

Inhoudsopgave

1	Codes, een inleiding	2
1.1	Inleiding	2
1.2	Praktische voorbeelden	2
1.3	Een aantal elementaire definities	3
1.4	MDS codes	6
2	Codes beschreven met algebra	8
2.1	Lineaire cyclische codes over \mathbb{F}_q	8
2.2	Cyclische zelfduale codes	10
2.3	Hamming codes	15
2.4	Sporen	16
2.5	Gebruik van sporen	18
3	Gewichtsverdelingen	20
3.1	Stelling van McWilliams	20
3.2	$BCH(m)$ -codes	27
3.3	Decoderen van $BCH(m)$ -codes	34
3.4	Melas codes	35
3.5	Een niet-binaire BCH -code	41
4	Goede codes	45
4.1	Onder- en bovengrens van $\alpha(\delta)$	45
4.2	De Reed-Solomon codes	49
4.3	Goppa-codes over \mathbb{P}^1	51
4.4	Goppa codes over willekeurige krommen	56
4.5	Elliptische codes	65

1 Codes, een inleiding

1.1 Inleiding

Bij dit vak willen we codes bestuderen. Codes zijn een manier om data te versturen. Op het moment dat deze te versturen data is omgezet in een ASCII-code of iets dergelijks, kan er worden gedacht aan een manier van coderen: hoe zet je de tekens om in een code die verstuurd kan worden, welke sleutel gebruik je hiervoor. Deze code kan worden verstuurd en als degene die het codewoord ontvangt de vertaalsleutel bezit, kan hij de originele data uit de code halen.

In principe zijn er twee redenen om de manier van coderen te bestuderen. Ten eerste kan het de bedoeling zijn om vertrouwelijke informatie op te sturen. Het is dan de bedoeling dat alleen degene, die de data behoort te ontvangen, de vertaalsleutel heeft en dat anderen zeer moeilijk achter de vertaalsleutel kunnen komen. Dit gebruik wordt bestudeerd in de cryptografie.

In coderingstheorie gaat het om een ander gebruik. Hierbij is het de bedoeling dat de data zo goed mogelijk ontvangen wordt. Immers bij het versturen van de code kan er de nodige ruis ontstaan. De ontvangen codewoorden zijn niet altijd hetzelfde als de verstuurde. Vragen als hoe je deze ruis kunt herkennen en hoe je de ruis volledig kunt corrigeren, staan centraal in dit vak.

In dit vak gaan we daarom op zoek naar codes die de nodige robuustheid hebben en die binnen een bepaalde foutmarge toch de juiste data uit het ontvangen woord weten te verkrijgen.

1.2 Praktische voorbeelden

Codes zie je overal om je heen, kijk maar naar de streepjes-code op een pak melk, de ISBN-code op een boek, de 10-cijferige code op een bankbiljet en ga zo maar door. Deze codes hebben een ingebouwde ‘parity-check’, zodat kan worden nagegaan of zo’n code werkelijk goed is ingevoerd in een computer. Een voorbeeld is de beroemde ISBN-code. De code van het boek *Introduction to Coding Theory and Algebraic Geometry* van *Jacobus H. van Lint* en *Gerard van der Geer* is

$$3 - 7643 - 2230 - 6$$

In het algemeen is de ISBN code een 10-cijferige code $(a_1, a_2, \dots, a_{10})$, met de volgende parity-check:

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + \dots + 2 \cdot a_9 + 1 \cdot a_{10} \equiv 0 \pmod{11}$$

en inderdaad geldt bij het bovengenoemde voorbeeld

$$10 \cdot 3 + 9 \cdot 7 + \dots + 2 \cdot 0 + 1 \cdot 6 \pmod{11} = 0 \pmod{11},$$

zoals eenvoudig is na te rekenen. De nummers op een Nederlands bankbiljet bestaan uit 10 cijfers $(a_1, a_2, \dots, a_{10})$, met als parity-check

$$a_1 + a_2 + \dots + a_{10} \pmod{9} \equiv 0,$$

controleer maar in een voorbeeld.

De kunst nu is om zulke codes te maken die veel fouten kunnen verbeteren. Een voorbeeld van zo'n 'goede' code is de Reed Solomon - code die gebruikt wordt in CD's. Hiermee is ook direct het grote voordeel van CD's boven LP's blootgelegd: Wanneer er ook maar één enkel krasje op een LP zit, kun je hem wel weggooien, terwijl zelfs een gaatje in een CD niet eens altijd tot verlies van geluidskwaliteit leidt. Maar probeer dit toch liever niet met je favoriete discs...

Allereerst zullen we echter een aantal begrippen moeten invoeren waarmee we codes nauwkeurig kunnen beschrijven.

1.3 Een aantal elementaire definities

Wat is nu precies een code? Beschouw een lichaam F , dan definiëren we een code van lengte n als volgt:

Definitie 1.3.1 *Een code van lengte n is een niet lege deelverzameling C van F^n . Een element $c \in C$ noemen we een woord in de code.*

In het vervolg van dit dictaat zullen we alleen met eindige lichamen werken, genoteerd als \mathbb{F}_q , het lichaam met q elementen. Een code C is dan een deelverzameling van \mathbb{F}_q^n . We hebben dus voor een woord $c \in C$, dat $c = (a_0, \dots, a_{n-1})$, met $a_i \in \mathbb{F}_q$. De a_i worden ook wel de coëfficiënten van het codewoord c genoemd. Bij deze definitie van een code kunnen we een afstandsbegrip invoeren.

Definitie 1.3.2 *Laat $c_1, c_2 \in \mathbb{F}_q^n$, dan is de Hammingafstand van c_1 en c_2 , genoteerd als $d(c_1, c_2)$, per definitie het aantal coëfficiënten waarin c_1 en c_2 verschillen.*

Merk op dat direct uit de definitie volgt dat d voldoet aan

- (i) $d \geq 0$ en $d(c_1, c_2) = 0 \Leftrightarrow c_1 = c_2$;
- (ii) $d(c_1, c_2) = d(c_2, c_1)$;
- (iii) $d(c_1, c_2) \leq d(c_1, c_3) + d(c_2, c_3)$.

Dit zegt precies, dat d een metriek is op \mathbb{F}_q^n (en dus ook op elke code C binnen \mathbb{F}_q^n).

We willen graag codes hebben die in staat zijn zoveel mogelijk fouten te herstellen die tijdens het versturen zijn ontstaan. Fouten zijn gemakkelijker te herstellen als de afstand tussen de woorden van de code groot is. Een goede code is dus een code waarbij de afstand tussen de woorden van de code groot is. Als maat hiervoor introduceren we de minimale afstand van een code:

Definitie 1.3.3 De minimale afstand van een code C , notatie d_{min} , is

$$d_{min} = \min_{c_1, c_2 \in C, c_1 \neq c_2} d(c_1, c_2).$$

Hiermee kunnen we een kleine stelling formuleren die iets zegt over de mogelijkheid van foutcorrectie:

Stelling 1.3.4 Laat C een code zijn. Als $0 \leq m < \frac{d_{min}}{2}$ en c is een ontvangen woord, met $d(c, c_1) = m$ voor zekere $c_1 \in C$, dan is, mits maximaal m fouten zijn gemaakt, het verzonden woord c_1 .

Bewijs. Stel het verzonden woord is $c_2 \in C$ met $c_2 \neq c_1$, dan weten we dat $d(c, c_2) \leq m$, omdat er maximaal m fouten zijn gemaakt. Er volgt dan, dat $d(c_1, c_2) \leq d(c_1, c) + d(c, c_2) \leq m + m < d_{min}$, maar dit kan niet want $d(c_1, c_2) \geq d_{min}$ en dus is het verzonden woord c_1 . \square

Tot nog toe weten we vrij weinig van een code: het is een deelverzameling van \mathbb{F}_q^n . Om de codes wat gemakkelijker te kunnen beschrijven, zullen we nu gaan kijken naar lineaire en cyclische codes.

Definitie 1.3.5 Een lineaire code C is een code $C \subset \mathbb{F}_q^n$, die een lineaire deelruimte is van \mathbb{F}_q^n .

Een lineaire code C is zelf dus een lineaire ruimte over \mathbb{F}_q . We noteren een lineaire code C als $[n, k, d]$ -code indien

- (i) n = lengte van de code;
- (ii) $k = \dim_{\mathbb{F}_q}(C)$;
- (iii) $d = d_{min}$.

Propositie 1.3.6 Zij $C \subset \mathbb{F}_q^n$ een lineaire code, dan geldt

$$d_{min} = \min_{(v_0, \dots, v_{n-1}) \in C \setminus \{0\}} \#\{i \mid v_i \neq 0\}.$$

Dus de minimale afstand is niets anders dan het minimale aantal coëfficiënten ongelijk aan nul van niet nul-woorden in C .

Bewijs. We noteren codewoorden $b, c \in C$ als $b = (b_0, \dots, b_{n-1})$ en $c = (c_0, \dots, c_{n-1})$. Dan geldt

$$d_{\min} = \min_{b, c \in C, b \neq c} d(b, c) = \min_{b, c \in C, b \neq c} (\text{aantal } b_i - c_i \neq 0) = \min_{c \in C \setminus \{0\}} (\text{aantal } c_i \neq 0)$$

omdat met b en c ook $b - c$ een codewoord is. \square

Definitie 1.3.7 Een cyclische code is een code $C \subset \mathbb{F}_q^n$ zodanig dat als $c = (c_0, \dots, c_{n-1}) \in C$ dan ook $(c_1, \dots, c_{n-1}, c_0) \in C$.

Bij een code C definiëren we als volgt de *duale*

$$C^\perp = \{(a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} a_i c_i = 0 \quad \forall (c_0, \dots, c_{n-1}) \in C\}.$$

Opmerking 1.3.8 (i) Wat C ook moge zijn, C^\perp is altijd lineair.

(ii) Als C een $[n, k, d]$ -code dan is C^\perp een $[n, n - k, ?]$ -code, immers als C over \mathbb{F}_q als basis $\{v_1, \dots, v_k\}$ heeft, dan horen bij de vergelijking

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0$$

precies $n - k$ vectoren die een basis vormen voor de oplossingen van de vergelijking. Immers, de matrix hier met de vectoren v_i als rijen heeft rang k en dus $n - k$ als dimensie van de kern. En deze kern bestaat precies uit de vectoren die in C^\perp zitten.

Het is niet zo direct duidelijk wat de minimale afstand van een code C^\perp zou kunnen zijn. Een grens ervoor is te vinden uit de volgende algemene relatie tussen de parameters n, k, d van een $[n, k, d]$ -code.

Lemma 1.3.9 Voor een willekeurige $[n, k, d]$ -code geldt $d \leq n - k + 1$.

Bewijs. Als we van alle codewoorden hun laatste $d - 1$ coëfficiënten weglaten, blijven ze nog steeds allemaal verschillend. Deze bewerking levert daarom een injectieve, lineaire afbeelding van de code naar \mathbb{F}_q^{n-d+1} . Dus is de dimensie van onze code hooguit $n - d + 1$, met andere woorden $k \leq n - d + 1$ oftewel $d \leq n - k + 1$. \square

1.4 MDS codes

Definitie 1.4.1 Een ‘multiple distance separable’ (MDS) code is een lineaire code met parameters $[n, k, n + 1 - k]$.

Uit Lemma 1.3.9 blijkt dus, dat voor zo’n code de minimale afstand tussen de codewoorden maximaal is.

Stelling 1.4.2 De duale van een MDS-code is weer een MDS-code.

Bewijs. Stel C is een $[n, k, n + 1 - k]$ -code over \mathbb{F}_q . Per definitie is dan

$$C^\perp = \{(a_1, a_2, \dots, a_n) \in \mathbb{F}_q^n \mid a_1 \cdot v_1 + a_2 \cdot v_2 + \dots + a_n \cdot v_n = 0, \forall (v_1, v_2, \dots, v_n) \in C\}.$$

We weten al dat de lengte van C^\perp gelijk is aan n en de dimensie over \mathbb{F}_q is gelijk aan $n - k$. Laat d de minimale afstand zijn van de code C^\perp , dus

$$\begin{aligned} d &= \min_{v, w \in C^\perp, v \neq w} \{ \# \text{ coëfficiënten waarin } v \text{ en } w \text{ verschillen} \} \\ &= \min_{0 \neq v \in C^\perp} \{ \# \text{ coëfficiënten waarin } v \neq 0 \}. \end{aligned}$$

We weten vanwege Lemma 1.3.9 dat

$$d \leq n - (n - k) + 1 = k + 1.$$

Om gelijkheid te bewijzen, moeten we dus nog de andere kant op.

Stel dat in de code C^\perp de minimale afstand $\leq k$ is, dan bestaat er dus een woord $(0, 0, \dots, 0) \neq (w_1, w_2, \dots, w_n) \in C^\perp$, dat hoogstens k coëfficiënten $\neq 0$ heeft. Zeg dat $w_{i_1}, w_{i_2}, \dots, w_{i_j} \neq 0$ zijn, met $1 \leq i_1 < i_2 < \dots < i_j \leq n$ en $j \leq k$. Beschouw nu de oorspronkelijke code C , en wel in het bijzonder de $n - k$ coëfficiënten, van woorden in C , met de volgende eigenschap:

$\{i_1, i_2, \dots, i_j\}$ is een deelverzameling van de verzameling van indices, die corresponderen met de overige k coëfficiënten. Dus we kiezen $1 \leq l_1 < l_2 < \dots < l_k \leq n$ zodanig dat $i_1, i_2, \dots, i_j \in I := \{l_1, l_2, \dots, l_k\}$. Bij een woord $v = (v_1, v_2, \dots, v_n) \in C$ bestuderen we dan de coëfficiënten v_r , met $r \in I^c := \{1, 2, \dots, n\} \setminus \{l_1, l_2, \dots, l_k\}$.

Stel nu dat $v, w \in C$ en $v \neq w$, dan verschillen v en w in tenminste $n + 1 - k$ coëfficiënten. Wanneer we nu de coëfficiënten die corresponderen met de indices uit I^c weglaten, dan geldt nog steeds $v \neq w$. Doen we dit bij alle woorden in C , dan geeft dit een ‘nieuwe’ code in \mathbb{F}_q^k , van dimensie k en minimale afstand 1. Deze ‘nieuwe’ code heeft q^k woorden, dus deze code is gelijk aan de hele \mathbb{F}_q^k . Er geldt:

$$\{(v_{l_1}, v_{l_2}, \dots, v_{l_k}) \mid (v_1, v_2, \dots, v_n) \in C\} = \mathbb{F}_q^k.$$

Van een woord $v \in C$ kennen we dus de coëfficiënten v_r waar $r \in I$. Omdat $\{i_1, i_2, \dots, i_j\} \subset I$ kunnen we de volgende woorden in C definiëren:

$$\begin{aligned} e^{(1)} &= (e_1^{(1)}, e_2^{(1)}, \dots, e_n^{(1)}) && \text{met } e_{i_1}^{(1)} = 1 \text{ en } e_r^{(1)} = 0, r \in I \setminus \{i_1\}, \\ e^{(2)} &= (e_1^{(2)}, e_2^{(2)}, \dots, e_n^{(2)}) && \text{met } e_{i_2}^{(2)} = 1 \text{ en } e_r^{(2)} = 0, r \in I \setminus \{i_2\}, \\ &&& \vdots \\ e^{(j)} &= (e_1^{(j)}, e_2^{(j)}, \dots, e_n^{(j)}) && \text{met } e_{i_j}^{(j)} = 1 \text{ en } e_r^{(j)} = 0, r \in I \setminus \{i_j\}. \end{aligned}$$

Omdat w 'loodrecht staat' op de woorden $e^{(1)}, e^{(2)}, \dots, e^{(j)}$ zien we, omdat $w_r = 0$ voor alle $r \in I^c$, dat

$$w_{i_1} = w_{i_2} = \dots = w_{i_j} = 0.$$

Dit is echter in tegenspraak met de aanname dat $w \neq 0$. Dus de minimale afstand is groter dan k , ofwel $d \geq k + 1$. Met bovenstaande geldt dus

$$d = k + 1.$$

Hiermee is bewezen dat de duale van een MDS-code wederom MDS is. \square

Tenslotte definiëren we de gewichtsverdeling van een code.

Definitie 1.4.3 *Zij C een code en $v = (v_0, \dots, v_{n-1}) \in C$, dan is het gewicht van v , genoteerd als $w(v)$, het aantal coëfficiënten ongelijk aan 0 in v . De gewichtsverdeling is een afbeelding:*

$$\{0, \dots, n\} \rightarrow \mathbb{Z}_{\geq 0}$$

gegeven door $i \mapsto A_i$ waarbij $A_i =$ aantal woorden in C met gewicht i . Het gewichtsverdeling-polynoom is $P_C(X) = A_0 + A_1X + \dots + A_nX^n$.

Merk op dat $P_C(1) = \#C$ en in het geval van een lineaire code $\text{ord}_0(P_C(X) - A_0) = d_{\min}$. Immers, volgens Propositie 1.3.6 is $d_{\min} = \min_{v=(v_0, \dots, v_{n-1}) \in C \setminus \{0\}} \#\{i | v_i \neq 0\}$. Laat $v = (v_0, \dots, v_{n-1}) \in C \setminus \{0\}$ met $w(v) = d_{\min}$, dan is $A_i = 0$ voor $1 \leq i < w(v)$, omdat er anders een $v' \in C \setminus \{0\}$ bestaat met $w(v') < d_{\min}$, zodat $d(v', 0) < d_{\min}$ ($0 \in C$, want C is een lineaire code). Er geldt ook dat $A_{w(v)} \neq 0$, omdat $v \in C$. Hieruit volgt dat $\text{ord}_0(P_C(X) - A_0) = \text{ord}_0(A_{w(v)}X^{w(v)} + \dots + A_nX^n) = w(v) = d_{\min}$.

2 Codes beschreven met algebra

2.1 Lineaire cyclische codes over \mathbb{F}_q

We gaan nu kijken naar codes C met $C \subset \mathbb{F}_q^n$ die lineair en cyclisch zijn. We proberen daar met behulp van enige algebra wat meer over te zeggen.

Voorbeeld 2.1.1 Laat $C \subset \mathbb{F}_2^3$, met C lineair en cyclisch. Omdat C lineair is, is C een vectorruimte over \mathbb{F}_2 . We kunnen in \mathbb{F}_2^3 codes C maken met dimensie 0,1,2 en 3.

Als nu $(1, 0, 0) \in C$, dan volgt wegens het cyclisch zijn dat ook $(0, 1, 0), (0, 0, 1) \in C$, maar dan zitten er in C drie onafhankelijke vectoren, zodat $\dim_{\mathbb{F}_2} C = 3$ en dus geldt $C = \mathbb{F}_2^3$.

Duidelijk is dat $C = \langle (1, 1, 1) \rangle$ een lineaire, cyclische code is met $\dim_{\mathbb{F}_2} C = 1$. Tenslotte een code met dimensie 2: beschouw $C = \{v = (v_1, v_2, v_3) \in \mathbb{F}_2^3 \mid v_1 + v_2 + v_3 = 0\}$, dan is C een lineaire deelruimte van \mathbb{F}_2^3 en zelfs geldt $C = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ en dus C is ook cyclisch. De dimensie van C is 2. De genoemde codes, plus de code bestaande uit alleen maar de nulvector, zijn de enige lineaire cyclische codes in \mathbb{F}_2^3 .

2.1.2 Uit de algebra weten we dat \mathbb{F}_q^n als vectorruimte isomorf is met $R = \mathbb{F}_q[X]/(X^n - 1) = \{a_0 + a_1X + \dots + a_{n-1}X^{n-1} \bmod (X^n - 1) \mid a_0, \dots, a_{n-1} \in \mathbb{F}_q\}$, via het isomorfisme g dat $(b_0, \dots, b_{n-1}) \in \mathbb{F}_q^n$ afbeeldt op $b_0 + b_1X + \dots + b_{n-1}X^{n-1} \bmod (X^n - 1) \in R$.

In het vervolg noteren we elementen uit R als $\overline{f} \in R$, waarbij dan $f \in \mathbb{F}_q[X]$. Een lineaire, cyclische code $C \subset \mathbb{F}_q^n$ wordt dan afgebeeld op $\tilde{C} \subset R$. Welke eigenschappen heeft \tilde{C} als C lineair en cyclisch is?

Dat C lineair is, betekent voor \tilde{C} dat:

- (i) $0 \in \tilde{C}$, immers $(0, 0, \dots, 0) \in C$;
- (ii) $\overline{f_1}, \overline{f_2} \in \tilde{C}, a \in \mathbb{F}_q \Rightarrow \overline{f_1 - af_2} \in \tilde{C}$, immers als $\overline{f_i} = g(c_i)$, dan $c_1 - ac_2 \in C$ en dus $\overline{f_1 - af_2} = g(c_1 - ac_2) \in \tilde{C}$.

C is tevens cyclisch, oftewel $(b_0, b_1, \dots, b_{n-1}) \in C \Rightarrow (b_{n-1}, b_0, \dots, b_{n-2}) \in C$. Vertaald naar \tilde{C} betekent dit: $\overline{f} = b_0 + b_1X + \dots + b_{n-1}X^{n-1} \bmod (X^n - 1) \in \tilde{C} \Rightarrow \overline{b_{n-1} + b_0X + \dots + b_{n-2}X^{n-1}} \bmod (X^n - 1) \in \tilde{C}$. In R geldt $\overline{b_{n-1} + b_0X + \dots + b_{n-2}X^{n-1}} \bmod (X^n - 1) = \overline{b_{n-1} + b_0X + \dots + b_{n-2}X^{n-1} + b_{n-1}(X^n - 1)} \bmod (X^n - 1) = \overline{b_0X + \dots + b_{n-2}X^{n-1} + b_{n-1}X^n} \bmod (X^n - 1) = \overline{X(b_0 + \dots + b_{n-1}X^{n-1})} \bmod (X^n - 1) = \overline{Xf}$.

Hiermee hebben we aangetoond dat cyclisch zijn voor \tilde{C} niets anders betekent dan: $\overline{f} \in \tilde{C} \Rightarrow \overline{Xf} \in \tilde{C}$.

Dit gegeven samen met het feit dat \tilde{C} lineair is, levert ons dat voor willekeurige $\bar{f} \in \tilde{C}, \bar{g} \in R$ ook het produkt $\overline{fg} = \overline{gf} \in \tilde{C}$. Onze derde eigenschap wordt daarmee

$$(iii) \bar{f} \in \tilde{C}, \bar{g} \in R \Rightarrow \overline{fg}, \overline{gf} \in \tilde{C}.$$

De eigenschappen (i),(ii) en (iii) definiëren precies het begrip ideaal, we kunnen dus concluderen dat

Stelling 2.1.3 $\tilde{C} \subset R$ is lineair en cyclisch $\Leftrightarrow \tilde{C}$ is een ideaal.

Met deze stelling is de vraag hoe we lineaire en cyclische codes kunnen vinden in \mathbf{F}_q^n gereduceerd tot de vraag hoe we idealen kunnen vinden in R . Deze vraag beantwoorden we met de volgende stelling.

Stelling 2.1.4 I is een ideaal van $R \Leftrightarrow I = \bar{f}R$ met $f \mid X^n - 1$.

Bewijs. Uit de derde isomorfiestelling voor ringen volgt dat elk ideaal I in R het beeld is onder de kanonieke afbeelding van een ideaal J in $\mathbb{F}_q[X]$ met $(X^n - 1) \in J$. Uit de algebra weten we verder dat een polynoomring een hoofdideaalring is. J is dus te schrijven als $f \cdot \mathbb{F}_q[X]$, dus $(X^n - 1) \cdot \mathbb{F}_q[X] \subset f \cdot \mathbb{F}_q[X]$, en dat betekent precies $f \mid X^n - 1$, dus I is te schrijven als $\bar{f} \cdot R$, met $f \mid X^n - 1$. \square

Voorbeeld 2.1.5 Bekijken we weer als in het voorbeeld 2.1.1 codes in \mathbb{F}_2^3 , dan hebben we $R = \mathbb{F}_2[X]/(X^3 - 1)$ en $X^3 - 1 = (X + 1)(X^2 + X + 1)$, zodat we alle lineaire cyclische codes krijgen door achtereenvolgens de idealen $(1), (X + 1), (X^2 + X + 1)$ en $(X^3 - 1)$ te bekijken (voor het gemak laten we de streep op elke klasse \bar{f} hier weg): $(1) = R$ en heeft dus dimensie 3. Verder $(X + 1) = \{0, 1 + X, 1 + X^2, X + X^2\}$ met dimensie 2, deze correspondeert met $C = \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$, zoals we die in het vorige voorbeeld gevonden hebben. $(X^2 + X + 1) = \{0, 1 + X + X^2\}$ en tenslotte $(X^3 - 1) = \{0\}$.

Voor zo'n lineaire cyclische code $\tilde{C} = \bar{f}R$, met $f \mid X^n - 1$ hebben we ook een uitdrukking voor de dimensie van \tilde{C} over \mathbb{F}_q .

Stelling 2.1.6 Laat $f \mid X^n - 1 \in \mathbb{F}_q[X]$, dan heeft de code (\bar{f}) dimensie $n - \text{gr}(f)$.

Bewijs. We weten met de derde isomorfiestelling dat $R/\bar{f}R = (\mathbb{F}_q[X]/(X^n - 1))/(\bar{f}) \cong \mathbb{F}_q[X]/(f)$, zodat ook het aantal elementen van beide verzamelingen gelijk moet zijn. Dit is $\#R/\bar{f}R = \frac{q^n}{\#(\bar{f})} = \#\mathbb{F}_q[X]/(f) = q^{\text{gr}(f)} \Rightarrow \#(\bar{f}) = q^{n - \text{gr}(f)}$.

En dus volgt, dat $\dim_{\mathbb{F}_q}(\bar{f}) = n - \text{gr}(f)$. \square

Opmerking 2.1.7 Met behulp van de voorgaande stelling 2.1.6 is vervolgens eenvoudig een basis voor de cyclische code $C := (\overline{f}) \subset \mathbb{F}_q[X]/(X^n - 1)$, voor een $f|X^n - 1$, te halen. Namelijk, schrijf $k = \text{gr}(f)$. Elk van de elementen $\overline{X^i f}$ zit in C , en als we schrijven $f = \sum_{j=0}^k a_j X^j$, dan corresponderen deze elementen voor $i \leq n - k - 1$ met de rijtjes

$$(a_0, \dots, a_k, 0, \dots, 0), (0, a_0, \dots, a_k, 0, \dots, 0), \dots, (0, \dots, 0, a_0, \dots, a_k) \in \mathbb{F}_q^n.$$

Deze rijtjes zijn lineair onafhankelijk, want de eerste $n - k$ coördinaten vormen de rijen van een bovendriehoeksmatrix met determinant $\neq 0$. We vinden dus evenveel onafhankelijke elementen als de dimensie van C , dus kennelijk vormen die elementen een basis.

2.2 Cyclische zelfduale codes

We gaan proberen zelfduale, lineaire, cyclische codes van lengte n te construeren.

Oplossing:

Als C een zelfduale lineaire cyclische code is in \mathbb{F}_q^n , met, zeg, dimensie over \mathbb{F}_q gelijk aan k , dan moet n even zijn. Immers

$$C \text{ is een } [n, k, d]\text{-code} \implies C^\perp \text{ is een } [n, n - k, ?]\text{-code.}$$

Als nu $C^\perp = C$, dan moeten de dimensies gelijk zijn, dus $n - k = k$, waaruit volgt $n = 2k$ is even. Eerst wat heuristiek:

lengte 2 Neem $C \subset \mathbb{F}_2^2$, gedefinieerd door

$$C = \langle (1, 1) \rangle.$$

Dus $C = \{(0, 0), (1, 1)\}$.

