruit vinden we voor de (verschillende) nulpunten $x_1, x_2, \ldots, x_e$ van $\Psi_e(x)$

$$(7.2.12)\qquad \prod_{i=1}^{e} x_i = e!\, 2^{-e} \sum_{i=0}^{e} \binom{n}{i},$$

$$(7.2.13)\qquad \sum_{i=1}^{e} x_i = \tfrac{1}{2}e(n+1),$$

$$(7.2.14)\qquad \sum_{i<j} x_i x_j = \frac{1}{24}\, e(e-1)\{3n^2 + 3n + 2e + 2\}.$$

Merk op dat (7.2.13) ook volgt uit het feit dat $\Psi_e(x) = (-1)^e\ \Psi_e(n+1-x)$.
Door berekening van $\Psi_e(1)$ en $\Psi_e(2)$ vinden we als boven

(7.2.15) $$\prod_{i=1}^{e} (x_i-1) = 2^{-e} (n-1)(n-2)\ldots(n-e),$$

(7.2.16) $$\prod_{i=1}^{e} (x_i-2) = 2^{-e}(n-1-2e)(n-2)(n-3)\ldots(n-e).$$

(lit. GOETHALS & VAN TILBORG (1975), VAN LINT (1971), (1974)).

7.3. HET KARAKTERISTIEKE POLYNOOM VAN EEN CODE

Zij C een code in X. Voor $j = 0,1,\ldots,n$ definiëren we de *karakteristieke getallen* B_j van C door

(7.3.1) $$B_j := |C|^{-2} \sum_{\underline{u}\in Y_j} |\chi_{\underline{u}}(C)|^2.$$

Zij $N(C) := \{j \mid 1 \le j \le n,\ B_j \neq 0\}$. We definiëren het *karakteristieke polynoom* van C door

(7.3.2) $$F_C(x) := 2^n|C|^{-1} \prod_{j\in N(C)} (1-x/j).$$

Merk op dat als C een lineaire code is de redenering van Lemma (3.6.6) aantoont dat B_j het aantal woorden van gewicht j in $C^\perp$ voorstelt. Dus is N(C) dan het aantal gewichten $\neq 0$ dat in $C^\perp$ voorkomt.

(7.3.3) <u>STELLING</u>: *Laten $\alpha_0,\alpha_1,\ldots,\alpha_n$ de coefficiënten uit de Krawtchouk ontwikkeling van $F_C(x)$ zijn. Dan geldt in A*

$$\sum \alpha_i Y_i * C = S_n.$$

<u>BEWIJS</u>. Zij $\underline{u} \in X$, $w(\underline{u}) = j$. Volgens (7.2.3) en (7.2.6) is

$$\chi_{\underline{u}}(\sum \alpha_i Y_i * C) = \chi_{\underline{u}}(\sum \alpha_i Y_i)\chi_{\underline{u}}(C) = \chi_{\underline{u}}(C) \sum \alpha_i K_i(n,j) = \chi_{\underline{u}}(C)F_C(j).$$

Als $\underline{u} \neq \underline{0}$ dan is het laatste lid 0 op grond van de definitie van $F_C(x)$. Is $\underline{u} = \underline{0}$ dan is het laatste lid 2^n. Het gestelde volgt dus uit (7.2.4). □

(7.3.4) <u>GEVOLG</u>: *Voor de coëfficienten $\alpha_0,\alpha_1,\ldots,\alpha_n$ van de Krawtchouk ontwikkeling van $F_C(x)$ en iedere $\underline{u} \in X$ geldt*

$$\sum_{i=0}^{n} \alpha_i \; B(\underline{u},i) = 1.$$

De *overdekkingsstraal* $\rho(C)$ van een code is de kleinste ρ zo dat bollen met straal ρ om de codewoorden de hele ruimte X overdekken. Dus

(7.3.5) $\qquad \rho(C) := \max\{\rho(\underline{x},C) \mid \underline{x} \in X\}.$

Merk op dat uit (7.3.4) volgt dat $\rho(C) \leq |N(C)| =: s$.

We vermelden hier zonder bewijs de *identiteit van MacWilliams* (waarvan het bewijs door eenvoudige algebraïsche manipulatie is te geven, zie (3.6.5)).

(7.3.6) <u>STELLING</u>: *Laat voor* $j = 0,1,\ldots,n$

$$C_j := |C|^{-1} \sum_{\underline{u}\in Y_j} \chi_{\underline{u}}(C).$$

Dan geldt voor de weight enumerator $W_C(z)$ *van* C

$$W_C(z) = 2^{-n}|C| \sum_{j=0}^{n} C_j (1-z)^j (1+z)^{n-j}.$$

7.4. GELIJKMATIG VERDEELDE CODES

We beschouwen in deze paragraaf codes die ontstaan zijn als generalisatie van de *perfecte codes*. Een perfecte e-fouten-verbeterende code C is een code met minimum afstand $d = 2e + 1$ en $\rho(C) = e$. Merk op dat voor zo'n code geldt (in $\mathcal{A}$): $S_e * C = S_n$. De weinige interessante voorbeelden van perfecte codes zijn we in vorige hoofdstukken al tegengekomen.

We beschouwen nu codes met $d \geq 2e + 1$ en $\rho(C) = e + 1$. Hierdoor worden de perfecte codes tegelijk behandeld, namelijk as $d = 2e + 3$. De bollen met straal $e - 1$ om codewoorden zijn disjunct en ieder woord dat niet in één zo'n bol ligt heeft afstand e of e + 1 tot tenminste één codewoord.

(7.4.1) <u>DEFINITIE</u>. Een code C met $\rho(C) = e + 1$ en $d \geq 2e + 1$ heet *gelijkmatig verdeeld met parameter* r als ieder woord $\underline{u}$ met $\rho(\underline{u},C) \geq e$ afstand e of e + 1 tot precies r codewoorden heeft.

Merk op dat als $r = 1$ de code C een perfecte $(e+1)$-fouten-verbeterende code is. Daar $d \geq 2e + 1$ heeft een woord $\underline{u}$ met $\rho(u,C) = e$ afstand e tot precies één codewoord. Dit volgt uit de driehoeksongelijkheid en op dezelfde wijze ziet men direct in dat

(7.4.2) $$r \leq \frac{n}{e+1}$$

In het geval dat $r = \lfloor \frac{n}{e+1} \rfloor$ noemt men C *bijna perfect*.

(7.4.3) STELLING: *Een code* C *met* $\rho(C) = e + 1$ *en* $d \geq 2e + 1$ *is gelijkmatig verdeeld met parameter* r *dan en slechts dan als (in* A)

$$\{Y_0 \oplus Y_1 \oplus \ldots \oplus Y_{e-1} \oplus \frac{1}{r}(Y_e \oplus Y_{e+1})\} * C = S_n.$$

BEWIJS. Dit is een direct gevolg van (7.1.9) en (7.4.1). □

(7.4.4) STELLING: *Een code* C *met* $\rho(C) = e + 1$ *en* $d \geq 2e + 1$ *is gelijkmatig verdeeld met parameter* r *dan en slechts dan als voor de Krawtchouk ontwikkeling van* $F_C(x)$ *geldt* $s = e + 1$ *en*

$$\alpha_0 = \alpha_1 = \ldots = \alpha_{e-1} = 1 \text{ en } \alpha_e = \alpha_{e+1} = \frac{1}{r}.$$

BEWIJS.

(i) Als $\alpha_0 = \alpha_1 = \ldots = \alpha_{e-1} = 1$ en $\alpha_e = \alpha_{e+1} = \frac{1}{r}$ dan volgt uit (7.3.3) en (7.4.3) dat C gelijkmatig verdeeld is.

(ii) Laat C gelijkmatig verdeeld zijn. De graad s van $F_C(x)$ is $\geq e+1$. Zij verder $F(x)$ het polynoom $\sum_{i=0}^{e+1} \alpha_i K_i(n,x)$ met $\alpha_0 = \alpha_1 = \ldots = \alpha_{e-1} = 1$, $\alpha_e = \alpha_{e+1} = \frac{1}{r}$. Als $\underline{u} \in X$ en $w(\underline{u}) = j \neq 0$ en $\chi_{\underline{u}}(C) \neq 0$, dan is op grond van (7.4.3), (7.2.3), (7.2.6) en (7.2.10) $F(j) = 0$. Dus is op grond van (7.3.2) het polynoom $F(x)$ deelbaar door $F_C(x)$. Dus is $s = e + 1$ en $F(x) = aF_C(x)$ voor zekere a. Daar $F(0) = 2^n|C|^{-1}$, volgens (7.4.3), is $a = 1$. □

Uit het bewijs van (7.4.4) volgt de volgende uitbreiding van een stelling die door S.P. Lloyd voor lineaire perfecte codes is bewezen (zie LLOYD (1957)).

(7.4.5) STELLING. *Als een gelijkmatig verdeelde code* C *met* $\rho(C) = e + 1$ *en* $d \geq 2e + 1$ *bestaat dan heeft*

$$F(x) := \sum_{i=0}^{e-1} K_i(n,x) + \frac{1}{r}\{K_e(n,x) + K_{e+1}(n,x)\}$$

$e + 1$ *verschillende gehele nulpunten op* $[1,n]$ *en verder is* $F(0) = 2^n|C|^{-1}$.

Merk op dat de eis betreffende F(0) volgens (7.2.5) neerkomt op

$$(7.4.6) \qquad |C|\left\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}\binom{n+1}{e+1}\right\} = 2^n,$$

hetgeen de tellende vorm van (7.4.3) is.
Bij een willekeurige code C geldt (7.4.6) als we r interpreteren als het *gemiddelde* aantal code woorden op afstand e of e + 1 tot de woorden $\underline{u}$ met $\rho(\underline{u},C) \geq e$.

We zullen het bewijs hier niet geven maar we merken op dat m.b.v. (7.3.6) is aan te tonen dat gelijkmatig verdeelde codes volledig regulier zijn.

In het algemeen is de definitie (7.4.1) niet een eenvoudige manier om na te gaan of een bepaalde code gelijkmatig verdeeld is. We zullen nu aantonen dat voor een lineaire code C met e = 1 veel eenvoudiger is na te gaan of C gelijkmatig verdeeld is. Volgens (7.4.4) moet $F_C(x)$ graad 2 hebben. In de opmerking na (7.3.2) zagen we dat dit betekent dat in $C^\perp$ slechts 2 gewichten w_1 en w_2 ($\neq 0$) voorkomen. Laat omgekeerd $C^\perp$ deze eigenschap hebben, dus

$$W_{C^\perp}(z) = 1 + N_1 z^{w_1} + N_2 z^{w_2} .$$

We vullen (7.2.7) in (7.3.6) in en gebruiken het feit dat $d \geq 3$. Dit geeft ons 3 vergelijkingen

$$1 + N_1 + N_2 = 2^n|C|^{-1}$$

en

$$K_k(n,0) + N_1K_k(n,w_1) + N_2K_k(n,w_2) = 0 \qquad (k=1,2).$$

Wederom gebruik makend van de opmerking na (7.3.2) zien we dat $F_C(x)$ graad 2 heeft en dat $F_C(w_1) = F_C(w_2) = 0$ en $F_C(0) = 2^n|C|^{-1}$. Voor de coëfficiënten $\alpha_0,\alpha_1,\alpha_2$ in de Krawtchouk ontwikkeling van $F_C(x)$ vinden we zo m.b.v. (7.2.5)

$$\alpha_0 + \alpha_1 n + \alpha_2\binom{n}{2} = 2^n|C|^{-1},$$

$$\alpha_0 + \alpha_1(n-2w_i) + \alpha_2\left\{2w_i^2 - 2nw_i + \binom{n}{2}\right\} = 0 \qquad (i=1,2)$$

Door combinatie met de vergelijkingen voor N_1 en N_2 volgt dan $\alpha_0 = 1$. Definiëren we nog

$$r := 2(n+1)w_1 - 2w_1^2 - \frac{n(n+1)}{2}$$

dan is $\alpha_1 = \alpha_2 = \frac{1}{r}$ onder de voorwaarde $w_1 + w_2 = n + 1$.

We hebben dus bewezen:

(7.4.7) <u>STELLING</u>: *Een lineaire code* C *met* $\rho(C) = 2$, $d \geq 3$ *is gelijkmatig verdeeld dan en slechts dan als in* $C^\perp$ *slechts twee gewichten* w_1 *en* w_2 *voorkomen met* $w_1 + w_2 = n + 1$.

(lit. GOETHALS & VAN TILBORG (1975)).

7.5. VOORBEELDEN

(7.5.1) In ons eerste voorbeeld gebruiken we voor de twee symbolen van het alfabet + en - i.p.v. 0 en 1. Zij H_{12} een Hadamard matrix van de orde 12. Definieer de code C door van de 24 woorden van H_{12} en $-H_{12}$ de eerste letter weg te laten. We vinden zo een code C met $n = 11$ en $d = 5$ (zie § 2.2).

Een willekeurig woord $\underline{z}$ heeft afstand 2 of 3 tot ten hoogste 4 codewoorden. Deze situatie kan alleen als volgt ontstaan: na vermenigvuldiging van zekere coördinaten met - 1 en na permutatie zijn z en de vier codewoorden $\underline{x}_i$

$$\begin{array}{lllll} \underline{z} = & - - & + + + & + + + & + + + \\ \underline{x}_1 = & + + & + + + & + + + & + + + \\ \underline{x}_2 = & - - & - - - & + + + & + + + \\ \underline{x}_3 = & - - & + + + & - - - & + + + \\ \underline{x}_4 = & - - & + + + & + + + & - - - \end{array}$$

Dit betekent dat H_{12} vier rijen $(+,\underline{x}_1)$, $(-,\underline{x}_2)$, $(-,\underline{x}_3)$, $(-,\underline{x}_4)$ heeft. De rij $(-4,-4,-4,0,0,\ldots,0)$ is een lineaire combinatie van deze vier en deze rij kan niet inproduct 0 met een $\pm$ rij hebben. We zien uit (7.4.6) door invullen van $|C| = 24$ en $n = 11$ dat gemiddeld de woorden $\underline{z}$ met $\rho(\underline{z},C) > 1$ tot 3 codewoorden afstand 2 of 3 hebben. Dus moet ieder van deze $\underline{z}$ afstand 2 of 3 tot precies 3 codewoorden hebben. Dus is C gelijkmatig verdeeld met $r = 3$. (zie VAN LINT (1974)).

(7.5.2) Zij V de 6 dimensionale vectorruimte over GF(2) en zij W de verzameling van de 35 punten $\underline{x}$ in $V\backslash\{0\}$ op de kwadriek

$$x_1x_2 + x_3x_4 + x_5x_6 = 0.$$

We nummeren deze 35 elementen $\underline{w}_1,\underline{w}_2,\ldots\underline{w}_{35}$.

We schrijven deze 35 vectoren als kolommen van een 6×35 matrix G. Dus

$$(G)_{i,j} = (w_j)_i, \text{ de } i^{de} \text{ coördinaat van } w_j.$$

In woorden: i^{de} rij van G is de karakteristieke vector van de doorsnijding van W met het hypervlak $x_i = 1$. Evenzo is $\underline{a}^TG$, $\underline{a} \in V$, de karakteristieke vector van de doorsnijding van W met het hypervlak $\sum_{i=1}^{6} a_ix_i = 1$. Het gewicht van $\underline{a}^TG$ is dus het aantal oplossingen in V van

$$x_1x_2 + x_3x_4 + x_5x_6 = 0$$

en

$$\sum_{i=1}^{6} a_ix_i = 1.$$

Als $\underline{a} \neq 0$ mogen we zonder verlies van algemeenheid aannemen dat $a_1 = 1$. Substitutie levert dan dat we de oplossingen tellen van

$$(1+a_2x_2+a_3x_3+\ldots+a_6x_6)x_2 + x_3x_4 + x_5x_6 = 0,$$

ofwel

$$(1+a_2+a_3a_4+a_5a_6)x_2 + (x_3+a_4x_2)(x_4+a_3x_2) + (x_5+a_6x_2)(x_6+a_5x_2) = 0$$

Daar de affiene transformatie, gegeven door

$$x_2 \to y_2,\quad x_3 + a_4x_2 \to y_3,\quad x_5 + a_6x_2 \to y_5,$$
$$x_4 + a_3x_2 \to y_4,\quad x_6 + a_5x_2 \to y_6,$$

inverteerbaar is, tellen we eigenlijk de oplossingen van

$$(1+a_2+a_3+a_4+a_5a_6)y_2 + y_3y_4 + y_5y_6 = 0.$$

Als de coëfficient van y_2 gelijk is aan 1, dan is dit 16 en anders 20.

Zij C nu de code met lengte 35 die G als parity check matrix heeft. Daar de kolommen van G allen verschillend zijn geldt dat $d \geq 3$. Hierboven is nu bewezen dat $F_C(x) = 2^6(1-\frac{x}{16})(1-\frac{x}{20})$.

