Quaternaire codes

Codes over $\mathbb{Z}/4\mathbb{Z}$

Tjapko Struik
Studentnummer: 0615315
Begeleider: dr. Wieb Bosma

Opleiding Wiskunde
Radboud Universiteit Nijmegen
Bachelorscriptie, 14 juli 2011

Radboud Universiteit Nijmegen

Samenvatting

Quaternaire codes zijn verzamelingen woorden, opgebouwd vanuit een alfabet van 4 letters. Op dit alfabet mag een zekere structuur liggen. Er zijn twee keuzes, met veel structuur, die voor voor de hand liggen. De eerste keuze is codes over $\mathbb{F}_4$, het lichaam met vier elementen, een structuur waarin ieder element een inverse heeft. Een tweede keuze is de codes over $\mathbb{Z}/4\mathbb{Z}$, met een structuur van rekenen modulo 4, en afgezien van inverteerbaarheid dezelfde eigenschappen. In deze scriptie wordt uitgelegd door welke ontdekking de populariteit voor codes over $\mathbb{Z}/4\mathbb{Z}$ is gegroeid. Tot slot wordt een extra motivatie gegeven voor het gebruik van deze vorm van quaternaire codes, namelijk de uitbreiding van binaire kwadraatrestcodes met behulp van het lemma van Hensel.

Inhoudsopgave

Hoofdstuk 1

Introductie

Ter afsluiting van mijn Bachelor Wiskunde schrijf ik deze scriptie. Hoewel ik geen noodzaak zag in toepassingen, zag ik al in een eerstejaarscursus lineaire algebra de schoonheid en het algemeen nut van codes. De zoektocht naar de beste foutverbeterende codes met zo min mogelijk rekenwerk is tenslotte één van de weinige zaken die je bezig kunnen houden in ons oppervlakkige menselijke bestaan. In deze introductie zal ik uitleggen wat codes zijn en in vogelvlucht door mijn scriptie gaan, maar niet voordat ik de volgende mensen bedankt heb. Ten eerste mijn ouders, die mij gedurende mijn hele bachelor, die strikt meer dan drie jaar in beslag neemt, gesteund hebben. Daarnaast ook mijn vriendin Merel, die altijd met frisse tegenzin mijn uitleg aanhoorde, maar inmiddels wel haar favoriete wiskundige concept, de MacWilliamstransformatie, tot in ondenkbare precisie uit weet te leggen. Tot slot wil ik mijn scriptiebegeleider Wieb van harte bedanken, niet alleen voor het in den treure geduld op brengen, maar ook voor de vele espresso's en wiskundige inzichten die hij met mij gedeeld heeft.

Dan is het nu tijd om mijn twee beloftes na te komen. Ten eerste codes, dit zijn verzamelingen woorden van een vaste lengte. Denk aan lengte 8, met de woorden 'wiskundig', 'bijectie', en 'ijscoman'. Door ook spaties toe te laten kun je iedere tekst opknippen in een aantal *codewoorden*. Het belangrijke verschil met normale taal, tot de norm verheven omdat wiskundigen tot op heden altijd in de minderheid zijn geweest binnen de totale populatie mensen, is het alfabet. Voor codes wordt meestal een klein alfabet gekozen, al is dít niet noodzakelijk, met een zekere structuur op dat alfabet. Bij een structuur moet je denken aan optellen en vermenigvuldigen van je letters. Die letters mogen ook getallen zijn, bijvoorbeeld 0 en 1, waarna dit iets realistischer klinkt. Een verhaal met *echte* letters

kun je altijd omschrijven door alle gebruikte symbolen te nummeren en die nummers binair te schrijven, zoals iedere computer dat doet. Met dit begrip van codes, zal ik een iets technischer overzicht geven van wat er verder in mijn scriptie staat.

Het geheel is opgesplitst in twee delen, een deel over binaire codes en een deel over quaternaire codes. De quaternaire codes, waarin we het ongebruikelijke alfabet $0, 1, 2, 3$ hanteren, staan in deze scriptie centraal. Omdat in de praktijk meestal binaire codes worden gebruikt, alleen 0 en 1 dus, nemen we dat als uitgangspunt. We beginnen met een introductie tot codetheorie en bewijzen één van de belangrijkste stellingen in de codetheorie, de stelling van MacWilliams. Daarna zullen we een constructie geven van binaire Kerdock codes, dit zijn goede foutverbeterende codes, wat erg prettig is voor het versturen van informatie. Helaas is het omschrijven van deze codes niet zo efficiënt en dat is nadelig in het gebruik ervan. We eidigen het binaire deel met een introductie tot kwadraatresten en een constructie voor kwadraatrestcodes. In het quaternaire deel worden enkele verbindingen gelegd tussen binaire en quaternaire codes en ook worden de verschillen benadrukt. Daarna gaan we door op de kwadraatresten, maar dan met quaternaire codes, het zogenaamde *liften* van de binaire codes gebeurt het toepassen van het lemma van Hensel.

We eindigen met quaternaire Kerdock codes, we kunnen ze beschrijven door onder andere gebruik te maken van de quaternaire kwadraatrestcodes. In quaternaire vorm blijken deze codes ineens wel heel efficiënt beschreven kunnen worden. Door het bestaan van bovendien een uiterst simpele vertaling tussen binaire en quaternaire codes, de Gray-afbeelding, is de praktijk een goede foutverbeterende code rijker. Hiermee is de clou weliswaar verklapt, maar het is de schoonheid van de wiskunde die de lezer rest.

Hoofdstuk 2

Binaire codes

Hoewel binaire codes centraal zullen staan in dit hoofdstuk, zal hier en daar alvast een voorzet worden gegeven voor het hoofdstuk over quaternaire codes. De motivatie voor quaternaire codes staat namelijk centraal in deze scriptie. Voorlopig zullen we ons echter beperken to het alfabet van twee letters, 0 en 1. Voor later gemak worden nu eerst enkele begrippen gedefiniëerd (Dougherthy, p.508-510 [4], van Lint, p.4-6 [11], Wan p.1-34 [21]). Per code verschilt het welke representatie de kortste omschrijving geeft, daarom zullen er meerdere manieren getoond worden om codes te omschrijven, die allen equivalent zijn.

2.1 Codes: een introductie

Definitie 2.1.1. Een code C over een alfabet A is een deelverzameling van A^n. Het bevat dus een een deel van alle lettercombinaties van A van lengte n. We noemen de lettercombinaties in C woorden of codewoorden.

Definitie 2.1.2. Een lineaire code C van lengte n en dimensie k is een k-dimensionale lineaire deelruimte van een vectorruimte $\mathbb{F}_q^n$, waar $\mathbb{F}_q$ het eindige lichaam met q elementen is.

Enkele van de codes die we tegenkomen, zullen cyclisch zijn. Dit wil zeggen dat een cyclische verschuiving van een codewoord altijd weer een codewoord geeft en dat de code bovendien lineair is.

Definitie 2.1.3. Een lineaire code C heet cyclisch als voor alle $(c_1, c_2, \ldots, c_n) \in C$ geldt dat $(c_n, c_1, c_2, \ldots, c_{n-1}) \in C$.

Afstand en gewicht

Om uit te drukken of een code efficiënt of goed is, maken we vaak gebruik van de begrippen *afstand* en *gewicht*. Er zijn verschillende mogelijkheden om afstand en gewicht aan te geven, we gebruiken hier de Hammings criterium.

Definitie 2.1.4. De Hamming afstand $\text{dist}(a, b)$ tussen twee codewoorden $a, b \in C$, waar $a = (a_1, \ldots, a_n)$ en $b = (b_1, \ldots, b_n)$, is het aantal plaatsen i waar $a_i \neq b_i$. De minimumafstand d van een code C is $\min_{a,b \in C, a \neq b} \text{dist}(a, b)$.

Voorbeeld 2.1.5. *Zij C een binaire code van lengte 8 en laat $a, b \in C$ twee codewoorden zijn, gegeven door $a = (1\ 1\ 0\ 1\ 0\ 0\ 1\ 1)$ en $b = (1\ 0\ 1\ 1\ 1\ 0\ 0\ 0)$, dan dist$(a, b) = 5$.*

Een lineaire code C met codewoorden van lengte n, dimensie k en minimumafstand d wordt ook wel een lineaire $[n, k, d]$-code genoemd. Vooralsnog gebruiken we alleen Hamming afstand. Voor codes over $\mathbb{Z}/2\mathbb{Z}$ is dit het meest natuurlijk. In paragraaf 3.2 gebruiken we Lee afstand voor codes over $\mathbb{Z}/4\mathbb{Z}$. Een motivatie daarvoor wordt ook in die paragraaf gegeven. Behalve afstand gebruiken we ook het begrip gewicht. Hiermee kunnen we een waarde toekennen aan één individueel woord.

Definitie 2.1.6. Het Hamming gewicht w van een codewoord $c \in C$ is het aantal plaatsen in c ongelijk aan 0. Oftewel $w(c) = |\ \{j \mid c_j \neq 0\}\ |$. Het minimumgewicht d van een code C wordt gegeven door $\min_{a \in C, a \neq 0} w(a) = \min_{a \in C, a \neq 0} \text{dist}(a, 0)$.

Voorbeeld 2.1.7. *Zij C een binaire code van lengte 5 en laat $c = (1, 0, 1, 1, 0, 1) \in C$. Dan is het Hamming gewicht $w(c) = 4$.*

Om meer te kunnen zeggen over je code kijk je hoe de codewoorden, ten opzichte van hun gewicht, verdeeld zijn. Deze gewichtsverdeling kun je met één polynoom, de gewichtsteller, vastleggen.