Stel nu dat $(x_1, x_2) \in C^\perp$, dan geldt

$$x_1 + x_2 = 0 \implies x_1 = x_2,$$

dus $(0, 0)$ en $(1, 1)$ zijn de enige woorden die in C^\perp zouden kunnen zitten. Echter door directe verificatie volgt dat deze woorden ook daadwerkelijk loodrecht staan op de woorden in C . Conclusie:

$$C^\perp = \{(0, 0), (1, 1)\} = C.$$

lengte 4 Neem $C \subset \mathbb{F}_2^4$, gedefinieerd door

$$C = \langle (0, 1, 0, 1), (1, 0, 1, 0) \rangle.$$

Dan is $C = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}$.

Als nu (x_1, x_2, x_3, x_4) in C^\perp zit, dan geldt:

$$x_1 + x_3 = 0 \quad (1)$$

$$x_2 + x_4 = 0 \quad (2)$$

$$x_1 + x_2 + x_3 + x_4 = 0 \quad (3)$$

Merk op dat (3) overbodig is.

We hebben dus de volgende mogelijkheden:

$$\left(0, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

en

$$\left(1, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

Anders gezegd: de woorden $(0, 0, 0, 0)$, $(0, 1, 0, 1)$, $(1, 0, 1, 0)$, $(1, 1, 1, 1)$ kunnen in C zitten. Wederom door directe verificatie blijkt dat

$$C^\perp = C.$$

Eerst nu een stukje algemene theorie:

We weten dat een lineaire, cyclische $[n, k, d]$ -code $C \subset \mathbb{F}_q$ correspondeert met een ideaal

$\tilde{C} = (\bar{f}) \subset \mathbb{F}_q[X]/(X^n - 1)$, waar $\deg(f) = n - k$ en $f \mid X^n - 1$.

Stel nu dat $X^n - 1 = f(X) \cdot g(X)$, dan geldt

Claim:

$$\tilde{C}^\perp = (\overline{g^*}) \subset \mathbb{F}_q[X]/(X^n - 1) \quad \text{waar } g^*(X) = X^k \cdot g\left(\frac{1}{X}\right).$$

Bewijs:

Stel

$$f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$$

en

$$g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1},$$

met

$$X^n - 1 = f(X) \cdot g(X).$$

Dit uitschrijven levert:

$$\begin{aligned}
X^n - 1 &= a_0 b_0 \\
&+ (a_0 b_1 + a_1 b_0) X \\
&+ (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 \\
&\vdots \\
&+ (a_0 b_{n-1} + a_1 b_{n-2} + \cdots + a_{n-2} b_1 + a_{n-1} b_0) X^{n-1} \\
&+ (a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-2} b_2 + a_{n-1} b_1) X^n \\
&+ (a_2 b_{n-1} + a_3 b_{n-2} + \cdots + a_{n-2} b_3 + a_{n-1} b_2) X^{n+1} \\
&\vdots \\
&+ (a_{n-3} b_{n-1} + a_{n-2} b_{n-2} + a_{n-1} b_{n-3}) X^{2n-4} \\
&+ (a_{n-2} b_{n-1} + a_{n-1} b_{n-2}) X^{2n-3} \\
&+ (a_{n-1} b_{n-1}) X^{2n-1}
\end{aligned}$$

Bekijk de $(n-1)^e$ coëfficiënt:

$$a_0 b_{n-1} + a_1 b_{n-2} + \cdots + a_{n-2} b_1 + a_{n-1} b_0 = 0.$$

En verdere bestudering van coëfficiënten levert ook

$$\underbrace{a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1}_{= 1} + \underbrace{a_0 b_0}_{= -1} = 0.$$

Evenzo

$$\underbrace{a_2 b_{n-1} + a_3 b_{n-2} + \cdots + a_{n-2} b_3 + a_{n-1} b_2}_{= 0} + \underbrace{a_0 b_1 + a_1 b_0}_{= 0} = 0,$$

\vdots

$$\underbrace{a_{n-1} b_{n-1}}_{= 0} + \underbrace{a_0 b_{n-2} + \cdots + a_{n-3} b_1 + a_{n-2} b_0}_{\text{coëff. voor } X^{n-2}, \text{ dus } = 0} = 0.$$

We zien dat $(b_{n-1}, b_{n-2}, \dots, b_0)$ loodrecht staat op de woorden

$$\begin{aligned}
a^{(0)} &:= (a_0, a_1, \dots, a_{n-1}) \\
a^{(1)} &:= (a_1, a_2, \dots, a_0) \\
a^{(2)} &:= (a_2, a_3, \dots, a_1) \\
&\vdots \\
a^{(n-1)} &:= (a_{n-1}, a_0, \dots, a_{n-2}).
\end{aligned}$$

Dus, omdat deze $a^{(i)}$ een basis bevatten voor C , volgt

$$g^* \leftrightarrow (b_{n-1}, b_{n-2}, \dots, b_0) \in C^\perp \leftrightarrow \tilde{C}^\perp.$$

Dus

$$g^* \in \tilde{C}^\perp.$$

Echter $\deg(f) = n - k$ en dus $\deg(g) = k$. Hieruit volgt $\deg(g^*) = k$ en bovendien geldt

$$X^k g \left(\frac{1}{X} \right) = g^*(X) \mid X^n - 1$$

want

$$f(X)g(X) = X^n - 1 \iff X^n f \left(\frac{1}{X} \right) g \left(\frac{1}{X} \right) = 1 - X^n,$$

en dit betekent

$$-X^{n-k} f \left(\frac{1}{X} \right) X^k g \left(\frac{1}{X} \right) = X^n - 1$$

(oftewel, het reciproke polynoom bij f maal g^* is op een teken na gelijk aan $X^n - 1$). We zien dus dat

$$\tilde{C}^\perp = (\overline{g^*}) \in \mathbb{F}_q[X]/(X^n - 1).$$

(Immers C^\perp is een $[n, n - k, ?]$ -code, die bovendien zelf ook cyclisch is omdat C dat is. Dit impliceert dat met $\overline{g^*}$ ook alle veelvouden van dit polynoom in \tilde{C}^\perp zitten, dus $(\overline{g^*}) \subset \tilde{C}^\perp$. Deze inclusie moet dan wel een gelijkheid zijn, want beide ruimten hebben dezelfde dimensie.)

Laten we nu, in het algemeen, naar een lineaire, cyclische, zelfduale code $C \subset \mathbb{F}_2^n$ kijken, waar n even is. Omdat $C^\perp = C$ zal gelden

$$\dim_{\mathbb{F}_2} C = \dim_{\mathbb{F}_2} C^\perp = \frac{n}{2}.$$

We gaan op zoek naar polynomen f en g met $\deg(f) = \frac{n}{2}$ en $\deg g = n - \frac{n}{2} = \frac{n}{2}$ en waarvoor geldt

1.

$$f(X) \cdot g(X) = X^n - 1 = X^n + 1$$

2.

$$g^*(X) = X^{n/2} g \left(\frac{1}{X} \right) = f(X)$$

Dit is echter erg gemakkelijk, want in $\mathbb{F}_2[X]$ geldt:

$$(X^{n/2} + 1) \cdot (X^{n/2} + 1) = X^n + 2X^{n/2} + 1 = X^n + 1$$

en

$$X^{n/2} \cdot \left(\left(\frac{1}{X} \right)^{n/2} + 1 \right) = X^{n/2} + 1.$$

We zien nu direct dat een zelfduale, lineaire, cyclische code over \mathbb{F}_2 van lengte 6 wordt gegeven door het ideaal

$$\left(\overline{X^3 + 1} \right) \in \mathbb{F}_2[X]/(X^6 - 1)$$

en analoog voor lengte 8.

Voor $n = 2$ stemt de nu gevonden code precies overeen, met dat wat we op heuristische manier gevonden hadden:

Bij lengte 2 wordt de zelfduale, lineaire, cyclische code \tilde{C} gegeven door het ideaal

$$\left(\overline{X + 1} \right) \in \mathbb{F}_2[X]/(X^2 - 1).$$

De polynomen van graad ≤ 1 in $\mathbb{F}_2[X]$ zijn:

$$0, 1, X, X + 1.$$

Dus

$$\tilde{C} = \left\{ \overline{0}, \overline{X + 1}, \overline{X^2 + X}, \overline{(X + 1)^2} \right\} = \{ \overline{0}, \overline{X + 1}, \overline{1 + X}, \overline{0} \}$$

en we zien

$$\tilde{C} = \{ \overline{0}, \overline{X + 1} \} \longleftrightarrow \{(0, 0), (1, 1)\} = C.$$

Hiermee zijn overigens nog lang niet alle mogelijkheden gevonden: we hebben alleen maar gevallen met $q = 2$ (of een macht van 2, dat gaat volstrekt hetzelfde) waar bovendien $g = g^*$. Een geval dat we nog niet hebben is bijvoorbeeld degene die correspondeert met de ontbinding

$$X^{14} - 1 = (X^7 + X^6 + X^5 + X^4 + X + 1)(X^7 + X^6 + X^3 + X^2 + X + 1).$$

Merk tenslotte op, dat het geen toeval is dat we alleen in karakteristiek 2 voorbeelden vinden. Immers, we zoeken naar ontbindingen $X^n - 1 = g \cdot g^*$ waarin g^* het reciproke polynoom is van g . Dit reciproke polynoom heeft als nulpunten precies alle $1/\alpha$'s, waarbij α de nulpunten van g doorloopt. Nu is 1 een nulpunt van $X^n - 1$, en dus ook van g of van g^* , en dus van zowel g als g^* . Maar dan volgt, dat 1 een dubbel nulpunt is van $X^n - 1$. Het is daarmee ook

een nulpunt van de afgeleide, en dat is $\overline{n}X^{n-1}$. Hieruit volgt $n \bmod p = 0$, oftewel n is een veelvoud van de karakteristiek. De multipliciteit van het nulpunt 1 is dan zelfs een macht van p , en de helft hiervan zou zowel de multipliciteit in g als in g^* moeten zijn. Die helft is evenwel geen geheel getal, tenzij $p = 2$.

2.3 Hamming codes

Een belangrijke klasse lineaire cyclische codes zijn de zogenaamde ‘‘Hamming-achtige’’ codes. Dit zijn codes over \mathbb{F}_q . Laat $m \geq 1$ en beschouw $\mathbb{F}_{q^m}^*$. We weten dat dit een cyclische groep is met $q^m - 1$ elementen. Er bestaat dus een $\alpha \in \mathbb{F}_{q^m}^*$ met $\mathbb{F}_{q^m}^* = \langle \alpha \rangle$. Deze α kunnen we als volgt construeren (in feite geven we hier min of meer een bewijs voor het feit dat de vermenigvuldiggroep van een eindig lichaam cyclisch is):

Laat l een priemgetal met $l \mid q^m - 1$, en laat $n \in \mathbb{Z}$ zodanig dat n het aantal voorkomens is van l in de priemontbinding van $q^m - 1$ (dus $l^n \mid q^m - 1$, maar $l^{n+1} \nmid q^m - 1$). We noteren dit als $l^n \parallel q^m - 1$. Omdat $x^{q^m-1} = 1$ voor elke $x \in \mathbb{F}_{q^m}^*$ (want $\text{ord}(x) \mid \#\mathbb{F}_{q^m}^* = q^m - 1$), geldt dat het polynoom $X^{q^m-1} - 1$ volledig splijt in $\mathbb{F}_{q^m}[X]$. Hiermee splijt ook $X^{l^n} - 1$ volledig in $\mathbb{F}_{q^m}[X]$, want $X^{l^n} - 1 \mid X^{q^m-1} - 1$ (immers $q^m - 1 = kl^n$ voor zekere $k \in \mathbb{Z}$ en dus $X^{q^m-1} - 1 = (X^{l^n} - 1)(X^{(k-1)l^n} + X^{(k-2)l^n} + \dots + 1)$).

Beschouw nu de nulpunten β van $X^{l^n} - 1$. Omdat $X^{l^n} - 1$ volledig splijt, hebben we precies l^n van zulke nulpunten β . Voor deze nulpunten geldt $\beta^{l^n} = 1$ en dus $\text{ord}(\beta) \in \{1, l, \dots, l^n\}$. Als $\text{ord}(\beta) = l^k$, dan is β een nulpunt van $X^{l^k} - 1$. Dit polynoom heeft hoogstens l^k nulpunten en dus zijn er hoogstens $1 + l + \dots + l^{n-1} < l^n$ nulpunten met $\text{ord}(\beta) < l^n$. Hieruit volgt dat er een nulpunt β_l bestaat met $\text{ord}(\beta_l) = l^n$.

Zo'n β_l kun je voor elk priemgetal $l \mid q^m - 1$ vinden. Definieer nu α als het produkt van deze β_l 's, dan is $\text{ord}(\alpha) = \prod_{l^n \parallel q^m - 1, l \text{ priem}} l^n = q^m - 1$. Oftewel α is een voortbrenger van $\mathbb{F}_{q^m}^* = \langle \alpha \rangle$.

Schrijf nu $f_{\mathbb{F}_q}^\alpha$ voor het minimumpolynoom van α over \mathbb{F}_q , dan geldt $\text{gr}(f_{\mathbb{F}_q}^\alpha) = m$. Omdat $f_{\mathbb{F}_q}^\alpha$ per definitie irreducibel is en α een nulpunt van $X^{q^m-1} - 1$ geldt $f_{\mathbb{F}_q}^\alpha \mid X^{q^m-1}$. Met behulp van dit polynoom definiëren we de Hamming-code.

Definitie 2.3.1 *De Hamming code $H_q(m)$ is als volgt gedefinieerd:*

$$H_q(m) = \overline{f_{\mathbb{F}_q}^\alpha} R$$

waarbij $R = \mathbb{F}_q[X]/(X^{q^m-1} - 1)$.

Omdat volgens het bovenstaande $f_{\mathbb{F}_q}^\alpha \mid X^{q^m-1} - 1$, geldt met stelling 2.1.4 en 2.1.3 dat $H_q(m)$ een lineaire, cyclische code is, met lengte $q^m - 1$ en dimensie $q^m - 1 - \text{gr}(f_{\mathbb{F}_q}^\alpha) = q^m - 1 - m$. Over de minimale afstand d_{\min} kunnen we nog geen uitspraak doen. Woorden uit de Hammingcode zijn van de vorm $\overline{f_{\mathbb{F}_q}^\alpha \bar{g}}$ met $\bar{g} \in R$.

Stel nu dat we een willekeurige $\bar{h} \in R$ hebben, hoe kunnen we dan zien of $\bar{h} \in H_q(m)$?

Lemma 2.3.2 $\bar{h} \in H_q(m) \Leftrightarrow f_{\mathbb{F}_q}^\alpha \mid h \Leftrightarrow h(\alpha) = 0$.

Het bewijs van dit lemma is vrij triviaal.

2.3.3 Laat $\bar{g} = \overline{a_0 + a_1X + \dots + a_kX^k}$ met $k = q^m - 2$, dan correspondeert g met $a = (a_0, \dots, a_k) \in \mathbb{F}_q^{k+1}$ en dus geldt $a \in H_q(m) \Leftrightarrow g(\alpha) = 0 \Leftrightarrow a_0 + a_1\alpha + \dots + a_k\alpha^k = 0 \Leftrightarrow a \perp (1, \alpha, \dots, \alpha^k) \in \mathbb{F}_q^{k+1}$.

We hebben zo dus $H_q(m) = \{g = \overline{a_0 + a_1X + \dots + a_{q^m-2}X^{q^m-2}} \in R \mid g(\alpha) = 0\} = \{a = (a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q^{q^m-1} \mid a \perp (1, \alpha, \dots, \alpha^{q^m-2}) \in \mathbb{F}_q^{q^m-1}\}$. Omdat $\{1, \alpha, \dots, \alpha^{q^m-2}\} = \mathbb{F}_q^*$, geldt dat $H_q(m)$ op permutatie na onafhankelijk is van de keuze van de voortbrenger α van \mathbb{F}_q^* .

Merk op dat we $H_q(m)$ ook kunnen schrijven als een doorsnede:

$$H_q(m) = \mathbb{F}_q^{q^m-1} \cap \langle (1, \alpha, \dots, \alpha^k) \rangle^\perp.$$

Dit kunnen we ook schrijven als $H_q(m) = \text{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \{(\mathbb{F}_{q^m} \cdot (1, \alpha, \dots, \alpha^{q^m-2}))^\perp\}$ waarbij de restrictie van $C \subset \mathbb{F}_{q^m}^N$ gedefinieerd is als $\text{Res}C = C \cap \mathbb{F}_q^N$. Deze definitie van restrictie zal ons van pas komen bij de berekening van de gewichtsverdeling van de Hamming-codes. Om restricties te bestuderen zullen we sporen gebruiken.

2.4 Sporen

Zij V een n -(dus eindig)dimensionale vectorruimte over K en $\phi : V \rightarrow V$ een lineaire afbeelding. Bij een gegeven basis voor V wordt ϕ gegeven door een matrix (a_{ij}) . Van deze matrix kunnen we het spoor (Engels 'trace') definiëren.

Definitie 2.4.1 Het spoor van ϕ , notatie $\text{tr}(\phi)$ is $\text{tr}(\phi) := a_{11} + a_{22} + \dots + a_{nn}$.

Dus het spoor van de lineaire afbeelding is het spoor van een bijbehorende matrix.

Bij een andere basis verandert de matrix van A in QAQ^{-1} , en omdat $tr(AB) = tr(BA)$ blijft het spoor dus onveranderd, en daarom is dit een goede definitie.

Als $K \subset L$ een eindige lichaamsuitbreiding is (L als vectorruimte eindig over K), en $\alpha \in L$ dan:

Definitie 2.4.2 $tr(\alpha) := tr(\phi_\alpha)$, met ϕ_α de K -lineaire afbeelding $L \rightarrow L$ gegeven door $\phi_\alpha(\beta) = \alpha\beta$.

Hiermee is tr een afbeelding $L \rightarrow K$, omdat L een vectorruimte over K is.

Stelling 2.4.3 Beschouw $tr : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$, dan geldt:

(i) tr is \mathbb{F}_q -lineair;

(ii) tr is surjectief;

(iii) $tr(\beta) = 0 \iff \beta = \gamma^q - \gamma$ voor een $\gamma \in \mathbb{F}_{q^m}$.

Bewijs. (i) lineariteit: $tr(\alpha + \lambda\beta) = tr(\phi_{\alpha+\lambda\beta}) = tr(\phi_\alpha + \lambda\phi_\beta) = tr(\phi_\alpha) + \lambda \cdot tr(\phi_\beta) = tr(\alpha) + \lambda \cdot tr(\beta)$ (met hier $\alpha, \beta \in \mathbb{F}_{q^m}$ en $\lambda \in \mathbb{F}_q$).

(ii) surjectief: Eerst leiden we een formule af voor tr . Neem $\beta \in \mathbb{F}_{q^m}$, dan $\mathbb{F}_q \subseteq \mathbb{F}_q(\beta) \subseteq \mathbb{F}_{q^m}$. Stel $f_{\mathbb{F}_q}^\beta = a_0 + a_1x + \dots + a_{d-1}x^{d-1} + x^d$ is het minimumpolynoom van β over \mathbb{F}_q .

Een basis voor $\mathbb{F}_q(\beta)$ over \mathbb{F}_q is $\{1, \beta, \dots, \beta^{d-1}\}$. Zo bestaat er ook een basis $\{1, \alpha_2, \dots, \alpha_n\}$ van \mathbb{F}_{q^m} over $\mathbb{F}_q(\beta)$, en er geldt dus $d \cdot n = m$.

Een basis voor \mathbb{F}_{q^m} over \mathbb{F}_q is dan:

$\{1, \beta, \dots, \beta^{d-1}, \alpha_2, \alpha_2\beta, \dots, \alpha_2\beta^{d-1}, \dots, \alpha_n, \alpha_n\beta, \dots, \alpha_n\beta^{d-1}\}$.

Bij deze basis krijg je als matrix voor $\phi_\beta : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ dus:

$$\begin{pmatrix} \begin{array}{cccc|cc} 0 & \cdots & & -a_0 & & \\ 1 & 0 & \cdots & -a_1 & & \\ 0 & 1 & \ddots & \vdots & 0 & 0 \\ \vdots & \ddots & \ddots & 0 & \vdots & \\ \vdots & & & 1 & -a_{d-1} & \\ & & & 0 & & idem & 0 \\ & & & 0 & & 0 & \ddots \end{array} \end{pmatrix}.$$

Hieruit volgt $tr(\beta) = -n \cdot a_{d-1}$.

Er geldt $0 = (\beta^d + a_{d-1}\beta^{d-1} + \dots + a_0)^q = \beta^{dq} + a_{d-1}^q\beta^{(d-1)q} + \dots + a_0^q \stackrel{a_i \in \mathbb{F}_q}{=} 0$

$(\beta^q)^d + a_{d-1}(\beta^q)^{d-1} + \dots + a_0$, dus β^q is ook een nulpunt van $f_{\mathbb{F}_q}^\beta$, en zo ook alle β^{q^i} voor $i \geq 1$. Hiervan zijn $\beta, \beta^q, \dots, \beta^{q^{d-1}}$ verschillend (ga na of zie de standaard algebra colleges), dus $f_{\mathbb{F}_q}^\beta = x^d + a_{d-1}x^{d-1} + \dots + a_0 = \prod_{i=0}^{d-1} (x - \beta^{q^i})$. Uit coëfficiënten vergelijken volgt dan, dat $-a_{d-1} = \sum_{i=0}^{d-1} \beta^{q^i}$, dus $tr(\beta) = n \cdot \sum_{i=0}^{d-1} \beta^{q^i}$. Omdat $\beta^{q^d} = \beta$, levert dit tenslotte de formule

$$tr(\beta) = \beta + \beta^q + \dots + \beta^{q^{m-1}}.$$

Omdat tr een \mathbb{F}_q -lineaire afbeelding $\mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ is, kan het beeld alleen maar 0 of de hele \mathbb{F}_q zijn. We weten verder dat tr gegeven wordt door $x \mapsto x^{q^{m-1}} + \dots + x^q + x$. Het polynoom $x^{q^{m-1}} + \dots + x^q + x$ heeft maximaal q^{m-1} nulpunten, maar \mathbb{F}_{q^m} heeft q^m elementen, dus er zijn elementen van \mathbb{F}_{q^m} , die niet op 0 worden afgebeeld. De conclusie is, dat het beeld van tr de hele \mathbb{F}_q is, en tr is dus surjectief.

(iii) kern(tr): tr is surjectief, dus $\dim(\text{kern}(tr)) = m - 1$.

Voor $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ beschouwen we het Frobenius automorfisme $F : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ gedefinieerd door $x \mapsto x^q$.

Er geldt $\text{kern}(F - id) = \mathbb{F}_q$, dus $\dim(\text{beeld}(F - id)) = m - 1$, dus om te bewijzen dat $\text{kern}(tr) = \text{beeld}(F - id)$ hoeft alleen maar bewezen te worden dat $\text{beeld}(F - id) \subset \text{kern}(tr)$.

Nu weten we dat $tr(\beta) = \sum_{i=0}^{m-1} F^i(\beta)$, dus $tr \circ (F - id) = (id + F + \dots + F^{m-1}) \circ (F - id) = F^m - id = 0$. Hiermee is de stelling bewezen. \square

2.5 Gebruik van sporen

Definitie 2.5.1 Zij $C \subset \mathbb{F}_{q^m}^{(N)}$ een code, dan is $tr(C) \subset \mathbb{F}_q^{(N)}$ de code die wordt verkregen, door van de coëfficiënten van alle vectoren in C het spoor te nemen. Dus $(a_1, \dots, a_N) \in C \rightsquigarrow (tr(a_1), \dots, tr(a_N)) \in tr(C)$.

Stelling 2.5.2 Voor $C \subset \mathbb{F}_{q^m}^{(N)}$ een lineaire code geldt: $\text{Res}(C^\perp) = (tr(C))^\perp$.

Bewijs. \subset : Zij $v \in \text{Res}(C^\perp)$, dan geldt dus $v = (v_1, \dots, v_N)$ voor zekere $v_i \in \mathbb{F}_q$, en $\sum v_i w_i = 0$ voor alle $w = (w_1, \dots, w_N) \in C$. Beschouw nu een element $(tr(z_1), \dots, tr(z_N)) \in tr(C)$, dan geldt $\sum v_i \cdot tr(z_i) = \sum tr(v_i z_i) = tr(\sum v_i z_i) = 0$, dus $v \in (tr(C))^\perp$.

\supset : zij $v \in (tr(C))^\perp$, dan $\sum v_i \cdot tr(w_i) = 0$ (ofwel $tr(\sum v_i w_i) = 0$), voor elke $(w_1, \dots, w_N) \in C$.

Maar C is \mathbb{F}_{q^m} -lineair, dus $\forall \lambda \in \mathbb{F}_{q^m}$ geldt, dat $\lambda(w_1, \dots, w_N) \in C$ en daarmee ook $\text{tr}(\lambda \sum v_i w_i) = 0$. Dan moet dus wel gelden dat $\sum v_i w_i = 0$ (anders kreeg je door vermenigvuldigen met alle mogelijke λ 's heel \mathbb{F}_{q^m} , en dus beelden $\neq 0$). De conclusie is dat $v \in C^\perp$, en v heeft coëfficiënten in \mathbb{F}_q , dus $v \in \text{Res}(C^\perp)$. \square

Voorbeeld 2.5.3 We gaan dit nu toepassen op de Hamming codes. Omdat $C^{\perp\perp} = C$ voor een lineaire code C , geldt:

$$\begin{aligned} H_q(m)^\perp &= (\text{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}((\mathbb{F}_{q^m} \cdot (1, \alpha, \dots, \alpha^{q^m-2}))^\perp))^\perp \\ &= (\text{tr}(\mathbb{F}_{q^m} \cdot (1, \alpha, \dots, \alpha^{q^m-2})))^{\perp\perp} \\ &= \text{tr}(\mathbb{F}_{q^m} \cdot (1, \alpha, \dots, \alpha^{q^m-2})). \end{aligned}$$

Van deze duale van de Hamming code gaan we de gewichtsverdeling bepalen. De codewoorden zijn van de vorm $\text{tr}(\lambda(1, \alpha, \dots, \alpha^{q^m-2})) = (\text{tr}(\lambda), \text{tr}(\lambda\alpha), \dots, \text{tr}(\lambda\alpha^{q^m-2}))$. Voor $\lambda = 0$ is dit dus een rijtje nullen, en anders is dit een rijtje met het spoor van precies alle elementen van $\mathbb{F}_{q^m}^*$. We hebben gezien dat het spoor een surjectieve \mathbb{F}_q -lineaire afbeelding $\mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ is, dus het is een (optel)groepshomomorfisme en elk beeld komt q^{m-1} keer voor, dus in het beeld van $\mathbb{F}_{q^m}^*$ ook, behalve 0, die dan een keer minder voorkomt. Het gewicht is daarom $(q^m - 1) - (q^{m-1} - 1) = q^m - q^{m-1}$ (totaal aantal elementen minus het aantal nullen).

Het gewichtsverdeling-polynoom is derhalve $1 + (q^m - 1)x^{q^m - q^{m-1}}$.

In het volgende hoofdstuk zullen we zien hoe hieruit de gewichtsverdeling van $H_q(m)$ zelf te vinden is.