Vanwege de opmerking onder (7.3.5) geldt $\rho(C) = 2$. Daar $16 + 20 = 35 + 1$, volgt uit stelling (7.4.7) dat C gelijkmatig verdeeld is (met $r = 10$).
(Zie GOETHALS & VAN TILBORG (1975)).

(7.5.3) Zij α een primitief element van $GF(2^5)$, $m_1(x)$ het minimaalpolynoom van α en $m_3(x)$ dat van α^3. De cyclische code H van lengte 31 met voortbrenger $m_1(x)$ is de Hamming code; de code B met voortbrenger $(x-1)m_1(x)m_3(x)$ is een BCH code met minimum afstand ≥ 6 welke bevat is in H. Zij $u(x) = x^{30} + x^{29} + \ldots + 1$ het woord met alle coördinaten 1.

We definieren een lineaire code C van dimensie 47 en lengte 63 door

$$C := \{(m(x),\ i,\ m(x) + (m(1)+i)u(x) + s(x)) \mid m(x) \in H,\ i \in \{0,1\},\ s(x) \in B\}.$$

Om het minimum gewicht van C te bepalen onderscheiden we 3 gevallen:

(i) $m(x) = 0$, $i = 0$, $s(x) \neq 0$. Nu is $w(s(x)) \geq 6$.

(ii) $m(x) = 0$, $i = 1$. Nu is $u(x) + s(x) \neq 0$ daar $u(x) \notin B$. Verder is $u(\alpha) + s(\alpha) = u(\alpha^3) + s(\alpha^3) = 0$. Dus is volgens BCH-grens het gewicht van $u(x) + s(x)$ tenminste 5.

(iii) $m(x) \neq 0$. Daar $m(x) + (m(1)+i)u(x) + s(x) \in H$ hebben we weer een woord van gewicht ≥ 6 tenzij $m(x) + (m(1)+i)u(x) + s(x) = 0$. Dit kan echter alleen als $m(\alpha^3) = 0$, d.w.x. $m(x) \in B$, dus het gewicht van $m(x) \geq 5$.

Uit (i), (ii) en (iii) volgt dat C minimum afstand ≥ 5 heeft.

De cyclische code H^* met voortbrenger $(x^{31}-1)/m_1(x)$ is een lichaam (zie § 5.2). Zij $f(x)$ het eenheidselement in dit lichaam (zie (5.4.1).) De bol S_1 in de ruimte van dimensie 31 bestaat uit $0,1,x,x^2,\ldots,x^{30}$. Aan ieder element $q(x)$ van S_1 voegen we toe het woord $(q(x),0,q(x)f(x))$. De collectie woorden van lengte 63 die zo ontstaat noemen we $\hat{S}_1$.

(7.5.4) <u>DEFINITIE</u>: De Preparata code K van lengte 63 is de vereniging van de nevenklassen van C met een representant in $\hat{S}_1$.

Om de minimum afstand van K (een niet lineaire code) te bepalen gaat men als volgt te werk. Neem een tweetal woorden. Aan de hand van de waarden van $q(x),m(x),s(x)$ en i kan men evenals we bij C gedaan hebben een aantal verschillende gevallen onderscheiden. Het is nogal wat gepruts maar niet wezenlijk lastiger dan wat we boven al hebben gedaan. Het resultaat is dat K minimum afstand 5 heeft. Uit de constructie volgt dat $|K| = 2^{52}$.
(Voor bewijs zie CAMERON & VAN LINT (1975)).

Nu substitueren we in (7.4.6) voor het aantal codewoorden 2^{52}, $n = 63$, $e = 2$ en interpreteren voorlopig r weer als het gemiddeld aantal codewoorden op afstand 2 of 3 van een woord $\underline{z}$ met $\rho(\underline{z},K) > 1$. We vinden dan

$$r = 21 = \frac{n}{e+1} .$$

Op grond van (7.4.2) moeten dan alle $\underline{z}$ met $\rho(\underline{z},K) > 1$ afstand 2 of 3 tot precies 21 codewoorden hebben.

We hebben dus aangetoond dat K een bijna perfecte niet lineaire code is.

7.6. NONEXISTENTIE STELLINGEN

Al enkele jaren is bekend dat de Golay en Hamming codes de enige niet triviale perfecte codes zijn over een alfabet waarvan het aantal elementen een macht van een priemgetal is (zie VAN LINT (1975)). Sinds kort (zie H.C.A. VAN TILBORG (1975)) is nu ook bekend dat er voor $e \geq 3$ zelfs geen andere gelijkmatig verdeelde codes zijn. Om een idee te geven van de bewijsmethodes beginnen we met een schets van het non-existentie bewijs voor perfecte codes.

Neem aan dat er een perfecte code C bestaat met $d = 2e + 1 > 3$ en woordlengte n. We passen nu (7.4.5) toe (met e i.p.v. e+1). We zien dat het in (7.2.11) gedefinieerde polynoom $\Psi_e(x)$ nulpunten $x_1 < x_2 < \ldots < x_e$ heeft die verschillend zijn, geheel, en in [1,n] liggen. Verder is volgens (7.4.5) en (7.2.5)

$$\sum_{i=0}^{e} \binom{n}{i} = 2^n |C|^{-1},$$

en dus is volgens (7.2.12)

$$\prod_{i=1}^{e} x_i = e!\, 2^{\ell} \tag{7.6.1}$$

met gehele ℓ.

Ons bewijs bestaat uit 3 stappen. Voor $x \in \mathbb{N}$ definiëren we A(x) als de grootste oneven deler van x. Uit (7.6.1) volgt

$$\prod_{i=1}^{e} A(x_i) = A(e!) < e! ,$$

d.w.z. er zijn twee nulpunten x_i en x_j met $A(x_i) = A(x_j)$, dus $x_i \leq 2x_j$ (of andersom). Dus is $2x_1 \leq x_e$ en daar met x_i ook $n + 1 - x_i$ een nulpunt van $\Psi_e(x)$ is vinden we

$$x_e - x_1 \geq \frac{1}{3} n. \tag{7.5.2}$$

Als tweede stap beschouwen we (7.2.13) en (7.2.14).
Hieruit volgt

$$\sum_{i=1}^{e}\sum_{j=1}^{e}(x_i-x_j)^2 = \tfrac{1}{2}e^2(e-1)(n-\frac{2e-1}{3}).$$

Hieruit volgt door op te merken dat de linkerkant minimaal is, als functie van $x_2,x_3,\ldots,x_{e-1}$, als alle e-2 variabelen gelijk aan $\frac{1}{2}(x_1+x_e)$ zijn:

(7.6.3) $\quad (x_e-x_1) \le e\,(\tfrac{1}{2}n)^{\frac{1}{2}}.$

Uit (7.6.2) en (7.6.3) volgt

(7.6.4) $\quad n \le \frac{9}{2}e^2.$

Nu beschouwen we (7.2.15) en (7.2.16). Daar voor iedere $x \in \mathbb{N}$ geldt $(x-1)(x-2) \equiv 0 \pmod 2$ vinden we

(7.6.5) $\quad (n-1-2e)(n-1)(n-2)^2(n-3)^2\ldots(n-e)^2 \equiv 0 \pmod{2^{3e}}.$

Zij 2^α de hoogste macht van 2 die een factor $n - j$ in het linkerlid van (7.6.5) deelt. Dan is de hoogste macht van 2 die het linkerlid van (7.6.5) deelt kleiner dan $2^{3\alpha+2e}$. Hieruit volgt $\alpha \ge \frac{1}{3}e$. Dus is

(7.6.6) $\quad n > 2^{\frac{1}{3}e}$ (tenzij $n = 2e+1$).

Voor grote e zijn (7.6.4) en (7.6.6) strijdig. De kleine e, en dus volgens (7.6.4) kleine n leveren eindig veel mogelijkheden die eenvoudig zijn te controleren. Met iets meer moeite kan men het aantal expliciet te controleren gevallen tot enkele beperken. Zo vindt men o.a. dat $e > 2$ alleen mogelijk is voor de Golay code en repetitie codes.

Om alle gelijkmatig verdeelde codes te behandelen zijn nog enkele andere trucs nodig vanwege de extra parameter r.

Analoog aan de perfecte codes vinden we

(7.6.7) $\quad x_{e+1}-x_1 \le (e+1)(\frac{n+1}{2})^{\frac{1}{2}}$

(7.6.8) $\quad n > 2^{\frac{e}{7}}.$

We hernummeren de wortels x_i tot $y_j = A(y_j)2^{\alpha_j}$, zodat

$$\alpha_1 \le \alpha_2 \le \ldots \le \alpha_{e+1}.$$

Nu geldt enerzijds

$$\prod_{i=1}^{e} \frac{|y_i - y_{i+1}|}{y_i} \ge \prod_{i=1}^{e} \frac{\text{g.g.d.}(y_i, y_{i+1})}{y_i} = \prod_{i=1}^{e} \frac{\text{g.g.d.}(A(y_i), A(y_{i+1}))2^{\alpha_i}}{y_i}$$

$$\ge \prod_{i=1}^{e} \frac{1}{A(y_i)} \ge \frac{1}{A(y_1 \cdots y_{e+1})} = \frac{A(|C|)}{A(r)A((e+1)!)} \ge \frac{1}{rA((e+1)!)}$$

en anderzijds

$$\prod_{i=1}^{e} \frac{|y_i - y_{i+1}|}{y_i} \le \frac{(x_{e+1}-x_1)^e}{y_1 \cdots y_e} \le \frac{n(x_{e+1}-x_1)^e}{x_1 x_2 \cdots x_{e+1}} = \frac{n(x_{e+1}-x_1)^e}{r(e+1)!} \frac{2^{e+1}|C|}{2^n}.$$

Derhalve vinden we

$$(x_{e+1}-x_1)^e \ge \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{2^n}{n|C|} \ge$$

$$\ge \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{1}{n} \sum_{i=0}^{e} \binom{n}{i} \ge \frac{(e+1)!}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot \frac{1}{n} \binom{n}{e},$$

dus

(7.6.9) $\quad (x_{e+1}-x_1)^e \ge \frac{e+1}{A((e+1)!)} \cdot \frac{1}{2^{e+1}} \cdot (n-1)(n-2)\ldots(n-e+1).$

Vergelijking van (7.6.7), (7.6.8) en (7.6.9) levert voor $e \ge 3$ een strijdigheid voor alle n en e, behoudens een begrensd gebied dat met verfijnde methodes gecontroleerd kan worden. De gevallen $e = 1$ en $e = 2$ kunnen direct met (7.4.5) behandeld worden.

We besluiten dit hoofdstuk met een tabel van alle perfecte, bijna perfecte en gelijkmatig verdeelde binaire codes.

e	n	$\|C\|$	type	naam
0	n	2^n	perfect	$\{0,1\}^n$
1	2^m-1	2^{n-m}	perfect	Hamming *)
1	2^m-2	2^{n-m}	bijna perfect	verkorte Hamming
1	$2^{2m-1}\pm 2^{m-1}-1$	2^{n-2m}	gelijkmatig verdeeld	projectieve code
2	$2^{2m}-1$	2^{n+1-4m}	bijna perfect	Preparata
2	$2^{2m+1}-1$	2^{n-4m-2}	gelijkmatig verdeeld	B.C.H.
2	11	24	gelijkmatig verdeeld	Hadamard
3	23	2^{12}	perfect	Golay
e	2e+1	2	perfect	repetitie
e	e	1	perfect	triviaal

*) Er zijn ook niet lineaire perfecte codes met e = 1.

Hoofdstuk VIII

GOPPA CODES

8.1. MOTIVATIE

Zoals een ieder zich zal herinneren ziet de parity check matrix van een BCH-code met ontwerp afstand d eruit als

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots\beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \dots\beta^{2(n-1)} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & \beta^{d-1} & \beta^{(d-1)2} & \dots\beta^{(d-1)(n-1)} \end{pmatrix}$$

waarbij β een primitieve n-de machts eenheidswortel in $GF(q^m)$ is, opgevat als kolomvector ter hoogte m met coordinaten in $GF(q)$.
[Hierbij is $n|q^m-1$, anders is er niet zo'n β.]

De reden dat het minimumgewicht van de code tenminste d is, is het feit dat de determinant op d-1 kolommen van H (opgevat als matrix over $GF(q^m)$) een Vandermonde determinant en dus ongelijk aan nul is.

Het is verschillende mensen opgevallen dat dezelfde redenering ook werkt voor de algemenere

$$H = \begin{pmatrix} h_0\beta_0 & h_1\beta_1 & \dots & h_{n-1}\beta_{n-1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ h_0\beta_0^{d-1} & h_1\beta_1^{d-1} & \dots & h_{n-1}\beta_{n-1}^{d-1} \end{pmatrix}$$

waarbij $h_j \in GF(q^m)\backslash\{0\}$, en alle β_i onderling verschillende elementen van $GF(q^m)\backslash\{0\}$ zijn. Als $h_j \in GF(q)$ (en i.h.b. als m=1) dan heeft de factor h_j hoegenaamd geen effect op de code: alleen de symbolen van het alfabet hebben nieuwe namen gekregen (op positie j). Met $h_j \in GF(q^m)$ echter kan $h_j\beta_i^t$ (opgevat als kolomvector over $GF(q)$) totaal verschillen van β_i^t.

Dat dit een echte verrijking is blijkt uit het feit dat BCH codes

asymptotisch slecht zijn terwijl deze gegeneraliseerde BCH codes de Gilbert bound halen (zie (4.2.2)).

8.2. GOPPA CODES

Zij $g(z)$ een polynoom van graad t over $GF(q^m)$. Zij $L = \{\gamma_1,\ldots,\gamma_n\} \subset GF(q^m)$, zodat $n = |L|$, een verzameling niet-nul punten van $g(z)$.

Dan wordt de Goppa code met Goppa polynoom $g(z)$ gedefinieerd als de verzameling van alle codewoorden $c = (c_\gamma) = (c_{\gamma_1},\ldots,c_{\gamma_n})$ over het alfabet $GF(q)$ met plaatsen geïndiceerd door L zodanig dat

$$\sum_{\gamma\in L} \frac{c_\gamma}{z-\gamma} \equiv 0 \pmod{g(z)}.$$

[Hierin stelt $\frac{1}{z-\gamma}$ het modulo $g(z)$ uniek bepaalde polynoom voor waarvoor $(z-\gamma)\cdot\frac{1}{z-\gamma} \equiv 1 \pmod{g(z)}$.]

Het is duidelijk dat Goppa codes lineair zijn. Laten we de parity check matrix uitrekenen:
aangezien

$$\frac{1}{z-\gamma} \equiv \frac{-1}{g(\gamma)} \cdot \left(\frac{g(z)-g(\gamma)}{z-\gamma}\right) \pmod{g(z)},$$

waarbij het rechterlid een polynoom van graad $< t$ is, wordt de parity check matrix voor de code gegeven door de rij

$$\left(\frac{1}{g(\gamma_1)} \cdot \frac{g(z)-g(\gamma_1)}{z-\gamma_1}, \quad \ldots \quad, \frac{1}{g(\gamma_n)} \cdot \frac{g(z)-g(\gamma_n)}{z-\gamma_n}\right).$$

Zij $h_j = g(\gamma_j)^{-1}$, dan is $h_j \neq 0$.

Als $g(z) = \sum_{i=0}^{t} g_i z^i$ dan vinden we na scheiding van de machten van z (merk op dat $\frac{g(z)-g(x)}{z-x} = \sum_i \sum_j g_{i+j+1}\, x^j z^i$):

$$\begin{pmatrix} h_1 g_t & \cdots & h_n g_t \\ h_1(g_{t-1}+g_t\gamma_1) & \cdots & h_n(g_{t-1}+g_t\gamma_n) \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ h_1(g_1+g_2\gamma_1+\ldots+g_t\gamma_1^{t-1}) & \cdots & h_n(g_1+g_2\gamma_n+\ldots+g_t\gamma_n^{t-1}) \end{pmatrix} .$$

Dit is een lineaire transformatie van (en equivalent met) de matrix die we hebben willen:

$$H = \begin{pmatrix} h_1 & \cdots & h_n \\ h_1\gamma_1 & \cdots & h_n\gamma_n \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ h_1\gamma_1^{t-1} & \cdots & h_n\gamma_n^{t-1} \end{pmatrix}$$

(merk op dat $g_t \neq 0$).

Het blijkt uit deze afleiding dat de minimale afstand van een Goppa code met Goppa polynoom $g(z)$ tenminste $1 + \text{graad}(g(z))$ is. (Ter vergelijking: bij cyclische codes en BCH codes kan in het algemeen niets gezegd worden over d als alleen de graad van het generator polynoom bekend is.)

(8.2.1) <u>VOORBEELD</u>: Iedere BCH code is een Goppa code.
Want: zij β een primitieve n-de machts eenheidswortel in $GF(q^m)$.
De BCH code met ontwerpafstand d is de Goppa code met Goppa polynoom $g(z) = z^{d-1}$ en $L = \{\beta^{-j} | 0 \leq j \leq n-1\}$.
(Opm.: In de literatuur wordt - ten onrechte - gesteld dat alleen primitieve BCH codes onder de Goppa codes vallen.)

Merk op dat hoewel de parity check matrix H hierboven grote gelijkenis vertoont met de in § 8.1 gegevene, deze toch iets minder algemeen is, daar de factoren h_j hier niet willekeurig gekozen kunnen worden. Immers, de $h_j^{-1} = g(\gamma_j)$ zijn functiewaarden van een polynoom van graad t.

8.3. MINIMUM AFSTAND VAN GOPPA CODES

Een ietwat andere manier om de Goppa codes te bekijken levert snel

schattingen voor de minimale afstand:

Zij S de n-dimensionale vectorruimte over GF(q) met Hamming metriek. Zij

$$R = \{\xi(z) = \sum_{i=1}^{n} \frac{b_i}{z-\gamma_i} \mid (b_1,\ldots,b_n) \in S\}$$

waarbij

$$L = \{\gamma_1,\ldots,\gamma_n\} \subset GF(q^m), \text{ met metriek}$$

$$d(\xi(z), \eta(z)) = \| \xi(z) - \eta(z) \|,$$

waarbij $\|\xi(z)\|$ = graad van de noemer van $\xi(z)$ wanneer als onvereenvoudigbare breuk $\frac{t(z)}{n(z)}$ geschreven.

Onmiddellijk blijkt dat de afbeelding $(b_1,\ldots,b_n) \longmapsto \sum_{i=1}^{n} \frac{b_i}{z-\gamma_i}$ een lineaire isometrie van S op R is, zodat een code als deelverzameling van R opgevat kan worden.

Zij nu $\xi(z) = \frac{t(z)}{n(z)} \in R\backslash\{0\}$. Dan is graad $n(z) \geq$ graad $t(z) + 1$ zodat de eis $\xi(z) \equiv 0 \pmod{g(z)}$ impliceert dat $g(z) | t(z)$ en $\| \xi(z) \|$ = graad $n(z)$ $\geq$ graad $t(z) + 1 \geq$ graad $g(z) + 1$. Dit is onze oude schatting $d_{min} \geq$ graad $g(z) + 1$.

Uit de afleiding blijkt dat de schatting verbeterd wordt als graad $n(z)$ - graad $t(z) > 1$. De coëfficiënt van z^{n-1} in $t(z)$ is $\sum_{i=1}^{n} b_i$, dus toevoeging van de parity check $\sum_{i=i}^{n} b_i = 0$ vermindert de dimensie met (ten hoogste) 1 en vergroot (de schatting voor) d_{min} met 1.

Oorspronkelijk hadden we een (n,n-tm,t+1)-code, nu krijgen we een (n,n-tm-1,t+2)-code.

Dit proces kan herhaald worden: de coëfficiënt van z^{n-s-1} in de teller is $(-1)^s \sum_{i=1}^{n} b_i \sum_{j_1\ldots j_s \neq i} \gamma_{j_1}\ldots\gamma_{j_s}$. Deze coëfficiënt kan uitgedrukt worden in de sommen $\sum_{i=1}^{n} b_i\gamma_i^{\,r}$ $(0 \leq r \leq s)$, d.w.z. als we de s + 1 parity checks $\sum_{i=1}^{n} b_i\gamma_i^r = 0$ $(0 \leq r \leq s)$ toevoegen dan krijgen we een (n,n-1-(t+s)m,(t+s)+2)-code.

Natuurlijk had dit effect ook bereikt kunnen worden door voor de graad van g(z) de waarde t + s te kiezen, maar op deze manier krijgen we tenminste eens in de q keer een onverwachte meevaller: uit $\sum b_i\gamma_i = 0$ volgt $\sum b_i\gamma_i^q = 0$ d.w.z. deze laatste parity check vermindert de dimensie niet.

Merk op dat wat we hier bekijken in feite de doorsnede van een BCH-code en een Goppa code is.

In het binaire geval kan de schatting voor d_{min} soms aanzienlijk verscherpt worden:

Laat met het codewoord $(c_1,\ldots,c_n)$ het polynoom $f(z) = \prod_{i=1}^{n} (z-\gamma_i)^{c_i}$ corresponderen. Nu is $\xi(z) = \sum_{i=1}^{n} \frac{c_i}{z-\gamma_i} = \frac{f'(z)}{f(z)}$. Als nu g(z) geen meervoudige wortels heeft dan volgt omdat f'(z) een volkomen kwadraat is (*alle voorkomende machten van z zijn even*): $g(z)^2 | f'(z)$ en $d_{min} \geq 2$ graad g(z) + 1.

Beide verscherpingen zijn onafhankelijk: ook in het binaire geval levert toevoegen van een parity check of doorsnijden met een BCH code weer de geschetste resultaten.

8.4. ASYMPTOTISCH GEDRAG VAN GOPPA CODES

Terwijl de BCH codes te mooi zijn om asymptotisch goed te kunnen zijn (het is bekend dat als in een rij codes met $n \to \infty$ en $d/n > \delta > 0$ alle codes invariant zijn onder een affiene permutatiegroep, dan is $\lim k/n = 0$ (zie LIN & WELDON (1967), KASAMI (1969)), geeft de mogelijkheid tot geschikte keuze van het Goppa polynoom g(z) voldoende vrijheid om de Gilbert bound (bijna) te halen:
Bekijk elk van de $(q-1)^d\binom{n}{d}$ woorden $(c_1,\ldots,c_n)$ met gewicht d. Zo'n woord zit in ten hoogste $\lfloor\frac{d-1}{t}\rfloor$ Goppa codes met irreducibel Goppa polynoom van de graad t (immers, elk van die polynomen deelt de teller van $\sum_{i=1}^{n} \frac{c_i}{z-\gamma_i}$). Dus als $\sum_{d=0}^{n} \lfloor\frac{d-1}{t}\rfloor (q-1)^d \binom{n}{d}$ kleiner is dan het aantal irreducibele monische polynomen over $GF(q^m)$ van graad t dan zijn er zeker Goppa codes met $d_{min} > D$, en rate $R \geqq 1 - \frac{mt}{n}$. Maar het aantal irreducibele polynomen van graad t is (cf. BERLEKAMP (1968)):

$$\frac{1}{t} \sum_{d|t} \mu(d) q^{mt/d} \geq \frac{q^{mt}}{t} (1 - q^{-(mt/2)+1}),$$

zodat (met $n=q^m$ en $t=n(1-R)/m$) een voldoende voorwaarde wordt (asymptotisch)

$$\sum_{d=0}^{D} (q-1)^d \binom{n}{d} < q^{(1-R)n}/D.$$

Dit is asymptotisch nauwelijks zwakker dan de Gilbert bound:

$$\sum_{d=0}^{D} (q-1)^d \binom{n}{d} < q^{(1-R)n}$$

8.5. HET MATTSON-SOLOMON POLYNOOM

Zoals al door Goppa aangegeven en recentelijk door CHIEN & CHOY (1975) verder uitgewerkt is, is de eis $\sum_{i=1}^{n} \frac{c_i}{z-\gamma_i} \equiv 0 \pmod{g(z)}$ in feite een deelbaarheidseis voor de Fourier getransformeerde (FT) van het polynoom $c(x) = \sum_{i=1}^{n} c_i x^i$.

De algemene theorie gaat ongeveer als volgt:

Zij $q = p^f$, $n|q^m-1$.

Zij T de verzameling van polynomen over $GF(q^m)$ van graad ten hoogste n.

Zij α een primitieve n-de machts eenheidswortel in $GF(q^m)$. Als $a(x) = \sum_{i=0}^{n-1} a_i x^i \in T$ dan is de Fourier getransformeerde (het Mattson-Solomon polynoom) van a(x) t.o.v. α:

$$(\Phi a)(X) = A(X) = \sum_{j=0}^{n-1} A_j X^j \in T$$

waarbij $A_j = a(\alpha^j)$. Aangezien

$$A(\alpha^{-k}) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i \alpha^{ij} \alpha^{-kj} = na_k$$

wordt de inverse transformatie gedefinieerd door

$$(\Phi^{-1}A)\ (x) = a(x) = \sum_{i=0}^{n-1} a_i x^i$$

waarbij $a_i = n^{-1}A(\alpha^{-i})$ en n^{-1} de inverse van n modulo p is. (In het bijzonder is $a_i = A(\alpha^{-i})$ als $p = 2$.)

De FT definieert een isomorfie tussen twee ringstructuren op T:

Zij $\circ$ vermenigvuldiging van polynomen modulo x^n-1, en zij $*$ gedefinieerd door

$$(\sum a_i x^i) * (\sum b_i x^i) := \sum a_i b_i x^i.$$

Dan is

$$\Phi\ (a \circ b) = \Phi a * \Phi b.$$

Het nut voor de coderingstheorie blijkt uit de volgende stelling.

(8.5.1) STELLING. *Zij* $a(x) \in T$. *Dan is het gewicht van* $a(x)$:

$$n - \text{graad}\ \{\text{ggd}\ (\Phi a,\ X^n-1)\}.$$

BEWIJS. $a_i = n^{-1}\Phi a(\alpha^{-1})$ d.w.z. het aantal coëfficiënten van $a(x)$ die gelijk aan nul zijn is gelijk aan het aantal gemeenschappelijke nulpunten van Φa en X^n-1. □

Merk op dat alle nulpunten van X^n-1 verschillend zijn.

Wil men dus garanderen dat alle vectoren $a(x)$ uit de code een hoog gewicht hebben dan moet men zorgen dat de graad van ggd $(\Phi a,\ X^n-1)$ klein is.

Bij BCH codes wordt hiervoor gezorgd door graad $\Phi(a)$ klein te nemen: eis van alle codewoorden dat ze nulpunten in $\alpha^{n-1},\ldots,\alpha^{n-t}$ hebben. Dit is echter niet nodig; Φa mag wel een hoge graad hebben, als dit maar veroorzaakt wordt door factoren die X^n-1 niet delen.

Dit leidt tot de volgende definitie van gegeneraliseerde BCH codes (GBCH codes):

Zij $S \subset T$ de verzameling van de polynomen in T met coëffiënten in $GF(q)$.

Laten $P(X)$ en $G(X)$ twee polynomen uit T zijn met

$$\text{ggd } (P(X),\ X^n-1) = \text{ggd } (G(X),\ X^n-1) = 1.$$

De GBCH code over GF(q) met lengte n en polynomenpaar (P(X), G(X)) wordt gedefinieerd als

$$C = \{v(x) \in S \mid P(X) \circ \Phi v\ (X) \equiv 0 \bmod G(X)\}.$$

C is kennelijk een lineaire code.

Een gemeenschappelijke factor f(X) van Φv en X^n-1 zit ook in $P(X) \circ \Phi v\ (X)$. Maar $G(X) \mid (P(X) \circ \Phi v\ (X))$ en ggd (f(X), G(X)) = 1. Dus de graad van f(X) is ten hoogste n-1-graad {G(X)}. Uit stelling (8.5.1) volgt dan dat de code een minimale afstand tenminste 1 + graad {G(X)} heeft.

(8.5.2) <u>VOORBEELD</u>. Zij $P(X) = X^{n-1}$, $G(X) = X^{d-1}$ dan $C = \{v(x) \in S \mid v(\alpha) = \ldots = v(\alpha^{d-1}) = 0\}$, de BCH code met ontwerpafstand d. De GBCH codes zijn dus inderdaad algemener dan de BCH codes (en geven dezelfde schatting voor d_{min}).

Het is geen toeval dat hier G(X) dezelfde waarde heeft als in het Goppa voorbeeld, want algemener geldt:

$$\text{zij } P(X) = X^{n-1},\ G(X) \text{ zonder nulpunten in } GF(q^m)\backslash\{0\};$$

dan is de bijbehorende code C de Goppa code met Goppa polynoom G(X) en $L = GF(q^m)\backslash\{0\} = \{1, \alpha, \ldots, \alpha^{n-1}\}$.

Op grond van dit voorbeeld beweren Chien & Choy dat de GBCH codes de Goppa codes bevatten. Goppa levert echter codes voor iedere $n \le q^m$ en niet alleen voor $n \mid q^m-1$ zodat deze bewering ongegrond is.

Wel is het zo dat de GBCH codes de parity check matrix leveren die in § 8.1 als doel gesteld werd:

$$\text{Zij } p(x) = (\Phi^{-1} P)(x) = \sum_{i=0}^{n-1} p_i x^i \text{ en } g(x) = (\Phi^{-1} G)(x) = \sum_{i=0}^{n-1} g_i x^i.$$

Nu geldt $p_i \neq 0$ en $g_i \neq 0$ $(0 \le i \le n-1)$ omdat $\text{ggd}(P(X), X^n-1) = \text{ggd}(G(X), X^n-1) = 1$. Is v(x) een codewoord, en $V(X) = (\Phi v)(X)$ dan geldt $P(X) \circ V(X) \equiv 0 \bmod G(X)$ d.w.z. er is een polynoom A(X) van graad ten hoogste n - 1 - graad {G(X)} zodanig dat

$$P(X) \circ V(X) = A(X)\ G(X) = A(X) \circ G(X).$$

Is $a(x) = (\Phi^{-1}A)(x) = \sum_{i=0}^{n-1} a_i x^i$ dan volgt

$$p(x) * v(x) = a(x) * g(x)$$

of wel

$$\sum_{i=0}^{n-1} p_i v_i x^i = \sum_{i=0}^{n-1} a_i g_i x^i$$

of wel $a_i = p_i g_i^{-1} v_i$ $(0 \le i \le n-1)$. Als nu $h_i = p_i g_i^{-1}$ dan volgt uit $a(\alpha^{n-j}) =$
$= \sum_{i=0}^{n-1} a_i\ \alpha^{i(n-j)} = \sum_{i=0}^{n-1} v_i h_i\ \alpha^{i(n-j)} = A_{n-j} = 0 (1 \le j \le$ graad $G(X))$ dat $vH^T = 0$
wanneer

$$H = \begin{pmatrix} h_0 & h_1\alpha^{n-1} & \dots & h_{n-1}\alpha^{(n-1)(n-1)} \\ h_0 & h_1\alpha^{n-2} & \dots & h_{n-1}\alpha^{(n-2)(n-1)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ h_0 & h_1\alpha^{n-t} & \dots & h_{n-1}\alpha^{(n-t)(n-1)} \end{pmatrix}$$

Omgekeerd volgt uit $vH^T = 0$ weer dat graad $A(X) \le n - 1 -$ graad$(G(X))$ dus $A(X)\ G(X) = A(X) \circ G(X)$ en $v \in C$. Dus H is een parity-check matrix voor C.

8.6. COMMENTAAR

Voor de publicatie van zijn nieuwe codes kreeg GOPPA (1973, 1973a, 1974) een prijs van de IEEE. Inmiddels is er al veel over deze codes geschreven. Goppa zelf gaf in zijn eerste artikel een decodeeralgorithme. Later toonde RETTER (1975) aan dat men een BCH-decoder gebruiken kan om Goppa codes te decoderen. Op BCH codes na zijn Goppa codes niet cyclisch maar BERLEKAMP en MORENO (1973) gaven een eenvoudig bewijs dat een verlengde 2-fouten-verbeterende Goppa code cyclisch is. Later toonden TZENG en

ZIMMERMAN (1975) aan dat diverse Goppa codes door verlenging cyclisch worden.

8.7. OPGAVEN

(8.7.1) Zij C_1 een BCH code met ontwerpafstand d_1 en zij C_2 een Goppa code met ontwerpafstand d_2, met $n = q^m-1$, $L = GF(q^m)\backslash\{0\}$. Dan heeft $C_1 \cap C_2$ een minimum afstand $d \geq d_1 + d_2 - 1$ en de verlengde code zelfs afstand $\geq d_1 + d_2$. Bewijs dit.

(8.7.2) Toon aan dat de GBCH-code gedefinieerd door een polynomenpaar $(P(X),G(X))$ alleen afhangt van $P(X)G(X)^{-1}$ en graad $(G(X))$ zodat deze code ook gedefinieerd kan worden met het paar $(P_1(X),X^t)$ voor zekere $P_1(X)$ en t.

Hoofdstuk IX

ASYMPTOTISCH GOEDE ALGEBRAISCHE CODES

9.1. EEN EENVOUDIG NIET-CONSTRUCTIEF BEWIJS

We hebben inmiddels vele methoden leren kennen om codes te construeren. Als we voor deze constructies nagaan hoe hun plaats in de figuur van hoofdstuk IV zou zijn dan wacht ons een teleurstelling. Voor de Hadamard codes uit § 2.2 nadert als $n \to \infty$ de rate R tot 0 en de grootheid δ uit § 4.1 (minimum afstand gedeeld door woordlengte) is steeds $\frac{1}{2}$. Dit levert een punt op de kromme voor de Gilbert bound (en op de δ-as). Voor Hamming codes nadert R tot 1 maar δ tot 0. Dit levert ons het andere eind van de kromme voor de Gilbert bound. De andere constructies zoals BCH, RS, etc. leveren slechts punten op de as. Steeds blijkt dat bij vaste R de grootheid δ tot 0 nadert. We zullen nu aantonen dat een eenvoudig algebraisch voorschrift toch goede codes kan leveren maar de methode is helaas niet constructief.