Definitie 2.1.8. Laat A_i het aantal codewoorden met Hamming gewicht i in C zijn, dan is $\{A_0, A_1, \ldots, A_n\}$ de gewichtsverdeling van C. De gewichtsteller W_C van een code C wordt gegegeven door een polynoom over $\mathbb{Z}$ in twee variabelen,

$$W_C(x, y) = \sum_{i=0}^{n} (A_i x^{n-i} y^i) = \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

Lineariteit

Door de lineariteit van de code kan ieder codewoord in de ruimte worden 'verschoven' tot een codewoord vlakbij de oorsprong. Daardoor is de minimumafstand van een lineaire code is gelijk aan het minimumgewicht. Dankzij de begrippen gewicht en afstand kun je een code 'goed' kiezen. Voor een goede code moet je natuurlijk aan allerlei zaken denken, maar in ieder geval moet je zorgen dat de code foutverbeterend is. Dat wil zeggen dat als je een codewoord verstuurt en er treedt een (kleine) fout in op, dat dan nog steeds het juiste woord te herkennen is.

Definitie 2.1.9. Een code C is e-foutverbeterend als voor alle $x_1, x_2 \in C$ geldt dat $B_e(x_1) \cap B_e(x_2) = \emptyset$, waar $B_e(x)$ de bol met straal e om x is, gegeven door $B_e(x) = \{y \in \mathbb{F}_q^n \mid d(x, y) \leq e\}$.

Een code probeer je daarom zo te kiezen dat je zoveel mogelijk niet-overlappende bollen kunt maken met je codewoorden als middelpunt én met een zo groot mogelijke straal.

Tot nu toe hebben we alleen gesproken over lineaire codes. Voordat we niet-lineaire codes bespreken, zullen we eerst laten zien dat lineariteit een prettige eigenschap is. Een lineaire code is namelijk erg eenvoudig te representeren, namelijk door een genererende matrix.

Definitie 2.1.10. Een matrix, waarvan de rijen een lineaire code als vectorruimte voortbrengen, wordt de genererende matrix G genoemd. Een k-dimensionale lineaire code met woordlengte n over $\mathbb{F}_2$, heeft een genererende matrix met rang k (er zijn k lineair onafhankelijk rijvectoren) en breedte n. Een dergelijke code bestaat uit 2^k codewoorden.

Voorbeeld 2.1.11. *Laat C een code, gerepresenteerd door onderstaande genererende matrix G. Hiervan kun je eenvoudig zeggen alle woorden van lengte 4 over het alfabet $\mathbb{Z}/2\mathbb{Z}$ die op plaats 3 en 4 hetzelfde hebben staan, in de code C zitten.*

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

Er is namelijk geen lineaire combinatie mogelijk van rijvectoren uit de genererende matrix die verschilt op plaats 3 en 4. Het omgekeerde is ook waar. De tweede en derde rijvector kunnen individueel plaats 1 en 2 bepalen, dus voor de rest zitten alle woorden in de code.

Deze manier van representeren kan niet bij een niet-lineaire code. In plaats van de kijken naar het minimumgewicht, zul je dan daadwerkelijk naar de minimumafstand moeten kijken om de foutverbeterendheid aan te kunnen geven.

Definitie 2.1.12. Een niet-lineaire code C met codewoorden van lengte n, M verschillende codewoorden en minimumafstand d wordt ook wel een niet-lineaire (n, M, d)-code genoemd.

Ook lineaire codes kun je op deze manier benoemen, maar wanneer een code kunt weergeven door basisvectoren, geniet dit de voorkeur. Een nog ander alternatief voor representatie van lineaire codes is het voortbrengende polynoom van een code. Dit zullen we nog terugzien bij de constructie van kwadraatrestcodes.

Definitie 2.1.13. Laat $\mathbb{F}_q$ een eindig lichaam met q elementen zijn. Een woord $a = a_{n-1} \dots a_0$ van lengte n, met $a_i \in \mathbb{F}_q$, correspondeert met het polynoom $a(x) = a_{n-1}x^{n-1} + \dots + a_0$. De code C correspondeert met het ideaal $(g(x))$, voortgebracht voor het polynoom $g(x)$ van graad $m \leq n$: C bestaat uit de codewoorden die corresponderen met de polynomen $c(x)$ van graad kleiner dan n waarvoor geldt dat $g(x)|c(x)$. Oftewel $C = (g(x)) = \{c \in \mathbb{F}_q^n \mid g(x)|c(x)\}$. We noemen het polynoom $g(x)$ het voortbrengende polynoom van de code C.

Dualiteit

Wanneer we willen spreken over de duale van een code, moeten we altijd opmerken ten opzichte waarvan de code duaal is [18]. In het algemeen zal dit zijn ten opzichte van het standaard inproduct.

Definitie 2.1.14. Voor ieder tweetal elementen $x, y \in \mathbb{F}_q^n$ is het standaard 'inproduct' gedefiniëerd door $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$.

Definitie 2.1.15. De duale code van C is een lineaire code $C^\perp \subset \mathbb{F}_q^n$, gegeven door $C^\perp = \{x \in \mathbb{F}_q^n \mid \forall c \in C : \langle x, c\rangle = 0\}$. Deze code is de verzameling van codewoorden die loodrecht staan op de codewoorden uit C. Verder geldt dat de som van de dimensies van C en zijn duale $C^\perp$ altijd n is.

Definitie 2.1.16. Een zelfduale code is een code C waarvoor geldt dat: $C = C^\perp$.

Dualiteit, of zelfs zelfdualiteit, geeft extra structuur aan codes en is wiskundig gezien fijn om mee te werken. Een dergelijke claim krijgt natuurlijk pas betekenis krijgt wanneer hij ondersteund wordt door een concreet voorbeeld. Het voorbeeld dat we hier zullen behandelen, is de stelling van MacWilliams, een zeer krachtige stelling binnen de codetheorie.

2.2 De stelling van MacWilliams

Florence Jessie Collinson MacWilliams is geboren in 1917 in Stoke-on-Trent, Engeland, en overleed in mei 1990. Toen zij in 1958 als computerprogrammeur werkte bij Bell Telephone Laboratories in Muyrray Hill, New Jersey, werd zij door een voordracht van R. C. Bose gegrepen door codetheorie. Om hier meer mee bezig te zijn, moest zij gaan werken op de technische afdeling van hetzelfde bedrijf. Hiervoor werd echter een PhD vereist, waarop zij in 1961 besloot aan Harvard haar PhD te behalen [25]. Na een jaar codetheorie bestudeerd te hebben, samen met Andrew Gleason, presenteerde zij in 1962 in haar proefschrift 'Combinatorial Problems of Elementary Group Theory' dat de gewichtsteller van de duale van een code volledig vastligt met de gewichtsteller van de oorspronkelijke code (Sloane p.3 [20]).

De stelling

De stelling van MacWilliams, waarin de zogenaamde 'MacWilliamsidentiteit' en de bijbehorende 'MacWilliamstransformatie' worden geïntroduceerd, zijn ook binnen deze scriptie van belang. Twee zeer nuttige codes, de Kerdock en Preparata codes, zijn namelijk elkaars MacWilliamstransformatie en dankzij dit gegeven valt er veel meer samenhang tussen de codes te beschrijven. Later in deze scriptie zullen we hierover in meer detail treden.

Het bewijs

In het bewijs van de stelling dat we hier geven, wordt gebruik gemaakt van karakters. Daarom introduceren we eerst enige theorie hierover, alvorens we de stelling zelf en zijn bewijs poneren (de inleidende theorie en het bewijs van de stelling is ontleend aan een diktaat van Jeurissen, p.54-57 [9]).

Karakters

Definitie 2.2.1. Zij q een macht van een priemgetal. De orde van een element $a \in F_q$ is het kleinste positieve m getal zodanig dat $a^m = 1$. Een element $\omega \in \mathbb{F}_{q^n}$ is een n-de eenheidswortel in $\mathbb{F}_q$ als $\omega^n = 1$. Als n de orde van ω is, dan noemen we ω een primitieve n-de eenheidswortel.

Definitie 2.2.2. De orde van een groep G is gelijk aan de kardinaliteit van de groep. In geval van eindige groepen is dit het aantal elementen van de groep G.

Definitie 2.2.3. Zij G een groep. Een karakter op een groep G is een homomorfisme van G naar de multiplicatieve groep van het lichaam $\mathbb{C}$. Het homomorfisme $\chi : G \to \mathbb{C}^*$ is dus een karakter op de groep G.

Een karakter heet triviaal als $\chi(g) = 1$ voor alle $g \in G$. We maken hier alleen gebruik van karakters op eindige groepen. Het beeld $\chi(G)$ wordt in dit geval volledig bepaald door zijn grootte.

Lemma 2.2.4. *Voor elk natuurlijk getal m geldt: $\mathbb{C}^*$ heeft precies één ondergroep van orde m, namelijk de (cyclische) groep der m-de eenheidswortels.*

Bewijs. De m-de eenheidswortels vormen inderdaad een groep E_m van orde m, cyclisch met voortbrenger $e^{2\pi i/m}$. Om de uniciteit aan te tonen, laat H een ondergroep van $\mathbb{C}^*$ van orde m. Dan $h^m = 1$ voor alle $h \in H$ en dus $H \subset E_m$. Aangezien de orde van H gelijk is aan de orde van E_m, geldt $H = E_m$. □

Lemma 2.2.5. *Laat χ een niet-triviaal karakter zijn en G eindig. Dan is $\sum_{g\in G} \chi(g) = 0$.*

Bewijs. χ is niet-triviaal, dus er is een $h \in G$, met $\chi(h) \neq 1$. Bovendien geldt $\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g)$. Dus $\sum_{g\in G} \chi(g) = 0$. □

Lemma 2.2.6. *Laat q een p-macht zijn. Dan heeft $\mathbb{F}_q^+$ heeft een niet-triviaal karakter.*

Bewijs. $\mathbb{F}_q$ is een vectorruimte over $\mathbb{F}_p$. Kies een willekeurige basis en laat $\phi : \mathbb{F}_q^+ \to \mathbb{F}_p^+$ het homomorfisme zijn dat aan ieder element zijn eerste coördinaat toevoegt. Laat $\rho : \mathbb{F}_p^+ \to E_p$ een homomorfisme zijn dat aan $\overline{k} \in \mathbb{F}_p$ het getal $e^{2k\pi i/p}$ toevoegt. Dan levert de samenstelling $\phi \circ \rho$ een niet-triviaal karakter op. □

Definitie 2.2.7. Laat χ een karakter op $\mathbb{F}_q^+$ zijn. Dan definiëren we voor iedere $x \in \mathbb{F}_q^n$ een karakter χ_x op $(\mathbb{F}_q^n)^+$ door , voor alle $z \in \mathbb{F}_q^n$:

$$\chi_x(z) = \chi(\langle x, z\rangle).$$

Opmerking 2.2.8. Voor iedere $x \in \mathbb{F}_q^n$ geldt dat $x \in U^\perp$ dan en slechts dan als het karakter χ_x triviaal is op U.