3 Gewichtsverdelingen

3.1 Stelling van McWilliams

Volgens de definitie uit hoofdstuk 1 is een gewichtsverdeling van een code een afbeelding $\{0, \dots, n\} \rightarrow \mathbb{Z}_{\geq 0}$ gegeven door $i \mapsto A_i =$ aantal woorden in C met gewicht i . Hierbij definieerden we tevens het gewichtsverdelingspolynoom als $P_C(X) = A_0 + A_1X + \dots + A_nX^n$. Volgens de stelling van McWilliams bestaat er een verband tussen de gewichtsverdeling van C en van C^\perp :

Stelling 3.1.1 (McWilliams, 1963) *Zij $C \subset \mathbb{F}_q^n$ een lineaire code, met gewichtsverdelingspolynoom*

$$W_C(X) = \sum_{i=0}^n A_i X^i.$$

Het gewichtsverdelingspolynoom van de duale code C^\perp wordt dan gegeven door

$$W_{C^\perp}(X) = \frac{1}{\#C} \sum_{i=0}^n A_i (1-X)^i (1+(q-1)X)^{n-i}.$$

Voorbeeld 3.1.2 Eerst geven we een paar toepassingen van deze stelling.

- (0) Neem $C = \{0\} \subseteq \mathbb{F}_q^n$. Deze heeft alleen maar een woord van gewicht nul, dus $W_C(X) = 1$. De duale code is de hele \mathbb{F}_q^n . Volgens de stelling van McWilliams is dus

$$W_{\mathbb{F}_q^n}(X) = (1+(q-1)X)^n = \sum_{i=0}^n \binom{n}{i} (q-1)^i X^i.$$

Hier staat, dat er precies $\binom{n}{i} (q-1)^i$ vectoren in \mathbb{F}_q^n zijn die uit precies $n-i$ nullen en i getallen $\neq 0$ bestaan. Ga na dat dit inderdaad het geval is.

- (1) De *parity check-code*.

Laat $P = \{(a_1, \dots, a_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^n a_i = 0\}$. Het is eenvoudig te verifiëren dat dit een lineaire code is van lengte n en, omdat er maar één lineaire voorwaarde is, van dimensie $n-1$. Het is zelfs zo dat $P = (1, \dots, 1)^\perp$. Hieruit volgt dat voor $x \in P^\perp = \langle (1, \dots, 1) \rangle$ geldt dat $x = (a, \dots, a)$ waarbij a de hele \mathbb{F}_q doorloopt. Het is duidelijk dat $w(x) = 0$ als $a = 0$ en $w(x) = n$ als $a \neq 0$. We weten dat

$\#P^\perp = q$, zodat het gewichtsverdelingspolynoom van P^\perp gelijk is aan $W_{P^\perp}(X) = 1 + (q-1)X^n$. Met McWilliams volgt nu dat

$$W_P(X) = W_{P^{\perp\perp}}(X) = \frac{1}{q} \left((1 + (q-1)X)^n + (q-1)(1-X)^n \right),$$

oftewel, iets verder uitgeschreven,

$$W_P(X) = \sum_{i=0}^n \binom{n}{i} \frac{(q-1)^i + (-1)^i(q-1)}{q} X^i.$$

Het is al wat lastiger om dit ook zonder de gebruikte stelling na te gaan.

(2) De *Hamming-code*.

Laat $C = \langle (tr(1), tr(\alpha), \dots, tr(\alpha^{q^m-2})) \rangle$, waarin α een voortbrenger van $\mathbb{F}_{q^m}^*$ is. We hebben in het vorige hoofdstuk gezien dat $H_q(m) = C^\perp$ en ook dat $W_C(X) = 1 + (q^m - 1)X^{q^m - q^{m-1}}$, zodat met McWilliams volgt

$$W_{H_q(m)}(X) = \frac{1}{q^m} \left((1 + (q-1)X)^{q^m-1} + (q^m - 1)(1-X)^{q^m - q^{m-1}} (1 + (q-1)X)^{q^{m-1}-1} \right).$$

In het bijzonder is hieruit met enig rekenwerk de minimale afstand d_{min} van de code $H_q(m)$ te bepalen (door namelijk de coëfficiënten van X, X^2 en X^3 te berekenen lukt dat al).

Bewijs. (McWilliams)

We zullen het bewijs in een zestal stappen geven. Merk vooraf op dat, als we schrijven $q = p^k$, dan is \mathbb{F}_q als optelgroep een lineaire ruimte over \mathbb{F}_p , dus: $\mathbb{F}_q = \mathbb{F}_p v_1 + \dots + \mathbb{F}_p v_k$ voor zekere $v_1, \dots, v_k \in \mathbb{F}_q$.

Laat $W_C(X) = \sum_{i=0}^n A_i X^i$.

- (1) Neem een “karakter” op \mathbb{F}_q dat niet triviaal is. Dat wil zeggen, laat χ een homomorfisme zijn met $\chi : (\mathbb{F}_q, +) \rightarrow (\mathbb{C}^*, \cdot)$. (Bijvoorbeeld $\chi(v_1) = e^{\frac{2\pi i}{p}}$ en $\chi(v_i) = 1$ voor alle $i \neq 1$).
- (2) Bij $f : \mathbb{F}_q^n \rightarrow \mathbb{C}[X]$ een willekeurige afbeelding definiëren we $\hat{f} : \mathbb{F}_q^n \rightarrow \mathbb{C}[X]$ door $\hat{f}(v) = \sum_{w \in \mathbb{F}_q^n} \chi(\langle v, w \rangle) f(w)$, waarbij voor $v = (v_1, \dots, v_n)$ en $w = (w_1, \dots, w_n)$ in \mathbb{F}_q^n de vorm $\langle v, w \rangle$ gedefinieerd is als $\langle v, w \rangle = \sum_{i=1}^n v_i w_i$.

(3) **Lemma 3.1.3** *Zij $C \subset \mathbb{F}_q^n$ een lineaire code en $w \in \mathbb{F}_q^n$, dan*

$$\sum_{v \in C} \chi(\langle v, w \rangle) = \begin{cases} \#C, & \text{als } w \in C^\perp; \\ 0, & \text{als } w \notin C^\perp. \end{cases}$$

Bewijs. (i) Als $w \in C^\perp$, dan geldt voor iedere $v \in C$ dat $\langle v, w \rangle = 0$, dus ook dat $\chi(\langle v, w \rangle) = 1$. Dit levert $\sum_{v \in C} \chi(\langle v, w \rangle) = \#C$.

(ii) Is omgekeerd $w \notin C^\perp$, dan bestaat er een $v_0 \in C$ met $\langle v_0, w \rangle \neq 0$. Omdat \mathbb{F}_q een lichaam is, neemt voor $\lambda \in \mathbb{F}_q$ de uitdrukking $\langle \lambda v_0, w \rangle = \lambda \langle v_0, w \rangle$ alle waarden in \mathbb{F}_q aan. Er bestaat dus een $\lambda_0 \in \mathbb{F}_q$ met $\chi(\langle \lambda_0 v_0, w \rangle) \neq 1$, want χ was niet triviaal.

Met het voorgaande volgt nu

$$\begin{aligned} \sum_{v \in C} \chi(\langle v, w \rangle) &= \sum_{v \in C} \chi(\langle v + \lambda_0 v_0, w \rangle) \\ &= \sum_{v \in C} \chi(\langle v, w \rangle + \langle \lambda_0 v_0, w \rangle) \\ &= \chi(\langle \lambda_0 v_0, w \rangle) \cdot \sum_{v \in C} \chi(\langle v, w \rangle). \end{aligned}$$

Maar $\chi(\langle \lambda_0 v_0, w \rangle) \neq 1$, zodat volgt $\sum_{v \in C} \chi(\langle v, w \rangle) = 0$. □

(4) We hebben nu

$$\begin{aligned} \sum_{w \in C} \hat{f}(w) &= \sum_{w \in C} \sum_{v \in \mathbb{F}_q^n} \chi(\langle v, w \rangle) f(v) \\ &= \sum_{v \in \mathbb{F}_q^n} \left(f(v) \sum_{w \in C} \chi(\langle v, w \rangle) \right) \\ &\stackrel{(3)}{=} \#C \sum_{v \in C^\perp} f(v). \end{aligned}$$

(5) Introduceer de volgende notaties:

Voor $w \in \mathbb{F}_q^n$ schrijven we $\|w\| = d(w, 0)$ voor $w \in \mathbb{F}_q^n$, waarbij d de Hammingafstand voorstelt.

Verder $|a| = 0$ als $a = 0$ en $|a| = 1$ als $a \in \mathbb{F}_q^*$.

We hebben dan $\|w\| = |w_1| + \dots + |w_n|$ met $w = (w_1, \dots, w_n)$.

Definiëer de functie $f : \mathbb{F}_q^n \rightarrow \mathbb{C}[X]$ door $f(v) = X^{\|v\|}$. Dan volgt direct dat $\sum_{v \in C} f(v) = W_C(X)$, immers $\|v\|$ is precies het gewicht van v , zodat de coëfficiënt voor X^n precies het aantal elementen $v \in C$ is met

$$w(v) = n.$$

Pas nu (4) toe op deze functie f , dan krijgen we

$$W_{C^\perp}(X) = \sum_{v \in C^\perp} f(v) = \frac{1}{\#C} \sum_{w \in C} \hat{f}(w).$$

(6) Neem $w = (w_1, \dots, w_n) \in C$ vast, dan hebben we

$$\begin{aligned} \hat{f}(w) &= \sum_{v=(v_1, \dots, v_n) \in \mathbb{F}_q^n} \chi(\langle v, w \rangle) f(v) = \sum_{v=(v_1, \dots, v_n) \in \mathbb{F}_q^n} \chi(\langle v, w \rangle) X^{\|v\|} \\ &= \sum_{(v_1, \dots, v_n) \in \mathbb{F}_q^n} \chi(v_1 w_1) \chi(v_2 w_2) \cdots \chi(v_n w_n) X^{|v_1|} X^{|v_2|} \cdots X^{|v_n|} \\ &= \sum_{(v_1, \dots, v_n) \in \mathbb{F}_q^n} \prod_{i=1}^n \chi(v_i w_i) X^{|v_i|} = \prod_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha w_i) X^{|\alpha|}. \end{aligned}$$

Voor het uitrekenen van deze laatste som onderscheiden we twee gevallen.

Als $w_i = 0$, dan hebben we

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha w_i) X^{|\alpha|} = \sum_{\alpha \in \mathbb{F}_q} X^{|\alpha|} = 1 + (q-1)X.$$

En is $w_i \neq 0$, dan

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha w_i) X^{|\alpha|} = 1 + X \sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha w_i) = 1 + X \sum_{\beta \in \mathbb{F}_q^*} \chi(\beta).$$

Claim: $\sum_{\beta \in \mathbb{F}_q} \chi(\beta) = 0$.

Immers, neem $\gamma \in \mathbb{F}_q$ zodanig dat $\chi(\gamma) \neq 1$. We hebben dan

$$\sum_{\beta \in \mathbb{F}_q} \chi(\beta) = \sum_{\beta \in \mathbb{F}_q} \chi(\beta + \gamma) = \chi(\gamma) \sum_{\beta \in \mathbb{F}_q} \chi(\beta),$$

en dus $\sum_{\beta \in \mathbb{F}_q} \chi(\beta) = 0$. □

Nu volgt $\sum_{\beta \in \mathbb{F}_q^*} \chi(\beta) = \left(\sum_{\beta \in \mathbb{F}_q} \chi(\beta) \right) - \chi(0) = 0 - 1 = -1$.

En dus krijgen we

$$\sum_{\alpha \in \mathbb{F}_q^n} \chi(\alpha w_i) X^{|\alpha|} = 1 - X.$$

We concluderen uit deze berekening, dat

$$\hat{f}(w) = \prod_{i=1}^n (1+(q-1)X)^{1-|w_i|} (1-X)^{|w_i|} = (1-X)^{\|w\|} (1+(q-1)X)^{n-\|w\|}.$$

Met behulp van (5) volgt zo tenslotte

$$\begin{aligned} W_{C^\perp}(X) &= \frac{1}{\#C} \sum_{w \in C} \hat{f}(w) = \frac{1}{\#C} \sum_{w \in C} (1-X)^{\|w\|} (1+(q-1)X)^{n-\|w\|} \\ &= \frac{1}{\#C} \sum_{i=0}^n A_i (1-X)^i (1+(q-1)X)^{n-i}, \end{aligned}$$

want precies A_i van de w 's in C voldoen aan $\|w\| = i$.

□

Voorbeeld 3.1.4 Zoals al opgemerkt, kunnen we met deze stelling de gewichtsverdeling van $H_q(m)$ bepalen. De minimale afstand (ongelijk 0) in $H_q(m)$ is overigens ook zonder de stelling wel te vinden. Immers laat $a = (a_0, \dots, a_{n-1})$ een woord in $H_q(m)$ zijn, dan geldt $\sum_{i=0}^{n-1} a_i \alpha^i = 0$, waarbij $\langle \alpha \rangle = \mathbb{F}_q^*$. Een woord met gewicht 1 kan niet bestaan, immers dan zou $0 = \sum_{i=0}^{n-1} a_i \alpha^i = a_j \alpha^j$ voor zekere $a_j \neq 0$, en dus $\alpha^j = 0$ en dat is niet het geval. Stel nu a is een woord met gewicht 2, dan $a = (0, \dots, 0, a_i, 0, \dots, 0, a_j, 0, \dots, 0)$ en dus $a_i \alpha^i + a_j \alpha^j = 0 \Rightarrow a_i + a_j \alpha^{j-i} = 0 \Rightarrow \alpha^{j-i} = -\frac{a_i}{a_j} \in \mathbb{F}_q^*$.

Merk op dat dit niet mogelijk is wanneer $-\frac{a_i}{a_j} = 1$. Immers $\alpha^{j-i} = 1 \Rightarrow q^m - 1 \mid (j-i)$, tegenspraak, want $0 \leq i < j \leq q^m - 2$. En omgekeerd, als er een $1 \neq x \in \mathbb{F}_q^*$ bestaat, dan bestaan er inderdaad i, j met $\alpha^{j-i} = x$, want α brengt als groep $\{1, \alpha, \dots, \alpha^{q^m-2}\} = \mathbb{F}_{q^m}^* \supset \mathbb{F}_q^*$ voort. Het is duidelijk dat als $q > 2$, dan bestaat zo'n x en is dus de minimale afstand in $H_q(m)$ gelijk aan 2. Voor $q = 2$ bestaat er geen woord van gewicht 2, want hier bestaat \mathbb{F}_q^* alleen uit het element 1.

Als $q = 2$ dan is de minimale afstand 3 en er geldt zelfs dat het aantal elementen met gewicht 3 gelijk is aan $(2^m - 1)(2^m - 2)/6$, mits $m \geq 3$ (ter illustratie leiden we dit eerst nu af uit de formule van $W_{H_q(m)}$, maar we geven ook een direct bewijsje):

We weten dat de gewichtsverdeling van $H_q(m)$ gegeven wordt door

$$W_{H_q(m)}(x) = \frac{1}{q^m} \left\{ (1+(q-1)x)^{q^m-1} + (q^m-1)(1-x)^{q^m-q^{m-1}}(1+(q-1)x)^{q^{m-1}-1} \right\}.$$

In het geval $q = 2$ staat hier

$$\begin{aligned}
W_{H_2(m)}(x) &= \frac{1}{2^m} \left\{ (1+x)^{2^m-1} + (2^m-1)(1-x) \overbrace{2^m - 2^{m-1}}^{= 2^{m-1}} (1+x)^{2^{m-1}-1} \right\} \\
&\stackrel{n=2^m}{=} \frac{1}{n} \left\{ (1+x)^{n-1} + (n-1)(1-x)^{n/2} (1+x)^{n/2-1} \right\} \\
&= \frac{1}{n} \left\{ \sum_{k=0}^{n-1} \binom{n-1}{k} x^k + (n-1) \cdot \left[\sum_{k=0}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} (-1)^k x^k \right] \cdot \left[\sum_{l=0}^{\frac{n}{2}-1} \binom{\frac{n}{2}-1}{l} x^l \right] \right\}.
\end{aligned}$$

Vervolgens bepalen we de coëfficiënten voor x^j ; de minimale afstand d is dan gelijk aan

$$d = \min_{1 \leq j \leq n-1} \{ \text{coëff. voor } x^j \text{ is } \neq 0 \}.$$

Voor $j = 0$ vinden we

$$\text{coëff.} = \frac{1}{n} \left\{ \binom{n-1}{0} + (n-1) \cdot \binom{\frac{n}{2}}{0} \cdot \binom{\frac{n}{2}}{0} \right\} = \frac{1}{n} (1 + (n-1)) = \frac{n}{n} = 1,$$

zoals we al wisten.

De volgende, $j = 1$, levert

$$\begin{aligned}
\text{coëff.} &= \frac{1}{n} \left\{ \binom{n-1}{1} + (n-1) \left[\binom{n/2}{0} \binom{n/2-1}{1} - \binom{n/2}{1} \binom{n/2-1}{0} \right] \right\} \\
&= \frac{1}{n} \left\{ n-1 + (n-1) \left[\frac{n}{2} - 1 - \frac{n}{2} \right] \right\} \\
&= 0,
\end{aligned}$$

en ook dit hadden we al met veel minder rekenwerk uit de definitie gezien.

Evenzo weten we dat voor $j = 2$ in het geval $q = 2$ de coefficient 0 is; uit de formule voor de gewichtsverdeling zien we dit als volgt.

$$\begin{aligned}
\text{coëff.} &= \frac{1}{n} \left\{ \binom{n-1}{2} + (n-1) \left[\binom{n/2-1}{2} - \binom{n/2}{1} \binom{n/2-1}{1} + \binom{n/2}{2} \right] \right\} \\
&= \frac{1}{n} \left\{ \frac{(n-1)(n-2)}{2!} + (n-1) \left[\frac{(\frac{n}{2}-1)(\frac{n}{2}-2)}{2!} - \binom{n}{2} \left(\frac{n}{2} - 1 \right) + \frac{(\frac{n}{2})(\frac{n}{2}-1)}{2!} \right] \right\} \\
&= \frac{1}{n} \left\{ \frac{(n-1)(n-2)}{2!} + \frac{(n-1)(\frac{n}{2}-1)}{2!} \underbrace{\left(\frac{n}{2} - 2 - 2\frac{n}{2} + \frac{n}{2} \right)}_{=-2} \right\} \\
&= \frac{1}{n} \left\{ \frac{(n-1)(n-2)}{2!} - \frac{(n-1)(n-2)}{2!} \right\} \\
&= 0.
\end{aligned}$$

Vervolgens gaan we naar $j = 3$. Daar vinden we een coëfficiënt

$$\begin{aligned}
& \frac{1}{n} \left\{ \binom{n-1}{3} + (n-1) \left[\binom{n/2}{0} \binom{n/2-1}{3} - \binom{n/2}{1} \binom{n/2-1}{2} \right] + \left[\binom{n/2}{2} \binom{n/2-1}{1} - \binom{n/2}{3} \binom{n/2-1}{0} \right] \right\} \\
&= \frac{1}{n} \left\{ \frac{(n-1)(n-2)(n-3)}{3!} + (n-1) \left[\frac{\binom{n/2-1}{2} \binom{n/2-2}{3} - \binom{n/2}{2} \binom{n/2-1}{2}}{3!} + \frac{\binom{n/2}{2} \binom{n/2-1}{1} - \binom{n/2}{3} \binom{n/2-1}{0}}{2!} \right] \right\} \\
&= \frac{1}{n} \left\{ \frac{(n-1)(n-2)(n-3)}{6} + \frac{(n-1)\binom{n/2-1}{2}}{6} \left[\binom{n/2-2}{2} \binom{n/2-3}{1} - 3 \binom{n/2}{2} \binom{n/2-2}{1} + 3 \binom{n/2}{2} \binom{n/2-1}{1} - \binom{n/2}{2} \binom{n/2-2}{0} \right] \right\}.
\end{aligned}$$

Het deel tussen rechte haken, $[\dots]$, is gelijk aan

$$\begin{aligned}
& \binom{n}{2}^2 - 5 \binom{n}{2} + 6 - 3 \binom{n}{2} \left(\frac{n}{2} - 2 - \frac{n}{2} + 1 \right) - \binom{n}{2} \left(\frac{n}{2} - 2 \right) \\
&= \\
& \binom{n}{2}^2 - 5 \frac{n}{2} + 6 + 3 \frac{n}{2} - \binom{n}{2}^2 + 2 \frac{n}{2} = 6.
\end{aligned}$$

Dus de coëfficiënt voor x^3 is gelijk aan

$$\begin{aligned}
\text{coeff} &= \frac{1}{n} \left\{ \frac{(n-1)(n-2)(n-3)}{3!} - (n-1) \binom{n/2-1}{2} \right\} \\
&= \frac{n-1}{3! \cdot n} \{ (n-2)(n-3) + 3(n-2) \} \\
&= \frac{n(n-1)(n-2)}{6n} \\
&\stackrel{n=2^m}{=} \frac{2^m(2^m-1)(2^m-2)}{6 \cdot 2^m} \\
&= \frac{(2^m-1)(2^m-2)}{6}.
\end{aligned}$$

We vinden dus, dat voor $m \geq 2$ de minimale afstand in de code $H_2(m)$ gelijk is aan 3, immers de coëfficiënt voor x^3 in de gewichtsverdeling $W_{H_2(m)}(x)$ is ongelijk aan 0.

Zoals beloofd, volgen nu dezelfde formules nog een keer met een heel ander bewijs. Merk daarvoor op, dat een woord van gewicht k in $H_2(m)$ overeenkomt met een collectie len op plaatsen i_1, \dots, i_k en nullen overal elders. Dit correspondeert dus met een uitdrukking $\alpha^{i_1} + \dots + \alpha^{i_k} = 0$, oftewel met een rij $x_1, \dots, x_k \in \mathbb{F}_{2^m}$, allemaal verschillend en ongelijk aan 0, met som 0. Hierbij verandert het bijbehorende codewoord niet als we de x_i 's permuteren. Met andere woorden, het aantal elementen van $H_2(m)$ met gewicht k is gelijk aan het aantal oplossingen in $\mathbb{F}_{2^m}^{(k)}$ van $x_1 + \dots + x_k = 0$, gedeeld door $k!$, waarin we alleen oplossingen bestaande uit onderling verschillende x_i 's die bovendien alle niet nul zijn beschouwen.

Dit laat zich voor kleine k gemakkelijk tellen. Voor $k = 3$ beschouwen we $x + y + z = 0$. Dit beschrijft een vlak in $\mathbb{F}_{2^m}^{(3)}$, dus in het bijzonder (het is een lineaire ruimte van dimensie 2) bevat dit vlak precies $(2^m)^2 = 2^{2m}$ punten. Als van zo'n punt een tweetal coördinaten gelijk zijn, dan tellen die beide coördinaten op tot nul, dus de derde coördinaat moet dan ook nul zijn. Hieraan zien we, dat de punten die geen aanleiding geven tot een codewoord van gewicht 3, minstens één coördinaat gelijk hebben aan nul. Zulke punten kunnen we ook tellen: staat op minstens twee plaatsen een nul, dan uiteraard op alle drie want de som is nul. Dit levert 1 punt. En is er precies één 0, dan zijn de overige twee coördinaten gelijk, en we hebben alle $2^m - 1$ mogelijkheden voor het element uit $\mathbb{F}_{2^m}^*$ dat op die beide plaatsen moet staan. Dit levert $3(2^m - 1)$ punten (de 3 is voor de keuze van de plaats waar een nul staat). Er resteren dus $2^{2m} - 3(2^m - 1) - 1 = (2^m - 1)(2^m - 2)$ punten die bij codewoorden van gewicht 3 horen, en dit aantal moet dan nog door $3! = 6$ worden gedeeld om het aantal zulke woorden te krijgen.

3.2 BCH(m)-codes

In deze paragraaf willen we de zogenaamde *BCH*-codes bestuderen. Deze codes zijn vernoemd naar Bose, Ray - Chauduri en Hocquenghem. Een *BCH*-code is een deelcode van $H_q(m)$: $BCH_q(m) \subset H_q(m) \subset \mathbb{F}_q^{q^m - 1}$ en is als volgt gedefinieerd:

Definitie 3.2.1 *Een BCH-code is per definitie*

$$BCH_q(m) = \text{Res} (\langle (1, \alpha, \dots, \alpha^{q^m - 2}), (1, \alpha^3, \dots, \alpha^{3(q^m - 2)}) \rangle^\perp). \quad (4)$$

Hierin is α een voortbrenger van de groep $\mathbb{F}_{q^m}^*$.

De lengte van een woord in $BCH_q(m)$ is dus $q^m - 1$. En $a = (a_0, \dots, a_{q^m - 2}) \in \mathbb{F}_q^{q^m - 1}$ is een element van $BCH_q(m)$ precies dan, als de twee sommen $\sum_{i=0}^{q^m - 2} a_i \alpha^i$ en $\sum_{i=0}^{q^m - 2} a_i \alpha^{3i}$ gelijk zijn aan 0.

We zullen de notatie $BCH(m)$ gebruiken voor $BCH_2(m)$.

Stelling 3.2.2 *Er geldt $\dim(BCH(m)) = 2^m - 1 - 2m$ als $m \geq 3$. Verder bestaan $BCH(1)$ en $BCH(2)$ uit alleen maar de nulvector.*

Bewijs. We geven eerst alleen een schets van een bewijs (voor $m \geq 3$). Laat $C = \langle (1, \alpha, \dots, \alpha^{q^m-2}), (1, \alpha^3, \dots, \alpha^{3(q^m-2)}) \rangle \in \mathbb{F}_2^{2^m-1}$. Dan is $BCH(m) = \text{Res}(C^\perp) = (\text{tr}(C))^\perp$. Dus is het genoeg om aan te tonen dat $\dim_{\mathbb{F}_2} \text{tr}(C) = 2m$. Omdat

$$\det \begin{pmatrix} 1 & \alpha \\ 1 & \alpha^3 \end{pmatrix} = \alpha^3 - \alpha = \alpha(\alpha + 1)^2 \neq 0,$$

zijn $(1, \alpha), (1, \alpha^3)$ lineair onafhankelijk over \mathbb{F}_{2^m} en dus zijn zeker ook $(1, \alpha, \dots, \alpha^{q^m-2})$ en $(1, \alpha^3, \dots, \alpha^{3(q^m-2)})$ lineair onafhankelijk. Hieruit concluderen we dat C een lineaire ruimte over \mathbb{F}_{2^m} is van dimensie 2, dus $\#C = (2^m)^2 = 2^{2m}$. Als vectorruimte over \mathbb{F}_2 heeft C dus dimensie $2m$.

Beschouw de afbeelding $C \xrightarrow{Tr} \mathbb{F}_2^{2^m-1}$ die aan elke coördinaat het spoor ervan toevoegt. Deze afbeelding is \mathbb{F}_2 -lineair. Als kunnen aantonen dat deze afbeelding injectief is, dan volgt dat $\dim_{\mathbb{F}_2} \text{Tr}(C) = \dim_{\mathbb{F}_2} C = 2m$ en we zijn klaar.

Nu, dit gaat als volgt. Tr is injectief desda $\ker(Tr) = (0, \dots, 0)$. Laat $v \in C$ zodanig dat $Tr(v) = 0$, dan $v = \lambda(1, \alpha, \dots, \alpha^{q^m-2}) + \mu(1, \alpha, \dots, \alpha^{q^m-2}) = (\lambda x + \mu x^3)_{x \in \mathbb{F}_{2^m}^*}$ voor zekere $\lambda, \mu \in \mathbb{F}_{2^m}$. Dan volgt uit de veronderstelling dat $\text{tr}(\lambda x + \mu x^3) = 0 \quad \forall x \in \mathbb{F}_{2^m}$ (tr is het spoor van \mathbb{F}_{2^m} naar \mathbb{F}_2). Volgens stelling 2.4.3(iii) geldt dus $\forall x \in \mathbb{F}_{2^m} \exists y \in \mathbb{F}_{2^m}$ zodanig dat $\lambda x + \mu x^3 = y^2 - y$.