We beperken ons tot $R = \frac{1}{2}$ (zie (9.5.1)). Bij vaste m kiezen we $\alpha = \alpha_m \in GF(2^m)$. Hoe α gekozen moet worden zullen we direct zien. We construeren nu de lineaire code C_α (een (2m,m)-code) door een rij $\underline{a} := (a_1, a_2, \ldots, a_m)$ van informatie-symbolen op te vatten als element van $GF(2^m)$ (dit is immers een m-dimensionale vectorruimte over GF(2)) en hieraan toe te voegen het codewoord $(\underline{a}, \alpha\underline{a})$. Bij gegeven $\lambda = \lambda_m$ vragen we ons af of de code C_α een woord $\neq \underline{0}$ bevat met gewicht kleiner dan $\lambda.2m$. Als dit het geval is kunnen we de tweede helft van dit woord door de eerste helft delen en α bepalen. Dit betekent dat er ten hoogste $\sum_{i<2\lambda m} \binom{2m}{i}$ waarden van α zijn zó dat de minimum afstand d van C_α minder dan $2\lambda m$ is. Kies nu $\lambda := H^{\leftarrow}\left(\frac{1}{2} - \frac{1}{\log m}\right)$. Volgens (0.4.5.(i)) is het aantal "slechte" keuzen van α dan $o(2^m)$. Hiermee is aangetoond dat voor bijna alle keuzen van α geldt

$$d \geq 2m\, H^{\leftarrow}\left(\frac{1}{2} - \frac{1}{\log m}\right).$$

We hebben nu voor rate $\frac{1}{2}$ een rij codes waarvoor geldt

$$\delta = H^{\leftarrow}(\tfrac{1}{2}) + o(1).$$

Deze rij codes haalt dus de Gilbert bound (4.2.5). Als we nu nog konden

aangeven (en wel expliciet) hoe α_m moet worden gekozen zou dit een sensationeel resultaat zijn. Tot voor enkele jaren twijfelde men er aan of een expliciete algebraische constructie van een rij codes met toenemende woordlengte en liminf $d/n > 0$ wel mogelijk is. In de volgende paragrafen geven we de nu bekende oplossing.

9.2. JUSTESEN CODES

De door JUSTESEN (1973) geconstrueerde codes zijn een generalisatie van de door FORNEY (1966) ontwikkelde *concatenated codes*. Beschouw de woorden (of delen daarvan) van een code C_1 als letters van een nieuw alfabet. Met deze letters maken we een nieuwe code C_2. Het procédé van coderen en decoderen gebeurt dan in 2 trappen. We beschouwen dit in iets meer detail. Laat C_2 een code zijn over $GF(2^m)$. Van een codewoord $(c_0,c_1,\ldots,c_{n-1})$ zijn de letters o.a. op te vatten als m-tallen, dat is $c_i = (c_{i1},c_{i2},\ldots,c_{im})$ $(i = 0,1,\ldots,n-1)$, met $c_{ij} \in GF(2)$. Zo'n m-tal is dan een serie informatiesymbolen voor de zgn. binnencode C_1. Neem het eenvoudigste geval van rate $\frac{1}{2}$. Dan behoort bij $c_i = (c_{i1},c_{i2},\ldots,c_{im})$ een codewoord van 2m letters uit GF(2). De rate van de concatenated code is dan de helft van de rate van C_2. Het idee van Justesen is om de binnencode te variëren, d.w.z. C_1 te laten afhangen van i. Daarbij zijn de binnencodes *systematisch* gekozen, hetgeen betekent dat het 2m-tal dat aan c_i wordt toegevoegd begint met $(c_{i1},c_{i2},\ldots,c_{im})$. Voor de buitencode C_2 neemt men meestal (ook Justesen) een RS-code.

We geven nu de details van Justesens constructie. We beginnen met de buitencode. Deze noemen we A_m. Het is de Reed-Solomon code met woordlengte $N := 2^m - 1$ over $GF(2^m)$ waarvan de voortbrenger het polynoom $g(x) = \prod_{i=1}^{d-1} (x-\alpha^i)$ is (α primitief element van $GF(2^m)$). De dimensie van A_m is K, de minimum afstand is $d = N + 1 - K$.
(N.B. N, d en K hangen van m af, K wordt later gekozen.)

(9.2.1) <u>DEFINITIE</u>. *De binaire code C_m met woordlengte* $n := n_m := 2mN$ *wordt gedefinieerd door* $C_m :=$
$\{\underline{c} = (c_0,c_1,\ldots,c_{N-1}) \mid c_j := (a_j,\alpha^j a_j),\ (a_0,a_1,\ldots,a_{N-1}) \in A_m\}$.

Hierin interpreteren we $(a_j, \alpha^j a_j)$ *als binair* 2m-*tal.*

We zien dat C_m een binaire code is met dimensie $k := mK$ en rate $R := \frac{1}{2}K/N$. We zullen gebruik maken van het feit dat een 2m-tal, dat als een c_j voorkomt in een codewoord $\underline{c}$, door de definitie van c_j reeds j bepaalt. Dit is hetzelfde idee dat ook in § 9.1 werd gebruikt.

(9.2.2) <u>LEMMA</u>. *Zij* $\gamma \in (0,1)$, $\delta \in (0,1)$. *Laat* $(M_L)_{L\in\mathbb{N}}$ *een rij natuurlijke getallen zijn met de eigenschap* $M_L 2^{-L\delta} = \gamma + o(1)$, $(L \to \infty)$. *Dan heeft ieder* M_L*-tal verschillende woorden in* $R^{(L)}$ *een totaal gewicht* W *waarvoor*

$$W \geq \gamma L\, 2^{L\delta}\{H^{\leftarrow}(\delta) + o(1)\}, \qquad (L \to \infty).$$

<u>BEWIJS</u>: Voor voldoend grote L definiëren we

$$\lambda := H^{\leftarrow}(\delta - \frac{1}{\log L}).$$

Volgens (0.4.5) geldt

$$\sum_{0\leq i\leq \lambda L} \binom{L}{i} \leq 2^{L(\delta - \frac{1}{\log L})}.$$

Dus geldt

$$\begin{aligned} W &\geq \{M_L - \sum_{0\leq i\leq\lambda L} \binom{L}{i}\}\lambda L \\ &\geq \lambda L\{M_L - 2^{L(\delta - \frac{1}{\log L})}\} \\ &= \lambda L\, 2^{L\delta}\{\gamma + o(1)\} \\ &= \gamma L\, 2^{L\delta}\{H^{\leftarrow}(\delta) + o(1)\}. \qquad \square \end{aligned}$$

Zij nu R vast, $0 < R < \frac{1}{2}$. Voor $m \in \mathbb{N}$ definiëren we als boven $N := 2^m - 1$ en nemen we voor K het kleinste gehele getal zo dat $R_m := \frac{K}{2N} \geq R$. Dan is de rij $(C_m)_{m\in\mathbb{N}}$ uit (9.2.1) een rij codes met rate $R_m \to R$ $(m \to \infty)$. We onderzoeken nu de minimum-afstand d_m van C_m. Ieder woord $\underline{a} \neq \underline{0}$ uit de buiten-

code (de Reed-Solomon-code A_m) heeft gewicht $w(\underline{a}) \geq N - K + 1$. Verder is

(9.2.3) $$N - K + 1 > N - K = N(1 - 2R_m)$$
$$= (2^m-1)(1-2R+o(1)), \qquad (m \to \infty).$$

Iedere coördinaat $a_j \neq 0$ geeft aanleiding tot een 2m-tal $c_j = (a_j, \alpha^j a_j)$ in het toegevoegde codewoord $\underline{a}$ van C_m. We merkten boven reeds op dat deze 2m-tallen van $\underline{c}$ verschillend zijn. We passen nu lemma (9.2.2) toe om het gewicht van $\underline{c}$ te schatten. We nemen hiertoe in het lemma $L := 2m$, $\delta := \frac{1}{2}$, $\gamma := 1 - 2R$ (dit kan volgens (9.2.3)). Volgens (9.2.2) is nu

(9.2.4) $$w(\underline{c}) \geq (1-2R)\cdot 2m\cdot 2^m\{H^{\leftarrow}(\tfrac{1}{2}) + o(1)\}, \qquad (m \to \infty) \quad .$$

Dus is

$$d_m/n \geq (1-2R)\ \{H^{\leftarrow}(\tfrac{1}{2}) + o(1)\}, \qquad (m \to \infty) \ .$$

Hiermee is bewezen:

(9.2.5) <u>STELLING</u>: *Zij* $0 < R < \frac{1}{2}$. *De Justesen code* C_m *zoals boven gedefinieerd heeft woordlengte* $n = 2m(2^m-1)$, *rate* R_m *en minimum-afstand* d_m *waarvoor geldt*

(9.2.6) $$R_m \to R, \qquad (m \to \infty),$$

(9.2.7) $$\liminf_{m\to\infty} d_m/n \geq (1-2R)H^{\leftarrow}(\tfrac{1}{2}) \ .$$

Met de notatie van § 4.1 is $\delta \geq (1-2R)\ H^{\leftarrow}(\frac{1}{2})$. Hier is R kleiner dan de grens $\alpha(\delta)$ uit (4.2.5). Bij gegeven $R < \frac{1}{2}$ is hier voor het eerst de limiet van δ niet 0.

We zullen nu een kleine verandering aanbrengen in bovengenoemde constructie om ook $R > \frac{1}{2}$ te kunnen bereiken. Laat $0 \leq s < m$ (we kiezen s later). Uit elk 2m-tal $c_j = (a_j, \alpha^j a_j)$ laten we de laatste s letters weg. De code die we aldus krijgen noemen we $C_{m,s}$. Zij R vast, $0 < R < 1$. Bij gegeven m en s kiezen we voor K het kleinste getal zó dat $R_{m,s} := \frac{m}{2m-s}\frac{K}{N} \geq R$ (dit kan mits $\frac{m}{2m-s} \geq R$). Een codewoord $\underline{a} \neq \underline{0}$ uit A_m geeft aanleiding tot allemaal verschillende 2m-tallen c_j ($\neq (0,0)$) maar de (2m-s)-tallen die na de

verkorting overblijven kunnen meerdere keren voorkomen, echter elk ten hoogste 2^s keer. Het aantal verschillende (2m-s)-tallen is dus tenminste:

$$(9.2.8) \qquad 2^{-s}(N-K) = 2^{-s}\, N(1 - \frac{2m-s}{m} R_{m,s}) \ .$$

Pas weer lemma (9.2.2) toe, nu met $L := 2m-s$, $\delta := \frac{m-s}{L}$, $\gamma := 1 - \frac{2m-s}{m} R$. Dan geldt voor de minimum-afstand $d_{m,s}$ van $C_{m,s}$

$$d_{m,s} \geq (1 - \frac{2m-s}{m} R)(2m-s)2^{m-s}\{H^{\leftarrow}(\frac{m-s}{2m-s}) + o(1)\}2^s, \qquad (m \to \infty),$$

dus

$$(9.2.9) \qquad d_{m,s}/n \geq (1 - \frac{2m-s}{m} R)\{H^{\leftarrow}(\frac{m-s}{2m-s}) + o(1)\}, \qquad (m \to \infty).$$

Zij nu $r \in (\frac{1}{2},1)$ vast. Kies $s := [m(\frac{2r-1}{r})] + 1$. Als $r \geq R$ dan is ook $\frac{m}{2m-s} \geq R$. We vinden uit (9.2.9) nu

$$(9.2.10) \qquad d_{m,s}/n \geq (1 - \frac{R}{r})\{H^{\leftarrow}(1-r) + o(1)\}, \qquad (m \to \infty).$$

Het rechterlid van (9.2.10) is maximaal als r voldoet aan

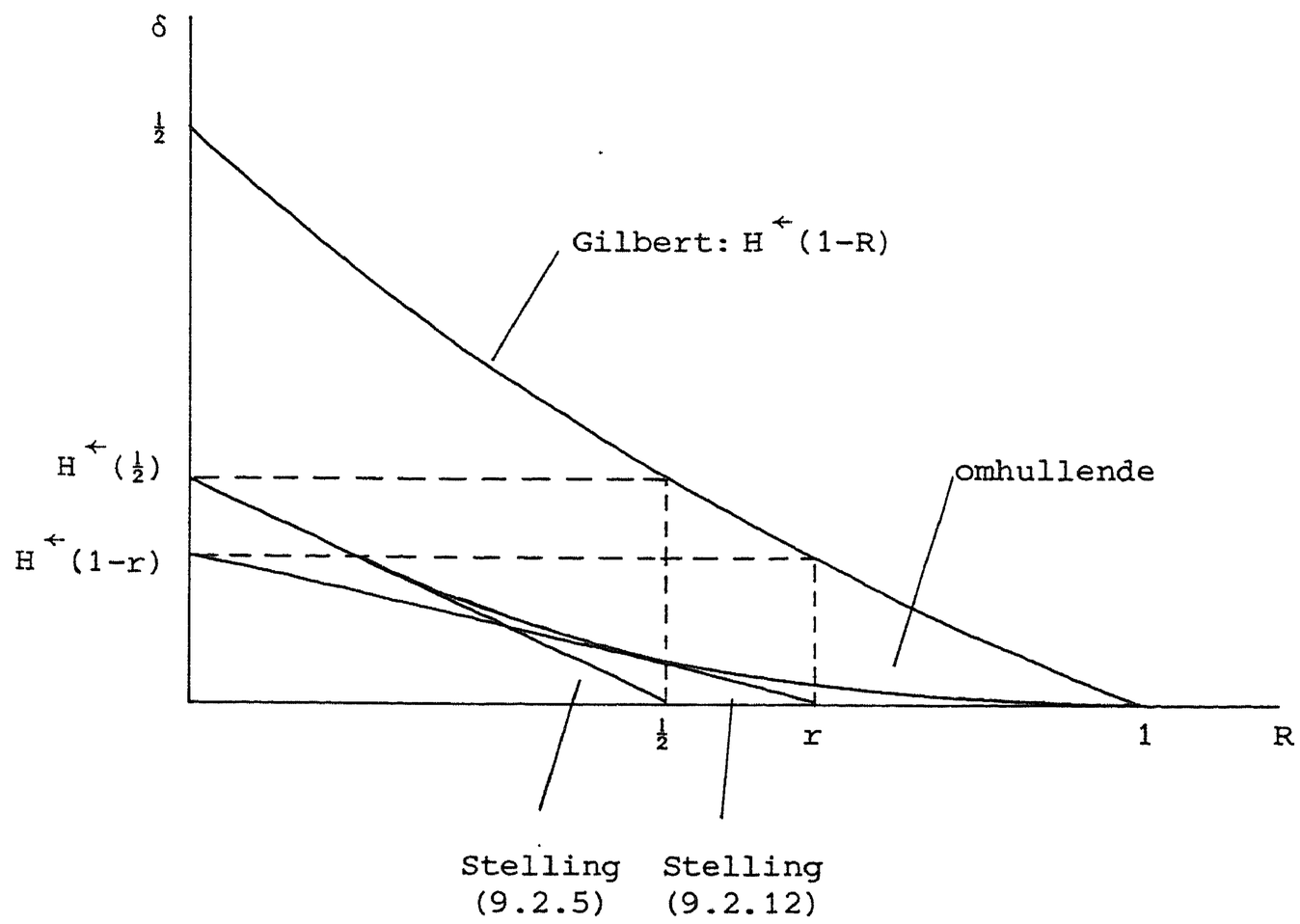
$$(9.2.11) \qquad R = \frac{r^2}{1 + \log\{1 - H^{\leftarrow}(1-r)\}} \ .$$

Is R zó klein dat uit (9.2.11) volgt $r < \frac{1}{2}$ dan nemen we $r = \frac{1}{2}$. We vatten dit nu samen in

(9.2.12) <u>STELLING</u>: *Zij* $0 < R < 1$ *en zij* r *het maximum van* $\frac{1}{2}$ *en de oplossing van* (9.2.10), $s = [m(\frac{2r-1}{r})] + 1$. *De Justesen codes* $C_{m,s}$ *hebben woordlengte* n, *rate* $R_{m,s}$ *en minimum-afstand* $d_{m,s}$ *waarvoor geldt*

$$\liminf d_{m,s}/n \geq (1 - \frac{R}{r})H^{\leftarrow}(1-r).$$

De resultaten van de stellingen (9.2.5) en (9.2.12) vergelijken we in onderstaande figuur met de Gilbert-bound.



9.3. DIRECTE CONSTRUCTIE

Eén van de bezwaren tegen de constructie van Justesen was het feit dat zowel voor de RS-code als voor de binnencode een primitief element van $GF(2^m)$ nodig is. Er is geen andere manier om zo'n element te vinden dan een zoekprocédé en men kan dan even goed een goede code direct construeren met een zoekprocédé. Daar m variabel is werd de oplossing niet constructief genoemd. In zijn artikel maakt Justesen een vage opmerking over een suggestie van R.J. McEliece om dit bezwaar op te heffen. We zullen dit idee hier uitvoeren. We beperken ons tot geschikte waarden van m en beschrijven $GF(2^m)$ op een eenvoudige manier.