Definitie 2.2.9. Gegeven een afbeelding $f : \mathbb{F}_q^n \to V$, met V een $\mathbb{C}$-vectorruimte, en een niet-triviaal karakter χ op $\mathbb{F}_q^+$, definiëren we een afbeelding $\hat{f} : \mathbb{F}_q^n \to V$ door

$$w \mapsto \sum_{z \in \mathbb{F}_q^n} \chi(\langle w, z \rangle) f(z) = \sum_{z \in \mathbb{F}_q^n} \chi_w(z) f(z).$$

Lemma 2.2.10. *Voor iedere deelvectorruimte U van $\mathbb{F}_q^n$ geldt dat*

$$\sum_{u \in U} \hat{f}(u) = |U| \sum_{z \in U^\perp} f(z).$$

Bewijs. In het bewijs splitsen we elementen van $\mathbb{F}_q^n$ op in elementen van $U^\perp$ en het complement ervan. Zoals in opmerking 2.2.8 is aangehaald, geven de elementen van $U^\perp$ precies de de triviale karakters op U. Dus de som van de triviale karakters is $\sum_{u \in U} \chi_z(u) = |U|$ en de som van de niet-triviale karakters is $\sum_{u \in U} \chi_z(u) = 0$. Hieruit volgt:

$$\begin{aligned}
\sum_{u \in U} \hat{f}(u) &= \sum_{u \in U} \sum_{z \in \mathbb{F}_q^n} \chi_u(z) f(z) \\
&= \sum_{z \in \mathbb{F}_q^n} [\sum_{u \in U} \chi_z(u)] f(z) \\
&= \sum_{z \in \mathbb{F}_q^n \setminus U^\perp} [\sum_{u \in U} \chi_z(u)] f(z) + \sum_{z \in U^\perp} [\sum_{u \in U} \chi_z(u)] f(z) \\
&= \sum_{z \in \mathbb{F}_q^n \setminus U^\perp} 0 f(z) + \sum_{z \in U^\perp} |U| f(z) \\
&= |U| \sum_{z \in U^\perp} f(z).
\end{aligned}$$

□

Na deze introductie tot karakters, kunnen we stelling van MacWilliams zonder veel extra moeite bewijzen.

Stelling 2.2.11. *(Stelling van MacWilliams, 1962) Gegeven een lineaire code C over $\mathbb{F}_q$,*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(y - x, y + (q-1)x).$$

Bewijs. Zij χ een niet-triviaal karakter op $\mathbb{F}_q^+$. De existentie hiervan is aangetoond in lemma 2.2.6. Laat $V = \mathbb{C}[x, y]$ en definiëer $f : \mathbb{F}_q^n \to V$ door $f(z) = x^{w(z)} y^{n - w(z)}$, waar n de lengte van C is. Dan is

$$W_{C^\perp}(x, y) = \sum_{v \in C^\perp} f(v)$$

Vanwege lemma 2.2.10 is dit gelijk aan

$$\begin{aligned} &= \frac{1}{|C|} \sum_{c \in C} \hat{f}(c) \\ &= \frac{1}{|C|} \sum_{c \in C} \sum_{z \in \mathbb{F}_q^n} \chi(\langle c, z \rangle) x^{w(z)} y^{n-w(z)} \end{aligned}$$

Zij $c = (c_1, \ldots, c_n), z = (z_1, \ldots, z_n)$, en laat $c_i^{'} = 0$ als $c_i = 0$ en $c_i^{'} = 1$ als $c_i \neq 0$, en $z_i^{'} = 0$ als $z_i = 0$ en $z_i^{'} = 1$ als $z_i \neq 0$. Dan geldt ook de volgende gelijkheid

$$\begin{aligned} &= \frac{1}{|C|} \sum_{c \in C} \sum_{z \in \mathbb{F}_q^n} \chi(c_1, z_1) \cdots \chi(c_n, z_n) x^{z_1^{'}} \cdots x^{z_n^{'}} y^{1-z_1^{'}} \cdots y^{1-z_n^{'}} \\ &= \frac{1}{|C|} \sum_{c \in C} (y-x)^{w(c)} (y + (q-1)x)^{n-w(c)} \\ &= \frac{1}{|C|} W_C(y-x, y+(q-1)x). \end{aligned}$$

□

Over een binaire vectorruimte, dus als $q = 2$, komt dit neer op het volgende.

Gevolg 2.2.12. *Zij C een binaire lineaire code over $\mathbb{F}_q$. Dan geldt*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(y - x, y + x).$$

MacWilliamstransformatie

Met deze identiteit kunnen we ook een afbeelding definiëren. Dit gebeurt in de volgende definitie, waarna we het beeld van de afbeelding de 'MacWilliamstransformatie' van het origineel zullen noemen.

Definitie 2.2.13. Laat C een binaire code van lengte n met gewichtsverdeling $\{A_0, \ldots, A_n\}$ en gewichtsteller $W_C(x, y)$ zijn. Dan zijn respectievelijk $\{A_0^{'}, \ldots, A_n^{'}\}$ en $W_C^{'}(x, y)$ hun MacWilliamstransformaties. De MacWilliamstransformatie van de gewichtsverdeling wordt gegeven door

$$A_k^{'} = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_k(i), \text{ voor } k = 0, 1, \ldots, n,$$

waar $K_k(i)$ het Krawtchoukpolynoom is, gegeven door

$$K_k(i) = K_k(i, n) = \sum_{j=0}^{k} (-1)^j \begin{pmatrix} i \\ j \end{pmatrix} \begin{pmatrix} n-i \\ k-j \end{pmatrix}, \ k = 0, 1, 2, \ldots,$$

en de MacWilliamstransformatie van de gewichtsteller wordt gegeven door

$$W_C^{'}(x,y) = \frac{1}{|C|}\, W_C(y+x, y-x).$$

Met deze relatie tussen W_C en $W_C^{'}$ kunnen we codes die op het eerste gezicht totaal verschillend lijken, soms toch met elkaar vergelijken. Een belangrijk voorbeeld hiervan zien we in de volgende paragraaf.

2.3 Kerdock en Preparata codes

De Kerdock en Preparata codes zijn twee codes die niet-lineair zijn, maar daarentegen goede foutverbeterende codes zijn. Alleen daarom al zijn ze interessant om te bekijken. De werkelijke redenen om de codes te bekijken zijn echter: 1.Hun onderlinge relatie: Kerdock en Preparata codes blijken namelijk elkaars MacWilliamstransformatie te zijn; 2. De alternatieve representatiewijze van beide codes: beide codes zijn niet-lineair, wat een minder eenvoudige constructie vergt dan voor lineaire codes. Aangezien de tweede codes een sterke onderlinge relatie hebben, zullen we qua constructie alleen ingaan op Kerdock codes. De Preparata codes kunnen vervolgens geconstrueerd worden door toepassing van de MacWilliamstransformatie. De constructie van de Kerdock codes vergt al voldoende inspanning en geeft daarmee tegelijkertijd een beeld waarom we open staan voor een alternatieve representatie. We zullen hier de binaire Kerdock codes definiëren als een deelverzameling van de tweede orde Reed-Mullercode $\mathrm{Re}(2,m)$.

Reed-Muller codes

In 1954 vonden de heren I. S. Reed en D. E. Muller goede foutverbeterende codes uit. De naar hen vernoemde Reed-Muller codes zijn, naast foutverbeterend, bovendien eenvoudig te decoderen. Om Reed-Muller codes te definiëren, maken we gebruik van Boolese polynomen [2] [12].

Definitie 2.3.1. Een Boolese polynoom is een lineaire combinatie van Boolese monomen met coëfficiënten in $\mathbb{F}_2$. Een Boolese monoom p in de variabelen $x_1, x_2, \ldots, x_m$ is van de vorm $p = x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}$ met $r_i \in \{0, 1, \ldots\}$ en $1 \leq i \leq m$.

Definitie 2.3.2. Een gereduceerde vorm p' van een monoom p verkrijg je door $x_i x_j = x_j x_i$ en $x_i^2 = x_i$ herhaald toe te passen totdat alle factoren verschillend zijn. Een polynoom is in gereduceerde vorm wanneer iedere monoom in gereduceerde vorm is.

Om een vertaling naar codes te maken, spreken we over vectoren die geassocieerd zijn met Boolese monomen. Het 0-*de graads monoom* $\underline{1}$ is geassocieerd met de vector die bestaat uit 2^m enen. De *eerstegraads monomen* x_i zijn geassocieerd met de vector van lengte 2^m die bestaat uit blokken van afgewisseld 2^{m-i} enen en 2^{m-i} nullen. Om de vectoren te bepalen die met *hogeregraads monomen* geassocieerd zijn, moet je eerst de gereduceerde vorm nemen. Dan vertaal je alle gereduceerde monomen naar vectoren. Door plaatsgewijze vermenigvulding van de vectoren verkrijg je nu de vectoren die geassocieerd zijn met de hogeregraads monomen. De vectoren geassocieerd met *polynomen* verkrijg je door plaatsgewijze optelling van de vectoren die geassocieerd zijn met je gereduceerde vorm van de monomen waaruit het polynoom bestaat.