Beschouw daarom de kromme $X = \{(x, y) \in \overline{\mathbb{F}_{2^m}}^2 \mid \lambda x + \mu x^3 = y^2 - y\}$.

Uit de algebraïsche meetkunde hebben we de volgende stelling:

Stelling 3.2.3 (Hasse) *Er geldt $\#X \leq (\sqrt{q} + 1)^2$ voor λ, μ niet beide nul.*

Met behulp van deze stelling kan nu bewezen worden dat Tr injectief is: als $\text{tr}(\lambda x + \mu x^3) = 0$ voor elke $x \in \mathbb{F}_{2^m}$, dan kunnen we voor elk van deze x een y vinden met $(x, y) \in X$. maar dan is ook $(x, y + 1) \in X$, want $y(y - 1) = y(y + 1) = (y + 1)((y + 1) - 1)$. Hiermee hebben we tenminste 2^{m+1} elementen in X . Omdat $\leq 1 + 2^m + 2\sqrt{2^m} < 2^{m+1}$ voor alle $m \geq 3$, volgt dan uit Hasse's stelling dat $\lambda = \mu = 0$. Dit impliceert dat Tr injectief is. \square

Bovenstaande schets geeft een aardig voorbeeld, hoe de meetkunde (in dit geval kennis over hoeveel punten er op een kromme kunnen liggen) kan worden toegepast in de coderingstheorie. We zullen hier nog veel meer van zien.

We kunnen het probleem ook vanuit een meer algebraïsche oogpunt bekijken. Dit levert ons een tweede en in feite vrij eenvoudig bewijs van Stelling 3.2.2.

Bewijs. Ga zelf na, dat er voor $m \leq 2$ inderdaad geen andere woorden dan de nulvector in $BCH(m)$ zitten. We gaan er dus verder van uit dat $m \geq 3$. Laat $f \in \mathbb{F}_2[X]$ het minimumpolynoom van α zijn, en $g \in \mathbb{F}_2[X]$ het minimumpolynoom van α^3 (beide over \mathbb{F}_2). Deze polynomen zijn per definitie irreducibel en er geldt $f \neq g$ als $m \neq 1$, immers f is een polynoom van graad m en we weten uit de algebra dat $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}\}$ precies de verzameling van alle wortels van f is. Merk op dat $\mathbb{F}_{2^m}^* = \{1, \alpha, \dots, \alpha^{2^m-2}\}$, zodat alle wortels van f verschillen van α^3 . En dus $f(\alpha^3) \neq 0$ zodat $f \neq g$ en bovendien $\text{kgv}(f, g) = fg$, want zowel f als g zijn bovendien irreducibel. *Claim:* $\text{gr}(g) = m$ als $m \neq 2$.

Bewijs. (van deze claim). We weten dat $\text{gr}(g) = [\mathbb{F}_2(\alpha^3) : \mathbb{F}_2]$. En ook is $\mathbb{F}_2 \subset \mathbb{F}_2(\alpha^3) \subset \mathbb{F}_2(\alpha) = \mathbb{F}_{2^m}$. Laat $d = \text{graad van het minimumpolynoom van } \alpha \text{ over } \mathbb{F}_2(\alpha^3)$. Omdat α een nulpunt is van $X^3 - \alpha^3 \in \mathbb{F}_2(\alpha^3)[X]$, geldt dat $d \leq 3$.

Als we schrijven $\mathbb{F}_2(\alpha^3) = \mathbb{F}_q$ dan volgt $\mathbb{F}_2(\alpha) = \mathbb{F}_{q^d}$ en $\langle \alpha^3 \rangle \subset \mathbb{F}_q^* \subset \mathbb{F}_{q^d}^* = \langle \alpha \rangle$. Nu is de index $[\langle \alpha \rangle : \langle \alpha^3 \rangle]$ gelijk aan 1 of 3, en de index $[\mathbb{F}_{q^d}^* : \mathbb{F}_q^*] = 1 + q + \dots + q^{d-1}$ is hier een deler van. We bekijken de beide mogelijkheden afzonderlijk:

De index is 3. Nu volgt $1 + q + \dots + q^{d-1} \mid 3$. Als $d \neq 1$, dan moet wel $d = 2$ en $q = 2$, zodat $\mathbb{F}_2(\alpha^3) = \mathbb{F}_2$. Hieruit zou volgen dat $\alpha^3 = 1$ en dus heeft $\mathbb{F}_2(\alpha)$ graad hoogstens 2 over \mathbb{F}_2 . Maar dat betekent $m \leq 2$, wat we uitgesloten hebben. De conclusie in dit geval is dat $d = 1$ en dus $\mathbb{F}_2(\alpha) = \mathbb{F}_2(\alpha^3)$, hetgeen impliceert dat $\text{gr}(g) = \text{gr}(f) = m$.

De index is 1. Dan volgt meteen $\langle \alpha^3 \rangle = \langle \alpha \rangle$ en dus $d = 1$, want $\mathbb{F}_{q^d}^* = \mathbb{F}_q^*$. We vinden dan opnieuw dat $m = \text{gr}(g)$. \square

Beschouw nu $BCH(m)$ als deelruimte van $\mathbb{F}_2[X]/(X^{2^m-1} - 1)$ (vergelijk dit met wat we gedaan hebben met $H_q(m)$ -codes). Dan is $BCH(m) = \{\bar{h} \mid h(\alpha) = h(\alpha^3) = 0\} = \{\bar{h} \mid f \mid h \text{ en } g \mid h\} = \{\bar{h} \mid \text{kgv}(f, g) \mid h\} \stackrel{\text{kgv}(f, g) = fg}{=} \{\bar{h} \mid fg \mid h\} = \overline{(fg)}$. De graad van fg is $2m$ en dus volgt dat $\dim BCH(m) = 2^m - 1 - 2m$ (vergelijk Stelling 2.1.6). \square

3.2.4 We willen nu iets over de gewichtsverdeling van de $BCH(m)$ -code proberen te zeggen. We stellen ons de vraag hoeveel woorden er in een $BCH(m)$ -code zijn met een gegeven (klein) gewicht. Het moge duidelijk zijn

dat de gewichten 1 en 2 niet voorkomen, immers die zijn er niet in $H_2(m)$ en dus zeker ook niet in $BCH(m) \subset H_2(m)$.

In het algemeen kunnen we zeggen dat een woord in $BCH(m)$ met gewicht $n \leq 2^m - 1$ een woord $w = (w_1, \dots, w_{2^m-1})$ is met $w_{i_1} = 1, \dots, w_{i_n} = 1$ met $1 \leq i_1 < \dots < i_n \leq 2^m - 1$ en $w_j = 0$ voor de overige j . Met vergelijking (4) volgt bovendien dat $\sum_{j=1}^n \alpha^{i_j} = \sum_{j=1}^n \alpha^{3i_j} = 0$. Noemen we bovendien $x_j = \alpha^{i_j}$ dan volgt dat een woord van gewicht n correspondeert met $x_1, \dots, x_n \in \mathbb{F}_{2^m}^*$ onderling verschillend en $\sum_{j=1}^n x_j = \sum_{j=1}^n x_j^3 = 0$.

We zullen nu gaan bekijken of er woorden van gewicht 3, 4 en 5 zijn en zoja, hoeveel dat er zijn.

Woorden van gewicht 3.

Deze woorden corresponderen met $x, y, z \in \mathbb{F}_{2^m}^*$ die paarsgewijs verschillend zijn en voldoen aan $x + y + z = x^3 + y^3 + z^3 = 0$. Hieruit volgt $z = -x - y = x + y \Rightarrow x^3 + y^3 + (x + y)^3 = xy(x + y) = 0 \Rightarrow x + y = 0$, want $x \neq 0 \neq y \Rightarrow x = y$. Maar x, y, z waren verschillend, zodat er geen woorden van gewicht 3 bestaan.

Woorden van gewicht 4

Deze woorden corresponderen met $x, y, z, w \in \mathbb{F}_{2^m}^*$ die paarsgewijs verschillend zijn en voldoen aan $x + y + z + w = x^3 + y^3 + z^3 + w^3 = 0$. Voor zo'n woord geldt dus in het bijzonder $w = x + y + z$, en daarmee $x^3 + y^3 + z^3 + (x + y + z)^3 = (x + y)z^2 + (x + y)^2z + xy(x + y) = (x + y)(z^2 + xz + yz + xy) = (x + y)(x + z)(y + z) = 0$. Hieruit volgt $x = y$ of $x = z$ of $y = z$, maar x, y, z, w waren onderling verschillend, zodat er ook geen woorden van gewicht 4 zijn.

Woorden van gewicht 5

Woorden van gewicht 5 corresponderen met $x, y, z, w, t \in \mathbb{F}_{2^m}^*$, paarsgewijs verschillend, die een niet triviale oplossing zijn van het stelsel

$$\begin{cases} x + y + z + w + t = 0 \\ x^3 + y^3 + z^3 + w^3 + t^3 = 0. \end{cases}$$

Merk op dat beide vergelijkingen homogeen zijn (d.w.z. de totale graad voor elk van de termen is gelijk), zodat bij een oplossing (a_1, \dots, a_5) er direct een verzameling oplossingen is, namelijk $\lambda(a_1, \dots, a_5)$, waarin $\lambda \in \mathbb{F}_{2^m}^*$ willekeurig is. We kunnen daarom gaan kijken naar *projectieve* oplossingen; dat zijn in ons geval oplossingen in de projectieve ruimte $\mathbb{P}^4(\mathbb{F}_{2^m})$. Deze ruimte bestaat per definitie uit alle 5-tallen $(a_1 : \dots : a_5)$ met de $a_i \in \mathbb{F}_{2^m}$ niet allemaal gelijk aan nul, waarbij verder geldt dat $(a_1 : \dots : a_5) = (b_1 : \dots : b_5)$ zodra er een λ bestaat waarvoor $(a_1, \dots, a_5) = \lambda(b_1, \dots, b_5)$. We proberen nu aan

te geven, hoe met behulp van algebraïsche meetkunde ons probleem van het aantal oplossingen vinden kan worden aangepakt.

We gaan terug naar de vergelijkingen. Werken we daaruit t weg, dan houden we over

$$x^3 + y^3 + z^3 + w^3 + (x + y + z + w)^3 = 0. \quad (5)$$

We bekijken de oplossingen voor deze vergelijking in de projectieve ruimte $\mathbb{P}^3(\mathbb{F}_{2^m})$.

Uit de algebraïsche meetkunde is bekend dat elk (glad en irreducibel) kubisch oppervlak (i.e. de verzameling nulpunten van een derdegraads homogeen polynoom, zoals we hier bekijken) als volgt verkregen kan worden. Neem zes punten $p_1, \dots, p_6 \in \mathbb{P}^2$ waarvan geen drietal op een lijn ligt, en evenmin een zestal op een door een tweedegraadsvergelijking gegeven kromme. In de meetkunde kent men een constructie die “het opblazen van deze punten” heet. Daarbij worden deze punten uit \mathbb{P}^2 vervangen door een \mathbb{P}^1 . Het zo verkregen nieuwe oppervlak is dan in te bedden in \mathbb{P}^3 , en daar wordt het gegeven door een derdegraads vergelijking. De coëfficiënten in die vergelijking zitten in hetzelfde lichaam waarover ook de 6 punten waarmee we zijn begonnen als verzameling zijn gedefinieerd. Hierop komen we nog terug. Het is verder bekend, dat ieder (glad en irreducibel) derdegraads oppervlak in \mathbb{P}^3 op deze manier wordt verkregen. We zullen nu kijken naar ons oppervlak, en dan tegelijk hopelijk iets van het bovenstaande verduidelijken.

Ons oppervlak wordt gegeven door $x^3 + y^3 + z^3 + w^3 + (x + y + z + w)^3 = 0$. Deze vergelijking heeft coëfficiënten in \mathbb{F}_2 , dus volgens de theorie wordt het oppervlak verkregen door een zestal punten over \mathbb{F}_2 in \mathbb{P}^2 op te blazen. Het “over \mathbb{F}_2 ” hier betekent *niet*, dat alle zes punten coördinaten in \mathbb{F}_2 hebben. Maar wel, dat voor elk punt ook al z’n geconjugeerden weer tot het zestal behoren. We bepalen nu eerst, hoeveel van het zestal in $\mathbb{P}^2(\mathbb{F}_2)$ zitten en hoeveel niet.

Stel dat er precies a in $\mathbb{P}^2(\mathbb{F}_2)$ zitten. Bij het opblazen worden deze vervangen door een \mathbb{P}^1 , en die \mathbb{P}^1 bevat precies 3 punten over \mathbb{F}_2 (namelijk $(0 : 1)$ en $(1 : 0)$ en $(1 : 1)$). De overige $6 - a$ punten bestaan uit onderling geconjugeerden, dus ook de \mathbb{P}^1 ’s waardoor ze worden vervangen zijn onderling geconjugerd en derhalve liggen er geen rationale punten op (want die zouden vastblijven onder alle conjugaties). Omdat $\mathbb{P}^2(\mathbb{F}_2)$ uit 7 punten bestaat, concluderen we dat ons oppervlak $7 - a + 3a = 7 + 2a$ punten met coördinaten in \mathbb{F}_2 heeft. We tellen dit aantal nu op een andere manier, namelijk direct uit de vergelijking. Merk op dat $x^3 = x$ voor elke $x \in \mathbb{F}_2$. Dus voor punten met coördinaten in \mathbb{F}_2 kunnen we de vergelijking ook schrijven als

$$x^3 + y^3 + z^3 + w^3 + (x + y + z + w)^3 = x + y + z + w + (x + y + z + w) = 0.$$

Hieraan voldoen precies alle punten in $\mathbb{P}^3(\mathbb{F}_2)$, dus het aantal oplossingen is 15. De conclusie is, dat $7 + 2a = 15$, dus $a = 4$. Dus hebben 4 van de 6 punten coördinaten in \mathbb{F}_2 , en het resterende paar is onderling geconjugeerd. Derhalve moet dat paar wel alle coördinaten in \mathbb{F}_4 (de enige kwadratische uitbreiding van \mathbb{F}_2) hebben.

Met behulp van het voorgaande kunnen we het aantal projectieve oplossingen van (5) over elke \mathbb{F}_{2^m} bepalen: $\mathbb{P}^2(\mathbb{F}_q) = \{(x : y : z) \mid x, y, z \in \mathbb{F}_q \text{ niet alle } 0\} = \{(0 : 0 : 1), (0 : 1 : x), (1 : y : z) \mid x, y, z \in \mathbb{F}_q\}$ en dus $\#\mathbb{P}^2(\mathbb{F}_q) = 1 + q + q^2$. Voor m even verwijderen we hieruit 6 punten en die worden vervangen door $\mathbb{P}^1(\mathbb{F}_q)$, die uit precies $2^m + 1$ punten bestaat (de bepaling hiervan gaat net zoals bij \mathbb{P}^2), zodat we precies $2^{2m} + 2^m + 1 - 6 + 6(2^m + 1) = 2^{2m} + 7 \cdot 2^m + 1$ oplossingen hebben. Voor oneven m hebben we precies 4 van de 6 punten rationaal en daarom is het aantal projectieve oplossingen gelijk aan $2^{2m} + 2^m + 1 - 4 + 4(2^m + 1) = 2^{2m} + 5 \cdot 2^m + 1$. We hebben dus als we schrijven $q = 2^m$, dat

$$\#\text{projectieve oplossingen} = \begin{cases} q^2 + 7q + 1 & \text{als } m \text{ even;} \\ q^2 + 5q + 1 & \text{als } m \text{ oneven.} \end{cases}$$

Dit betekent dat het aantal oplossingen in $(\mathbb{F}_q)^4$ ongelijk aan $(0, 0, 0, 0)$ gelijk is aan $(q - 1)(q^2 + 7q + 1)$ (resp. $(q - 1)(q^2 + 5q + 1)$). Hieruit halen we nu het aantal woorden met gewicht 5.

Een woord van gewicht 5 wordt gerepresenteerd door (x, y, z, w, t) die alle verschillend en ongelijk 0 zijn, en voldoen aan het stelsel

$$\begin{cases} x + y + z + w + t = 0 \\ x^3 + y^3 + z^3 + w^3 + t^3 = 0. \end{cases}$$

Hoeveel van de $1 + (q - 1)(q^2 + 7q + 1)$ (of 5 in plaats van 7) oplossingen hiervan komen *niet* overeen met een woord van gewicht 5? In zo'n oplossing zijn twee van de vijf coördinaten gelijk, of er is een coördinaat 0.

Is bijvoorbeeld $x = y$, dan reduceert het stelsel tot (we werken in karakteristiek 2):

$$\begin{cases} z + w + t = 0 \\ z^3 + w^3 + t^3 = 0. \end{cases}$$

We proberen nu het aantal oplossingen hiervan te bepalen. Omdat we weten dat er geen woorden van gewicht 3 bestaan, volgt dat tenminste één van z, w, t gelijk is aan 0. Welnu,

$z = 0 \Rightarrow w + t = 0 \Rightarrow w = t \Rightarrow$ een oplossing ziet er uit als $(x, x, 0, w, w)$;

$w = 0 \Rightarrow z = t \Rightarrow$ een oplossing ziet er uit als $(x, x, z, 0, z)$

$t = 0 \Rightarrow z = w \Rightarrow$ een oplossing ziet er uit als $(x, x, z, z, 0)$

Al deze oplossingen zijn (modulo permutatie van de coördinaten) van de

vorm - $(0, x, x, w, w)$. Hoeveel zijn dit er? We zullen de volgende gevallen onderscheiden:

Is x of w gelijk aan 0, zeg $x = 0$, dan ziet een oplossing er op permutaties na uit als $(0, 0, 0, w, w)$. Voor $w \neq 0$ zijn er $q - 1$ mogelijkheden en dus in totaal zijn er $\binom{5}{3}(q - 1) + 1 = 10(q - 1) + 1$ mogelijkheden.

Nu nog de mogelijkheid $x \neq 0, w \neq 0$. Dit splitst in twee gevallen. Als $x = w$, dan zijn er $\binom{5}{4}(q - 1) = 5(q - 1)$ mogelijkheden en als $x \neq w$, dan zijn dat er $\binom{q-1}{2}5 \cdot \binom{4}{2} = 15(q - 1)(q - 2)$.

In totaal hebben we dus $1 + (q - 1)(10 + 5 + 15(q - 2)) = 1 + (q - 1)(15q - 15)$ oplossingen waarin twee coördinaten gelijk zijn.

In het resterende geval zijn alle coördinaten verschillend, maar eentje ervan is gelijk aan 0. Omdat alle coördinaten verschillend zijn, kan er hoogstens één coördinaat 0 zijn. Zeg $x = 0$, dan ziet een oplossing eruit als $(0, y, z, w, t)$, met y, z, w en t alle verschillend en ongelijk 0. Maar zo'n (y, z, w, t) correspondeert precies met een woord van gewicht 4 en deze zijn er niet, zodat er ook geen oplossingen zijn van bovenstaande vorm.

Dus het aantal oplossingen dat geen woord van gewicht 5 is, is precies $1 + (q - 1)(15q - 15)$, zodat het aantal acceptabele oplossingen gelijk is aan $(q - 1)(q^2 + 7q + 1) - (q - 1)(15q - 15) = (q - 1)(q^2 - 8q + 16)$ (resp. $(q - 1)(q^2 - 10q + 16)$). Om hieruit het aantal woorden van gewicht 5 te halen moeten we tenslotte nog delen door $5!$, omdat een permutatie van de coördinaten van een oplossing hetzelfde woord representeert. We concluderen, met weer de notatie $q = 2^m$, dat

$$\# \text{woorden van gewicht 5 in } BCH(m) = \begin{cases} \frac{(q - 1)(q - 4)^2}{120} & \text{voor } m \text{ even;} \\ \frac{(q - 1)(q^2 - 10q + 16)}{120} & \text{voor } m \text{ oneven.} \end{cases}$$

Een ander, maar opnieuw geheel meetkundig bewijs voor deze formule wordt gegeven in een artikel van Marcel van der Vlugt, verschenen in het Nieuw Archief voor Wiskunde **14** (1996). Ook hij begint met hetzelfde kubische oppervlak in \mathbb{P}^3 . Vervolgens neemt hij een lijn die geheel binnen het oppervlak ligt, en dan de verzameling vlakken die deze lijn bevatten. Het blijkt dan mogelijk, in elk van die vlakken afzonderlijk het aantal punten in de doorsnede van het vlak met het kubische oppervlak te tellen. De reden dat dit lukt, is dat zo'n doorsnede de vereniging is van de lijn die eerst gekozen was, en nog een kromme die door een vergelijking van graad 2 wordt gegeven.

We merken tenslotte op, dat de formule ook te vinden is door gebruik te maken van de stelling van MacWilliams: de duale code is vrij gemakkelijk

als een ‘spoor-code’ te zien, zoals wij dat hier ook gedaan hebben voor de Hamming codes. Een bewijs langs deze weg is te vinden in Section 15.3 van het boek “*The theory of Error-Correcting Codes*” geschreven door J. MacWilliams en N.J.A. Sloane (1983).

3.3 Decoderen van $BCH(m)$ -codes

Stelling 3.3.1 *Voor $m \geq 3$ is de $BCH(m)$ code een code die tot en met 2 fouten kan corrigeren.*

Bewijs. Omdat $BCH(m)$ een lineaire code is volgt met stelling 1.2.6 dat de minimale afstand gelijk is aan $d_{min} = \min_{v=(v_0, \dots, v_{n-1}) \in BCH(m) \setminus \{0\}} (\text{aantal } v_i \neq 0) = \min_{v \in BCH(m) \setminus \{0\}} (\text{gewicht } v)$. Uit het voorgaande weten we dat voor het gewicht van een woord ($\neq (0, \dots, 0)$) tenminste 5 is, en voor $m \geq 3$ zijn er woorden van gewicht 5 zodat $d_{min} = 5$. De stelling volgt nu uit stelling 1.3.4 \square

Veronderstel in het vervolg dat het aantal fouten ≤ 2 is.

Stel dat $r = (a_0, \dots, a_{2^{m-1}-2}) \in \mathbb{F}_2^{2^{m-1}-1}$ een ontvangen woord is, dat correspondeert met $f_r = a_0 + \dots + a_{2^{m-1}-2} X^{2^{m-1}-2} \in \mathbb{F}_2[X]/(X^{2^m-1} - 1)$.

Als je nu $f_r(\alpha)$ en $f_r(\alpha^3)$ berekent, dan kun je hier de nodige informatie uit halen. Als namelijk blijkt dat beide 0 zijn, dan is r correct (of er zijn tenminste $d_{min} = 5$ fouten gemaakt).

Veronderstel nu dat niet beide 0 zijn, hoe kunnen we dan het verzonden woord uit r terugkrijgen?

#fouten = 2. Stel dat de i^e en de j^e coördinaat niet correct zijn ontvangen, dan zijn deze i en j als volgt te vinden. Omdat we over \mathbb{F}_2 werken, geldt dat het correcte codewoord $f_c(X) = f_r(X) + X^i + X^j$ is. Schrijf $a = \alpha^i, b = \alpha^j$, dan $f_c(\alpha) = 0$, omdat c een woord is. $f_c(\alpha) = f_r(\alpha) + a + b \Rightarrow f_r(\alpha) = a + b$. Evenzo $f_r(\alpha^3) = a^3 + b^3 = (a + b)(a^2 + ab + b^2) = f_r(\alpha)((a + b)^2 + ab) = f_r(\alpha)((f_r(\alpha))^2 + ab)$, zodat het zoeken van het verzonden woord niets anders is dan een oplossing zoeken van het stelsel

$$\begin{cases} a + b = f_r(\alpha) \\ ab = \frac{f_r(\alpha^3)}{f_r(\alpha)} + (f_r(\alpha))^2 \end{cases}$$

Merk op dat $f_r(\alpha) \neq 0$, want anders zou r een codewoord zijn van $H_2(m) \supset BCH(m)$. Ook c is dit, dus $r - c \in H_2(m)$. Deze heeft gewicht 2, maar $d_{min} > 2$ voor de code $H_2(m)$. Dit stelsel oplossen is equivalent met het

vinden van de wortels van de vergelijking

$$Y^2 - f_r(\alpha)Y + \frac{f_r(\alpha^3)}{f_r(\alpha)} + (f_r(\alpha))^2 = 0,$$

waarmee dan in principe de fouten zijn gecorrigeerd. Merk op dat we dit in karakteristiek 2 aan het doen zijn, zodat we geen (direct) gebruik kunnen maken van de *abc*-formule.

fouten = 1. Stel dat in de i^e coördinaat een fout gemaakt is, dan geldt dat het correcte woord $f_r(X) + X^i$ is, dus $f_r(\alpha) + \alpha^i = 0$. Uit deze vergelijking kunnen we weer de juiste i bepalen.

3.4 Melas codes

We nemen $m \in \mathbf{Z}_{\geq 1}$ en $q = 2^m$. Laat verder α een voortbrenger van de cyclische groep \mathbb{F}_q^* zijn.

Definitie 3.4.1 *De Melas-code $M(m)$ wordt gedefinieerd door*

$$M(m) = \left\{ (a_1, a_2, \dots, a_{q-1}) \in \mathbb{F}_2^{q-1} \mid \sum_{i=1}^{q-1} a_i \alpha^i = \sum_{i=1}^{q-1} a_i \alpha^{-i} = 0 \right\}.$$

Dit is dus geheel analoog aan de *BCH*-codes; het is dan ook niet verwonderlijk, dat ongeveer dezelfde berekeningen ervoor gedaan kunnen worden. Het vinden van het aantal woorden met gewicht 5 is overigens een stuk lastiger. Dit is in de literatuur op twee verschillende manieren gedaan, waarbij beide flink wat algebraïsche meetkunde gebruiken; zie *Journal of Combinatorial Theory series A* **57** (1991), pagina's 163 t/m 186 en ook *Journal für die reine und angewandte Mathematik* **432** (1992), pagina's 151 t/m 176. Wat we hier nu zullen doen is

- (a) De dimensie van $M(m)$ bepalen;
- (b) Het aantal woorden van gewicht 0, 1, 2, 3 en 4 berekenen.

Propositie 3.4.2 *Er geldt*

$$\dim_{\mathbb{F}_2}(M(m)) = \begin{cases} 0 & \text{als } m = 1; \\ 1 & \text{als } m = 2; \\ 2^m - 1 - 2m & \text{als } m \geq 3. \end{cases}$$

Bewijs. Allereerst merken we op $\langle \alpha \rangle = \mathbb{F}_q^*$, en dus is $\text{ord}(\alpha) = q-1 = 2^m - 1$.

Als $m = 1$ dan geldt $q = 2^1 = 2$ en dus

$$M(m) = M(1) = \left\{ a \in \mathbb{F}_2 \mid a\alpha = \frac{a}{\alpha} = 0 \right\},$$

waar $\langle \alpha \rangle = \mathbb{F}_2^*$ en dus $\alpha = 1$. Met andere woorden $M(1) = \{0\}$. We vinden dus in dit geval $\dim_{\mathbb{F}_2} M(1) = 0$.