(9.3.1) <u>LEMMA</u>. $3^{\beta+1} \parallel (2^{3^\beta}+1)$.

<u>BEWIJS</u>. (i) Voor $\beta = 0$ en 1 is de bewering direct duidelijk.

(ii) Stel $3^t \parallel (2^{3^\beta} + 1)$. Uit

$$(2^{3^{\beta+1}}+1) = (2^{3^\beta}+1)\ \{(2^{3^\beta}+1)(2^{3^\beta}-2) + 3\}$$

volgt, als $t \geq 2$,

$$3^{t+1} \parallel (2^{3^{\beta+1}}+1). \qquad \square$$

<u>GEVOLG</u>. Als m de orde van 2 (mod 3^ℓ) is, dan is $m = \phi(3^\ell) = 2.3^{\ell-1}$.

<u>BEWIJS</u>: Uit $2^\alpha \equiv 1 \pmod 3$ volgt $\alpha \equiv 0 \pmod 2$. Dus is $m = 2s$. Dan is dus $2^s + 1 \equiv 0 \pmod{3^\ell}$. Het gestelde volgt uit het lemma. $\square$

Voor deze m bevat $GF(2^m)$ een primitieve 3^ℓ-de eenheidswortel ξ (Euler-Fermat). Het minimaalpolynoom van ξ is blijkbaar

$$(x+\xi)(x+\xi^2)(x+\xi^4) \ldots (x+\xi^{2^{m-1}}),$$

een polynoom van de graad m. Merk op dat

$$1 + x^{3^\ell} = (1+x)(1+x+x^2)(1+x^3+x^6) \ldots (1+x^{3^{\ell-1}}+x^{2.3^{\ell-1}}).$$

Uit het voorafgaande volgt dat de laatste factor (rechts) *irreducibel* is. In het vervolg is $m = 2.3^{\ell-1}$ en $GF(2^m)$ de verzameling polynomen van graad $< m$ over $GF(2)$ met optelling en vermenigvuldiging mod $g(x)$, waarbij $g(x) := x^{2.3^{\ell-1}} + x^{3^{\ell-1}} + 1$.
We construeren nu direct de buitencode.

Een m-tal informatie-symbolen $(i_0,i_1,\ldots,i_{m-1})$ uit $GF(2)$, vatten we op als het element $i_0 + i_1 + \ldots i_{m-1}x^{m-1} \in GF(2^m)$. Aan K op elkaar volgende m-tallen, zeg $a_0,a_1,\ldots,a_{K-1}$ voegen we toe het polynoom $a(Z) := a_0 + a_1Z + \ldots + a_{K-1}Z^{K-1}$, waarbij de a_i nu elementen van het lichaam $GF(2^m)$ zijn.
Voor $j = 1,2,\ldots,2^m-1$ laat $j = \sum_{i=0}^{m-1} \varepsilon_i 2^i$ en $j(x) := \sum_{i=0}^{m-1} \varepsilon_i x^i$. Zo doorloopt $j(x)$ de elementen $\neq 0$ van $GF(2^m)$. Deze substitueren we achtereenvolgens voor Z in $a(Z)$. Zo onstaat een rij van $N := 2^m-1$ elementen van $GF(2^m)$. Zo hebben we dus een lineaire code met rate K/N over $GF(2^m)$ gemaakt. Daar $a(Z)$ graad $\leq K-1$ heeft, heeft dit polynoom $\leq K-1$ nulpunten in $GF(2^m)$, d.w.z. ieder codewoord $\neq 0$ heeft gewicht $D \geq N-K+1$. Hiermee is de eerste stap volledig constructief.

Bij de binnencode gaan we analoog te werk.

Is c_j de j-de letter van een codewoord van de buitencode, dus c_j een polynoom van graad $\leq m-1$, en $j(x)$ als boven, dan is

$$(c_j, j(x)c_j),$$

waarbij vermenigvuldiging als steeds mod g(x) is, op te vatten als een 2m-tal nullen en enen dat de eigenschap heeft die wezenlijk was voor Justesen's constructie, te weten: als $c_j \neq 0$ dan is j eenduidig bepaald door het 2m-tal (deling mod g(x)). Ook deze stap is nu volledig constructief.

9.4. COMMENTAAR

De eenvoudige constructie uit § 9.1 is gebaseerd op een suggestie van M. Staring. Het idee komt reeds eerder voor o.a. als de zgn. randomly shifted codes van Wozencraft. Een bewijs met de eenvoud van § 9.1 hebben we nergens in de literatuur aangetroffen. Het idee van § 9.2 is een van de belangrijke stappen vooruit in Coding Theory uit de laatste jaren.

9.5. OPGAVEN

(9.5.1) Laat met de inkortingsmethode van § 9.2 zien dat het idee van § 9.1 voor iedere R codes levert die de Gilbert bound halen.

Hoofdstuk X

ARITHMETISCHE CODES

10.1. AN-CODES

Arithmetische codes zijn bestemd voor het controleren van rekenkundige bewerkingen, in het bijzonder optelling en aftrekking. De te bewerken getallen dient men zich hierbij voor te stellen als geschreven in het r-tallig stelsel, waar r een vast geheel getal ≥ 2 is. Het binaire (r=2) en het decimale (r=10) geval zijn van overwegend praktisch belang.

Arithmetische codes verschillen van de andere in deze syllabus behandelde codes door de keuze van de *afstandsfunctie*. Hamming-afstand is minder geschikt voor het doel: één enkele vergissing bij een optelling kan immers verscheidene foute cijfers in de uitkomst tot gevolg hebben, zodat de Hamming-afstand tussen het juiste antwoord en de verkregen uitkomst geen ondergrens is voor het aantal gemaakte fouten.

Een afstandsbegrip dat beter overeenkomt met het soort fouten dat men verwacht wordt als volgt verkregen. Het *arithmetische gewicht* w(x) van een geheel getal x is per definitie het kleinste getal $t \geq 0$ waarvoor er een representatie

$$(10.1.1) \qquad x = \sum_{i=1}^{t} a_i r^{n(i)}$$

met

$$a_i,\ n(i) \in \mathbb{Z},\ |a_i| < r,\ n(i) \geq 0$$

(i=1,...,t) bestaat. De *arithmetische afstand* d(x,y) tussen twee gehele getallen x en y is gedefinieerd door

$$d(x,y) = w(x-y).$$

Men gaat gemakkelijk na dat d een metriek op $\mathbb{Z}$ is. Maakt men $\mathbb{Z}$ tot verzameling hoekpunten van een graph door x en x' te verbinden als

$$|x-x'| = c.r^i \text{ voor een } c \in \{1,2,\ldots, r-1\},\ i \in \mathbb{Z}_{\geq 0},$$

dan is de arithmetische afstand tussen twee gehele getallen gelijk aan hun afstand in deze graph. Arithmetische afstand is translatie-invariant: $d(x,y) = d(x+z,y+z)$ voor alle $x,y,z \in \mathbb{Z}$. Deze eigenschap heeft Hamming-afstand niet. Merk op dat de arithmetische afstand tussen twee niet-negatieve gehele getallen kleiner dan of gelijk aan hun Hamming-afstand is.

We zullen codes beschouwen van de vorm

$$C = \{AN \mid N \in \mathbb{Z}, 0 \leq N < B\}$$

waar A en B vaste positieve gehele getallen zijn; zulke codes heten *AN-codes*. Het gebruik van zo'n code moet men zich als volgt voorstellen. Om twee getallen N_1 en N_2 (niet negatief, en niet te groot t.o.v. B) op te tellen codeert men ze als AN_1 resp. AN_2. Vervolgens berekent men de som van AN_1 en AN_2; noem de uitkomst S. Als alles goed is gegaan is S een A-voud, en de som van N_1 en N_2 is dan S/A. Als S geen A-voud is, heeft men bij de optelling een vergissing gemaakt. Men bepaalt dan $AN_3 \in C$ met minimale $d(AN_3, S)$; het aantal gemaakte vergissingen is dan ten minste $d(AN_3,S)$, en de meest waarschijnlijke uitkomst voor $N_1 + N_2$ is N_3.

Opdat men op deze wijze alle ten hoogste e-voudige fouten kan corrigeren is nodig en voldoende dat geldt

$$d(AN,AN') \geq 2e + 1$$

voor alle $AN, AN' \in C$, $AN \neq AN'$. Dit is kennelijk hetzelfde als

$$w(AN) \geq 2e + 1 \text{ voor alle } AN \in C,\ AN \neq 0.$$

De tot nog toe gebruikte eigenschappen van C zijn voornamelijk te danken aan de gelijkenis van C met de ondergroep

$$H = \{AN \mid N \in \mathbb{Z}\};$$

vergelijk dit met de prominente plaats die *lineaire* codes in de codetheorie innemen. Het is helaas niet zinvol C = H te nemen, want er geldt

$$\min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\} \leq 2$$

voor alle $A \in \mathbb{Z}$ (zie (10.6.1)).

Dit ongemak omzeilen we door *modulaire* AN-codes te beschouwen. Zetten we, met A, B, C als boven,

$$m = AB,$$

dan kunnen we C opvatten als *ondergroep* van $\mathbb{Z}/m\mathbb{Z}$ (de gehele getallen modulo m). We moeten dan wel ons afstandsbegrip aanpassen. Hiertoe maken we $\mathbb{Z}/m\mathbb{Z}$ tot verzameling hoekpunten van een graph door (x mod m) en (x' mod m) te verbinden met een kant als

$$x - x' \equiv \pm c.r^j (\text{mod } m)$$

voor zekere $c,j \in \mathbb{Z}$, $0 < c < r$, $j \geq 0$. De *modulaire afstand* $d_m(\overline{x},\overline{y})$ tussen twee elementen $\overline{x},\overline{y}$ van $\mathbb{Z}/m\mathbb{Z}$ is dan de afstand tussen $\overline{x}$ en $\overline{y}$ in deze graph, en het *modulaire gewicht* $w_m(\overline{x})$ is gedefinieerd door $w_m(\overline{x}) = d_m(\overline{x},(0 \text{ mod } m))$. Voor $x,y \in \mathbb{Z}$ schrijven we in plaats van $d_m((x \text{ mod } m), (y \text{ mod } m))$ en $w_m((x \text{ mod } m))$ ook wel $d_m(x,y)$ en $w_m(x)$. Merk op dat geldt

$$w_m(x) = \min\{w(y) \mid y \in \mathbb{Z}, y \equiv x(\text{mod } m)\}$$

$$d_m(x,y) = w_m(x-y).$$

De code C kan nu gebruikt worden om twee getallen N_1 en N_2 modulo B op te tellen. Hierbij kunnen alle combinaties van ten hoogste e fouten hersteld worden dan en slechts dan als geldt

$$d_{min}(C) \geq 2e + 1$$

waar $d_{min}(C)$ de *minimum-afstand* van de code is:

$$d_{min}(C) = \min\{w_m(x) \mid x \in C,\ x \neq (0 \text{ mod } m)\}.$$

Niet iedere keuze voor m is zinvol. Als bijvoorbeeld m een priemgetal is waarvoor r een primitieve wortel is, dan geldt $w_m(x) \leq 1$ voor alle $x \in \mathbb{Z}$. Wij zullen ons in het vervolg beperken tot getallen van de vorm

$$m = r^n - 1,\ n \in \mathbb{Z},\ n \geq 2.$$

Deze keuze is voor de praktijk van belang, aangezien vele computers modulo 2^n-1 rekenen.

Elk geheel getal x kan modulo r^n-1 eenduidig geschreven worden als

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{(r^n-1)}$$

met $c_i \in \{0,1,\ldots,r-1\}$ $(0 \le i < n)$, niet alle $c_i = 0$. Dus $\mathbb{Z}/(r^n-1)$ is op te vatten als de verzameling woorden ter lengte n gevormd uit r letters, met uitzondering van het woord 00...0.

Deze laatste uitzondering zou overbodig geweest zijn als we hadden genomen $m = r^n$; dit is voor de praktijk eveneens een zinvolle keuze, daar ook vele computers modulo 2^n rekenen. Goede codes zijn voor $r = 2$, $m = 2^n$ echter niet te verwachten: uit $AB = m = 2^n$ volgt immers $A = 2^k$ voor zekere k, en de code bestaat dan uit de getallen

$$\sum_{i=0}^{n-1} c_i 2^i, \quad c_i \in \{0,1\}$$

waarvoor $c_0 = \ldots = c_{k-1} = 0$; het coderen van een getal $\sum_{i=0}^{n-k-1} d_i 2^i$ modulo B $(=2^{n-k})$ $(d_i \in \{0,1\})$ bestaat dan uit het achterplaatsen van k nullen, die niet eens een parity-check functie vervullen! Analoge bezwaren zijn er voor algemene r.

In het vervolg verstaan we onder een *cyclische AN-code* een ondergroep C van $\mathbb{Z}/(r^n-1)$; hieris n een geheel getal ≥ 2, de *woordlengte* van de code. Bij zo'n C is er steeds een eenduidig bepaald paar natuurlijke getallen A, B met

$$AB = r^n-1$$

$$C = \{(AN \bmod (r^n-1)) \mid N \in \mathbb{Z},\ 0 \le N < B\}.$$

We noemen A de *voortbrenger* van de code. We zijn primair geinteresseerd in codes waarvan de *rate* $\frac{1}{n} \cdot {}^r\log B$ en de minimum-afstand "groot" zijn.

Als abelse groep is C cyclisch van orde B. De benaming "cyclische AN-code" slaat echter op een andere eigenschap, die doet denken aan de cy-

clische codes over eindige lichamen: is $(x \bmod (r^n-1))$ een element van C,

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{(r^n-1)},$$

dan geldt

$$rx \equiv \sum_{i=0}^{n-1} c_{i-1} r^i \pmod{(r^n-1)}$$

(indices modulo n), en $(rx \bmod (r^n-1))$ is een element van C omdat C een ondergroep is. Dus de "cyclische opschuiving" van een codewoord behoort weer tot de code. De analogie met cyclische codes over eindige lichamen gaat verder: een cyclische AN-code is een ideaal van de ring $\mathbb{Z}/(r^n-1)$, een cyclische code over GF(q) is niets anders dan een ideaal in $GF(q)[x]/(x^n-1)$. Verder kan men r met x laten corresponderen, A met g(x) (= het voortbrengend polynoom van de code), en B met h(x) (het "check polynomial"). Op deze analogie komen we nog terug.

Men verkrijgt *negacyclische* AN-codes door $m = r^n + 1$ te nemen, en ondergroepen van $\mathbb{Z}/(r^n+1)$ te beschouwen. We laten het aan de lezer over, de resultaten van §§ 10.2 t/m 10.4 voor het negacyclische geval te formuleren en te bewijzen.

Referenties voor deze paragraaf: PETERSON & WELDON (1972), MASSEY & GARCIA (1972), RAO (1974) en de daar aangegeven literatuur. Deze auteurs beschouwen voornamelijk het binaire geval.

10.2. PERFECTE CYCLISCHE AN-CODES VAN ORDE 1

Zij $C \subset \mathbb{Z}/(r^n-1)$ een cyclische AN-code en e een geheel getal ≥ 1. We noemen C *perfect van orde e* als er voor elke $x \in \mathbb{Z}/(r^n-1)$ een eenduidig bepaald element $c \in C$ bestaat met $d_m(x,c) \leq e$; hier $m = r^n-1$. Zetten we

$$S_e = \{x \in \mathbb{Z}/(r^n-1) \mid w_m(x) \leq e\}$$

dan betekent dit dat elk element $x \in \mathbb{Z}/(r^n-1)$ een eenduidige voorstelling $x = c + y$, met $c \in C$, $y \in S_e$ heeft. Anders geformuleerd: de natuurlijke afbeelding

$$S_e \longrightarrow (\mathbb{Z}/(r^n-1))/C \cong \mathbb{Z}/A\mathbb{Z}$$

met bejectief zijn. Hier geeft A de voortbrenger van de code aan, als in 10.1. Merk op dat een perfecte code van orde e alle ten hoogste e-voudige fouten kan corrigeren, dus $d_{min}(C) \geq 2e + 1$.

We beschouwen in deze paragraaf het geval $e = 1$. Dan geldt $d_{min}(C) \geq 3$. Heeft C meer dan één element, dan hebben we bovendien $d_{min}(C) \leq n$, dus we mogen ons beperken tot het geval $n \geq 3$. Het is eenvoudig na te gaan dat S_1 dan precies $1 + 2(r-1)n$ elementen heeft, namelijk

$$0 \bmod (r^n-1),$$

$$c.r^j \bmod (r^n-1), c,j \in \mathbb{Z}, 0 < |c| < r, 0 \leq j < n.$$

De bijectie $S_1 \to \mathbb{Z}/A\mathbb{Z}$ levert dus $A = 1 + 2n(r-1)$, waaruit volgt dat $1 + 2n(r-1)$ een deler is van r^n-1 zodra er een perfecte code $C \subset \mathbb{Z}/(r^n-1)$ van orde 1 is: de "sphere packing condition".

