Errata syllabus studieweek inleiding in de coderingstheorie. (ZC 87/75)

(Een kleine selectie uit een tamelijk groot aantal onnauwkeurigheden, spel- en schoonheidsfouten).

pagina		correctie	
inhoud	r-6 :	Ir. H.C.A. van Tilborg	(ipv drs)
I-5	r-6 :	$\leq$	(ipv =)
II-2	r-11:	...is een code waarin in ieder codewoord de eerste k	
III-2	r+17:	A	(ipv Mmax)
III-4	r+5 :	(afgeleid van de Nordstrom-Robinson code)	
	r+5 :	[13,5]	(ipv [13,4])
III-8	r+4 :	(waaronder een constante)	
III-11	r+5 :	$0 \leq \lambda < \theta - \sqrt{\theta(\theta-\delta)}$	
	r+11:	$\lambda \in [0, \theta - \sqrt{\theta(\theta-\delta)})$	
	r-9 :	M_0^y	
	r-8 :	tot het woord y.	
III-12	r+9 :	als we M_r^0 met 0 schatten,	
II-15	r+3 :	$= \sum_{\substack{z\in Q^n \\ w_H(z)=r}} \left\| \sum_{x\in C} \omega^{<x,z>} \right\|^2 \geq 0$	
	r+6 :	$A_i \geq 0$	(ipv $A_i \in N$)
IV-3	r-7 :		(ipv niet triviale)
IV-6	r+13:	$v < (q-1)m$	
V-3	rr+7/+12:	{verwijder matrix haken}	
V-7	rr+7/+13:	{voeg matrix haken toe}	
V-10	r-8 :	posities	(ipv symbolen)
VI-6	r+17:	$d = 2e + 3$	
	r-1 :	$r = \left\lceil \frac{n}{e+1} \right\rceil$	
VI-11	rr+4/+5:	$m_1(x)$ het minimaalpolynoom van α en $m_3(x)$ van α^3.	
VI-13	r+4 :	$X_e - X_1 \geq \frac{1}{3} n$	
	r+6 :	$= \frac{1}{2} e^2(e-1) (n - \frac{2e-1}{3})$	
	r+8 :	$\leq e \sqrt{\frac{1}{2}} n$	
	r+10:	$\leq \frac{9}{2} e^2$	
VI-14	r+2 :	$(X_{e+1} - X_1) \leq$	
	r+7(2X)	g.g.d.	(ipv k.g.v)
VII-6	r+2 :	MATTSON	
VII-8	r+2 :	$GF(q^m)$	
	r+4 :	$n \leq q^m$	
VIII-3	r-10:	$W_m((X \bmod m))$ ook wel $d_m(x,y)$ en	
	r-7 :	$W_m(x-y)$	
VIII-15	r-7 :	inmiddels weerlegd	(ipv onbewezen)

stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZC 87/75 AUGUSTUS

STUDIEWEEK

INLEIDING IN DE CODERINGSTHEORIE

2e boerhaavestraat 49 amsterdam

STUDIEWEEK

INLEIDING IN DE CODERINGSTHEORIE

I N H O U D

Hoofdstuk I

DE STELLING VAN SHANNON

door

J.H. van Lint

Om een idee te krijgen van de practische oorsprong van Coding Theory 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 het helaas zo dat er een kans p is dat een 0 resp. 1 aankomt als 1 resp. 0. 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. Neem nu als voorbeeld p = 0,001. De kans dat de ontvanger verkeerd decodeert is dan

$$\sum_{k=0}^{N/2} \binom{N}{k} q^k p^{N-k} < (0{,}07)^N, \qquad (q = 1-p),$$

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

Nu we aan de gegeven snelheden gebonden zijn is de zaak veel lastiger. Ieder symbool 2 keer zenden heeft geen zin! De fundamentele stelling van Shannon uit de informatie-theorie zegt dat ondanks deze beperking toch willekeurig grote nauwkeurigheid is te bereiken. Een eerste idee over de metho-

de 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 een *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 gemiddeld 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!

We geven nu het bewijs van de stelling van Shannon voor dit voorbeeld. 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

$$(1) \qquad P_C := \text{de kans op een fout} = M^{-1} \sum_{i=1}^{N} P_i \ .$$

Definieer nu

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

Dan is:

STELLING van SHANNON: *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 zijn alle logaritmen met grondtal 2.)

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

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 $b := (\frac{np(1-p)}{\varepsilon/2})^{\frac{1}{2}}$ dan is volgens Bienaymé-Chebyshev:

$$(3) \qquad P(w > np+b) \leq \tfrac{1}{2}\varepsilon.$$

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

---

*) Hamming-afstand van twee woorden is het aantal plaatsen waar ze verschillen.

$$(4) \qquad |S_\rho(\underline{x})| = \sum_{w \le \rho} \binom{n}{w} < \tfrac{1}{2}n\binom{n}{\rho} \le \tfrac{1}{2}n\frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}} \quad .$$

Hierin volgt de laatste ongelijkheid uit

$$n^n = \{\rho + (n-\rho)\}^n = \ldots + \binom{n}{\rho}\, \rho^\rho (n-\rho)^{n-\rho} + \ldots \ .$$

Er geldt

$$(5) \qquad \frac{\rho}{n} \log \frac{\rho}{n} = \frac{1}{n}[np + b] \log \frac{[np + b]}{n} = p \log p + O(n^{-\frac{1}{2}})$$

en evenzo

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

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

$$(6) \qquad f(\underline{u},\underline{v}) := \begin{cases} 0 & \text{als} \quad d_H(\underline{u},\underline{v}) > \rho \\ 1 & \text{als} \quad d_H(\underline{u},\underline{v}) \le \rho. \end{cases}$$

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

$$(7) \qquad g_i(\underline{y}) := 1 - f(\underline{y},\underline{x}_i) + \sum_{j \neq 1} f(\underline{y},\underline{x}_j).$$

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 $g_i(\underline{y}) \ge 1$.

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 verschillende 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 $\underline{y} \notin S_\rho(\underline{x}_i)$. Deze kans hangt alleen van ρ en niet van $\underline{x}_i$ af. Noem die kans α_ρ. Volgens (3) is $\alpha_\rho \le \frac{1}{2}\varepsilon$. Volgens (1) is

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

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

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

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

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

Door de log te nemen, (4) en (5) te gebruiken en door n te delen, vinden we

$$n^{-1} \log(P^*(M,n,p) - \frac{\varepsilon}{2}) = n^{-1} \log M - (1 + p \log p + q \log q) + O(n^{-\frac{1}{2}}).$$

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

Hiermee is de stelling bewezen. □

Hoofdstuk II

LINEAIRE CODES

door

T.M.V. Janssen

1. BLOK CODES

Een code heet een *blok code* als de gecodeerde boodschap verdeeld kan worden in rijtjes symbolen van vaste lengte die onafhankelijk van elkaar gedecodeerd kunnen worden. De lengte van de blokken noemen we *blok lengte* of *woordlengte*.

Voorbeeld blok code : repetitie code
" code met variabele blok lengte : unaire getalsrepresentatie.
" code zonder blokken : convolutie code.

Tengevolge van storingen zal niet iedere ontvangen boodschap gelijk zijn aan de verzonden boodschap. Dit verschil kan groot of klein zijn; om dit nauwkeuriger te maken hebben we een afstandsbegrip nodig.

Laten $s_1 s_2 \ldots s_n$ en $t_1 t_2 \ldots t_n$ twee symboolrijtjes zijn. Hun *Hamming-distance* is gelijk aan het aantal posities i waarvoor $s_i \neq t_i$. De Hamming-distance tussen de symboolrijtjes $\underline{s}$ en $\underline{t}$ noteren we met $d_H(\underline{s},\underline{t})$.

De Hamming-distance 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.

Andere afstandsbegrippen zijn: Lee-distance, Arithmetical distance.

OPGAVEN

1.1. 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?

1.2. 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 $\underline{x}\neq\underline{y} \Rightarrow d_H(\underline{x},\underline{y}) \geq 3$?

2. LINEAIRE CODES

Coderen aan de hand van een volledige tabel boodschappen met hun codering wordt bij grote codes ondoenlijk. We willen daarom codes met een zekere structuur.

Zij $R^{(n)}$ de n dimensionale vectorruimte over het eindige lichaam GF(q); dus $q = p^f$, p priem. 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.

Het *gewicht* van een codewoord v uit een lineaire code, is de Hamming-afstand tot de oorsprong. Dit is dus het aantal symbolen v_i dat ongelijk is aan nul. Het gewicht geven we aan met w(v).

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

Een matrix heeft *gereduceerde echelonvorm* als hij van de vorm $(I_k\ P)$ is, waarbij I_k de k×k eenheidsmatrix is, en P een k×(n-k) matrix is.

Twee codes heten *equivalent* als de ene code te verkrijgen is door ieder codewoord (het rijtje symbolen) van de andere code op een vaste wijze te permuteren.

STELLING. *Bij iedere lineaire code is er een equivalente code die een generator in gereduceerde echelonvorm heeft.*

Een *systematische* (n,k) *code* is een codewoord waarbij de eerste k symbolen willekeurig gekozen kunnen worden, waarna de overige n-k symbolen bepaald zijn. De vrij te kiezen symbolen heten *informatie symbolen*, de overige *parity-check symbolen*.

STELLING. *Iedere lineaire code is equivalent met een systematische code.*

We willen een maat hebben voor de fractie aan informatie die een code verschaft. Het light voor de hand te definiëren: de *information rate* van een (n,k) code is $\frac{k}{n}$.

VOORBEELD. Je wilt een boodschap overseinen bestaande uit viermaal 1 of 0, gevolgd door 3 parity check symbolen: een die de pariteit geeft van de eerste 2 informatie symbolen, een van de laatste 2, en een van alle 4 de

informatie symbolen.

Deze code is een (7,4) code over GF(2) met generator

$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. De codering van $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ is dan $G^T \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$.

Coderen is nu matrix vermenigvuldiging en niet: opzoeken in tabellen.

OPGAVEN

2.1. Uit hoeveel codewoorden bestaat de code uit bovenstaand voorbeeld?

2.2. 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.

2.3. 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. FOUTEN

Wanneer we een boodschap ontvangen en het is een codewoord, dan zullen we aannemen dat er bij het overseinen geen fouten zijn gemaakt. Wanneer het ontvangen woord geen codewoord is, kunnen we aannemen dat het aantal gemaakte fouten zo klein mogelijk is, en de boodschap dus het dichtstbijzijnde codewoord voorstelt. Deze methode wordt *maximum-likelihood decoding* genoemd.

Een lineaire code V heet e-*error correcting* als

$$\forall \underline{x} \in V \quad \forall \underline{y} \in V[\underline{x} \neq \underline{y} \Rightarrow d_H(\underline{x},\underline{y}) \geq 2e+1].$$

Een lineaire code V heet e-*error detecting* als

$$\forall \underline{x} \in V \quad \forall \underline{y} \in V[\underline{x} \neq \underline{y} \Rightarrow d_H(\underline{x},\underline{y}) \geq 2e].$$

Error detecting is nuttig als je om herhaling van de boodschap kunt vragen, anders is alleen het correctievermogen van belang.

Een *error pattern* van een vector $\underline{w}$ is een vector $\underline{e}$ met de eigenschap dat $\underline{w}-\underline{e}$ een codewoord is.

Om te bepalen of een code e-error correcting is moeten we het minimum bepalen van alle afstanden tussen verschillende codewoorden. Bij lineaire codes is het echter niet nodig alle tweetallen codewoorden te inspecteren.

STELLING. *Voor een lineaire code* V *is de minimum van alle afstanden tussen verschillende codewoorden gelijk aan het minimale gewicht van de codewoorden ongelijk* $\underline{0}$.

OPGAVEN

3.1. Een werkgever wil de aktiviteiten van zijn werknemers rubriceren. Een aktiviteit wordt gecodeerd door een viertal cijfers gevolgd door een controle letter. De controle letter wordt bepaald door

$$11d_1 + 7d_2 + 5d_3 + 3d_4 + 1 \pmod{26}$$

te berekenen, en de letter met dit rangnummer te kiezen; b.v. 0 0 1 2 heeft als controle letter de $1\times5 + 2\times3+1 = 12$-de letter: L.
Hoeveel error correcting is de code, hoeveel detecting? Waarom zou d_4 niet met 2 vermenigvuldigd worden?

3.2. Beschouw het voorbeeld uit 2.1. Hoeveel error correcting is de code en hoeveel detecting? Ontwerp een systematische code voor dezelfde boodschappen, met hetzelfde correctie- en detectie-vermogen, maar met een hogere information rate.

3.3. Ontwerp een code met dezelfde woordlengte en rate als die uit 2.1, maar met een beter error-correcting vermogen.

4. DECODEREN

Het *orthogonaal complement* van een k dimensionale lineaire deelruimte V van R is de (n-k) dimensionale deelruimte $V^\perp$ van R zó dat $\forall \underline{x} \in V$ $\forall \underline{y} \in V^\perp[\langle \underline{x},\underline{y}\rangle = 0]$ waar $\langle \underline{x},\underline{y}\rangle$ het gewone inprodukt is.

Bij iedere lineaire deelruimte V van de n dimensionale vektorruimte R bestaat zo'n orthogonaal complement. Zij $G = (I_k\ P)$ een generator in echelonvorm van V. Dan is een generator van $V^\perp$: $H = (-P^T I_{n-k})$. Als V een code is noemen we $V^\perp$ de *duale code* van V.

Waarschuwing: er hoeft niet te gelden $\forall a \in R\ \exists \underline{x} \in V\ \exists \underline{y} \in V^\perp : \underline{a} = \underline{x} + \underline{y}$.

Een generator H voor de duale code van V noemen we een *parity-check matrix* voor V. Het *syndroom* van vector $\underline{x}$ is $\underline{x}H^T$.

VOORBEELD. De parity check van het voorbeeld in §2 is

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

STELLING. *Zij* V *een code met parity check* H. *Dan geldt*

$$\underline{x} \in V \iff \underline{x}H^T = \underline{0}$$

We beschouwen het probleem van error correctie in een lineaire code V. Neem een bepaald error pattern en tel dit op bij alle codewoorden. Dan krijgen we een coset: een verzameling W heet een *coset* van V als er een $\underline{e} \in R$ is zo dat $W = \{\underline{v} + \underline{e} \mid \underline{v} \in V\}$.

STELLING. *Twee vectoren* $\underline{x}$ *en* $\underline{y}$ *behoren tot dezelfde coset van* V *als en slechts als ze hetzelfde syndroom hebben.*

BEWIJS.

1) Zij $\underline{x} = \underline{v}_1 + \underline{e}$ en $\underline{y} = \underline{v}_2 + \underline{e}$ waarbij $\underline{v}_1, \underline{v}_2 \in V$,
   dan $\underline{x}H^T = (\underline{v}_1 + \underline{e})\, H^T = \underline{v}_1 H^T + \underline{e}H^T = \underline{e}H^T = \underline{y}H^T$;

2) zij $\underline{x}H^T = \underline{y}H^T$, dan $(\underline{x}-\underline{y})\, H^T = 0$, dus $\underline{x}-\underline{y} \in V$, we schrijven
   daarom $\underline{x} = (\underline{x}-\underline{y}) + \underline{y}$ en $\underline{y} = \underline{0} + \underline{y}$.

STELLING. *Zij* W *een coset van* V *met* $W = \{\underline{v} + \underline{e} \mid \underline{v} \in V\}$ *en* $\underline{x} \in W$ *dan is de verzameling mogelijke error patterns van* $\underline{x}$ *gelijk aan* W.

BEWIJS.

1) Zij $\underline{x} = \underline{v} + \underline{e}'$, dan is $\underline{e}' = \underline{x} - \underline{v} = \underline{v}' + \underline{e} - \underline{v} \in W$;

2) Zij $\underline{y} \in W$, dan is $\underline{x} = (\underline{x}-\underline{y}) + \underline{y}$ waarbij $\underline{x}-\underline{y} \in V$.

Wanneer we een boodschap $\underline{x}$ willen decoderen op basis van maximum-likelihood decoding, dan zijn niet alle error patterns even waarschijnlijk. We moeten een error pattern zoeken onder de kandidaten (dus een element in de coset van $\underline{x}$) met minimaal gewicht. Zo'n element noemen we *coset leader*. Het decodeerproces is nu als volgt:

1) bereken het syndroom van ontvangen boodschap $\underline{x}$,
2) zoek een coset leader $\underline{e}$ van de coset met dit syndroom,
3) trek $\underline{e}$ van $\underline{x}$ af.

Dit proces is beter dan alle codewoorden opschrijven en afstanden berekenen; het zwakke punt is echter het zoeken van de coset leader.

OPGAVEN

4.1. Neem het voorbeeld uit §2.

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.

4.2. De parity check van een 0-1 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.

4.3. Wat is de relatie tussen de parity check matrices van de codes uit opgave 2.3?

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

5. HAMMING CODE

STELLING. *Een binaire lineaire code* V *met parity check matrix* H *kan alle error patterns met één fout corrigeren dan en slechts dan als alle kolommen van* H *verschillend en ongelijk* 0 *zijn.*

BEWIJS.

1) Stel: alle kolommen van H zijn verschillend en ongelijk 0. Wanneer er een fout is gemaakt in het i-de symbool dan is het syndroom gelijk aan de i-de kolom van H. Dus als er één fout symbool is wordt de fout gelocaliseerd en gecorrigeerd.

2a) Stel de i-de kolom van H is gelijk aan 0. Dit betekent dat een fout in het i-de symbool géén invloed heeft op het syndroom, en dus onopgemerkt blijft.

2b) Stel de i-de en de j-de kolom van H zijn identiek. Dan geeft een fout in het i-de symbool dezelfde verandering van het syndroom als een fout in het j-de symbool. Zo'n fout kan dus niet met zekerheid gecorrigeerd worden. □

Deze stelling geeft ons de mogelijkheid een code te ontwerpen die alle enkelvoudige fouten verbetert.