Om bovenstaande vertaling toe te lichten, een klein voorbeeld.

Voorbeeld 2.3.3. *Gegeven is het polynoom* $x_1^2 + x_1x_2 + x_2 + x_3^2 + x_3x_4 + 1$. *Het gereduceerde Boolese polynoom is* $x_1 + x_1x_2 + x_2 + x_3 + x_3x_4 + 1$ *komt overeen met* $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0) + (1^2\ 1^2\ 1^2\ 1^2\ 10\ 10\ 10\ 10\ 01\ 01\ 01\ 01\ 0^2\ 0^2\ 0^2\ 0^2) + (1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0) + (1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0) + (1^2\ 10\ 01\ 0^2\ 1^2\ 10\ 01\ 0^2\ 1^2\ 10\ 01\ 0^2\ 1^2\ 10\ 01\ 0^2) + (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$, *waarbij we met* 01 *(respectievelijk* 10*) het product van* 1 *en* 0 *(respectievelijk* 0 *en* 1*) bedoelen, wat weer gelijk is aan* 0. *Oftewel, het het polynoom correspondeert met het codewoord* $(0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1)$.

Door een restrictie te leggen op de grootte van de machten van de polynomen, kunnen we spreken van Reed-Muller codes van verschillende orde.

Definitie 2.3.4. Een r-de orde Reed-Muller code van lengte $n = 2^m$ is de verzameling van alle binaire vectoren van lengte n die geassocieerd zijn met Boolese polynomen $p(x_1, x_2, \ldots, x_m)$ van graad kleiner of gelijk aan r. We noteren een r-de orde Reed-Muller code van lengte $n = 2^m$ als $\mathcal{R}(r, m)$.

Voor de constructie van Kerdock codes zijn we alleen geïnteresseerd in eerste en tweede orde Reed-Muller codes. Daarom van beide een voorbeeld.

Voorbeeld 2.3.5. *Een* $\mathcal{R}(1, m)$*-code kun je representeren met de* $\underline{1}$*-vector tezamen met* m *andere vectoren, oftewel met een* $(m + 1) \times 2^m$*-matrix. Voor* $m = 4$ *hebben we de* $\mathcal{R}(1, 4)$,

met de volgende generende matrix:

$$\begin{pmatrix} \underline{1} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Definitie 2.3.6. Laat $C \subset \mathbb{F}_2^n$ een k-dimensionale code en $x \in \mathbb{F}_2^n$. Dan heet de verzameling $x + C = \{x + y \mid y \in C\}$ een coset in C.

Met het begrip van cosets, kunnen we nu $\mathcal{R}(2,4)$ verkrijgen door de vereniging van cosets van $\mathcal{R}(1,m)$ te nemen.

Voorbeeld 2.3.7. *De tweede orde Reed-Muller code met $m = 4$ geeft ons $\mathcal{R}(2,4)$. De bijbehorende genererende matrix bestaat is een uitbreiding van $\binom{4}{2}$ vectoren ten opzichte van de genererende matrix van $\mathcal{R}(1,4)$.*

$$\begin{pmatrix} \underline{1} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_1x_2 \\ x_1x_3 \\ x_1x_4 \\ x_2x_3 \\ x_2x_4 \\ x_3x_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Opmerking 2.3.8. Bovenstaande voorbeelden generaliserend, kunnen we zeggen dat de dimensie van een $\mathcal{R}(r,m)$ code gelijk is aan het aantal vectoren van de genererende matrix, namelijk $\sum_{i=0}^{r} \binom{m}{i}$.

We gaan nu kijken naar een versie van codes die tussen de eerste en tweede orde Reed-Muller codes in ligt, de Kerdock codes.

Kerdock codes

Zoals al aangekondigd, hebben we de eerste en tweede orde Reed-Muller codes nodig om de Kerdock codes te construeren. Een andere manier om tegen de tweede orde Reed-Muller codes aan te kijken, is ze te zien als codes voortgebracht door polynomen van kwadratische vorm. Het gereduceerde polynoom dat geassocieerd is met een codewoord zal weliswaar nooit een kwadraat bevatten, maar de graad van ieder monoom is ten hoogste 2. Een Kerdock code is een deelverzameling van een tweede orde Reed-Muller code, waarbij we niet iedere kwadratische vorm toelaten. De precieze restrictie wordt bepaald door een verzameling symplectische matrices [12].

Definitie 2.3.9. Laat M een $2k \times 2k$-matrix over $\mathbb{F}_q$ zijn. Als er een inverteerbare matrix S bestaat die antisymmetrisch is, oftewel $S^T = -S$, en voldaan wordt aan de vergelijking $M^T S M = S$, dan heet M een symplectische matrix.

Opmerking 2.3.10. De matrix S waarover we spreken is in de literatuur meestal van de vorm

$$S = \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix},$$

waar I_k de $k \times k$ eenheidsmatrix is. Afhankelijk van de toepassingen worden er nog wel eens wat basistransformaties op toegepast, zoals het verwisselen van rijen of kolommen.

Voor $q = 2$ geldt dat M een symplectische matrix is als er een inverteerbare matrix S bestaat met $S^T = S$ zodanig dat $M^T S M = S$. De matrix S zal in de voorbeeld dat zometeen volgt, van de volgende vorm zijn:

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

Met behulp van deze matrix kun je eenvoudig controleren dat bepaalde matrices daadwerkelijk symplectisch zijn.

Definitie 2.3.11. Zij m even. Een verzameling met $2^{m-1} - 1$ symplectische $m \times m$-matrices, tezamen met de nulmatrix, zodanig dat het verschil van twee zulke matrices inverteerbaar is, heet een Kerdock verzameling.

Om aan te geven dat zulke verzamelingen ook daadwerkelijk bestaan, geven we hieronder een voorbeeld. Het voorbeeld is vrij specifiek gekozen. De verzameling zal namelijk de kleinste Kerdock code voort gaan brengen, de *Nordstrom Robinson code*.

Voorbeeld 2.3.12. *(**Nordstrom Robinson**) Voor $m = 4$ zijn $Q_1, \ldots, Q_8$, hieronder afgebeeld, de acht 4×4-matrices die een Kerdock verzameling vormen [22].*

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

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

Met behulp van een dergelijke verzameling kan een Kerdock code worden voortgebracht, die bestaat uit cosets van de Reed-Muller code $\mathcal{R}(1, m)$ en dus een deelverzameling van $\mathcal{R}(2, m)$ is. Zoals al aangehaald, zullen we niet alle cosets toelaten. Codewoorden in $\mathcal{R}(2, m)$ kunnen geschreven worden in de kwadratische vorm, $\sum_{1 \leq i < j \leq m} a_{ij} x_i x_j$, voor zekere coëfficiënten $a_{ij} \in \mathbb{F}_2$. Door ons herhaaldelijk te beperken tot coëfficiënten van een zekere symplectische matrix Q_t, $(1 \leq t \leq 2^{m-1})$, kunnen we 2^{m-1} deelverzamelingen bepalen van $\mathcal{R}(2, m)$. De vereniging van deze deelverzamelingen vormt een Kerdock code.

Definitie 2.3.13. Zij $m \geq 4$ even. Laat $l = 2^{m-1}$ zijn en $\{Q_1, Q_2, \ldots, Q_l\}$ een Kerdock verzameling. Een niet-lineaire code $\mathcal{K}(m)$ van lengte $n = 2^m$, bestaande uit de cosets van $\mathcal{R}(1, m)$ die corresponderen met $Q_1, Q_2, \ldots, Q_l$, heet een Kerdock code.

Opmerking 2.3.14. Het opsommen van alle 256 woorden van lengte 16 uit de *Nordstrom Robinson code*, voortgebracht door de symplextische matrices uit voorbeeld 2.3.12, wordt overgelaten aan de vlijtige lezer.

Tot slot nog enkele eigenschappen van niet-lineaire Kerdock codes $\mathcal{K}(m)$ die goed zijn om te weten, maar waar we verder niet op in zullen gaan. De lengte n van de code is altijd even en van de vorm $n = 2^m$. Het aantal woorden dat de code bevat is gelijk aan 2^{2m} en de minimumafstand van de code is $d = 2^{m-1} - 2^{(m-2)/2}$ [14].

2.4 Binaire codes van kwadraatresten

In deze paragraaf laten we een methode zien om binaire codes te maken met behulp van kwadraatresten. De reden dat deze methode is opgenomen, is dat met behulp van deze constructie ook een eenduidige methode bestaat om quaternaire codes te construeren.

Kwadraatresten

Om deze codes in te voeren, beginnen we met het begrip kwadraatresten [10]. We zullen er in deze paragraaf telkens vanuit gaan dat p een oneven priemgetal is.

Definitie 2.4.1. Een getal $a \in \mathbb{Z}$ is een *kwadraatrest modulo* p als $a \neq 0$ en er bestaat een $b \in \mathbb{Z}$ zodanig dat $b^2 \equiv a \mod p$. De verzameling kwadraatresten modulo p wordt weergegeven door $\mathbb{F}_p^{*2}$, waar $\mathbb{F}_p$ het lichaam met p elementen is.

Wanneer we spreken over een kwadraatrest bedoelen we een kwadraatrest modulo p. Deze toevoeging wordt hier en daar weggelaten om de leesbaarheid te bevorderen. Aangezien we modulo p willen weten of een getal een kwadraatrest is, kijken we naar de equivalentieklasse $\overline{a}$ in plaats van naar alleen a.

Definitie 2.4.2. Zij $a \in \mathbb{Z}$, dan is $\overline{a} = a + p\mathbb{Z}$ de equivalentieklasse van a in $\mathbb{F}_p$.

Om aan te duiden of een getal een kwadraatrest is, wordt doorgaans het Legendresymbool gebruikt.

Definitie 2.4.3. Zij p een oneven priemgetal en $a \in \mathbb{Z}$. Dan definiëren we

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{als } p \mid a, \\ 1 & \text{als } p \nmid a \text{ en } \overline{a} \text{ een kwadraat is in } \mathbb{F}_p, \\ -1 & \text{als } p \nmid a \text{ en } \overline{a} \text{ geen kwadraat is in } \mathbb{F}_p. \end{cases}$$

We noemen deze uitdrukking het Legendresymbool.

Nu we dit begrip ingevoerd hebben, willen we ook graag weten hoe we eenvoudig kunnen bepalen of een getal een kwadraatrest is of niet. Een waterdichte methode hiervoor is om alle getallen tussen 0 en p te kwadrateren modulo p, dan heb je namelijk precies de verzameling van alle kwadraatresten. Vervolgens is het dan alleen nog een kwestie van controleren of je getal in deze verzameling zit. Voor grote p is het echter niet wenselijk om die hele verzameling te construeren en is het volgende criterium een uitkomst.

Lemma 2.4.4. ***(Criterium van Euler)*** *Zij p een oneven priemgetal. Voor $a \in \mathbb{F}_p^*$ geldt: a is een kwadraat in $\mathbb{F}_p$ dan en slechts dan als $a^{\frac{p-1}{2}} = 1 \mod p$.*

Bewijs. $\Rightarrow$) Gegeven is dat a een kwadraat in $\mathbb{F}_p$ is. Dan is er een $x \in \mathbb{Z}$ zodanig dat $x^2 \equiv a \mod p$. Daaruit volgt $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p$.
$\Leftarrow$) Gegeven is dat $a^{\frac{p-1}{2}} \equiv 1 \mod p$. Dan zijn er een primitieve p-de eenheidswortel α en een $b \in \mathbb{Z}$ zodanig dat $a \equiv \alpha^b \mod p$. In het bijzonder is dan $\alpha^{\frac{b(p-1)}{2}} \equiv 1 \mod p$. Vanwege de 'Kleine Stelling van Fermat' geldt nu $p-1 \mid \frac{b(p-1)}{2}$, dus b is even. Kies nu $x = \alpha^{\frac{b}{2}} \in \mathbb{F}_p$. Voor deze x geldt dat $x^2 \equiv (\alpha^{\frac{b}{2}})^2 \equiv \alpha^b \equiv a \mod p$. □

Stelling 2.4.5. *Het Legendresymbool kunnen we uitrekenen door*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Bewijs. Pas het criterium van Euler (Lemma 2.4.4) toe. □

Voor $a = -1$ geldt zelfs gelijkheid, want iedere macht is gelijk aan 1 of -1.

Gevolg 2.4.6.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Voor andere getallen dan 1 en -1 zul je gebruik moeten van maken representanten van equivalentieklassen in $\mathbb{F}_p$. We gaan hiervoor de equivalentieklassen opdelen in twee stukken, S en $-S$. Vervolgens kijken we hoeveel elementen er, door vermenigvuldiging met $\overline{a}$, overgaan van S naar $-S$. Als dit een even aantal is, dan is zijn alle getallen $b \in \mathbb{Z}$, met $b \in \overline{a}$ kwadraatresten modulo p, waar p wederom een oneven priemgetal is. Deze methode wordt het criterium van Gauss genoemd.

Stelling 2.4.7. ***(Criterium van Gauss)*** *Zij p een oneven priemgetal. Laat $S \subset \mathbb{F}_p^*$ zodanig dat $S \cup -S = \mathbb{F}_p^*$ en $S \cap -S = \emptyset$. Dan geldt voor alle $a \in \mathbb{Z}$, met $p \nmid a$, dat*

$$\left(\frac{a}{p}\right) = (-1)^{\#\{\overline{a}S \cap -S\}}.$$

Bewijs. Zij $y = \prod_{\overline{s} \in S} \overline{s}$. Een vermenigvuldiging met a is voor een element $\overline{a} \in S$ een permutatie binnen $\mathbb{F}_p$. Als $\overline{a} \neq 0 \mod p$, dan zal $\overline{a}S$ overgaan in een deel van S en een deel van $-S$.

Voor $\overline{s}_1, \overline{s}_2 \in S$ zal $\overline{s}_1\overline{a} = -\overline{s}_2\overline{a}$ nooit optreden, want $s_1\overline{s}_1\ \overline{a}\ \overline{a}^{p-2} = -\overline{s}_2\ \overline{a}\ \overline{a}^{p-2} = -\overline{s}_2$ leidt tot een tegenspraak. Met $y \neq 0$ volgt nu uit

$$\begin{aligned}
\overline{a}^{\frac{p-1}{2}} y &= \overline{a}^{\frac{p-1}{2}} \prod_{\overline{s}\in S} \overline{s} \\
&= \prod_{\overline{s}\in S} \overline{as} \\
&= (-\overline{1})^{\#\{\overline{as} \mid \overline{s}\in S,\ \overline{as}\in -S\}} \prod_{\overline{s}\in S} \overline{s} \\
&= (-\overline{1})^{\#\{\overline{a}S\cap -S\}} \prod_{\overline{s}\in S} \overline{s} \\
&= (-\overline{1})^{\#\{\overline{a}S\cap -S\}}\ y
\end{aligned}$$

de volgende uitdrukking

$$\left(\frac{a}{p}\right) = \overline{a}^{\frac{p-1}{2}} = (-\overline{1})^{\#\{\overline{a}S\cap -S\}}.$$

□

Met behulp van dit criterium kunnen we zonder veel rekenwerk ook bepalen of 2 een kwadraatrest is. Hiervan maken we gebruik bij de constructie van de binaire kwadraatrestcodes.

Stelling 2.4.8. *Voor p een oneven priemgetal, geldt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Bewijs. Kies $S = \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$ en $-S = \{\overline{\frac{p+1}{2}}, \overline{\frac{p+3}{2}}, \ldots, \overline{p-1}\}$. Het criterium van Gauss (stelling 2.4.7) zegt dan dat

$$\left(\frac{a}{p}\right) = (-1)^{\#\{\overline{a}S\cap -S\}}.$$

$$\begin{aligned}
\#\{\overline{a}S \cap -S\} &= \#\{\overline{a} \in S \mid \overline{2a} \in -S\} \\
&= \#\{a \in \mathbb{Z} \mid 0 < a < \frac{p}{2} \text{ en } \frac{p}{2} < 2a < p\} \\
&= \#\{a \in \mathbb{Z} \mid \frac{p}{4} < a < \frac{p}{2}\} \\
&= \begin{cases} \#\{\frac{p+3}{4}, \ldots, \frac{p-1}{2}\} = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4} & \text{als } p \equiv 1 \mod 4, \\ \#\{\frac{p+1}{4}, \ldots, \frac{p-1}{2}\} = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4} & \text{als } p \equiv 3 \mod 4. \end{cases}
\end{aligned}$$

We willen weten of het aantal elementen in de verzameling $\{\overline{a}S \cap -S\}$ even of oneven is, dus vermenigvuldiging van een oneven getal maakt in de macht van het criterium van Gauss

niet uit. Dus, als $p \equiv 1 \mod 4$, dan is $\frac{p+1}{2} \equiv 1 \mod 2$ en hebben we

$$\frac{p-1}{4} \equiv \frac{p-1}{4}\frac{p+1}{2} \equiv \frac{p^2-1}{8} \mod 2.$$

Op dezelfde wijze, als $p \equiv 3 \mod 4$, dan is $\frac{p-1}{2} \equiv 1 \mod 2$ en hebben we

$$\frac{p+1}{4} \equiv \frac{p-1}{4}\frac{p+1}{2} \equiv \frac{p^2-1}{8} \mod 2.$$

Dus voor alle oneven priemgetallen p geldt

$$\left(\frac{2}{p}\right) = (-1)^{\#\{\overline{a}S \cap -S\}} = (-1)^{\frac{p^2-1}{8}}.$$

□

Een herformulering geeft ons precies wat we willen.

Gevolg 2.4.9. *Zij p een oneven priemgetal. 2 is een kwadraatrest modulo p dan en slechts dan als $p \equiv \pm 1 \mod 8$.*

Constructie van de binaire kwadraatrestcodes

De constructie [21] van de code is gebaseerd op het opsplitsen van de representanten modulo p in twee klassen: de kwadraatresten en die niet-kwadraatresten. Kies nu een priemgetal $p \equiv \pm 1 \mod 8$. Dan is 2 een kwadraatrest modulo p (zie Gevolg 2.4.9) en dus $2^{(p-1)/2} \equiv 1 \mod p$. Voor het kleinste positieve gehele getal m zodanig dat $p \mid 2^m - 1$ heeft $\mathbb{F}_{2^m}^*$ een ondergroep van orde p. De voortbrenger van deze ondergroep is de primitieve p-de eenheidswortel $\omega \in \mathbb{F}_{2^m}$. In $\mathbb{F}_{2^m}[x]$ kan $x^p - 1$ daarom volledig worden gefactoriseerd.

$$x^p - 1 = \prod_{i=0}^{p-1}(x - \omega^i) \in \mathbb{F}_{2^m}[x].$$

Merk op dat de machten van ω niet automatisch in $\mathbb{F}_p$ zitten. We kunnen daarom $x^p - 1$ niet automatisch factoriseren in polynomen in $\mathbb{F}_2[x]$. Dit blijkt wel te kunnen als we de machten van ω in de factorisatie verdelen in kwadraatresten en niet-kwadraatresten.

Definitie 2.4.10. Zij $\mathbb{F}_p^{*2}$, de verzameling van kwadraatresten, en $\mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$, de verzameling met alle niet-kwadraatresten modulo p. Dan definiëren we de bijbehorende polynomen door

$$g_2(x) = \prod_{r \in \mathbb{F}_p^{*2}} (x - \omega^r) \text{ en } h_2(x) = \prod_{s \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}} (x - \omega^s)$$

.