(10.2.1) <u>STELLING</u>. (zie GOTO & FUKUMURA (1975)). *Stel* $C \subset \mathbb{Z}/(r^n-1)$ *is een perfecte cyclische AN-code van orde 1 met voortbrenger* A *en woordlengte* $n \geq 3$. *Dan is* A *een priemgetal* $> r^2$, *de woordlengte* n *is oneven, en de ondergroep* $H \subset (\mathbb{Z}/A\mathbb{Z})^*$ (= *multiplicatieve groep van het lichaam* $\mathbb{Z}/A\mathbb{Z}$) *voortgebracht door* (r mod A) *heeft orde* n *en index* $2(r-1)$. *Bovendien vormen de elementen* ($\pm$ c mod A), $c = 1,2,\ldots, r-1$, *een volledig representantensysteem voor de nevenklassen van* H *in* $(\mathbb{Z}/A\mathbb{Z})^*$.

Omgekeerd, als A *een priemgetal* $> r^2$ *is met de eigenschap dat de ondergroep* $H \subset (\mathbb{Z}/A\mathbb{Z})^*$ *voortgebracht door* r *index* $2(r-1)$ *heeft, met* $\{\pm$ c mod A$|$ $c = 1,2,\ldots,r-1\}$ *als volledig representantensysteem voor de nevenklassen, dan is de orde* n *van* H *oneven, en de ondergroep* C *van* $\mathbb{Z}/(r^n-1)$ *voortgebracht door* A mod(r^n-1) *is een perfecte cyclische AN-code van orde* 1.

<u>BEWIJS</u>. Als $A = r^n-1$ dan is $A > r^2$ duidelijk. Als $A < r^n-1$ dan is (A mod r^n-1) een element ongelijk aan nul van C, dus $d_{min}(C) \geq 3$ impliceert $w(A) \geq w_m(A) \geq 3$, waaruit volgt $A > r^2$. Is A niet priem, dan $A = k.l$ met $k,l > 1$; we mogen aannemen $k > r$. Wegens de bijectie $S_1 \longrightarrow \mathbb{Z}/A\mathbb{Z}$ is er precies één geheel getal van de vorm $c.r^j$, $c,j \in \mathbb{Z}$, $|c| < r, j \geq 0$ met $k \equiv c.r^j \bmod A$. Kennelijk $c \neq 0$. Er volgt $k|c.r^j$. Ook $k|A|r^n-1$, dus $(k,r) =$

$= 1$ en $k|c$. Dit is in tegenspraak met $k > r$, $0 < |c| < r$. Dus A is priem.

De bijectie $S_1 \to \mathbb{Z}/A\mathbb{Z}$ levert nu een bijectie

$$\{\pm c.r^j \mid c = 1,2,\ldots,r-1,\ j = 0,1,\ldots,n-1\} \to (\mathbb{Z}/A\mathbb{Z})^*.$$

Het beeld van $\{r^j \mid j = 0,1,\ldots,n-1\}$ is net de ondergroep H voortgebracht door (r mod A), want $r^n \equiv 1 \bmod A$. Deze ondergroep heeft dus orde n, en kennelijk is $\{\pm c \bmod A \mid c = 1,2,\ldots,r-1\}$ een representantensysteem voor $(\mathbb{Z}/A\mathbb{Z})^*/H$. In het bijzonder geldt $(-1 \bmod A) \notin H$, dus de orde n van H is oneven. Dit bewijst de eerste helft van de stelling. De omkering laten we aan de lezer over. □

(10.2.2) <u>GEVOLG</u> (zie PETERSON & WELDON (1972)). *Stel* p *is een priemgetal* $\equiv 3 \pmod 4$ *waarvoor* -2 *een primitieve wortel is. Dan is de ondergroep* $C \subset \mathbb{Z}/(2^{\frac{1}{2}(p-1)}-1)$ *voortgebracht door* p mod $(2^{\frac{1}{2}(p-1)}-1)$ *een perfecte binaire cyclische AN-code van orde 1. Bovendien is elke perfecte binaire cyclische AN-code van orde 1 van deze vorm.*

<u>BEWIJS</u>. Dit volgt direkt uit (10.2.1). De voorwaarde op p is slechts een vertaling van de eis dat $(2 \bmod p) \in (\mathbb{Z}/p\mathbb{Z})^*$ een ondergroep van index 2 voortbrengt waar $(-1 \bmod p)$ niet in zit. □

Priemgetallen p die aan de voorwaarden van (10.2.2) voldoen zijn bijvoorbeeld: $p = 7$ (levert een triviale code), $p = 23$, $p = 47$, $p = 71$, $p = 79$. Merk op dat p noodzakelijk 7 mod 8 is.

Priemgetallen p waarvoor 2 een primitieve wortel is geven aanleiding tot perfecte *negacyclische* codes, cf. PETERSON & WELDON (1972). Vergelijk dit met de cyclische beschrijving van binaire Hamming codes: is $g(x) \in GF(2)[x]$ een irreducibel polynoom zodat x een primitieve wortel mod g(x) is, dan brengt g(x) in $GF(2)[x]/(x^n-1)$, $n = 2^{\text{graad}(g)}-1$, een perfecte code van orde 1 voort.

Het volgende gevolg bewijst men als het vorige.

(10.2.3) <u>GEVOLG</u> (zie GRITSENKO (1969)). *Stel* p *is een priemgetal* $\equiv 5 \bmod 8$ *zodat* $(3 \bmod p) \in (\mathbb{Z}/p\mathbb{Z})^*$ *een ondergroep van index 4 voortbrengt. Dan brengt* (p mod $(3^{\frac{1}{4}(p-1)}-1)$) *een perfecte ternaire cyclische AN-code van orde 1 in* $\mathbb{Z}/(3^{\frac{1}{4}(p-1)}-1)$ *voort. Bovendien is elke perfecte ternaire cyclische AN-code van orde 1 van deze vorm.* □

Elk priemgetal p dat aan de voorwaarden van dit gevolg voldoet is congruent met 13 modulo 24; voorbeelden zijn $p = 13$, $p = 109$, $p = 181$.

Niet voor elke r bestaan er cyclische AN-codes van orde 1:

(10.2.4) GEVOLG (zie BOYARINOV & KABATYANSKY (1973)). *Er bestaat geen perfecte AN-code van orde 1 met* $r = 2^k$, $k \in \mathbb{Z}$, $k > 1$.

BEWIJS. Stel C is zo'n code, met voortbrenger A. Zij $H' \subset (\mathbb{Z}/A\mathbb{Z})^*$ voortgebracht door (r mod A) en (-1 mod A). Wegens de stelling heeft $(\mathbb{Z}/A\mathbb{Z})^*/H'$ orde $r - 1 = 2^k - 1$ en een volledig representantensysteem {(1 mod A), (2 mod A),...,(r-1 mod A)}. Hieruit ziet men dat de orde van het beeld van (2 mod A) in $(\mathbb{Z}/A\mathbb{Z})^*/H'$ gelijk is aan k. Omdat de orde van een element de orde van de groep deelt, volgt $k | 2^k - 1$. Zij nu q het kleinste priemgetal dat k deelt. Dan $2^k \equiv 1 \bmod q$, $2^{q-1} \equiv 1 \bmod q$ (Fermat), en $(k, q-1) = 1$, dus $2^1 \equiv 1 \bmod q$, tegenspraak. □

(10.2.5) GEVOLG (zie GOTO (1975)). *Er bestaat geen perfecte decimale cyclische AN-code van orde 1.*

BEWIJS. Brengt A zo'n code voort, en is $H' \subset (\mathbb{Z}/A\mathbb{Z})^*$ voortgebracht door de restklassen van 10 en -1, dan heeft $(\mathbb{Z}/A\mathbb{Z})^*/H'$ orde 9. Geven we het beeld van (i mod A) in deze groep aan met $\overline{i}$, dan

$$(\mathbb{Z}/A\mathbb{Z})^*/H' = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}.$$

Uit $\overline{2}^3 = \overline{8} \neq \overline{1}$ volgt orde $(\overline{2}) = 9$, dus $\overline{2}$ brengt de groep voort. Verder $\overline{2}.\overline{5} = \overline{10} = \overline{1}$ dus $\overline{5} = \overline{2}^8$. Zij $\overline{3} = \overline{2}^x$, met $0 \leq x < 9$. Als $x = 0, 1, 2, 3$ of 8, dan $\overline{3} = \overline{1}, \overline{2}, \overline{4}, \overline{8}$ of $\overline{5}$, respectievelijk, een tegenspraak. Als $x = 4, 5$ of 6 dan $\overline{9} = \overline{2}^{2x} = \overline{5}, \overline{2}$ of $\overline{8}$, weer een tegenspraak. Tenslotte levert ook $x = 7$ een tegenspraak: $\overline{6} = \overline{2}^{x+1} = \overline{5}$. □

Meer non-existentiestellingen van dit type vindt men in GOTO & FUKUMURA (1975); hier worden ook negacyclische codes beschouwd. Perfecte codes van orde 1 met $r = 4, 5, 8, 9$ of 10 bestaan niet; voor $r = 6$ of 7 worden perfecte cyclische codes van orde 1 geleverd door:

r	A	n
6	18191	1819
6	20611	2061
7	19237	1603
7	30013	2501.

Voor hogere r zijn er geen voorbeelden bekend; deze bestaan echter waarschijnlijk wel, bijvoorbeeld voor r = 11, 12, 14, 15, 17, ... Deze verwachting is gebaseerd op overwegingen uit de algebraïsche getaltheorie, waar we hier niet verder op ingaan.

Voor niet-perfecte AN-codes die enkelvoudige fouten kunnen corrigeren zie men GRITSENKO (1969) en NEUMANN & RAO (1975).

10.3. BEREKENING VAN HET ARITHMETISCHE EN MODULAIRE GEWICHT

Voor het construeren van AN-codes die meer fouten kunnen corrigeren hebben we een goede manier nodig om het arithmetische of modulaire gewicht van een geheel getal te bepalen.

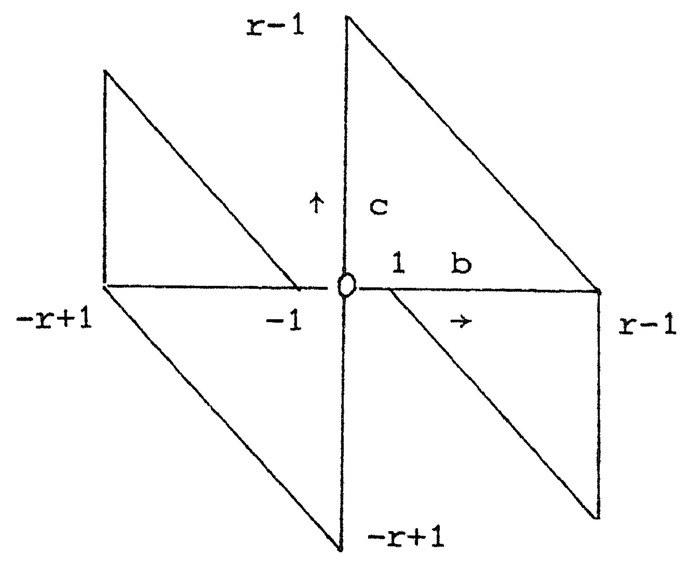
Elk geheel getal x kan, per definitie van w, geschreven worden als

$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)}$$

met a_i, $n(i) \in \mathbb{Z}$, $|a_i| < r$, $n(i) \geq 0$ $(i=1,\ldots,w(x))$. Aan de hand van voorbeelden ziet men gemakkelijk in dat deze schrijfwijze niet eenduidig hoeft te zijn. Er is echter één zo'n representatie die bijzonder eenvoudig te bepalen is; deze is als volgt gedefinieerd.

Laat b, c $\in \mathbb{Z}$, $|b|$, $|c| < r$. We noemen het paar (b,c) *toegelaten* als geldt:

als bc > 0 dan $|b+c| < r$,
als bc < 0 dan $|b| > |c|$.



Het toegelaten gebied.

Een schrijfwijze

$$(10.3.1) \qquad x = \sum_{i=0}^{\infty} c_i r^i$$

met $c_i \in \mathbb{Z}$, $|c_i| < r$ voor alle i, en $c_i = 0$ voor i groot genoeg, heet een NAF voor x als voor elke $i \geq 0$ het paar (c_{i+1}, c_i) toegelaten is. In het binaire geval betekent dit $c_{i+1} \cdot c_i = 0$ voor alle i, oftewel: twee naburige "cijfers" mogen niet allebei ongelijk aan nul zijn. De afkorting "NAF", aan het binaire geval ontleend, betekent dan ook "non-adjacent form".

(10.3.2) STELLING. *Elk geheel getal* x *heeft precies één NAF; bovendien, als* (10.3.1) *een NAF is voor* x, *dan is*

$$w(x) = |\{i \mid i \geq 0,\ c_i \neq 0\}|$$

Voor een (onnodig lang) bewijs van deze stelling verwijzen we naar CLARK & LIANG (1973). Daar vindt men ook een algoritme om een NAF voor x te berekenen uitgaande van een willekeurige representatie (10.1.1): men zorgt er eerst voor dat alle n(i) verschillend zijn, zodat de representatie de vorm $x = \sum_{i=0}^{\infty} b_i r^i$ heeft ($|b_i| < r$, en $b_i = 0$ voor i groot genoeg), en dan maakt men, te beginnen bij i = 0, achtereenvolgens alle paren (b_{i+1}, b_i) toegelaten, door zo nodig zo'n paar te vervangen door $(b_{i+1} \pm 1, b_i \mp r)$. We laten de details aan de lezer.

De volgende stelling geeft een andere manier om een NAF voor x te berekenen:

(10.3.3) STELLING. *Zij* $x \in \mathbb{Z}$, $x \geq 0$. *Schrijf* $(r+1).x$ *en* x *in het* r*-tallig stelsel:*

$$(r+1).x = \sum_{j=0}^{\infty} a_j r^j,$$

$$x = \sum_{j=0}^{\infty} b_j r^j$$

met $a_j, b_j \in \{0,1,\ldots,r-1\}$ *voor alle* j, *en* $a_j = b_j = 0$ *voor* j *groot genoeg. Dan wordt de NAF van* x *gegeven door*

$$x = \sum_{j=0}^{\infty} (a_{j+1} - b_{j+1}).\ r^j. \qquad \square$$

Definiëren we de *graad* $gr(x)$ van een geheel getal x door

$$gr(0) = -1$$

$$gr(x) = \max\{i \mid c_i \neq 0\},\ x \neq 0,$$

als (10.3.1) een NAF voor x is, dan kan men eenvoudig bewijzen:

(10.3.4) STELLING. *Zij* $k \in \mathbb{Z}$, $k \geq -1$, *en* $x \in \mathbb{Z}$. *Dan geldt*

$$gr(x) \leq k \Longleftrightarrow |x| < \frac{r^{k+2}}{r+1}. \qquad \square$$

Vervolgens beschouwen we de analoge stellingen voor het *modulaire* gewicht w_m, met $m = r^n - 1$, $n \geq 2$.

We noemen een representatie

$$(10.3.5) \qquad x \equiv \sum_{i=0}^{n-1} c_i r^i \bmod m$$

met $c_i \in \mathbb{Z}$, $|c_i| < r$ een CNAF (= cyclische NAF) voor x modulo m, als (c_{i+1}, c_i) toegelaten is voor $i = 0,1,\ldots,n-1$; hier is $c_n = c_0$.

(10.3.6) STELLING. *Elk geheel getal* x *heeft een CNAF modulo* m*; deze CNAF is uniek behalve als*

$$(r+1)x \equiv 0 \not\equiv x \bmod m$$

in welk geval er twee CNAFs voor x *modulo* m *zijn. Is (10.3.5) een CNAF voor* x *modulo* m, *dan geldt*

$$w_m(x) = |\{i \mid 0 \le i < n,\ c_i \ne 0\}|. \qquad \square$$

(10.3.7) STELLING. *Als* $(r+1)x \equiv 0 \not\equiv x$ *mod* m, *dan geldt* $w_m(x) = n$, *behalve als*

$$n \equiv 0 \text{ mod } 2 \text{ en } x \equiv \pm \frac{m}{r+1} \text{ mod } m,$$

in welk geval geldt $w_m(x) = \frac{1}{2}n$. $\square$

We verwijzen naar CLARK & LIANG (1974) voor meer over CNAF's o.a. voor een algoritme om een CNAF van een geheel getal te bepalen.

Stelling (10.3.4) impliceert gemakkelijk:

(10.3.8) STELLING. *Een geheel getal* x *heeft een CNAF (10.3.5) met* $c_{n-1} = 0$ *dan en slechts dan als er een* $y \in \mathbb{Z}$ *is met*

$$x \equiv y (\text{mod } m),\ |y| \le \frac{m}{r+1}. \qquad \square$$

Heeft x een CNAF (10.3.5), dan wordt een CNAF voor rx gegeven door

$$rx \equiv \sum_{i=0}^{n-1} c_{i-1} r^i \ (\text{mod } m) \ (\text{indices modulo } n).$$

Uit stelling (10.3.6) volgt dus

(10.3.9) $\quad w_m(rx) = w_m(x),$

hetgeen ook direct in te zien is.

Op dezelfde wijze ziet men dat de kopcoëfficiënt c'_{n-1} van de CNAF van $r^j.x$ gelijk is aan de n-1-j-de coëfficiënt c_{n-1-j} van de CNAF van x (aangenomen dat deze CNAF uniek is). Het al of niet nul zijn van c_{n-1-j} kan men dus bepalen door (10.3.8) op $r^j.x$ toe te passen, en men vindt:

(10.3.10) STELLING. *Voor* $x \in \mathbb{Z}$ *geldt*

$$w_m(x) = |\{j \mid 0 \le j < n, \text{ en er is een } y \in \mathbb{Z},$$

$$\frac{m}{r+1} < y \le \frac{mr}{r+1}, \text{ met } r^j x \equiv y \text{ mod } m\}|. \qquad \square$$

10.4. MANDELBAUM-BARROWS CODES

(10.4.1) STELLING. *Zij* $C \subset \mathbb{Z}/(r^n-1)$ *een cyclische AN-code met voortbrenger* A, *en zij* $B = (r^n-1)/A = |C|$. *Dan geldt*

$$\sum_{x\in C} w_m(x) = n.\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right).$$

BEWIJS. Schrijf elke $x \in C$ in CNAF:

$$x = \left(\sum_{i=0}^{n-1} c_{i,x} r^i \bmod (r^n-1)\right),$$

dan moeten we het aantal coëfficiënten ongelijk aan nul van de matrix $(c_{i,x})_{0\le i\le n-1,\ x\in C}$ bepalen.
Neem voor de eenvoud aan dat elke $x \in C$ een *unieke* CNAF heeft. Dan bevat elke kolom van de matrix $(c_{i,x})$ evenveel nullen, wegens het cyclische karakter van de code. Dus het gevraagde aantal is

$$n.\ |\{x \in C|\ c_{n-1,x} \neq 0\}|.$$

Bezit x een unieke CNAF, dan is wegens (10.3.8) de kopcoëfficiënt $c_{n-1,x}$ hiervan ongelijk aan nul dan en slechts dan als er een $y \in \mathbb{Z}$ is met

$$x = (y \bmod r^n-1),\ \frac{m}{r+1} < y \le \frac{mr}{r+1}.$$

Schrijven we $x = (AN \bmod r^n-1)$, $0 \le N < B$, dan betekent dit

$$\frac{B}{r+1} < N \le \frac{Br}{r+1}.$$

Het aantal van zulke N is kennelijk $\left\lfloor\frac{Br}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor$.

Het geval dat C een element met twee CNAFs bevat vereist enige extra zorg, die aan de lezer toevertrouwd kan worden. □

De uitdrukking in (10.4.1) is ongeveer gelijk aan

$$n.|C|.\frac{r-1}{r+1}.$$

Vergelijk hiermee het analoge resultaat voor cyclische codes over GF(q): is C zo'n code, met woordlengte n, dan

$$\sum_{x\in C} w_H(x) = n.\ |C|.\ \frac{q-1}{q} \qquad (w_H = \text{Hamming-gewicht}).$$

De volgende stelling beschrijft de gegeneraliseerde Mandelbaum-Barrows codes, zie MASSEY & GARCIA (1972) voor referenties voor het binaire geval. Een code heet *equidistant* als $d_m(x,x') = d_m(y,y')$ voor alle $x,x',y,y' \in C$, $x \neq x'$, $y \neq y'$.

(10.4.2) <u>STELLING</u>. *Zij* B *een priemgetal dat* r *niet deelt, met de eigenschap dat* $(\mathbb{Z}/B\mathbb{Z})^*$ *wordt voortgebracht door de restklassen van* r *en* -1. *Zij* n *een positief geheel getal met* $r^n \equiv 1$ *mod* B, *en laat* $A = (r^n-1)/B$. *Dan is de code* $C \subset \mathbb{Z}/(r^n-1)$ *voortgebracht door* A *equidistant met afstand*

$$\frac{n}{B-1}\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right).$$

<u>BEWIJS</u>. Zij $x \in C$, $x \neq 0$ willekeurig; dan geldt $x = (AN \bmod r^n-1)$, met $N \not\equiv 0 \bmod B$. De aannamen van de stelling impliceren dat $N \equiv \pm r^j \bmod B$ voor zekere j, dus $w_m(x) = w_m(\pm r^j A) = w_m(A)$ (wegens (10.3.9)). Hieruit blijkt dat alle elementen van C ongelijk nul hetzelfde modulaire gewicht hebben, dus C is equidistant. De afstand berekenen we met (10.4.1):

$$w_m(A) = \frac{1}{B-1}\sum_{x\in C,\ x\neq 0} w_m(x) = \frac{n}{B-1}\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right). \qquad \square$$

We merken op dat de woordlengte n in (10.4.2) ten minste $\frac{B-1}{2}$ is; dit is nogal groot ten opzichte van het aantal codewoorden, nl. B. Voor de praktijk lijken de Mandelbaum-Barrows codes dan ook niet belangrijk.

De Mandelbaum-Barrows codes corresponderen met de "maximum-length" codes over eindige lichamen. Dit zijn cyclische codes met woordlengte q^k-1 waarvan het check polynoom h(x) een primitief irreducibel polynoom van graad k is (*primitief* betekent dat de nulpunten van h(x) multiplicatieve orde q^k-1 hebben). Deze codes zijn equidistant met afstand $(q-1).q^{k-1}$. (Zie § 5.2).

Er bestaan generalisaties van (10.4.2) voor het geval B een natuurlijk getal, relatief priem met r, is, met de eigenschap dat de groep van eenheden $(\mathbb{Z}/B\mathbb{Z})^*$ van de ring $\mathbb{Z}/B\mathbb{Z}$ wordt voortgebracht door (r mod B) en (-1 mod B). In dit geval hoeft de verkregen AN-code C niet equidistant te zijn, maar wel is het zo dat het modulaire gewicht van een codewoord alleen van zijn orde in de groep C ($\cong \mathbb{Z}/B\mathbb{Z}$) afhangt. Door (10.4.1) op subcodes van C toe te passen kan men dan met Moebius-inversie de gewichtsenumerator van C opstellen; vergelijk TSAO-WU & CHANG (1969) voor het binaire geval. Voor deze codes geldt hetzelfde als voor de Mandelbaum-Barrows codes: een grote woordlengte en slechts weinig codewoorden.

Tenslotte noemen we een methode waarmee men de gewichten van een gegeven cyclische AN-code $C \subset \mathbb{Z}/(r^n-1)$ kan bepalen. Zij A de voortbrenger, en $AB = r^n - 1 = m$. Met H geven we de ondergroep van $(\mathbb{Z}/B\mathbb{Z})^*$ aan die wordt voortgebracht door de restklassen van r en -1. De groep H werkt op $\mathbb{Z}/B\mathbb{Z}$ door vermenigvuldiging; voor $N \in \mathbb{Z}$ geven we de baan van (N mod B) onder H met H.N aan:

$$H.N = \{\pm r^j N \bmod B \mid j = 0,1,2,\ldots\} \subset \mathbb{Z}/B\mathbb{Z}.$$

(10.4.3) <u>STELLING</u>. *Het modulaire gewicht* $w_m(AN)$ *hangt alleen van de baan* H.N *af; er geldt*

$$w_m(AN) = n.\frac{\left|HN \cap \{y \bmod B \mid \frac{B}{r+1} < y \le \frac{Br}{r+1}\}\right|}{|HN|}$$

<u>BEWIJS</u>. Dit is in essentie een herformulering van (10.3.10). □

(10.4.4) <u>VOORBEELD</u>: r = 2, B = 109, n = 36. De groep $H \subset (\mathbb{Z}/109\,\mathbb{Z})^*$ heeft orde 36, en $\mathbb{Z}/109\,\mathbb{Z}$ valt onder H in vier banen uiteen:

H.0, H.1, H.3, H.9.

Doorsnijdt men deze banen met $\{y \bmod 109 \mid \frac{109}{3} < y \le \frac{2.109}{3}\} =$ $= \{37, 38, \ldots, 72\}$, dan vindt men

$\emptyset$, {±38, ±41, ±43, ±45, ±46, ±54},

{±40, ±48, ±51, ±52, ±53}, {±37, ±39, ±42, ±44, ±47, ±49, ±50},

dus de AN-code $C \subset \mathbb{Z}/(2^{36}-1)$ voortgebracht door $A = (2^{36}-1)/109$ heeft één element met gewicht 0 (het nul-element van C); 36 elementen met gewicht 12; 36 elementen met gewicht 10; en 36 elementen met gewicht 14. Er volgt $d_{min}(C) = 10$. Zie MASSEY & GARCIA (1972) § 3.6 voor meer voorbeelden.

In SEGUIN (1973) vindt men een manier om uit (10.4.3) een ondergrens voor $d_{min}(C)$ af te leiden.

10.5. CHEN-CHIEN-LIU CODES

De reeds vaker vermelde analogie met cyclische codes over een eindig lichaam heeft de gedachte in het leven geroepen dat er een klasse AN-codes bestaat die correspondeert met de klasse der BCH-codes. Voor een inmiddels weerlegd vermoeden hierover zie men MASSEY & GARCIA (1972) § 3.7.

De enige bekende klasse AN-codes die enigszins doet denken aan BCH-codes wordt beschreven door de volgende stelling, die men voor $r = 2$ kan vinden bij CHEN, CHIEN & LIU (1974).

(10.5.1) STELLING. *Laten* a *en* b *twee onderling ondeelbare getallen* ≥ 2 *zijn. Dan heeft de cyclische AN-code* $C \subset \mathbb{Z}/(r^{ab}-1)$ *voortgebracht door*

$$A = \frac{(r^{ab}-1)\ (r-1)}{(r^{a}-1)\ (r^{b}-1)}$$

minimum-afstand gelijk aan min $\{a,b\}$.

Dat de minimumafstand van C ten hoogste $\min\{a,b\}$ is blijkt uit de aanwezigheid van de codewoorden $(r^{ab}-1)/(r^{a}-1) = \sum_{i=0}^{b-1} r^{ia}$ en $(r^{ab}-1)/(r^{b}-1) = \sum_{j=0}^{a-1} r^{jb}$. De andere ongelijkheid is minder evident. Beneden schetsen we een bewijs voor het binaire geval, uitgaande van de onvolledige argumentatie van CHEN, CHIEN & LIU (1974), § 4. Het algemene geval laten we aan de lezer over, zie (10.6.3).

De analogie met BCH-codes is als volgt. Is q een priemmacht, en zijn a, b twee onderling ondeelbare getallen ≥ 2 met $(ab,q) = 1$, dan heeft het polynoom

$$g(x) = \frac{(x^{ab}-1)\ (x-1)}{(x^{a}-1)\ (x^{b}-1)} \in GF(q)[x]$$

min {a,b} - 1 "opeenvolgende" nulpunten

$$\alpha,\ \alpha^2,\ \ldots\ ,\ \alpha^{\min\{a,b\}-1}$$

waar α een primitieve ab-de eenheidswortel in een uitbreiding van GF(q) voorstelt. De BCH-grens impliceert dan dat de code

$$(g(x)) \subset GF(q)[x]/(x^{ab}-1)$$

minimum-afstand $\geq \min\{a,b\}$ heeft. In feite is de minimum-afstand *gelijk* aan $\min\{a,b\}$, want $(g(x))$ bevat de codewoorden $\sum_{i=0}^{b-1} x^{ia}$ en $\sum_{j=0}^{a-1} x^{jb}$.

We merken op dat de voorwaarde $(ab,q) = 1$ overbodig is: dit blijkt te volgen uit de methode waarmee (10.5.1) bewezen wordt.

<u>BEWIJS</u> van (10.5.1) voor $r = 2$. Zij $m = 2^{ab}-1$, en $y = AN \in C$, $y \neq (0 \bmod m)$. We moeten bewijzen dat $w_m(y) \geq \min\{a,b\}$.

Zetten we $x = (2^a-1).y = 2^a.y-y$, dan geldt wegens (10.3.9):

(10.5.2) $\quad w_m(x) \leq w_m(2^a.y) + w_m(y) = 2.w_m(y).$

Verder $x = N.(2^{ab}-1)/(2^b-1)$, dus

$$2^b x \equiv x \bmod m.$$

Dit betekent dat we, door de cijfers van een CNAF van x modulo m over b plaatsen op te schuiven, opnieuw een CNAF van x modulo m krijgen. Heeft x een unieke CNAF modulo m, dan kan dit alleen als deze CNAF periode b heeft:

$$x \equiv \sum_{i=0}^{ab-1} c_i 2^i \mod m, \qquad c_i = c_{i+b} \text{ als } 0 \leq i < ab-b.$$

In het uitzonderlijke geval dat x <u>twee</u> CNAF's modulo m bezit blijkt deze periodiciteit voor beide te gelden. Dus

$$w_m(x) = a.|\{i \mid 0 \leq i < b,\ c_i \neq 0\}|$$

en dit is deelbaar door a. Als $w_m(x) \geq 2a$, dan $w_m(y) \geq a$ wegens (10.5.2), en we zijn klaar. Als $w_m(x) = 0$, dan $x \equiv 0 \bmod m$, dus $2^a y \equiv y \bmod m$, en hieruit volgt op analoge wijze dat $w_m(y)$ deelbaar is door b, dus inderdaad $w_m(y) \geq b \geq \min\{a,b\}$ als $w_m(y) \neq 0$. We concluderen dat we alleen blijven zitten met het geval $w_m(x) = a$.
Dan

$$x \equiv \varepsilon \cdot \sum_{\ell=0}^{a-1} 2^{i+\ell b} = \varepsilon \cdot 2^i \cdot \frac{2^{ab}-1}{2^b-1} \mod m$$

voor een $\varepsilon \in \{\pm 1\}$ en een $i \in \{0,1,\ldots,b-1\}$. Wegens $x = N \cdot (2^{ab}-1)/(2^b-1)$ impliceert dit

$$N \equiv \varepsilon \cdot 2^i \mod (2^b-1).$$

Verwisseling van a en b toont aan dat we ook mogen aannemen

$$N \equiv \eta \cdot 2^j \mod (2^a-1)$$

voor een $\eta \in \{\pm 1\}$ en een $j \in \{0,1,\ldots,a-1\}$. Kies nu $k \in \{0,1,\ldots,ab-1\}$ met $k \equiv -i \bmod b$ en $k \equiv -j \bmod a$, en vervang N door $\varepsilon \cdot 2^k \cdot N$. Dit verandert $w_m(NA)$ niet, en we krijgen

$$N \equiv 1 \mod (2^b-1), \qquad N \equiv \pm 1 \mod (2^a-1).$$

Wegens $(2^a-1, 2^b-1) = 1$ blijven er voor N dan slechts 2 waarden over modulo $(2^a-1)(2^b-1)$; en omdat (NA mod m) alleen afhangt van (N mod $(2^a-1)(2^b-1)$), zien we dat we nog slechts met twee codewoorden y te maken hebben. Het eerste correspondeert met N = 1, en is de voortbrenger van de code: y = A. Het tweede noemen we A'; het is bepaald door

(10.5.3) $\quad A' \equiv A \mod (2^{ab}-1)/(2^a-1)$

(10.5.4) $\quad A' \equiv -A \mod (2^{ab}-1)/(2^b-1).$

We moeten bewijzen

$$w_m(A) \geq \min\{a,b\}, \qquad w_m(A') \geq \min\{a,b\}.$$

(10.5.5) LEMMA. Stel $x \equiv \sum_{i=0}^{ab-1} \varepsilon_i 2^i \bmod m$, met $\varepsilon_i \in \{0,1,-1\}$ voor alle i, en $\varepsilon_i = 0$ voor ten minste één i, zodanig dat

(10.5.6) er is geen i met $\varepsilon_i = \varepsilon_{i+1} \neq 0$

(indices modulo ab). Dan geldt

$$w_m(x) \geq |\{i \mid \varepsilon_i = 1\}|.$$

BEWIJS (schets): roteer x zó, dat $\varepsilon_{ab-1} = 0$, en bereken de NAF van $\sum \varepsilon_i 2^i$ volgens de algoritme gegeven na (10.3.2); dit blijkt een CNAF $\sum c_i 2^i$ voor x mod m te leveren met de eigenschap $\varepsilon_i = 1 \Rightarrow c_i \neq 0$ of $c_{i-1} \neq 0$. □

Kies gehele getallen λ en μ met

$$\lambda a \equiv 1 \bmod b, \qquad 1 \leq \lambda \leq b,$$
$$\mu b \equiv 1 \bmod a, \qquad 1 \leq \mu \leq a.$$

Eenvoudig bewijst men

$$\lambda a + \mu b = 1 + ab$$

(10.5.7) $\lambda \cdot \mu \geq \min\{a,b\}$.

Verder zetten we

$$f = \frac{(X^{ab}-1)(X-1)}{(X^a-1)(X^b-1)}.$$

(10.5.8) LEMMA. (a) Er geldt

$$f = \sum_{i=0}^{\lambda-1} \sum_{j=0}^{\mu-1} X^{ia+jb} - \sum_{i=\lambda}^{b-1} \sum_{j=\mu}^{a-1} X^{ia+jb-ab}.$$

(b) Als $V = \{sa+tb \mid s,t \in \mathbb{Z}_{\geq 0}\}$, dan

$$f = (1-X) \cdot \sum_{v \in V} X^v.$$

(c) f is een polynoom van de graad $(a-1)(b-1)$, en de coëfficiënten van f die ongelijk aan nul zijn, zijn afwisselend +1 en -1.

BEWIJS: overgelaten aan de lezer; de laatste bewering van (c) volgt uit (b). □

Het bewijs van $w_m(A) \geq \min\{a,b\}$ is nu niet lastig meer: we hebben $A = f(2)$, en wegens (10.5.8)(c) geeft dit een representatie van A waarop we lemma (10.5.5) kunnen toepassen. Met behulp van (10.5.8)(a) en (10.5.7) vinden we dan

$$w_m(A) \geq \lambda \cdot \mu \geq \min\{a,b\},$$

zoals verlangd.

Om A' te kunnen behandelen voeren we een nieuwe notatie in. We zeggen dat een $b \times a$-matrix $(e_{ij})_{0 \leq i < b,\ 0 \leq j < a}$ met gehele coëfficiënten een geheel getal x representeert als

$$x \equiv \sum_{i=0}^{b-1} \sum_{j=0}^{a-1} e_{ij} 2^{ia+jb} \mod (2^{ab}-1).$$

Omdat elk geheel getal k modulo ab eenduidig te schrijven is als $ia + jb$, met $0 \leq i < b$ en $0 \leq j < a$, kunnen we elke "gewone" ontwikkeling $x \equiv \sum_{k=0}^{ab-1} e_k 2^k \mod (2^{ab}-1)$ in matrix-vorm brengen, en omgekeerd. Het getal $A = f(2)$ kunnen we wegens (10.5.8)(a) bijvoorbeeld representeren door de matrix

(10.5.9)
$$\begin{array}{c} \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & -1 \end{array}\right] \begin{array}{l} \}\ \lambda \\ \}\ b-\lambda \end{array} \\ \begin{array}{cc} \underbrace{\quad}_{\mu} & \underbrace{\quad}_{a-\mu} \end{array} \end{array}$$

(de "1" linksboven slaat hier op een $\lambda\times\mu$-matrix vol met enen, etc.). De congruentie $2 \equiv 2^{\lambda a+\mu b} \bmod (2^{ab}-1)$ toont dat het "cyclisch opschuiven" van een schrijfwijze $\sum e_k 2^k$er in matrix-notatie op neerkomt dat de rijen over een verticale afstand λ cyclisch worden opgeschoven, en de kolommen over een horizontale afstand μ. Bovenstaand voorbeeld geeft dan

$$\begin{array}{c} \left[\begin{array}{c|c|c} 0 & 1 & 0 \\ \hline -1 & 0 & -1 \\ \hline 0 & 1 & 0 \end{array}\right] \begin{array}{l} 2\lambda-b \\ b-\lambda \\ b-\lambda \end{array} \\ \begin{array}{ccc} \mu & \mu & a-2\mu \end{array} \end{array}$$

We zien dat deze matrix en matrix (10.5.9) op geen enkele plaats dezelfde coëfficiënt $\neq 0$ hebben staan. Dit bewijst opnieuw dat de representatie (10.5.9) voor A voldoet aan conditie (10.5.6) van lemma (10.5.5). Ter rechtvaardiging van het plaatje merken we op dat we zonder verlies van algemeenheid mogen aannemen

$$\lambda > \tfrac{1}{2}\, b, \qquad \mu \leq \tfrac{1}{2}\, a,$$

zoals de lezer eenvoudig nagaat.

Het blijkt dat deze techniek zich ook laat toepassen op A'. We kunnen A' laten representeren door

$$\text{(10.5.10)} \qquad \begin{array}{c} \left[\begin{array}{c|c} 0 & 1 \\ \hline -1 & 0 \end{array}\right] \begin{array}{l} \lambda \\ b-\lambda \end{array} \\ \begin{array}{cc} \mu & a-\mu \end{array} \end{array}$$

Immers, trekken we deze matrix af van (10.5.9), dan vinden we een matrix waarvan alle rijen gelijk zijn, en die dus een getal representeert dat deelbaar is door $(2^{ab}-1)/(2^{a}-1)$, in overeenstemming met (10.5.3). Evenzo controleert men (10.5.4) door beide matrices op te tellen.

De bovenbeschreven cyclische opschuiving geeft ons de volgende representatie voor 2.A':

(10.5.11)
$$\begin{array}{c|c} \left[\begin{array}{c|c|c} 1 & 0 & 1 \\ \hline 0 & -1 & 0 \\ \hline 1 & 0 & 1 \end{array}\right] & \begin{array}{l} 2\lambda-b \\ b-\lambda \\ b-\lambda \end{array} \\ \begin{array}{ccc} \mu & \mu & a-2\mu \end{array} & \end{array}$$

De 1 rechtsboven laat evenwel zien, dat (ingeval $\mu<\frac{1}{2}a$) de representatie (10.5.10) niet aan conditie (10.5.6) voldoet. Trekken we (10.5.10) af van (10.5.11) dan krijgen we de matrix

$$\left[\begin{array}{c|c|c} 1 & -1 & 0 \\ \hline 0 & -2 & -1 \\ \hline 2 & 0 & 1 \end{array}\right]$$

die het getal 2A'-A' = A' representeert. De 2 linksonder valt gelukkigerwijze weg tegen de helft van de -2 in het midden, dus A' wordt ook gerepresenteerd door

(10.5.12)
$$\left[\begin{array}{c|c|c} 1 & -1 & 0 \\ \hline 0 & -1 & -1 \\ \hline 0 & \underbrace{0}_{\mu} & 1 \end{array}\right] \begin{array}{l} \left.\begin{array}{l} \\ \\ \end{array}\right\} \lambda \\ \\ \end{array}$$

Een ogenblik staren op deze matrix voert tot het inzicht dat deze representatie voor A' inderdaad aan (10.5.6) voldoet. Passen we dus (10.5.5) toe (met x = -A') dan vinden we dat $w_m(A')$ ten minste gelijk is aan het aantal

coëfficiënten -1 in (10.5.12), en dat is $\geq \lambda \cdot \mu \geq \min\{a,b\}$, wegens (10.5.7). $\square$

10.6. OPGAVEN

(10.6.1) Bewijs dat

$$\min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\} \leq 2$$

voor alle $A \in \mathbb{Z}$.

(10.6.2) Generaliseer de resultaten van §§ 10.2 t/m 10.4 voor het negacyclische geval.

(10.6.3) Voer het bewijs van (10.5.1) door voor $r > 2$.

LITERATUUR

AX, J., *Zeroes of polynomials over finite fields*, Am.J.Math. 86 (1964), 255-261.

BAUMERT, L.D. & R.J. McELIECE, *A note on the Griesmer bound*, IEEE Trans. Inform. Theory 19 (1973) 134-135.

BERLEKAMP, E.R., *Algebraic Coding Theory*, McGraw Hill, New York (1968).

BERLEKAMP, E.R. and O. MORENO, *Extended double-error-correcting binary Goppa codes are cyclic*, IEEE Trans. Inform. Theory 19 (1973) 817-818.

BEST, M.R. & A.E. BROUWER, *The triply shortened binary Hamming code is optimal*, Discr. Math., 17 (1977) 235-245.

BEST, M.R., A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than 25*, IEEE Trans. on Information Theory 24 (1978) 81-93.

BLAKE, I.F. & R.C. MULLIN, *The mathematical theory of coding*, Academic Press, New York (1975).

BOYARINOV, I.M. & G.A. KABATYANSKY, *On perfect arithmetic AN-codes*, Int. Symp. Inf. Theory Talin, SSSR, (1973), pp. 41-43 (Russisch).

CAMERON, P.J. & J.H. VAN LINT, *Graph Theory, Coding Theory and Block Designs*, London Math. Soc. Lecture Note Series 19, Cambr. Univ. Press, (1975).

CHEN, C.L., R.T. CHIEN & C.K. LIU, *On the binary representation form of certain integers*, SIAM J. Appl. Math. 26 (1974), 285-293.

CHEVALLEY, C., *Demonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Hamburg 11 (1936), 73-75.

CHIEN, R.T. & D.M. CHOY, *Algebraic generalization of BCH-Goppa-Helgert codes*, IEEE Trans. Inform. Theory (1975), pp. 70-79.

CLARK, W.E. & J.J. LIANG, *On arithmetic weight for a general radix representation of integers*, IEEE Trans. Inform. Theory IT-19 (1973), 823-826.

—— *On modular weight and cyclic nonadjacent forms for arithmetic codes*, IEEE Trans. Inform. Theory IT-20 (1974), 767-770.

DELSARTE, P., *Bounds for unrestricted codes, by linear programming*, Philips Res. Repts. 27 (1972), 272-289.

DELSARTE, P., *An algebraic approach to the association schemes of coding theory*, Philips Res. Repts. Suppl. (1973) no. 10.

DELSARTE, P., J.M. GOETHALS and F.J. MAC WILLIAMS, *On generalized Reed-Muller codes and their relatives*, Inf. and Control 16 (1970), 403-442.

DICKSON, L.E., *Theory of Numbers*, Vol. I, p. 271, Chelsea (1952).

FORNEY, Jr. G.D., *Concatenated Codes*, M.I.T. Press, Cambridge, Mass. (1966).

GILBERT, E.N., *A comparison of signalling alphabets*, Bell Syst. Tech. J. 31 (1952), 504-522.

GOETHALS, J.M., *On the Golay perfect binary code*, J. Comb. Theory 11 (1971), 178-186.

GOETHALS, J.M. & H.C.A. VAN TILBORG, *Uniformly packed codes*, Philips Res. Repts. 30 (1975), 9-36.

GOLAY, M.J.E., *Notes on digital coding*, Proc. IRE. 37 (1949), 657.

GOPPA, V.D., *A new class of linear error-correcting codes*. Problems of Information Transmission (1973), pp. 207-212 = Problemy Peredachi Informatsii 1970, Vol. 6, No. 3, pp. 24-30.

-- *A rational representation of codes and* (L,g)*-codes*. Ibid (1973), pp. 223-229 (1971, Vol. 7, No. 3, pp. 41-49).

-- *Codes constructed on the base of* (L,g) *codes*. Ibid (1974), pp. 165-166 (1972, Vol. 8, No. 2, pp. 107-109).

GOTO, M., *A note on perfect decimal AN codes*, Inform. & Control 29 (1975) 385-387.

GOTO, M. & T. FUKUMURA, *Perfect nonbinary AN codes with distance three*, Information and Control 27 (1975), 336-348.

GRIESMER, J.H., *A bound for error correcting codes*, IBM J. Res. & Dev. 4 (1960), 532-542.

GRITSENKO, V.M., *Nonbinary arithmetic correcting codes*, Problems of Information Transmission 5 (1969), 15-22.

HALL, Jr, M., *Combinatorial Theory*, Blaisdell, Waltham, Mass. (1967).

HAMMING, R.W., *Error detecting and error correcting codes*, Bell Syst. Tech. J. 29 (1950), 147-160.

HARTMANN, C.R.P. & K.K. TZENG, *Generalization of the* BCH *bound*, Inf. & Control 20 (1972) 489-498.

HELGERT, H.J. & R.D. STINAFF, *Minimum-distance bounds for binary linear codes*, IEEE Trans. Inform. Theory 19, no. 3 (1973), 344-356.

JOHNSON, S.M., *A new upper bound for error correcting codes*, IRE Trans. Inform. Theory 8 (1962), 203-207.

-- *Improved asymptotic bounds for error correcting codes*, IEEE Trans. Inform. Theory 9 (1963), 193-205.

-- *On upper bounds for unrestricted binary error-correcting codes*, IEEE Trans. Inform. Theory 17 (1971), 466-478.

JOLY, J.R., *Equations et variétés algebriques sur un corps fini*, Enseign. Math. 19 (1973)

JUSTESEN, J., *A Class of Constructive Asymptotically Good Algebraic Codes*, IEEE Trans. on Inform. Theory, IT 18, 1972, 652-656.

KASAMI, T., *An upper bound on* k/n *for affine invariant codes with fixed* d/n, IEEE Trans. Inform. Theory 15 (1969), 171-176.

LEVENSHTEIN, V.I., *On the Minimal Redundancy of Binary Error-Correcting Codes*, Inf. and Control 28 (1975), 268-291.

LIN, S. & E.J. WELDON, *Long* BCH *codes are bad*, Inf. and Control 11 (1967), 445-451.

LINDSTRÖM, K., *The nonexistence of unknown nearly perfect binary codes*, Ann. Univ. Turku A 169 (1975).

VAN LINT, J.H., *Coding Theory*, Lecture Notes in Math. 201, Springer Verlag, Berlin etc. (1971).

-- *Recent results on perfect codes and related topics*, Combinatorics Part 1, Math. Centre Tracts 55 (1974), 158-178.

-- *A survey of perfect codes*, Rocky Mount. J. of Math. 5 (1975), 199-224.

LLOYD, S.P., *Binary block coding*, Bell System Tech. J. 36 (1957), 517-535.

McELIECE, R.J., E.R. RODEMICH, H.C. RUMSEY jr. & L.R. WELCH, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, to appear.

MacWILLIAMS, F.J., *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. 42 (1963), 79-94.

MASSEY, J.L., *Threshold Decoding*, M.I.T. Press, Cambridge, Mass. (1963).

MASSEY, J.L., D.J. COSTELLO & J. JUSTESEN, *Polynomial Weights and Code Construction*, IEEE Trans. on Inform. Theory, IT-19 (1973), 101-110.

MASSEY, J.L. & O.N. GARCIA, *Error-correcting codes in computer arithmetic*, Advances in Information Systems Science (J.T. Tou, ed.), 4, Ch. 5 (273-326), Plenum Press, (1972).

NEUMANN, P.G. & T.R.N. RAO, *Error-correcting codes for byte-organized arithmetic processors*, IEEE Trans. Computers C-24 (1975), 226-232.

NORDSTROM, A.W. & J.P. ROBINSON, *An optimal nonlinear code*, Inform. Contr. 11 (1967), 613-616.

PETERSON, W.W. & E.J. WELDON, JR., *Error-correcting codes*, Second edition, The MIT Press, (1972).

PLOTKIN, M., *Binary codes with specified minimum distance*, IEEE Trans. Inform. Theory 6 (1960), 445-450.

POSNER, E.C., *Combinatorial Structures in Planetary Reconnaissance*, p. 15-46 in H.B. MANN, Error correcting codes, Wiley, New York, 1968.

RAO, T.R.N., *Error coding for arithmetic processors*, Academic Press, New York-London, (1974).

RETTER, C.T., *Decoding Goppa codes with a* BCH *decoder*, IEEE Trans. Inform. Theory 21 (1975), 112.

SEGUIN, G., *Bounds for certain cyclic AN-codes*, Information and Control 23 (1973), 41-47.

SHANNON, C.E., *Mathematical Theory of Communication*, Bell System Tech. J. 27 (1948) 379-423.

SIDELNIKOV, V.M., *Upper Bounds on the Cardinality of a Binary Code with a Given Minimum Distance*, Inf. and Control 28 (1975), 292-303.

SLOANE, N.J.A., *A survey of constructive coding theory, and a table of binary codes of highest known rate*, Discrete Math. 3 (1972), 265-294.

SLOANE, N.J.A., S.M. REDDY & C.L. CHEN, *New binary codes*, IEEE Trans. Inform. Theory IT-18 (1972), 503-510.

SLOANE, N.J.A. & D.S. WHITEHEAD, *A new family of single-error-correcting codes*, IEEE Trans. Inform. Theory, IT-16 (1970), 717-719.

SZEGÖ, G., *Orthogonal polynomials*, A.M.S. Coll. Publ. 23 (1959).

VAN TILBORG, H.C.A., *All binary* (n,e,r)*-uniformly packed codes are known*, Memorandum 1975-08, T.H. Eindhoven (1975).

TSAO-WU, N.T. & S.-H. CHANG, *On the evaluation of minimum distance of binary arithmetic cyclic codes*, IEEE Trans. Inform. Theory IT-15 (1969), 628-631.

TZENG K.K. and K. ZIMMERMAN, *On extending Goppa codes to cyclic codes*, IEEE Trans. Inform. Theory 21 (1975), 712-715.

WARNING, E., *Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Hamburg 11 (1936), 76-83.