Voorbeeld: neem als kolommen de binaire getallen 1 t/m 7:

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

Wanneer het syndroom van een ontvangen boodschap de binaire representatie van k is, dan is er waarschijnlijk één fout gemaakt in het k-de symbool.

Een binaire lineaire code waarvan de kolommen van de parity check matrix de binaire representatie zijn van $1,2,\ldots,2^r-1$ wordt genoemd de *$(2^r-1, 2^r-1-r)$ Hamming code.*

Een e-error correcting code $V \subset R$ heet *perfect* als

$$\bigcup_{\underline{x}\in V} \{\underline{y} \mid d_H(\underline{y},\underline{x}) \leq e\} = R.$$

STELLING. *De binaire Hamming codes zijn perfect.*

Het idee achter Hamming codes is niet beperkt tot binaire codes. De parity check matrix van een *Hamming code over GF(q)* wordt als volgt verkregen. Neem als kolommen van de parity check alle kolommen ongelijk $\underline{0}$ met r elementen uit GF(q), met de restrictie dat het eerste symbool (van bovenaf) ongelijk 0 steeds een 1 is.

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

BEWIJS.

1) Een lineaire combinatie van 2 kolommen van de parity check matrix H kan niet $\underline{0}$ zijn. Dus $\underline{x}H^T = \underline{0}$ impliceert $\underline{x} = \underline{0}$ of $w(x) \geq 3$. Dus de bollen met straal 1 rond codewoorden zijn disjunct.
2) De woordlengte van een Hammingcode is gelijk aan het aantal kolommen dat aan bovenstaande eisen voldoet. Dit is

$$n = \frac{1}{q-1}(q^r-1).$$

Daar H dimensie r×n heeft, is de dimensie van de code n-r. In een bol met straal 1 rond een codewoord zitten

$$1 + (q-1)n = q^r \text{ punten.}$$

Nu is $q^r \cdot q^{n-r} = q^n$, dus de code is perfect. □

Een gevolg van het feit dat de Hammingcodes perfect zijn, is dat ze geen enkel error pattern met 2 fouten kunnen signaleren. In het binaire ge-

val is er een eenvoudige remedie. Voeg aan ieder woord een symbool toe zo dat de som van alle symbolen nul wordt. Deze code heet de *extended Hamming code*. Als H de parity check matrix van een Hamming code is, dan is die van de extended code

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

OPGAVEN

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

4.2. Is Uw oplossing van opg. 3.2 hetzelfde als de (7,4) Hamming code?

4.3. U speelt mee in de voetbaltoto en wilt zeker zijn van de 1^e of 2^e 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 de door U ingevulde rijtjes?

6. THRESHOLD DECODING

We zullen nu een decodeermethode bespreken die de naam *threshold decoding* draagt. Deze methode heeft het voordeel dat hij vaak meer fouten correct corrigeert dan het aantal waarvoor hij ontworpen werd, en er zijn gemakkelijk schakelingen voor te ontwerpen.

Als eerste (eenvoudige) voorbeeld beschouwen we de repetitie code met woordlengte 2n+1. Als parity-check vergelijkingen kunnen we kiezen

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ \quad \cdots \\ x_1 + x_{2n+1} = 0 \end{cases}$$

Wanneer het ontvangen woord $\underline{y} = \underline{x} + \underline{e}$, dan is $y_1 + y_i = e_1 + e_i$. Indien meer dan n van de uitdrukkingen $y_1 + y_i$ gelijk aan 1 zijn, kan dit verklaard worden door minder dan n fouten, waaronder $e_1 = 1$, of door meer dan n fouten en $e_1 = 0$. Het eerste is waarschijnlijker. Dus de meerderheid van

stemmen onder $y_1 + y_i$ beslist tussen $e_1 = 0$ of $e_1 = 1$. Als het aantal stemmen de drempel (threshold) n overschrijdt, dan nemen we aan dat e = 1.

Zij V een lineaire code met woordlengte n. Een stel parity check vergelijkingen voor V heet *orthogonaal op de posities* $P \subset \{1,2,...n\}$ indien geldt:

1) voor iedere $i \in P$ komt de term x_i in iedere vergelijking voor met coëfficient ongelijk aan 0;
2) voor iedere $i \notin P$ komt de term x_i voor met coëfficient ongelijk aan 0 in ten hoogste één van de vergelijkingen.

We zullen nu beschrijven hoe zo'n stelsel parity check vergelijkingen gebruikt kan worden. Beschouw de duale code C van de (7,4) Hamming code. Als H de parity check matrix is van deze code, dan geldt dat de som van een tweetal kolommen (ongelijk $\underline{0}$) weer een kolom van H is. Zo'n drietal kolommen bepaalt een parity check vergelijking met drie termen voor C. Bij deze vergelijkingen zijn er 3 waarin x_1 voorkomt:

$$\begin{cases} x_1 = x_2 + x_3 \\ x_1 = x_4 + x_5 \\ x_1 = x_6 + x_7 \end{cases}$$

Dit stelsel is orthogonaal voor positie 1. Voor het symbool x_1 hebben we dus de vergelijkingen:

$$\begin{cases} y_1 = x_1 + e_1 \\ y_2 + y_3 = x_1 + (e_2+e_3) \\ y_4 + y_5 = x_1 + (e_4+e_5) \\ y_6 + y_7 = x_1 + (e_6+e_7) \end{cases}$$

Als er één fout is ontstaan door het overseinen, dan levert de meerderheid onder de linkerleden de juiste waarde van x_1. Als de uitkomst 2 - 2 is, dan redeneren we als volgt. Kans $(e_1=0) = 1 - p$, en Kans $(e_i+e_j=0) =$ $= (1-p)^2 + p^2 < 1 - p$. Het is dus waarschijnlijkste dat $y_1 = x_1$. Nadat we het eerste symbool op deze wijze gedecodeerd hebben kunnen we een verzameling parity check vergelijkingen voor de 2^e positie gebruiken (waarbij het gecorrigeerde eerste symbool gebruikt wordt).

OPGAVEN

6.1. Decodeer 1 1 1 0 0 0 0 volgens bovenstaande methode.

7. WEIGHT ENUMERATOR

Wanneer we het corrigerend vermogen van een lineaire code willen beoordelen, is het van belang te weten wat het minimale gewicht van de code is. Ook andere gewichten zijn van belang wanneer we willen berekenen hoe groot de kans is dat een boodschap goed gedecodeerd wordt. Wanneer een error pattern van gewicht i een codewoord in een ander codewoord omzet, wordt deze fout niet gesignaleerd. Wanneer er nog een fout meer gemaakt wordt (gewicht error pattern i+1), en de code minstens 1 error correcting is, dan wordt 1 van de i+1 fouten gecorrigeerd. Wordt er echter 1 fout minder gemaakt (gewicht error pattern i-1), dan wordt er door het error correctie proces een extra fout geïntroduceerd. Het is dus nuttig de verdeling van de gewichten van een code te kennen. Als A_i het aantal codewoorden is van gewicht i in een code met woordlengte i, dan is de *weight enumerator* gedefinieerd door

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

VOORBEELD. Beschouw de generator matrix van het voorbeeld in paragraaf 2. Inspectie van deze generator leert ons dat er geen codewoorden zijn van gewicht 1, 2 van gewicht 2, 4 van gewicht 3, 5 van gewicht 4, en 4 van gewicht 5. De weight enumerator is dus $1 + 2z^2 + 4z^3 + 5z^4 + 4z^5$.

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 mogelijkheden 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 $i = 1,\ldots,n+2$

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

dus

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

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

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

In VAN LINT *Coding Theory* (pp.25-26) wordt voor deze code de verwachting berekend van het aantal fouten (na decodering). Het blijkt dat deze waarde in somme gevallen groter is dan vóór de foutencorrectie. We hebben dus codes nodig die veel beter zijn dan Hamming codes.

OPGAVEN

7.1. Wat is de weight enumerator van de (8,4) extended binaire Hamming code?

7.2. Wat is de weight enumerator van de extended binaire Hamming code (met woordlengte n).

8. MAC WILLIAMS IDENTITEIT

We willen 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 $\mathbb{C}^\times$ de groep van de complexe getallen met modulus gelijk aan 1 en met vermenigvuldiging als operatie. Een *karakter* χ is een homomorfisme $\chi: G \to \mathbb{C}^\times$. Dus

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

en

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

LEMMA. *Zij* 0 *de eenheid in* (G,+). *Dan is* $\chi(0) = 1$.

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

LEMMA. *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 $\sum_{g\in G} \chi(g) =$
$= \sum_{g\in G} 1 = |G|$. □

STELLING. *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*

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

LEMMA. *Definieer* $g(\underline{u}) = \sum_{\underline{v}\in R} \chi(<\underline{u},\underline{v}>) \, z^{w(\underline{v})}$ *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).

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

$$= \sum_{\underline{v}\notin V^{\perp}} z^{w(\underline{v})} \sum_{\underline{u}\in V} \chi(<\underline{u},\underline{v}>) + \sum_{\underline{v}\in V^{\perp}} z^{w(\underline{v})} \sum_{\underline{u}\in V} \chi(<\underline{u},\underline{v}>)$$

$$= 0 + \sum_{\underline{v}\in V^{\perp}} z^{w(\underline{v})} \, |V| = |V| \, B(z).$$

In de binnenste som van de linkerterm neemt $<\underline{u},\underline{v}>$ iedere waarde uit GF(q) evenvaak aan, en daar $\sum_{\alpha\in GF(q)} \chi(\alpha) = 0$ is de linkerterm 0. □

BEWIJS DER STELLING.

Zij g gedefinieerd als in het lemma, zij $\underline{u} = u_1 u_2 \ldots u_n$ en breid w uit tot GF(q) door

$$w(v) = \begin{cases} 0 & \text{als } v = 0 \\ 1 & \text{anders} \end{cases}$$

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

$$= \sum_{v_1 \ldots v_n \in R} z^{w(v_1)+\ldots+w(v_n)}\ \chi(u_1v_1+\ldots u_nv_n)$$

$$= \sum_{v_1 \ldots v_n} z^{w(v_1)}\ \chi(u_iv_i) \ldots z^{w(v_n)}\ \chi(u_nv_n)$$

$$= \prod_{i=0}^{n} \sum_{v\in GF(q)} z^{w(v)}\ \chi(u_iv)$$

als $u_i = 0$ dan is de sommatie gelijk aan $1 + (q-1)z$,

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

Dus

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

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

Nu is

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

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

Deze formule wordt genoemd de *Mac Williams identiteit*. □

Hoofdstuk III

GRENZEN AAN CODES

door

M.R. Best

Bij dit onderwerp zullen we ons niets aantrekken van de bruikbaarheid van een code. 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 klassen van "goede" codes diegenen 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 notaties in:

We werken over een *alfabet* $Q = \{0,1,\ldots,q-1\}$ met $q \geq 2$.
Ter afkorting voeren we in: $\theta = (q-1)/q$.
Een *woord* ter *lengte* n is een element van Q^n, dus een rijtje van n natuurlijke getallen*) kleiner dan q.
De *(Hamming-)afstand* $d_H(x,y)$ tussen twee woorden x en y is het aantal plaatsen waar zij verschillen.
De *oorsprong* is het woord $0 = (0,0,\ldots,0)$.
Het *gewicht* $W_H(x)$ van een woord x is het aantal elementen ongelijk nul in x: $W_H(x) = d_H(x,0)$.
Een *code* is een niet-lege deelverzameling van Q^n.
Een code heet *triviaal* als hij uit slechts één woord bestaat.
Een code heet *binair* als $q = 2$, *ternair* als $q = 3$, etc.
De *minimale afstand* van een niet-triviale code is de kleinste voorkomende afstand tussen twee verschillende codewoorden.
Het *minimale gewicht* van een niet-triviale code is het kleinste voorkomende

---

*) We rekenen nul tot de natuurlijke getallen: $0 \in \mathbb{N}$.

positieve gewicht van een codewoord.
Als $\mathcal{Q}$ een groepsstructuur bezit, dan heet een code een *groepcode* als hij een ondergroep is van de productgroep $\mathcal{Q}^n$.
Als $\mathcal{Q}$ een lichaamsstructuur bezit, dan heet een code een *lineaire code* als hij een deelruimte is van de vectorruimte $\mathcal{Q}^n$.

De (*information-*)*rate* R van een code wordt gedefinieerd als $n^{-1}\ {}^q\log M$, waarin n de woordlengte en M het aantal woorden van de code voorstelt. Kennelijk is $0 \leq R \leq 1$. Voor de practijk is deze rate een goede graadmeter voor een code: hij geeft ruwweg aan welke fractie van de bits informatie draagt.

En [n,d]-*code* is een triviale code met lengte n of een niet-triviale code met lengte n en minimale afstand minstens d. 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:

$$A(n,d) = \max\{M \mid \text{er is een } [n,d]\text{-code met } M \text{ woorden}\}.$$

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

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

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

We behandelen eerst de

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 minstens d tot de code bestaat, m.a.w. de bollen met straal d - 1 om de codewoorden overdekken $\mathcal{Q}^n$.

LEMMA 1. *Het volume (= cardinaliteit) van een bol* $B_r(x) = \{y \mid y \in Q^n \wedge d_H(x,y) \leq r\}$ *met straal* r *om een punt* $x \in Q^n$ *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:

STELLING 1 [*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:

STELLING 2 [*Gilbert bound voor lineaire codes*]. *Als* $n \in \mathbb{N}$, $d \in \mathbb{N}$, *en* $k \in \mathbb{N}$, *voldoen aan* $V(n,d-1) \leq q^{n-k}$, *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 $x \in Q^n$ met $d_H(x,C_{k-1}) \geq d$. Zij nu C_k het lineair omhulsel van $C_{k-1} \cup \{x\}$. Dan is C_k een lineaire [n,d]-code van dimensie k, want als $z \in C_k$, dan is $z = ax + y$ met $a \in Q$, $y \in C_{k-1}$, dus

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

en

$$W_H(z) = W_H(y) \geq d \qquad \text{als } a = 0.$$

□

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

Dan is

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

Dus

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

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 Nordstrom-Robinson-code), en van een lineaire [13,4]-code van dimensie 5, dus met 32 codewoorden (de verkorte eerste orde Reed-Muller-code met lengte 16).

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

$$H_q(x) = x\ {}^q\log\ (q-1) - x\ {}^q\log\ x - (1-x)\ {}^q\log\ (1-x).$$

H_q heet de *entropiefunctie*.

LEMMA 2. *Zij* $0 \leq \lambda \leq \theta$, $q \geq 2$. *Dan is*

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

BEWIJS: Volgens Stirling is

$$n^{-1}\ \log\left(\binom{n}{\lfloor \lambda n \rfloor}(q-1)^{\lfloor \lambda n \rfloor}\right) \sim n^{-1}\ \log\left(\frac{n^n (q-1)^{\lfloor \lambda n \rfloor}}{\lfloor \lambda n \rfloor^{\lfloor \lambda n \rfloor}(n-\lfloor \lambda n \rfloor)^{n-\lfloor \lambda n \rfloor}}\right) \sim$$

$$\sim n^{-1}\ \log\left(\frac{(q-1)^{\lambda n}}{\lambda^{\lambda n}(1-\lambda)^{(1-\lambda)n}}\right) =$$

$$= \lambda \log(q-1) - \lambda \log \lambda - (1-\lambda) \log (1-\lambda).$$

Ook is

$$\sum_{i\leq\lambda n} \binom{n}{i}(q-1)^i \leq x^{\lambda n} \sum_{i\leq\lambda n} \binom{n}{i}(q-1)^i x^{-i} \leq x^{\lambda n} \sum_{i=0}^{n} \binom{n}{i}\left(\frac{q-1}{x}\right)^i =$$

$$= x^{\lambda n}\left(1 + \frac{q-1}{x}\right)^n \qquad \text{voor iedere } x \geq 1.$$

Neem nu

$$x = (q-1)\ \frac{1-\lambda}{\lambda}.$$

Dan is $x \geq 1$ en dus

$$\sum_{i\leq\lambda n} \binom{n}{i}(q-1)^i \leq (q-1)^{\lambda n}\left(\frac{1-\lambda}{\lambda}\right)^{\lambda n}\left(\frac{1}{1-\lambda}\right)^n = (q-1)^{\lambda n}\ \lambda^{-\lambda n}(1-\lambda)^{-(1-\lambda)n}.$$

Hieruit volgt de gevraagde limiet. □

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

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

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

Dus:

STELLING 3 [*Asymptotische Gilbert bound*].

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

BOVENGRENZEN.

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

I. DE SINGLETON BOUND

In de coderingstheorie wordt veelvuldig een code geconstrueerd door een grotere code in te korten. Dit kan op twee manieren:

(i) Men schrapt van alle codewoorden het laatste bit. Hierdoor onstaat uit een $[n,d]$-code een $[n-1,d-1]$-code met evenveel woorden.

(ii) Men zoekt alle codewoorden uit met het laatste bit gelijk aan de meest voorkomende waarde, en laat dit bit vervolgens weg. Hierdoor ontstaat uit een $[n,d]$-code een $[n-1,d]$-code met minstens $1/q$ van het oorspronkelijk aantal woorden.

Als men één van beide procédés 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

STELLING 4 [*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:

STELLING 5 [*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

STELLING 6 [*Asymptotische Singleton bound*].

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

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 alle 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:

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

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

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

Hieruit volgt:

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

Als $d \leq \theta n$, 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 minstens $Mq^{-n+n'}$ woorden. Passen we nu de bovenstaande ongelijkheid toe, dan is

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

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

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

Dus

STELLING 7 [*Plotkin bound*]. *Als* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$ *en* $\theta = 1 - q^{-1}$, *dan is*

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

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

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

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

Asymptotisch levert de Plotkin bound:

STELLING 8 [*Asymptotische Plotkin bound*].

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

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

Voor *lineaire* codes vond Griesmer een grens, die asymptotisch gelijk is aan de Plotkin bound, maar in speciale gevallen scherper is. Schrijf de generatormatrix 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 minstens $\lceil d/q \rceil$ 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 getal 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 $[n - \sum_{i=1}^{k-1} \lceil d/q^i \rceil, d]$-code van dimensie 1. Dus $d \leq n - \sum_{i=1}^{k-1} \lceil d/q^i \rceil$, ofwel:

STELLING 9 [*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, er toch geldt niet. $18 \geq 9 + 5 + 3 + 2$. (Deze code kan men verkrijgen uit de Hadamard-matrix van orde 20 door twee kolommen (weer onder een constante) en vier rijen weg te laten.)

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

$$13 < 5 + 3 + 2 + 1 + 1 + 1 + 1,$$

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

III. DE HAMMING BOUND

Bij een $[n,d]$-code met M woorden zijn de bollen met straal $\lfloor (d-1)/2 \rfloor$ om de codewoorden disjunct, dus $M.V(n,\lfloor (d-1)/2 \rfloor) \leq q^n$.

STELLING 10 [*Hamming bound*]. *Als* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$, *dan is*

$$A(n,d) \leq q^n / V(n,\lfloor (d-1)/2 \rfloor).$$

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

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

Dus

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

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

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

dus

STELLING 11 [*Asymptotische Hamming bound*].

$$\alpha(\delta) \leq 1 - H_q(\delta/2).$$

IV. DE ELIAS BOUND

De Plotkin bound is gebaseerd op het feit dat de minimale afstand hoogstens 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.

LEMMA 3. *Zij* $A,C \subseteq Q^n$. *Dan is er een* $x \in Q^n$ *zodat*

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

BEWIJS:

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

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

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

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

We berekenen nu weer de som van alle afstanden van geordende paren verschillende codewoorden in $\mathcal{B}_r(0)$. We schrijven deze codewoorden als rijen van een K × 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

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

is

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

en

$$\sum_{i=1}^{n} m_{io}^2 \geq n^{-1}\left(\sum_{i=0}^{n} m_{io}\right)^2 = n^{-1}S^2.$$

Dus de totale som is:

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

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

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

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

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

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

dus

LEMMA 4. *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

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

Combinaties van de gevonden resultaten levert:

STELLING 12 [*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*

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

BEWIJS:

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

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

Met $r = 0$ volgt $A(n,d) \leq 8192$,

met $r = 1$ volgt $A(n,d) \leq 927$,

met $r = 2$ volgt $A(n,d) \leq 275$,

met $r = 3$ volgt $A(n,d) \leq 281$,

terwijl voor $4 < r \leq 6$ de noemer negatief wordt. Dus $A(13,5) \leq 275$. Door eerst verkorting toe te passen kunnen we komen tot $A(13,5) \leq 267$.

Asymptotisch levert de Elias bound:

STELLING 13 [*Asymptotische Elias bound*].

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

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

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

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

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

Dus

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

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

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

V. DE JOHNSON BOUND

Johnson verscherpt de Hamming bound door ook te kijken wat er zich buiten de bollen met straal $\lfloor (d-1)/2 \rfloor$ afspeelt. Stel we hebben een [n,d]-code C met M woorden. We definiëren C^i als de verzameling woorden met afstand i tot C. Dus $C^0 = C$ en $\sum_{i=0}^{\infty} |C^i| = q^n$.

Definëer M_r^x als het aantal woorden in C^r dat op afstand r ligt van het codewoord x, en M_0 als het aantal codewoorden dat minimale afstand heeft tot het woord Q. Dan is

$$\sum_{x \in C^0} M_r^x = \sum_{y \in C^r} M_0^y.$$

Definiëren we verder

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

en

$$M_0^r = \max_{y \in C^r} M_0^y,$$

dan is

$$|C^0| M_r^0 \leq \sum_{x \in C^0} M_r^x = \sum_{y \in C^r} M_0^y \leq |C^r| M_0^r,$$

dus

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

We vinden zo:

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

dus

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

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 $r \geq d/2$.

Als we M_0^r 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_{e+1}^0 en M_0^{e+1}, en schatten M_r^0 voor $r \geq e + 2$ met 0.

Eerst definiëren we: $N(n,r,d)$ is het maximaal aantal woorden in Q^n met gewicht r en onderlinge afstand $\geq d$. Hiervoor geldt:

LEMMA 5.

$$N(n,r,d) \leq \left[\frac{n}{r}\left[\frac{n-1}{r-1}\left[\ \cdots\ \left[\frac{n-r+e+1}{e+1}\right]\ \cdots\ \right]\right]\right].$$

BEWIJS: Stel er is een verzameling van K woorden in $\{0,1\}^n$ met gewicht r en onderlinge afstand $\geq d$. Schrijf deze kolommen als rijen van een $K \times n$ - matrix. In iedere kolom staan hoogstens $N(n-1,r-1,d)$ enen. Het totaal aantal enen is

$$Kr \leq nN(n-1,r-1,d),$$

dus

$$N(n,r,d) \leq \left[\frac{n}{r} N(n-1,r-1,d)\right]$$

Door $N(n,e+1,d) = \left[\frac{n}{e+1}\right]$, is

$$N(n,r,d) \leq \left[\frac{n}{r}\left[\frac{n-1}{r-1}\left[\cdots\left[\frac{n-r+e+2}{e+2} N(n-r+e+1,e+1,d)\right]\ \cdots\right]\right]\right] \leq$$

$$\leq \left[\frac{n}{r}\left[\frac{n-1}{r-1}\left[\cdots\left[\frac{n-r+e+2}{e+2}\left[\frac{n-r+e+1}{e+1}\right]\right]\ \cdots\right]\right]\right]. \qquad \square$$

LEMMA 6.

$$M_{e+1}^0 \geq \binom{n}{e+1} - \binom{d}{e} N(n,d,d).$$

BEWIJS: Zij $x \in C$. We mogen aannemen dat $x = 0$. Het aantal codewoorden van gewicht d is hoogstens $N(n,d,d)$. Het aantal woorden van gewicht $e + 1$ en afstand e tot de code is hoogstens $\binom{d}{e} N(n,d,d)$.

Het aantal woorden van gewicht e + 1 en afstand e + 1 tot de code is dus

$$M_{e+1}^{x} \geq \binom{n}{e+1} - \binom{d}{e} N(n,d,d). \qquad \square$$

LEMMA 7.

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

BEWIJS: Zij $y \in C^{e+1}$. We mogen aannemen dat $y = 0$. Dan is het aantal codewoorden met gewicht e + 1 gelijk aan

$$M_0^{y} \leq N(n,e+1,d) = \left\lfloor \frac{n}{e+1} \right\rfloor .$$

We hebben zo gevonden:

STELLING 14 [*Johnson bound*]. *Zij* $q = 2$, $n,e \in \mathbb{N}$, $d = 2e + 1$. *Dan is*

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

waarin

$$N(n,d,d) \leq \left[\frac{n}{d}\left[\frac{n-1}{d-1}\left[\ldots\left[\frac{n-e}{d-e}\right]\ldots\right]\right]\right].$$

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

Dan is

$$N(13,5,5) \leq \left[\frac{13}{5}\left[\frac{12}{4}\left[\frac{11}{3}\right]\right]\right] = 23,$$

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

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 McWilliams identiteit voor duale (lineaire) codes.

Voor vaste q en n definiëren we eerst:

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

Voor vaste q, n en r is P_r^i een polynoom in i, het z.g. Krawtchouk-polynoom.

De getallen P_r^i voldoen aan een eenvoudige recurrente betrekking.

$$P_r^i = P_r^{i-1} - (q-1)P_{r-1}^i - P_{r-1}^{i-1},$$

met $P_0^i = 1$, $P_r^0 = \binom{n}{r}(q-1)^r$.

Er geldt nu:

LEMMA 8. *Zij* ω *een primitieve* q^{de} *eenheidswortel, en* $x \in Q^n$ *een vast woord van gewicht* i. *Dan is*

$$\sum_{\substack{y \in Q^n \\ W_H(y)=r}} \omega^{\langle x,y \rangle} = P_r^i .$$

BEWIJS: We mogen aannemen dat

$$x = (x_1, \ldots\ldots\ldots\ldots x_i, 0, \ldots\ldots\ldots\ldots, 0)$$

met $1 \leq x_h < q$ voor $0 < h \leq i$.

Een willekeurig woord y van gewicht r ziet er uit als

$$y = (y_1, \ldots, y_j, 0, \ldots, 0, y_{j+1}, \ldots, y_r, 0, \ldots, 0)$$

met $1 \leq y_h < q$ voor $0 < h \leq r$.

Nu is

$$\sum_{\substack{y \in Q^n \\ W_H(y)=r}} \omega^{\langle x,y \rangle} = \sum_j \binom{i}{j}\binom{n-i}{r-j} \sum_{y_1,\ldots,y_r=1}^{q-1} \omega^{x_1y_1+\ldots+x_jy_j} =$$

$$= \sum_j \binom{i}{j}\binom{n-i}{r-j} \prod_{h=1}^{j} \sum_{y_h=1}^{q-1} \omega^{n_hy_h} \prod_{h=j+1}^{r} \sum_{y_h=1}^{q-1} 1 =$$

$$= \sum_j \binom{i}{j}\binom{n-i}{r-j}(-1)^j(q-1)^{r-j} . \qquad \square$$

LEMMA 9. *Zij* $C \subseteq Q^n$ *een code met* M *woorden en gemiddeld* A_i *woorden op afstand* i *van een vast codewoord, dus*

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

Dan is

$$\sum_{i=0}^{n} A_i P_r^i \geq 0 \qquad \text{voor iedere } r \in \{0,1,\ldots,n\}.$$

BEWIJS:

$$\sum_{i=0}^{n} A_i P_r^i = \sum_{i=0}^{n} \sum_{\substack{x,y\in C \\ d_H(x,y)=i}} \sum_{\substack{z\in Q^n \\ W_H(z)=r}} \omega^{<x-y,z>} =$$

$$= \sum_{\substack{z\in Q^n \\ W_H(z)=r}} \left(\sum_{x\in C} \omega^{<x,z>} \right)^2 \geq 0. \qquad \square$$

STELLING 15. *Zij* $q,n,d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$. *Dan is*

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

$$\left. A_i \in \mathbb{N},\ \sum_{i=0}^{n} A_i P_r^i \geq 0 \quad \textit{voor } r \in \{1,\ldots,n\} \right\}.$$

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

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.

LITERATUUR

BERLEKAMP, E.R., *Algebraic Coding Theory*, McGraw Hill, New York (1968).

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.

GILBERT, E.N., *A comparison of signalling alphabets*, Bell Syst. Tech. J. 31 (1952), 504-522.

GRIESMER, J.H., *A bound for error correcting codes*, IBM J. Res. & Dev. 4 (1960), 532-542.

HAMMING, R.W., *Error detecting and error correcting codes*, Bell Syst. Tech. J. 29 (1950), 147-160.

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.

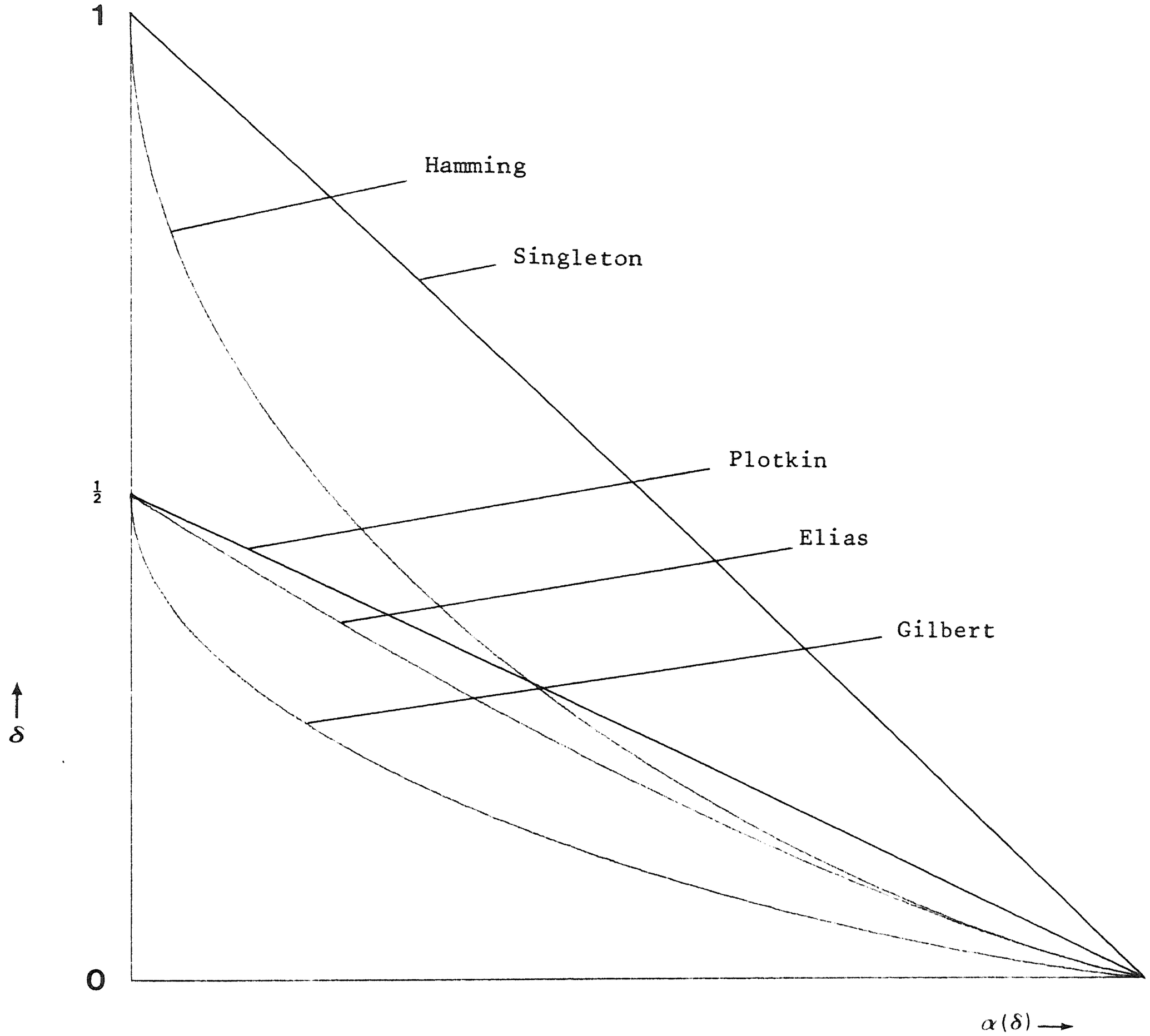
JOHNSON, S.M., *Improved asymptotic bounds for error correcting codes*, IEEE Trans. Inform. Theory 9 (1963), 193-205.

JOHNSON, S.M., *On upper bounds for unrestricted binary error-correcting codes*, IEEE Trans. Inform. Theory 17 (1971), 466-478.

NORDSTROM, A.W. & J.P. ROBINSON, *An optimal nonlinear code*, Inform. Contr. 11 (1967), 613-616.

PLOTKIN, M., *Binary codes with specified minimum distance*, IEEE Trans. Inform. Theory 6 (1960), 445-450.

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.



De verschillende grenzen in het geval q = 2

Hoofdstuk IV

REED-MULLER CODES EN DE STELLING VAN CHEVALLEY

door

P. van Emde Boas

Het doel van dit hoofdstuk is om met een minimum aan voorkennis en/of rekenwerk te komen tot: eerstens het bewijs dat een tweetal sterk verschillende beschrijvingen van een stelsel lineaire codes in feite equivalente code's beschrijven (hetgeen de aldus gedefinieerd gegeneraliseerde Reed-Muller codes tot een wiskundig interessant object maakt) en tweedens het bepalen van het minimale gewicht van deze codes, hetgeen op zijn beurt leidt tot een nieuw bewijs voor de bekende stelling van Chevalley en generalisaties van deze stelling.

4.1. FUNCTIES EN POLYNOMEN OVER EINDIGE LICHAMEN

Het "welbekende feit" dat een polynoom f in k[X] dat alle elementen van een oneindig lichaam k tot nulpunt heeft ook alle coëfficienten gelijk nul heeft, is onjuist indien k een eindig lichaam is; 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 kennelijk tegenvoorbeeld is. Met de generalisatie voor polynomen in meerderlijke veranderlijken is het al even slecht gesteld. Hoe slecht hoop ik in deze paragraaf te verduidelijken.

Zij V een m-dimensionale vectorruimte over $k = \mathbb{F}_q$ i.e. $V \cong (k)^m$. 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 van deze afbeelding J is een ideaal in $k[X_1,\ldots,X_m]$. Kennelijk geldt $f \in J$ d.e.s.d. 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 schrij-

ven als een polynoom f^* dat de eigenschap heeft dat voor iedere en ieder in f^* optredent 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 verz. gereduceerde polynomen duiden we aan met R.

STELLING. $J \cap R = \{0\}$ *en* $I = J$. *Verder geldt* $R/J = k[X_1,\ldots,X_m]/J$.

BEWIJS: 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:

$$f = f_0 + f_1 X_m + f_2 X_m^2 + \ldots + f_{q-1} X_m^{q-1},$$

waarbij de $f_i \in k[X_1,\ldots,X_{m-1}]$ en gereduceerd.

Voor vaste elementen $\alpha_1,\ldots,\alpha_{m-1} \in k$ geldt dat $f(\alpha_1,\ldots,\alpha_{m-1},X_m) \in k[X_m]$ een 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.

De bewering $I \subset J$ duidelijk zijnde beschouwen we 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 rechtstrecks. □

GEVOLG: *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)*.

BEWIJS 1: (dimensies tellen). $k[X_1,\ldots,X_m]/J \cong R$. Het aantal verschillende gereduceerde monomen bedraagt q^m en dit is tevens de dimensie van k^V. Omdat E als kern J heeft moet E dus wel surjectief zijn.

BEWIJS 2: (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

$$f_{a_i}(a) = \underline{\text{if}}\ a = a_i\ \underline{\text{then}}\ 1\ \underline{\text{else}}\ 0\ \underline{\text{fi}}$$

(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

$$f_{\underline{a}} = \prod_{j=1}^{m} \Big(- \prod_{\substack{b\in k \\ b\neq a_j}} (x_j - b)\Big).$$

Kennelijk geldt

$$f_{\underline{a}}(\underline{b}) = \underline{\text{if}}\ \underline{a} = \underline{b}\ \underline{\text{then}}\ 1\ \underline{\text{else}}\ 0\ \underline{\text{fi}}.$$

Het is bovendien duidelijk dat $f\underline{a} \in R$. Schrijven we nu voor willekeurig $f \in k^V$ het polynoom

$$g = \sum_{\underline{a}\in V} f(\underline{a}).f_{\underline{a}} \in R$$

dan volgt direct dat $E(g) = f$ weshalve E surjectief is. □

CONCLUSIES: We hoeven alleen maar naar gereduceerde polynomen te kijken en alle functies in k^V worden door een gereduceerd polynoom gerepresenteerd.

4.2. 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.

STELLING [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.* $\exists \underline{a} \in V$, $\underline{a} \neq 0$ *en* $f_1(\underline{a}) = \ldots = f_s(\underline{a}) = 0$).

Er geldt in feite nog meer: het aantal niet triviale gemeenschappelijke nulpunten is deelbaar door p (de karacteristiek van k). Deze laatste verscherping volgt rechtstreeks uit het bewijs.

BEWIJS: 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. In dien we G reduceren (mod I) tot G^* geldt $\deg(G^*) \leq \deg(G) = (q-1).d$. Kennelijk geldt $\deg(G^*-H) = \deg(0) = 0$ ergo $\deg(G^*) = \deg(H)$. Bezien we de hoogste graadsterm van $f_{\underline{a}}$, zijnde $(-1)^m X_1^{q-1} \ldots X_m^{q-1}$ van graad $m(q-1)$ en onafhankelijk van $\underline{a}$. Wil in H geen term van deze graad voorkomen dan moet het aantal polynomen fa dat wordt opgeteld om H te vormen een veelvoud van p zijn, i.e. $\#W \equiv 0 \pmod p$. □

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 Reed-Muller codes.

Een generalisatie die zich uitspreekt over de deelbaarheids eigenschappen van het aantal nulpunten is de volgende

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 verhaal geen bewijs geven.

4.3. DE REED-MULLER CODES

Zij $V \cong (k^m)$, $k = \mathbb{F}_q$. 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 $S: k^V \to (k)^{q^m}$.

DEFINITIE. De (gegeneraliseerde) Reed-Muller code RM(m,v,q) is het beeld onder de afbeelding S∘E van de verz. van polynomen
$\{f \notin k[X_1,\ldots,X_m] \mid \deg(f) \leq v\}$ waarbij $k = \mathbb{F}_q$.

Om deze definitie goed te praten moeten we laten zien dat de code niet afhangt van de (implicite) 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 hoofdstuk 2. 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:

LEMMA. *Zij* $\sigma: V \to V$ *een automorfisme en zij* $\underline{a} \in k^m$ *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:

$$f(X_1,\ldots,X_m) \to f(\Sigma\sigma_{i_1} X_i + a_1,\ldots,\Sigma\sigma_{i_m} X_i + a_m)$$

en onder deze transformatie stijgt de graad niet. De graad kan ook niet dalen want τ^{**} is een isomorfisme. □

GEVOLG: *De groep van affiene transformaties van* V *die we hierboven hebben ingevoerd, werkende op de posities van de code* RM(n,v,q) *(op gevat als punten in* V*) voert deze code in zich zelve over.*

DEFINITIE. Een lineaire code heet uitgebreid cyclisch (extended cyclic) 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.

De coëfficient van de gefixeerde plaats staat bekend als pariteits symbool. De code die ontstaat door dit symbool weg te laten heet cyclisch, en de uitgebreide cyclische code is kennelijk een uitbreiding van de bijbehorende cyclische code in de zin van Hoofdstuk 2.

FEIT. Zij $v < m(q-1)$, dan is de code RM(m,v,q) uitgebruide 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 verwisselt. Dit laat zien dat er een affiene transformatie van V bestaat met de gewenste vorm van de banen.

Om de tweede voorwaarde in de definitie te controleren moeten we de som van alle coordinaten van S(E(f)) op tellen. Dit is juist het getal:

$$\sum_{\underline{a}\in(k)^m} f(\underline{a}) = \sum_{g \text{ monoom in } f} \sum_{\underline{a}\in(k)^m} g(\underline{a}) =$$

stel $g = X_1^{d_{1g}},\ldots,X_m^{d_{mg}}$

$$= \sum_{g} \prod_{i\le m} \sum_{a\in k} a^{d_{ig}} \qquad \text{waarbij} \qquad \sum_{i\le m} d_{ig} \le v \quad \text{voor ieder monoom } g.$$

Omdat $\sum_{i\le m} d_{ig} < m(q-1)$ is er minstens één i waarvoor $d_{ig} < q-1$. Nu geldt voor een eindig lichaam:

$$\sum_{x\in \mathbb{F}_q} x^j = \underline{\text{if}}\ j > 0\ \underline{\text{and}}\ j \equiv 0 \bmod(q-1)\ \underline{\text{then}}\ -1\ \underline{\text{else}}\ 0\ \underline{\text{fi}}$$

hetgeen laat zien dat $\sum_{\underline{a}\in(k)^m} f(\underline{a}) = 0$. □

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 hoogstens 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 < kunnen we schrijven

$$v = r.(q-1) + s \qquad 0 \le s \le q-1.$$

Vormen we het polynoom

$$f = (1-x_1^{q-1})\ldots(1-x_r^{q-1}) \prod_{0<i\le s} (x_{r+1}-\alpha^i)$$

(waarbij α een primitief element van $\mathbb{F}_q$ is) dan zien we dat dit polynoom graad v heeft. Een niet-nulpunt van f heeft de vorm

$$\underline{a} = (a_1,\ldots,a_m) \qquad \text{waarbij} \qquad a_1 = a_2 = \ldots = a_r = 0$$

$$\text{en} \qquad a_{r+1} \neq \alpha^i \qquad \text{voor } 0 < i \le \delta.$$

Het aantal niet-nulpunten van f is derhalve

$$q^{m-r-1} \cdot (q-s).$$

En dit getal is een kennelijke bovengrens voor het minimale gewicht in RM(m,v,q). De oplettende lezer merke op dat uit het voorafgaande volgt dat deze grens exact is voor v = 0,1 en v = m(q-1).

CLAIM [Reed-Muller grens]. *Onder gebruikmaking van bovengenoemde notaties is het minimale gewicht van RM(m,v,q) gelijk* $q^{m-r-1}.(q-s)$.

Beschouwen we het geval q = 2. Omdat q - 1 = 1 zijn de gereduceerde monomen lineair in iedere er in optredende variabele. De Reed-Muller grens voor R(m,v,2) levert 2^{m-v}. Bij een polynoom f beschouwen we het polynoom q = 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 de zelfde graad.

Volgens de stelling van Warning is het aantal nulpunten van g minstens 2^{n-v}. Kennelijk is de stelling van Warning voor q = 2 equivalent met de Reed-Muller grens.

Algemeen geldt:

PROPOSITIE. *De Reed-Muller grens impliceert de stelling van Warning.*

BEWIJS: Zij g een polynoom van graad d < m. Beschouw het polynoom f^* dat ontstaat door $f = (g^{q-1}-1)$ te reduceren mod I. De graad van f^* is ≤ de graad van f zijnde d(q-1). Verder geldt $g(\underline{x}) = 0 \iff f(\underline{x}) \neq 0$. Als g minstens één nulpunt heeft is E(f) niet identiek gelijk nul, dus w := S(E(f)) is niet het 0-woord. Omdat $w \in RM(m,d(q-1),q)$ bedraagt het gewicht van w volgens de Reed-Muller grens minstens $q^{(m-d)}$. □

4.4. 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 ≤ v ≤ q - 1 bedraagt ≥ q - v hetgeen precies is wat de Reed-Muller grens verlangt.

Het algemene geval berust op de volgende truuk. 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 nouwkeurig 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:

$$\begin{array}{ccc} V & \xrightarrow{f} & \mathbb{F}_q \\ \| s & \nearrow & \cap \\ \mathbb{F}_{q^m} & \xrightarrow[f^*]{} & \mathbb{F}_{q^m} \end{array} \qquad f \in \mathbb{F}_q[X_1,\ldots,X_m] \qquad f^* \in \mathbb{F}_{q^m}[X]$$

of het diagram

$$\begin{array}{ccc} E^{-1}(S^{-1}(RM)(m,v,q))) & \xrightarrow{*} & A = \{f^* \mid f \in B\} \\ \| & & \\ B := \{f \in \mathbb{F}_q[X_1,\ldots,X_m] \mid \deg f \le v\} & & \cap \\ \cap & & \\ \mathbb{F}_q[X_1,\ldots,X_m] & \xrightarrow{*} & \mathbb{F}_{q^m}[X]. \end{array}$$

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 hoogstens 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 de 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.

STAP 1: *Bepaling van de $\mathbb{F}_q$-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 $q^{(m^2)}$. Indien wij evenveel van dit soort functies kunnen opschrijven hebben we de gehele verzameling bepaald.

Welnu, kies $\underline{\beta} = (\beta_0,\ldots,\beta_{m_1}) \in (\mathbb{F}_{q^m})^m$ en beschouw de functie f_β gedefinieerd door $\alpha \to \sum_{i=0}^{m-1} \beta_i.\alpha^{q^i}$ (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 $\mathbb{F}_{\underline{\beta}}$ gereduceerd zijn (als polynomen in $\mathbb{F}_{q^m}[X]$) dat $f_{\underline{\beta}} = f_{\underline{\beta}'}$ d.e.s.d. als $\underline{\beta} = \underline{\beta}'$. Het tellen van dimensies leert dat hiermede alle $\mathbb{F}_q$-lineaire functies gevonden zijn. □

OPMERKING: 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 $0 \leq i \leq m-2$ en $\beta_{m-1}^q = \beta_0$.

LEMMA. *Zij* $c_q(n)$ *de som van de cijfers van* n *bij ontwikkeling van* n *in het* q*-tallig stelsel.*

(i) $c_q(n) + c_q(m) \geq c_q(n+m)$ $\qquad n,m \geq 0$

(ii) $c_q(n) + c_q(m) \equiv c_q(n+m) \pmod{q-1}$ $\qquad n,m \geq 0$

(iii) *indien* $n \equiv m \bmod (q^t-1)$ *en* $0 \leq n < q^t - 1 \leq m$ *dan geldt*

$c_q(n) \leq c_q(m)$ *en* $c_q(n) \equiv c_q(m) \bmod (q-1)$.

BEWIJS: (i) en (ii) zijn vanzelfsprekent. (iii) volgt daar reductie van m mod $q^t - 1$ neerkomt op het optellen van blokken van t opeenvolgende cijfers van m, waarna het resultaat op dezelfde wijze behandeld wordt tot een getal ontstaat dat hoogstens t cijfers heeft. Het verwerken van een "overdracht" doet de cijfersom met $q - 1$ dalen. □

STAP 2: *Bepaling van* A.

De $\mathbb{F}_q$-lineaire polynomen in $\mathbb{F}_{q^m}[X]$ hebben de eigenschap dat ieder er in 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 $\leq v$. Omgekeerd kan ieder zodanig monoom op deze wijze gevormd worden.

GEVOLG:

$$A = \{f \mid f = \sum_{\substack{i<q^m \\ c_q(i)\leq v}} \beta_i X^i \quad \textit{en} \quad f^q \equiv f \pmod{X^{q^m}-X}\}.$$

STAP 3: *Bepaling der maximale graad van een element in* A.

Na 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 dat deze exponent zich laat schrijven als

$$\overbrace{\underline{q-1} \quad \underline{q-1} \quad \ldots \quad \underline{q-1}}^{r} \quad s \quad \overbrace{0 \quad 0 \quad \ldots \quad 0}^{m-1-r} \qquad (q\text{-tallig})$$

en dus als waarde heeft $q^n - (q-s).q^{m-r-1}$.

GEVOLG 1 [*Reed-Muller grens*]. (Notaties als boven.)

Zij deg $f \leq v$ dan geldt deg$(f^*) \leq q^n - (q-s).q^{m-r-1}$. Dientengevolge heeft f^* hoogstens $q^n - (q-s).q^{m-r-1}$ nulpunten en minstens $(q-s).q^{m-r-1}$ niet nulpunten hetgeen de gezochte grens voor het minimale gewicht van

S(E(f)) in RM(m,v,q) oplevert, gegeven de aanwezigheid van woor met precies dit gewicht. □

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 enerzijds 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 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. Men kan anderzijds gebruik maken van het (niet hier bewezen) feit dat

$$A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = A^*.$$

Overigens kan men eveneens rechtstreeks door de exponenten in een monoom $X_1^{e_1},\ldots,X_m^{e_m}$ te lezen als een q-tallig getal tot hetzelfde resultaat komen.

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 is door DELSARTE, GOETHALS & MacWILLIAMS.

4.5. 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 karacteristieke 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 $f \in A$ i.e. de in f optredende exponenten hebben cijfersom $\leq v$.
Dit impliceert

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^{q^m-1-j} = 0 \qquad \text{als } c_q(j) > v,\ 0 < j \leq q^{n-1}.$$

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 geldt voor $0 \leq j \leq q^{m-1}$

$$c_q(j) > v \iff c_q(q^m-1-j) < m(q-1) - v.$$

Derhalve geldt:

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^j = 0 \qquad \text{voor } 0 \leq j < q^m - 1 \text{ en } c_q(j) < m(q-1) - v$$

hetgeen als bijzonder geval oplevert:

$$\sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) = 0,$$

iets dat we reeds eerder hebben opgemerkt, toen we bewezen dat RM(m,v,q) een uitgebreide cyclische code is.

Vooruitlopende op het hoofdstuk over cyclische codes vermelden we de volgende beschrijving van een uitgebreide cyclische code $C \subset k^{n+1}$.

Schrijf

$$C \subset k^{n+1} \cong k[X]/(X^n-1) \oplus k$$

waarbij de eerste coëfficienten van de monomen $X^0,\ldots,X^{n-1}$ afkomstig zijn van de plaatsen in C die in deze volgorde door een cykel gepermuteerd worden die de code invariant laat, en waarbij de laatste coëfficient het pariteits symbool is.

Onder deze interpretatie geldt

$$C = \{(f,\gamma) \mid f = \sum_{j=1}^{h-1} f_j X^j \in L \subset k[X]/(X^n-1) \text{ en } \gamma = -\sum_{j=0}^{n-1} f_j\}.$$

Het blijkt dat de verzameling optredende (restklassen van) polynomen L (i.e. het beeld van de bijbehorende cyclische code) een ideaal is in de ring $k[X]/(X^n-1)$. Indien we aannemen dat n en de karacteristiek van k relatief priem zijn dan laat zo een ideaal zich bepalen als de verzameling polynomen die een aantal elementen in een uitbreidingslichaam K van k tot gemeenschappelijke nulpunten hebben:

$$\exists_{\beta_1,\ldots,\beta_t \in K} \quad \text{zodat}$$

$$f \in L \text{ d.e.s.d. als } f(\beta_1) = f(\beta_2) = \ldots = f(\beta_t) = 0.$$

In het concrete geval van de code RM(n,v,q) ziet deze beschrijving er als volgt uit.

De plaatsen in RM(m,v,q) waren reeds geidentificeerd met de elementen van $\mathbb{F}_{q^n}$. Neem een primitief element γ van $\mathbb{F}_{q^n}$, en schrijf vervolgens voor $f \in \mathbb{F}_q^{\mathbb{F}_{q^m}}$

$$f = \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha) \cdot f_\alpha = \sum_{\alpha\in\mathbb{F}_{q^m}^*} f(\alpha) \cdot f_\alpha + f(0) \cdot f_0 =$$

$$= \sum_{j=0}^{q^{m-2}} f(\gamma^j) f_{\gamma j} + f(0) \cdot f_0.$$

We identificeren nu $f_{\gamma j}$ met X^j en vatten de waarden $f(\gamma^j)$ als coëfficienten op. De coëfficient van f_0 vatten we op als pariteits symbool. Derhalve:

$$RM(m,v,q) \cong \left\{\left(\sum_{j=0}^{q^{m-2}} f(\gamma^j) \cdot X^j,\ f(0)\right) \mid f \in A\right\}.$$

Zij L de verzameling optredende oplynomen $\sum_{j=0}^{q^{m-2}} f(\gamma^j)X^j$. Volgens de geciteerde theorie is L een ideaal in $\mathbb{F}_q[X]/(X^{q^{m-1}-1})$ en omdat aan de voor-

waarde dat q en $q^n - 1$ relatief priem zijn is voldaan mogen we dus vragen naar de gezamelijke nulpunten van L. Een aantal van deze nulpunten zijn 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:

$$0 = \sum_{\alpha \in \mathbb{F}_{q^m}} f(\alpha) \cdot \alpha^j = \sum_{\alpha \in \mathbb{F}_{q^m}^*} f(\alpha) \cdot \alpha^j = \sum_{i=0}^{q^m-2} f(\gamma^i)\gamma^{ij} =$$

$$= \sum_{i=0}^{q^m-2} f(\gamma^i)(\gamma^j)^i.$$

Hetgeen wil zeggen dat de punten γ^j met $0 < j < q^m - 1$ en $c_q(j) < m(q-1) - v$ gemeenschappelijke nulpunten zijn 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 $\mathbb{F}_q[X]/(X^{q^m-1}-1)$ 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 hoofd ideaal ring is wordt L^* voortgebracht als ideaal door het minimale polynoom dat alle punten γ^j met $c_q(j) < m(q-1) - v$ tot nulpunt heeft, i.e. 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 kennelijk 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). Deze hebben we in de voorafgaande paragraaf uitgerekend waarbij de uitkomst was

$$f = \#\{j \mid 0 \le j \le q^m - 1 \quad \text{en} \quad c_q(j) \le v\}$$

en aangezien we hebben aangenomen dat $v < (q-1)m$ geldt

$$f = \#\{j \mid 0 \le j < q^m - 1 \quad \text{en} \quad c_q(j) \le v\}.$$

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

$$d + f = \#\{j \mid (0<j<q^m-1 \text{ en } c_q(j)\leq v) \quad \underline{\text{of}} \quad (0<j\leq q^m-1 \text{ en } c_q(j)>v)\} =$$

$$= q^m - 1.$$

Hieruit volgt $f = q^m - 1 - d$, i.e. $L = L^*$, vaarmede het bewijs voltooid is.