Als $m = 2$, dan is $q = 2^m = 4$, $\mathbb{F}_4^* = \langle \alpha \rangle = \{1, \alpha, \alpha^2\}$ en

$$M(m) = M(2) = \left\{ (a_1, a_2, a_3) \in \mathbb{F}_2^3 \mid a_1 + a_2\alpha + a_3\alpha^2 = a_1 + \frac{a_2}{\alpha} + \frac{a_3}{\alpha^2} = 0 \right\}.$$

Stel nu dat $(a, b, c) \in M(2)$, dan geldt

$$a + b\alpha + c\alpha^2 = 0 \tag{6}$$

$$a + \frac{b}{\alpha} + \frac{c}{\alpha^2} = 0. \tag{7}$$

Uit (6) volgt dat α een nulpunt is van het polynoom $f(X) := a + bX + cX^2$. Echter, in het algemeen, als $\langle \beta \rangle = \mathbb{F}_{p^n}^*$, dan is $\text{ord}(\beta) = p^n - 1$ en

$$\mathbb{F}_{p^n} = \mathbb{F}_p[\beta].$$

Immers, stel van niet, dan hebben we vanwege $\beta \in \mathbb{F}_{p^n}$ de gelijkheid $\mathbb{F}_p[\beta] = \mathbb{F}_{p^k}$, voor zekere $k < n$. Dus zou β een nulpunt zijn van $X^{p^k} - X$ en dus $\beta^{p^k} = \beta$, in tegenspraak met het feit dat $\text{ord}(\beta) = p^n - 1$.

Dus het minimumpolynoom van α over \mathbb{F}_2 heeft graad

$$\deg(f_{\mathbb{F}_2}^\alpha) = [\mathbb{F}_2[\alpha] : \mathbb{F}_2] = [\mathbb{F}_{2^2} : \mathbb{F}_2] = 2.$$

Dus òf $f \equiv 0$ òf $f(X) = 1 + X + X^2$, het enige monisch en irreducibele polynoom van graad 2 in $\mathbb{F}_2[X]$. In het eerste geval krijgen we het woord $(0, 0, 0)$ en in het tweede geval het woord $(1, 1, 1)$. Het woord $(0, 0, 0)$ zit zeker in $M(2)$, want $M(m)$ is lineair. Omdat $(1, 1, 1)$ aan (6) voldoet (het minimumpolynoom van α over \mathbb{F}_2 is immers gelijk aan $1 + X + X^2$), zien we door deling van $1 + \alpha + \alpha^2$ door α^2 dat het woord $(1, 1, 1)$ ook aan (7) voldoet. Dus

$$M(2) = \{(0, 0, 0), (1, 1, 1)\}.$$

Conclusie

$$\dim_{\mathbb{F}_2} M(2) = 1.$$

Tenslotte kijken we naar het geval $m \geq 3$. Hier geldt

$$\begin{aligned} M(m) &= \left\{ (a_1, a_2, \dots, a_{q-1}) \in \mathbb{F}_2^{q-1} \mid \sum_{i=1}^{q-1} a_i \alpha^i = \sum_{i=1}^{q-1} a_i \alpha^{-i} = 0 \right\} \\ &= \text{Res}_{\mathbb{F}_q/\mathbb{F}_2} \left(\left\langle (1, \alpha, \dots, \alpha^{q-1}), \left(1, \frac{1}{\alpha}, \dots, \frac{1}{\alpha^{q-1}} \right) \right\rangle^\perp \right). \end{aligned}$$

Laat nu

$$f = f_{\mathbb{F}_2}^\alpha, \quad \text{het minimumpolynoom van } \alpha \text{ over } \mathbb{F}_2$$

en

$$g = f_{\mathbb{F}_2}^{1/\alpha}, \quad \text{het minimumpolynoom van } \frac{1}{\alpha} \text{ over } \mathbb{F}_2.$$

Dan zijn f en g monisch en irreducibele polynomen in $\mathbb{F}_2[X]$. Verder geldt

$$\mathbb{F}_2[\alpha] = \mathbb{F}_2 \left[\frac{1}{\alpha} \right]$$

want $\alpha \in \mathbb{F}_2[\alpha^{-1}]$ en $\alpha^{-1} \in \mathbb{F}_2[\alpha]$, en dus

$$\deg(f) = [\mathbb{F}_2[\alpha] : \mathbb{F}_2] = [\mathbb{F}_2[\alpha^{-1}] : \mathbb{F}_2] = \deg(g).$$

Verder geldt voor $m \geq 3$ dat f en g verschillend zijn, immers

$$\alpha^{-1} = \alpha^{q-2} \notin \{\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}\},$$

want als $\alpha^{-1} = \alpha^{2^m-2} = \alpha^{2^k}$ voor zekere $k \in \{1, 2, \dots, m-1\}$ dan moet $2^m - 2 = 2^k$. Echter

$$2^m = 2 \cdot 2^{m-1} = 2^{m-1} + 2^{m-1} \stackrel{m-1 \geq 2}{>} 2 + 2^{m-1} \geq 2 + 2^k.$$

De verzameling $\{\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}\}$ is de nulpuntenverzameling van f (dit feitje uit de algebra is al meerdere malen in dit dictaat gebruikt). Dus is α^{-1} geen nulpunt van f , terwijl het wel een nulpunt van g is. Dus f en g zijn verschillend. Hieruit zien we dat $M(m)$, opgevat als deelverzameling van $\mathbb{F}_2[X]/(X^{2^m-1} - 1)$, gelijk is aan het ideaal

$$\begin{aligned} M(m) &= \{\bar{h} \mid h(\alpha) = h(\alpha^{-1}) = 0\} \\ &\stackrel{(*)}{=} \{\bar{h} \mid f \mid h \text{ en } g \mid h\} \\ &= \{\bar{h} \mid \text{kgv}(f, g) \mid h\} \\ &= \{\bar{h} \mid f \cdot g \mid h\} \\ &= \overline{(f \cdot g)}. \end{aligned}$$

Nu (*):

Er geldt

$$\bar{h} \in M(m) \iff f \mid h \text{ en } g \mid h.$$

Bewijs:

\Rightarrow Stel $\bar{h} \in M(m)$, dan is $h(\alpha) = 0$. Stel verder dat $f \nmid h$, dan bestaat er een $r \neq 0$, $\deg(r) < \deg(f)$ zodanig dat $h = q \cdot f + r$. Invullen van α geeft, daar $h(\alpha) = f(\alpha) = 0$, $r(\alpha) = 0$ en dus zou f *niet* het minimumpolynoom van α over \mathbb{F}_2 zijn. Tegenspraak.

Door f te vervangen door g en α door α^{-1} zien we analoog dat $g \mid h$.

\Leftarrow Stel $g \mid h$, dan volgt $h = q \cdot g$ voor e.o.a. polynoom $q \in \mathbb{F}_2[X]$. Hieruit volgt $g(\alpha^{-1}) = q(\alpha^{-1}) \cdot g(\alpha^{-1}) = 0$, want $g(\alpha^{-1}) = 0$. Analoog ook $h(\alpha) = 0$. Conclusie is dat $\bar{h} \in M(m)$ zit.

Verder geldt

$$\deg(f \cdot g) = \deg(f) + \deg(g) = m + m = 2m$$

en dus is

$$\dim_{\mathbb{F}_2} M(m) = 2^m - 1 - 2m.$$

Hiermee is het gestelde bewezen. \square

We gaan nu op zoek naar het aantal woorden in $M(m)$ van gewicht 0, 1, 2, 3 en 4. Voor $v \in M(m)$ schrijven we als gebruikelijk $w(v) = \#[\text{coeff. } v_i \text{ van } v \text{ ongelijk } 0]$ en $A_i = \#[\text{woorden van gewicht } i]$.

De nulvector zit in de (lineaire) code $M(m)$, dus $A_0 = 1$.

Wat $\#v : w(v) = 1$ betreft, zulke woorden zijn er niet, want $M(m) \subset H_2(m)$ en die laatste heeft ook geen woord(en) van gewicht 1. Dus $A_1 = 0$.

Dan $\#v : w(v) = 2$.

Zulke woorden bestaan ook al niet in $H_2(m)$. Dus $A_2 = 0$.

Vervolgens $\#v : w(v) = 3$.

Dit correspondeert met $x, y, z \in \mathbb{F}_q^* = \mathbb{F}_{2^m}^*$, onderling verschillend, met de eigenschappen

$$x + y + z = 0 \tag{8}$$

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 0. \tag{9}$$

Uit (8) volgt $z = x + y$. Dit substituerend in (9) geeft

$$1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{x+y} = \frac{y(x+y) + x(x+y) + xy}{xy(x+y)}.$$

Dus

$$(x+y)(x+y) + xy = x^2 + xy + y^2 = 0.$$

Wanneer we delen door y (dat mag, want $y \neq 0$) zien we dat we oplossingen in \mathbb{F}_q^* moeten zoeken van de vergelijking

$$w^2 + w + 1 = 0.$$

Echter uit deze laatste volgt:

$$w^3 - 1 = (w - 1)(w^2 + w + 1) = 0.$$

Dus we moeten op zoek naar elementen $w \in \mathbb{F}_q^*$ met de eigenschap $w \neq 1$ en $w^3 = 1$. Dus zijn we op zoek naar elementen $w \in \mathbb{F}_q^*$ met $\text{ord}(w) = 3$.

Altijd geldt $\text{ord}(w) \mid \#\mathbb{F}_q^* = q - 1 = 2^m - 1$.

Claim:

$$3 \mid 2^m - 1 \iff 2 \mid m \iff m \text{ is even.}$$

Bewijs: we moeten aantonen dat $2^m - 1 \pmod{3} \equiv 0$ precies dan als m even is. Dit is direct duidelijk uit het feit dat $2 \equiv -1 \pmod{3}$, dus $2^m \equiv (-1)^m \pmod{3}$. Wat we dus zien is, dat als m oneven, dan zijn er geen elementen $w \in \mathbb{F}_q^*$ met $\text{ord}(w) = 3$, immers als wel, dan zou $3 \mid 2^m - 1$, in tegenspraak met bovenstaande. In dat geval is A_3 dus gelijk aan 0. We beperken ons nu tot m even. Stel dat $w \in \mathbb{F}_q^*$ een element van orde 3 is, dat betekent:

$$w^3 = 1, \quad w \neq 1$$

ofwel: $w^2 + w + 1 = 0$ en dus is w een nulpunt (in \mathbb{F}_q^*) van het polynoom $X^2 + X + 1$. Dit polynoom heeft ten hoogste 2 nulpunten in \mathbb{F}_q^* (want het is een polynoom van graad 2). We maken nu gebruik van de volgende stelling uit de algebra:

Is G een eindige groep, en is p een priemgetal dat het aantal elementen van G deelt, dan bestaat er een element $g \in G$ met $\text{ord}(g) = p$.

Dit toepassende op $G = \mathbb{F}_q^*$ en $p = 3$ zien we dat er inderdaad een nulpunt, zeg w_1 , in \mathbb{F}_q^* , van het polynoom $X^2 + X + 1$ bestaat. Hieruit volgt

$$X^2 + X + 1 = (X - w_1) \cdot r(X)$$

waar r een polynoom in $\mathbb{F}_q^*[X]$ is van graad 1, dus er bestaan zelfs twee nulpunten in \mathbb{F}_q^* , zeg w_1 en w_2 . Verder zijn w_1 en w_2 verschillend, want als ze hetzelfde zouden zijn, dan impliceert uitschrijven van $X^2 + X + 1 = (X - w_1)(X - w_2)$ dat $w_1^2 = 1$, in tegenspraak met het feit dat $\text{ord}(w_1) = 3$. Laten we nu eerst naar w_1 kijken. Er geldt

$$\frac{x}{y} = w_1$$

en dus $x = w_1 y$. Met y gekozen ligt x dus vast en ook $z = x + y = (w_1 + 1)y$. Als $y \in \mathbb{F}_q^*$ dan geldt

- $0 \neq x \neq y$: De eerste gelijkheid is triviaal. Stel $x = y$ dan geldt $y = w_1 y$ en dus $1 = y \cdot y^{-1} = w_1$, tegenspraak.
- $z \neq 0$, want als $z = 0$, dan $x = y$ en dat was niet zo, getuige het eerste item.
- $x \neq z \neq y$ Immers, als b.v. $x = z$ dan geldt $y = 0$, tegenspraak.

Dus elke $y \in \mathbb{F}_q^*$ correspondeert met een woord van lengte 3 in onze code $M(m)$. Dit geeft $q - 1 = 2^m - 1$ stuks. Voor w_2 geldt een analoog verhaal. Tezamen geeft dit $2 \cdot (2^m - 1)$ woorden. Echter de eerste index hebben we geassocieerd met x , de tweede met y en de derde met z , terwijl dit volstrekt willekeurig was. Met andere woorden: we moeten het gevonden resultaat nog delen door het aantal manieren waarop we drie elementen over drie plaatsen kunnen verdelen en dat zijn er $3! = 6$. Met andere woorden

$$A_3 = \begin{cases} 0 & \text{voor } m \text{ even;} \\ \frac{2^m - 1}{3} & \text{voor } m \text{ oneven.} \end{cases}$$

Tenslotte nog $\#v : w(v) = 4$.

Dit correspondeert met $x, y, z, w \in \mathbb{F}_q^*$, onderling verschillend, met

$$x + y + z + w = 0 \tag{10}$$

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} = 0. \tag{11}$$

Uit (10) volgt, analoog aan bovenstaande, $w = x + y + z$ en dus

$$\begin{aligned} \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{x + y + z} &= 0 \\ \iff \\ \frac{yz + xz + xy}{xyz} &= \frac{1}{x + y + z}. \end{aligned}$$

Hieruit zien we:

$$xyz = xyz + x^2z + x^2y + y^2z + xyz + xy^2 + yz^2 + xz^2 + xyz.$$

Dus

$$\begin{aligned} 0 &= x^2y + xyz + xy^2 + y^2z + x^2z + xz^2 + xyz + yz^2 \\ &= (x^2 + xz + xy + yz)(y + z) \\ &= (x + y)(x + z)(y + z). \end{aligned}$$

Er zou dan moeten gelden $x = y$, $x = z$ of $y = z$, in tegenspraak met het gestelde dat x , y en z onderling verschillend moeten zijn. Hiermee is bewezen dat ook $A_4 = 0$.

3.5 Een niet-binaire BCH-code

We kijken tenslotte in dit hoofdstuk naar een code over \mathbb{F}_p , namelijk $C := BCH_p(1)$. In sommige literatuur wordt dit een Reed-Solomon code genoemd; op dit soort codes komen we in het volgende hoofdstuk nog terug. We herhalen eerst de definitie van C . Neem p een priemgetal. *We zullen er voor het gemak steeds van uitgaan, dat $p > 3$.* Laat β een voortbrenger zijn van de cyclische groep \mathbb{F}_p^* , dan is C de code over \mathbb{F}_p gegeven door

$$C = \left\{ (a_1, a_2, \dots, a_{p-1}) \mid \sum_{i=1}^{p-1} a_i \beta^i = \sum_{i=1}^{p-1} a_i \beta^{3i} = 0 \right\}.$$

We willen de gewichtsverdeling van de code C bepalen.

Dit gaat als volgt.

Allereerst merken we op dat

$$C^\perp = \langle (\beta, \beta^2, \dots, \beta^{p-1}), (\beta^3, \beta^6, \dots, \beta^{3(p-1)}) \rangle$$

een lineaire code over \mathbb{F}_p is met dimensie $\dim_{\mathbb{F}_p} C^\perp = 2$.

Immers, daar p priem en $p \geq 5$, is $p \neq 1, 2$, en 3 . Verder geldt

$$\det \begin{pmatrix} 1 & 1 \\ \beta & \beta^3 \end{pmatrix} = \beta^3 - \beta = 0 \iff \beta^2 = 1$$

Hieruit zou volgen $ord(\beta) \mid 2$ en dus $ord(\beta) \leq 2$, in tegenspraak met het feit dat $ord(\beta) = p - 1 \geq 3$. Dus de vectoren $(1, \beta)^t$ en $(1, \beta^3)^t$ zijn lineair onafhankelijk, waarmee het gestelde bewezen is.

We zien dus dat $\#C^\perp = p^2$. Stel nu dat

$$W_{C^\perp}(x) = \sum_{i=0}^{p-1} a_i x^i$$

dan is

$$W_C(x) = \frac{1}{\#C^\perp} \sum_{i=0}^{p-1} a_i (1-x)^i (1+(p-1)x)^{p-1-i} \quad (*)$$

We maken in het vervolg gebruik van de volgende twee lemma's:

Lemma 3.5.1 *Als p priem en $x \in \mathbb{F}_p^*$ met $x^2 = 1$, dan volgt $x = -1$ of $x = 1$.*

Bewijs. $x^2 = 1 \implies x^2 - 1 = 0 \implies p \mid x^2 - 1 = (x-1)(x+1)$. Dus $p \mid x-1$ of $p \mid x+1$. Hieruit volgt $x = 1$ of $x = -1$. \square

Lemma 3.5.2 *Als p priem, dan bevat \mathbb{F}_p^* precies $\frac{p-1}{2}$ kwadraten.*

Bewijs. Beschouw de afbeelding

$$f : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$$

gedefinieerd door

$$f(x) = x \cdot x = x^2$$

Deze f is een homomorfisme, immers $f(1) = 1$ en $f(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$ voor alle $x, y \in \mathbb{F}_p^*$. Verder geldt dat als $x \in \ker(f)$, dan $f(x) = 1$ en dus $x^2 = 1$. Uit lemma 3.5.1 volgt dan dat $\ker(f) = \{-1, 1\}$, dus

$$\# \text{ beeld } (f) = \frac{p-1}{2}$$

waarmee het gestelde is bewezen. \square

Een woord v in de code C^\perp ziet eruit als

$$v = (a\beta + b\beta^3, a\beta^2 + b\beta^6, \dots, a\beta^{p-1} + b\beta^{3(p-1)}) \quad \text{voor zekere } a, b \in \mathbb{F}_p.$$

We onderscheiden nu een tweetal gevallen:

$b = 0$. In dit geval ziet v eruit als

$$v = (a\beta, a\beta^2, \dots, a\beta^{p-1})$$

en dit woord heeft gewicht

$$\begin{cases} 0 & \text{als } a = 0 \\ p-1 & \text{als } a \neq 0, \end{cases}$$

immers als $a \neq 0$, dan geldt per definitie van een *lichaam* dat $a\beta^k \neq 0$ voor iedere $k \in \{1, 2, \dots, p-1\}$. Bovendien zijn er precies $p-1$ elementen ongelijk aan 0 in \mathbb{F}_p . Dus we hebben, met $b = 0$, precies één woord van gewicht 0 en $p-1$ woorden van gewicht $p-1$.

$b \neq 0$. Als $a = 0$, dan krijgen we analoog aan bovenstaande $p-1$ woorden van gewicht $p-1$.

Als $a \neq 0$, dan mogen en zullen we schrijven

$$v = (ax + bx^3)_{x \in \mathbb{F}_p^*}.$$

We willen nu tellen hoeveel van de $ax + bx^3$ ongelijk aan 0 zijn. Welnu, als $ax + bx^3 = 0$, dan volgt, daar $b \neq 0$ en $x \neq 0$, dat

$$\frac{a}{b} + x^2 = 0, \quad \text{oftewel} \quad x^2 = -\frac{a}{b}.$$

– Als $-\frac{a}{b}$ een kwadraat is, dan is

$$-\frac{a}{b} = \alpha^2$$

voor een of andere $\alpha \in \mathbb{F}_p^*$. In dit geval zijn er twee oplossingen van de vergelijking $x^2 = \alpha^2$, namelijk $x = \pm\alpha$, immers

$$x^2 = \alpha^2 \iff \left(\frac{x}{\alpha}\right)^2 = 1 \stackrel{\text{Lemma 3.5.1}}{\implies} \frac{x}{\alpha} = \pm 1.$$

Met andere woorden: Ons woord v heeft in dit geval gewicht $p-3$. Verder weten we uit Lemma 3.5.2 dat er $\frac{p-1}{2}$ kwadraten zijn. Als we dan α hebben gekozen, dan is $a = -b\alpha$. Kiezen we verder ook b nog, dan ligt a vast. In totaal hebben we dus

$$\underbrace{(p-1)}_{\# \text{keuzes voor } b} \cdot \underbrace{\frac{p-1}{2}}_{\# \text{keuzes voor de kwadraten}} \text{ woorden van lengte } p-3.$$

– Als $-\frac{a}{b}$ geen kwadraat is, dan heeft de vergelijking

$$x^2 = -\frac{a}{b}$$

geen oplossing, en dus hebben we ook $\frac{(p-1)^2}{2}$ woorden van gewicht $p-1$ (Lemma 3.5.2 zegt ook: Er zijn $\frac{p-1}{2}$ niet-kwadragen!!).

Conclusie:

$$\begin{aligned} W_{C^\perp}(x) &= 1 + \frac{(p-1)^2}{2}x^{p-3} + \left((p-1) + (p-1) + \frac{(p-1)^2}{2} \right) x^{p-1} \\ &= 1 + \frac{(p-1)^2}{2}x^{p-3} + \frac{(p-1)(p+3)}{2}x^{p-1}. \end{aligned}$$

Een kleine controle leert dat de som van de coëfficiënten gelijk is aan $p^2 = \#C^\perp$, zoals het zijn moet. Met behulp van (*) kunnen we nu de gewichtsverdeling van de code C schrijven als $W_C(x) =$

$$\begin{aligned} &= \frac{1}{p^2} \sum_{i=0}^{p-1} a_i (1-x)^i (1+(p-1)x)^{p-1-i} \\ &= \frac{1}{p^2} \left\{ (1+(p-1)x)^{p-1} + \frac{(p-1)^2}{2} (1-x)^{p-3} (1+(p-1)x)^2 + \frac{(p-1)(p+3)}{2} (1-x)^{p-1} \right\} \\ &= \frac{1}{p^2} \left\{ \begin{aligned} &\sum_{i=0}^{p-1} \binom{p-1}{i} (p-1)^i x^i \\ &+ \\ &\frac{(p-1)^2}{2} (1+2(p-1)x+(p-1)^2x^2) \sum_{i=0}^{p-3} \binom{p-3}{i} (-1)^i x^i \\ &+ \\ &\frac{(p-1)(p+3)}{2} \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^i x^i \end{aligned} \right\}. \end{aligned}$$

De code C blijkt minimale afstand $d_{min} = 2$ te hebben, zoals zowel uit bovenstaande formule als uit een directe berekening te halen is. Er zijn precies $(p-1)^2/2$ woorden met gewicht 2 in C .

4 Goede codes

Zij $C \subset \mathbb{F}_q^n$ een code. De relevante parameters ervan worden geschreven als (lengte= n , # woorden= M , min. afstand= d). Is bijvoorbeeld C een lineaire $[n, k, d]$ -code, dan zijn deze parameters (n, q^k, d) . Je kunt nu proberen om bij vaste n en d het maximale aantal codewoorden te vinden; dit hangt uiteraard ook van q af.

Definitie 4.0.3 Voor $n \in \mathbb{Z}_{\geq 1}$ en $r \in \mathbb{R}_{\geq 0}$ is $A(n, r)$ gedefiniëerd als het maximale aantal woorden in een code van lengte n over \mathbb{F}_q met de eigenschap $d_{\min} \geq r$.

Verder is het interessant om een soort maximale informatiedichtheid bij een gegeven minimale afstand te definiëren, en te kijken hoe groot die kan zijn voor $n \rightarrow \infty$. Dit leidt tot het volgende.

Definitie 4.0.4 Voor $0 \leq \delta \leq 1$ schrijven we $\alpha(\delta) := \limsup_{n \rightarrow \infty} \frac{q \log A(n, \delta n)}{n}$.

Hier kan je als volgt aan denken. In een woord van lengte n zullen, afhankelijk van de kwaliteit van het kanaal waarover je het verstuurt, in de regel hoogstens een bepaalde fractie van de n letters foutief aankomen. Het getal δ in bovenstaande definitie is een bovengrens voor deze fractie. Het is dus een maat voor de kwaliteit van het kanaal waarover we gegevens versturen. Bij een gegeven δ kijken we vervolgens naar de maximale informatiedichtheid van codes van lengte n en $d_{\min} \geq \delta n$, en tenslotte wordt voor $n \rightarrow \infty$ een grootste limietpunt genomen. Er geldt dan dat $\alpha(\delta) \leq 1$, en hoe groter dit getal is voor een gegeven waarde van δ , hoe gunstiger de informatiedichtheid zal zijn van zekere families van codes met groeiende lengte en bepaalde, proportioneel met die lengte groeiende minimale afstand.

4.1 Onder- en bovengrens van $\alpha(\delta)$

We beginnen met een eerste afschatting.

Stelling 4.1.1 Er geldt $\alpha(\delta) \leq 1 - \delta$.

Bewijs. Beschouw een (n, M, d) -code C . Laat nu de laatste $d-1$ coördinaten weg. De zo verkregen code C' is dan een $(n-d+1, M, \geq 1)$ -code, dus $M \leq q^{n-d+1}$. Hieruit volgt dat $A(n, d) \leq q^{n-d-1}$, en daarmee $\frac{q \log A(n, d)}{n} \leq \frac{n-d+1}{n} \rightarrow 1 - \delta$. \square

Stelling 4.1.2 (Plotkin) Er geldt

$$\alpha(\delta) \leq \begin{cases} 1 - \frac{\delta}{1-1/q} & \text{als } \delta \leq 1 - \frac{1}{q}; \\ 0 & \text{als } \delta \geq 1 - \frac{1}{q}. \end{cases}$$

Bewijs. Neem een (n, M, d) code C , en schrijf $C = \{v_1, \dots, v_M\}$.

Beschouw dan $\sum_{v_1 \neq v_2} d(v_1, v_2)$, de som van alle geordende paren elementen in C (dus elk paar elementen levert 2 bijdragen aan de som). Het aantal paren dat een bijdrage $\neq 0$ levert is $M \cdot (M-1)$, dus de som is $\geq M \cdot (M-1) \cdot d$. Als je alle elementen van C onder elkaar schrijft, kun je dit opvatten als een matrix.

Neem daar een kolom van en stel $m(\alpha) := \#$ keer α in de kolom. Je hebt dan dus $M - m(\alpha)$ elementen $\neq \alpha$, dus de kolom draagt $\sum_{\alpha \in \mathbb{F}_q} m(\alpha)(M - m(\alpha)) = M \sum_{\alpha} m(\alpha) - \sum_{\alpha} m(\alpha)^2 = M^2 - \sum_{\alpha} m(\alpha)^2$ bij aan $\sum_{v_1 \neq v_2} d(v_1, v_2)$.

Beschouw nu in \mathbb{Z}^q de vectoren $a = (m(\alpha_1), \dots, m(\alpha_q))$ en $b = (1, \dots, 1)$, dan volgt met Cauchy-Schwartz: $\|a\|^2 \cdot \|b\|^2 \geq \langle a, b \rangle^2$, oftewel $\sum_{\alpha} m(\alpha)^2 \cdot q \geq (\sum_{\alpha} m(\alpha))^2 = M^2$. Dus de bijdrage van onze kolom is

$$M^2 - \sum_{\alpha} m(\alpha)^2 \leq M^2 - M^2/q.$$

Nu is $\sum_{v_1 \neq v_2} d(v_1, v_2)$ gelijk aan de bijdragen van alle kolommen gesommeerd, en omdat er n kolommen zijn is dit

$$\leq n \cdot \left(1 - \frac{1}{q}\right) \cdot M^2.$$

Schrijven we $\theta = \left(1 - \frac{1}{q}\right)$, dan volgt nu dus: $M(M-1)d \leq nM^2\theta$, oftewel $M \leq 1 + \frac{n\theta}{d}M$. Dit kunnen we schrijven als $M\left(1 - \frac{n\theta}{d}\right) \leq 1$. De conclusie is, dat als $n\theta < d$, dan $M \leq \frac{d}{d-n\theta}$. Dus dan $\alpha(\delta) \leq \limsup_{n \rightarrow \infty} \frac{q \log\left(\frac{\delta n}{\delta n - n\theta}\right)}{n} = \limsup_{n \rightarrow \infty} \frac{q \log\left(\frac{\delta}{\delta - \theta}\right)}{n} = 0$, en daarmee $\alpha(\delta) = 0$ voor $\delta > \theta$.

Stel nu dat C een (n, M, d) code is met $d < n\theta$. We gaan een af-schatting voor M bepalen, door een nieuwe code te maken waarvoor wel $d > n\theta$. Kies $n' = \lfloor \frac{d-1}{\theta} \rfloor$ (Hier is voor r een reëel getal $\lfloor r \rfloor$ de *entier* van r , dat is de grootste $k \in \mathbb{Z}$ met $k \leq r$). Er geldt dan $n'\theta = \lfloor \frac{d-1}{\theta} \rfloor \theta \leq d-1 < d$. Kies nu een $w \in C$, dan kun je een nieuwe code maken, waarbij de codewoorden uit de eerste n' coëfficiënten bestaan van alle codewoorden in C die dezelfde laatste $(n - n')$ coëfficiënten als w hebben. Dit wordt dan een (n', M', d') -code, met $d' \geq d > n'\theta$. Nu volgt dus $M' \leq \frac{d}{d-n'\theta}$.

Er zijn $q^{n-n'}$ mogelijke 'staartstukken' (laatste $n - n'$ coëfficiënten), elk behorend bij maximaal $\frac{d}{d-n'\theta}$ woorden, dus $M \leq q^{n-n'} \cdot \frac{d}{d-n'\theta}$. Hieruit volgt

$$\alpha(\delta) \leq \lim_{n \rightarrow \infty} \frac{q \log(q^{n-n'}) \cdot \frac{\delta n}{\delta n - n'\theta}}{n} = \lim_{n \rightarrow \infty} \frac{n - n' + q \log\left(\frac{\delta}{(\delta - n'\theta)/n}\right)}{n} = 1 - \frac{\delta}{\theta}.$$

Voor het laatste gelijkteken gebruiken we dat $\frac{\delta n - 1 - \theta}{\theta} \leq n' \leq \frac{\delta n - 1}{\theta}$, oftewel dat $\frac{\delta n - 1}{\delta n} \leq \frac{\theta n'}{\delta n} \leq \frac{\delta n - 1 - \theta}{\delta n}$, dus $\frac{1}{\delta n} \leq 1 - \frac{\theta n'}{\delta n} \leq \frac{1 + \theta}{\delta n}$. Hieruit volgt $\frac{\log\left(\frac{1}{\delta n}\right)}{n} \leq$

$\frac{\log(1-\frac{\theta n'}{\delta n})}{n} \leq \frac{\log(\frac{1+\theta}{\delta n})}{n}$. De buitenste twee gaan naar 0 voor $n \rightarrow \infty$, want $\lim_{x \rightarrow 0} x \log(x) = 0$. En daarmee convergeert ook de middelste term naar 0. \square

Vervolgens gaan we een ondergrens voor $\alpha(\delta)$ bepalen. Merk op, dat we al weten dat $\alpha(\delta) = 0$ voor $\delta \geq 1 - 1/q$.

Stelling 4.1.3 (Gilbert-Varshamov) Voor $\delta \leq 1 - 1/q$ geldt

$$\alpha(\delta) \geq 1 + \delta \log \delta + (1 - \delta) \log(1 - \delta) - \delta \log(q - 1),$$

waarin de logaritme ($\log = {}^q\log$) is.

Bewijs. Beschouw een (n, M, d) -code C met M maximaal, d.w.z. C is niet uit te breiden tot een $(n, M + 1, d)$ -code. Dan geldt dus voor elke $v \notin \mathbb{F}_q^n$ dat $d(v, c) \leq d - 1$ voor een $c \in C$. Dit betekent, dat $\bigcup_{c \in C} B_{d-1}(c) = \mathbb{F}_q^n$, waarin $B_{d-1}(c) := \{v \in \mathbb{F}_q^n \mid d(v, c) \leq d - 1\}$.

Kennelijk is dus $q^n \leq \sum_{c \in C} \#B_{d-1}(c)$.

Het aantal elementen van $B_{d-1}(c)$ is onafhankelijk van c , want er is een bijectie tussen $B_{d-1}(c)$ en $B_{d-1}(0)$, namelijk de translatie over $-c$. Er geldt $\#B_{d-1}(0) = 1 + \binom{n}{1} \cdot (q - 1) + \dots + \binom{n}{d-1} \cdot (q - 1)^{d-1}$, want er is 1 element dat op 0 plaatsen van $(0, \dots, 0)$ verschilt, er zijn er $\binom{n}{1}(q - 1)$, die op precies 1 plaats van de nulvector verschillen (n keuzes voor de plek en dan $q - 1$ voor het element van \mathbb{F}_q^* dat we op die plek zetten), enzovoort.

Er volgt dus

$$q^n \leq \sum_{c \in C} \#B_{d-1}(c) = M \cdot \sum_{i=0}^{d-1} \binom{n}{i} \cdot (q - 1)^i.$$

Door dit te herschrijven, volgt

$$\alpha(\delta) = \limsup_{n \rightarrow \infty} \frac{{}^q \log A(n, \delta n)}{n} \geq \lim_{n \rightarrow \infty} \frac{n - {}^q \log \left(\sum_{i < \delta n} \binom{n}{i} \cdot (q - 1)^i \right)}{n}.$$

We zullen laten zien dat voor $\delta \leq \theta = 1 - 1/q$ deze limiet bestaat, en gelijk is aan het rechterlid zoals gegeven in de stelling.

Beschouw de som $\sum_{i < \delta n} \binom{n}{i} \cdot (q - 1)^i$. Hierin is de maximale term die bij de grootst mogelijke waarde voor i , want: $\binom{n}{i-1} \cdot (q - 1)^{i-1} \leq \binom{n}{i} \cdot (q - 1)^i \iff \frac{1}{n-i+1} \leq \frac{q-1}{i} \iff i \leq (q-1) \cdot (n-i+1) = (n+1) \cdot (q-1) - i \cdot (q-1) \iff iq \leq (n+1) \cdot (q-1) \iff i \leq (n+1) \cdot \theta$, en aan deze voorwaarde op i is bij ons voldaan omdat

$$i < \delta n \leq \theta n < \theta \cdot (n + 1).$$

Schrijven we $d - 1$ voor het grootste gehele getal $< \delta n$, dan concluderen we

$$\binom{n}{d-1} \cdot (q-1)^{d-1} \leq \#B_{d-1}(0) \leq d \cdot \binom{n}{d-1} \cdot (q-1)^{d-1}.$$

We willen $\lim_{n \rightarrow \infty} ({}^q\log(\#B_{d-1}(0)))/n$ bepalen, en dit kan met de zojuist gevonden afchatting. Deze geeft links en rechts dezelfde limiet, want rechts is $\frac{{}^q\log(d)}{n}$ meer en dat gaat toch naar nul. De limiet wordt dus (met de linker):

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{{}^q\log\left(\binom{n}{d-1} \cdot (q-1)^{d-1}\right)}{n} &= \lim_{n \rightarrow \infty} \left(\frac{{}^q\log\left(\binom{n}{d-1}\right)}{n} + \frac{(d-1) \cdot {}^q\log(q-1)}{n} \right) \\ &= \lim_{n \rightarrow \infty} \frac{{}^q\log\left(\binom{n}{d-1}\right)}{n} + \delta \cdot {}^q\log(q-1). \end{aligned}$$

Hierin gebruiken we onder meer dat $\lim_{n \rightarrow \infty} n/d = \delta$, immers $d - 1 \leq \delta n < d \leq \delta n + 1$. Nu gaan we de resterende term uitrekenen. Er geldt

$$\begin{aligned} {}^q\log\left(\binom{n}{d-1}\right) &= {}^q\log(n!) - {}^q\log((d-1)!) - {}^q\log((n-d+1)!) \\ &= \sum_{i=1}^n {}^q\log i - \sum_{i=1}^{d-1} {}^q\log i - \sum_{i=1}^{n-d+1} {}^q\log i \\ &= \sum_{i=1}^{n-d+1} {}^q\log\left(1 + \frac{d-1}{i}\right). \end{aligned}$$

We kunnen dan de uitdrukking waarvan we de limiet willen bepalen, benaderen door

$$(1/n) \int_1^{n-d} {}^q\log(1 + (d-1)/x) dx.$$

De integraal hierin is met wat rekenwerk expliciet te bepalen; er komt uit

$$(1-d) {}^q\log\left(\frac{d-1}{n-d}\right) + (n-1) {}^q\log\left(\frac{n-1}{n-d}\right) + (d-1) {}^q\log(d-1) - d {}^q\log(d).$$

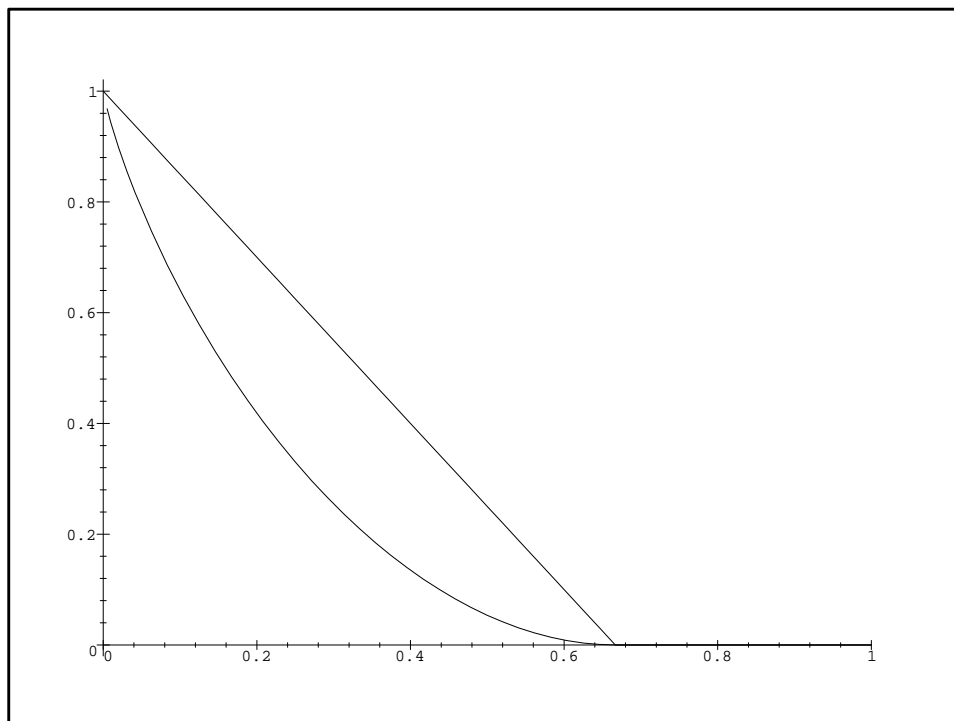
De fout die gemaakt wordt door de som door een integraal te vervangen, blijkt voor $n \rightarrow \infty$ naar een eindige limiet te gaan, dus bij deling door n gaat deze zelfs naar nul. Het is niet moeilijk om te berekenen dat bovenstaande expressie gedeeld door n , voor $n \rightarrow \infty$ convergeert naar

$$-\delta \cdot {}^q\log(\delta) - (1-\delta) \cdot {}^q\log(1-\delta).$$

Uit deze berekeningen volgt tenslotte, dat

$$\lim_{n \rightarrow \infty} \frac{{}^q\log(\#B_{d-1}(0))}{n} = -\delta \cdot {}^q\log \delta - (1-\delta) \cdot {}^q\log(1-\delta) + \delta \cdot {}^q\log(q-1),$$

waarmee we de genoemde ondergrens voor $\alpha(\delta)$ hebben gevonden. \square



Onder- en bovengrens voor $\alpha(\delta)$ bij $q = 3$.

4.2 De Reed-Solomon codes

In CD's wordt gebruik gemaakt van een Reed-Solomon code. Dit is een voorbeeld van een code met $\frac{d}{n}$ "groot".

We weten dat $\mathbb{F}_q^* = \langle \beta \rangle$ voor zekere β . Kies $1 \leq m \leq q-1$, dan:

Definitie 4.2.1 De Reed-Solomon-code $RS_{q,\beta}(m)$ wordt gedefiniëerd als

$$\left\{ (a_0, \dots, a_{q-2}) \in \mathbb{F}_q^{q-1} \mid \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 1 & \beta^2 & \beta^4 & \dots & \\ \vdots & & & & \vdots \\ 1 & \beta^m & \beta^{2m} & \dots & \beta^{m(q-2)} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_{q-2} \end{pmatrix} = 0 \right\}.$$

De code $RS_{q,\beta}(m)$ is, opgevat als deelverzameling van $\mathbb{F}_q[X]/(X^{q-1} - 1)$, gelijk aan het ideaal $(\text{kgv}((X - \beta), \dots, (X - \beta^m)) \bmod (X^{q-1} - 1))$, want $f := a_0 + a_1X + \dots + a_{q-2}X^{q-2}$ correspondeert met een codewoord precies dan, als β, \dots, β^m allemaal nulpunten van f zijn, dus als f een veelvoud is van het genoemde kleinste gemene veelvoud. Omdat β, \dots, β^m allemaal verschillend zijn, geldt $\text{kgv}((X - \beta), \dots, (X - \beta^m)) = \prod_{i=1}^m (X - \beta^i)$, dus

$\dim RS_{q,\beta}(m) = q - 1 - m$.

Dit is ook op een andere manier in te zien. Schrijf B voor de matrix die in de definitie van $RS_{q,\beta}(m)$ voorkomt. Door $q - 1 - m$ willekeurige kolommen uit B weg te laten krijg je een vierkante matrix van de vorm

$$X = \begin{pmatrix} x_1 & \cdots & x_m \\ \vdots & & \vdots \\ x_1^m & \cdots & x_m^m \end{pmatrix}$$

Zo'n zogeheten *Vandermonde matrix* heeft altijd volle rang als de x_i verschillend en $\neq 0$ zijn (en dat zijn ze in ons geval). Dit is als volgt in te zien. X heeft volle rang als de determinant van $X \neq 0$ is, ofwel als $\det(X') \neq 0$, met X' de matrix verkregen door voor elke i de i^e -kolom door x_i te delen.

De afbeelding $\mathcal{P}_{m-1}(F) \rightarrow F^m$ (waarin met $\mathcal{P}_{m-1}(F)$ de vectorruimte bestaande uit alle polynomen met graad $\leq m - 1$ wordt aangeduid), gegeven door $f \mapsto (f(x_1), \dots, f(x_m))$, is surjectief, want er zijn legendre-polynomen die als beeld de standaard basisvectoren van F^m hebben. Dit impliceert, omdat beide vectorruimten dezelfde dimensie hebben, dat het een isomorfisme is. In het bijzonder vormen de beelden van de elementen uit de basis $1, x, \dots, x^{m-1}$ van $\mathcal{P}_{m-1}(F)$ een basis voor F^m . Dit zijn precies de kolommen van X' , dus X' en daarmee ook X heeft determinant $\neq 0$.

Uit het voorgaande volgt dat B zeker ook volle rang heeft, en met de dimensie-formule volgt dan dat de dimensie van de code (die de kern is van de matrix-afbeelding) $q - 1 - m$ is.

We weten nu dat $RS_{q,\beta}(m)$ een $[q-1, q-1-m, d]$ code is, waarbij d nog moet worden bepaald. Er geldt algemeen voor een $[n, k, d]$ -code dat $k \leq n - d + 1$, dus in ons geval $d \leq (q - 1) - (q - 1 - m) + 1 = m + 1$. Beschouw een woord v , met (minimale) afstand d tot $(0, \dots, 0)$. Stel dat de coëfficiënten $\neq 0$ staan op de plaatsen n_1, \dots, n_d . Dan zit $v' = (v_{n_1}, \dots, v_{n_d})$ in de kern van de matrix B' , verkregen door alleen de kolommen n_1, \dots, n_d uit B te nemen. B' is dan een $m \times d$ matrix, met maximale rang (dit gaat precies zo als bij B). Als zou gelden $d \leq m$, dan is die rang d , gelijk aan het aantal kolommen van B' . Maar dat is in tegenspraak met het feit dat v' in de kern van B' zit. Dus volgt: $d = m + 1$, dus $RS_{q,\beta}(m)$ is een $[q - 1, q - 1 - m, m + 1]$ code. Samengevat, hebben we het volgende over deze Reed-Solomon codes bewezen.

Stelling 4.2.2 *De Reed-Solomon-code $RS_{q,\beta}(m)$ is een MDS-code met parameters $[q - 1, q - 1 - m, m + 1]$.*

Helaas kun je zo bij een vast grondlichaam \mathbb{F}_q , alleen een code van lengte $q - 1$ maken, terwijl juist gewenst is dat je codes van willekeurig grote lengte kunt maken.

4.3 Goppa-codes over \mathbb{P}^1

Neem een lichaam K dat perfect is (dat wil zeggen elk irreducibel polynoom in $K[X]$ heeft ggd 1 met zijn afgeleide). De projectieve lijn \mathbb{P}^1 is gedefinieerd als $\mathbb{P}^1 := \{(x : y) \mid x, y \in \overline{K}, (x : y) \neq (0 : 0)\}$, waarbij verder $(x : y) = (v : w)$ als $(x, y) = \lambda(v, w)$ voor zekere $\lambda \in \overline{K}$.

Beschouw $\frac{a(t)}{b(t)} \in K(t)$. Zo'n rationale functie kan opgevat worden als een (niet overal gedefinieerde) functie op \mathbb{P}^1 . Vul daartoe $\frac{x}{y}$ in voor t . Dit levert $\frac{a(\frac{x}{y})}{b(\frac{x}{y})} = \frac{y^n}{y^n} \cdot \frac{a(\frac{x}{y})}{b(\frac{x}{y})} = \frac{A(x,y)}{B(x,y)}$, waarbij $n = \max(\text{gr}(a), \text{gr}(b))$.

Deze $\frac{A}{B}$ is nu goed gedefinieerd op bijna alle punten van \mathbb{P}^1 , want $\frac{A(\lambda x, \lambda y)}{B(\lambda x, \lambda y)} = \frac{A(x,y)}{B(x,y)}$. (Dit volgt uit het feit dat A en B homogeen en van dezelfde graad zijn; een polynoom heet homogeen als al zijn termen dezelfde totale graad hebben.)

Definitie 4.3.1 Voor een irreducibel, monisch polynoom $P \in K[X]$, en een $r \in K(X)$ schrijven we

$$\text{ord}_P(r) := \#P \text{ in teller} - \#P \text{ in noemer.}$$

Omdat zo'n monisch en irreducibel polynoom P volledig wordt bepaald door z'n nulpunten in $\alpha_1, \dots, \alpha_n \in \overline{K}$, wordt ook wel geschreven $\text{ord}_{\alpha_i}(r)$. Wij willen nu bovenstaande definitie zo aanpassen dat we er ook de orde van rationale functies in een punt van \mathbb{P}^1 mee beschrijven. Daartoe moet je in plaats van monische irreducibele $P \in K[X]$ (corresponderend met hun nulpunten $\alpha \in \overline{K}$), monische irreducibele *homogene* polynomen in $K[X, Y]$ nemen. Deze worden ook bepaald door hun nulpunten. Het polynoom $\prod_i (x - \alpha_i)$ in $K[x]$ met nulpunten α_i correspondeert dan met het homogene polynoom $\prod_i (x - \alpha_i y)$ met nulpunten $(\alpha_i : 1) \in \mathbb{P}^1$. En er is dan ook nog het polynoom y , met nulpunt $(1 : 0)$.

Als we met $r = \frac{a}{b}$ zoals hierboven $\frac{A}{B}$ associëren, en met $\alpha \in \overline{K}$ het irreducibele polynoom $P := f_K^\alpha$ en $Q \in K[x, y]$ de homogeen gemaakte P , dan is

$$\text{ord}_\alpha(r) = \text{ord}_P(a/b) = \text{ord}_Q(A/B),$$

waarin ord_Q volkomen analoog aan ord_P wordt gedefiniëerd. Dus zo krijgen we het begrip 'orde van een rationale functie in een punt $(\alpha : 1)$ van \mathbb{P}^1 '. Evenzo correspondeert het resterende punt $(1 : 0)$ met het irreducibele polynoom y , en $\text{ord}_y(A/B) = \text{ord}_y(A) - \text{ord}_y(B) = -\text{gr}(r) = -\text{gr}(a) + \text{gr}(b)$.

Definitie 4.3.2 Een divisor D op \mathbb{P}^1 is een eindige formele som $D = \sum n_P [P]$ waarin de $n_P \in \mathbb{Z}$, en de som wordt genomen over (monische) irreducibele homogene polynomen in $K[X, Y]$.

De graad van zo'n divisor wordt gedefiniëerd als $\text{deg}(D) := \sum n_P \cdot \text{gr}(P)$.

Hierin zijn de $[P]$ gewoon symbolen. Het woord monisch betekent gewoon monisch als polynoom in X , als X tenminste voorkomt. Het enige polynoom dat wordt beschouwd waar geen X in voorkomt, is Y .

We gaan nu met een functie $\frac{A}{B}$ een divisor associëren.

Definitie 4.3.3 Voor een functie $r \in K(t)$ als eerder beschouwd, met de eigenschap $r \neq 0$, en met bijbehorende homogene polynomen A, B schrijven we $\text{div}(r) := \sum_P \text{ord}_P(\frac{A}{B})[P]$.

Merk op dat dit inderdaad een eindige som is, want in A, B komen maar eindig veel irreducibele factoren voor.

Lemma 4.3.4 Voor $r \in K(t)^*$ geldt $\deg(\text{div}(r)) = 0$.

Bewijs. Als r correspondeert met A/B voor homogene polynomen A, B , dan is de gevraagde graad gelijk aan $\sum \text{ord}_P(\frac{A}{B}) \cdot \text{gr}(P)$, en dit is dus de graad van de teller min de graad van de noemer, dus nul. \square

Definitie 4.3.5 Gegeven een divisor D , dan schrijven we $L(D) := \{r \in K(t)^* \mid \text{div}(r) + D \text{ heeft alleen coëfficiënten } \geq 0\} \cup \{0\}$.

Na al deze begrippen uit de meetkunde, komen we eindelijk weer terug bij codes. Kies daartoe een divisor D , en punten $p_1, \dots, p_n \in \mathbb{P}^1(K) := \{(a : b) \in \mathbb{P}^1 \mid a, b \in K\}$ waarbij de p_i niet voorkomen in D . Hiermee wordt bedoeld dat het bijbehorende polynoom (dit is bij $p = (a : b)$ het, eventueel monisch gemaakte, polynoom $bX - aY$), niet voorkomt als polynoom met coëfficiënt $\neq 0$ in D . Dan:

Definitie 4.3.6 De Goppa-code bij p_1, \dots, p_n en D is

$$C(p_1, \dots, p_n, D) := \{(r(p_1), \dots, r(p_n)) \mid r \in L(D)\}.$$

Merk op, dat de schrijfwijze “ $r = A/B$ ” zo te kiezen is, dat p_i geen nulpunt is van B . Dit volgt uit de definitie van $L(D)$ plus het feit, dat p_i niet voorkomt in D . Hieruit volgt, dat de Goppa code goed gedefinieerd is.

Stelling 4.3.7 $L(D)$ en $C(p_1, \dots, p_n, D)$ zijn vectorruimten over K .

Bewijs. In het bewijs dat $L(D)$ een vectorruimte is, is het enige dat niet onmiddellijk duidelijk is: $r_1, r_2 \in L(D) \Rightarrow r_1 + r_2 \in L(D)$.

Als $r_i \in L(D)$, dan $\text{div}(r_i) + D \geq 0$ (waarmee bedoeld wordt dat er geen coëfficiënten < 0 zijn). Er geldt echter $\text{ord}_P(r_1 + r_2) \geq \min(\text{ord}_P(r_1), \text{ord}_P(r_2))$, dus dan ook $\text{div}(r_1 + r_2) + D \geq 0$, dus $r_1 + r_2 \in L(D)$. Er volgt dat $L(D)$ een vectorruimte is.

Nu het bewijs voor $C(p_1, \dots, p_n, D)$. Beschouw de afbeelding $L(D) \rightarrow K^n$, gegeven door $r \mapsto (r(p_1), \dots, r(p_n))$. Deze afbeelding is duidelijk lineair, dus het beeld ervan is ook een vectorruimte. En dit beeld is precies $C(p_1, \dots, p_n, D)$. \square

Voorbeeld 4.3.8 Neem $K = \mathbb{F}_2$ en $D = [X^2 + XY + Y^2] - [Y]$. Verder geven de de punten $p_1 = (0 : 1)$ en $p_2 = (1 : 1)$ in $\mathbb{P}^1(\mathbb{F}_2)$. (Merk op dat inderdaad de p_i 's niet in D voorkomen.)

Per definitie is

$$L(D) = \{r \in \mathbb{F}_2(t)^* \mid \text{div}(r) + D \text{ heeft alleen maar coeff. } \geq 0\} \cup \{0\}.$$

Stel

$$r(t) = \frac{f(t)}{g(t)} \in L(D).$$

Voor elk monisch en irreducibel polynoom $P(t) \in \mathbb{F}_2[t]$ is

$$\text{ord}_P(r) = \text{ord}_P(f) - \text{ord}_P(g) = \text{aantal factoren } P \text{ in } f - \text{aantal factoren } P \text{ in } g$$

en

$$\text{ord}_Y(r) = \text{ord}_{(1:0)}(r) = -\text{gr}(r) = \text{gr}(g) - \text{gr}(f)$$

We onderscheiden, voor een willekeurig monisch en irreducibel polynoom $P(t) \in \mathbb{F}_2[t]$ of P corresponderend met $(1 : 0)$ een drietal gevallen:

- $P(t) \neq t^2 + t + 1$ en P correspondeert niet met $(1 : 0)$.
De eis $r \in L(D)$ levert dan voor P dat

$$\text{ord}_P(f) - \text{ord}_P(g) \geq 0.$$

Met andere woorden: zo'n monisch en irreducibel polynoom in $\mathbb{F}_2[t]$ dat ongelijk is aan $t^2 + t + 1$ komt in de teller f minstens even vaak voor als in de noemer g . Omdat we kunnen veronderstellen dat f en g geen gemeenschappelijke factoren hebben, kan dus alleen het monisch en irreducibele polynoom $P(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$ in $g(t)$ voorkomen.

- $P(t) = t^2 + t + 1$.
Hiervoor geeft $r \in L(D)$ dat $\text{ord}_{t^2+t+1}(f) - \text{ord}_{t^2+t+1}(g) + 1 \geq 0$. Omdat de factor $t^2 + t + 1$ niet in zowel f als g voorkomt, volgt dat in g de factor $t^2 + t + 1$ ten hoogste één keer voor kan komen.
- P correspondeert met $(1 : 0)$.
Voor dit resterende geval levert de eis $r \in L(D)$ dat $\text{gr}(g) - \text{gr}(f) - 1 \geq 0$. Omdat altijd geldt $\text{gr}(f) \geq 0$, mag g niet constant zijn en daarmee volgt $g(t) = t^2 + t + 1$. Daar $\text{gr}(f) \leq \text{gr}(g) - 1 = 2 - 1 = 1$ moet f dus gelijk zijn aan $f(t) = a + bt$ voor zekere $a, b \in \mathbb{F}_2$.

Er volgt dus dat

$$L(D) = \left\{ \frac{a + bt}{t^2 + t + 1} \mid a, b \in \mathbb{F}_2 \right\}.$$

We vinden de Goppa-code $C(p_1, p_2, D)$ door de punten p_1, p_2 in te vullen in de functies uit $L(D)$. Er geldt

$$(0 : 1) \longleftrightarrow \frac{0}{1} = 0$$

en

$$(1 : 1) \longleftrightarrow \frac{1}{1} = 1.$$

Dus

$$C(p_1, p_2, D) = \{(a, a + b) \mid a, b \in \mathbb{F}_2\} = \mathbb{F}_2^2.$$

Dit levert dus een niet erg interessant voorbeeld. We zullen verderop zien dat we dit zonder rekenwerk al hadden kunnen voorspellen.

Voorbeeld 4.3.9 Omdat het bovenstaande voorbeeld uiteindelijk weinig interessants opleverde, doen we nog een tweede voorbeeld. Neem $K = \mathbb{F}_3$ en $D = [x^3 - xy^2 + y^3] - [x^2 + y^2]$, en p_1, \dots, p_4 alle vier punten van $\mathbb{P}^1(\mathbb{F}_3)$. Dan zit een $r = \frac{a(t)}{b(t)} \rightsquigarrow \frac{A(x,y)}{B(x,y)}$ in $L(D)$, precies dan als voor $P \neq x^3 - xy^2 + y^3, x^2 + y^2$ geldt: $\text{ord}_P(A) - \text{ord}_P(B) \geq 0$. Dus alleen $x^3 - xy^2 + y^3$ kan in B voorkomen, en dan ook nog maximaal 1 keer. Bovendien moet $x^2 + y^2$ minstens één keer in de teller voorkomen. De conclusie is, dat precies alle $A/B = (ax + by)(x^2 + y^2)/(x^3 - xy^2 + y^3)$ in $L(D)$ zitten. De afbeelding ev is in ons geval het evalueren in alle 4 punten van $\mathbb{P}^1(\mathbb{F}_3)$, en een A/B in de kern hiervan moet dus de waarde 0 hebben op al deze punten. Anders gezegd, de teller A zou deelbaar moeten zijn door elk van $x, x - y, x + y$ en y . Met een A/B in $L(D)$ is dit alleen mogelijk voor $A = 0$. We concluderen dat ev injectief is, en dus heeft de Goppa code die we hier krijgen dimensie gelijk aan de dimensie van $L(D)$, en die is 2.

We laten vervolgens zien, dat de minimale afstand in deze Goppa code gelijk is aan 3. Immers, die minimale afstand in onze lineaire code is gelijk aan het minimale aantal coördinaten $\neq 0$ in een codewoord $\neq 0$. Maar dit is gelijk aan 4 minus het maximale aantal nulpunten in $\mathbb{P}^1(\mathbb{F}_3)$ van een niet-nul functie uit $L(D)$. Zo'n functie uit $L(D)$ is te schrijven als $(ax + by)(x^2 + y^2)/(x^3 - xy^2 + y^3)$, en heeft dus precies één nulpunt in $\mathbb{P}^1(\mathbb{F}_3)$, namelijk $(b : -a)$. De minimale afstand is daarom $4 - 1 = 3$.

We concluderen, dat de Goppa code die we zo vinden een $[4, 2, 3]$ -code is, dus in het bijzonder zelfs een MDS-code. We zullen verderop laten zien, dat dit voor heel veel Goppa codes bij \mathbb{P}^1 het geval is.

We gaan nu de parameters van een code $C(p_1, \dots, p_n, D)$ uitrekenen. De lengte is gewoon n . Voor de dimensie kunnen we de al eerder gebruikte lineaire afbeelding van $L(D)$ naar $C(p_1, \dots, p_n, D)$ gebruiken. Noem deze afbeelding ev ; dus $ev(r) = (r(p_1), \dots, r(p_n))$. Dan geldt $\dim C(p_1, \dots, p_n, D) = \dim(L(D)) - \dim(\ker(ev))$. Noem de met de som van de p_i 's geassocieerde divisor G . Dan is $\ker(ev) = L(D - G)$, want $r \in \ker(ev) \iff$ de polynomen bij alle p_i hebben coëfficiënt ≥ 1 in $\text{div}(r) \iff r \in L(D - G)$, want er gold al $r \in L(D)$, en G en D zijn disjunct. Hiermee volgt dus: $\dim(C(p_1, \dots, p_n, D)) = \dim(L(D)) - \dim(L(D - G))$. Wat we dus nog nodig blijken te hebben, is een resultaat over de dimensies van zulke ruimten $L(D)$. Hiervoor bewijzen we eerst een simpel hulpresultaat.

Lemma 4.3.10 *De ruimte $L(n[y]) \subset K(t)$ bestaat voor $n < 0$ alleen uit 0 en voor $n \geq 0$ uit alle polynomen in $K[t]$ van graad $\leq n$.*

In het bijzonder is dus de dimensie van deze ruimte 0 voor $n < 0$ en $n+1$ voor $n \geq 0$.

Bewijs. Een $r \in L(n[y])$ correspondeert met een quotient van homogene polynomen A/B zonder gemeenschappelijke factoren, waarvoor geldt $\text{ord}_P(A) - \text{ord}_P(B) \geq 0$ voor elke $P \neq y$, en $\text{ord}_y(A) - \text{ord}_y(B) + n \geq 0$. Er volgt dat er geen $P \neq y$ kan voorkomen in B , want zo'n P zou in zowel A als B moeten voorkomen. Dus B is een macht van y . Is B constant, dan A evenzo omdat ze dezelfde graad hebben. En is $B = y^k$ met $k \geq 0$, dan moet $\text{ord}_y(A) = 0$ en derhalve $-k + n \geq 0$, dus $k \leq n$. Hieruit volgt het lemma. \square

Stelling 4.3.11 (Riemann-Roch voor \mathbb{P}^1 .) *Voor een divisor D op \mathbb{P}^1 is*
 - $L(D) = 0$ als $\text{deg}(D) < 0$;
 - $\dim(L(D)) = \text{deg}(D) + 1$ als $\text{deg}(D) \geq 0$.

Bewijs. Voor $D = \sum n_P [P]$ schrijven we, zoals gebruikelijk, $D \geq 0$ indien alle $n_P \geq 0$.

-Voor $r \in K(t)^*$ geldt: $L(D) \cong L(D - \text{div}(r))$, waarbij een isomorfisme gegeven wordt door de vermenigvuldiging met r . Er geldt namelijk $\text{div}(s) + D \geq 0 \iff \text{div}(s \cdot r) + D - \text{div}(r) = \text{div}(s) + \text{div}(r) + D - \text{div}(r) \geq 0$. (En elke $u \in K(t)^*$ is natuurlijk te schrijven als $s \cdot r$, voor een unieke $s \in K(t)^*$.) We gaan nu geschikte functies r kiezen en op die manier de divisor D door een zo mogelijk eenvoudiger divisor van dezelfde graad vervangen. Stel $D = D' + n[P]$. Kies dan $r = (P/y^{\text{deg}(P)})^n$. Dan is $\text{div}(r) = n[P] - n \text{deg}(P) \cdot [y]$, en daarom $L(D) \cong L(D' + n \text{deg}(P) \cdot [y])$. Als we zo alle termen langs gaan, dan krijg je uiteindelijk

$$L(D) \cong L(\text{deg}(D) \cdot [y]).$$

De stelling volgt nu direct uit Lemma 4.3.10. \square

Stelling 4.3.12 *Voor $n > \deg(D) \geq 0$ is de Goppa code $C(p_1, \dots, p_n, D)$ bij \mathbb{P}^1 een $[n, \deg(D) + 1, n - \deg(D)]$ -code. In het bijzonder is het dus een MDS-code.*

Bewijs. Stel dat er een woord met gewicht $d > 0$ is in $C(p_1, \dots, p_n, D)$. Dat is dan van de vorm $(r(p_1), \dots, r(p_n))$, voor een $r \in L(D)$, en deze r heeft $n-d$ van de p_i 's als nulpunt. Noem de bij die p_i behorende homogene eerstegraads polynomen Q_1, \dots, Q_{n-d} . Dan volgt $r \in L(D - [Q_1] - \dots - [Q_{n-d}])$. Omdat $r \neq 0$ moet dan wel $\deg(D - [Q_1] - \dots - [Q_{n-d}]) \geq 0$. Dus er geldt $0 \leq \deg(D) - n + d$, oftewel $d \geq n - \deg(D)$.

We wisten al dat $C(p_1, \dots, p_n, D)$ een $[n, \dim(L(D)) - \dim(L(D - [Q_1] - \dots - [Q_{n-d}]))]$, d_{min} code is. De aanname dat $n > \deg(D) \geq 0$ geeft dan met Riemann-Roch, dat de dimensie van $C(p_1, \dots, p_n, D)$ gelijk is aan $\deg(D) + 1$. Verder geldt algemeen voor een $[n, k, d]$ code dat $d \leq n - k + 1$, dus in ons geval $d_{min} \leq n - \deg(D)$. We zagen echter al dat ook $d_{min} \geq n - \deg(D)$, dus moet wel $d_{min} = n - \deg(D)$. Dit bewijst de stelling. \square

Opmerking 4.3.13 Omdat de punten p_i die voor de Goppa code $C(p_1, \dots, p_n, D)$ gebruikt worden, uit $\mathbb{P}^1(\mathbb{F}_q)$ komen, is de maximale lengte van zo'n code over \mathbb{F}_q dus $q + 1$. En die lengte kunnen we ook bereiken met een MDS-code als in bovenstaande stelling. Daarvoor moeten we namelijk de divisor D zo kiezen, dat er geen eerstegraads homogene polynomen in voorkomen (want de p_i 's moeten disjunct zijn van D). Dit is voor iedere graad van D mogelijk. Uit de algebra weten we namelijk, dat er bij iedere graad een irreducibel polynoom in $\mathbb{F}_q[t]$ van die graad te vinden is. Neem dan de divisor bij een verschil $[Q] - [P]$, met P, Q homogeen en irreducibel van graad 3 en 2, en neem als D een veelvoud hiervan. Zo krijg je in het bijzonder voor elke gewenste graad ≥ 0 en $< q + 1$ een divisor die disjunct is van p_1, \dots, p_n . Hiermee zien we dat er $[n, k, n - k + 1]$ -codes over \mathbb{F}_q bestaan, voor elke $n \leq q + 1$ en elke k met $1 \leq k \leq n$.

4.4 Goppa codes over willekeurige krommen

We zullen nu proberen aan te geven hoe je meer algemeen een Goppa code over een kromme kunt definiëren. Hierbij proberen we niet om alle definities heel precies te maken, maar juist om aan te geven hoe de analogie met het geval van \mathbb{P}^1 werkt.

4.4.1 de analogie. In plaats van met $\mathbb{F}_q(t)$, beginnen we nu met een eindige uitbreiding K van $\mathbb{F}_q(t)$. We stellen daarbij de voorwaarde, dat $K \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$.

We beschouwen elementen van $\mathbb{F}_q(t)$ als functies op \mathbb{P}^1 ; evenzo kan men elementen van zo'n eindige uitbreiding als functies op een zekere *kromme* zien. Dit lichten we toe aan een klein voorbeeld.

Voorbeeld 4.4.2 We bekijken de uitbreiding $\mathbb{F}_2(t) \subset \mathbb{F}_2(t, s)$, waarbij s als minimumpolynoom $f_{\mathbb{F}_2(t)}^s = x^2 + x + t^3 + t$ heeft over $\mathbb{F}_2(t)$. Elk element $r \in \mathbb{F}_2(t, s)$ is dus te schrijven als $u + v \cdot s$, met $u, v \in \mathbb{F}_2(t)$ (dit volgt uit het feit dat $\text{gr}(f_{\mathbb{F}_2(t)}^s) = 2$). Beschouw de kromme E gegeven door

$$E := \{(x : y : z) \in \mathbb{P}^2 \mid y^2z + yz^2 + x^3 + xz^2 = 0\}.$$

Een functie op E is dan, in navolging van het voorbeeld van de \mathbb{P}^1 , een quotiënt A/B waarbij in dit geval A, B homogene polynomen in x, y, z van dezelfde graad zijn. Zo'n A/B is dan te schrijven als rationale uitdrukking in het paar $x/z, y/z$, namelijk door zowel A als B te delen door z^d waarin d de graad van A en B is. Nu moeten we er rekening mee houden, dat we functies op E willen bekijken, en niet noodzakelijk functies op de hele \mathbb{P}^2 . Dit heeft tot gevolg dat functies die verschillend zijn op \mathbb{P}^2 , heel goed gelijk kunnen zijn op $E \subset \mathbb{P}^2$. Hier krijg je als volgt voorbeelden van. De punten $(x : y : z)$ van E voldoen aan $y^2z + yz^2 + x^3 + xz^2 = 0$, dus is (delen door z^3) bijvoorbeeld $(y/z)^2 = y/z + (x/z)^3 + x/z$. Met andere woorden, tussen x/z en y/z geldt precies dezelfde relatie als tussen t en s in $\mathbb{F}_2(t, s)$. We kunnen daarom elke functie weergeven in de vorm $u(x/z) + v(x/z)y/z$, voor rationale functies u, v . En omgekeerd, $r = u + vs \in \mathbb{F}_2(t, s)$ definieert een functie (eventueel niet overal gedefinieerd) op E , gegeven door $(x : y : z) \mapsto u(x/z) + v(x/z)y/z$.

Net als voor \mathbb{P}^1 , is het vervolgens mogelijk de orde van een functie in een punt van de kromme, opnieuw geschreven als $\text{ord}_P(r)$, te definiëren. Hierbij moet je denken aan de multipliciteit van een nulpunt of 'pool' van de functie in zo'n punt. Deze begrippen blijken dus ook in de context van krommen over bijvoorbeeld een eindig lichaam zin te hebben.

Evenals voor \mathbb{P}^1 kunnen we vervolgens divisoren definiëren als eindige formele sommen van punten op de kromme. Daarbij komt dan opnieuw de eis, dat we omdat we over een vast lichaam \mathbb{F}_q willen werken, dat als $n[P]$ voorkomt in de divisor D , dan ook $n[P']$, waarbij P' het punt is dat je krijgt

door de coördinaten van P tot de macht q te verheffen. Merk op dat zo'n P' weer een punt op de kromme is.

De graad $\deg(D)$ van een divisor D wordt op precies dezelfde manier als voor \mathbb{P}^1 gegeven.

Bij een $r \in K^*$ hoort de divisor $\operatorname{div}(r) := \sum_P \operatorname{ord}_P(r)[P]$. Het is een feit dat hiervoor weer geldt $\deg(\operatorname{div}(r)) = 0$.

Vervolgens wordt de vectorruimte $L(D)$ bij een divisor D weer gemaakt, en tenslotte bij gegeven punten p_1, \dots, p_n op de kromme met alle coördinaten in \mathbb{F}_q , die geen van alle in de divisor D voorkomen, krijgen we weer de Goppa code

$$C(p_1, \dots, p_n, D) := \{(r(p_1), \dots, r(p_n)) \mid r \in L(D)\}.$$

Over de invarianten van Goppa-codes is dan wat te zeggen met behulp van dezelfde stelling als voor \mathbb{P}^1 .

Stelling 4.4.3 (Riemann-Roch voor algemene krommen.) *Bij iedere kromme hoort een geheel getal $g \geq 0$ dat het geslacht van de kromme wordt genoemd. Er geldt dan voor een divisor D op een kromme, dat*
 $\dim(L(D)) = 0$ als $\deg(D) < 0$;
 $\dim(L(D)) \geq \deg(D) + 1 - g$, met gelijkheid wanneer $\deg(D) > 2g - 2$.

Opmerking 4.4.4

1. Zoals hier geformuleerd, heeft de stelling in het geval $0 \leq \deg(D) \leq 2g - 2$ dus alleen een ondergrens voor de dimensie van $L(D)$. Dat is eigenlijk helemaal niet verwonderlijk, want neem bijvoorbeeld een divisor D met graad 0. Dan zit een functie $r \neq 0$ in $L(D)$ precies dan, als $D + \operatorname{div}(r)$ alleen maar coëfficiënten ≥ 0 heeft. Echter, de som van diezelfde coëfficiënten is gelijk aan 0, dus moet wel $\operatorname{div}(1/r) = -\operatorname{div}(r) = D$. Dus $L(D)$ is 0 als D niet de divisor van een functie is, en $L(D)$ is niet de nulruimte als D wel de divisor van een functie is. Dit is kennelijk iets dat echt van de divisor D afhangt, en niet alleen maar van de graad ervan.
2. Het geslacht g van een kromme is in het algemeen gemakkelijk te berekenen. Is bijvoorbeeld $f \in \mathbb{F}_q[x, y, z]$ een homogeen polynoom van graad d waarvoor over $\overline{\mathbb{F}_q}$ geen punten $\neq (0, 0, 0)$ voldoen aan $f = \partial f / \partial x = \partial f / \partial y = \partial f / \partial z = 0$, dan heeft de kromme in \mathbb{P}^2 gegeven door $f = 0$ geslacht $(d - 1)(d - 2)/2$. In het bijzonder heeft dus de kromme genoemd in Voorbeeld 4.4.2 geslacht 1.
3. Je kan je natuurlijk afvragen waarom juist *krommen* gebruikt worden om codes bij te maken. Je zou immers ook hoger dimensionale dingen

kunnen nemen, en functies daarop. De reden is onder meer, dat je bij krommen zowel voorbeelden kunt maken met heel veel punten over \mathbb{F}_q (al zou dat met iets hoger dimensionaals nog eenvoudiger gaan; neem bijvoorbeeld de \mathbb{P}^n), als dat je een vrij eenvoudige Riemann-Roch stelling hebt die je in staat stelt iets over invarianten van de zo gekregen Goppa codes te zeggen. Hier komt nog het praktische voordeel bij, dat men juist voor krommen vrij efficiënte manieren kent om een ruimte $L(D)$ ook echt te vinden, en bovendien zelfs goede manieren om bij de hiermee verkregen codes fouten te verbeteren.

Voorbeeld 4.4.5 We gaan hier verder met de in Voorbeeld 4.4.2 gegeven kromme E over \mathbb{F}_2 . We hebben al opgemerkt dat het geslacht g van deze kromme 1 is. Op E liggen de punten $p_0 = (0 : 1 : 0)$ en $p_1 = (0 : 0 : 1)$ en $p_2 = (1 : 0 : 1)$ en $p_3 = (0 : 1 : 1)$ en $p_4 = (1 : 1 : 1)$. Een code $C(p_0, \dots, p_4, D)$ zou dus lengte 5 hebben en dat is meer dan we met \mathbb{P}^1 over \mathbb{F}_2 konden bereiken. Wij zullen ons hier tevreden stellen met lengte 4, en daarvoor bekijken we $C_n := C(p_1, \dots, p_4, n[p_0])$. De ruimte $L(n[p_0])$ heeft dimensie n als $n \geq 1$. Voor $n = 1$ zitten er precies de constante functies in. Voor $n = 2$ komt er de functie $t = x/z$ bij, en voor $n = 3$ eveneens $s = y/z$. Voor grotere n krijgen we steeds nieuwe producten van machten van t en eventueel s in $L(n[p_0])$. Een functie in de kern van het evalueren in p_1, \dots, p_4 zal in $L(n[p_0] - [p_1] - \dots - [p_4])$ moeten zitten. Als $n < 4$ dan impliceert dit dat de functie 0 is.

Wij nemen $n = 3$, en dus de code C_3 . Uit bovenstaande blijkt, dat deze dimensie 3 heeft. Een woord met minimale afstand correspondeert met een functie $a + bt + cs$ die zoveel mogelijk nulpunten heeft onder p_1 t/m p_4 . Anders gezegd, met een lijn $a + bx + cy = 0$ in het vlak die zoveel mogelijk van deze p_i 's bevat. Omdat geen enkel drietal uit p_1, \dots, p_4 op een lijn ligt, is dit maximale aantal nulpunten dus ≤ 2 , en daarom precies gelijk aan 2. De minimale afstand in C_3 is daarom $4 - 2 = 2$, dus C_3 is een $[4, 3, 2]$ -code; in het bijzonder is dit een MDS-code.

Omdat $1, t, s$ een basis voor $L(3[p_0])$ vormen, zijn hun beelden onder evalueren een basis voor C_3 . Deze beelden zijn de vectoren $(1, 1, 1, 1)$ en $(0, 1, 0, 1)$ en $(0, 0, 1, 1)$.

Voorbeeld 4.4.6 De *Klein kromme* \mathcal{C} is de kromme in \mathbb{P}^2 gegeven door de vergelijking $x^3y + y^3z + z^3x = 0$. We beschouwen deze hier als een kromme over \mathbb{F}_8 . Het geslacht van \mathcal{C} is gelijk is aan 3.

Neem de divisor $D = 10 \cdot [(0 : 0 : 1)]$ en laat p_1, \dots, p_n alle overige punten op $\mathcal{C}(\mathbb{F}_8)$ zijn. We gaan aantonen dat $C(p_1, \dots, p_n, D)$ een $[23, 8, 13]$ -code is.

Als $z = 0$, dan reduceert de vergelijking tot $x^3y = 0$, waaruit volgt $x = 0$ of $y = 0$ en dus hebben we twee *projectieve* oplossingen, namelijk $(1 : 0 : 0)$ en $(0 : 1 : 0)$.

Als $z \neq 0$, dan mogen we, omdat we alleen kijken naar projectieve oplossingen, zonder verlies van algemeenheid stellen $z = 1$. Dit levert de vergelijking

$$x^3y + y^3 + x = 0.$$

We zien direct dat $(0 : 0 : 1)$ ook een oplossing is.

Alle overige oplossingen hebben zowel x als y ongelijk aan 0.

Laat nu a een primitieve wortel van \mathbb{F}_8 zijn, dat wil zeggen $\langle a \rangle = \mathbb{F}_8^*$. Als (x_0, y_0) een oplossing is van de vergelijking

$$x^3y + y^3 + x = 0$$

dan voldoet ook (a^3x_0, ay_0) , immers

$$(a^3x_0)^3 (ay_0) + (ay_0)^3 + a^3x_0 = a^{10}x_0^3y_0 + a^3y_0^3 + a^3x_0$$

$$\stackrel{\text{ord}(a)=7}{=} a^3x_0^3y_0 + a^3y_0^3 + a^3x_0 = 0.$$

Dit herhaald toepassen, gebruikmakend van het feit dat $a^7 = 1$, geeft met $(x_0 : y_0 : 1) \in \mathcal{C}(\mathbb{F}_8)$ ook de punten

$$(a^3x_0 : ay_0 : 1), (a^6x_0 : a^2y_0 : 1), (a^2x_0 : a^3y_0 : 1),$$

$$(a^5x_0 : a^4y_0 : 1), (ax_0 : a^5y_0 : 1), (a^4x_0 : a^6y_0 : 1) \in \mathcal{C}(\mathbb{F}_8).$$

In deze baan van oplossingen komt niet tweemaal eenzelfde punt voor, want $\text{ord}(a) = 7$ en $y_0 \neq 0$, dus $\{y_0, ay_0, a^2y_0, a^3y_0, a^4y_0, a^5y_0, a^6y_0\} = \mathbb{F}_8^*$.

In zo'n baan van oplossingen hebben we dus in het bijzonder altijd precies één punt met een y -coördinaat gelijk aan 1. Voor zo'n punt reduceert de vergelijking tot

$$x^3 + x + 1 = 0.$$

Omdat het polynoom $X^3 + X + 1$ irreducibel is in \mathbb{F}_2 en graad 3 heeft, brengt elk van z'n drie nulpunten het lichaam \mathbb{F}_8 voort over \mathbb{F}_2 . Dus het polynoom $X^3 + X + 1$ heeft al z'n nulpunten in \mathbb{F}_8 . Dit levert drie punten $(x : 1 : 1) \in \mathcal{C}(\mathbb{F}_8)$, en voor elk hiervan kunnen we een baan van zeven oplossingen doorlopen. We vinden zo $3 \cdot 7 = 21$ oplossingen. Tezamen met

de eerder gevonden oplossingen $(0 : 0 : 1)$, $(0 : 1 : 0)$ en $(1 : 0 : 0)$ levert dit dus $\#\mathcal{C}(\mathbb{F}_8) = 24$.

Omdat $2g - 2 = 4 < 10 = \deg(D)$, volgt uit Stelling 4.4.3 (Riemann-Roch) dat $\dim L(D) = \deg(D) + 1 - g = 8$. Tenslotte geldt, dat een woord van gewicht $d > 0$ in deze code correspondeert met een functie $r \in L(D)$ die in precies $23 - d$ van de punten p_1, \dots, p_{23} een nulpunt heeft. Maar dit betekent dat $r \in L(D - [p_{i_1}] - \dots - [p_{i_{23-d}}])$ voor een zekere deelverzameling $p_{i_1}, \dots, p_{i_{23-d}}$ van de p_i 's. De graad van de divisor die we hier hebben is $10 - 23 + d$, dus zo'n functie $r \neq 0$ is er zeker niet als $10 - 23 + d < 0$. Kortom, $d \geq 13$.

Verder geldt algemeen voor een lineaire code de ongelijkheid $d_{\min} \leq \text{ lengte} - \text{dimensie} + 1$, dus in ons geval weten we $d_{\min} \leq 23 - 8 + 1 = 16$. Samen leveren de genoemde ongelijkheden

$$13 \leq d_{\min} \leq 16.$$

Als we echt willen weten wat de minimale afstand voor onze code is, dan zal er vervolgens expliciet gerekend moeten worden. De ruimte $L(D)$ heeft, zoals we zagen, dimensie 8. Een basis ervoor blijkt te zijn

$$1, z/x, yz/x^2, z^2/x^2, z^3/x^2y, z^2y/x^3, z^3/x^3 \quad \text{en} \quad z^4/x^3y.$$

We zoeken dan een niet-triviale lineaire combinatie van deze functies, die zoveel mogelijk van de punten p_1 t/m p_{23} als nulpunten heeft. Zoals al eerder gezegd, een woord van gewicht $d > 0$ correspondeert met een functie $r \neq 0$ (een lineaire combinatie van bovenstaande acht functies) met $23 - d$ nulpunten onder de p_i 's. Het laagst eventueel mogelijke gewicht, 13, zou dus bij een functie met 10 nulpunten horen. Nu is de graad van de divisor van een functie gelijk aan nul, dus een functie heeft (met multipliciteit gerekend) evenveel nulpunten als polen. Onze eventuele functie heeft 10 nulpunten, dus ook 10 polen. En omdat de functie bovendien in $L(D)$ moet zitten, is het enige punt waar we een pool mogen hebben het punt p_0 . Dus kennelijk zoeken we naar een functie die in p_0 een pool van orde 10 heeft, en als enige nulpunten 10 van de overige p_i 's.

We gaan zo'n functie maken, en daarbij gebruiken we voor de tweede keer de afbeelding $\varphi : \mathcal{C} \rightarrow \mathcal{C}$ gegeven door $\varphi(x : y : z) = (a^3x : ay : z)$ waarin $a^7 = 1$ maar $a \neq 1$. Merk op, dat voor een constante t de functie $f_t := z^3/x^2y - t \in L(D)$ invariant is onder φ , oftewel $f_t(\varphi(P)) = f_t(P)$ voor elke $P \neq p_0$ in \mathcal{C} . Hieruit volgt in het bijzonder, dat als P een nulpunt is van f_t , dan is elke macht $\varphi^k(P)$ eveneens een nulpunt. Kies nu een $x \in \mathbb{F}_8^*$ die voldoet aan $x^3 + x + 1 = 0$. Dan is $P := (x : 1 : 1) \in \mathcal{C}(\mathbb{F}_8)$ een nulpunt van

f_t , als we $t = 1/x^2 = x^2 + x + 1$ kiezen. Deze f_t uit $L(D)$ heeft dus alle 7 punten van de baan van P onder de machten van φ als nulpunt. Vervolgens bekijken we de functie $g := z/x - 1 \in L(D)$. Het is niet moeilijk na te gaan, dat deze drie nulpunten heeft van de vorm $(\xi : 1 : \xi) \in \mathcal{C}(\mathbb{F}_8)$, waarin ξ de drie oplossingen van $X^3 + X^2 + 1 = 0$ in \mathbb{F}_8 doorloopt. Samen met de 7 punten in de baan boven levert dit precies 10 punten op \mathcal{C} , want de $(\xi : 1 : \xi)$ blijken niet in de baan voor te komen. We concluderen dat het product $f_t \cdot g$ al deze 10 punten als nulpunt heeft. Dit product zit in $L(D)$, dus het levert een codewoord van gewicht $\leq 23 - 10 = 13$. Er volgt dat

$$d_{min} = 13.$$

Uit voorbeelden als het bovenstaande wordt al de indruk gekregen dat Goppa codes heel goede codes kunnen zijn. Dit wordt bevestigd door het volgende resultaat.

