Syllabus Coderingstheorie

G. van der Geer & M. van der Vlugt

Tweede Staat van de Syllabus Coderingstheorie van G. van der Geer (UvA) en M. van der Vlugt (UL)

Inleiding

In de coderingstheorie worden methoden ontwikkeld om de betrouwbaarheid en doelmatigheid van communicatiesystemen die digitale informatie verwerken te verhogen. Bij deze systemen wordt informatie getransporteerd via een kanaal dat niet storingsvrij is, waardoor ontvangen informatie kan verschillen van uitgezonden informatie. Het basisprincipe van de coderingstheorie is het toevoegen van controlesymbolen (redundantie) aan de te verzenden berichten, waardoor fouten ontdekt en eventueel verbeterd kunnen worden.

De situatie doet denken aan het gebruik van de natuurlijke talen. Ook hier is veel redundantie in de woorden aanwezig en we gebruiken slechts een klein deel van alle mogelijke lettercombinaties. Door de afspraak alleen de woorden uit het woordenboek te gebruiken herkennen we typefouten vaak gemakkelijk en we kunnen deze meestal eenvoudig corrigeren. (Neem het "dichtstbijzijnde" woord in het woordenboek.) In deze analogie vormt het woordenboek de code en zijn de daarin bevatte woorden de codewoorden.

Een van de fundamenten van de coderingstheorie is het artikel van C. Shannon: "A mathematical theory of communication" uit 1948 waarin hij met stochastische methoden de volgende fundamentele stelling bewees:

Afhankelijk van het kanaal bestaan er codes (= verzamelingen codewoorden) met beperkte redundantie waarbij de kans op een decodeerfout willekeurig klein is.

Het probleem is nu deze goede codes te vinden; goed betekent hierbij
i) de kans op een decodeerfout is klein,
ii) de redundantie blijft beperkt,
iii) het codeer- en decodeermechanisme is vrij eenvoudig.

Hierbij wordt afhankelijk van het communicatiesysteem en de eisen die men daaraan stelt aan elk van deze drie eisen een kleiner of groter gewicht toegekend.

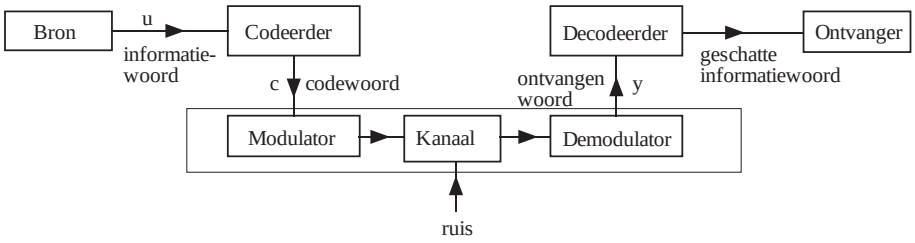
Om deze doelen te bereiken proberen we codes te vinden die struktuur bezitten, bijv. een algebraïsche of combinatorische struktuur. In het college zal de nadruk liggen op de algebraïsche coderingstheorie. De hiermee samenhangende codes worden in de praktijk veel gebruikt.

De coderingstheorie bestaat naast een beperkt deel algemene theorie uit een groot aantal voorbeelden van codes en de bepaling van parameters van zulke codes. Werden in het verleden voornamelijk wapens uit de algebra en de combinatoriek in stelling gebracht voor dit doel, meer recent wordt ook veel gebruik gemaakt van resultaten uit de algebraïsche meetkunde, in het bizonder van de theorie van algebraïsche krommen over eindige lichamen.

Hoofdstuk I. Lineaire Codes

§1. *Inleiding lineaire codes, voortbrengermatrix en toetsmatrix*

Bekijken we de schematische voorstelling van een communicatiesysteem waarin een code gebruikt wordt (zie Fig. 1).



Figuur 1

De bron zendt berichten uit die bestaan uit informatiewoorden van lengte k met letters uit een eindig alfabet van cardinaliteit q. We nemen hiervoor meestal een eindig lichaam $\mathbb{F}_q$. De informatiewoorden zijn dan elementen van de $\mathbb{F}_q$-vectorruimte $\mathbb{F}_q^k$ van k-tallen $(u_1, \ldots, u_k)$ met $u_i \in \mathbb{F}_q$.

De codeerder voegt volgens een of andere regel $n-k$ controlesymbolen toe aan het informatiewoord, waardoor een codewoord van lengte n ontstaat. Men kan zich de codeerder dus voorstellen als een *injectieve* afbeelding:

$$\phi : \mathbb{F}_q^k \to \mathbb{F}_q^n, \quad u = (u_1, ..., u_k) \mapsto x = (x_1, ..., x_n),$$

waarbij het informatiewoord u naar het *codewoord* x wordt gestuurd.

De beeldverzameling $C \subseteq \mathbb{F}_q^n$ heet een *code*, en wel een *blokcode* omdat het codewoord als uitvoer van de codeerder slechts afhangt van één informatiewoord. Codes waarbij de uitvoer van de codeerder op tijdstip t ook afhangt van informatiewoorden op eerdere tijdstippen heten *convolutiecodes*. De codeerder werkt dan met een geheugen. Wij zullen ons steeds met blokcodes bezighouden.

We noemen n de *lengte* van de code en $R = \log_q(\#C)/n$ het *informatiegehalte of rendement* van de code.

(1.1) Definitie. De (blok)code $C \subseteq \mathbb{F}_q^n$ heet *lineair* als de codeerder $\mathbb{F}_q^k \to \mathbb{F}_q^n$ een lineaire afbeelding van $\mathbb{F}_q$-vectorruimten is.

Nu heet k de *dimensie* van de code en $r = n - k$ de *redundantie*. We vinden $R = k/n$ voor het rendement van de (blok)code; we spreken van een (n, k)-lineaire code over $\mathbb{F}_q$ of kortweg (n, k)-code $/\mathbb{F}_q$.

Een (n, k)-code is dus niets anders dan een k-dimensionale lineaire deelruimte van de $\mathbb{F}_q$-vectorruimte $\mathbb{F}_q^n$ van n-tallen $(x_1, \ldots, x_n)$.

Het codewoord x wordt verstuurd via het kanaal. We vatten het kanaal op als een stochastische afbeelding. De decodeerder ontvangt de vector $y \in \mathbb{F}_q^n$; de fout is dus $e = y - x$. De decodeerder zet nu volgens een welbepaalde regel het ontvangen woord y om in een codewoord x'. Hiermee correspondeert via ϕ een element $u' \in \mathbb{F}_q^k$, d.w.z. $\phi(u') = x'$. Dit woord u' gaat naar de ontvanger. De decodeerder is dus een afbeelding $\mathbb{F}_q^n \to \mathbb{F}_q^k$.

Lineaire codes hebben belangrijke voordelen boven niet-lineaire:

1) lineaire codes zijn eenvoudig te beschrijven: het is voldoende een basis van k vectoren te geven;

2) coderen komt neer op matrixvermenigvuldiging en dit is technisch goed uitvoerbaar.

Verder is het in bepaalde opzichten geen beperking als we slechts lineaire codes beschouwen. Bijvoorbeeld, in de stelling van Shannon mogen we het begrip code door lineaire code vervangen.

Vanaf nu zullen al onze codes lineair zijn, tenzij anders wordt vermeld.

Laat C een (n,k)-lineaire code/$\mathbb{F}_q$ zijn met basis $x_1, ..., x_k$. Ten opzichte van een basis van $\mathbb{F}_q^n$ (waarvoor we steeds de standaardbasis zullen nemen) kan men de coördinatenmatrix van $x_1, ..., x_k$ opstellen

$$G = \begin{pmatrix} x_{11} & x_{12} & ... & ... & x_{1n} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ x_{k1} & x_{k2} & ... & ... & x_{kn} \end{pmatrix},$$

waar de rijen de vectoren x_j voorstellen.

De $k \times n-$matrix G heet een *voortbrengermatrix* of *generatormatrix* van C en deze levert een codeervoorschrift (codeerder)

$$\mathbb{F}_q^k \to \mathbb{F}_q^n, \quad u \mapsto uG.$$

We beginnen nu met een aantal voorbeelden van lineaire codes.

(1.2) Voorbeelden van binaire codes (d.w.z. over $\mathbb{F}_2$):

i) Zij C de code met $G = (11111)$ zodat de codeerder is: $u \mapsto (u, u, u, u, u)$. Deze code heet de $(5,1)$-repetitie-code. Deze bestaat uit twee vectoren: $C = \{\underline{0}, \underline{1}\}$.

ii) Zij C de $(6,3)$-code gegeven door de codeerder

$$u = (u_1, u_2, u_3) \mapsto (u_1 + u_2 + u_3, u_3, u_2 + u_3, u_1 + u_2, u_1, u_2).$$

Een voortbrengermatrix is hier:

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

iii) De $(7,4)$ Hamming code is een code met codeerder:

$$(u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_3, u_4, u_2 + u_3 + u_4, u_1 + u_3 + u_4, u_1 + u_2 + u_4).$$

Bepaal een voortbrengermatrix.

Een $k \times n$-matrix is een matrix in *gereduceerde rijentrapvorm* als

i) het meest linkse element $\neq 0$ in een rij gelijk aan 1 is,

ii) een kolom die zo een meest linkse 1 bevat verder alleen uit nullen bestaat,

iii) de matrix in trapvorm is (d.w.z. als de meest linkse 1 in rij i op plaats j_i staat, dan $j_1 < j_2 < \ldots < j_k$.).

Met behulp van elementaire lineaire algebra zien we in dat er onder de verschillende voortbrengermatrices van een lineaire code C er precies één is in *gereduceerde rijentrapvorm*. Een voorbeeld:

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

$$\sim \begin{pmatrix} \underline{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \underline{1} & 0 & 1 \\ 0 & 0 & 0 & \underline{1} & 1 \end{pmatrix} = G'.$$

Als we nu G' als codeerder gebruiken dan wordt het codeervoorschrift

$$(u_1, u_2, u_3) \mapsto (\underline{u}_1, u_1, \underline{u}_2, \underline{u}_3, u_1 + u_2 + u_3).$$

Dus bij gebruik van een voortbrengermatrix in gereduceerde rijentrapvorm is het informatiewoord een deel van het codewoord. Een codeerder met deze eigenschap heet *systematisch*. De bijbehorende code heet een *systematische code*. Lineaire codes zijn dus systematische codes.

(1.3) Definitie. Twee (n, k)-codes over $\mathbb{F}_q$, zeg C_1 en C_2, heten *equivalent* (notatie: $C_1 \sim C_2$) als ze uit elkaar te verkrijgen zijn via een permutatie van de coördinaatplaatsen en een vermenigvuldiging met een element uit $\mathbb{F}_q^*$ per coördinaatplaats. Schematisch

$$C_2 = C_1 \cdot P \cdot D,$$

met P een $n \times n$-permutatiematrix en D een niet-singuliere $n \times n$ diagonaalmatrix.

Het zal blijken dat bij geheugenloze kanalen equivalente codes dezelfde corrigerende eigenschappen hebben.

(1.4) Stelling. *Elke (n, k)-code is equivalent met een lineaire code die een generatormatrix heeft van het type*

$$G = (I_k | A),$$

waarbij I_k de $k \times k$-eenheidsmatrix is.

Bewijs. Pas een geschikte permutatiematrix toe op de kolommen van de voortbrengermatrix in gereduceerde rijentrapvorm. □

Zo een G heet een *voortbrengermatrix in standaardvorm*. We zullen ons vaak beperken tot lineaire codes die een voortbrengermatrix in standaardvorm hebben. Op equivalentie na is dit geen beperking van de algemeenheid. Gebruik van zo een $G = (I_k|A)$ als codeerder levert een codeervoorschrift van de vorm

$$(u_1, ..., u_k) \mapsto (u_1, ..., u_k, *, *, ..., *) = (u, uA),$$

waarbij de sterretjes $n-k$ *controlesymbolen* aangeven.

Bij de generatormatrix interpreteren we $C \subset \mathbb{F}_q^n$ als beeld van $\mathbb{F}_q^k$. We kunnen C ook interpreteren als kern van de lineaire afbeelding (quotiëntafbeelding)

$$\mathbb{F}_q^n \to \mathbb{F}_q^n / C.$$

Bij deze interpretatie hoort een zogenaamde *parity-check-* of *toetsmatrix*.

Een *parity-check* of *toets* voor een lineaire code is een lineaire vergelijking

$$a_1 x_1 + ... + a_n x_n = 0 \qquad (\text{met } a_i \in \mathbb{F}_q)$$

waaraan alle $x = (x_1, ..., x_n) \in C$ voldoen.

(1.5) Definitie. De *duale code* $C^\perp$ van C is

$$\{a \in \mathbb{F}_q^n : (a, x) = 0 \text{ voor alle } x \in C\},$$

waarbij (a, x) staat voor het inproduct $\sum_{i=1}^n a_i x_i$ in $\mathbb{F}_q^n$.

De lineaire deelruimte $C^\perp$ van $\mathbb{F}_q^n$ is een $(n, n-k)$-lineaire code over $\mathbb{F}_q$.

(1.6) Definitie. Een voortbrengermatrix van $C^\perp$ heet een *parity-check matrix* of ook wel *toetsmatrix* van C.

Uit een toetsmatrix van C kunnen we C weer terugvinden :

(1.7) Propositie. *Als H een toetsmatrix is van C dan geldt*

$$C = \{x \in \mathbb{F}_q^n : Hx^t = 0\}.$$

(We mogen de conditie $Hx^t = 0$ natuurlijk ook schrijven als $xH^t = 0$.)

Bewijs. Omdat $C \subseteq (C^\perp)^\perp$ en $\dim(C) = \dim(C^\perp)^\perp$ geldt $C = (C^\perp)^\perp$. Laat H een voortbrengermatrix van $C^\perp$ zijn met als rijvectoren a_i voor $i = 1, ..., n-k$. Dan vinden we

$$C = (C^\perp)^\perp = \{x \in \mathbb{F}_q^n : (a_i, x) = 0, \quad i = 1, ..., n-k\} = \{x \in \mathbb{F}_q^n : Hx^t = 0\}. \quad \square$$

(1.8) Lemma. *Als C een (n,k)-code is met voortbrengermatrix G dan is een $(n-k, n)$-matrix H met rang $n-k$ een toetsmatrix dan en slechts dan als $GH^t =$ nulmatrix.* $\square$

Opmerking. Bij een voortbrengermatrix in standaardvorm $G = (I_k|A)$ hoort een toetsmatrix in de vorm: $H = (-A^t|I_{n-k})$. Als de voortbrengermatrix G in gereduceerde rijentrapvorm is en P een permutatiematrix is met $GP = (I_k|A)$ dan is $H = (-A^t|I_{n-k})P^{-1}$ een toetsmatrix.

§2. *Syndroomdecodering van lineaire codes.*

Als een woord $x \in \mathbb{F}_q^n$ wordt verzonden via het kanaal en een woord $y \in \mathbb{F}_q^n$ wordt ontvangen, dan heet $e = y - x$ de *fout* of het *foutenpatroon*. Als $e_i \neq 0$ dan is er op de i-de plaats een fout ontstaan. Om te decoderen moet een decodeervoorschrift worden opgesteld, d.w.z. aan elke ontvangen $y \in \mathbb{F}_q^n$ moet een $x \in C$ worden toegevoegd. We

denken ons het kanaal als een stochastische afbeelding tussen de ruimten "Invoer kanaal" en "Uitvoer kanaal", zodat het zinvol is te spreken van de waarschijnlijkheid dat een bepaalde fout optreedt.