CONCLUSIE. Voor $v < m(q-1)$ is de code $RM(m,v,q)$ een uitgebreide 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 primitieve 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.

OPMERKING: Het feit dat de polynomen in L de punten γ^j vor $1 \leq j \leq q^m - 1$ en $c_q(j) < n(q-1) - v$ levert ons met behulp van de zogeheten BCH grens een nieuw bewijs voor de Reed-Muller grens. De BCH grens spreekt uit dat een cyclische code waarvan de getallen $\gamma,\gamma^2,\ldots,\gamma^d$ gezamelijke nulpunten zijn minimaal gewicht $\geq d + 1$ heeft; deze grens volgt direct uit de non-singulariteit der Vandermonde determinant. Bovendien volgt dat het minimale gewicht van de uitgebreide code $\geq d + 2$ is. 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 $v = r(q-1) + s$, $0 \leq s \leq q - 1$. 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:

$$0, \quad 0, \quad \ldots \quad 0, \quad \underline{q-1-s}, \quad \underbrace{\underline{q-1}, \quad \ldots, \quad \underline{q-1}}_{m-r-1} = (q-s).q^{m-r-1} - 1.$$

We mogen derhalve $d = (q-s)q^{m-r-1} - 2$ stellen zodat $d + 2 = (q-s)q^{m-r-1}$, hetgeen te bewijzen viel.

4.6. DUALITEIT VAN REED-MULLER CODES

STELLING. *De code* $C = RM(qn,v,q)$ *is de duale van de code* $C' = RM(m,m(q-1)-v-1,q)$.

BEWIJS: 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 x,x' uit C resp. C' inproduct nul hebben.

Stel

$$x = S(E(f)) \qquad \text{met} \qquad \deg(f) \le v \qquad \text{en}$$

$$x' = S(E(f')) \qquad \text{met} \qquad \deg(f') \le m(q-1) - v - 1$$

dan volgt

$$\langle x,x' \rangle = \sum_{a \in (\mathbb{F}_q)^m} f(a) \cdot f'(a) = \sum_{a \in (\mathbb{F}_q)^m} (f.f')(a)$$

nu is S(E(f.f')) een element van RM(m,m(q-1)-1,q) dus de som der coëfficiënten van S(E(f.f')) is gelijk nul. Hieruit volgt $\langle x,x' \rangle = 0$. □

4.7. GEOMETRISCHE INTERPRETATIE VOOR q = 2

Beschouw de code RM(m,v,2). Aangezien $\mathbb{F}_2$ slechts twee elementen bevat kunnen we de functies $f: (\mathbb{F}_2)^m \to \mathbb{F}_2$ opvatten als karakteristieke functies. De gereduceerde monomen hebben de vorm $X_{j_1}, X_{j_2}, \ldots, X_{j_n}$. Opgevat als karakteristieke functie beschrijft dit monoom de affiene deel verz. gedefiniëerd door $X_{j_1} = X_{j_2} = \ldots = X_{j_n} = 1$ van dimensie m - n. Omgekeerd gaat men gemakkelijk na dat iedere affiene deelverzameling van dimensie $\ge m - v$ een karakteristieke functie heeft die tot RM(m,v,2) behoort. Niet alle elementen van RM(m,v,2) zijn van deze vorm, maar de code wordt wel door deze elementen als additieve groep voortgebracht.

We kunnen de code op deze wijze geometrisch interpreteren als een stelsel deelverzamelingen van $(\mathbb{F}_2)^m$. De som van twee elementen is het symetrisch verschil van de verzamelingen en het product van twee functies correspondeert met de doorsnede van de bijbehorende verzamelingen. Het "inproduct" van twee verzamelingen is het aantal elementen van hun doorsnede modulo twee.

De "rechtstandige" affiene deelruimten gedefiniëerd door $X_{j_1} = X_{j_2} = \ldots = X_{j_n} = 0$ met $j_1 < j_2 < \ldots < j_n \le m$ en $n \le v$ vormen een basis voor RM(m,v,2). Notaite $V(\Gamma)$ met $\Gamma = \{j_1, \ldots, j_n\}$. Bij deze affiene deelruimte horen de translaties

$$X_{j_1} = \varepsilon_1,\ X_{j_2} = \varepsilon_2,\ \ldots,\ X_{j_n} = \varepsilon_n \qquad \text{met } \varepsilon_i = 0 \text{ of } 1.$$

De verz. $\{j_1,\ldots,j_n\}$ heet de orientatie van deze deelruimte. Beschouw nu het decodeer probleem voor RM(m,v,2). Een overgeseind woord met fouten is een willekeurige deelverzameling $A \subset (\mathbb{F}_2)^m$. De minimale afstand van RM(m,v,2) is gelijk 2^{m-v} zodat we in staat moeten zijn $e = 2^{m-v-1} - 1$ fouten te corrigeren.

Stel $A = B + C$ met $B \in RM(m,v,2)$ en $\#C \leq e$. We kunnen schrijven

$$B = \sum_{\#\Gamma \leq v} \varepsilon_\Gamma V(\Gamma) \qquad \text{met } \varepsilon_\Gamma = 0 \text{ of } 1$$

en het probleem is de ε_Γ uit te rekenen.

Stel $\#\Gamma = v$ en kies $\Delta = \{1,\ldots,m\}\backslash\Gamma$ dan geldt $\#(V(\Gamma)\cap V(\Delta)) = 1$. Dit geldt niet alleen voor $V(\Delta)$ zelve maar eveneens voor de 2^{m-v} translaties van $V(\Delta)$. Anderzijds geldt voor $\Gamma' \neq \Gamma$, $\#\Gamma' \leq v$ dat $\#(V(\Gamma')\cap V(\Delta)) \equiv 0 \bmod 2$ en idem voor de translaties van $V(\Delta)$. De conclusie is dat we 2^{m-v} disjuncte pariteits condities hebben om het getal ε_Γ uit te rekenen:

$$\#(A\cap V(\Delta)) \equiv \#((B+C)\cap V(\Delta)) \equiv \#(B\cap v(\Delta)) + \#(C\cap V(\Delta)) = \varepsilon_\Gamma + \text{storing}$$

en idem voor de translaties van $V(\Delta)$.

Omdat bij aanname C hoogstens $e = 2^{m-v-1} - 1$ elementen bevat die ieder hoogstens één uitkomst storen kan op deze wijze de waarde van ε_Γ worden bepaald bij meerderheid van stemmen.

Indien ε_Γ eenmaal bepaald is voor alle Γ met $\#\Gamma = v$ kan men de bewuste termen van A aftrekken en de ε_Γ voor $\#\Gamma < v$ op analoge wijze uitrekenen.

LITTERATUUR

Het hier weergegeven bewijs is afkomstig van H.W. LENSTRA II. De stelling dat de twee beschrijvingen van de gegeneraliseerde Reed-Muller codes equivalent zijn kan men o.m. aantreffen in VAN LINT: *Coding Theory*, LNM 201, Springer (1971) en in I.F. BLAKE & R.C. MULLIN: *The mathematical theory of Coding*, Acd. Press (1975). Dit laatste boek zegt het weergegeven bewijs (dat algebraïsch gezien het onze redelijk benadert) is ontleend aan het artikel *On Generalized Reed-Muller Codes and their Relatives* van de hand van P. DELSARTE, J.M. GOETHALS & F.J. MacWILLIAMS, Inf. and Control 16 (1970), 403-442. Voor de theorie over eindige lichamen verwijs ik naar *Equations et variétés algebriques sur un corps fini* van J.R. JOLY, Enseign. Math. 19 (1973), Fasc 1-2.

Hoofdstuk V

CYCLISCHE CODES

door

A. Schrijver

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 ee cyclische code is de code V ter lengte 2k met: $(a_0,\ldots,a_{2k-1}) \in V \iff a_0=a_k,\ a_1=a_{k+1},\ldots,a_{k-1}=a_{2k-1}$. Zij $R^{(n)}$ de n-dimensionale rektorruimte 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 vektor uit $R^{(n)}$ voor te stellen als een element van (een volledig representantensystem van) de restklassenring $\mathbb{F}[x]/(x^n-1)$. Het is duidelijk dat deze relatie een 1-1-correspondentie geeft tussen elementen van $R^{(n)}$ 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 $R^{(n)}$ of R. Een cyclische code V is dus een deelverzameling van $\mathbb{F}[x]/(x^n-1)$ en wel een ideaal. Want als f(x) en g(x) $\in$ V dan ook f(x)+g(x) $\in$ V en als f(x) $\in$ V en g(x) $\in R$ dan f(x)·g(x) $\in$ V (deze laatste vermenigvuldiging uiteraard in the restklassenring). Omgekeerd bepaalt ieder ideaal in $R^{(n)}$ een cyclische code. Immers, de verschuiving $(a_0,\ldots,a_{n-1}) \to (a_{n-1},a_0,\ldots,a_{n-2})$ komt overeen met een vermenigvuldiging met het polynoom x. Zij $q := |\mathbb{F}|$. We beperken ons in het vervolg to 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) and R g(x) := het ideaal in R voortgebracht door g(x). Dus $R = {}^{R}/_{S}$. Omdat R een hoofideaalring is, is ook ieder ideaal in R een hoofdideaal, en ieder ideaal V in R wordt voortge-

bracht door een monisch polynoom g(x) met de laagste graad in V. Dit uniek bepaalde polynoom 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) and 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.

2. GENERATOR-MATRIX EN CHECK-POLYNOOM

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

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

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

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

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

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

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

Dan

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

$$= G$$

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

Een pariteits-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-d heeft, zal $h(x)$ de graad d hebben. Dus:

$$h(x) = h_0 + h_1x + \ldots + h_dx^d:$$

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

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

Als nu:

$$H = \begin{pmatrix} 0 \ldots\ldots\ldots 0 & h_d & \ldots\ldots\ldots & h_1 & h_0 \\ 0 \quad\quad\quad 0 & h_d & h_{d-1} & \ldots\ldots\ldots & h_0 \; 0 \\ \cdot \quad\quad\quad \cdot \; \cdot & \cdot & & & \cdot \; \cdot \\ \cdot \quad\quad\quad \cdot \; \cdot & \cdot & & & \cdot \; \cdot \\ \cdot \quad\quad\quad \cdot \; \cdot & \cdot & & & \cdot \; \cdot \\ h_d \ldots\ldots\ldots\ldots h_0 & 0 & \ldots\ldots\ldots\ldots & 0 & \end{pmatrix}$$

dan geldt dus $G.H^T = 0$ (omdat $h_{d+1} = \ldots = h_{n-1} = 0$), d.w.z. H is de pariteits-check-matrix van de code. Hieruit volgt ook dat de code $Rh(x)$ equivalent is met de duale code van $Rg(x)$. $h(x)$ 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 $\mathbb{F} = GF(2)$ 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. $Rg(x)$ is equivalent met de (7,4)-Hamming-code.

3. NULPUNTEN VAN EEN CYCLISCHE CODE

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

$Rf_i(x) = \{v(x) \mid v(\beta_i) = 0\}$ (want f_i is het minimaalpolynoom van β_i).

Algemeen kan een cyclische code V gespecificeerd 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 machts eenheidswortels zijn. De generator van V is nu het produkt van de minimaalpolynomen van de β_j's, zonder herhaling van faktoren. 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 kolomvektor ter hoogte m over GF(q). De eis $v(\beta) = 0$ wordt nu: $vH^T = 0$, met $H = (\underline{1}\ \underline{\beta}\ \underline{\beta^2} \ldots \beta^{n-1})$. 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. *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* $(m,q-1) = 1$.

GEVOLG. *Iedere binaire Hamming-code is (equivalent met) een cyclische code.*

BEWIJS VAN DE STELLING

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

Immers, $(m,q-1) = (n,q-1)$, want:

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

Dan: $\forall\ i = 1,\ldots,n-1: \beta^i \notin GF(q) \Leftrightarrow \forall\ i = 1,\ldots,n-1: \beta^{i(q-1)} \neq 1 \Leftrightarrow$
$\forall\ i = 1,\ldots,n-1: n \nmid i(q-1) \Leftrightarrow (n,q-1) = (m,q-1) = 1$. □

4. DE IDEMPOTENT VAN EEN CYCLISCHE CODE

STELLING. *Zij* V *een cyclische code. Dan bevat* V *een (uniek bepaald) codewoord* c(x) *dat een eenheid 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 eenheid 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. 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 (waarbij $q = |\mathbb{F}|$). Zij m het kleinste positive 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 produkt van de minimale polynomen van $\beta, \beta^2, \ldots, \beta^{d-1}$ (zò dat geen faktor dubbel voorkomt). Dan heet de cyclische code R g(x) een *BCH-code* met *ontwerp-afstand* d. Dit is dus de code:

$$\{v(x) \mid v(\beta) = v(\beta^2) = \ldots = v(\beta^{d-1}) = 0\} \text{ (zoals in § 3).}$$

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:

STELLING. *De minimum-afstand van een* BCH-*code met ontwerpafstand* d *is ten minste* d.

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

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

Iedere β^i hierin stelt een kolom ter hoogte m voor als beschreven in § 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:

$$\begin{matrix} \xi_1 & \ldots\ldots\ldots & \xi_{d-1} \\ \xi_1^2 & \ldots\ldots\ldots & \xi_{d-1}^2 \\ . & & . \\ . & & . \\ . & & . \\ . & & . \\ \xi_1^{d-1} & \ldots\ldots\ldots & \xi_{d-1}^{d-1} \end{matrix}$$

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

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

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

In het algemeen is het vinden van de feitelijk minimum-afstand een moeilijk probleem. Niet altijd is de minimum-afstand gelijk aan de ontwerpafstand. 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 produkt (zonder faktor-herhaling) 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 ontwerpafstand 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.

6. EEN PROCEDURE VOOR HET CORRIGEREN VAN FOUTEN BY BCH-CODES

Stel dat een codewoord C(x) van een BCH-code (met ontwerp-afstand d, ter lengte n, over het lichaam GF(q), en m en β als in § 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 fouten-patroon. 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 $E_i = \dfrac{\omega(\beta^{-i})}{\sigma'(\beta^{-i})}$

We berekenen nu:

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

Voor $1 \leq \ell \leq 2t$ is $E(\beta^\ell) = R(\beta^\ell)$, dus aan de ontvanger van het codewoord bekend. D.w.z. $\dfrac{\omega(z)}{\sigma(z)}$ is bekend modulo z^{2t+1}. De kunst is nu om polynomen $\sigma(z)$ en $\omega(z)$ van zo laag mogelijke graad te vinden zo 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 $\sigma(z) = \sum_{i=0}^{\infty} \sigma_i z^i$. Dan is:

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

Daar $\omega(z)$ de graad e heeft, volgt:

$\sum_{i+\ell=k} S_\ell\sigma_i = 0$ voor $e + 1 \leq k \leq 2t$. Dit zijn 2t-e vergelijkingen voor de e onbekenden $\sigma_1,\ldots,\sigma_e$ (want $\sigma_0 = 1$ is bekend). Als $e \leq t$ 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 $e + 1 \leq k \leq 2t$:

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

Dit zijn 2t-e vergelijkingen voor de onbekenden $E_i\tilde{\sigma}(\beta^{-1})$. 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 $\tilde{\sigma} = \sigma$.
Dus als we polynomen $\omega(z)$ en $\sigma(z)$ van zo laag mogelijke graad gevonden hebben, dan zijn dit de gevraagde $\omega(z)$ en $\sigma(z)$.

7. REED-SOLOMON-CODES

Een *Reed-Solomon-code* of *RS-code* is een primitieve BCH-code waarbij $m = 1$, $n = q-1$. Een RS-code wordt wel een *optimale code* genoemd, omdat voor de minimum-afstand d' geldt: $d' = n-k+1$. Volgens Singleton geldt altijd: $d' \leq n-k+1$. Als d de ontwerp-afstand van de code is dan $d' \geq d$. Verder wordt de code voortgebracht door het polynoom $g(x) = \prod_{i=1}^{d-1} (x-\alpha^i)$ (dit is een polynoom in $GF(q)[x]$), dus: $k = n-d+1 \geq n-d'+1$, d.w.z. $d' \geq n-k+1$.
De RS-codes worden vooral gebruikt voor burst-error correcting: nemen we $q = 2^r$ dan hebben we een binaire code met woordlengte $r(2^r-1)$ en dimensie rk. Een burst error die bits wijzigt in een traject ter lengte $b \leq ([d/2]-1)r+1$, verandert hooguit $[d/2]$ symbolen van de oorspronkelijke code (over $GF(2^r)$). Maar deze fout kan dus gecorrigeerd worden.

8. KWADRATISCHE REST-CODES

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

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

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:

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

DEFINITIE: 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 *uitgebreide QR-code* van lengte n+1 over GF(q) wordt verkregen door aan de code met generator $g_0(x)$ een extra pariteits-check symbool toe te voegen.

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:

$$\pi_j(\ell) \equiv j\ell \pmod n,\ 0 \le \pi_j(\ell) < n,$$

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

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

en: $R_0 = jR_1$, geldt:

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

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

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.

STELLING. *Zij* $c(x)$ *een codewoord van* $Rg_0(x)$, *zo dat* $c(x) \notin R\,(x-1)g_0(x)$. *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 $d \equiv 3 \pmod 4$.

BEWIJS

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

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

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

Maar dan:

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

(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:

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

(iii) Zij $c(x) = \sum_{i=1}^{d} x^{e_i}$. Dan

$c(x)\pi_{-1}c(x) = \sum_{i \neq j} x^{e_i-e_j}$. 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: $d \equiv 3 \pmod)$(d is oneven, omdat $c(x) \notin R\,(x-1)g_0(x)$). ||.

Hoofdstuk VI

GELIJKMATIG VERDEELDE CODES

door

J.H. van Lint & H.C.A. van Tilborg

1. INLEIDING

In dit hoofdstuk beperken we ons tot binaire codes. Om inzicht te krijin resultaten en bewijsmethoden van dit deel van Coding Theory is dit voldoende. Vrijwel alles gaat (met iets meer werk) precies zo over codes over een alfabet van meer dan twee symbolen.

Om de codes die ons nu interesseren te definieren 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

$$(1.1) \qquad A_C(z) := \sum_{i=0}^{n} a_i z^i := |C|^{-1} \sum_{\underline{u}\in C,\underline{v}\in C} z^{d(\underline{u},\underline{v})} .$$

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,...,n, en wel

$$(1.2) \qquad B(\underline{x},i) := \#\text{ elementen van C met afstand i tot } \underline{x}.$$

Met $B(\underline{x})$ geven we de rij van B met nummer $\underline{x}$ aan. Merk op dat

$$(1.3) \qquad \underline{a} = |C|^{-1} \sum_{\underline{x}\in C} B(\underline{x}).$$

$$(1.4) \qquad B(\underline{x},0) = 1 \iff \underline{x} \in C.$$

Als alle rijen van B die met 1 beginnen hetzelfde zijn noemt men C een *reguliere* code. De code C heet *volledig regulier* als

$$(1.5) \qquad \forall_{\underline{x}\in X}\, \forall_{\underline{y}\in X}[(\rho(\underline{x},C) = \rho(\underline{y},C)) \Rightarrow (B(\underline{x}) = B(\underline{y}))],$$

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. [2])

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 vermenigsvuldiging *, gedefinieerd door

$$(1.6) \qquad \sum_{\underline{x}\in X} \alpha(\underline{x})\underline{x} * \sum_{\underline{y}\in X} \beta(\underline{y})\underline{y} := \sum_{\underline{z}\in X} \Big(\sum_{\underline{x}+\underline{y}=\underline{z}} \alpha(\underline{x})\beta(\underline{y}) \Big)\underline{z}.$$

Aan een deelverzameling Y van X voegen we toe het element $\sum_{\underline{y}\in Y} \underline{y}$ 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.

$$(1.7) \qquad Y_i := \{\underline{x} \in X \mid w(\underline{x}) = i\} ,$$

$$(1.8) \qquad S_j := \{\underline{x} \in X \mid w(\underline{x}) \leq j\} .$$

Nu geldt voor een code C met outer distribution B

$$(1.9) \qquad Y_i * C = \sum_{\underline{x}\in X} B(\underline{x},i)\underline{x}.$$

Zij $D(\underline{x},y)$ het aantal codewoorden met afstand $\leq j$ tot $\underline{x}$, d.w.z. $D(\underline{x},j) = \sum_{i\leq j} B(x,i)$. Dan is volgens (1.8) en (1.9)

$$(1.10) \qquad S_j * C = \sum D(\underline{x},j)\underline{x}.$$

(zie o.a. [4]).

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

$$(2.1) \qquad \forall_{\underline{v}\in X}[\chi_{\underline{u}}(\underline{v}) := \chi((\underline{u},\underline{v})) = (-1)^{(\underline{u},\underline{v})}],$$

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 A door

$$(2.2) \qquad \chi_{\underline{u}}(\sum \alpha(\underline{x})\underline{x}) = \sum \alpha(\underline{x})\chi_{\underline{u}}(\underline{x}).$$

De volgende twee beweringen volgen eenvoudig uit de definities. We laten het bewijs als oefening aan de lezer over.

$$(2.3) \qquad \forall_{\underline{u}\in X} \forall_{A\in A} \forall_{B\in A} [\chi_{\underline{u}}(A*B) = \chi_{\underline{u}}(A)\chi_{\underline{u}}(B)]$$

(2.4) S_n is het enige element van 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

$$(2.5) \qquad K_k(n,x) := \sum_{i=0}^{k} (-1)^i \binom{x}{i}\binom{n-x}{k-i},$$

waarin $\binom{x}{a} := x(x-1)\ldots(x-a+1)/a!$.

We hebben dan aangetoond dat

$$(2.6) \qquad \chi_{\underline{u}}(Y_k) = K_k(n,w(\underline{u})).$$

De Krawtchouk polynomen zijn bekend uit de theorie van orthogonale polynomen op een discrete verzameling (cf. SZEGÖ [6], *Orthogonal Polynomials* §2.8). We noemen een aantal eigenschappen welke de lezer eenvoudig kan verifiëren resp. uit de algemene theorie halen.

$$(2.7) \qquad \sum_{k=0}^{\infty} K_k(n,x)z^k = (1+z)^{n-x}(1-z)^x,$$

$$(2.8) \qquad K_k(n,x) = \sum_{j=0}^{k} (-2)^j \binom{n-j}{k-j}\binom{x}{j},$$

dus K_k is een polynoom van de graad k in x.

$$(2.9) \qquad \sum_{m=0}^{n} \binom{n}{m} K_k(n,m)K_\ell(n,m) = \delta_{k,\ell}\binom{n}{k}2^n.$$

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 $\leq n$, dan is F(x) éénduidig te schrijven als lineaire combinatie van de $K_k(n,x)$, $0 \leq k \leq n$:

$$(2.10) \qquad F(x) = \sum_{k=0}^{n} \alpha_k K_k(n,x);$$

we noemen dit de Krawtchouk-ontwikkeling van F(x).

Uit (2.6) volgt via een eenvoudige berekening dat als $w(\underline{u}) = x$.

$$(2.11) \qquad \chi_{\underline{u}}(S_j) = K_j(n-1,x-1) =: \Psi_j(x).$$

Uit (2.8) kan men eenvoudig de coëfficiënten 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 $\Psi_e(x)$

$$(2.12) \qquad \prod_{i=1}^{e} x_i = e!\, 2^{-e} \sum_{i=0}^{e} \binom{n}{i},$$

$$(2.13) \qquad \sum_{i=1}^{e} x_i = \tfrac{1}{2}e(n+1),$$

$$(2.14) \qquad \sum_{i<j} x_i x_j = \frac{1}{24}\, e(e-1)\{3n^2 + 3n + 2e + 2\}.$$

Merk op dat (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

$$(2.15) \qquad \prod_{i=1}^{e} (x_i-1) = 2^{-e}(n-1)(n-2)\ldots(n-e),$$

$$(2.16) \qquad \prod_{i=1}^{e} (x_i-2) = 2^{-e}(n-1-2e)(n-2)(n-3)\ldots(n-e).$$

(lit. [3], [4], [5]).

3. HET KARAKTERISTIEKE POLYNOOM VAN EEN CODE

Zij C een code in X. Voor j = 0,1,...,n definiëren we de *karakteristieke getallen* B_j van C door

$$B_j := |C|^{-2} \sum_{u \in Y_j} |\chi_{\underline{u}}(C)|^2. \tag{3.1}$$

Zij $N(C) := \{j \mid 1 \le j \le n,\ B_j \neq 0\}$. We definiëren het *karakteristieke polynoom* van C door

$$F_C(x) := 2^n |C|^{-1} \prod_{j \in N(C)} (1-x/j). \tag{3.2}$$

(3.3) STELLING: *Laten* $\alpha_0,\alpha_1,\ldots,\alpha_n$ *de coëfficiënten uit de Krawtchouk ontwikkeling van* $F_C(x)$ *zijn. Dan geldt in* A

$$\sum \alpha_i Y_i * C = S_n.$$

BEWIJS. Zij $\underline{u} \in X$, $w(\underline{u}) = j$. Volgens (2.3) en (2.6) is

$$\chi_{\underline{u}}(\sum \alpha_i Y_i * C) = \chi_{\underline{u}}(\sum \alpha_i Y_i)\chi_{\underline{u}}(C) = \chi_{\underline{u}}(C) \sum \alpha_i P_i(j) = \chi_{\underline{u}}(C) F_C(j).$$

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 (2.4). □

(3.4) GEVOLG: *Voor de coëfficiënten* $\alpha_0,\alpha_1,\ldots,\alpha_n$ *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

$$\rho(C) := \max\{\rho(\underline{x},C) \mid \underline{x} \in X\}. \tag{3.5}$$

Merk op dat uit (3.4) volgt dat $\rho(C) \le |N(C)| =: s$.

We vermelden hier zonder bewijs de *identiteit van MacWilliams* (waarvan het bewijs door eenvoudige algebraïsche manipulatie is te geven).

(3.6) STELLING: *Laat voor* $j = 0,1,\ldots,n$

$$G := |C|^{-1} \sum_{\underline{u}\in Y_j} \chi_{\underline{u}}(C).$$

Dan geldt voor de weight enumerator $W_C(z)$ *van* C.

$$W_C(z) = 2^{-n}|C| \sum_{j=0}^{n} C_j(1-z)^j(1+z)^{n-j}.$$

Merk op dat als C een lineaire code is dan $\chi_{\underline{u}}(C) = |C|$ als $u \in C^{\perp}$, maar $\chi_{\underline{u}}(C) = 0$ voor alle andere $\underline{u}$. Dat betekent dat in dat geval $C_j = B_j$ = aantal woorden van gewicht j in $C^{\perp}$. Dan geeft (3.6) een verband tussen de weightenumerator van C en die van $C^{\perp}$.
(lit. [3]).

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 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 als $d = 2e + 1$. 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.

(4.1) DEFINITIE. 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

$$(4.2) \qquad r \leq \frac{n}{e+1}$$

In het geval dat $r = \left[\frac{n}{e+2}\right]$ noemt met C *bijna perfect*.

(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 (1.9) en (4.1). □

(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 (3.3) en (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 $\chi_u(C) \neq 0$, dan is op grond van (4.3), (2.3), (2.6) en (2.10) $F(j) = 0$. Dus is op grond van (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 (4.3), is $a = 1$. □

Uit het bewijs van (4.4) volgt de volgende uitbreiding van een stelling die door S.P. Lloyd voor lineaire perfecte codes is bewezen.

(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 (2.5) neerkomt op

$$(4.6) \qquad |C|\left\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}\binom{n+1}{e+1}\right\} = 2^n,$$

hetgeen de tellende vorm van (4.3) is.

We zullen het bewijs hier niet geven maar we merken op dat m.b.v. (3.6) is aan te tonen dat gelijkmatig verdeelde codes volledig regulier zijn.

In het algemeen is de definitie (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 (4.4) moet $F_C(x)$ graad 2 hebben. In de opmerking na (3.6) 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 (2.7) in (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

$$K_k(n,0) + N_1 K_k(n,w_1) + N_2 K_k(n,w_2) = 0 \qquad (k=1,2).$$

Wederom gebruik makend van de opmerking na (3.6) 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. (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:

(4.7) STELLING. *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. [3]).

5. VOORBEELDEN

(a) 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.

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 $\underline{x}_i$

$$\underline{z} = - - \quad + + + \quad + + + \quad + + +$$

$$\underline{x}_1 = + + \quad + + + \quad + + + \quad + + +$$

$$\underline{x}_2 = - - \quad - - - \quad + + + \quad + + +$$

$$\underline{x}_3 = - - \quad + + + \quad - - - \quad + + +$$

$$\underline{x}_4 = - - \quad + + + \quad + + + \quad - - -$$

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 $\underline{+}$ rij hebben. We zien uit (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 [5]).

(b) 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 $\underline{w}_1, \underline{w}_2, \ldots, \underline{w}_{35}$.

Zij G de 6 x 35 matrix gedefinieerd door

$$(G)_{i,j} = \begin{cases} 1 & \text{als de } i^{de} \text{ coördinaat van } w_j \text{ 1 is,} \\ 0 & \text{als deze 0 is.} \end{cases}$$

In woorden de i^{de} rij van G is de karakteristieke vector van de doorsnijding van W met het hypervlak $x_i = 1$. Evenzo is $\underline{a}^T G$, $\underline{a} \in V$, de karakteristieke vector van de doorsnijding van W met het hypervlak $\sum_{i=1}^{6} a_i x_i = 1$. Het gewicht van $\underline{a}^T G$ is dus het aantal oplossingen in V van

$$x_1x_2 + x_3x_4 + x_5x_6 = 0$$

en

$$\sum_{i=1}^{6} a_i x_i = 1.$$

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

$$(1+a_2+a_3a_4+a_5x_6)x_2 + (x_3+a_4x_2)(x_4+a_3x_2) + (x_5+a_6x_2)(x_6+a_5x_2) = 0.$$

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

$$(1+a_2+a_3a_4+a_5a_6)y_2 + y_3y_4 + y_5y_6 = 0.$$

Als de coëfficient van y_2 1 is, 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 (3.5) geldt $\rho(C) = 2$. Daar

$16 + 20 = 35 + 1$, volgt uit stelling (4.7) dat C gelijkmatig verdeeld is.

(Zie [3]).

(c) Zij α een primitief element van $GF(2^5)$, $m_1(x)$ het minimaalpolynoom 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 de 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.z. $m(x) \in B$, 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. Zij $f(x)$ het eenheidselement in dit lichaam. 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 $\hat{S}_1$.

DEFINITIE. 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 [1]).

Nu substitueren we in (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 (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.

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. Sinds zeer kort [7] 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 (4.5) toe (met e i.p.v. e+1). We zien dat het in (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 (4.5) en (2.5)

$$\sum_{i=0}^{e} \binom{n}{i} = 2^n |C|^{-1},$$

en dus is volgens (2.12)

$$(6.1) \qquad \prod_{i=1}^{e} x_i = e!\, 2^{\ell}$$

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 (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 $\underline{\Psi}_e(x)$ is vinden we

$$x_e - x_1 \geq \frac{2}{3} n. \tag{6.2}$$

Als tweede stap beschouwen we (2.13) en (2.14). Hieruit volgt

$$\sum_{i=1}^{e} \sum_{j=1}^{e} (x_i - x_j)^2 = \frac{1}{2} (e+1)^2 (n - \frac{2e-1}{3}).$$

Hieruit volgt dan weer

$$(x_e - x_1) \leq \frac{1}{2} (e+1)(en)^{\frac{1}{2}} \tag{6.3}$$

Uit (6.2) en (6.3) vinden we

$$n \leq \frac{9}{16} e(e+1)^2. \tag{6.4}$$

Nu beschouwen we (2.15) en (2.16). Daar voor iedere $x \in \mathbb{N}$ geldt $(x-1)(x-2) \equiv 0 \pmod 2$ vinden we

$$(n-1-2e)(n-1)(n-2)^2(n-3)^2 \ldots (n-e)^2 \equiv 0 \pmod{2^{3e}}. \tag{6.5}$$

Zij 2^α de hoogste macht van 2 die een factor $n - j$ in het linkerlid van (6.5) deelt. Dan is de hoogste macht van 2 die het linkerlid van (6.5) deelt kleiner dan $2^{3\alpha+2e}$. Hieruit volgt $\alpha \geq \frac{1}{3} e$. Dus is

$$n > 2^{\frac{1}{3} e}. \tag{6.6}$$

Voor grote e zijn (6.4) en (6.6) strijdig. De kleine e, en dus volgens (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

$$(6.7) \qquad (x_{e+1}-x_1)^2 \leq (e+1)\left(\frac{n+1}{2}\right)^{\frac{e}{7}}$$

$$(6.8) \qquad n > 2^{\frac{e}{7}}.$$

We hernummeren de wortels x_i tot $y_j = A(y_j)2^{\alpha_j}$, zodat

$$\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{e+1}.$$

Nu geldt enerzijds

$$\prod_{i=1}^{e} \frac{|y_i-y_{i+1}|}{y_i} \geq \prod_{i=1}^{e} \frac{k.g.v.(y_i,y_{i+1})}{y_i} = \prod_{i=1}^{e} \frac{k.g.v.(A(y_i),A(y_{i+1}))2^{\alpha_i}}{y_i} \geq$$

$$\prod_{i=1}^{e} \frac{1}{A(y_i)} \geq \frac{1}{A(y_1 \ldots y_{e+1})} = \frac{A(|C|)}{A(r)A((e+1)!)} \geq \frac{1}{rA((e+1)!)}$$

en anderzijds

$$\prod_{i=1}^{e} \frac{|y_i-y_{i+1}|}{y_i} \leq \frac{(x_{e+1}-x_1)^e}{y_1 \ldots y_e} \leq \frac{n(x_{e+1}-x_1)^e}{x_1 x_2 \ldots x_{e+1}} = \frac{n(x_{e+1}-x_1)^e}{r(e+1)!} \quad \frac{2^{e+1}|C|}{2^n} .$$

Derhalve vinden we

$$(x_{e+1}-x_1)^e \geq \frac{(e+1)!}{A((e+1)!)n2^{e+1}} \frac{2^n}{|C|} \geq \frac{1}{n} \sum_{i=0}^{e} \binom{n}{i} \geq \frac{1}{n} \binom{n}{e},$$

dus

$$(6.9) \qquad (x_{e+1}-x_1)^e \geq \frac{(n-1)(n-2)\ldots(n-e+1)}{e!} .$$

Vergelijking van (6.7), (6.8) en (6.9) levert voor $e \geq 3$ 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 (4.5) behandeld worden (lit. [3], [7]).

We besluiten dit hoofdstuk met een tabel van alle perfecte, bijna perfecte en gelijkmatig verdeelde, bineaire codes.

e	n	|C|	type	naam
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

LITERATUUR

[1] CAMERON, P.J. & J.H. VAN LINT, *Graph Theory, Coding, Block Designs*, London Math. Soc. Lecture Note Series 19, Cambr. Univ. Press, 1975.

[2] DELSARTE, P., *An algebraic approach to the association schemes of coding theory*, Philips Res. Repts. Suppl. (1973), No. 10.

[3] GOETHALS, J.M. & H.C.A. VAN TILBURG, *Uniformly packed codes*, Philips Res. Repts. 30 (1975), 9-36.

[4] VAN LINT, J.H., *Coding Theory*, Lecture Notes in Math. 201, Springer Verlag, Berlin etc. 1971.

[5] VAN LINT, J.H., *Recent results on perfect codes and related topics*, Combinatorics I, Math. Centre Tracts 55 (1974), 158-178.

[6] SZEGÖ, G., *Orthogonal polynomials*, A.M.S. Coll. Publ. 23 (1959).

[7] VAN TILBURG, H.C.A., *All binary* (n,e,r)*-uniformly packed codes are known*, Memorandum 1975-08, T.H. Eindhoven.

Hoofdstuk VII

GOPPA CODES

door

A.E. Brouwer

0. MOTIVATIE

Zoals een ieder zich zal herinneren ziet de parity check matrix van een BCH code met ontwerp afstand d eruit als

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

waarbij β een primitieve n-de machts eenheidswortel in $GF(q^m)$ is, opgevat als kolomvector ter hoogte m met entries in GF(q).
[Hierbij is $n \mid q^m-1$ 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 algemene

$$H = \begin{pmatrix} h_0\beta_0 & h_1\beta_1 & \dots & h_{n-1}\beta_{n-1} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ h_0\beta_0^{d-1} & h_{n-1} & \dots & h_{n-1}\beta_{n-1}^{d-1} \end{pmatrix}$$

waarbij $h_j \in GF(q^m)\setminus\{0\}$, en alle β_i onderling verschillende elementen van

$GF(q^m)\setminus\{0\}$ zijn. Als $h_j \in GF(q)$ (en ihb 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 limiet halen.

1. 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) gedefineerd 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

$$\sum_{\gamma\in L} \frac{C_\gamma}{z-\gamma} \equiv 0 \mod g(z).$$

Het is duidelijk dat Goppa codes lineair zijn. Laten we de parity check matrix uitrekenen:

Aangezien

$$\frac{1}{z-\gamma} \equiv -\frac{1}{g(\gamma)} \cdot \left(\frac{g(z)-g(\gamma)}{z-\gamma}\right) \mod g(z),$$

waarbij het rechterlid een polynoom van graad < t is, wordt de parity check matrix voor de code gegeven door de rij

$$\left(\frac{1}{g(\gamma_1)} \cdot \frac{g(z)-g(\gamma_1)}{z-\gamma_1}, \quad \cdots \quad, \frac{1}{g(\gamma_n)} \cdot \frac{g(z)-g(\gamma_n)}{z-\gamma_n}\right).$$

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 + graad$(g(z))$ is. (Ter vergelijking: by cyclische codes en BCH codes kan in het algemeen niets gezegd worden over d als alleen de graad van het generator polynoom bekend is.)

VOORBEELD: 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 $L = \{\beta^{-j} \mid 0 \leq j \leq n-1\}$.
(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 § 0 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.

2. 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

$L = \{\gamma_1,\ldots,\gamma_n\} \subset GF(q^m)$, 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.

Onmiddelijk 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 $\xi(z) \equiv 0 \bmod g(z)$ impliceert dat $g(z) \mid t(z)$ 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 kopcoëfficiënt van $t(z)$ 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 $\sum_{i=0}^{n} b_i\gamma_i^r = 0$ $(0 \leq r \leq s)$ toevoegen dan krijgen we een $(n,n-1-(t+s)m,(t+s)+2)$ code.

Natuurlijk had dit effect ook bereikt kunnen worden door de graad van g(z) 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 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.

ASYMPTOTISCH GEDRAG

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 $\lim k/n = 0$), 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 $(q-1)^d\binom{n}{d}$ worden $(C_1,\ldots,C_n)$ met gewicht d. Zo'n woord zit ten hoogste $\left[\frac{d-1}{t}\right]$ 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

$$\sum_{d=0}^{D} \left[\frac{d-1}{t}\right] (q-1)^d \binom{n}{d} < \#\text{ irreducibele polynomen over } GF(q^m) \text{ van graad t}$$

dan zijn er zeker Goppa codes met $d_{min} > D$, en rste $R \geq 1 - \frac{mt}{n}$. Maar het aantal irreducibele polynomen van graad t is

$$\frac{1}{t} \sum_{d|t} \mu(d) q^{mt/d} \geq \frac{q^{mt}}{t} (1 - q^{-(mt/2)+1}),$$

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:

$$\sum_{d=0}^{D} (q-1)^d \binom{n}{d} < q^{(1-R)n}$$

3. HET MATTSOM-SOLOMON POLYNOOM

Zoals al door Goppa aangegeven en recentelijk door Chien & Choy verder uitgewerkt is, is de eis $\sum_{i=1}^{n} \frac{1}{z-\gamma_i} \equiv 0 \pmod{g(z)}$ in feite een deelbaarheidseis voor de Fourier Transform 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 Transform (het Mattsom 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

$$A(\alpha^{-k}) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i \alpha^{ij} \alpha^{-kj} = n a_k$$

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 mod p is. (In het bijzonder is voor $p = 2$ $a_i = A(\alpha^{-i})$.)

De FT definieert een isomorfie tussen twee ringstructuren op T:

Zij $\circ$ vermenigvuldiging van polynomen modulo $x^n - 1$, en zij $*$ de convolutie: $(\sum a_i x^i) * (\sum b_i x^i) = \sum a_i b_i x^i$.

Dan is

$$\Phi (a \circ b) = \Phi a * \Phi b.$$

Het nut voor de coderingstheorie blijkt uit de volgende

STELLING. Zij $a(x) \in T$. Dan is het gewicht van a(x):

n-graad {ggd (Φa, X^n-1)}.

BEWIJS. $a_i = n^{-1} \cdot \Phi a(\alpha^{-1})$ 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.

Als ik dus will garanderen dat alle vectoren a(x) uit de code een hoog gewicht hebben dan moet ik zorgen dat de graad van ggd (Φa, 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 coëfficiënten 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 hoogstens n-1-graad {G(X)}. Uit de bovenstaande stelling volgt dan dat de code een minimale afstand tenminste 1 + graad {G(X)} heeft.

VOORBEELD. 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:

zij $P(X) = X^{n-1}$, G(X) zonder nulpunten in $GF(q^m) \setminus \{0\}$

dan is de bijbehorende code C de Goppa code met Goppa polynoom G(X) en $L = GF(q^{-n})\backslash\{0\} = \{1,\alpha,\ldots,\alpha^{n-1}\}$.

Op grond van dit voorbeeld claimen Chien & Choy dat de GBCH codes de Goppa codes bevatten. Goppa levert echter codes voor iedere $n \geq q^m$ en niet alleen voor $n|q^m-1$ zodat deze claim ongegrond is.

Wel is het zo dat de GBCH codes de parity check matrix leveren die in §0 als doelgesteld werd:

Zij $p(x) = (\Phi^{-1} P)(x) = \sum_{i=0}^{n-1} P_i X^i$ en $g(x) = (\Phi^{-1} G)(x) = \sum_{i=0}^{n-1} g_i x^i$. Nu geldt $p_i \neq$ en $g_i \neq 0$ $(0 \leq i \leq n-1)$ omdat ggd $(P(X),X^n-1) =$ 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)} zdd

$$P(X) \circ V(X) = A(X)\ G(X) = A(X) \circ G(X).$$

$$\text{Is } a(x) = (\Phi^{-1} A)(x) = \sum_{i=0}^{n-1} a_i x^i \text{ dan volgt}$$

$$p(x) * v(x) = a(x) * g(x)$$

oftewel

$$\sum_{i=0}^{n-1} p_i v_i x^i = \sum_{i=0}^{n-1} a_i g_i x^i$$

oftewel $a_i = p_i g_i^{-1} v_i$ $(0 \leq i \leq n-1)$. Als nu $h_i = p_i g_i^{-1}$ dan volgt uit

$$a(\alpha^{n-j}) = \sum_{i=0}^{n-1} a_i\ \alpha^{i(n-j)} = \sum_{i=0}^{n-1} v_i h_i\ \alpha^{i(n-j)} = A_{n-j} = 0 \quad (1 \leq j \leq \text{graad } G(X))$$

dat $vH^T = 0$ wanneer

$$H = \begin{pmatrix} h_0 & h_1\alpha^{n-1} & \ldots & h_{n-1}\alpha^{(n-1)(n-1)} \\ h_0 & h_1\alpha^{n-2} & \ldots & h_{n-1}\alpha^{(n-2)(n-1)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ h_0 & h_1\alpha^{n-t} & \ldots & h_{n-1}\alpha^{(n-t)(n-1)} \end{pmatrix}.$$

Omgekeerd volgt uit $vH^T = 0$ weer dat graad A(X) $\leq$ 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.

Met $\beta = \alpha^{-1} = \alpha^{n-1}$ krijgen we:

$$H = \begin{pmatrix} h_0 & h_1\beta & \dots & h_{n-1}\beta^{n-1} \\ h_0 & h_1\beta^2 & \dots & h_{n-1}\beta^{(n-1)2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ h_0 & h_1\beta^t & \dots & h_{n-1}\beta^{(n-1)t} \end{pmatrix} .$$

Hier zijn de h_i inderdaad geheel willekeurig (mits ongelijk aan nul). Ook blijkt dat de code geheel bepaald wordt door $P(X)\ G(X)^{-1}$ en graad $(G(X))$, m.a.w. we zouden altijd $G(X) = X^t$ kunnen nemen.

Voor een nadere analyse van deze codes, zie [1].

LITERATUUR

[1] CHIEN, R.T. & D.M. CHOY, *Algebraic generalization of BCH-Goppa-Helgert codes*. IEEE trans.inf.theory 1975, pp. 70-79.

[2] 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.

[3] – *A rational representation of codes and* (L,g)*-codes*. Ibid 1973, pp. 223-229 (1971, Vol. 7, No. 3, pp. 41-49).

[4] – *Codes constructed on the base of* (L,g) *codes*. Ibid 1974, pp. 165-166 (1972, Vol. 8, No. 2, pp. 107-109).

Hoofdstuk VIII

ARITHMETISCHE CODES

door

H.W. Lenstra Jr.

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

$$x = \sum_{i=1}^{t} a_i r^{n(i)} \tag{1.1}$$

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 net 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.

Wij 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 minstens $d(AN_3, S)$, 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 $\in$ $\mathbb{Z}$ (ga na) (*opgave*).

Dit ongemak omzeilen we door *modulaire* AN-codes te beschouwen. Zetten we, met A, B, C als als boven,

$$m = AB,$$

dan kunnen we C opvatten als *ondergroep* van Z/m (de gehele getallen modulo m). We moeten dan wel ons afstandsbegrip aanpassen. Hiertoe maken we Z/m tot verzameling hoekpunten van een graph door (x mod m) en (x' mod m) te verbinden met een kant als

$$x - x' \equiv \pm c.r^j \bmod m$$

voor zekere c,j $\in$ $\mathbb{Z}$, 0 < c < r, j $\geq$ 0. De *modulaire afstand* $d_m(\bar{x},\bar{y})$ tussen twee elementen $\bar{x},\bar{y}$ van $\mathbb{Z}/m$ is dan de afstand tussen $\bar{x}$ en $\bar{y}$ in deze graph, en het *modulaire gewicht* $w_m(\bar{x})$ is gedefinieerd door $w_m(\bar{x}) = d_m(x,(0 \bmod m))$. Voor x,y $\in$ $\mathbb{Z}$ schrijven we in plaats van $d_m((x \bmod m), (y \bmod m))$ en $w_m((x \bmod m), (y \bmod m))$ en $w_m((x \bmod m))$ ook wel eenvoudig $d_m(x,y)$ en $w_m(x)$. Merk op dat geldt

$$w_m(x) = \min\{w(y) \mid y \in \mathbb{Z},\ y \equiv x \bmod m\}$$

$$d_m(x,y) = w(x-y)$$

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 en slechts dan als geldt

$$d_{min}(C) \geq 2e + 1$$

waar $d_{min}(C)$ de *minimum-afstand* van de code is:

$$d_{min}(C) = \min\{w_m(x) \mid x \in C,\ x \neq (0 \bmod m)\}.$$

Niet iedere keuze voor m is zinvol. Als bijvoorbeeld m een priemgetal is waarvoor r een primitieve wortels 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

$$m = r^n - 1, \quad n \in \mathbb{Z}, \ n \geq 2.$$

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

$$x \equiv \sum_{i=0}^{n-1} c_i . r^i \mod (r^n-1)$$

met $c_i \in \{0,1,\ldots, r-1\}$ $(0 \leq i < n)$, 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 $c_0 = c_1 = \ldots = c_{k-1} = 0$; 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 *cyklische AN-code* een ondergroep C van $\mathbb{Z}/(r^n-1)$; hier is 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

$$AB = r^n-1$$

$$C = \{(AN \bmod (r^n-1)) \mid N \in \mathbb{Z}, \ 0 \leq N < B\}.$$

We noemen A de *voortbrenger* van de code. We zijn primair geinteresseerd in

codes waarvan de *rate* $\frac{1}{n}.{}^{r}\log B$ en de minimum-afstand "groot" zijn.

Als abelse groep is C cyklisch van orde B. De benaming "cyklische AN-code" slaat echter op een andere eigenschap, die doet denken aan de cyklische codes over eindige lichamen: is $(x \bmod(r^n-1))$ een element van C_1

$$x \equiv \sum_{i=0}^{n-1} C_i r^i \quad \bmod(r^n-1),$$

dan geldt

$$rx \equiv \sum_{i=0}^{n-1} C_{i-1} r^i \quad \bmod(r^n-1)$$

(indices modulo n), en $(rx \bmod(r^n-1))$ is een element van C omdat C een ondergroep is. Dus de "cyklische opschuiving" van een codewoord behoort weer tot de code. De analogie met cyklische codes over eindige lichamen gaat verder: een cyklische AN-code is een ideaal van de ring $\mathbb{Z}/(r^n-1)$, een cyklische code over GF(q) is niets anders dan een ideaal in $GF(g)[x]/(x^n-1)$. Verder kan men r met X laten corresponderen, A met g(x) (= het voortbrengend polynoom van de code), en met h(x) (het "check polynomial"). Op deze analogie komen we nog terug.

Men verkrijgt *negacyklische* 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 §§ 2,3,4 voor het negacyklische geval te formuleren en te bewijzen.

Referenties voor deze paragraaf: PETERSON & WELDON [11], MASSEY & GARCIA [9], en de daar aangegeven literatuur. Deze auteurs beschouwen voornamelijk het binaire geval.

2. PERFECTE CYKLISCHE AN-CODES VAN ORDE 1.

Zij $C \subset \mathbb{Z}/(r^n-1)$ een cyklische 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

$$S_e \longrightarrow (\mathbb{Z}/(r^n-1))/AC \sim \mathbb{Z}/A$$

moet bijectief zijn. Hier geeft A de voortbrenger van de code aan, als in §1. Merk op dat een perfecte code van orde e alle hoogstens 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

$$0 \bmod (r^n-1),$$

$$c.r^j \bmod (r^n-1), \quad c,j \in \mathbb{Z},\ 0 < |c| < r,\ 0 \leq j < n.$$

De bijectie $S_1 \rightarrow \mathbb{Z}/A$ 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".

STELLING (2.1) [7]. *Stel* $C \subset \mathbb{Z}/(r^n-1)$ *is een perfecte cyklische 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* $H \subset (\mathbb{Z}/A)^*$ (= *multiplicatieve groep van het lichaam* $\mathbb{Z}/A$ *voortgebracht door* (r mod A) *heeft orde* n *en index* 2(r-1). *Bovendien vormen de elementen* ($\pm$ c mod A), c = 1,2,..., r - 1, *een volledig representantensysteem voor de nevenklassen van* H *in* $(\mathbb{Z}/A)^*$.

Omgekeerd, als A *een priemgetal* $> r^2$ *is met de eigenschap dat de ondergroep* $H \subset (\mathbb{Z}/A)^*$ *voortgebracht door* r *index* 2(r-1) *heeft, met* {$\pm$ c mod A| c = 1,2,..., 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 cyklische AN-code van orde* 1.

BEWIJS. 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 $S_1 \longrightarrow \mathbb{Z}/A$ 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 $S_1 \longrightarrow \mathbb{Z}/A$ levert nu een bijectie

$$\{\pm\ c.r^j \mid\ c = 1,2,\ldots,\ r-1,\quad j = 0,1,\ldots\ n-1\} \longrightarrow (\mathbb{Z}/A)^*.$$

Het beeld van $\{r^j \mid\ j = 0,1,\ldots,\ n-1\}$ is net de ondergroep 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 $(\mathbb{Z}/A)^*/H$. In het bijzonder geldt $(-1 \bmod A) \notin H$, dus de orde n van H is oneven. Dit bewijs de eerste helft van de stelling. De omkering laten we aan de lezer over. □

GEVOLG (2.2) [11]. *Stel* p *is een priemgetal* $\equiv 3 \bmod 4$ *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 cyklische AN-code van orde 1. Bovendien is elke perfecte binaire cyklische AN-code van orde 1 van deze vorm.*

BEWIJS. Dit volgt direkt uit de stelling (2.1). De voorwaarde op p is slechts een vertaling van de eis dat $(2 \bmod p) \in (\mathbb{Z}/p)^*$ een ondergroep van index 2 voortbrengt waar $(-1 \bmod p)$ niet in zit. □

Priemgetallen p die aan de voorwaarden van 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 *negcayklische* codes, cf. [11]. Vergelijk dit met de cyklische 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.

GEVOLG (2.3) [18]. *Stel* p *is een priemgetal* $\equiv 5 \bmod 8$ *zodat* $(3 \bmod p) \in (\mathbb{Z}/p)^*$ *een ondergroep van index 4 voortbrengt. Dan brengt* (p mod $(3^{\frac{1}{4}(p-1)}-1)$) *een perfecte ternaire cyklische AN-code van orde 1 in* $\mathbb{Z}/(3^{\frac{1}{4}(p-1)}-1)$ *voort. Bovendien is elke perfecte ternaire cyklische AN-code van orde 1 van deze vorm.*

Een priemgetal p dat aan de voorwaarden van dit gevolg voldoet is automatisch 13 mod 24; voorbeelden zijn p = 13, p = 109.

Niet voor elke r bestaan er perfecte cyklische AN-codes van orde 1:

GEVOLG (24) [2]. *Er bestaat geen perfecte cyklische 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 $H' \subset (\mathbb{Z}/A)$ voortgebracht door (r mod A) en (-1 mod A). Wegens de stelling heeft $(\mathbb{Z}/A)^*/H'$ 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 $(\mathbb{Z}/A)^*/H'$ 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. □

GEVOLG (2.5) [6]. *Er bestaat geen perfecte decimale cyklische AN-code van orde 1.*

BEWIJS. Brengt A zo'n code voort, en is $H^1 \subset (\mathbb{Z}/A)^*$ voortgebracht door de restklassen van 10 en -1, dan heeft $(\mathbb{Z}/A)^*/H^1$ orde 9. Geven we het beeld van (i mod A) in deze groep aan met $\bar{i}$, dan

$$(\mathbb{Z}/A)^*/H^1 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}.$$

Uit $\bar{2}^3 = \bar{8} \neq \bar{1}$ volgt orde $(\bar{2}) = 9$, dus $\bar{2}$ brengt de groep voort. Verder $\bar{2}.\bar{5} = \overline{10} = \bar{1}$ dus $\bar{5} = \bar{2}^8$. Zij $\bar{3} = \bar{2}^x$, met $0 \leq x < 9$. Als $x = 0, 1, 2, 3$ of 8, dan $\bar{3} = \bar{1}, \bar{2}, \bar{4}, \bar{8}$ of $\bar{5}$, respectievelijk, een tegenspraak. Als $x = 4, 5$ of 6 dan $\bar{9} = \bar{2}^{2x} = \bar{5}, \bar{2}$ of $\bar{8}$, weer een tegenspraak. Tenslotte levert ook $x = 7$ een tegenspraak: $\bar{6} = \bar{2}^{x+1} = \bar{5}$. □

Meer non-existentiestellingen van dit ype vindt men in [7]; hier worden ook negacyklische codes beschouwd. Perfecte codes van orde 1 met r = 4, 5, 8, 9 of 10 bestaan niet; voor r = 6 of 7 worden perfecte cyklische 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 [8] en [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

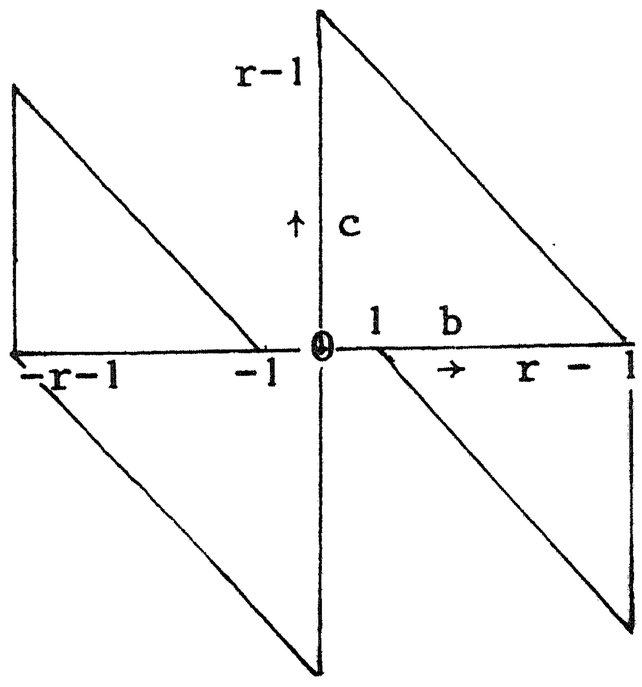
$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)}$$

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 $\in$ Z, $|b|$, $|c| < r$. We noemen het paar (b,c) *toegelaten* als geldt:

als b c $\geq$ 0 dan $|b+c| < r$,

als b c $<$ 0 dan $|b| > |c|$.



Het toegelaten gebied.

Een schrijfwijze

$$x = \sum_{i=0}^{\infty} c_i r^i \tag{3.1}$$

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 $c_{i+1} . c_i = 0$ 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".

STELLING (3.2) [4]. *Elk geheel getal* x *heeft precies één NAF; bovendien, is* (3.1) *een* NAF *voor* x, *dan*

$$w(x) = \#\{i \mid i \geq 0,\ c_i \neq 0\}$$

Voor een (onnodig lang) bewijs van deze stelling verwijzen we naar [4]. Daar vindt men ook een algoritme om een NAF voor x te berekenen uitgaande van een willekeurige representatie (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:

STELLING (3.3) [4]. *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*

$$x = \sum_{j=0}^{\infty} (a_{j+1} - b_{j+1}) . r^j . \quad \square$$

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 (3.1) een NAF voor x is, dan kan men eenvoudig bewijzen:

STELLING (3.4) [5]. *Zij* $k \in \mathbb{Z}$, $k \geq -1$, *en* $x \in \mathbb{Z}$. *Dan geldt*

$$gr(x) \leq k \iff |x| < \frac{r^{k+2}}{r+1}. \quad \square$$

Vervolgens beschouwen we de analoge stellingen voor het *modulaire* gewicht w_m, met $m = r^n - 1$, $n \geq 2$.

We noemen een representatie

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \bmod m \tag{3.5}$$

met $c_i \in \mathbb{Z}$, $|c_i| < r$ een CNAF (= cyklische NAF) voor x modulo m, als (c_{i+1}, c_i) toegelaten is voor $i = 0,1,\ldots, n-1$, hier is $c_n = c_0$.

STELLING (3.6) [5]. *Elke 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 (3.5) een CNAF voor* x *modulo* m, *dan geldt*

$$w_m(x) = \not\equiv \{i \mid 0 \leq i < n,\ c_i \neq 0\}. \quad \square$$

STELLING (3.7) *Als* $(r+1)x \equiv 0 \not\equiv x$ *mod* m, *dan geldt* $w_m(x) = n$, *behalve als*

$$n \equiv 0 \bmod 2 \text{ en } x \equiv \pm \frac{m}{r+1} \bmod m,$$

in welk geval geldt $w_m(x) = \frac{1}{2} n$. $\square$

We verwijzen naar [5] voor een algoritme om een CNAF van een geheel getal te bepalen.

Stelling (3.4) impliceert gemakkelijk:

STELLING (3.8). *Een geheel getal* x *heeft een CNAF (3.5) met* $c_{n-1} = 0$ *dan en slechts dan als er een* $y \in \mathbb{Z}$ *is met*

$$x \equiv y \ mod\ m,\ |y| \leq \frac{m}{r+1}. \quad \square$$

Heeft x een CNAF (3.5), dan wordt een CNAF voor rx gegeven door

$$rx \equiv \sum_{i=0}^{n-1} c_{i-1} r^i \bmod m, \text{ (indices modulo n)}.$$

Uit stelling (3.6) volgt dus

$$w_m(rx) = w_m(x) \tag{3.9}$$

hetgeen ook direct in te zien is.

Op dezelfde wijze ziet men dat de kopcoefficient 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 (3.8) op $r^j.x$ toe te passen, en men vindt:

STELLING (3.10) [5]. *Voor* $x \in \mathbb{Z}$ *geldt*

$$w_m(x) = \#\{j \mid 0 \leq j < n, \text{ en er is een } y \in \mathbb{Z},$$

$$\frac{m}{r+1} < y \leq \frac{mr}{r+1}, \text{ met } r^j x \equiv y \ mod\ m\} \quad \square$$

4. MANDELBAUM-BARROWS CODES

STELLING (4.1). *Zij* $C \subset \mathbb{Z}/(r^n-1)$ *een cyklische AN-code met voortbrenger* A, *en zij* $B = (r^n-1)/A = \#\ C$. *Dan geldt*

$$\sum_{x \in C} w_m(x) = n.\left(\left[\frac{rB}{r+1}\right] - \left[\frac{B}{r+1}\right]\right).$$

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 coëfficienten ongelijk aan nul van de matrix $(c_{i,x})$ $0 \leq i \leq n-1$, $x \in C$ 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 cyklische 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 (3.8) de kopcoëfficient $c_{n-1,x}$ hiervan ongelijk aan nul dan en slechts dan als er een $y \in \mathbf{Z}$ is met

$$x = (y \bmod r^n-1),\quad \frac{m}{r+1} < y \leq \frac{mr}{r+1}.$$

Schrijven we $x = (AN \bmod r^n-1)$, $0 \leq N < B$, dan betekent dit

$$\frac{B}{r+1} < N \leq \frac{Br}{r+1}$$

Het aantal van zulke N is kennelijk $\left[\frac{Br}{r+1}\right] - \left[\frac{B}{r+1}\right]$.

Het geval dat C een element met twee CNAFs bevat vereist enige extra zorg, die aan de lezer toevertrouwd kan worden. □

De uitdrukking in (4.1) is ongeveer gelijk aan

$$n.\ \#C.\ \frac{r-1}{r+1}.$$

Vergelijk hiermee het analoge resultaat voor cyklische codes over GF(q): is C zo'n code, met woordlengte n, dan

$$\sum_{x \in C} w_H(x) = n.\ \#C.\ \frac{q-1}{q}\quad (w_H = \text{Hamming-gewicht}).$$

De volgende stelling beschrijft de gegeneraliseerde Mandelbaum-Barrows codes, zie [9] voor referenties voor het binaire geval. Een code C heet *equidistant* als $d_m(x,x') = d_m(y,y')$ voor alle $x,x', y,y' \in C$, $x \neq x'$, $y \neq y'$.

STELLING (4.2) [5]. *Zij* B *een priemgetal dat* r *niet deelt, met de eigenschap dat* $(\mathbb{Z}/B)^*$ *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*

$$\frac{n}{B-1}\left(\left[\frac{rB}{r+1}\right] - \left[\frac{B}{r+1}\right]\right).$$

BEWIJS. 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(3.9)). Hieruit blijkt dat alle elementen van C ongelijk nul hetzelfde modulaire gewicht hebben, dus C is equidistant. De afstand berekenen we met (4.1):

$$w_m(A) = \frac{1}{B-1} \sum_{x \in C,\ x \neq 0} w_m(x) = \frac{n}{B-1}\left(\left[\frac{rB}{r+1}\right] - \left[\frac{B}{r+1}\right]\right). \quad \square$$

We merken op dat de woordlengte n in (4.2) minstens $\frac{B-1}{2}$ 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 [1, p. 48/49]. Dit zijn cyklische codes met woordlengte q^k-1 waarvan het "check polynomisl" h(x) een primitief irreducibel polynoom van graad m is (*primitief* betekent dat de nulpunten van h(x) multiplicatieve orde $q^k - 1$ hebben). Deze codes zijn equidistant met afstand $(q-1).\ q^{k-1}$.

Er bestaan generalisaties van (4.2) voor het geval B een natuurlijk getal, relatief priem met r, is, met de eigenschap dat de groep van eenheden $(\mathbb{Z}/B)^*$ van de ring $\mathbb{Z}/B$ 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 ($\simeq \mathbb{Z}/B$) afhangt. Door (4.1) op subcodes van C toe te passen kan men dan met Moebius-inversie de gewichtsenumerator van C opstellen; vergelijk [13] 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 cyklische AN-code $C \subset \mathbb{Z}/(r^n-1)$ kan bepalen. Zij A de voortbrenger, en $AB = r^n - 1 = m$. Met H geven de de ondergroep van $(\mathbb{Z}/B)^*$ aan die wordt voortgebracht door de restklassen van r en −1. De groep H werkt op $\mathbb{Z}/B$ door vermenigvuldiging; voor $N \in \mathbb{Z}$ geven we de baan van (N mod B) onder H met H.N aan:

$$H.N = \{\pm r^j N \bmod B \mid j = 0,1,2,\ldots\} \subset \mathbb{Z}/B.$$

STELLING (4.3). *Het modulaire gewicht* $w_m(AN)$ *hangt alleen van de baan* H.N *af; er geldt*

$$w_m(AN) = n.\frac{\#(HN \cap \{y \bmod B \mid \frac{B}{r+1} < y \leq \frac{Br}{r+1}\})}{\#\ HN}$$

BEWIJS. Dit is in essentie een herformulering van (3.10). □

VOORBEELD: r = 2, B = 109, n = 36. De groep $H \subset (\mathbb{Z}/109)^*$ heeft orde 36, en $\mathbb{Z}/109$ valt onder H in vier banen uiteen:

$$H.0,\ H.1,\ H.3,\ H.9.$$

Doorsnijdt men deze banen met $\{y \bmod 109 \mid \frac{109}{3} < y \leq \frac{2.109}{3}\} =$
$= \{37, 38, \ldots, 72\}$, dan vindt men

$$\emptyset,\ \{\pm 38, \pm 41, \pm 43, \pm 45, \pm 46, \pm 46, \pm 54\},$$
$$\{\pm 40, \pm 48, \pm 51, \pm 52, \pm 53\},\ \{\pm 37, \pm 39, \pm 42, \pm 44, \pm 47, \pm 49, \pm 50\},$$

dus de AN-code $C \subset \mathbb{Z}/(2^{36}-1)$ voortgebracht door $A = (2^{36}-1)/109$ heeft één element met gewricht 0 (het nul-element van C); 36 elementen met gewricht 12; 36 elementen met gewricht 10; en 36 elementen met gewricht 14. Er volgt $d_{min}(C) = 10$. Zie [9, §3.6] voor meer voorbeelden.

In [12] vindt men een manier om uit (4.3) een ondergrens voor $d_{min}(C)$ af te leiden.

5. CHEN-CHIEN-LIU CODES.

De reeds vaker vermelde analogie met cyklische codes over een eindig lichaam heeft voedsel gegeven aan de gedachte dat er een klasse AN-codes bestaat die correspondeert met de klasse der BCH-codes. Voor een onbewezen vermoeden hierover zie men [9, §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 [3]:

STELLING (5.1). *Laten* a *en* b *twee relatief prieme getallen* ≥ 2 *zijn. Dan heeft de cyklische 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).

Het bewijs van (5.1) geven we hier niet. Dat de minimumafstand hoogstens 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 echter minder evident. Een aanzet tot bewijs in het binaire geval vindt men in [3, §4]; de daar gegeven argumenten zijn evenwel niet volledig.

De analogie met BCH-codes is als volgt. Is q een priemmacht, en zijn a, b twee relatief prieme 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 [11, §9.1] impliceert dan dat de code

$$(g(x)) \subset GF(q)[x]/(x^{ab}-1)$$

minimuum-afstand ≥ 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 (5.1) bewezen wordt.

LITERATUUR.

[1] I.F. BLAKE, R.C. MULLIN, *The mathematical theory of Coding, Academic Press 1975.*

[2] I.M. BOYARINOV, G.A. KABATYANSKY, *On perfect arithmetic AN-codes*, Int. Symp. Inf. Theory Talin, SSSR, 1973, pp. 41-43 (Russisch).

[3] C.L. CHEN, R.T. CHIEN & C.K. LIU, *On the binary representation form of certain integers*. SIAM J. Appl. Math. 26 (1974), 285-293.

[4] W.E. CLARK & J.J. LIANG, *On arithmetic weight for a general radix representation of integers*, IEEE Trans. Information Theory IT-19 (1973), 823-826.

[5] W. E. CLARK & J.J. LIANG, *On modular weight and cyclic nonadjacent forms for arithmetic codes*, IEEE Trans. Information Theory IT-20 (1974), 767-770.

[6]. M. GOTO, *A note on decimal perfect AN-codes*, the Research Reports of Gifu University 25 (1975), 24-26.

[7] M. GOTO & T. FUKUMURA, *Perfect nonbinary AN codes with distance three*, Information and Control 27 (1975), 336-348.

[8] V.M. GRITSENKO, *Nonbinary arithmetic correcting codes*, Problems of Information transmission 5 (1969), 15-22.

[9] J.L. MASSEY & 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.

[10] P.G. NEUMANN & T.R.N. RAO, *Error-correcting codes for byte-organized arithmetic processors*, IEEE trans. Computers C-24 (1975), 226-232.

[11] W.W. PETERSON & E.J. WELDON, JR., *Error-correcting codes*, Second edition the MIT Press, 1972.

[12]. G. SEGUIN, *Bounds for certain cyclic AN-codes*, Information and Control 23 (1973), 41-47.

[13] N.T. TSAO-WU & S.-H. CHANG, *On the evaluation of minimum distance of binary arithmetic cyclic codes*, IEEE trans. Information theory IT-15 (1969), 628-631.