Stelling 4.4.7 *Stel we hebben krommen $\mathcal{C}_1, \mathcal{C}_2, \dots$ over \mathbb{F}_q waarbij \mathcal{C}_i geslacht g_i heeft, en $g_i \rightarrow \infty$ voor $i \rightarrow \infty$. Stel bovendien dat $\gamma := \lim_{i \rightarrow \infty} g_i / \#\mathcal{C}_i(\mathbb{F}_q)$ bestaat.*

Dan kunnen we bij elke $\epsilon \in [0, 1]$ codes C_1, C_2, \dots construeren waarvoor geldt dat $(\frac{d}{n}, \frac{k}{n})$ voor $n \rightarrow \infty$ convergeert naar een punt (δ, α) met $\delta \geq \epsilon$ en $\alpha \geq 1 - \gamma - \epsilon$.

Deze stelling zegt, dat we bij elk punt $(\epsilon, 1 - \gamma - \epsilon)$ in het vierkant $[0, 1] \times [0, 1]$ een limietpunt bij een rij codes kunnen maken dat “linksboven” dit punt ligt. Hoe kleiner γ genomen kan worden, hoe hoger de lijn met vergelijking $\alpha + \delta = 1 - \gamma$ ligt in het vierkant δ, α -vlak. Het blijkt mogelijk, γ zo klein te nemen dat een stukje van deze lijn boven de grafiek van de in de Gilbert-Varshamov grens genoemde functie ligt. Dit was in de jaren '80 een opzienbarende doorbraak in de coderingstheorie. Merk op dat een kleine γ overeenkomt met krommen die veel punten hebben over \mathbb{F}_q , in relatie tot hun geslacht.

We weten overigens, dat voor zo'n limietpunt (δ, α) geldt $\alpha = 0$ zodra $\delta \geq 1 - 1/q$. Dus door in bovenstaande stelling $\epsilon = 1 - 1/q$ te kiezen, volgt $\gamma \geq 1/q$. Dit wil zeggen dat voor “een rij krommen” moet gelden dat het aantal punten over \mathbb{F}_q dat er op ligt hooguit ongeveer $g \cdot q$ is. Uit de meetkunde is veel meer bekend dan dit; bijvoorbeeld geldt zelfs $\gamma \geq 1/(2\sqrt{q})$ voor zo'n limiet γ (de zogenaamde “Weil grens”).

Bewijs. Kies een $\epsilon \in [0, 1]$ willekeurig en laat P_i een punt in $\mathcal{C}_i(\mathbb{F}_q)$ zijn. Schrijf $N_i = \#\mathcal{C}_i(\mathbb{F}_q)$. Kies positieve gehele getallen $m_i < N_i - 1$ zodat $m_i/N_i \rightarrow 1 - \epsilon$ voor $i \rightarrow \infty$. Vervolgens nemen we de divisor $D_i := m_i[P_i]$

op \mathcal{C}_i , en de code $C_i := C(p_1, \dots, p_{N_i-1}, D_i)$, waarbij de p_j alle punten $\neq P_i$ in $\mathcal{C}_i(\mathbb{F}_q)$ zijn.

De dimensie k_i van C_i is dan gelijk aan die van $L(D_i)$, want evalueren in alle p_j 's heeft als kern de functies in $L(D_i - \sum [p_j]) = 0$ vanwege $\deg(D_i) - (N_i - 1) = m_i - N_i + 1 < 0$. En dus $k_i = \dim L(D_i) \geq m_i + 1 - g_i$ vanwege Riemann-Roch. Na eventueel over te stappen op een deelrij, kunnen we veronderstellen dat $\delta := \lim_{i \rightarrow \infty} k_i / (N_i - 1)$ bestaat, en hiervoor geldt dan

$$\delta \geq \lim_{i \rightarrow \infty} (m_i + 1 - g_i) / N_i = 1 - \epsilon - \gamma.$$

Verder is het aantal nulpunten van een functie $\neq 0$ in $L(D_i)$ hoogstens $m_i = \deg(D_i)$. Dus een codewoord $\neq 0$ in C_i heeft gewicht $\geq N_i - 1 - m_i$. De minimale afstand gedeeld door de lengte heeft dan, na eventueel opnieuw op een deelrij over te gaan, een limiet die $\geq 1 - 1 + \epsilon = \epsilon$ is. \square

Met deze stelling hebben we in principe een methode gevonden om asymptotisch goede codes te vinden: we kunnen proberen krommes over \mathbb{F}_q te construeren waarbij het punten met coördinaten in \mathbb{F}_q meer is het geslacht van de kromme. Dat dit geen eenvoudige eis is, blijkt al uit het volgende voorbeeld.

Voorbeeld 4.4.8 Laat $\mathcal{C}_F = \{(X : Y : Z) \mid F(X, Y, Z) = 0\} \subset \mathbb{P}^2$ een kromme in \mathbb{P}^2 zijn. We veronderstellen dat F homogeen is van graad d en $\frac{\partial}{\partial X} F = \frac{\partial}{\partial Y} F = \frac{\partial}{\partial Z} F = F = 0$ heeft alleen $(0, 0, 0)$ als oplossing (en heeft dus geen oplossing in \mathbb{P}^2).

Deze veronderstelling impliceert dat het geslacht van \mathcal{C}_F gelijk is aan $(d - 1)(d - 2)/2$.

Het polynoom F bestaat uit de som van monomen van de vorm $a_{ijk} X^i Y^j Z^k$ met $i + j + k = d$. Hier zijn er precies $\sum_{i=0}^d d - i + 1 = \sum_{i=1}^{d+1} i = \frac{(d+1)(d+2)}{2}$ van. Elke eis dat een bepaald punt $P \in \mathbb{P}^2$ op \mathcal{C}_F ligt, levert een lineaire conditie op de a_{ijk} 's. Dus we mogen hopen om F 's te vinden met zo'n $\frac{(d+1)(d+2)}{2}$ punten in $\mathcal{C}_F(\mathbb{F}_q)$. Dit zou leiden tot

$$\text{geslacht} / \#\mathcal{C}_F(\mathbb{F}_q) \sim \left(\frac{(d-1)(d-2)}{2} \right) / \left(\frac{(d+1)(d+2)}{2} \right) \rightarrow 1.$$

Zo'n waarde voor γ levert echter een lijn $\delta + \alpha = 0$ op, die behalve $(0, 0)$ geen enkel punt met het vierkant $[0, 1] \times [0, 1]$ gemeenschappelijk heeft.

Merk bovendien op, dat we werken over een vaste \mathbb{F}_q , en dan hebben we voor een kromme als boven, dat $\mathcal{C}_F(\mathbb{F}_q) \subset \mathbb{P}^2(\mathbb{F}_q)$, en die heeft slechts $q^2 + q + 1$ punten. We kunnen dus voor "goede" Goppa codes niet werken met krommen in \mathbb{P}^2 , of zelfs in welke andere vaste \mathbb{P}^n dan ook.

De moraal van dit voorbeeld is dat om asymptotisch goede codes te krijgen, het aantal punten op de kromme vele malen groter moet zijn dan het geslacht. Dat dit mogelijk is blijkt uit het volgende voorbeeld.

Voorbeeld 4.4.9 Laat p een priemgetal zijn, en $r = p^n$ en $q = r^2 = p^{2n}$. Bij het polynoom $F := X^{r+1} + Y^{r+1} + Z^{r+1}$ beschouwen we de kromme \mathcal{C} over \mathbb{F}_q gegeven door

$$\mathcal{C} := \{(X : Y : Z) \mid F(X, Y, Z) = 0\} \subset \mathbb{P}^2.$$

Het stelsel $F = \frac{\partial}{\partial X}F = \frac{\partial}{\partial Y}F = \frac{\partial}{\partial Z}F = 0$ heeft als enige oplossing $(0, 0, 0)$. We hebben dus dat het geslacht van de kromme \mathcal{C} gelijk is aan $g = r(r-1)/2$.

Om $\#\mathcal{C}(\mathbb{F}_q)$ te bepalen, zullen we een aantal gevallen onderscheiden.

Punten met tenminste één coördinaat 0.

Uit bijvoorbeeld $Z = 0$ volgt $X^{r+1} = -Y^{r+1}$. Dit impliceert $X \neq 0 \neq Y$, zodat we $Y = 1$ mogen nemen. De vergelijking reduceert dan tot $X^{r+1} = -1$. We weten dat $\mathbb{F}_q^* = \mathbb{F}_{r^2}^*$ een cyclische groep van orde $r^2 - 1 = (r-1)(r+1)$ is. Beschouw het homomorfisme van \mathbb{F}_q^* naar zichzelf, gegeven door $x \mapsto x^{r+1}$. Omdat $(x^{r+1})^{r-1} = x^{r^2-1} = 1$, geldt dat de elementen in het beeld voldoen aan $y^r = y$, dus in het bijzonder is dit beeld bevat in \mathbb{F}_r^* . Verder is de kern een cyclische groep van orde $r+1$, dus het beeld bestaat uit $(q-1)/(r+1) = r-1$ elementen. We concluderen dat ons homomorfisme een surjectieve afbeelding van \mathbb{F}_q^* naar \mathbb{F}_r^* is.

Het aantal originelen in \mathbb{F}_q^* van $-1 \in \mathbb{F}_r^*$ onder $x \mapsto x^{r+1}$ is dus $r+1$. Hiermee is aangetoond dat er precies $r+1$ punten in $\mathcal{C}(\mathbb{F}_q)$ zijn met $Z = 0$. Hetzelfde argument voor $X = 0$ en voor $Y = 0$ levert, dat er in totaal $3(r+1)$ punten in $\mathcal{C}(\mathbb{F}_q)$ zijn met tenminste één coördinaat gelijk aan 0.

Punten met alle coördinaten ongelijk 0.

Nu mogen we veronderstellen dat $Z = 1$ en dus reduceert de vergelijking tot $X^{r+1} = -1 - Y^{r+1}$. Beschouw de afbeelding $\mathbb{F}_{r^2}^* \rightarrow \mathbb{F}_r^*$, gegeven door $y \mapsto -1 - y^{r+1}$. Het beeld van deze afbeelding bestaat uit alle elementen $\neq -1$ van \mathbb{F}_r^* .

Neem een $w \neq -1$ in \mathbb{F}_r^* , dan weten we met het voorgaande dat er precies $r+1$ elementen $x \in \mathbb{F}_q^*$ zijn met $x^{r+1} = w$. Tevens weten we dat elke $y \in \mathbb{F}_{r^2}^*$ als beeld onder $y \mapsto -1 - y^{r+1}$ zo'n element w oplevert, behalve als $-1 - y^{r+1} = -1$ (en dus $y = 0$), en als y voldoet aan $-1 - y^{r+1} = 0$ (en dus $y^{r+1} = 1$). Van de laatstgenoemde vergelijking hebben we hierboven gezien dat deze precies $r+1$ oplossingen in \mathbb{F}_q heeft. Dus in totaal zijn er $1 + (r+1) = r+2$ waarden voor y die niet tot een $x \neq 0$ in \mathbb{F}_q leiden met $x^{r+1} = -1 - y^{r+1}$ waarbij ook $y \neq 0$. Er blijven dus nog $r^2 - r - 2$ waarden voor y over, en bij elk daarvan behoren $r+1$ waarden $x \in \mathbb{F}_q^*$ met $x^{r+1} = -1 - y^{r+1}$. Zo vinden we $(r^2 - r - 2)(r+1) = (r+1)^2(r-2)$ punten

in $\mathcal{C}(\mathbb{F}_q)$ met alle coördinaten $\neq 0$.

In totaal hebben we dus $3(r+1) + (r+1)^2(r-2) = (r+1)(r^2 - r - 1)$ punten in $\mathcal{C}(\mathbb{F}_q)$, zodat er inderdaad veel meer punten op de kromme liggen dan het geslacht $g = r(r-1)/2$.

Merk op, dat in dit voorbeeld weliswaar de fractie $g/\#\mathcal{C}(\mathbb{F}_q)$ naar nul convergeert, maar dat levert geen rij codes zoals we wel zouden willen. Immers, elke kromme hoort bij een andere q , en dus veranderen we ook steeds het alfabet waarover we codes maken. Door q te veranderen kan men overigens nog wel veel eenvoudiger voorbeelden maken waar dezelfde ratio naar nul gaat. Neem bijvoorbeeld de kromme C vast, en bekijk dan $C(\mathbb{F}_q)$ voor steeds grotere q . Het is niet moeilijk om deze q 's zo te kiezen dat het aantal punten steeds groter wordt, terwijl hier het geslacht vast is.

4.5 Elliptische codes

Zij $F \in \mathbb{F}_q[X, Y, Z]$ een homogeen polynoom van graad 3, met de eigenschap dat $F = \frac{\partial}{\partial X}F = \frac{\partial}{\partial Y}F = \frac{\partial}{\partial Z}F = 0$ over $\overline{\mathbb{F}_q}$ alleen $(0, 0, 0)$ als oplossing heeft. Laat

$$E := \{(X : Y : Z) \in \mathbb{P}^2 \mid F(X, Y, Z) = 0\}.$$

Deze E is een kromme met geslacht 1.

De stelling van Riemann-Roch voor krommen met geslacht 1 luidt:

$$\dim L(D) = \begin{cases} \deg(D) & \text{als } \deg(D) > 0; \\ 0 & \text{als } \deg(D) < 0, \end{cases}$$

voor een divisor D op E .

Definitie 4.5.1 Een code C over \mathbb{F}_q heet een elliptische code als $C = C(p_1, \dots, p_n, D)$ waarin D een divisor is op een kromme E als boven, en $p_1, \dots, p_n \in E(\mathbb{F}_q)$ (zoals altijd, onderling verschillend).

Propositie 4.5.2 Voor een elliptische code $C(p_1, \dots, p_n, D)$, met de eigenschap $n > \deg(D) > 0$, geldt

- (i) de lengte is n ;
- (ii) de dimensie is $\deg(D)$;
- (iii) de minimale afstand is ófwel $n - \deg(D)$, ófwel $n - \deg(D) + 1$.
- (iv) De code $C(p_1, \dots, p_n, D)$ is een MDS code dan en slechts dan als voor elke deelverzameling G van $\{p_1, \dots, p_n\}$ met precies $\deg(D)$ elementen, er geen functie op E bestaat met als divisor $D - G$. Anders gezegd, als $L(D - G) = 0$ voor elk van deze G .

Bewijs. Dit resultaat volgt direct uit de definitie van een Goppa code plus de stelling van Riemann-Roch. De ondergrens voor de minimale afstand volgt uit de observatie, dat een functie $\neq 0$ in $L(D)$ niet meer dan $\deg(D)$ nulpunten buiten D kan hebben. De bovengrens volgt uit het algemene feit dat $d \leq n - k + 1$ voor een $[n, k, d]$ -code.

Voor het bewijs van (iv) merken we op, dat de code niet MDS is, precies dan als er een woord van gewicht $n - \deg(D)$ in de code bestaat. Dit correspondeert met een functie $r \in L(D)$ die precies $\deg(D)$ van de p_i 's als nulpunt heeft. Zo'n functie zit dan in $L(D - G)$, waarin G de divisor corresponderend met de nulpunten van r onder de p_i 's is. \square

Merk op, dat de divisoren $D - G$ die in bovenstaand bewijs voorkomen, graad 0 hebben. We gaan nu voor zulke divisoren de eis $L(D - G) \neq 0$ nader onderzoeken.

Definitie 4.5.3 *Bij E een kromme van geslacht 1, als in het voorgaande, definiëren we de volgende groepen.*

1. $Div(E)$ is de groep van alle divisoren op E .
2. Hierin is $Div^0(E)$ de ondergroep bestaande uit alle divisoren van graad 0.
3. Verder is $HDiv(E)$ de groep bestaande uit alle divisoren van de vorm $div(r)$, waarbij r de functies $\neq 0$ op E doorloopt. Dit is een ondergroep van $Div^0(E)$.
4. Tenslotte is $Pic^0(E) := Div^0(E)/HDiv(E)$.

De theorie van krommen van geslacht 1 onderscheidt zich van die van andere krommen met name vanwege het volgende resultaat.

Stelling 4.5.4 *Kies $O \in E(\mathbb{F}_q)$, dan is de afbeelding $E \rightarrow Pic^0(E)$, gegeven door $P \mapsto [P - O]$, een bijectie.*

Bewijs. (Schets.) Het injectief zijn van deze afbeelding volgt uit Riemann-Roch. Immers, als $[P - O] = [Q - O]$ in $Pic^0(E)$, dan zou het verschil $P - Q$ de divisor van een functie r moeten zijn. Die r zou dan een element van $L(Q)$ zijn, en dat is een vectorruimte van dimensie 1 waar alle constante functies al in zitten, en dus niets meer. Er volgt dat $P = Q$.

Surjectief kan op een heel meetkundige manier bewezen worden: we moeten daarvoor inzien, dat een divisor D van graad 0 is over te voeren naar een divisor van de vorm $P - O$, door er de divisor van een geschikt gekozen functie

bij op te tellen. Stel daartoe, dat $D = (P_1 + \dots + P_t) - (Q_1 + \dots + Q_t)$. Laat $f = 0$ de vergelijking van de lijn door P_t en P_{t-1} zijn (eventueel de raaklijn in P_t als $P_t = P_{t-1}$), en evenzo $g = 0$ de lijn door Q_t en Q_{t-1} . De functie g/f heeft dan een nulpunt in de drie snijpunten van $g = 0$ met E , en een pool in de drie snijpunten van $f = 0$ met E . Derhalve komen in $D + \text{div}(g/f)$ twee punten minder voor dan in D .

Zo doorgaande komen we tenslotte bij een divisor $P - Q$. We willen die overvoeren in een zekere $R - O$, en daarvoor hebben we een functie r nodig met $\text{div}(r) = P + O - Q - R$. Neem daarvoor eerst de lijn door P en O en schrijf deze als $f = 0$. Deze lijn snijdt E in nog een derde punt, zeg S . Vervolgens nemen we de lijn $g = 0$ door Q en S . Het derde snijpunt van deze lijn met E noemen we R . Er geldt dan $\text{div}(f/g) = P + O - Q - R$, en daarmee is de stelling bewezen. \square

Deze stelling stelt ons in staat, op E de structuur van een abelse groep te leggen. Immers kies een punt $O \in E$. Voor twee punten $P, Q \in E$ geldt dan in $\text{Pic}^0(E)$ dat $[P - O] + [Q - O] = [R - O]$ voor zekere R , en dan definiëren we $P + Q = R$. Uit bovenstaand bewijs zien we bovendien, hoe we deze R moeten vinden: snij de lijn door P en Q met E . Het derde snijpunt noemen we S . Dan is R vervolgens het derde snijpunt van de lijn door S en O met E .

Ook de tegengestelde $-P$ van een punt P laat zich zo vinden: de tegengestelde van de divisor $[P - O]$ is namelijk $[O - P]$, en die willen we overvoeren in een zekere $[R - O]$. Daartoe moet $P + R - 2O$ de divisor van een functie zijn. Begin daarom met de raaklijn aan E in O . Deze snijdt E in nog een punt, zeg S . Neen vervolgens de lijn door S en P . Het derde snijpunt van die lijn met E noemen we R , en het quotient van beide vergelijkingen heeft de gevraagde divisor. Deze R is dus $-P$ in de zo gemaakte groepsstructuur op E .

Merk tenslotte op, dat als $O \in E(\mathbb{F}_q)$, dan geldt voor alle $P, Q \in E(\mathbb{F}_q)$ dat ook $P + Q$ en $-P$ in $E(\mathbb{F}_q)$ zitten. Er volgt dan dat $E(\mathbb{F}_q)$ een ondergroep is van E .

Gevolg 4.5.5 *Een elliptische code $C(p_1, \dots, p_n, D)$ met $n > \deg(D) > 0$ is MDS precies dan, als voor $d := \deg(D)$ geldt: elk d -tal punten uit p_1 t/m p_n heeft in de groepsstructuur op E een som die verschillend is van de som van de punten in D .*

Hierin wordt met de som van de punten uit $D = \sum n_P P$ bedoeld, dat we in de groepsstructuur op E de som $\sum n_P P$ bepalen. Merk overigens op, dat de uitspraak in het gevolg niet afhangt van de keuze van het punt O .

Bewijs. Uit Propositie 4.5.2(iv) weten we al, dat MDS zijn equivalent is met de eis dat het verschil van D met een willekeurig d -tal van de p_i 's niet in $\text{HDiv}(E)$ zit. Maar dat betekent precies, dat zo'n verschil $\neq 0$ is in $\text{Pic}^0(E)$, en uit de definitie van de groepsstructuur volgt daarmee de bewering. \square

Voorbeeld 4.5.6 We keren terug naar Voorbeeld 4.4.2 en Voorbeeld 4.4.5, waar we de geslacht 1 kromme E over \mathbb{F}_2 bij de vergelijking $y^2z + yz^2 + x^3 + xz^2 = 0$ beschouwden. De punten p_0, \dots, p_4 op die kromme blijken de enige punten in $E(\mathbb{F}_2)$ te zijn, en dus moet wel gelden dat als groep $E(\mathbb{F}_2) \cong \mathbb{Z}/5\mathbb{Z}$. We kiezen $O = p_0$ en $D = 3[p_0]$. In de code $C(p_1, p_2, p_3, p_4, D)$ is de som van de punten in D uiteraard gelijk aan O . Verder is de som van ieder drietal uit p_1, \dots, p_4 niet gelijk aan O , want drie onderling verschillende elementen $\neq 0$ in $\mathbb{Z}/5\mathbb{Z}$ hebben als som de tegengestelde van het vierde element $\neq 0$. Dit levert een alternatieve manier om in te zien, dat de genoemde code MDS is.

Voorbeeld 4.5.7 We kijken tenslotte naar MDS-codes over \mathbb{F}_q van lengte $q+2$. Merk allereerst op, dat zo'n code niet te realiseren is als Goppa-code bij \mathbb{P}^1 , immers zo'n code kan hooguit lengte $q+1$ hebben. We zullen proberen, met behulp van geslacht 1 krommen zulke codes te maken. Schrijf d voor de minimale afstand, dan willen we dus $[q+2, q-d+3, d]$ -codes.

Het eerste niet geheel triviale geval is $d = 2$. Hier zoeken we een elliptische $[q+2, q+1, 2]$ -code, dus een divisor van graad $q+1$, en $q+2$ rationale punten die niet in die divisor voorkomen, en elk $q+1$ -tal van de gegeven rationale punten heeft een som die verschillend is van de som die bij D hoort.

Voor $q = 2$ is zo'n code al in Voorbeeld 4.4.5 gegeven. Stel vervolgens $q > 2$ en $\mathbb{F}_q \supset \mathbb{F}_2$. Het is uit de theorie van geslacht 1 krommen bekend, dat er zo'n kromme E over \mathbb{F}_q bestaat met $\#E(\mathbb{F}_q) = q+4$. Dit aantal is even, dus in het bijzonder bevat de groep $E(\mathbb{F}_q)$ dan een element T van orde 2. Dit element is uniek, want de theorie van de elliptische krommen leert, dat zo'n kromme in karakteristiek 2 ofwel precies één, ofwel helemaal geen elementen van orde twee kan hebben. Schrijf nu $E(\mathbb{F}_q) = \{O, T, p_1, \dots, p_{q+2}\}$. De code $C(p_1, \dots, p_{q+2}, q[T] + [O])$ is dan de gevraagde MDS-code. Immers, voor elk van de p_i geldt $p_i \neq -p_i$, want anders zou p_i orde 1 of 2 hebben. Hieruit volgt, dat de som van *alle* p_i 's gelijk is aan O . Laten we een punt, zeg p_j , weg, dan levert de resterende som dus $O - p_j = -p_j$. Dit is ongelijk aan $qT + O = O$, en hieruit volgt dat de code $[q+2, q+1, 2]$ is.

Het geval van een oneven q resteert nog. Hier is bekend, dat er een E bestaat met $\#E(\mathbb{F}_q) = q+3$. Noem de som van alle punten in de groepswet T . Deze T is een punt van orde 1 of 2. De punten $p_i \neq T$ tellen dan op tot O , en laten we daar een punt p uit weg, dan wordt de som $-p$. Deze $-p$ is niet gelijk aan $(q+1)T = O$, en hieruit volgt dat de code $C(p_1, \dots, p_{q+2}, (q+1)[T])$ een $[q+2, q+1, 2]$ -code is.

We zien zelfs al bij minimale afstand 2, dat het vinden van elliptische MDS-codes neerkomt op wat kennis over de mogelijke groepsstructuur van een $E(\mathbb{F}_q)$. In het algemeen zijn dit vrij lastige vragen. We volstaan daarom met nog een laatste kleine voorbeeld, namelijk een $[6, 3, 4]$ -code over \mathbb{F}_4 . Hiervoor nemen we

$$E : y^2z + yz^2 + x^3 = 0$$

over \mathbb{F}_4 . Een beetje rekenwerk levert, dat $E(\mathbb{F}_4)$ uit precies 9 punten bestaat. Al deze punten hebben de eigenschap dat de raaklijn aan E in zo'n punt een buigraaklijn is (dat wil zeggen, hij snijdt de kromme in het punt met multipliciteit 3). Hieruit volgt, dat als we $(0 : 1 : 0)$ als eenheidselement nemen, dan is $3p = O$ voor elk punt $p \in E(\mathbb{F}_4)$. We concluderen, dat

$$E(\mathbb{F}_4) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Om hierbij een MDS-code te maken van dimensie 3, hebben we een divisor van graad 3 nodig. Neem daarvoor $D = 2[O] + [P]$, waarin $P \neq O$ willekeurig is. Er zijn dan precies 6 punten p_i die $\neq O, \pm P$ zijn. We beweren, dat de code $C(p_1, \dots, p_6, D)$ de gezochte eigenschappen heeft. Kies hiertoe een basis van $E(\mathbb{F}_4)$, gezien als vectorruimte over \mathbb{F}_3 , bestaande uit P en nog een punt. Ten opzichte van die basis worden de p_i gegeven door alle (a, b) met $b \neq 0$, en $a, b \in \mathbb{F}_3$. We moeten dan inzien, dat een som van drie onderling verschillende elementen

$$(a_1, b_1) + (a_2, b_2) + (a_3, b_3)$$

met alle $b_i \neq 0$, niet gelijk kan zijn aan $(1, 0)$. Welnu, als dit het geval was, dan zouden alle b_i gelijk moeten zijn. Immers, ze zijn niet 0, dus $b_i = \pm 1$, en daaruit volgt het gemakkelijk. Willen de drie punten dan onderling verschillend zijn, dan moeten dus alle drie mogelijke a_i 's echt voorkomen. Dit kan niet, want dan zou hun som 0 zijn en niet 1. Zo volgt, dat de hier gegeven code een $[6, 3, 4]$ -code is. Dit voorbeeld is afkomstig uit het afstudeerverslag van Eelco Marinkelle (Groningen, 1994).