Hiermee kunnen we een nieuwe factorisatie van $x^p - 1$ geven, maar nu in $\mathbb{F}_2[x]$ in plaats van $\mathbb{F}_{2^m}[x]$.

Stelling 2.4.11. *Gegeven zijn de polynomen $g_2(x)$ en $h_2(x)$, zoals hierboven gedefiniëerd. Dan hebben we een factorisatie van $x^p - 1 = (x-1)\ g_2(x)\ h_2(x)$, waarbij*

$$g_2(x),\ h_2(x)\ \in \mathbb{F}_2[x]$$

Bewijs. We hebben geëist $p \equiv \pm 1 \mod 8$ en daarmee dat 2 een kwadraatrest is. Vermenigvuldiging met 2 is in $\mathbb{F}_p$ een permutatie. Bovendien is het product van twee kwadraatresten weer een kwadraatrest, dus $\overline{2}\mathbb{F}_p^{*2} = \mathbb{F}_p^{*2}$ en ook $\prod_{i \in \mathbb{F}_p^{*2}} x - \omega^i = \prod_{i \in \mathbb{F}_p^{*2}} x - (\omega^i)^2$.
Voor zekere indexverzamelingen $Z_j \subset (\mathbb{F}_p^{*2} \cup \{0\})$ en bijbehorende $b_j \in \mathbb{F}_{2^m}$ kunnen we het polynoom $g_2(x)$ ook schrijven als

$$g_2(x) = \prod_{i \in \mathbb{F}_p^{*2}} x - \omega^i = \sum_{j=0}^{\frac{p-1}{2}} (\prod_{z \in Z_j} \omega^z)\ x^j = \sum_{j=0}^{\frac{p-1}{2}} b_j\ x^j.$$

Net zo geldt

$$g_2(x) = \prod_{i \in \mathbb{F}_p^{*2}} x - (\omega^i)^2 = \sum_{j=0}^{\frac{p-1}{2}} (\prod_{z \in Z_j} (\omega^z)^2)\ x^j = \sum_{j=0}^{\frac{p-1}{2}} (\prod_{z \in Z_j} \omega^z)^2\ x^j = \sum_{j=0}^{\frac{p-1}{2}} b_j^2\ x^j.$$

Dus voor alle j met $1 \leq j \leq \frac{p-1}{2}$ geldt $b_j = b_j^2$. Oftewel $0 = b_j^2 - b_j = b_j(b_j - 1)$ en dus $b_j = 0$ of $b_j = 1$. Alle coëfficiënten van $g_2(x)$ zitten in $\mathbb{F}_2$, dus $g_2(x) \in \mathbb{F}_2[x]$. Aangezien $(x-1), g_2(x) \in \mathbb{F}_2[x]$ en het product $x^p - 1 = (x-1)g_2(x)h_2(x) \in \mathbb{F}_2[x]$, moet gelden dat $h_2(x) \in \mathbb{F}_2[x]$. □

Met behulp van de factorisatie van $x^p - 1$ hebben we vier polynomen verkregen, waarvan de idealen voortgebracht door deze polynomen, corresponderen met een binaire cyclische codes van lengte p. Dit zijn $(g_2(x))$, $(h_2(x))$, $((x-1)g_2(x))$ en $((x-1)h_2(x))$.

De codes die bij de eerste twee idealen horen, worden ook wel *binaire geaugmenteerde kwadraatrestcodes* genoemd en hebben dimensie $\frac{p+1}{2}$. De codes die bij de laatste twee idealen horen, zijn *binaire geëxpurgeerde kwadraatrestcodes* en hebben dimensie $\frac{p-1}{2}$.

Quaternaire codes

We bouwen de quaternaire kwadraatrestcodes op vanuit binaire kwadraatrestcodes. Dit komt aan de orde in het volgende hoofdstuk.

Hoofdstuk 3

Quaternaire codes

Een quaternaire code heeft een alfabet van vier letters met een bepaalde structuur erop. Dit kan de structuur van een lichaam zijn, namelijk die van $\mathbb{F}_4$. Het kan echter ook de structuur van de ring $\mathbb{Z}/4\mathbb{Z}$ zijn, dus met de elementen $\overline{0}, \overline{1}, \overline{2}$ en $\overline{3}$. We zullen in het vervolg deze strepen weglaten, hoewel we nog steeds de equivalentieklassen bedoelen. Wellicht ten overvloede, maar om duidelijk te maken dat het gebruik van een ring normaliter een beperking is, geven we hier de eigenschappen van een ring en een lichaam. Een ring R, met optellen en vermenigvuldiging als bewerkingen, voldoet aan de volgende eigenschappen:

1. Voor alle $a, b \in R$ geldt dat $a + b \in R$ en $ab \in R$.
2. Voor alle $a, b, c \in R$ geldt dat $a + (b + c) = (a + b) + c$.
3. Er is een element $0 \in R$ zodanig dat voor alle $a \in R$ geldt dat $a + 0 = 0 + a = a$.
4. Voor alle $a \in R$ is er een $b \in R$ zodanig dat $a + b = 0$.
5. Voor alle $a, b \in R$ geldt dat $a + b = b + a$.
6. Voor alle $a, b, c \in R$ geldt dat $a(bc) = (ab)c$.
7. Er is een element $1 \in R$ met $1 \neq 0$ zodanig dat voor alle $a \in R$ geldt dat $a \cdot 1 = 1 \cdot a = a$.
8. Voor alle $a, b \in R$ geldt dat $ab = ba$.
9. Voor alle $a, b, c \in R$ geldt dat $a \cdot (b + c) = a \cdot b + a \cdot c$ en $(a + b) \cdot c = a \cdot c + b \cdot c$.

Soms wordt er minder geëist voor het zijn van een ring, maar zelfs met al deze eisen is er nog een verschil met een lichaam.

Een lichaam L is een ring die bovendien aan de volgende eigenschap voldoet. Voor alle $a \in L$, met $a \neq 0$, is er een $b \in L$ zodanig dat $ab = ba = 1$.

3.1 Codes over $\mathbb{Z}/4\mathbb{Z}$

Wanneer je alleen geïnteresseerd bent in de grootte van het alfabet van je code, dan is het logischer om te kijken naar quaternaire codes over $\mathbb{F}_4$, omdat $\mathbb{F}_4$ meer structuur heeft dan het alternatief $\mathbb{Z}/4\mathbb{Z}$. De vraag is dan ook waarom je toch voor quaternaire codes over $\mathbb{Z}/4\mathbb{Z}$ zou kiezen, waar de code geen deelruimte een vectorruimte is, omdat het alfabet geen lichaam is. In dit hoofstuk zullen we met een quaternaire code altijd een code over $\mathbb{Z}/4\mathbb{Z}$ bedoelen.

Definitie 3.1.1. Een quaternaire code C is een code over $\mathbb{Z}/4\mathbb{Z}$.

Oorsprong

Aan de hand van twee verschillende artikelen (Bonnecaze en Solé [1], Sloane en Conway [3]) is deze keuze vrij snel uit te leggen. Aan de invoering liggen enkele andere codes ten grondslag, namelijk niet-lineaire binaire codes. Je wilt, ook in het binaire geval, liever werken met lineaire codes, maar er zijn meer eigenschappen die codes aantrekkelijk kunnen maken. Zo zijn de Kerdock, Nordstrom-Robinson en de Preparata codes heel erg goede binaire *foutverbeterende* codes. De laatste twee zijn zelfs tweemaal zo groot als de beste lineaire codes met dezelfde parameters.

De link naar quaternaire codes werd gelegd dankzij het verband tussen de Kerdock en Preparata codes. Deze twee codes zijn elkaars 'MacWilliams transformatie van de afstandsverdeling'. Om dit algebraïsch uit te drukken, moeten de codes lineair zijn. Door de Gray afbeelding kunnen bepaalde lineaire codes over $\mathbb{Z}/4\mathbb{Z}$ afgebeeld worden op de Kerdock en Preparata codes, waar de codes precies elkaars duale zullen zijn. Om de Gray afbeelding overtuigend in te voeren, zal tevens wat algemene informatie over afstandsbegrip binnen deze vorm van quaternaire codes worden gegeven.

Tot slot zullen in het einde van het hoofdstuk kwadraatrestcodes van het alfabet $\mathbb{Z}/2\mathbb{Z}$, geïntroduceerd in het eerste hoofdstuk, uitbreiden tot codes over $\mathbb{Z}/4\mathbb{Z}$. Hieruit blijkt wederom dat er over $\mathbb{Z}/4\mathbb{Z}$ uitstekend codes te maken zijn.

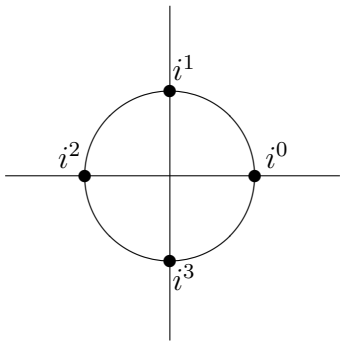
3.2 De Gray-afbeelding

Voordat we concrete voorbeelden van quaternaire codes geven, zullen we eerst wat definities invoeren met betrekking tot afstand en gewicht. Met behulp hiervan zullen we het verband tussen binaire en quaternaire codes proberen duidelijk te maken.

Lee gewicht

In quaternaire codes over $\mathbb{Z}/4\mathbb{Z}$ kun je het beste werken met Lee gewicht en Lee afstand, in plaats van het meer gebruikelijke Hamming gewicht en Hamming afstand. Deze gewichten worden gegeven aan de hand van de volgende meetkundige uitbreiding van $\mathbb{Z}/2\mathbb{Z}$ naar $\mathbb{Z}/4\mathbb{Z}$.

De afstandsfunctie herschrijven we in de complexe getallen [21], waar we het alfabet $\mathbb{Z}/4\mathbb{Z}$ beschouwen als signaalpunten, namelijk de machten van i in het complexe vlak.



Voor de volledigheid, dit is niet meer dan het toewijzen van $i^0 = 1$, $i^1 = i$, $i^2 = -1$ en $i^3 = -i$ aan respectievelijk $0, 1, 2$ en 3.

Definitie 3.2.1. Dan definiëren we de Lee afstand

$$d_L(a, b) = \frac{1}{2} d_E^2(i^a, i^b),$$

met $d_E^2(x, y)$ het kwadraat van de Euclidische afstand in het complexe vlak, gegeven door

$$d_E(x, y) = \left(\Big(\mathrm{Re}(x) - \mathrm{Re}(y) \Big)^2 + \Big(\mathrm{Im}(x) - \mathrm{Im}(y) \Big)^2 \right)^{\frac{1}{2}},$$

waar Re staat voor het reële deel en Im voor het imaginaire deel van het complexe getal.

Definitie 3.2.2. Laat $d_L(x, y)$ de Lee afstand zijn tussen $x, y \in \mathbb{Z}/4\mathbb{Z}$. Dan is, uitgebreid naar $(\mathbb{Z}/4\mathbb{Z})^n$, voor $x, y \in (\mathbb{Z}/4\mathbb{Z})^n$, met $x = (x_0, \ldots, x_{n-1})$ en $y = (y_0, \ldots, y_{n-1})$ de Lee afstand gegeven door

$$d_L(x, y) = \left(\sum_{i=0}^{n-1} d_L(x_i, y_i) \right)^{\frac{1}{2}},$$

op dezelfde wijze als de uitbreiding van de Euclische afstand naar meerdere dimensies. Oftewel, de Lee afstand uitgedrukt in Euclidische afstand, is

$$d_L(x, y) = \frac{1}{2} d_E^2(i^x, i^y).$$

Aangezien de afstand in het algemeen ook kan worden gedefiniëerd door het gewicht van de verschilfunctie van twee woorden, moeten de gewichten zorgvuldig worden gekozen [19]. De gewichten zijn zodoende als volgt gedefiniëerd.

Definitie 3.2.3. Het Lee gewicht w_L van een element $c \in \mathbb{Z}/4\mathbb{Z}$ wordt gegeven door

$$\begin{array}{cccccc} c & 0 & 1 & 2 & 3 \\ w_L(c) & 0 & 1 & 2 & 1 \end{array},$$

gegeneraliseerd naar $\mathbb{Z}/4\mathbb{Z}^n$ betekent dit

$$w_L(u) = \sum_{i=1}^{n} w_L(u_i),$$

waar $u = (u_1, \ldots, u_n) \in (\mathbb{Z}/4\mathbb{Z})^n$. Hiermee kun je ook direct de Lee afstand definiëren, $\mathrm{dist}_L(u, v) = w_L(u - v)$.

Definitie 3.2.4. De Lee gewichtsteller van een lineaire code C over $\mathbb{Z}/4\mathbb{Z}$ is

$$\mathrm{Lee}_C(x, y) = \sum_{u \in C} x^{2n - w_L(u)} y^{w_L(u)},$$

De Gray-afbeelding

De Gray-afbeelding is een afbeelding tussen $\mathbb{Z}/4\mathbb{Z}$ en $(\mathbb{Z}/2\mathbb{Z})^2$, die een verband aangeeft tussen codes van lengte n over $\mathbb{Z}/4\mathbb{Z}$ met Lee afstand en codes van lengte $2n$ over $\mathbb{Z}/2\mathbb{Z}$ met Hamming afstand. Met de definitie van de Lee gewichten, zoals hierboven, is het voor behoud van gewicht en afstand noodzakelijk om 2 naar 11 te sturen en 3 naar 10 in plaats van de binaire representatie te gebruiken. Dit geeft ons noodzakelijkerwijs de volgende definitie.

Definitie 3.2.5. De Gray-afbeelding $\phi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2$ wordt gegeven door:
$\phi(0) = 00,\ \phi(1) = 01,\ \phi(2) = 11,\ \phi(3) = 10.$

3.3 Quaternaire codes van kwadraatresten

In paragraaf 2.4.11 van het vorige hoofdstuk hebben we een constructie gegeven van binaire kwadraatrestcodes. Met behulp van het *Lemma van Hensel* gaan we de binaire kwadraatrestcodes *liften* tot quaternaire kwadraatrestcodes. Deze *Hensel lift* van een binaire code is een erg handige quaternaire code, zoals we bij de constructie van de quaternaire Kerdock codes terug zullen zien. Voordat we met een Hensel lift een code gaan beschrijven, nu eerst het lemma [17].

Lemma 3.3.1. ***(Lemma van Hensel)*** *Zij p een priemgetal. Laat $f(x)$ een monisch polynoom in $\mathbb{Z}[x]$ zijn. Laat $f(v) \equiv 0 \mod p$ zijn en laat voor de afgeleide van f in het punt v gelden dat $f'(v) \not\equiv 0 \mod p$. Dan bestaat er voor iedere geheeltallige $k \geq 1$ een rij $(v_j)_{j=1}^{k}$ zodanig dat $v_1 = v$, $v_k - v_{k-1} \equiv 0 \mod p^{k-1}$ en $f(v_k) \equiv 0 \mod p^k$. Bovendien is v_k uniek modulo p^k.*

Bewijs. Het bewijs voor existentie gaat met inductie naar k. Voor $k = 1$ hebben we $v_1 = v$, want gegeven is $f(v) \equiv 0 \mod p$. Neem nu aan dat er voor vaste k een rij $(v_j)_{j=1}^{k}$ bestaat die aan de beweringen van het lemma voldoet. Dan moeten we nog aantonen dat er een v_{k+1} is, en daarmee een rij $(v_j)_{j=1}^{k+1}$, zodanig dat $f(v_{k+1}) \equiv 0 \mod p^{k+1}$. Sowieso moet gelden dat $v_{k+1} - v_k \equiv 0 \mod p^k$, dus $v_{k+1} = v_k + b_k p^k$ voor zekere $b \in \mathbb{Z}$. Aangezien $k \geq 1$, geldt dat $2k \geq k + 1$ en hebben we met de binomiale expansie van $v_{k+1} = v_k + b_k p^k$ de volgende uitdrukking

$$f(v_{k+1}) \equiv f(v_k + b_k p^k) \equiv f(v_k) + b_k p^k f'(v_k) \mod p^{k+1}.$$

$f(v_k) \equiv 0 \mod p$, dus er is een $c_k \in \mathbb{Z}$ met $f(v_k) = c_k p^k$. Verder weten we dat $v_k \equiv v \mod p$, dus $f'(v_k) \equiv f'(v) \mod p$ heeft een inverse $m \in \mathbb{F}_p$. Oftewel $mf'(v_k) \equiv 1 \mod p$ en er is een $l \in \mathbb{Z}$ met $mf'(v_k) = 1 + lp$. Kies nu $b_k = -mc_k$, dan geldt

$$\begin{aligned} f(v_{k+1}) &= f(v_k) + b_k p^k f'(v_k) \\ &= c_k p^k - m\, c_k\, p^k\, f'(v_k) \\ &= c_k p^k - c_k\, p^k\, (1 + lp) \\ &= -c_k\, l\, p^{k+1}, \end{aligned}$$

waarmee aan gewenste voorwaarde $f(v_{k+1}) \equiv 0 \mod p^{k+1}$ wordt voldaan. Nu het bestaan van b_k is aangetoond, kaan aan de tweede voorwaarde eenvoudig worden voldaan. $v_{k+1} - v_k \equiv (v_k + b_k p^k) - v_k \equiv v_k - mc_k p^k - v_k \equiv 0 \mod p^k$. De uniciteit van $v_{k+1} \in \mathbb{F}_p$ ligt reeds verscholen in de constructie. Stel, er is een $\hat{v}_{k+1} \in \mathbb{F}_p$ met dezelfde twee eigenschappen als v_{k+1}. Dan is

er een $\hat{b}_k$ zodanig dat $\hat{v}_{k+1} = v_k + \hat{b}_k p^k$, vanwege de eigenschap $\hat{v}_{k+1} - v_k \equiv 0 \mod p^k$. Ook geldt $f(\hat{v}_{k+1}) \equiv 0 \mod p^{k+1}$, dus $\hat{b}_k = -\hat{m}\hat{c}_k$ voor zekere $\hat{m}$ en $\hat{c}_k$. Aangezien $\hat{c}_k$ uniek is en $\hat{m}$ uniek modulo p^{k+1}, geldt dat $\hat{c}_k = c_k$ en $\hat{m} = m$. Oftewel $\hat{v}_{k+1} \equiv v_k + \hat{b}_k p^k \equiv v_k - \hat{m}\hat{c}_k p^k \equiv v_k - m c_k p^k \equiv v_k + b_k p^k \equiv v_{k+1} \mod p^{k+1}$. □

De code

In propositie 2.4.11 is reeds genoemd dat $x^p - 1 = (x-1)g_2(x)h_2(x)$ in $\mathbb{F}_2[x]$. Met de constructie van de voortbrengende polynomen $g_2(x)$ en $h_2(x)$ in $\mathbb{F}_2[x]$ is het meeste werk reeds gedaan. Door het Lemma van Hensel (3.3.1) toe te passen op deze resultaten, weten we dat er monische polynomen $(x-a),\ g(x),\ h(x) \in \mathbb{Z}/4\mathbb{Z}[x]$ bestaan zodanig dat

$$x^p - 1 = (x-a)g(x)h(x) \ \in \ \mathbb{Z}/4\mathbb{Z}[x].$$

Aangezien ω een primitieve p-de eenheidswortel is, is p het kleinste getal zodanig dat $\omega^p = 1$. Daarom is 1 geen nulpunt van $g_2(x)$. Voor een oplossing v_2 van de Hensel lift $g(x) \equiv 0 \mod 2^2$, behorend bij $g_2(x) \equiv 0 \mod 2$ geldt dat $v_2 - v_1 \equiv 0 \mod 2$. Daarom is $v_2 \not\equiv 1 \mod 2^2$ (en $v_2 \not\equiv 3 \mod 2^2$), dus 1 is geen nulpunt van $g(x)$. Hetzelfde geldt voor $h(x)$. Door $x = 1$ in te vullen, zien we $1^p - 1 = (1-a)g(1)h(1)$. Met bovenstaande opmerkingen kunnen we nu onmiddelijk concluderen dat $a = 1$ noodzakelijk is, oftewel

$$x^p - 1 = (x-1)g(x)h(x) \ \in \ \mathbb{Z}/4\mathbb{Z}[x].$$

Gevolg 3.3.2. *De Hensel lifts $g(x)$ en $h(x)$ in $\mathbb{Z}/4\mathbb{Z}[x]$ liggen uniek vast door de polynomen $g_2(x)$ en $h_2(x)$ in $\mathbb{F}_2[x]$, de essentiëlen polynomen voor de binaire kwadraatrestcodes. Op dezelfde wijze als bij binaire codes brengen de polynomen over $\mathbb{Z}/4\mathbb{Z}$ idealen voort, namelijk $(g(x)), (h(x)), ((x-1)g(x)), ((x-1)h(x))$, die corresponderen met codes - quaternaire codes.*

3.4 Quaternaire Kerdock codes

In paragraaf 2.3 hebben we de binaire constructie van Kerdock codes behandeld. Aan de hand van het voorbeeld van de Nordstrom-Robinson code zagen we dat er geen korte omschrijving is, zoals bij lineaire codes. In deze paragraaf zullen we de codes opnieuw beschouwen, maar dan over $\mathbb{Z}/4\mathbb{Z}$. Om op een nette manier aan te tonen dat de codes daadwerkelijk overeenkomen, is aanzienlijk wat meer nodig dan wat hier gegeven is. In plaats van een bewijs, zullen we daarom het voorbeeld van de kleinste Kerdock code aanhalen, de Nordstrom-Robinson code. Dit geeft in ieder geval weer wat het verschil in complexiteit is.

Om de quaternaire Kerdock codes gemakkelijk te kunnen omschrijven, hebben we eerst de verkorte quaternaire Kerdock codes nodig [21]. Dit zijn codes die worden voorgebracht door reciproke polynomen, waarbij we eerst basis-primitieve polynomomen moeten bepalen.

Definitie 3.4.1. Een polynoom $f(x)$ over $\mathbb{F}_p$ is primitief als er geen enkel niet-inverteerbaar element in $\mathbb{F}_p$ is dat alle coëfficiënten van $f(x)$ deelt.

We maken gebruik van de overgang van $\mathbb{F}_2$ naar $\mathbb{Z}_4$, dus we hebben met slechts een vrij specifiek geval te maken. In $\mathbb{F}_2$ zijn er maar twee elementen, dus behalve het nulpolynoom zijn alle polynomen primitief.

Definitie 3.4.2. Een monisch polynoom $h(x) = \sum_{i=0}^{m} a_i x^i$ van graad $m \geq 1$ over $\mathbb{Z}/4\mathbb{Z}$ is basis-primitief als $\bar{h}(x) = \sum_{i=0}^{m} b_i x^i$ primitief is over $\mathbb{F}_2$, waarbij $b_i \equiv a_i \mod 2$.

Definitie 3.4.3. Zij $h(x) = \sum_{i=0}^{m} h_i x^i$, met $h_0 = h_m = 1$. Dan wordt het reciproke polynoom gegeven door $g(x) = \sum_{i=0}^{m} h_{m-i} x^i$.

Laat $h(x)$ een basis-primitief polynoom van graad $m \geq 2$ over $\mathbb{Z}/4\mathbb{Z}$ zijn zodanig dat $h(x) \mid x^{2^m-1} - 1$. Het bestaan van zo'n polynoom $h(x)$ is een gevolg van het lemma van Hensel, besproken we in de vorige paragraaf. Laat verder $n = 2^m - 1$ en $g(x)$ het reciproke polynoom van $(x^n - 1)/(x - 1)h(x)$, dan kunnen we de volgende codes invoeren.

Definitie 3.4.4. (Verkorte quaternaire Kerdock codes) Een verkorte quaternaire Kerdock code $K(M)^-$ is de quaternaire cyclische code van lengte $2^m - 1$ met als voortbrenger het polynoom $g(x)$. De posities van de coördinaten van de codewoorden zijn genummerd door $0, 1, 2, \ldots, 2^m - 2$.

De uiteindelijke quaternaire Kerdock codes, waarvan het beeld onder de Gray-afbeelding de binaire Kerdock codes geeft, is een kleine variatie op de verkorte versie.

Definitie 3.4.5. (Quaternaire Kerdock codes) De quaternaire Kerdock code $K(m)$ is de code verkregen door het toevoegen van een nulsom symbool aan ieder codewoord van $K(m)^-$ op locatie ∞. Het nulsomsymbool van een codewoord $c \in K(m)^-$ is het getal $s_c \in \mathbb{Z}/4\mathbb{Z}$ zodanig dat $s_c + \sum_{i=0}^{2^m-1} c_i = 0$. Om praktische redenen wordt deze positie vóór positie 0 geplaatst.

We sluiten af met een voorbeeld.

Voorbeeld 3.4.6. ***(Nordstrom Robinson)*** *Een voorbeeld van een quaternaire Kerdock code is de Nordstrom-Robinson code:*

$$\begin{pmatrix} 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{pmatrix}$$

De Gray-afbeelding ($0 \mapsto, 00,\ 1 \mapsto 01,\ 2 \mapsto 11$, en $3 \mapsto 10$) van de code, voortgebracht door de rijvectoren van bovenstaande matrix, is de binaire Nordstrom-Robinson code.

Bibliografie

[1] Bonnecaze, A., Solé, P., Calderbank, A.R., *Quaternary Quadratic Residue Codes and Unimodular Lattices*, IEEE Transactions on Information Theory, Volume 41, no 2 (1995).

[2] Cooke, B., *Reed-Muller Error Correcting Codes*, MIT Undergraduate Journal of Mathemetics (2004).

[3] Conway, J.H., Sloane, N.J.A., *Self-Dual Codes over the Integers Modulo 4*, Journal of Combinatorial Theory, Serie A 62, 30-45 (1993).

[4] Dougherthy, S.T., Masaaki.H., Patrick S., *Shadow Codes over* $\mathbb{Z}/4\mathbb{Z}$, Finite Fields and Their Applications 7, 507-529 (2001).

[5] Eisenbud, D., *Commutative algebra with a view to algebraic geometry*, Graduate Texts in Mathematics, Springer-Verlag New York (2004).

[6] Hall, J.I., *Notes on Coding Theory*, (2003), (niet gepubliseerd).

[7] Honold, T., *A proof of MacWilliams' identity*, Journal of Geometry, Volume 57, Numbers 1-2, 120-122 (1996).

[8] Huffman, W.C., Pless, V., *Fundamentals of error-correcting codes*, Cambridge University Press (2003).

[9] Jeurissen, R.H., Leijenhorst, D.C. van, *Codetheorie*, diktaat van Mathematisch Instituut KU Nijmegen (1998).

[10] Keune, F., *Getallen: van natuurlijk naar imaginair*, uitgeverij Epsilon, Volume 65 (2009).

[11] Lint, J.H. van, *Introduction to coding theory*, Springer-Verlag Berlin Heidelberg New York (1999).

[12] Lint, J.H. van, *Kerdock Codes and Preparata Codes*, Congressus Numerantum, Volume 39, 25-41 (1983).

[13] MacWilliams, F.J., Odlyzko, A.M., Sloane, N.J.A., Ward, H.N., *Self-Dual Codes over GF(4)*, Journal of Combinatorial Theory, Series A 25, 288-318 (1978).

[14] MacWilliams, F.J., Sloane, N.J.O., *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, Volume 16 (1981).

[15] Nebe, G., Rains, E.M., Sloane, N.J.A., *Self-dual codes and invariant theory*, Springer-Verlag Berlin Heidelberg New York (2000).

[16] Nebe, G., Rains, E.M., Sloane, N.J.A., *Codes and invariant theory*, Mathematische Nachrichten, Volume 274-275 Issue 1, Pages 104-116 (2004).

[17] Paranjape, K.H., *Some Lectures on Number Theory, Elliptic Curves and Cryptology*, source: imsc.res.in/ kapil/crypto/notes.

[18] Rains, E.M., Sloane, N.J.A., *Self-Dual codes*, Information Sciences Research (1998).

[19] Sloane, N. J. A., *Algebraic Coding Theory: Recent Developments Related to the Integers Mod 4*, Study of Algebraic Combinatorics, Research Institute for Mathematical Sciences, Kyoto, 38-52 (1995).

[20] Sloane, N.J.A., *Gleason's Theorem on Self-Dual Codes and Its Generalizations*, AT&T Shannon Labs, Flohrham Park, NJ, USA (2006).

[21] Wan, Z.-X., *Quaternary codes*, World Scientific Publishing Co. Pte. Ltd. (1997).

[22] Ward, H. N. e.a., *Coding Theory and Quantum Computing*, an International Conference on Coding Theory and Quantum Computing, University of Virginia (May 20-24, 2003).

[23] Yang, K., Helleset, T., *Two New Infinite Families of 3-Designs from Kerdock Codes over* $\mathbb{Z}/4\mathbb{Z}$, Designs, Codes and Cryptography, 15, p.201-214 (1998).

[24] http://mint.sbg.ac.at, website van de database MinT.

[25] http://www.awm-math.org/noetherbrochure/MacWilliams80.html, webpagina over F. Jessie MacWilliams, onderdeel van 'Profiles of Women in Mathematics'.

[26] http://www2.research.att.com/ njas/doc/Z4.html, website van Sloane met een overzicht van artikelen aangaande 'codes over $\mathbb{Z}/4\mathbb{Z}$'.