We bekijken nu twee decodeervoorschriften.
Decodeervoorschrift I : de ontvangen y wordt gedecodeerd als een $x \in C$ waarvoor de voorwaardelijke waarschijnlijkheid $p(x|y)$ maximaal is. Dit decodeervoorschrift heet MED (minimale fout-decodering/ minimum error probability decoding) omdat de kans op een decodeerfout bij ontvangen y wordt geminimaliseerd.
Decodeervoorschrift II : de ontvangen y wordt gedecodeerd als $x \in C$ waarvoor de voorwaardelijke waarschijnlijkheid $p(y|x)$ maximaal is. Dit voorschrift heet MLD (maximale waarschijnlijkheid- decodering/ maximum likelihood decoding). Als alle codewoorden even waarschijnlijk zijn komt dit neer op het maximaliseren van $p(x|y)$.

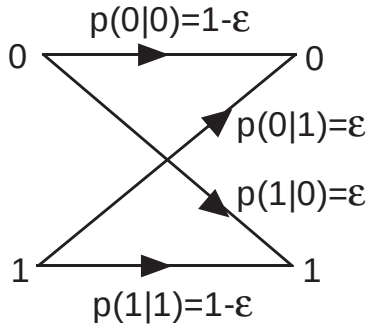
Vanaf nu nemen we aan dat alle codewoorden even waarschijnlijk zijn en werken MLD nader uit. Daartoe moet het kanaal waarover wordt gezonden nader worden gespecificeerd. Wij zullen hier in het vervolg aannemen dat het kanaal een *geheugenloos q-ledig symmetrisch kanaal (qSC)* is. Dit betekent het volgende.

i) Een ontvangen symbool y_i is slechts afhankelijk van één uitgezonden symbool x_i (geheugenloos);

ii) voor alle i geldt voor de overgangswaarschijnlijkheden $p(y_i|x_i) = \epsilon$ als $y_i \neq x_i$, en $p(y_i|x_i) = 1 - (q-1)\epsilon$ als $y_i = x_i$ (symmetrisch).

Uit i) volgt dat $p(y|x) = \prod_{i=1}^{n} p(y_i|x_i)$.

Voorbeeld. Schematische voorstelling van het binair symmetrisch kanaal.



We kunnen nu voor het q-ledige symmetrisch kanaal de voorwaardelijke waarschijnlijkheid $p(y|x)$ berekenen.

Daartoe introduceren we het *(Hamming-)gewicht* $w(z)$ van een element $z \in \mathbb{F}_q^n$:

$$w(z) = \#\{i \in \{1, 2, ..., n\} : z_i \neq 0\}.$$

Er geldt nu:

$$p(y|x) = \prod_{i=1}^{n} p(y_i|x_i) = \epsilon^{w(y-x)} \cdot (1 - (q-1)\epsilon)^{n-w(y-x)}.$$

Als nu $\epsilon < 1/q$ dan is het rechterlid een dalende functie van $w(y-x)$. Voor het gekozen kanaal met $\epsilon < 1/q$ leidt MLD dus tot het decodeervoorschrift:

zoek bij de ontvangen y een $x \in C$ waarvoor $e = y - x$ een minimaal gewicht heeft.

Of

zoek een $x \in C$ die op zo weinig mogelijk plaatsen verschilt van y.

Dit decodeervoorschrift heet *nabuurdecoderen* (NND, nearest neighbour decoding).

Merk nu op dat de verzameling

$$\{y - x : x \in C\} = y + C$$

van alle mogelijke foutenpatronen bij de ontvangen y precies een nevenklasse van C in $\mathbb{F}_q^n$ is. Nabuurdecoderen komt dus neer op het zoeken van een element van minimaal gewicht in de nevenklasse $y+C$ van het ontvangen woord y. Zo een element van minimaal gewicht heet een *nevenklassehoofd* (of *coset leader*). (Zo een element hoeft niet uniek te zijn.) Voor deze manier van decoderen gebruikt men de zgn. *standaardtabel* van de code. Dit is een tabel waarvan de eerste rij bestaat uit de codewoorden beginnend met $0 \in C$. De volgende rijen bestaan uit de (andere) nevenklassen in $\mathbb{F}_q^n$ van C waarbij links altijd een nevenklassehoofd staat.

Voorbeeld Standaardtabel

$C \rightarrow$	000000 001011 010101 100110 011110 101101 110011 111000
	000001 001010 010100 100111 011111 101100 110010 111001
	000010 001001 010111 100100 011100 101111 110001 111010
	000100 001111 010001 100010 011010 101001 110111 111100
	001000 000011 011101 101110 010110 100101 111011 110000
	010000 011011 000101 110110 001110 111101 100011 101000
	100000 101011 110101 000110 111110 001101 010011 011000
	100001 101010 110100 000111 111111 001100 010010 011001

Benodigde zoektijd en opslagruimte maken decoderen met behulp van de standaardtabel bij grote n en k onbruikbaar. Zoals we nu zullen zien kan er met de toetsmatrix van de code veel efficiënter gedecodeerd worden.

De verzameling van nevenklassen van C kan geïdentificeerd worden met de elementen van de quotiëntruimte $\mathbb{F}_q^n/C$. Dit is een $(n-k)$-dimensionale $\mathbb{F}_q$-vectorruimte. Als we nu een toetsmatrix H van C hebben kunnen we deze quotiëntruimte identificeren met $\mathbb{F}_q^{n-k}$ op de volgende manier: de lineaire afbeelding

$$\mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-k}, \quad x \mapsto s = Hx^t$$

heeft als kern precies C en geeft dus aanleiding tot een isomorfisme $\mathbb{F}_q^n/C \rightarrow \mathbb{F}_q^{n-k}$.

De uitdrukking $s(x) = Hx^t$ heet het *syndroom* van $x \in \mathbb{F}_q^n$. Er geldt

$$s(x) = 0 \Leftrightarrow x \in C.$$

Het syndroom hangt slechts af van het foutenpatroon e en niet van het uitgezonden woord x; immers, $s = Hy^t = H(x^t + e^t) = He^t$.

Om nu snel te kunnen decoderen maken we een lijst van de syndromen en bijbehorende nevenklassehoofden. Syndroomdecodering verloopt dan als volgt:

i) bepaal voor een ontvangen y het syndroom $s = Hy^t$;

ii) zoek het nevenklassehoofd e van s in de lijst;

iii) decodeer: $x = y - e$.

Voor syndroomdecodering bij andere kanalen neemt men als nevenklassehoofden die foutenpatronen die bij het gegeven kanaal het meest waarschijnlijk zijn.

Voorbeeld. Neem de binaire (6.3)-code uit het voorbeeld van de standaardtabel met voortbrengermatrix G

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

De syndroomtabel die ontstaat via de kanonieke toetsmatrix H bij G is:

syndroom	*nevenklassehoofd*
000	000000
001	000001
010	000010
100	000100
011	001000
101	010000
110	100000
111	100001

(Ga na.)

We besluiten deze paragraaf met een eenvoudig voorbeeld van foutencorrectie met een code.

Voorbeeld. Beschouw de binaire $(7, 4)$-code met controlematrix H waarvan de kolommen de binaire representaties van de gehele getallen $1, ..., 7$ zijn:

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

Stel dat we een woord x verzenden en $x + e$ ontvangen. Neem aan dat $w(e) \leq 1$, m.a.w. er is op hoogstens één plaats een fout gemaakt. Dan geldt: òf $Hx^t = 0$ (als $x \in C$) òf Hx^t is de binaire representatie van de plaats van de fout. Dus fouten met $w(e) = 1$ kunnen we eenvoudig corrigeren.

§3. *Het vermogen van een code om fouten te corrigeren.*

In de vorige paragraaf hebben we gezien dat de nevenklassehoofden de corrigeerbare foutenpatronen zijn. Bepaling en opslag van een syndroomtabel is bij grote codes en redundantie onpraktisch. Om ook zonder zo een tabel uitspraken te kunnen doen over het foutcorrigerend vermogen van een code voeren we een metriek in op $\mathbb{F}_q^n$ als volgt.Met het *Hamming gewicht*

$$w(x) = \#\{i : x_i \neq 0\}$$

van een vector $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ kunnen we een afstand definiëren op $\mathbb{F}_q^n$:

$$d(x, y) = \#\{i : x_i \neq y_i\} = w(y - x).$$

Hiermee wordt $\mathbb{F}_q^n$ een metrische ruimte en de afstandsfunctie is translatie-invariant: $d(x+z, y+z) = d(x, y)$. (Ga na.)

Opmerking. Als x_1 en x_2 in $\mathbb{F}_q^n$ woorden zijn met $d(x_1, x_2) = m$ dan zijn er woorden $y_1 = x_1, y_2, \ldots, y_m, y_{m+1} = x_2$ met $d(y_i, y_{i+1}) = 1$ voor $i = 1, \ldots, m$. Geldt $m \leq 2t$ dan zijn de ballen met straal t om x_1 en x_2 niet disjunct.

In het vervolg gaan we uit van de veronderstelling dat het voorkomen van alle codewoorden uit een gegeven code C even waarschijnlijk is; we passen dan het decodeervoorschrift NND (nabuurdecoderen) toe: *zoek bij het ontvangen woord $y \in \mathbb{F}_q^n$ een $x \in C$ waarvoor $d(x, y)$ minimaal is.*

(3.1) Stelling. *Alle foutenpatronen met op $\leq t$ plaatsen een fout worden bij decodering gecorrigeerd $\iff$ $d(x, x') \geq 2t + 1$ voor alle $x, x' \in C$ met $x \neq x'$.*

Bewijs. Alle foutenpatronen van gewicht $\leq t$ worden juist gedecodeerd $\iff$ de bollen met straal t om de codewoorden zijn disjunct $\iff$ $d(x, x') \geq 2t+1$ voor alle paren x, x' met $x \neq x'$. (Zie bovenstaande opmerking.) $\square$

Als $d(x, x') = 2t$ raken de bollen met straal t om de codewoorden elkaar. Foutenpatronen met op t plaatsen een fout worden wel ontdekt maar niet altijd juist gedecodeerd.

(3.2) Definitie. De *minimumafstand* $d(C)$ van een code C wordt gedefinieerd als volgt:

$$d(C) = \min\{d(x, x') : x \in C, x' \in C, x \neq x'\}.$$

De conclusie van (3.1) kan nu geformuleerd worden als:

een code corrigeert alle foutenpatronen van gewicht $\leq t \quad \iff \quad t \leq [(d(C)-1)/2]$.

Voor een code zijn lengte, aantal woorden en minimumafstand de belangrijkste parameters. Hierbij is de minimumafstand meestal het lastigst te bepalen. Voor lineaire codes hoeft men om d te bepalen niet alle afstanden tussen de woorden uit te rekenen vanwege

$$d(x, x') = w(x - x') \quad \text{en} \quad x - x' \in C,$$

zodat

$$d = \textit{minimumgewicht} \; = \min_{x \in C, x \neq 0} w(x)$$

en we alleen de gewichten van alle woorden hoeven te kennen.

Soms kan men de minimumafstand eenvoudig bepalen m.b.v. een toetsmatrix van C.

(3.3) Propositie. *Als C een lineaire code is $/\mathbb{F}_q$ met toetsmatrix H dan is $d(C)$ gelijk aan het minimale aantal kolommen van H dat lineair afhankelijk is.*

Bewijs. Laat k_i met $i = 1, ..., n$ de kolommen van H zijn. Dan geldt: $x = (x_1, ..., x_n)$ ligt in $C \iff Hx^t = \sum_{i-1}^{n} x_i k_i = 0$, waar de nul staat voor de nulkolom. Een codewoord van gewicht $w \neq 0$ levert een niet-triviale relatie tussen w kolommen van H. $\square$

(3.4) Voorbeeld. De binaire $(7,4)$-Hamming code uit (1.2. iii) heeft toetsmatrix

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

Uit Proposition 3.3 volgt dat de minimumafstand $d = 3$, zodat alle fouten van gewicht 1 gecorrigeerd kunnen worden. (Vgl. ook het voorbeeld aan het eind van de vorige paragraaf.)

§4. *De kans op een decodeerfout en de gewichtsverdeling van een code*

Zij P_E de kans op een decodeerfout, d.w.z. de kans dat het resultaat van de decodeerder bij het decoderen van een woord onjuist is. Bij syndroomdecodering ontstaat precies dan een decodeerfout als het foutenpatroon niet gelijk is aan het nevenklassehoofd:

$$P_E = p(\text{foutenpatroon} \neq \text{nevenklassehoofd}).$$

Neem nu aan dat het kanaal een binair symmetrisch kanaal is met kans op een kanaalfout per symbool gelijk aan ϵ. Als e een nevenklassehoofd is met gewicht $w(e)$ dan vinden we

$$p(\text{foutenpatroon} = e) = \epsilon^{w(e)}(1-\epsilon)^{n-w(e)},$$

waarbij n de lengte van de code is.

Laat α_i het aantal nevenklassehoofden van gewicht i zijn. Dan vinden we

$$P_E = 1 - \sum_{i=0}^{n} \alpha_i \epsilon^i (1-\epsilon)^{n-i}.$$

Omdat syndroomdecodering op een binair symmetrisch kanaal (bSC) een vorm van MED is geldt voor ieder ander decodeervoorschrift bij lineaire codes op zo een kanaal:

$$P_E \geq 1 - \sum_{i=0}^{n} \alpha_i \epsilon^i (1-\epsilon)^{n-i}.$$

Bepaling van de α_i is meestal erg lastig en geldt als een van de moeilijkste problemen uit de coderingstheorie.

(4.1) Definitie. Als $\alpha_i = 0$ voor $i > t = [(d(C)-1)/2]$ met $d(C)$ de minimumafstand van C dan heet C *een perfecte (t-fouten corrigerende) lineaire code.*

Algemeen geldt dat woorden uit $\mathbb{F}_q^n$ van gewicht $\leq [(d(C)-1)/2]$ nevenklassehoofden zijn omdat op grond van de driehoeksongelijkheid elke nevenklasse precies een zo'n woord kan bevatten. Voor een perfecte code zijn de woorden van gewicht $s \leq [(d(C)-1)/2]$ precies de nevenklassehoofden. Hieruit volgt dat de bollen om de codewoorden met straal $[(d(C)-1)/2] = t$ niet alleen disjunct zijn maar ook heel $\mathbb{F}_q^n$ overdekken. Dit laatste neemt men als definitie van een niet noodzakelijk lineaire t-fouten corrigerende perfecte code.

Behalve voor het corrigeren van fouten kan men een lineaire code (van lengte n) ook gebruiken voor het opsporen (detecteren) van fouten. Als de code uitsluitend voor foutdetectie wordt gebruikt worden alle patronen van $t \leq d(C) - 1$ fouten ontdekt. Er ontstaat een decodeerfout als een ontvangen woord onterecht als een uitgezonden woord wordt geaccepteerd. Dit gebeurt als voor een uitgezonden woord $x \in C$ met fout $e \neq 0$ geldt $x + e \in C$, d.w.z. $e \in C$. De kans op zo een niet ontdekte fout is

$$\sum_{x \in C, x \neq o} p(\text{fout} = x) = \sum_{i=1}^{n} A_i \epsilon^i (1-\epsilon)^{n-i}, \quad \text{waarbij } A_i = \#\{x \in C : w(x) = i\}.$$

(4.2) Definitie. Als C een lineaire code is in $\mathbb{F}_q^n$ dan heet het polynoom

$$A(z) = \sum_{x \in C} z^{w(x)} = A_0 + A_1 z + ... + A_n z^n \quad (\in \mathbb{Z}[z])$$

met

$$A_i = \#\{x \in C : w(x) = i\}$$

het *gewichtsverdelingspolynoom* van C.

Het gewichtsverdelingspolynoom speelt ook een belangrijke rol bij de bepaling van de kans op een decodeerfout. Dit moge blijken uit het volgende resultaat:

(4.3) Stelling. (McEliece) Als C een lineaire code is die wordt gebruikt bij communicatie over een geheugenloos kanaal met MLD dan geldt: $P_E < A(\gamma) - 1$, waarbij γ van het kanaal afhangt. □

Voor een binair symmetrisch kanaal met kanaalfoutkans ϵ hebben we: $\gamma = 2\sqrt{\epsilon(1-\epsilon)}$.

§5. *De formule van MacWilliams*

De formule van MacWilliams – bewezen in 1963– is een van de fundamentele resultaten uit de coderingstheorie. Zij geeft een verband tussen de gewichtsverdeling van een lineaire code en die van de duale code.

(5.1) Stelling. *Zij $A(z)$ het gewichtspolynoom van een lineaire code C van dimensie k en lengte n over $\mathbb{F}_q$. Dan wordt het gewichtspolynoom $B(z)$ van de duale code $C^\perp$ gegeven door*

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

Het bewijs van deze stelling berust op enkele resultaten uit de harmonische analyse (over eindige lichamen).

Neem een niet triviaal karakter χ op de additieve groep $\mathbb{F}_q^+$, d.w.z. een niet-triviaal homomorfisme $\chi : \mathbb{F}_q^+ \to \mathbb{C}^*$. Definieer voor $x \in \mathbb{F}_q^n$ de functie

$$\chi_x : \mathbb{F}_q^n \to \mathbb{C}^*, \quad y \mapsto \chi((x, y)).$$

(5.2) Lemma. *Als $C \subset \mathbb{F}_q^n$ een lineaire deelruimte is, dan geldt*

$$\sum_{y \in C} \chi_x(y) = \begin{cases} \#C & \text{als } x \in C^\perp, \\ 0 & \text{als } x \notin C^\perp. \end{cases}$$

Bewijs. Het eerste geval is eenvoudig. Neem nu aan dat $x \notin C^\perp$. Dan is er een $y' \in C$ met $\chi_x(y') \neq 1$. We vinden dan

$$\sum_{y \in C} \chi_x(y) = \sum_{y \in C} \chi_x(y + y') = \chi_x(y') \sum_{y \in C} \chi_x(y)$$

en hieruit volgt de bewering direct. □

Zij f een afbeelding $\mathbb{F}_q^n \to V$, waar V een $\mathbb{C}$-vectorruimte is. Dan wordt de *Fourier-getransformeerde* van f gedefinieerd als de afbeelding

$$\hat{f}\colon \mathbb{F}_q^n \to V, \quad y \mapsto \sum_{x \in \mathbb{F}_q^n} \chi_x(y) f(x).$$

(5.3) Lemma. *(Poisson sommatieformule) Voor elke lineaire deelruimte $C \subset \mathbb{F}_q^n$ geldt:*

$$\sum_{y \in C} \hat{f}(y) = (\#C) \sum_{x \in C^\perp} f(x).$$

Bewijs. Er geldt

$$\sum_{y \in C} \hat{f}(y) = \sum_{y \in C} \sum_{x \in \mathbb{F}_q^n} \chi_x(y) f(x) = \sum_{x \in \mathbb{F}_q^n} f(x) \sum_{y \in C} \chi_x(y) =$$

$$= (\#C) \sum_{x \in C^\perp} f(x). \qquad \square$$

Bewijs van Stelling (5.1). Neem als afbeelding $f\colon \mathbb{F}_q^n \to \mathbb{C}[z]$ de afbeelding gegeven door

$$x \mapsto z^{w(x)}.$$

Nu geldt

$$\sum_{y \in C} \hat{f}(y) = (\#C) \sum_{x \in C^\perp} z^{w(x)} = (\#C) B(z).$$

Definieer de functie w op $\mathbb{F}_q$ via $w(0) = 0$ en $w(x) = 1$ als $x \neq 0$. Dan krijgen we

$$\hat{f}(y) = \sum_{x \in \mathbb{F}_q^n} \chi_x(y) z^{w(x)} = \sum_{x = (x_1, \ldots, x_n)} z^{w(x_1) + \ldots + w(x_n)} \chi(x_1 y_1 + \ldots + x_n y_n) =$$

$$= \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} z^{w(x_1)} \chi(x_1 y_1) \cdot \ldots \cdot z^{w(x_n)} \chi(x_n y_n) =$$

$$= \prod_{i=1}^{n} (\sum_{x \in \mathbb{F}_q} \chi(xy_i) z^{w(x)}).$$

Uit (5.2) volgt:

$$\sum_{x \in \mathbb{F}_q} \chi(xy_i) z^{w(x)} = \begin{cases} 1 + (q-1)z & \text{als } y_i = 0 \\ 1 - z & \text{als } y_i \neq 0. \end{cases}$$

Dus we zien

$$\hat{f}(y) = (1-z)^{w(y)} (1 + (q-1)z)^{n - w(y)}$$

zodat

$$\sum_{y \in C} \hat{f}(y) = (1 + (q-1)z)^n \sum_{y \in C} (\frac{1-z}{1+(q-1)z})^{w(y)} =$$

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

□

Het bepalen van de gewichtsverdeling van grote codes is een moeilijk probleem. Soms kunnen we snel informatie krijgen door naar de duale te kijken, bijvoorbeeld als voor vaste n de dimensie k van C groot is. Dan is namelijk de dimensie $n - k$ van de duale $C^\perp$ klein en daardoor is de gewichtsverdeling van $C^\perp$ eenvoudiger te bepalen. Met de MacWilliams-formule volgt dan de gewichtsverdeling van C.

Voorbeeld. Laat C de binaire code zijn met voortbrengermatrix

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

Een toetsmatrix van C is

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

Nu is H een voortbrengermatrix van $C^\perp$ zodat $B_0 = 1, B_2 = 1$, en $B_4 = 2$ en $B(z) = 1 + z^2 + 2z^4$. Voor C vinden we nu

$$A(z) = \frac{1}{4}(1+z)^5 B(\frac{1-z}{1+z}) = 1 + 3z^2 + 3z^3 + z^5.$$

De formule van MacWilliams impliceert identiteiten tussen de A_i's en de B_i's. Deze kan men soms gebruiken om onbekende A_i of B_i te bepalen.

We geven een voorbeeld van zulke identiteiten voor het binaire geval met $q = 2$. Door substitutie van $w = z - 1$ gaat (5.1) over in:

$$B(1+w) = 2^{-k}(2+w)^n A(\frac{-w}{2+w}),$$

ofwel

$$\sum_{i=0}^{n} B_i(1+w)^i = 2^{-k}\sum_{i=0}^{n} A_i(-w)^i(2+w)^{n-i}.$$

Uitwerking hiervan en vergelijken van coëfficiënten van w^s levert

(5.4) Formule.

$$\sum_{i=0}^{n}\binom{i}{s}B_i = 2^{n-s-k}\sum_{i=0}^{n}(-1)^i\binom{n-i}{s-i}A_i \quad (s=0,1,...,n).$$

Als nu de B_i's bekend zijn op $B_{j_1},...,B_{j_t}$ na en $A_0,...,A_{t-1}$ zijn bekend, dan volgen de ontbrekende B_i's eenduidig uit de identiteiten van (5.4). Voor $s=0,1,...,t-1$ leiden de identiteiten namelijk tot een stelsel van t lineaire vergelijkingen met onbekenden $B_{j_1},...,B_{j_t}$ en coëfficiëntendeterminant $\neq 0$.

Opgaven Hoofdstuk 1

Indien niet nadrukkelijk anders vermeld zijn codes binair.

1) Gegeven is de $(6,3)$-code C met voortbrengermatrix

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

i) Bepaal de voortbrengermatrix in gereduceerde rijentrapvorm.
ii) Bepaal een toetsmatrix voor C.
iii) Bereken de minimumafstand d van C.
iv) Codeer het informatiewoord (101) met de gereduceerde codeerder.
v) Decodeer (111010), (000011), (101010) en (100110) volgens NND.
vi) Bepaal de nevenklassenhoofden voor de nevenklassen van C; geef de standaardtabel voor C en een syndroomtabel.
vii) Decodeer (100110) via de syndroomtabel.

2) Beantwoord dezelfde vragen als in Opgave 1) voor de $(6,3)$-code C met voortbrengermatrix

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

3) i) Bewijs dat de volgende twee matrices equivalente codes voortbrengen:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

ii) Bewijs dat de volgende matrices equivalente codes voortbrengen:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

4) Ga na of de codes uit Opg. 1 en Opg. 2 equivalent met elkaar zijn.

5) Zij C de code met toetsmatrix

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

Decodeer (110110) en (010100).

6) Over een binair kanaal moeten woorden van lengte 6 verzonden worden. De enige foutenpatronen die kunnen optreden zijn:

$$(000000), (000001), (000011), (000111), (001111), (011111), (111111).$$

Geef een lineaire code van lengte 6, met een zo groot mogelijk rendement, waarmee deze fouten te corrigeren zijn.

7) i) Bewijs dat in een lineaire code alle woorden met een 0 beginnen of dat er evenveel met een 0 als met een 1 beginnen.
ii) Bewijs dat in een lineaire code alle woorden even gewicht hebben of dat er evenveel woorden van even als van oneven gewicht zijn.

8) Bewijs dat voor $x, y \in \mathbb{F}_2^n$ geldt

$$w(x+y) = w(x) + w(y) - 2w(x * y),$$

waarbij $x * y = (x_1y_1, \ldots, x_ny_n)$ als $x = (x_1, \ldots, x_n)$ en $y = (y_1, \ldots, y_n)$.

9) Toon aan dat de woorden van even gewicht in $\mathbb{F}_2^n$ een $(n, n-1)$-code vormen. Geef een voortbrengermatrix in gereduceerde rijentrapvorm en een toetsmatrix van deze code.

10) Gegeven is een lineaire code C met $C \subseteq C^\perp$. i) Bewijs dat elk codewoord even gewicht heeft. ii) Bewijs dat als het gewicht van elke rij van een voortbrengermatrix van C een viervoud is, er geldt $w(x) \equiv 0 (\mathrm{mod} 4)$ voor alle $x \in C$.

11) i) Als C een lineaire code is in $\mathbb{F}_2^n$ en $x \in \mathbb{F}_2^n$ dan is $C \cup x + C$ ook een lineaire code.
ii) Laat n oneven zijn en laat C een $(n, (n-1)/2)$-code zijn met $C \subseteq C^\perp$. Bewijs dat $C^\perp = C \cup \underline{1} + C$ met $\underline{1} = (1, \ldots, 1)$.

12) i) Een code kan alle patronen van $\leq s$ fouten ontdekken $\iff$ $s < d(C)$. Bewijs dit.
ii) Een code C kan gebruikt worden om alle patronen van $\leq t$ fouten te corrigeren en alle patronen van $> t$ en $\leq s$ fouten te ontdekken (met $s > t$) als $s + t < d(C)$. Bewijs dit.
iii) Een code C kan gebruikt worden om alle patronen van $\leq t$ fouten en $\leq s$ uitwissingen te corrigeren als $s + 2t < d(C)$. Bewijs dit.

13) Gegeven is het lichaam $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ met $\alpha^2 + \alpha + 1 = 0$. De code $C/\mathbb{F}_4$ heeft voortbrengermatrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha \\ 0 & 0 & 1 & 1 & 1+\alpha \end{pmatrix}.$$

Toon aan dat C een perfecte code is.

14) i) Laat C een lineaire code zijn met $w(x) \equiv 0(\text{mod}4)$ voor alle $x \in C$. Bewijs dat $C \subseteq C^{\perp}$.
ii) Laat C een $(24, 12, 8)$ code zijn met $w(x) \equiv 0(\text{mod}4)$ voor alle $x \in C$. Bereken de gewichtsverdeling van C.

15) Bewijs de volgende identiteiten van MacWilliams:

$$\sum_{i=0}^{n} \binom{n-i}{s} B_i = 2^{n-s-k} \sum_{i=0}^{n} \binom{n-i}{s-i} A_i \quad \text{voor} \quad s = 0, \ldots, n.$$

Hoofdstuk II. Grenzen voor lineaire codes.

§1. *Een voorbeeld: Hamming codes*

In deze paragraaf beschouwen we lineaire codes $/\mathbb{F}_q$ die één fout verbeteren, d.w.z. die minimumafstand $d = 3$ hebben. Bij gebruik van $r \geq 2$ controlesymbolen heeft een toetsmatrix van zo een code r rijen. Op grond van (3.3) moet elk tweetal kolommen onafhankelijk zijn. Dat betekent dat geen tweetal kolomvectoren op dezelfde lijn door de oorsprong van $\mathbb{F}_q^r$ ligt. Het komt er dus op neer een maximaal aantal verschillende punten uit de $r-1$-dimensionale projectieve ruimte over $\mathbb{F}_q$, dwz uit $\mathbb{P}^{r-1} = \mathbb{P}(\mathbb{F}_q^r)$ te kiezen (zie Aanhangsel voor de definitie van projectieve ruimte). We weten $\#\mathbb{P}^{r-1}(\mathbb{F}_q) = (q^r-1)/(q-1)$.

(1.1) Definitie. Laat $r \geq 2$ en $n = (q^r-1)/(q-1)$. Dan is de $(n, n-r)$-*Hamming code* $/\mathbb{F}_q$ een code met als toetsmatrix een matrix bestaande uit een maximaal stelsel paarsgewijs onafhankelijke kolommen uit $\mathbb{F}_q^r$ die elk als eerste component $\neq 0$ een 1 hebben.

Uit de definitie volgt dat de minimumafstand d van een Hamming code 3 is; Hamming codes zijn dus 1-fout verbeterend.

(1.2) Stelling. *Hamming codes zijn perfect.*

Bewijs. Laat $n = (q^r-1)/(q-1)$ en zij C de $(n, n-r)$-Hamming code $/\mathbb{F}_q$. Voor een $x \in C$ bevat de bol met straal $1 = [(d-1)/2]$ om x in totaal $1 + n(q-1) = q^r$ punten. Bekijkt men deze bollen om de codewoorden, dan zijn ze disjunct (wegens $d = 3$) en ze bevatten $q^{n-r} \cdot q^r = q^n$ punten. Dus $\mathbb{F}_q^n$ wordt zonder overlappingen volledig bedekt en de Hamming codes zijn perfect. □

(1.3) Tabel. *De karakteristieken van binaire Hamming codes $\mathcal{H}_r$ zijn:*

$$\begin{aligned} \textit{Lengte} &: n = 2^r - 1, \\ \textit{Dimensie} &: k = 2^r - 1 - r, \\ \textit{Redundantie} &: r = n - k, \\ \textit{Minimumafstand} &: d = 3. \end{aligned}$$

Een toetsmatrix wordt gegeven door een matrix waarvan de kolommen de elementen van $\mathbb{P}^{r-1}(\mathbb{F}_2) = \mathbb{F}_2^r - \{0\}$ zijn.

Het belang van de binaire $\mathcal{H}_r$ is gelegen in het feit dat syndroomdecoderen bizonder eenvoudig is.

i) Bepaal het syndroom $s = Hy^t$ van het ontvangen woord y;

ii) Als $s = 0$ dan decodeer y;

iii) Als $s \neq 0$, dan is $s \in \mathbb{F}_2^r - \{0\}$ gelijk aan een kolom van H , zeg $s = k_i$ (i-de kolom). Wijzig het symbool op de i-de plaats in y. Het resultaat is het gedecodeerde woord.

In het bizonder kunnen we de kolommen ordenen zodat ze de binaire representaties van $1, ..., n$ geven (Vergelijk het voorbeeld aan het einde van §2 van Hoofdstuk I.) Als $s \neq 0$ dan representeert s binair de plaats waar de fout is gemaakt.

De gewichtsverdeling van $\mathcal{H}_r$ bepalen we via die van $\mathcal{H}_r^\perp$ met de MacWilliams-formule.

(1.4) Stelling. *Alle woorden $\neq 0$ in de duale code $\mathcal{H}_r^\perp$ van de $(n, n-r)$ Hamming-code $\mathcal{H}_r$ over $\mathbb{F}_q$ hebben gewicht q^{r-1}.*

Bewijs. De rijen van de toetsmatrix corresponderen met de coordinaatfuncties x_i, $i = 0, \ldots, r-1$. De rijen geven de "waarden" van de coordinaatfuncties op de punten van $\mathbb{P}^{r-1}(\mathbb{F}_q)$ aan. Het aantal nulpunten van x_i is gelijk aan $\#\mathbb{P}^{r-2}(\mathbb{F}_q) = (q^{r-1}-1)/(q-1)$ zodat het aantal punten met $x_i \neq 0$ gelijk is aan $(q^r-1)/(q-1) - (q^{r-1}-1)/(q-1) = q^{r-1}$. Een willekeurig woord $\neq 0$ in $\mathcal{H}_r^\perp$ correspondeert met de niet-triviale lineaire combinatie $a_0x_0 + \ldots + a_{r-1}x_{r-1}$ met $a_i \in \mathbb{F}_q$. Deze lineaire combinatie van de coordinaatfuncties heeft ook $(q^r-1)/(q-1)$ nulpunten in $\mathbb{P}^{r-1}(\mathbb{F}_q)$ zodat elk woord $\neq 0$ in $\mathcal{H}_r^\perp$ gewicht q^{r-1} heeft. □

We noemen $\mathcal{H}_r^\perp$ op grond van (1.4) een *equidistante code* of *simplex code*. Passen we nu de MacWilliamsformule toe, dan vinden we de gewichtsverdeling van $\mathcal{H}_r^\perp$.

Het gewichtsverdelingspolynoom van de binaire $\mathcal{H}_r^\perp$ is:

$$B(z) = 1 + nz^{(n+1)/2}$$

en het gewichtsverdelingspolynoom van de binaire $\mathcal{H}_r$ is:

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

§2. *Het construeren van nieuwe codes uit een gegeven code*

We geven zes elementaire manieren aan om uit een gegeven code C een nieuwe code te maken.

1. Uitbreiden van een code.

Vindt plaats door aan elk codewoord $x \in C$ een controlesymbool toe te voegen volgens een vaste lineaire regel: $x_{n+1} = \sum_{i=1}^n a_i x_i$ als $(x_1, \ldots, x_n) \in C$ met vaste $a_i \in \mathbb{F}_q$. Een veel gebruikte regel is aanvullen zodat de som der coordinaten nul is:

$$\overline{C} = \{(x_1, ..., x_n, x_{n+1}) : (x_1, ..., x_n) \in C, \sum_{i=1}^{n+1} x_i = 0\}.$$

In het binaire geval volgt dan dat $d(\overline{C})$ even is. De toets $\sum_{i=1}^{n+1} x_i = 0$ heet *totale toets* (overall parity check). Als we uitgaan van een (n, k, d)-code C met d oneven vinden we een $\overline{C}$ met parameters $(n+1, k, d+1)$.

2. Puncteren van een code.

Vindt plaats door weglaten van een of meer controlesymbolen. In het algemeen neemt d af en wel met 1 per gepuncteerde component. Dit procédé kan herhaald worden zolang $d > 1$.

3. Aanvullen van een code.

Vindt plaats door toevoeging van codewoorden. Dit komt neer op het uitbreiden van de basis van de code: $C \to \mathbb{F}_q a + C$ met $a \in \mathbb{F}_q^n - C$. Een bekende manier in de binaire situatie is toevoeging van alle complementaire woorden (d.w.z. $(1-x_1, ..., 1-x_n)$ voor $(x_1, ..., x_n) \in C$), uiteraard indien deze nog niet tot de code behoren. Nu ontstaat $C \cup \mathbf{1} + C$, waardoor een (n, k, d)-code overgaat in een $(n, k+1, d')$-code met $d' = \min(d, n - \delta)$; hier is δ het maximumgewicht in C.

4. Opzuiveren van een code.

Vindt plaats door verwijdering van codewoorden, en wel de woorden uit het complement van een deelcode. In de binaire situatie worden vaak de woorden van oneven gewicht verwijderd, waardoor een (n, k, d)-code overgaat in een $(n, k-1, d')$-code met vaak $d' > d$ (i.h.b. als d oneven is).

5. Verlengen van een code.

Vindt plaats door toevoeging van een informatiesymbool via een combinatie van aanvullen en uitbreiden waarbij een (n, k)-code overgaat in een $(n+1, k+1)$-code. In de binaire situatie gebruikt men vaak

$$C \mapsto \overline{C \cup \mathbf{1} + C}.$$

6. Verkorten van een code.

Vindt plaats door verwijdering van een informatiesymbool via een combinatie van opzuiveren en puncteren. Neem bijv. alle codewoorden die op een zekere plaats hetzelfde symbool hebben. Laat uit die woorden dat symbool weg. Als het betreffende symbool 0 is, gaat een (n, k, d)-code over in een $(n-1, k-1, d')$-code met $d' \geq d$.

Voorbeeld i) Varianten van de binaire Hamming-code voor $r \geq 3$ zijn:

–De Hamming-code $\mathcal{H}_r$; een $(2^r - 1, 2^r - r - 1, 3)$ -code.

–De even-gewicht deelcode $\mathcal{H}_r^{even}$; een $(2^r - 1, 2^r - r - 2, 4)$-code.

–De uitgebreide Hamming-code $\overline{\mathcal{H}}_r$; een $(2^r, 2^r - r - 1, 4)$-code.

Opgave. Controleer de parameters van deze codes en geef aan hoe deze codes via de zojuist gedefinieerde zes bewerkingen uit elkaar ontstaan.

ii) Varianten van de duale binaire Hamming code voor $r \geq 3$ zijn:

–De simplex-code $\mathcal{H}_r^{\perp}$; een $(2^r - 1, r, 2^{r-1})$-code.

–De eerste-orde Reed-Muller code

$$\mathcal{R}(1, r) = \overline{\mathcal{H}_r^{\perp} \cup \underline{1} + \mathcal{H}_r^{\perp}};$$

een $(2^r, r+1, 2^{r-1})$-code.

–De gepuncteerde $\mathcal{R}(1, r)$; een $(2^r - 1, r+1, 2^{r-1} - 1)$-code.

Opgave. Ga ook van deze codes de parameters en de samenhang na.

§3. *Grenzen voor lineaire codes*

Een fundamenteel probleem in de coderingstheorie is de bepaling van het getal $A(n,d)$ dat gedefinieerd is *als het maximale aantal codewoorden in een code* $/\mathbb{F}_q$ *van lengte* n *en minimumafstand* d. In deze paragraaf besteden we aandacht aan het analoge probleem voor lineaire codes en we noteren $B(n,d) =$ *maximale aantal codewoorden in een lineaire code* $/\mathbb{F}_q$ *van lengte* n *en minimumafstand* d. Nauw verwant is het probleem om bij gegeven lengte en dimensie de grootst mogelijke minimumafstand te bepalen voor een $\mathbb{F}_q$-code.

Een eerste eenvoudig feit is het volgende.

(3.1) Stelling. *Er geldt :* $B(n,d) \leq qB(n-1,d)$.

Bewijs. Ga uit van een code die $B(n,d)$ realizeert. Kies een positie waarop niet alle codewoorden een coördinaat 0 hebben. Verkort nu op deze positie. Dan ontstaat zo een $(n-1,d)$-code waarvan het aantal woorden $(1/q)B(n,d)$ is. Dus $B(n-1,d) \geq (1/q)B(n,d)$. □

(3.2) Stelling. *Voor binaire codes geldt:* $B(n,2t) = B(n-1,2t-1)$.

Bewijs. Breid een $B(n-1,2t-1)$-code uit. Dan ontstaat een $(n,2t)$-code met $B(n-1,2t-1)$ codewoorden. Dus er geldt: $B(n,2t) \geq B(n-1,2t-1)$. Anderzijds levert puncteren op een geschikte plaats van een $B(n,2t)$-code een $(n-1,2t-1)$-code met $B(n,2t)$ codewoorden. Dus we zien: $B(n-1,2t-1) \geq B(n,2t)$. Tezamen geeft dit het resultaat. □

Bepaling van $B(n,d)$ is moeilijk. Wel kan men boven- en ondergrenzen aangeven.

I. Bovengrenzen

Laat $B_t^n(q) = \{x \in \mathbb{F}_q^n : w(x) \leq t\}$ de bal met straal t om 0 in $\mathbb{F}_q^n$ zijn.

(3.3) Hamming-grens (bolstapelingsgrens). *Voor een lineaire* (n,k)*-code die* t *fouten kan verbeteren geldt:*

$$q^k \leq \frac{q^n}{1 + \binom{n}{1}(q-1) + ... + \binom{n}{t}(q-1)^t} = \frac{q^n}{\#B_t^n(q)}$$

Bewijs. De bollen om de codewoorden met straal t in $\mathbb{F}_q^n$ zijn disjunct. Zo een bol bevat $1 + \binom{n}{1}(q-1) + ... + \binom{n}{t}(q-1)^t$ punten. Dus

$$q^n \geq q^k(1 + \binom{n}{1}(q-1) + ... + \binom{n}{t}(q-1)^t).$$

□

Gevolg.

$$B(n, 2t+1) \leq \frac{q^n}{1 + \binom{n}{1}(q-1) + ... + \binom{n}{t}(q-1)^t}.$$

Voorbeeld. Als $q = 2, n = 13$ en $d = 5$ dan vinden we $B(13, 5) \leq 64$.

Opmerking. Voor perfecte codes die t fouten verbeteren geldt gelijkheid.

(3.4) Singleton-grens. *Voor een lineaire (n, k)-code met minimumafstand d geldt*

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

Bewijs. De toetsmatrix van de code heeft rang $(n - k)$ = maximale aantal lineair onafhankelijke kolommen. Dus $d \leq n - k + 1$ zodat $k \leq n - d + 1$. □

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

Voorbeeld. Als $q = 2, n = 13$ en $d = 5$ vinden we $B(13, 5) \leq 2^9$.

Opmerking. Codes die deze grens halen heten *maximum distance separable (MDS).*

(3.5) Plotkin-grens. *Voor een lineaire (n, k)-code met minimumafstand d geldt:*

$$q^k \leq \frac{d}{d - n + (n/q)} \quad \textit{als} \quad d > (1 - \frac{1}{q})n.$$

Bewijs. Beschouw de projectie $C \to \mathbb{F}_q$ op de i-de coordinaat. Als niet voor alle $x \in C$ geldt $x_i = 0$ dan is het aantal x met $x_i \neq 0$ gelijk aan $q^k - q^{k-1}$. De som van de gewichten van alle woorden van C is dus $\leq n(q^k - q^{k-1})$. Het gemiddelde gewicht per woord $x \neq 0$ is $\leq n(q^k - q^{k-1})/(q^k - 1)$. Hieruit volgt $d \leq n(q^k - q^{k-1})/(q^k - 1)$. Zo zien we dat $q^k \leq d/(d - n + (n/q))$ als de noemer positief is. □

Als een code niet aan de voorwaarde $d > (1 - \frac{1}{q})n$ voldoet kan men dit bereiken door een geschikt aantal malen te verkorten.

Voorbeeld. Verkort een binaire $(13, k, 5)$-code met $k \geq 5$ vier keer. Dan ontstaat een $(9, k - 4, \geq 5)$-code waarvoor geldt: $2^{k-4} \leq 10$ zodat $k \leq 7$.

Opmerking. De Plotkin-grens wordt alleen gehaald door equidistante codes .

(3.6) Griesmer-grens. *Voor een lineaire (n, k)-code met minimumafstand d geldt*

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

Bewijs. De ongelijkheid geldt voor $k = 1$. Voor $k > 1$ kunnen we aannemen dat de $k \times n$-voortbrengermatrix van de code C de volgende gedaante heeft:

$$\begin{pmatrix} \overbrace{1\ldots1}^{d} & \overbrace{0\ldots0}^{n-d} \\ G_1 & G_2 \end{pmatrix},$$

waar er in de eerste rij d enen en $n-d$ nullen staan en het aantal rijen gelijk is aan k. De $(k-1) \times (n-d)$-matrix G_2 kan opgevat worden als de voortbrengermatrix van een $(n-d, k-1)$-code C'. Met elk woord $x' = (x_{d+1}, ..., x_n) \in C'$ corresponderen q woorden uit C:

$$x^{(i)} = (x_1 + i, ..., x_d + i, x_{d+1}, ..., x_n) \quad \text{voor} \quad i \in \mathbb{F}_q.$$

De som van de gewichten van deze q woorden is $qw(x') + d(q-1) \geq qd$. (Merk op dat onder de q elementen $x_j + i$ met $i \in \mathbb{F}_q$ er $q-1$ ongelijk aan nul zijn.) Voor de code C' geldt dus: $d(C') \geq d/q$. Herhaald toepassen van ditzelfde procédé levert uiteindelijk een code $C^{(k-1)}$ met parameters

$$(n - d - d(C') - \ldots - d(C^{(k-2)}), 1, d(C^{(k-1)}),$$

waarbij $d(C^{(i)}) \geq d/q^i$. Hieruit volgt: $n \geq \sum_{i=0}^{k-1} d(C^{(i)}) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. □

Voorbeeld. Laat $q = 2, n = 13$ en $d = 5$. Uit $13 = \sum_{i=0}^{5} \lceil 5/2^i \rceil$ volgt $B(13, 5) \leq 2^6$.

II. Een Ondergrens

(3.7a) Gilbert-Varshamov grens. *(De versie van Gilbert) Voor $n, k, d \in \mathbb{Z}_{>0}$ met $q^{n-k+1} > \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$ bestaat er een lineaire (n,k)-code over $\mathbb{F}_q$ met minimumafstand d.*

Bewijs. Construeer een $(k \times n)$-matrix G die een voortbrengermatrix van zo een code is.

Neem als eerste rij een vector van gewicht d uit $\mathbb{F}_q^n$. Vul aan met rijen zodat de i-de rij onafhankelijk is van de eerste $i-1$ rijen en afstand $\geq d$ heeft tot de woorden van de code voortgebracht door de eerste $i-1$ rijen. Zo een i-de rij bestaat als er in $\mathbb{F}_q^n$ nog punten zijn buiten de bollen met straal $d-1$ om de q^{i-1} lineaire combinaties van de eerste $i-1$ rijen, ofwel als $q^n > q^{i-1}(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots \binom{n}{d-1}(q-1)^{d-1})$. Indien dus

$$q^n > q^{k-1}(\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i),$$

dan kan men de gewenste $(k \times n)$-matrix construeren. □

Opmerking. De optimale keuze voor k is

$$n - [\log_q \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i].$$

Hieruit volgt

$$B(n,d) \geq q^{n-[\log_q \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i]}.$$

Voorbeeld. Als $q=2, n=13, d=5$ dan geldt: $B(13,5) \geq 2^3$.

(3.7b) Gilbert-Varshamovgrens. *(De versie van Varshamov) Voor $n,k \in \mathbb{Z}_{>0}$ en $d \in \mathbb{Z}_{>1}$ met $q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i$ bestaat er een lineaire (n,k)-code over $\mathbb{F}_q$ met minimumafstand $\geq d$.*

Bewijs. Construeer een $(n-k)\times n$-matrix H zodat elk $(d-1)$-tal kolommen onafhankelijk is.

Neem als eerste kolom een vector uit $\mathbb{F}_q^{n-k} - \{0\}$. Vul verder aan met kolommen zodat de i-de kolom geen lineaire combinatie is van $(d-2)$ (of minder) der voorgaande kolommen.

Er kan nog een $(i+1)$-ste kolom worden gevonden als het aantal niet-triviale lineaire combinaties van $(d-2)$ (of minder) kolommen uit de eerste i kleiner is dan $q^{n-k}-1$, ofwel:

$$q^{n-k} - 1 > \binom{i}{1}(q-1) + \binom{i}{2}(q-1)^2 + \ldots + \binom{i}{d-2}(q-1)^{d-2}.$$

Als deze ongelijkheid geldt voor $i = n-1$ kan men een $(n-k)\times n$-matrix H construeren waarin elk $(d-1)$-tal kolommen onafhankelijk is. Dit levert de toetsmatrix voor een $(n,k,\geq d)$-code. $\square$

Opmerking. De optimale keuze voor k is

$$n - [\log_q \sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i] - 1.$$

We vinden dan: $B(n,d) \geq q^{n-[\log_q \sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i]-1}$.

Voorbeeld. Als $q=2, n=13, d=5$ dan $B(13,5) \geq 2^4$.

Uit de grenzen volgt dus:

$$2^4 \leq B(13,5) \leq 2^6.$$

Er blijkt: $B(13,5) = 2^5$.

Opgave. Construeer een binaire $(13,5,5)$-code.

Opgaven Hoofdstuk II

1. i) Bepaal een voortbrengermatrix voor de binaire Hammingcode van lengte 7.
ii) Bewijs met behulp van een voortbrengermatrix dat de minimumafstand van de genoemde code 3 is.
iii) Bepaal een toetsmatrix voor de ternaire Hamming code van lengte 13.
iv) Beschrijf een decodeerprocedure voor de code uit iii) bij gebruik als 1-fout-corrigerende code.

2) Bereken de kans op een decodeerfout voor de binaire Hamming-codes $\mathcal{H}_3, \mathcal{H}_4$ en $\mathcal{H}_5$ als de kans op een kanaalfout $0,01$ is.

3) i) Bepaal voor de uitgebreide $(8,4,4)$-Hammingcode bij gebruik als foutontdekkende code de kans op een niet-ontdekte fout bij kanaalfoutkans $0,01$. ii) Beschrijf een decodeerprocedure bij gebruik van de uitgebreide $(8,4,4)$ Hammingcode als 1-foutcorrigerende en 2-foutontdekkende code.

4) i) Toon aan dat de binaire $\mathcal{H}_r$ uniek is, d.w.z. elke lineaire code met parameters $n = 2^r - 1$, $k = 2^r - r - 1$ en $d = 3$ is equivalent met $\mathcal{H}_r$. ii) Bewijs dat alle lineaire $(8,4,4)$-codes onderling equivalent zijn.

5) i) Gegeven is de $\mathbb{F}_3$-code C_1 met voortbrengermatrix

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

Breid C_1 uit. Geef een voortbrengermatrix en een toetsmatrix voor de uitbreiding $\overline{C}_1$ en ga na wat er met d gebeurt. ii) Doe hetzelfde voor de $\mathbb{F}_3$-code met voortbrengermatrix

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

6) Bepaal een voortbrengermatrix en een toetsmatrix voor de codes die voorkomen in de voorbeelden op blz. 20 voor het geval $r = 3$.

7) Bewijs dat voor een binaire (n,k)-code geldt: $d \leq n2^{k-1}/(2^k - 1)$.

8) Bewijs dat voor een binaire (n,k)-code met minimumafstand $d(\leq n/2)$ geldt $2^k \leq 2^{n+2-2d}d$.

9) Bestaat er een $(n = 12, k = 6, d = 5)$ code?

10) i) Bewijs: als er een binaire (n,k,d)-code bestaat, dan bestaat er een $(n-d, k-1, \geq d/2)$-code. ii) Bestaat er een $(15,8,5)$-code ? iii) Bepaal grenzen voor $B(15,5)$.

11) Bepaal grenzen voor $B(16,9)$.

12) Bewijs dat perfecte codes optimaal zijn.

13) Bewijs dat de eerste-orde Reed-Muller codes optimaal zijn.

14) i) Laat zien dat er geen $(13,6,5)$-code bestaat. ii) Geef een voorbeeld van een $(13,5,5)$-code.

15) De enige binaire MDS-codes zijn de triviale $(n, 1, n)$-code, de $(n, n-1, 2)$-code en de $(n, n, 1)$-code. Bewijs dit.

16) In de voortbrengermatrix van een (n, k)-code die MDS is, is elk k-tal kolomvectoren lineair onafhankelijk. Bewijs dit.

17) Bewijs: Als C een MDS-code is over $\mathbb{F}_q$ dan is $C^\perp$ dat ook.

18) Bewijs: als C een MDS-code is over $\mathbb{F}_q$ met $k \geq 2$ dan geldt: $q \geq n - k + 1$. Als $k \leq n - 2$ dan $q \geq k + 1$.

19) Bewijs dat de simplex-codes $\mathcal{H}_r^\perp$ de Griesmer-grens halen.

Hoofdstuk III. Cyclische Codes

§1 *Inleiding cyclische codes*

(1.1) Definitie. We noemen een lineaire code $C \subseteq \mathbb{F}_q^n$ *cyclisch* als met ieder codewoord $(c_0, c_1, \ldots, c_{n-1})$ in C ook de cyclische verschuiving $(c_{n-1}, c_0, \ldots, c_{n-2})$ tot C behoort.
Voorbeeld. De binaire $(3,2)$-code $C = \{(000), (101), (110), (011)\}$ is cyclisch.

Cyclische codes behoren tot de meest intensief bestudeerde codes. Argumenten hiervoor zijn: i) cyclische codes hebben een extra algebraische struktuur waardoor er veel wiskundige aanknopingspunten zijn. ii) voor cyclische codes bestaan technisch eenvoudig te realiseren codeer- en decodeerprocedures.

De belangrijkste blokcodes voor de toepassingen zijn dan ook cyclische codes.

Voor de bestudering van cyclische codes is de volgende identifikatie van $\mathbb{F}_q$-vectorruimten van belang:

$$\mathbb{F}_q^n \cong \mathbb{F}_q[X]/(X^n - 1), \quad (c_0, \ldots, c_{n-1}) \longleftrightarrow c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}.$$

Onder dit isomorfisme van $\mathbb{F}_q$-vectorruimten gaat een code $C \subseteq \mathbb{F}_q^n$ over in een lineaire deelruimte van polynomen $\bmod(X^n - 1)$. Een codewoord noteren we met $c = (c_0, \ldots, c_{n-1})$ of ook met $c(X) = \sum_{i=0}^{n-1} c_i X^i$. Soms schrijven we c in plaats van $c(X)$. Bij de polynoomnotatie rekenen we steeds modulo $X^n - 1$.

Voorbeeld. Bovenstaande $(3,2)$-code C identificeren we met $\{0, 1 + X^2, 1 + X, X + X^2\} \subset \mathbb{F}_2[X]/(X^3 - 1)$. De cyclische verschuiving $(101) \mapsto (110)$ correspondeert met $1 + X^2 \mapsto X(1 + X^2) = 1 + X$.

(1.2) Stelling. *Een lineaire code $C \subset \mathbb{F}_q^n$ is cyclisch dan en slechts dan als C een ideaal is in $\mathbb{F}_q[X]/(X^n - 1)$.*

Bewijs. "⇒" C is cyclisch, dus met $c(X) = \sum_{i=0}^{n-1} c_i X^i$ zit ook $Xc(X) = c_{n-1} + \sum_{i=0}^{n-2} c_i X^{i+1}$ in C. Dan $X^l c(X) \in C$ voor alle $l \in \mathbb{Z}_{\geq 1}$ en dus $f(X)c(X) \in C$ voor alle $f(X) \in \mathbb{F}_q[X]/(X^n - 1)$ en alle $c(X) \in C$. Hieruit volgt dat C een ideaal is.

"⇐" Omdat C een ideaal is zit met $c(X)$ ook $Xc(X)$ in C. Hieruit volgt dat C cyclisch is. □

Voorbeeld. De cyclische $(3,2)$-code uit deze paragraaf is het ideaal $(1 + X)$ in de ring $\mathbb{F}_2[X]/(X^3 - 1)$.

§2 *Het voortbrengerpolynoom en het toetspolynoom van een cyclische code.*

Afspraak. In het vervolg laten we de cyclische code $C = \{0\}$ buiten beschouwing.

Met het ideaal $C \subset \mathbb{F}_q[X]/(X^n - 1)$ correspondeert een-eenduidig een ideaal $I = \phi^{-1}(C) \subset \mathbb{F}_q[X]$ via het natuurlijk homomorfisme $\phi\colon \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(X^n - 1)$. Er geldt: $(X^n - 1) \subsetneq I$. Omdat $\mathbb{F}_q[X]$ een hoofdideaalring is (want euclidisch) geldt dat $I = (g(X))$ met $g = g(X)$ van minimale graad in I; eisen we verder nog dat de

kopcoefficient van g gelijk is aan 1, dan is g eenduidig bepaald. Omdat $(X^n-1) \subsetneq (g(X))$ geldt dat g een echte deler van $X^n - 1$ is. Dan is C gelijk aan $(\phi(g))$ en ook in C is $\phi(g)$ weer van minimale graad omdat ϕ injectief is op de polynomen van graad $< n$. Kortheidshalve noteren we $\phi(g)$ weer met g.

(2.1) Conclusie. Als C cyclisch is van lengte n over $\mathbb{F}_q$ dan is er precies één monisch polynoom $g \in C$ van minimale graad. Dit polynoom brengt C voort, en heet het voortbrengerpolynoom (of generatorpolynoom) van C. Opgevat als element van $\mathbb{F}_q[X]$ deelt het $X^n - 1$.

(2.2) Stelling. *Zij C een cyclische code met voortbrengerpolynoom g. Dan geldt:* $\dim C = n - \text{graad}(g)$.

Bewijs. Laat $\text{graad}(g) = n - k$. Dan liggen de elementen

$$g, Xg, X^2g, \ldots, X^{k-1}g$$

in C en zijn $\mathbb{F}_q$-onafhankelijk. Verder brengen deze veeltermen de code C voort wegens de identiteit

$$c = fg = \{qh + r\}g = rg$$

met $h = (X^n - 1)/g$ en $\text{graad}(r) < k = \text{graad}(h)$. Dus elk element $c \in C$ is van de vorm

$$c = c(X) = (a_0 + \ldots + a_{k-1}X^{k-1})g(X)$$

zodat C een (n, k)-code is met basis $g, Xg, X^2g, \ldots, X^{k-1}g$, waarbij $k = n - \text{graad}(g)$. □

Uit het bewijs kunnen we voortbrengermatrix voor C afleiden.
Als $g = g_0 + g_1X + \ldots + g_{n-k}X^{n-k}$ dan is de matrix

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & & g_{n-k} \end{pmatrix}$$

een voortbrengermatrix van C. Het informatiewoord $a = (a_0, \ldots, a_{k-1})$ coderen we als aG wat neerkomt op polynoomvermenigvuldiging:

$$(a_0 + a_1X \ldots + a_{k-1}X^{k-1})g(X).$$

Polynoomvermenigvuldiging met een vast polynoom is technisch zeer eenvoudig te realiseren met behulp van een schuifregistercircuit.

Een voortbrengermatrix in standaardvorm kunnen we als volgt bepalen.
Voor $i = n - k, n - k + 1, \ldots, n - 1$ voeren we een deling uit:

$$X^i = q_i(X)g(X) + r_i(X) \qquad \text{met } \text{graad}(r_i) < n - k.$$

Dan is het stelsel

$$\{X^i - r_i(X) : i = n - k, \ldots, n - 1\}$$

een onafhankelijk stelsel in C bestaande uit k elementen, dus een basis van C. Deze basis levert een voortbrengermatrix in "standaardvorm":

$$\begin{pmatrix} -r_{n-k} & \vdots & 1 & 0 & \dots & & 0 \\ -r_{n-k+1} & \vdots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \ddots & & \vdots \\ -r_{n-1} & \vdots & 0 & & \dots & 0 & 1 \end{pmatrix}.$$

Hierbij is r_{n-k+i} de vector van lengte $n-k$ gegeven door de coefficienten van $r_{n-k+i}(X)$. De k rijen van de matrix zijn de codewoorden corresponderend met de informatiewoorden $(0,\dots,0,1,0\dots,0)$, ofwel X^i voor $i=0,\dots,k-1$. De systematische wijze van coderen met deze matrix komt in termen van polynomen neer op:

i) vermenigvuldig het informatiewoord $(a_0,a_1,\dots,a_{k-1})$ gerepresenteerd door $a(X)$ met X^{n-k},

ii) bepaal de rest van $a(X)X^{n-k}$ na deling door $g(X)$, zeg $\rho(X)=\sum_{i=0}^{n-k-1}\rho_i X^i$,

iii) het codewoord is $a(X)X^{n-k}-\rho(X)$, ofwel $(-\rho_0,\dots,-\rho_{n-k-1},a_0,\dots,a_{k-1})$.

Deze bewerkingen van polynomen over eindige lichamen realiseert men door middel van schuifregistercircuits.

Voorbeeld. Laat C de binaire cyclische $(7,4)$-code zijn met voortbrengerpolynoom $g=X^3+X+1$. Laat $a=(1010)$ een informatiewoord zijn. Hiermee correspondeert het polynoom $a=1+X^2$. Bij gebruik van niet-systematische codering vinden we

$$(1010)\mapsto(1110010),$$

en bij gebruik van systematische codering

$$(1010)\mapsto(001\underline{1010}).$$

Zij C een cyclische code van lengte n over $\mathbb{F}_q$ met voortbrengerpolynoom $g=\sum_{i=0}^{n-k}g_iX^i$.

(2.3) Definitie. Het monisch polynoom $h=(X^n-1)/g=\sum_{i=0}^{k}h_iX^i$ heet het *toetspolynoom* (of *check polynoom*) van C.

(2.4) Eigenschap. Er geldt: $C=\{c(X)\colon c(X)h(X)=0\in\mathbb{F}_q[X]/(X^n-1)\}$.

Als $c=c(X)\in C$ dan geldt $c=fg$ zodat $ch=f(X^n-1)=0$ in $\mathbb{F}_q[X]/(X^n-1)$. Omgekeerd volgt uit $ch=0$ in $\mathbb{F}_q[X]/(X^n-1)$ dat in $\mathbb{F}_q[X]$ geldt

$$ch=f(X^n-1)=fgh.$$

Dus $c=fg$ zodat $c\in C$. □

(2.5) Definitie. De cyclische code van lengte n over $\mathbb{F}_q$ voortgebracht door h heet de *cyclische duaal* van C.

Met behulp van het toetspolynoom kunnen we een toetsmatrix van C bepalen. Daartoe eerst een lemma.

(2.6) Lemma. *Als* $a = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$ *en* $b = b_0 + \ldots + b_{n-1}X^{n-1}$ *dan geldt:* $ab = 0$ *in* $\mathbb{F}_q[X]/(X^n - 1) \iff (a_0, a_1, \ldots, a_{n-1})$ *is orthogonaal met alle cyclische verschuivingen van* $(b_{n-1}, b_{n-2}, \ldots, b_0)$ *in* $\mathbb{F}_q^n$.

Bewijs. De coefficient van X^t in ab mod $(X^n - 1)$ is

$$(a_0b_t + a_1b_{t-1} + \ldots + a_tb_0) + (a_{t+1}b_{n-1} + \ldots + a_{n-1}b_{t+1}).$$

Dit is gelijk aan het inwendig product van $(a_0, \ldots, a_{n-1})$ met de $(t+1)$ ste cyclische verschuiving van $(b_{n-1}, b_{n-2}, \ldots, b_0)$. $\square$

Combinatie van dit lemma met (2.4) levert het volgende stelsel toetsvergelijkingen op voor C:

(2.7). $(c_0, c_1, \ldots, c_{n-1}) \in C \iff \sum_{i=0}^{n-1} c_ih_{t-i} = 0 \quad \text{voor} \quad t = 0, \ldots, n-1.$

Voor $t = k, k+1, \ldots, n-1$ hoort bij deze vergelijkingen de $(n-k) \times n$-matrix

$$\begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & & h_0 & 0 & \ldots & 0 \\ \vdots & & \ddots & & & \ddots & & \vdots \\ 0 & \ldots & & h_k & \ldots & & & h_0 \end{pmatrix}.$$

Merk op dat de rijen van de matrix een code voortbrengen die bevat is in $C^\perp$ (wegens (2.7)) waarvan de dimensie gelijk is aan $n - k = \dim(C^\perp)$. Associeer met de matrix het polynoom

$$h^* = h_k + h_{k-1}X + \ldots + h_0X^k = X^kh(1/X).$$

Omdat $h^*(X)$ het polynoom $X^n - 1$ deelt is h^* voortbrengerpolynoom van de cyclische code die deze matrix als voortbrengermatrix heeft. We concluderen dat $C^\perp$ ook een cyclische code is en wel met voortbrengerpolynoom $h^*(X)$. De boven aangegeven matrix is dus een toetsmatrix van C.

Opmerking. De cyclische duaal is in het algemeen niet gelijk aan $C^\perp$. Wel geldt dat de cyclische duaal van C, die als voortbrengermatrix heeft

$$\begin{pmatrix} h_0 & h_1 & \ldots & h_k & 0 & \ldots & 0 \\ & \ddots & & & \ddots & & \vdots \\ 0 & \ldots & h_0 & h_1 & \ldots & & h_k \end{pmatrix},$$

equivalent is met $C^\perp$ en bestaat uit de codewoorden van $C^\perp$ in omgekeerde volgorde. In de literatuur noemt men de cyclische duaal vaak kortweg toch de duale code van C.

Codering met behulp van h vindt evenals codering met g plaats door middel van een *schuifregistercircuit*.

§3 *Schuifregistercircuits voor cyclische codes*

Dat cyclische codes zo een grote rol spelen in de practische toepassingen van de coderingstheorie is gelegen in het feit dat codering en decodering kunnen worden gerealiseerd met *schuifregistercircuits* (src's). Een dergelijke realisatie is in technisch opzich zeer efficiënt.

De wiskundige operaties die bij uitstek geschikt zijn om uit te voeren met behulp van src's zijn de rekenkundige bewerkingen in eindige lichamen en bewerkingen met vceeltermen over eindige lichamen. Bij de laatste bewerkingen moet men o.a. denken aan:

-vermenigvuldiging met een vast polynoom,

-bepaling van quotient en rest bij deling van polynomen door een vast polynoom,

-bepaling van de ggd van twee polynomen,

-bepaling van de waarde van een polynoom in een punt.

Deze relatie tussen schuifregistertechnieken en arithmetiek van eindige lichamen is een van de redenen dat de belangrijkste ideeën uit de coderingstheorie samenhangen met de aritmetiek van eindige lichamen.

Schuifregistercircuits zijn opgebouwd uit de volgende componenten:

1) Geheugenelementen (flip-flops), aangegeven door $\longrightarrow \square \longrightarrow$. Deze elementen werken in nauwe samenhang met een klok. Bij elke tik van de klok is de uitvoer gelijk aan de invoer van het vorige tijdstip, terwijl de nieuwe invoer wordt opgeslagen.

2) Optellers, aangegeven door middel van

$$\xrightarrow{\alpha} \bigoplus \xrightarrow{\alpha+\beta}$$
$$\uparrow \beta$$

Een opteller bepaalt de som van de invoersignalen.

3) Constante vermenigvuldigers, aangegeven door

$$\xrightarrow{\alpha} \textcircled{c} \xrightarrow{c\alpha}$$

welke het invoersignaal vermenigvuldigt met een constante c.
(Al deze componenten kunnen meerdere uitvoerkanalen hebben die allemaal de uitkomst geven.)

Voorbeelden van coderingscircuits voor cyclische codes.

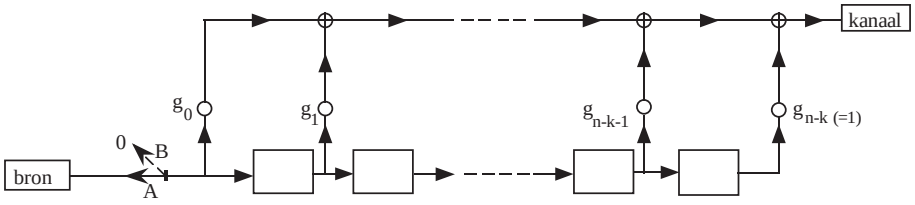
We gaan uit van een cyclische code C met voortbrengerpolynoom

$$g = X^{n-k} + g_{n-k-1}X^{n-k-1} + \ldots + g_0$$

en toetspolynoom

$$h = X^k + h_{k-1}X^{k-1} + \ldots + h_0.$$

a) *Circuit voor niet-systematische codering m.b.v. g.*



Stel het woord dat gecodeerd moet worden is

$$a = a_0 + a_1 X + \ldots + a_{k-1} X^{k-1}.$$

Op het tijdstip $t = 0$ is de inhoud van de geheugenelementen nul. We voeren nu gedurende de eerste k tikken van de klok de symbolen $a_0, a_1, \ldots, a_{k-1}$ in; daarna gaat de schakelaar van stand A in stand B en worden gedurende $n-k$ tikken nullen ingevoerd om her register van de geheugenelementen weer op nul te zetten.

Dit circuit bootst de polynoomvermenigvulding $a \mapsto ag$ na. Namelijk, na de j-de klokpuls is de inhoud van het schuifregister

$$a_{j-1}, a_{j-2}, \ldots, a_{j-(n-k)}.$$

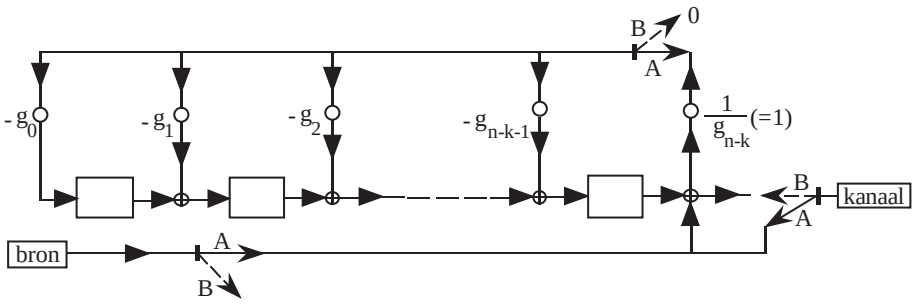
Op de $j+1$-ste puls is de invoer a_j en de uitvoer

$$a_j g_0 + a_{j-1} g_1 + \ldots a_{j-(n-k)} g_{n-k},$$

wat precies de coëfficiënt van X^j in het codewoord ag is.

b) *Circuit voor systematische codering met behulp van $g(X)$*

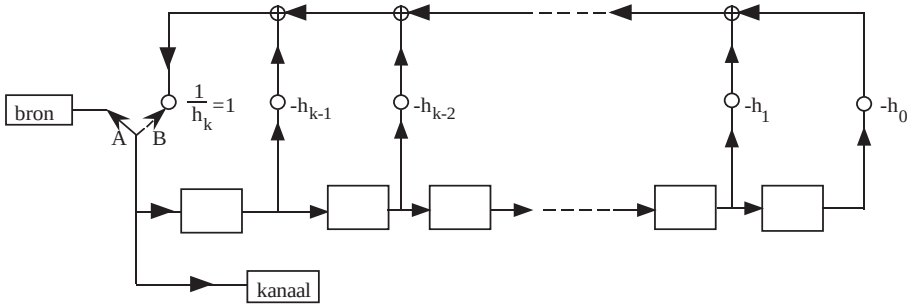
Dit circuit moet de deling van $X^{n-k} a(X)$ door $g(X)$ nabootsen.



De invoer vindt plaats in de volgorde $a_{k-1}, a_{k-2}, \ldots, a_0$ en wel aan de rechterkant van het circuit. Nadat a_0 is ingevoerd gaan de schakelaars van stand A in stand B en in het register bevindt zich dan $-\rho(X)$ (vgl p. ?) Gedurende de volgende $n-k$ tikken gaan de controlesymbolen naar het kanaal en wordt de inhoud van het register weer op nul gezet.

c) *Circuit voor systematische codering met behulp van $h(X)$.*

Dit circuit moet de relaties (2.7) nabootsen.



Eerst worden de k informatiesymbolen in de volgorde $a_{k-1}, a_{k-2}, \ldots, a_0$ in het kanaal en het register ingevoerd. Dan gaat de schakelaar van stand A naar stand B en worden de controlesymbolen die voldoen aan de relaties (2.7) naar het kanaal en het register gevoerd.

In het algemeen kiest men bij het coderen van cyclische codes voor een systematische codeerder en de keuze tussen b) en c) wordt bepaald door het aantal benodigde geheugenelementen.

§4. *Karakterisering van cyclische codes via nulpunten van polynomen*

Vanaf nu beschouwen we cyclische codes van lengte n over $\mathbb{F}_q$ met $(n, q) = 1$. Dan heeft het polynoom $X^n - 1$ slechts enkelvoudige nulpunten in een uitbreiding van $\mathbb{F}_q$.

De ontbinding van $X^n - 1 = \prod_{i=1}^{t} f_i$ in $\mathbb{F}_q[X]$ met f_i irreducibel en monisch levert de 2^t mogelijke cyclische codes over $\mathbb{F}_q$ van lengte n.

(4.1) Intermezzo. De factoren van $X^n - 1$ in $\mathbb{F}_q[X]$.

Het *ontbindingslichaam* of *splitsingslichaam* van $X^n - 1$ t.o.v. $\mathbb{F}_q$ is de kleinste lichaamsuitbreiding $\mathbb{F}_q$ waarover dit polynoom in lineaire factoren splitst (equivalent: alle nulpunten van dit polynoom bevat). De nulpunten van dit polynoom in het ontbindingslichaam vormen een cyclische groep (eindige ondergroep van de multiplicatieve groep van een lichaam). Laat α een voortbrenger van deze groep zijn. Dan heet α een *primitieve n-de machts eenheidswortel* en het ontbindingslichaam verkrijgen we door α aan $\mathbb{F}_q$ te adjungeren: $\mathbb{F}_q(\alpha)$.

Nu is $\mathbb{F}_q(\alpha)$ van de vorm $\mathbb{F}_{q^m}$ voor zekere $m \in \mathbb{Z}_{>0}$. Deze m is minimaal onder de gehele getallen m met $\alpha^{q^m} = \alpha$, ofwel (omdat $\alpha \neq 0$) $\alpha^{q^m - 1} = 1$. Omdat de orde van α gelijk is aan n is m minimaal zodat n deler is van $q^m - 1$, ofwel $q^m \equiv 1 (\mathrm{mod} n)$.
Conclusie: Het ontbindingslichaam van $X^n - 1$ ten opzichte van $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$ met m de orde van q modulo n.

Stel nu dat f_i een irreducibele factor van $X^n - 1$ is met $\deg(f_i) = m_i$. Laat β een nulpunt zijn van f_i in het ontbindingslichaam van $X^n - 1$. Dan zijn de nulpunten van f_i:

$$\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m_i - 1}}.$$

Schrijf $\beta = \alpha^s$. Dan zijn de nulpunten dus

$$\alpha^s, \alpha^{qs}, \alpha^{q^2 s}, \ldots, \alpha^{sq^{m_i-1}}.$$

De exponenten $\{s, sq, \ldots, sq^{m_i-1}\}$ die horen bij f_i vormen de *cyclotomische nevenklasse* van s modulo n t.o.v. $\mathbb{F}_q$.

Merk op dat m_i het minimale natuurlijke getal is waarvoor geldt $\beta^{q^{m_i}} = \beta$, ofwel $\alpha^{sq^{m_i}} = \alpha^s$, d.w.z. $sq^{m_i} \equiv s (\mathrm{mod} n)$.

Als men zo alle factoren f_i doorloopt dan worden de gehelen mod$n$ ingedeeld in cyclotomische nevenklassen.

(4.2) Eigenschappen: Het aantal cyclotomische nevenklassen is gelijk aan het aantal irreducibele factoren van $X^n - 1$ in $\mathbb{F}_q[X]$; de graad van een irreducibele factor is gelijk aan het aantal elementen van de bijbehorende cyclotomische nevenklasse.

Voorbeeld. Voor $n = 15, q = 2$ zijn de cyclotomische nevenklassen:

$$\{0\}, \{1, 2, 4, 8\}, \{3, 6, 12, 9\}, \{5, 10\}, \{7, 14, 13, 11\}.$$

Dit betekent dat $x^{15} - 1$ in $\mathbb{F}_2[x]$ uiteenvalt in vijf irreducibele factoren: drie van graad 4, een kwadratische factor en een lineaire. Dit klopt:

$$x^{15} - 1 = (1 + x)(1 + x + x^2)(1 + x^3 + x^4)(1 + x + x^4)(1 + x + x^2 + x^3 + x^4).$$

(einde intermezzo)

Zij C een cyclische code van lengte n over $\mathbb{F}_q$ met voortbrengerpolynoom g waarvan de nulpunten $\alpha_1, \ldots, \alpha_s$ gelegen zijn in het ontbindingslichaam van $X^n - 1$ t.o.v. $\mathbb{F}_q$. We kunnen nu de code C ook schrijven als

$$\begin{aligned} C =& \{c \in \mathbb{F}_q[X]/(X^n - 1) : c = qg\} \\ =& \{c \in \mathbb{F}_q[X]/(X^n - 1) : c(\alpha_i) = 0 \quad i = 1, \ldots, s\}. \end{aligned}$$

Het is niet nodig alle nulpunten van g te specificeren om de code te bepalen. Als namelijk f een irreducibele factor van g is en γ is een nulpunt van f dan betekent $g(\gamma) = 0$ dat $f|g$ en dat ieder nulpunt van f een nulpunt van g is. Hebben we dus een ontbinding

$$g = \prod_{i=1}^{v} f_i$$

met f_i irreducibel en is α_i een nulpunt van f_i voor $i = 1, \ldots, v$ dan is

$$C = \{c \in \mathbb{F}_q[X]/(X^n - 1) : c(\alpha_i) = 0 \quad i = 1, \ldots, v\}$$

een cyclische code met voortbrengerpolynoom g.

Beginnen we met een collectie n-de eenheidswortels $\gamma_1, \ldots, \gamma_w$ dan is

$$\{c \in \mathbb{F}_q[X]/(X^n - 1) : c(\gamma_i) = 0 \quad i = 1, \ldots, w\}$$

een cyclische code met als voortbrengerpolynoom het k.g.v. van de minimumpolynomen van de γ_i's.

Wanneer men een cyclische code vastlegt door middel van n-de eenheidswortels kan men als volgt een toetsmatrix construeren.

Veronderstel dat de gegeven eenheidswortels $\alpha_1, \ldots, \alpha_s$ in $\mathbb{F}_{q^m}$ liggen. Nu geldt dat $c = (c_0, \ldots, c_{n-1})$ in C ligt dan en slechts dan als het polynoom $c(X) = \sum_{i=0}^{n-1} c_i X^i$ nulpunten $\alpha_1, \ldots, \alpha_s$ heeft. Dit komt in matrix-notatie neer op

$$(1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n-1}) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0 \qquad \text{voor} \quad i = 1, \ldots, s.$$

Dus

$$c \in C \iff \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & & \vdots & \\ 1 & \alpha_s & \ldots & \alpha_s^{n-1} \end{pmatrix} c^t = 0,$$

ofwel $Hc^t = 0$, waarbij H de aangegeven matrix is. Deze matrix heeft elementen in $\mathbb{F}_{q^m}$. We krijgen nu een toetsmatrix met elementen uit $\mathbb{F}_q$ door de elementen van $\mathbb{F}_{q^m}$ te schrijven als een kolomvector ten opzichte van een gekozen $\mathbb{F}_q$-basis van $\mathbb{F}_{q^m}$. Zo ontstaat een $sm \times n$-matrix H waarvan de rijen niet noodzakelijkerwijs alle onafhankelijk zijn. Verder geldt $c \in C \iff Hc^t = 0$. Door nu lineair afhankelijke rijen successievelijk te verwijderen ontstaat een toetsmatrix van C die gedefinieerd is over $\mathbb{F}_q$.

Voorbeeld. Neem $n = 7, q = 2$ en α een primitieve 7-de machts eenheidswortel.

De orde van $q = 2$ modulo 7 is 3, dus het ontbindingslichaam van $X^7 - 1$ over $\mathbb{F}_2$ is $\mathbb{F}_{2^3}$ en $X^7 - 1$ splitst als

$$X^7 - 1 = (X + 1)(X^3 + X^2 + 1)(X^3 + X + 1).$$

Bij de cyclische code

$$C = \{c \in \mathbb{F}_2[X]/(X^7 - 1) : c(\alpha) = 0\}$$

krijgt men op de zojuist beschreven manier

$$H = (\, 1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \ldots \quad \alpha^6 \,).$$

Veronderstel dat $X^3 + X^2 + 1$ het minimumpolynoom is van α en neem $1, \alpha, \alpha^2$ als basis van $\mathbb{F}_2(\alpha)/\mathbb{F}_2$. Dan vinden we voor H

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

Dus C is de $(7, 4)$-Hamming code. Dit geldt algemener:

(4.3) Stelling. *Als $n = (q^r - 1)/(q - 1)$ met $(r, q - 1) = 1$ en α is een primitieve n-de machtseenheidswortel, dan is de cyclische code*

$$C = \{c \in \mathbb{F}_q[X]/(X^n - 1) : c(\alpha) = 0\}$$

equivalent met de $(n, n - r)$-Hamming code.

Bewijs. Er geldt $(n, q) = 1$, terwijl de orde van q modulo n gelijk is aan r, zodat $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$.

Omdat $(r, q - 1) = 1$ geldt ook dat $(n, q - 1) = 1$ want n is te schrijven als

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

Uit $(n, q - 1) = 1$ volgt dat $\alpha^i \notin \mathbb{F}_q$ voor $i = 1, 2, \ldots, n - 1$.

Bij de gegeven cyclische code hoort de matrix

$$H = (\,1 \quad \alpha \quad \alpha^2 \quad \ldots \quad \alpha^{n-1}\,),$$

waarbij alleen het element $1 = \alpha^0$ in $\mathbb{F}_q$ ligt, zodat elk tweetal elementen onafhankelijk is ten opzichte van $\mathbb{F}_q$. Schrijft men deze matrix uit t.o.v. een $\mathbb{F}_q$-basis in $\mathbb{F}_{q^r}$ dan ontstaat een $(n = (q^r - 1)/(q - 1), r)$-matrix waarvan elk paar kolommen onafhankelijk is. Dus op equivalentie na is deze toetsmatrix van C de toetsmatrix van de $(n, n - r)$-Hamming code. □

§5 *Idempotente voortbrengers van cyclische codes*

Voortbrengerpolynomen van cyclische codes van lengte n met $(n, q) = 1$ delen $X^n - 1$. De factorisatie van $X^n - 1$ in $\mathbb{F}_q[X]$ bepalen kan lastig zijn. In karakteristiek 2 kan men ook zonder de factorisatie te bepalen voortbrengers van cyclische codes bepalen: idempotente voortbrengers. Deze blijken op diverse andere plaatsen in de theorie van cyclische codes een rol te spelen.

(5.1) Definitie. Een element $c = c(X) \in \mathbb{F}_q[X]/(X^n - 1)$ heet idempotent als geldt: $c^2 = c$.

Voorbeeld. $X^3 + X^6$ is een idempotent in $\mathbb{F}_2[X]/(X^9 - 1)$ want $(X^3 + X^6)^2 = X^6 + X^{12} = X^6 + X^3$.

(5.2) Stelling. *Zij $C \subset \mathbb{F}_q[X]/(X^n - 1)$ een cyclische code. Dan is er precies één $c = c(X) \in C$ die een eenheidselement is in de deelring C. Deze c is idempotent.*

Bewijs. Laat $h = (X^n - 1)/g$ met g het voortbrengerpolynoom van C. Dan zijn g en h onderling ondeelbaar, dus er zijn a en b in $\mathbb{F}_q[X]$ met $ag + bh = 1$. Dan geldt $ag^2 + bhg = g$. Dus neem nu $c = ag$. Wegens $cg = ag^2 = g$ is c eenheidselement van de deelring voortgebracht door g. Zo een eenheidselement is automatisch uniek. Verder is duidelijk dat c idempotent is, want $c^2 = a^2g^2 = ag = c$. □

(5.3) Opmerkingen. 1) De c uit (5.2) brengt C voort, want als $v \in C$ dan $v = vc$ zodat $C \subset (c)$, dus $C = (c)$.

2) Het voortbrengerpolynoom van C is g.g.d.$(c, X^n - 1)$.

(5.4) Definitie. De voortbrenger c van C uit (5.2) heet de *idempotente voortbrenger* van C.

Voorbeeld. De idempotente voortbrenger van de binaire (7,4)-Hamming code met $g = X^3 + X + 1$ is $X^4 + X^2 + X$.

Elke idempotent $c \in \mathbb{F}_q[X]/(X^n - 1)$ is idempotente voortbrenger van een cyclische code, namelijk van $C = (c)$. Dit levert een $1-1$-correspondentie tussen idempotenten en cyclische codes $C \subset \mathbb{F}_q[X]/(X^n - 1)$.

In het binaire geval kunnen we de idempotenten als volgt bepalen. Merk eerst op dat als

$$\{a, 2a, 4a, \ldots, 2^l a\}$$

een cyclotomische nevenklassse modulo n t.o.v. $\mathbb{F}_2$ is, dan is $X^a + X^{2a} + \ldots + X^{2^l a}$ een idempotent. Zo ontstaan t "elementaire idempotenten", waarbij

$$t = \#\text{cyclotomische nevenklassen} = \#\text{ irreducibele factoren van } X^{n-1}.$$

Een som van dergelijke idempotenten is weer een idempotent, zodat in totaal 2^t idempotenten ontstaan welke de 2^t cyclische codes leveren in $\mathbb{F}_q[X]/(X^n - 1)$, waarvan deze idempotenten de unieke idempotente voortbrengers zijn. Zo vinden we alle binaire cyclische codes van lengte n zonder de ontbinding van $X^n - 1$ in $\mathbb{F}_2[X]$ te bepalen.

§6 *De automorfismengroep van een code*

Zij C een code van lengte n. De groep van permutaties van $\{1, 2, \ldots, n\}$ geven we aan met S_n.

(6.1) Definitie. De permutaties $\sigma \in S_n$ met $\sigma(C) = C$ vormen een groep, de *automorfismengroep* van de code C, genoteerd met $\mathrm{Aut}(C)$.

Wegens $C \subset \mathbb{F}_q^n$ is $\mathrm{Aut}(C)$ op te vatten als ondergroep van de groep van $n \times n$-permutatiematrices. Codes die equivalent zijn via een permutatie van de coordinaatplaatsen hebben isomorfe automorfismengroepen.

De groep van een code is een hulpmiddel bij de bepaling van de struktuur van een code (i.h.b. de gewichtsverdeling) en om goede decodeermethoden te ontwerpen (permutatiedecoderen).

De bepaling van $\mathrm{Aut}(C)$ is een lastig probleem; vaak is het eenvoudiger om niet-triviale ondergroepen van $\mathrm{Aut}(C)$ aan te geven.

We noemen in het vervolg een ondergroep G van S_n een *permutatiegroep* op $\{1, 2, \ldots, n\}$. Een permutatiegroep G heet *transitief* als bij elk paar $i, j \in \{1, 2, \ldots, n\}$ er een $\sigma \in G$ bestaat zodat $\sigma(i) = j$.

(6.2) Definitie. De code C heet *transitief* als $\mathrm{Aut}(C)$ een transitieve permutatiegroep bevat.

Een cyclische code is een voorbeeld van een transitieve code, want $\mathrm{Aut}(C)$ bevat de ondergroep voortgebracht door de cyclische verschuiving $\sigma : i \mapsto i - 1 (\mathrm{mod} n)$ en deze ondergroep is transitief.

(6.3) Stelling. *Laat C een transitieve code zijn. Dan zijn alle enkelvoudig gepuncteerde codes die uit C ontstaan equivalent.*

Bewijs. Puncteer C op de plaatsen i en j en maak zo de codes C_i en C_j. Het automorfisme σ met $\sigma(i) = j$ levert $(\sigma(C))_i \sim C_j$. Anderzijds hebben we $(\sigma(C))_i = C_i$ omdat $\sigma(C) = C$, dus $C_i \sim C_j$. □

(6.4) Stelling. *Laat C een transitieve code zijn. Als M_i de matrix is waarvan de rijen gevormd worden door de woorden van gewicht i uit C dan hebben alle kolommen van M_i hetzelfde gewicht.*

Bewijs. Neem $l \neq 1$ en $\sigma \in \mathrm{Aut}(C)$ met $\sigma(1) = l$. De permutatie σ induceert op M_i een herschikking van de rijen zodat het gewicht van de l-de kolom gelijk is aan dat van de eerste. □

(6.5) Stelling. *Laat C een transitieve code over $\mathbb{F}_q$ zijn van lengte $n \geq 2$ en $d(C) > 1$. Laat C' de code zijn ontstaan uit C door enkelvoudige punctering. Definieer $A_i = \#\{c \in C : w(c) = i\}$ en $a_i = \#\{c' \in C' : w(c') = i\}$. Dan geldt:*

$$a_i = \frac{n-i}{n} A_i + \frac{i+1}{n} A_{i+1} \quad \text{voor} \quad i = 1, \ldots, n-1.$$

Bewijs. De matrix M_i uit (6.4) heeft gewicht iA_i. Elke kolom heeft volgens (6.4) gewicht r zodat $nr = iA_i$. Het aantal nullen per kolom van M_i is dus

$$A_i - \frac{iA_i}{n} = \frac{n-i}{n} A_i.$$

Een woord van gewicht i in C' is afkomstig van een woord van gewicht i uit C met een nul op de gepuncteerde plaats of van een woord van gewicht $i+1$ uit C met een symbool $\neq 0$ op de gepuncteerde plaats. Dus

$$a_i = \frac{n-i}{n} A_i + \frac{i+1}{n} A_{i+1}. \qquad \square$$

(6.6) Gevolg. *Als C een binaire transitieve lineaire code is (met $n \geq 2$) en alle woorden hebben even gewicht, dan is $d(C')$ oneven.*

Opgaven Hoofdstuk III

1. Laat C een cyclische code zijn in $\mathbb{F}_2^{15}$ met voortbrengerpolynoom $g = X^4 + X + 1$.
   a) Bepaal het toetspolynoom h van C.
   b) Bepaal het voortbrengerpolynoom van $C^\perp$.
   c) Geef een voortbrengermatrix en een toetsmatrix van C in standaardvorm.

2) Idem dito voor het voortbrengerpolynoom

$$g = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1).$$

3) a) Bepaal het voortbrengerpolynoom van de binaire cyclische code

$$\{(0000), (0101), (1010), (1111)\}.$$

b) Beschrijf de kleinste binaire cyclische code die (0011010) bevat.

4) i) Als g een deler is van $X^n - 1$ en C is het ideaal $(g) \subseteq \mathbb{F}_q[X]/(X^n - 1)$ dan is g het voortbrengerpolynoom van C. Bewijs dit.

ii) Laat C een ideaal zijn in $\mathbb{F}_q[X]/(X^n - 1)$ voortgebracht door f. Bewijs: het voortbrengerpolynoom van C is $g.g.d.(f, X^n - 1)$.

iii) Bewijs: $f \in \mathbb{F}_q[X]/(X^n - 1)$ is een eenheid $\iff$ $g.g.d.(f, X^n - 1) = 1$.

iv) Bewijs dat g en g^2 hetzelfde ideaal voortbrengen in $\mathbb{F}_q[X]/(X^n - 1)$ als $(n, q) = 1$.

5) Laat C_1 en C_2 cyclische codes zijn met voortbrengerpolynomen g_1 en g_2. Bewijs:
   a) $C_1 \subset C_2 \iff g_2$ deelt g_1.
   b) $C_1 \cap C_2$ is cyclisch met voortbrengerpolynoom $k.g.v.(g_1, g_2)$.
   c) $C_1 + C_2$ is cyclisch met voortbrengerpolynoom $g.g.d.(g_1, g_2)$.
   d) $C_1 C_2$ is cyclisch met voortbrengerpolynoom $g.g.d.(g_1 g_2, X^n - 1)$.

6) Gegeven is de lineaire code $C \subseteq \mathbb{F}_2^9$ bestaande uit de woorden $c = (c_0, \ldots, c_8)$ met $c_0 = c_1 = c_2$, $c_3 = c_4 = c_5$ en $c_6 = c_7 = c_8$. Bewijs dat C equivalent is met een cyclische code en bepaal het voortbrengerpolynoom van deze laatste.

7) Bepaal alle binaire cyclische codes die (0100111) bevatten.

8) Laat C een cyclische code in $\mathbb{F}_2^n$ zijn met voortbrengerpolynoom g. Als g het polynoom $X^m - 1$ niet deelt voor $m < n$ dan geldt $d \geq 3$.

9) Laat C een cyclische code in $\mathbb{F}_q^n$ zijn met voortbrengerpolynoom g en toetspolynoom h. Bewijs:
   i) C is een even-gewichtscode $\iff$ $X - 1$ deelt g.
   ii) Als $C \subseteq C^\perp$ dan deelt $X - 1$ het polynoom g.

iii) Er geldt: $C \subseteq C^{\perp} \iff X^{\text{graad}(h)}h(1/X)$ deelt g.

iv) Als de lengte van C oneven is geldt: $\underline{1} \in C \iff g(1) \neq 0$.

v) Als de lengte van C oneven is geldt:C bevat een woord van oneven gewicht $\iff$ $\underline{1} \in C$.

10) a) Bepaal het aantal binaire cyclische codes van lengte 15.
b) Geef het voortbrengerpolynoom voor vier van deze codes en hun duale codes.
c) Bepaal de dimensie van de codes uit b).
d) Zoek een binaire cyclische code van lengte 15 met $C \subseteq C^{\perp}$.

11) i) Bepaal de graden van de irreducibele factoren van $X^{17} - 1$ in $\mathbb{F}_2[X]$. ii) Bereken de graad van het ontbindingslichaam van $X^{17} - 1$ over $\mathbb{F}_2$.

12) Idem dito als in 11) voor $X^9 - 1$, $X^{13} - 1$, $X^{23} - 1$ en $X^{63} - 1$.

13) i) Zij $g \in \mathbb{F}_q[X]$ het voortbrengerpolynoom van een cyclische code. Bewijs dat $g^*(X) = X^{\deg(g)}g(1/X)$ het voortbrengerpolynoom van een equivalente code is.

ii) Toon aan dat $X^4 + X + 1$ en $X^4 + X^3 + 1$ equivalente cyclische codes van lengte 15 over $\mathbb{F}_2$ voortbrengen.

iii) Toon aan dat $X^5 + X^2 + 1$ en $X^5 + X^3 + X^2 + X + 1$ equivalente cyclische codes van lengte 31 over $\mathbb{F}_2$ voortbrengen.

14) Bepaal de idempotente voortbrenger van de binaire $(15, 11)$-Hamming code.

15) Bepaal de idempotente voortbrengers van de binaire cyclische codes van lengte 23 en bepaal de dimensies van deze codes.

16) Laat C een cyclische code zijn over $\mathbb{F}_2$ met idempotente voortbrenger $c(X)$.
i) Bewijs dat de idempotente voortbrenger van $C^{\perp}$ gelijk is aan $(1 + c(X))^*$.
ii) Bewijs dat de idempotente voortbrenger van de cyclische duaal van C gelijk is aan $1 + c(X)$.
iii) Er geldt $C_1 \subseteq C_2 \iff$ voor de idempotente voortbrengers geldt: $c_1(X)c_2(X) = c_1(X)$.

17) Bewijs dat voor een lineaire code geldt: $\text{Aut}(C) = \text{Aut}(C^{\perp})$.

18) Laat C een binaire code van oneven lengte zijn waarvan de woorden even gewicht hebben. Bewijs: $\text{Aut}(C \cup \underline{1} + C) = \text{Aut}(C)$.

19) i) Laat A een permutatiematrix zijn. Bewijs: $A \in \text{Aut}(C) \iff$ er is een niet-singuliere matrix K zodat $KG = GA$, waarin G een voortbrengermatrix van de gegeven code C is.
ii) Bewijs dat de automorfismengroep van de $(7, 4, 3)$-Hamming code isomorf is met de groep van de niet-singuliere 3×3-matrices met coëfficiënten uit $\mathbb{F}_2$.

20) Laat C een cyklische code van lengte n over $\mathbb{F}_q$ zijn met $(q, n) = 1$. Laat zien dat elke permutatie $i \mapsto qi(\mathrm{mod}n)$ een element van $\mathrm{Aut}(C)$ is en bepaal de orde van dit element.

21) i) Beschrijf de werking op de cyclotomische nevenklassen modulo 15 ten opzichte van $\mathbb{F}_2$ van de permutaties: $i \mapsto 4i(\mathrm{mod}15)$ en $i \mapsto 7i(\mathrm{mod}15)$.
ii) Bewijs dat de de permutatie $\sigma_a : i \mapsto ai(\,\mathrm{mod}\,n)$ met $(a, n) = 1$ cyclotomische nevenklassen $(\mathrm{mod}n)$ overvoert in cyclotomische nevenklassen.
iii) Laat C een binaire cyklische code van lengte n zijn en laat $\sigma_a : i \mapsto ai(\mathrm{mod}n)$ met $(a, n) = 1$. Toon aan dat $\sigma_a(C)$ een cyklische code is.

Hoofdstuk IV. Enkele belangrijke families van cyclische codes

§1 *BCH-codes*

De BCH-codes vormen een familie van codes ontdekt rond 1960 door Bose en Ray-Chaudhuri, en onafhankelijk van hen door Hocquenghem. Het zijn cyclische codes ontworpen om een voorgegeven aantal fouten te corrigeren als generalisatie van de 1-fout corrigerende Hamming codes. Deze codes zijn in de praktijk goed bruikbaar omdat er eenvoudige codeer- en decodeertechnieken bestaan. Ze leveren goede prestaties als het aantal fouten klein is in vergelijking met de lengte.

We nemen weer aan dat $(n, q) = 1$ en dat α een primitieve n-de machtseenheidswortel is in een uitbreidingslichaam $\mathbb{F}_{q^m}$ van $\mathbb{F}_q$.

(1.1) Definitie. Een cyclische code van lengte n over $\mathbb{F}_q$ heet een *BCH-code van ontwerpafstand* δ als het voortbrengerpolynoom van de code het kleinste gemene veelvoud is van de minimumpolynomen van $\alpha^l, \alpha^{l+1}, \ldots, \alpha^{l+\delta-2}$ voor zekere l.

In het algemeen neemt men $l = 1$ en men spreekt dan van een *BCH-code in strikte zin*.

Als $n = q^m - 1$ dan is α een primitief element van $\mathbb{F}_{q^m}$ en spreekt men van een *primitieve BCH-code*.

(1.2) Stelling. *(BCH-grens) Voor de minimumafstand $d(C)$ van een BCH-code C van lengte n over $\mathbb{F}_q$ met ontwerpafstand δ geldt $d(C) \geq \delta$.*

Bewijs. We hebben gezien:

$$c \in C \iff \begin{pmatrix} 1 & \alpha^l & \ldots & \alpha^{l(n-1)} \\ 1 & \alpha^{l+1} & \ldots & \alpha^{(l+1)(n-1)} \\ \vdots & & \vdots & \\ 1 & \alpha^{l+\delta-2} & \ldots & \alpha^{(l+\delta-2)(n-1)} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

De bewering is dat elk $(\delta - 1)$-tal kolommen uit deze matrix onafhankelijk is zodat $w(c) \geq \delta$ als $c \neq 0$.

Beschouw namelijk $\delta - 1$ kolommen uit de matrix die, zeg, als eerste rij opleveren:

$$\alpha^{li_1}, \alpha^{li_2}, \ldots, \alpha^{li_{\delta-1}}.$$

De determinant van deze $(\delta - 1) \times (\delta - 1)$-matrix die zo ontstaat is een VanderMonde determinant:

$$\alpha^{l(i_1+\ldots+i_{\delta-1})} \det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \ldots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & & \vdots \end{pmatrix} = \alpha^{l(i_1+\ldots+i_{\delta-1})} \prod_{r>s} (\alpha^{i_r} - \alpha^{i_s}) \neq 0.$$

Dus de $\delta - 1$ kolommen zijn onafhankelijk zodat $d(C) \geq \delta$. $\square$

De BCH-grens is niet scherp. Het vinden van de werkelijke minimumafstand is in het algemeen een moeilijk probleem.

Er zijn verscherpingen van de BCH-grens voor cyclische codes waarbij in de exponenten van de nulpuntenverzameling andere regelmatigheden dan een opeenvolging optreden.

(1.3) Stelling. *(Hartman-Tzeng (1972)) Zij C een cyclische code van lengte n over $\mathbb{F}_q$ en α een primitieve n-de machts-eenheidswortel. Als $(n, c_1) = 1$, $(n, c_2) < d_0$ en C heeft nulpunten*

$$\alpha^{l+i_1c_1+i_2c_2} \qquad \text{voor} \quad 0 \le i_1 \le d_0 - 2 \quad \text{en} \quad 0 \le i_2 \le s \quad \text{en zekere } l \in \mathbb{Z}$$

dan geldt $d(C) \ge d_0 + s$.

Voor een bewijs zie: J.H. van Lint, *Introduction to Coding Theory*.

Voor $c_1 = 1, c_2 = 1$, $d_0 = 2$ en $s = \delta - 2$ is dit de bovenstaande BCH-grens.

Voorbeeld. Beschouw de binaire cyclische code C van lengte 51 met nulpunten α, α^9 dan levert de BCH-grens: $d \ge 3$. De nulpunten van C bevatten $\alpha, \alpha^2, \alpha^8, \alpha^9, \alpha^{15}, \alpha^{16}$. Neem nu $l = 1$, $c_1 = 1$, $c_2 = 7$ dan zijn deze nulpunten van de vorm

$$\alpha^{1+i_1+7i_2} \quad \text{met} \quad i_1 = 0, 1 \quad \text{en} \quad i_2 = 0, 1, 2.$$

Dit betekent $d \ge d_0 + s = 3 + 2 = 5$.

(1.4) Stelling. *Voor de dimensie k van een BCH-code van lengte n over $\mathbb{F}_q$ met ontwerpafstand δ geldt*

$$k \ge n - m(\delta - 1),$$

waarbij m de orde van q modulo n is.

Bewijs. Uit de in het bewijs van (1.2) aangegeven matrix kan men, door op kolomvectoren in $\mathbb{F}_q^m$ (met m de orde van q modulo n) over te gaan, een toetsmatrix van C maken waarvan de afmetingen zijn:

$$(\le m(\delta - 1)) \times n.$$

Dus voor de dimensie van de BCH-code C met ontwerpafstand δ vinden we

$$n - k \le m(\delta - 1) \qquad \text{ofwel} \quad k \ge n - m(\delta - 1). \qquad \square$$

Vanaf nu nemen we $l = 1$.

Als $q = 2$ kan de ondergrens voor de dimensie als volgt worden verscherpt. In deze situatie is het minimumpolynoom van α^s gelijk aan dat van α^{2s}. Ook kunnen we aannemen dat δ oneven is want de codes met $\delta = 2t$ en $\delta = 2t + 1$ vallen samen, omdat ze beide als voortbrengerpolynoom hebben

$$\text{k.g.v.}(p(\alpha), p(\alpha^3), \ldots, p(\alpha^{2t-1})) = g,$$

waarbij $p(\alpha^i)$ het minimumpolynoom van α^i aangeeft. Nu is de graad van g kleiner of gelijk aan mt, dus voor de dimensie k van de binaire BCH-code met $\delta = 2t + 1$ geldt $k \ge n - mt$.

(1.5) Stelling. *Voor elke $m \geq 1$ en $t \leq 2^{m-1}-1$ bestaat er een binaire BCH-code van lengte $n = 2^m - 1$ die t fouten corrigeert en waarvan de dimensie $\geq n - mt$ is.*

Bewijs. Zij α een primitief element van $\mathbb{F}_{2^m}$ en neem voor C de code van lengte $n = 2^m - 1$ met nulpunten $\alpha, \alpha^2, \ldots, \alpha^{2t-1}, \alpha^{2t}$. Deze code heeft de genoemde eigenschappen. $\square$

Voorbeelden van BCH-codes.

1) Neem $n = 15$ en α een primitieve 15-de machtseenheidswortel. De orde van 2(mod 15)is 4, dus het ontbindingslichaam $\mathbb{F}_2(\alpha)$ van $X^{15}-1$ ten opzichte van $\mathbb{F}_2$ is $\mathbb{F}_{2^4}$. Kies voor α dat element dat als minimumpolynoom $X^4 + X + 1$ heeft. Nemen we $\delta = 7$ dan is de cyclische code met nulpunten $\alpha, \alpha^2, \ldots, \alpha^6$ een BCH-code van ontwerpafstand 7. Het voortbrengerpolynoom g is het k.g.v. van de minimumpolynomen van $\alpha, \alpha^3, \alpha^5$ en is gelijk aan

$$(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1) = X^{10}+X^8+X^5+X^4+X^2+X+1.$$

De dimensie van deze code is dus $15 - 10 = 5$ en omdat $w(g) = 7$ geldt $d = 7$.

2) Neem $n = 23$ en α een primitieve 23-ste eenheidswortel. De orde van 2(mod23) is 11, dus het ontbindingslichaam van $X^{23}-1$ is $\mathbb{F}_{2^{11}}$. Het minimumpolynoom g van α heeft wortels

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^9, \alpha^{18}, \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}.$$

Nemen we $\delta = 5$ dan is de cyclische code C met als nulpunten $\alpha, \alpha^2, \alpha^3, \alpha^4$ een BCH-code van ontwerpafstand 5. De dimensie van deze code is $23 - 11 = 12$ en er zal blijken dat $d(C) = 7$.

De automorfismengroep van een uitgebreide primitieve BCH-code.

Laat $\mathbb{F}$ een eindig lichaam zijn. De affiene lijn $\mathbb{A}^1 = \mathbb{A}^1_{\mathbb{F}}$ over $\mathbb{F}$ is de verzameling $\mathbb{F}$. Hierop werkt de affiene groep $AGL(\mathbb{F})$ van permutaties bestaande uit de zogeheten affiene lineaire transformaties

$$x \mapsto ax + b \qquad \text{met} \quad a, b \in \mathbb{F}, a \neq 0.$$

De groep $AGL(\mathbb{F})$ heet de affiene groep op $\mathbb{F}$ en deze werkt transitief op $\mathbb{A}^1_{\mathbb{F}}$.

Laat nu C een lineaire code over $\mathbb{F}_q$ zijn met lengte $n = q^m - 1$. Dan kunnen we de coördinaatplaatsen $0, 1, \ldots, n-1$ indexeren met de elementen $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ van

$$\mathbb{F}^*_{q^m} \subset \mathbb{A}^1,$$

waarbij

$$\mathbb{F} = \mathbb{F}_{q^m} = \{0, \alpha^i : i = 0, \ldots, n-1\}$$

met α een voortbrenger van $\mathbb{F}^*_{q^m}$. We breiden C nu uit tot $\overline{C}$ met behulp van de totale toets $\sum_{i=0}^{n} c_i = 0$. We laten de extra coördinaatplaats corresponderen met $0 \in \mathbb{A}^1$. Dus een woord van $\overline{C}$ is van de vorm $(c_i)_{i \in \mathbb{A}^1}$.

(1.6) Stelling. *Als C een primitieve BCH-code is van lengte $n = q^m - 1$ dan bevat de automorfismengroep van de uitgebreide code $\overline{C}$ de affiene groep $AGL(\mathbb{F}_{q^m})$.*

Bewijs. Neem aan dat C ontwerpafstand δ heeft. Laat $(c_i)_{i\in\mathbb{A}^1}$ een woord van $\overline{C}$ zijn. We voeren nu voor $l = 0, 1, \ldots$ de uitdrukkingen

$$t_l = \sum_{i\in\mathbb{A}^1} c_i i^l$$

in. Er geldt $t_0 = 0$ want $c \in \overline{C}$. Voor $l = 1, 2, \ldots, \delta - 1$ geldt $t_l = \sum c_i(i^l) = 0$ vanwege de definitie van de BCH-code. We passen nu een affien-lineaire transformatie σ gegeven door $x \mapsto ax + b$ toe:

$$c = (c_i)_{i\in\mathbb{A}^1} \mapsto \sigma(c) := (c_{ai+b})_{i\in\mathbb{A}^1}.$$

We beweren dat $\sigma(c)$ weer in $\overline{C}$ ligt. Neem aan dat de inverse transformatie σ^{-1} wordt gegeven door $x \mapsto rx + s$ (met $r = a^{-1}$ en $s = -b/a$). Als $0 \le l \le \delta - 1$ vinden we voor $\sigma(c)$

$$t'_l = \sum_{i\in\mathbb{A}^1} c_{\sigma(i)} i^l = \sum_{i\in\mathbb{A}^1} c_i(\sigma^{-1}(i))^l = \sum_{i\in\mathbb{A}^1} c_i(ri+s)^l =$$

$$= \sum_{j=0}^{l} \binom{l}{j} r^j s^{l-j} \sum_{i\in\mathbb{A}^1} c_i i^j = \sum_{j=0}^{l} \binom{l}{j} r^j s^{l-j} t_j = 0.$$

De vergelijkingen $t'_l = 0$ voor $0 \le l \le \delta - 1$ definiëren de code $\overline{C}$, dus $\sigma(c) \in \overline{C}$. □

(1.7) Gevolg. *Voor een binaire strikte primitieve BCH-code geldt dat de minimumafstand d oneven is.*

Pas (III, 6.6) toe op de code die is uitgebreid door middel van de totale toets.

Decoderen van BCH-codes

BCH-codes zijn van praktisch belang omdat er efficiënte decodeermethoden bestaan voor deze codes. Het snelste decodeeralgoritme is afkomstig van Berlekamp (1968). In 1975 ontdekten Sugiyama c.s. dat decodering ook mogelijk is met behulp van het euklidisch algoritme. Omdat deze laatste methode inzichtelijker is zal het algoritme van Sugiyama nader worden bekeken.

Ga uit van een BCH-code van lengte n over $\mathbb{F}_q$ met oneven ontwerpafstand $\delta = 2t + 1$, zodat alle foutenpatronen van gewicht $\le t$ kunnen worden gecorrigeerd. Zij α een primitieve n-de eenheidswortel in $\mathbb{F}_{q^m}$. