Reed-Muller codes en de stelling van Chevalley

Hoofdstuk VI

REED-MULLER CODES EN DE STELLING VAN CHEVALLEY

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

6.1. VOORBEREIDINGEN

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

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

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

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

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

BEWIJS: Zoals bekend is

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

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

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

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

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

Hieruit volgt het gestelde met volledige inductie. □

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

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

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

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

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

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

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

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

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

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

en evenzo daar $i_0 \geq 2^n$

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

waaruit het gestelde volgt.

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

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

(6.1.3) DEFINITIES:

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

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

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

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

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

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

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

dan is

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

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

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

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

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

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

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

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

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

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

BEWIJS:

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

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

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

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

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

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

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

6.2. BINAIRE REED-MULLER CODES

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

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

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

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

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

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

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

Uit (a) en (b) volgt het gestelde. □

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

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

BEWIJS: Zij $\underline{f} = \sum_{j=0}^{m-1} f_j \underline{e}_j$ de karakteristieke functie van A.
Volgens (6.1.3) (iv) en (6.1.5) (iii) is

$$\underline{e}_j = \sum_{s=0}^{m} \sum_{\substack{(i_1,\ldots,i_s) \\ j\in C(i_1,\ldots i_s)}} \underline{v}_{i_1}\underline{v}_{i_2}\cdots\underline{v}_{i_s}$$

zodat

$$\underline{f} = \sum_{s=0}^{m} \sum_{(i_1,i_2,\ldots,i_s)} \left(\sum_{j\in C(i_1,\ldots,i_s)} f_j \right) \underline{v}_{i_1}\underline{v}_{i_2}\cdots\underline{v}_{i_s}.$$

De binnenste som telt het aantal punten uit de doorsnede van A met de s-dimensionale affiene deelruimte

$$L := \{\underline{x}_j \in AG(m,2) \mid j \in C(i_1,\ldots,i_s)\}.$$

Voor $s > m-\ell$ is $L \cap A$ leeg of een affiene deelruimte van positieve dimensie. In beide gevallen is $|L \cap A|$ even, d.w.z. de coefficient van $\underline{v}_{i_1}\underline{v}_{i_2}\cdots\underline{v}_{i_s}$ is 0. □

(6.2.5) STELLING: *Binaire* RM-*codes zijn equivalent met verlengde cyclische codes.*

BEWIJS: Laat uit E de 0-de kolom weg. De overige kolommen zijn op te vatten als de elementen $\neq 0$ uit $GF(2^m)$. Dit is t.a.v. vermenigvuldiging een cyclische groep met voortbrenger ξ, een primitief element van $GF(2^m)$. De afbeelding $\alpha : GF(2^m) \to GF(2^m)$ gedefinieerd door $\alpha(x) = \xi x$ is kennelijk een niet-singuliere lineaire afbeelding van AG(m,2) in zichzelf. Verder is α, opgevat als permutatie van $AG(m,2)\setminus\{\underline{0}\}$ van de orde n-1. Iedere affiene deelruimte van AG(m,2) wordt door α afgebeeld op een affiene deelruimte van dezelfde dimensie. Het gestelde volgt nu uit (6.1.5) (i), (6.2.1) en (6.2.4). □

(6.2.6) STELLING: *De groep* G *van affiene transformaties van* AG(m,2) *is een groep van automorfismen van elke* RM-*code van lengte* 2^m.

BEWIJS. De transformaties van AG(m,2) komen overeen met permutaties van de symbolen van codewoorden. Evenals in (6.2.5) volgt het gestelde onmiddelijk uit het feit dat $(a_0,a_1,\ldots,a_{n-1})$ dan en slechts dan een codewoord van een RM-code van lengte 2^m en orde r is als het een lineaire combinatie is van karakteristieke functies van affiene deelruimten van dimensie $\geq m-r$. Deze zijn invariant onder G. □

We merken nog op dat G een drievoudig transitieve groep is; dat wil zeggen, dat ieder drietal punten in ieder ander drietal punten wordt overgevoerd door een element van G [omdat over een lichaam van karakteristiek 2 twee vectoren lineair onafhankelijk zijn zodra ze verschillend en ongelijk nul zijn].

We gaan nog kort in op een decodeerprocedure die voor deze codes gebruikt wordt. Beschouw een RM-code C van lengte 2^m en orde r. Volgens (6.2.3) en (6.2.4) is de karakteristieke functie van een (r+1)-dimensionale affiene deelruimte van AG(m,2) een parity-check vector voor C. Voor iedere r-dimensionale affiene deelruimte A van AG(m,2) zijn er $2^{m-r}-1$ verschillende (r+1)-dimensionale affiene deelruimten van AG(m,2) die A bevatten. Ieder punt niet in A ligt in precies één van deze deelruimten. Elk van deze (r+1)-dimensionale deelruimten bestaat uit de $|A|$ punten van A en evenveel andere

punten. Is a de som van de coordinaten van een codewoord op de plaatsen van A dan is de som van de coordinaten op het andere $|A|$-tal plaatsen blijkbaar ook a. We berekenen nu de uitkomsten van de $2^{m-r}-1$ parity check vergelijkingen. Stel dat het aantal fouten in een ontvangen woord $\leq 2^{m-r-1}-1$ is. Stel nu dat t van de parity-check vergelijkingen een 1 geven.
Er zijn 2 verklaringen te geven:

(i) dat dit is veroorzaakt door een oneven aantal fouten op de plaatsen van A en $2^{m-r}-1-t$ keer gecompenseerd wordt door een oneven aantal fouten op de andere $|A|$ plaatsen van zo'n parity check vergelijking.

(ii) dat op de plaatsen van A geen fout (of een even aantal) is gemaakt maar dat in t van de parity check vergelijkingen op de andere helft een oneven aantal fouten is gemaakt. In geval (i) is het aantal fouten $\geq 2^{m-r}-t$ en in geval (ii) is het $\geq t$. Precies als bij de eerder behandelde drempeldecodering (§ 3.5) is de waarde van t bepalend voor de keuze tussen (i) en (ii). Op deze manier is voor iedere r-dimensionale affiene deelruimte A uit te maken of het ontvangen woord een oneven aantal fouten op de plaatsen van A bevat. Door een soort inductie procédé kunnen we in een aantal analoge stappen de fouten localiseren. Dit proces heet "*multistep majority decoding*".

6.3. FUNCTIES EN POLYNOMEN OVER EINDIGE LICHAMEN

In het vervolg van dit hoofdstuk zullen we ons bezig houden met de generalisatie van de hiervoor voor q = 2 beschouwde Reed-Muller codes voor willekeurige q. Hierbij zullen we een tweetal beschrijvingen van de gegeneraliseerde Reed-Muller codes tegenkomen. De eerste beschrijving sluit aan op de meetkundige behandeling van het geval q = 2 in § 6.2. Bij de tweede beschrijving staat het feit dat de codes verlengde cyclische codes zijn centraal. Verder zal blijken dat de bepaling van het minimale gewicht van de gegeneraliseerde Reed-Muller codes ons in staat stelt een klassieke stelling uit de algebra nl. de stelling van CHEVALLEY (1936) en een verscherping: de stelling van WARNING (1936) als gevolg mee te nemen.

Voor een eindig lichaam k kan een polynoom f in k[X] alle elementen van k als nulpunt hebben zonder dat alle coefficienten van f ook 0 zijn; zo geldt voor iedere $x \in \mathbb{F}_q$ dat $x^q-x = 0$ hetgeen impliceert dat het polynoom $X^q-X \in \mathbb{F}_q[X]$ een voorbeeld van zo'n polynoom is. We houden ons in deze paragraaf bezig met een generalisatie van deze situatie voor polynomen in

meer veranderlijken.

Zij V een m-dimensionale vectorruimte over $k = \mathbb{F}_q$ zodat $V \cong (k)^m$. Polynomen in $k[X_1,\ldots,X_m]$ laten zich op natuurlijke wijze opvatten als functies van V in k; bovendien is deze voor de hand liggende afbeelding E: $k[X_1,\ldots,X_m] \to k^V$ een homomorfisme van ringen. De kern J van deze afbeelding is een ideaal in $k[X_1,\ldots,X_m]$. Kennelijk geldt $f \in J$ als en alleen als E(f) identiek nul op V is.

Voorbeelden van functies in J zijn de polynomen $X_i^q - X_i$ $(i=1,\ldots,m)$. Deze functies brengen een ideaal voort dat we met I zullen aanduiden. Het is duidelijk dat modulo I ieder polynoom f in $k[X_1,\ldots,X_m]$ zich laat schrijven als een polynoom f^* dat de eigenschap heeft dat voor iedere i en ieder in f^* optredend monoom $X_1^{d_1}\ldots X_m^{d_m}$ de graad $d_i \leq q-1$ is. Een dergelijk polynoom zullen we gereduceerd noemen en de verzameling gereduceerde polynomen duiden we aan met R.

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

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:

$$f = f_0 + f_1X_m + f_2X_m^2 + \ldots + f_{q-1}X_m^{q-1},$$

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

Voor vaste elementen $\alpha_1,\ldots,\alpha_{m-1} \in k$ geldt dat $f(\alpha_1,\ldots,\alpha_{m-1},X_m) \in k[X_m]$ een gereduceerd polynoom is dat overal nul is. Dientengevolge geldt $f_j(\alpha_1,\ldots,\alpha_{m-1}) = 0$ voor $j = 0,\ldots,q-1$. Aangezien $\alpha_1,\ldots,\alpha_{m-1}$ willekeurig waren gekozen volgt nu met inductie dat alle f_j identiek nul zijn.

Het is duidelijk dat $I \subset J$. Beschouw derhalve het quotient J/I. Iedere restklasse in dit quotient bezit een gereduceerde representant maar dat kan alleen maar het nul polynoom zijn daar $J \cap R = \{0\}$. De derde bewering in de stelling volgt nu rechtstreeks. □

(6.3.2) 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 met coefficient 1 bedraagt q^m en dit is tevens de

dimensie van k^V. Omdat E als kern J heeft moet E dus wel surjectief zijn.

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

$$f_{a_i}(a) = \begin{cases} 1 & \text{als } a = a_i, \\ 0 & \text{anders,} \end{cases}$$

(gebruik hierbij dat het product van alle elementen in $\mathbb{F}_q^*$ gelijk -1 is). Voor $\underline{a} = (a_1,\ldots,a_m) \in V$ definiëren we

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

Kennelijk geldt

$$f_{\underline{a}}(\underline{b}) = \begin{cases} 1 & \text{als } \underline{a} = \underline{b}, \\ 0 & \text{anders.} \end{cases}$$

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

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

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

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

6.4. DE STELLING VAN CHEVALLEY EN GENERALISATIES

Aangezien iedere functie beschreven wordt door een polynoom is in het

algemeen niets te zeggen over het aantal nulpunten van een polynoom. Kijken we naar gereduceerde polynomen zonder constante term dan weten we dat de oorsprong van V een nulpunt is. We vragen ons af of dit nulpunt uniek is.

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

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

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. Indien we G reduceren (mod I) tot G^* geldt graad $(G^*) \leq$ graad $(G) = (q-1).d$. Maar volgens (6.3.1) is $G^* = H$ zodat graad $(H) \leq (q-1).d$. Merk nu op dat de hoogste graadsterm van $f_{\underline{a}}$, zijnde $(-1)^m X_1^{q-1} \ldots X_m^{q-1}$, van graad $m(q-1)$ is en niet van $\underline{a}$ afhangt. Wil in H geen term van deze graad voorkomen dan moet het aantal polynomen $f_{\underline{a}}$ dat wordt opgeteld om H te vormen een veelvoud van p zijn, i.e. $|W| \equiv 0 \pmod p$. □

(6.4.2) GENERALISATIE [WARNING]: Onder de bovengenoemde aannamen en met gebruikmaking der notaties uit het bewijs geldt $|W| \geq q^{m-d}$.

Deze generalisatie zal bewezen worden als gevolg van de grens voor het minimale gewicht voor de nog in te voeren gegeneraliseerde Reed-Muller codes.

Een generalisatie die zich uitspreekt over de deelbaarheids eigenschappen van het aantal nulpunten is de volgende stelling van AX (1964).

(6.4.3) STELLING [AX]: *Zij* f *een polynoom in* $k[X_1,\ldots,X_m]$ *van de graad* $d < m$. *Stel* $b = [m/d]$ *en zij* W *de verz. nulpunten van* f *in* k^m. *Dan geldt* $|W| \equiv 0 \pmod{q^b}$.

Van deze generalisatie zullen we in dit hoofdstuk geen bewijs geven.

6.5. DE GEGENERALISEERDE REED-MULLER CODES

Zij $V \simeq (k^m)$, $k = \mathbb{F}_q$. Bij een gegeven functie $f \in k^V$ kunnen we de tabel van waarden van f vormen, onder weglating der argumenten die wij op een of andere vaste wijze geënumereerd achten te zijn. Dit levert een afbeelding $S: k^V \to (k)^{q^m}$.

(6.5.1) DEFINITIE: De (gegeneraliseerde) *Reed-Muller code* RM(m,v,q) is het beeld onder de afbeelding S∘E van de verz. van polynomen

$$\{f \in k[X_1,\ldots,X_m] \mid \text{graad } (f) \leq v\} \text{ waarbij } k = \mathbb{F}_q.$$

Om deze definitie goed te praten moeten we laten zien dat de code niet afhangt van de (impliciete) basiskeuzen gemaakt in de definities van E en S. Wat betreft S is het duidelijk dat een omnummering van de elementen van V leidt tot een equivalente code in de zin als beschreven in (3.2.3). Minder duidelijk is het wat de invloed is van de keuze van de basis die ten grondslag ligt aan de isomorfie $V \cong k^m$. Immers een andere keuze van een basis impliceert dat de monomen $X_1,\ldots,X_m$ worden afgebeeld op andere functies in k^V. De *graad* van een polynoom wordt hierdoor echter niet beinvloed:

(6.5.2) LEMMA. *Zij* $\sigma: V \to V$ *een automorfisme en zij* $\underline{a} \in V$ *een vast element. Beschouw de affiene afbeelding* $\tau = \sigma + \underline{a}: V \to V$ *gedefiniëerd door* $\tau(\underline{x}) = \sigma(\underline{x}) + \underline{a}$. *Deze induceert een isomorfisme* $\tau^*: k^V \to k^V$ *door* $\tau^*(h) = h\circ\tau$. *Dan geldt dat het isomorfisme* $\tau^{**}: R \to R$ *gedefiniëerd door* $\tau^{**} = E^{-1}\circ\tau^*\circ E$ *de graad respecteert.*

BEWIJS: Uitschrijven leert dat τ^{**} de vorm heeft:

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

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

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

Een lineaire code is equivalent met een verlengde cyclische code als hij invariant is onder een permutatie van de plaatsen die een plaats vast laat, en de overige posities cyclisch verwisselt, terwijl bovendien alle woorden in de code de eigenschap hebben dat de som der coëfficienten gelijk nul is.

(6.5.4) STELLING: *Als* $v < m(q-1)$ *dan is de code* RM(m,v,q) *equivalent met een verlengde cyclische code.*

BEWIJS: Zij α een primitieve wortel van $\mathbb{F}_{q^m} \supset \mathbb{F}_q$. $\mathbb{F}_{q^m}$ is als $\mathbb{F}_q$-lineaire ruimte isomorf met $(\mathbb{F}_q)^m$. Bovendien is vermenigvuldigen met α een $\mathbb{F}_q$-lineair automorfisme van $\mathbb{F}_{q^m}$. Onder dit automorfisme blijft het element 0 op zijn plaats terwijl de elementen van $\mathbb{F}_{q^m}^*$ cyclisch worden verwisseld. Dit laat zien dat er een affiene transformatie van V bestaat met de gewenste vorm van de banen.

Om de tweede voorwaarde te controleren moeten we de som bepalen van de coordinaten in S(E(f)). Deze som $\sum$ is:

$$\sum = \sum_{\underline{a} \in (k)^m} f(\underline{a}) = \sum_{g \text{ monoom in } f} \text{coeff. van } g. \left(\sum_{\underline{a} \in (k)^m} g(\underline{a}) \right).$$

Schrijf een term g als:

$g = \alpha_g X_1^{d_{1g}} \cdot \ldots \cdot X_m^{d_{mg}}$. Dan vinden we

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

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

$$\sum_{x \in \mathbb{F}_q} x^j = \begin{cases} -1 & \text{als} \quad j > 0 \text{ en } j \equiv 0 \pmod{q-1}, \\ 0 & \text{anders,} \end{cases}$$

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

(6.5.5) OPMERKING. Voor v = 0 is R(m,v,q) de repetitie code van lengte q^m. Voor v = 1 bestaat R(m,v,q) uit de "tabellen" van alle affiene functies op V. Omdat een niet identiek nul zijnde affiene functie ten hoogste q^{m-1} nulpunten heeft bedraagt het minimale gewicht in dit geval $(q-1)q^{m-1}$. Voor v = (q-1)m beslaat R(m,v,q) de gehele ruimte $(k)^{q^m}$.

Voor willekeurige v < (q-1)m kunnen we schrijven

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

Beschouw vervolgens het polynoom

$$f = (1-X_1^{q-1})\ldots(1-X_r^{q-1}) \prod_{0<i\leq s} (X_{r+1} - \alpha_i)$$

(waarbij de α_i verschillende elementen van $\mathbb{F}_q$ zijn). Dan zien we dat dit polynoom graad v heeft. Een niet-nulpunt van f heeft de vorm

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

$$\text{en} \qquad a_{r+1} \neq \alpha_i \quad \text{voor } 0 < i \leq s.$$

Het aantal niet-nulpunten van f is derhalve

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

Dit getal is dus een bovengrens voor het minimale gewicht in RM(m,v,q). De oplettende lezer zal wellicht opmerken dat deze grens exact is voor v = 0,1 en v = m(q-1). Dat dit geen toeval is blijkt uit de volgende stelling (zie ook (6.2.2)).

(6.5.6) STELLING. (= Reed-Muller grens). *Het minimale gewicht van* RM(m,v,q) *is* $q^{m-r-1}(q-s)$.

We zullen deze stelling in § 6.6 bewijzen. Om enig inzicht te krijgen

in de algebraïsche achtergronden beschouwen we het geval q = 2. Omdat q - 1 = 1 zijn de gereduceerde monomen lineair in iedere optredende variabele. De Reed-Muller grens voor R(m,v,2) levert 2^{m-v}. Bij een polynoom f beschouwen we het polynoom g = 1 + f dat nul is waar f geen nulpunt heeft en omgekeerd. Derhalve is het gewicht van S(f) gelijk aan het aantal nulpunten van g. Bovendien hebben f en g dezelfde graad.

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

Algemeen geldt:

(6.5.7) STELLING. *De stelling van Warning is een direct gevolg van de Reed-Muller grens.*

BEWIJS: Zij $g_1,\ldots,g_s$ een stelsel gereduceerde polynomen met graden d_i waarbij $\Sigma d_i = d < m$. Beschouw het polynoom f^* dat ontstaat door het product $f = \prod_{i=1}^{s} (g_i^{q-1}-1)$ te reduceren. Dan geldt

$$\deg(f^*) \leq \deg(f) = (q-1)d < m(q-1).$$

Bovendien geldt

$$(f(\underline{x}) \neq 0) \Leftrightarrow (g_1(\underline{x}) = g_2(\underline{x}) = \ldots = g_s(\underline{x}) = 0).$$

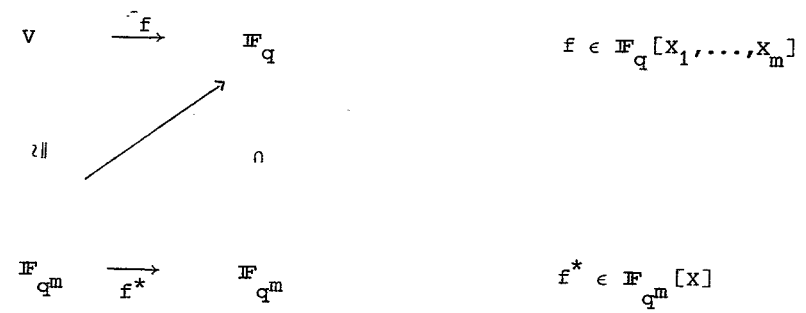
Aannemende dat de g_i ten minste één gemeenschappelijk nulpunt bezitten leiden we af dat f niet identiek 0 is. Volgens de Reed-Muller grens bedraagt het gewicht van het woord w:= S(E(f)) (N.B. $w \neq \underline{0}$) dat bevat is in RM(m,d(q-1),q) ten minste q^{m-d}. Dit is de gevraagde ondergrens voor het aantal gemeenschappelijke nulpunten der g_i. □

6.6. BEWIJS DER REED-MULLER GRENS

Het bewijs van de Reed-Muller grens is triviaal indien m = 1. De polynomen zijn in dit geval polynomen in één veranderlijke zodat het aantal nulpunten begrensd wordt door de graad van het polynoom. Het aantal niet-nulpunten van een niet-nul polynoom van de graad $\leq v \leq q - 1$ is ten minste q - v hetgeen precies is wat de Reed-Muller grens verlangt.

Het algemene geval berust op de volgende truc. Omdat $(\mathbb{F}_q)^m$ en $\mathbb{F}_{q^m}$

als $\mathbb{F}_q$-vectorruimte isomorf zijn kunnen we de functies in $\mathbb{F}_q^{(\mathbb{F}_q)^m}$ opvatten als functies in $\mathbb{F}_q^{\mathbb{F}_{q^m}}$ die zich laten weergeven door polynomen in één variabele en dan functies beschrijven in $\mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$. We moeten nauwkeurig nagaan wat er met het begrip graad gebeurt; indien we de graad van de te genereren polynomen in $\mathbb{F}_{q^m}[X]$ "laag" kunnen houden levert dit een ondergrens op voor het minimale gewicht. Zie ook het volgende diagram:



of het hiermee samenhangende diagram:

$$E^{-1}(S^{-1}(RM(m,v,q))) \xrightarrow{\ *\ } A = \{f^* \mid f \in B\}$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad \cap$$

$$B := \{f \in \mathbb{F}_q[X_1,\ldots,X_m] \mid \text{graad } (f) \leq v\} \qquad \cap$$

$$\cap$$

$$\mathbb{F}_q[X_1,\ldots,X_m] \xrightarrow{\ *\ } \mathbb{F}_{q^m}[X].$$

Om de $\mathbb{F}_q$-lineaire deelruimte A in $\mathbb{F}_{q^m}[X]$ te bepalen gebruiken we de volgende strategie. Eerst bepalen we welke elementen in $\mathbb{F}_{q^m}[X]$ optreden als beeld van een $\mathbb{F}_q$-lineaire functie. Daarna vormen we producten van deze functies opgebouwd uit ten hoogste v termen. Lineaire combinaties daarvan vormen de verzameling A.

Tijdens het bewijs zal blijken dat het voor het bepalen van de maximale graad van een element in A niet nodig is gebruik te maken van het feit dat functies $f^* \in \mathbb{F}_{q^m}[X]$ die afkomstig zijn van $\mathbb{F}_q[X_1,\ldots,X_m]$ bij substitutie van elementen in $\mathbb{F}_{q^m}$ alleen maar waarden in $\mathbb{F}_q$ aannemen.

(6.6.1) STAP 1: *Bepaling van $\mathbb{F}_q$-lineaire functies in $\mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$ (zonder constante term).*

Deze functies laten zich beschrijven door $m \times m$ matrices met elementen in $\mathbb{F}_q$ (vat $\mathbb{F}_{q^m}$ op als $(\mathbb{F}_q)^m$). Het aantal van deze functies bedraagt dus $q^{(m^2)}$.

We kunnen deze verzameling dus karakteriseren door een even grote verzameling van $\mathbb{F}_q$-lineaire functies te verzinnen.

Zij $\underline{\beta} = (\beta_0,\ldots,\beta_{m-1}) \in (\mathbb{F}_{q^m})^m$ en beschouw de functie $f_{\underline{\beta}}$ gedefinieerd door $\alpha \to \sum_{i=0}^{m-1} \beta_i \cdot \alpha^{q^i}$ (waarbij α een primitief element van $\mathbb{F}_{q^m}$ is). Men verifieert eenvoudig dat $f_{\underline{\beta}}$ $\mathbb{F}_q$-lineair is. Bovendien geldt op grond van het feit dat de $f_{\underline{\beta}}$ gereduceerd zijn (als polynomen in $\mathbb{F}_{q^m}[X]$) dat $f_{\underline{\beta}} = f_{\underline{\beta}'}$, d.e.s.d. als $\underline{\beta} = \underline{\beta}'$. Tellen van dimensies leert dat hiermede alle $\mathbb{F}_q$-lineaire functies gevonden zijn. □

(6.6.2) 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 $0 \le i \le m-2$ en $\beta_{m-1}^q = \beta_0$.

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

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

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

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

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

BEWIJS: (i) is vanzelfsprekend en (ii) drukt uit dat het verwerken van een overdracht (carry) de cijfersom met $(q-1)$ doet dalen. Omdat het reduceren van m modulo (q^t-1) neerkomt op het herhaald optellen van blokken van t opeenvolgende cijfers in het q-tallig stelsel is (iii) een rechtstreeks gevolg van (i) en (ii). □

(6.6.4) STAP 2: *Bepaling van* A.

De $\mathbb{F}_q$-lineaire polynomen in $\mathbb{F}_{q^m}[X]$ hebben de eigenschap dat ieder optredend monoom een exponent heeft met cijfersom ≤ 1. Vormen we van deze polynomen een v-voudig product dan heeft de exponent van ieder in dit product optredend monoom cijfersom $\le v$. Omgekeerd kan ieder zodanig monoom op deze wijze gevormd worden.

(6.6.5) GEVOLG:

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

(6.6.6) STAP 3: *Bepaling van de maximale graad van een element in* A.

Op grond van het voorafgaande hoeven we alleen maar de maximale exponent met cijfersom ≤ v te bepalen. Schrijven we als tevoren $v = r.(q-1) + s$, $0 \le s \le q-1$, dan zien we gemakkelijk in dat deze exponent zich laat schrijven als

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

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

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

Zij graad (f) ≤ v dan geldt graad $(f^*) \le q^n - (q-s).q^{m-r-1}$. Dientengevolge heeft f^* hoogstens $q^n - (q-s).q^{m-r-1}$ nulpunten en tan minste $(q-s).q^{m-r-1}$ niet-nulpunten. Gezien de aanwezigheid van woorden met precies dit gewicht is de Reed-Muller grens hiermee bewezen. □

(6.6.8) GEVOLG 2 [*dimensie Reed-Muller code*]. Uit de bovenstaande beschrijving blijkt direct dat de volledige verzameling

$$A^* = \{f \mid f = \sum_{\substack{i<q^m \\ c_q(i)\le v}} \beta_i X^i\}$$

over $\mathbb{F}_{q^m}$ de dimensie $u := |\{j \mid 0 \le j < q^m \text{ en } c_q(j) \le v\}|$ heeft. In feite zijn we geinteresseerd in de dimensie van A over $\mathbb{F}_q$. Deze twee dimensies zijn echter gelijk. Dit kan men ondermeer controleren door na te gaan hoe de eis $f^q \equiv f \pmod{X^q - X}$ de keuzevrijheid der β_i beperkt: gebruikmakende van de conditie $\beta_i^q = \beta_{iq}$ en rekening houdende met het mogelijk optreden van tussenlichamen tussen $\mathbb{F}_q$ en $\mathbb{F}_{q^m}$ ingeval $iq^\ell \equiv i$ voor $\ell < m$ (er is niet gegeven dat $(m, q^m-1) = 1$) leidt men af dat deze congruentie-eis de multiplicatieve factor m precies opheft. Ook kan men gebruik maken van het (niet hier bewezen) feit dat

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

Tenslotte kan men rechtstreeks (door de exponenten in een monoom

$x_1^{e_1} \cdot \ldots \cdot x_m^{e_m}$ te lezen als een q-tallig getal) tot hetzelfde inzicht komen.

(6.6.9) OPMERKING: Men kan zich afvragen of de aangegeven woorden van minimaal gewicht (modulo symmetrie onder de werking van $Gl(\mathbb{F}_q,m)$) de enige woorden van minimaal gewicht zijn. Dit is inderdaad het geval zoals bewezen door DELSARTE, GOETHALS & MacWILLIAMS (1970). Het door hun aangegeven bewijs is te uitgebreid om op deze plaats te worden behandeld. Voor het speciale geval dat s = 0 is het resultaat door Peterson bewezen onder gebruikmaking van genererende functies. Het ziet er niet naar uit dat het bewijs van Delsarte c.s., dat wezenlijk gebruik maakt van de affien-meetkundige structuur van $(\mathbb{F}_q)^m$ zich laat vereenvoudigen door de hierboven beschreven methode berustende op de identificatie van $(\mathbb{F}_q)^m$ en $\mathbb{F}_{q^m}$.

6.7. ALTERNATIEVE BESCHRIJVING DER REED-MULLER CODE

We beschouwen als tevoren de code RM(m,v,q) met $v < m(q-1)$. Zij α een element van $\mathbb{F}_{q^m}$. Zoals we eerder zagen gedraagt de functie $f_\alpha = 1 - (X-\alpha)^{q^m-1}$ zich als de karakteristieke functie van het element α. Voor willekeurige functies $f \in \mathbb{F}_{q^m}^{\mathbb{F}_{q^m}}$ kunnen we dus schrijven

$$f = \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha).f_\alpha = \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha).(1-(X-\alpha)^{q^m-1}).$$

Deze som laat zich als volgt uitwerken:

$$(X-\alpha)^{q^m-1} = \frac{X^{q^m} - \alpha^{q^m}}{X - \alpha} = \sum_{j=0}^{q^m-1} X^j \alpha^{q^m-1-j}.$$

Zodat

$$f = \sum_{j=0}^{q^m-1} \left(\sum_{\alpha\in\mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j + \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha) =$$

$$= \sum_{j=1}^{q^m-1} \left(\sum_{\alpha\in\mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j - \sum_{\alpha\in\mathbb{F}_{q^m}} f(\alpha)(\alpha^{q^m-1} - 1) =$$

$$= \sum_{j=1}^{q^m-1} \left(\sum_{\alpha \in \mathbb{F}_{q^m}} - f(\alpha) \cdot \alpha^{q^m-1-j} \right) X^j + f(0).$$

Stel nu dat $f \in A$, d.w.z. de exponenten van in f optredende monomen hebben som $\leq v$. Dan geldt

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

Omdat $q^m - 1$ uitgeschreven in het q-tallig stelsel er als volgt uit ziet:

$$\underbrace{\underline{q-1} \quad \underline{q-1} \quad \cdots \quad \underline{q-1}}_{m}$$

controleert men eenvoudig dat voor $0 \leq j \leq q^{m-1}$ geldt

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

We vinden dus

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

Als bijzonder geval geeft dit:

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

wat we reeds hebben opgemerkt bij het bewijs dat RM(m,v,q) equivalent is met een verlengde cyclische code (6.5.4).

Willen we een code in $\mathbb{F}_q^{\mathbb{F}_q^m}$ beschrijven als verlengde cyclische code dan moeten we een plaats identificeren met het parity-check symbool en de overige q^m-1 plaatsen opvatten als coefficienten van polynomen in $\mathbb{F}_q[X]/(X^{q^m-1}-1)$. Merk op dat $(q^m-1,q) = 1$ zodat een cyclische code geheel bepaald is door zijn nulpunten. In het concrete geval van de code RM(m,v,q) ziet deze beschrijving er als volgt uit. Zij γ een primitief element van

$\mathbb{F}_{q^m}$. Voor iedere $f \in \mathbb{F}_q^{\mathbb{F}_{q^m}}$ geldt nu:

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

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

We identificeren nu $f_{\gamma j}$ met x^j en vatten de waarden $f(\gamma^j)$ als coëfficienten op. Let op dat dit geen isomorfisme van ringen is aangezien in het algemeen $f_{\gamma i} f_{\gamma j} \neq f_{\gamma i+j}$. De coëfficient van f_0 vatten we op als parity-check symbool.
We verkrijgen zo

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

waarbij het rechterlid nog steeds een verlengde cyclische code is.

Zij L de verzameling optredende polynomen $\sum_{j=0}^{q^m-2} f(\gamma^j) X^j$. Dan is L een ideaal in $\mathbb{F}_q[X]/(X^{q^m-1}-1)$ en we mogen dus vragen naar de gemeenschappelijke nulpunten van L. Van deze nulpunten is een aantal reeds bekend.

Zij als hiervoor γ een primitief element. Voor $f \in RM(m,v,q)$ en $0 < j < q^m - 1$ en $c_q(j) < m(q-1) - v$ geldt:

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

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

Kennelijk zijn de punten γ^j met $0 < j < q^m - 1$ en $c_q(j) < m(q-1) - v$ gemeenschappelijke nulpunten van de elementen van L.

Dat de polynomen in L niet meer gemeenschappelijke nulpunten kunnen hebben zien we als volgt in. Zij L^* het ideaal in $\mathbb{F}_q[X]/(X^{q^m-1})$ bestaande uit de polynomen die de punten γ^j voor $c_q(j) < m(q-1) - v$ tot nulpunt

hebben. Uit het voorafgaande volgt $L^* \supset L$. Omdat $\mathbb{F}_q[X]$ een hoofdideaal ring is wordt L^* als ideaal voortgebracht door het minimale polynoom dat alle punten γ^j met $c_q(j) < m(q-1) - v$ tot nulpunt heeft. Dit is het polynoom

$$\prod_{\substack{0 \le j < q^m - 1 \\ c_q(j) < m(q-1) - v}} (X - \gamma^j)$$

(ga na dat dit een polynoom in $\mathbb{F}_q[X]$ is!). De graad van dit polynoom is gelijk aan

$$d = \left| \{ j \mid 0 < j < q^m - 1,\ c_q(j) < m(q-1) - v \} \right|$$

en de dimensie over $\mathbb{F}_q$ van het ideaal L^* is dus $q^m - 1 - d$.

Anderzijds is de dimensie van het ideaal L gelijk aan de dimensie van de code RM(m,v,q). In de voorafgaande paragraaf hebben we deze dimensie uitgerekend waarbij de uitkomst was

$$f = \left| \{ j \mid 0 \le j \le q^m - 1 \text{ en } c_q(j) \le v \} \right|.$$

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

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

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

$$d + f = \left| \{ j \mid (0 < j < q^m - 1 \text{ en } c_q(j) \le v) \text{ of } (0 < j \le q^m - 1 \text{ en } c_q(j) > v) \} \right| =$$

$$= q^m - 1.$$

Hieruit volgt $f = q^m - 1 - d$, dus $L = L^*$, zodat het bewijs voltooid is.

(6.7.1) CONCLUSIE. Voor $v < m(q-1)$ is de code RM(m,v,q) een verlengde cyclische code, waarvoor de bijbehorende cyclische code afkomstig is van het ideaal $L \subset \mathbb{F}_q[X]/(X^{q^m-1} - 1)$ dat voor een vaste primi-

tieve wortel $\gamma \in \mathbb{F}_{q^m}$ alle machten γ^j met $0 < j < q^m - 1$ en cijfersom $c_q(j)$ kleiner dan $m(q-1) - v$ als gemeenschappelijke nulpunten heeft.

OPMERKING: Het feit dat de polynomen in L de punten γ^j voor $1 \le j \le q^m - 1$ en $c_q(j) < n(q-1) - v$ als nulpunten hebben levert ons met behulp van de BCH-grens (5.5.1) een nieuw bewijs voor de Reed-Muller grens. Aangezien het kleinste getal j met $c_q(j) = m(q-1) - v$ ontstaat door grote cijfers zo ver mogelijk naar rechts te schuiven laat dit getal zich makkelijk berekenen. Stel $v = r(q-1) + s$, $0 \le s \le q - 1$. Dan geldt $m(q-1) - v = (m-r-1)(q-1) + (q-1-s)$ zodat het minimale getal met cijfersom $m(q-1) - v$ er uitziet als:

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

De BCH-grens levert derhalve een minimaal gewicht van $(q-s)q^{m-r-1}-2 + 2 = (q-s)q^{m-r-1}$ evenals in (6.5.6) [zie (5.10.10)]. Merk op dat de Reed-Muller code een deelcode is van de verlengde BCH-code met ontwerpafstand $(q-s)q^{m-r-1}$. Daar dit het minimale gewicht van RM(m,v,q) is hebben we hier voorbeelden van BCH-codes waarvoor de minimale afstand gelijk is aan de ontwerpafstand.

6.8. DUALITEIT VAN REED-MULLER CODES

(6.8.1) STELLING. *De code* C = RM(m,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 $\underline{x},\underline{x}'$ uit C resp. C' inproduct nul hebben.

Stel

$$\underline{x} = S(E(f)) \qquad \text{met} \qquad \text{graad } (f) \leq v \qquad \text{en}$$
$$\underline{x}' = S(E(f')) \qquad \text{met} \qquad \text{graad } (f') \leq m(q-1) - v - 1$$

dan volgt

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

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

6.9. COMMENTAAR

Voor gedeeltelijk andere maar in wezen equivalente beschrijvingen van RM-codes verwijzen we naar BERLEKAMP (1968), VAN LINT (1971), CAMERON & VAN LINT (1975). Hier treft men o.a. een bewijs aan dat de beschrijvingen van gegeneraliseerde RM-codes equivalent zijn. Het hier weergegeven bewijs is in deze vorm afkomstig van H.W. Lenstra, Jr. Voor meer informatie over de stellingen van Chevalley, Warning en Ax verwijzen we naar JOLY (1973).

6.10. OPGAVEN

(6.10.1) Zij $Tr : \mathbb{F}_{2m} \longrightarrow \mathbb{F}_2$ het spoor gedefiniëerd door

$$Tr(\xi) := \xi + \xi^2 + \xi^4 + \ldots + \xi^{2^{m-1}}.$$

Als we $\mathbb{F}_{2m}$ opvatten als m-dimensionale vectorruimte V over $\mathbb{F}_2$ is door

$$L_\eta(\xi) := Tr(\xi\eta)$$

een lineaire afbeelding L_η gegeven. Zij $n = 2^m-1$. Zij ω een primitieve n-de eenheidswortel in $\mathbb{F}_{2m}$.
Beschouw

$$C := \{u(x) = u_0 + u_1 x + \ldots + u_{n-1} x^{n-1} \mid u_i = L_\eta(\omega^i),$$

$$0 \leq i \leq n-1,\ \eta \in V\}.$$

Bewijs dat C de verkorte 1^e orde RM-code is.

(6.10.2) Bij gebruik van de 2^e orde RM-code van lengte 32 ontvangen we

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

Wat was het codewoord?

(6.10.3) Beschouw de 2^e orde binaire RM-code van lengte 2^m. Welke gewichten kunnen voorkomen? M.a.w. bepaal de coefficienten van de weight-enumerator die 0 zijn.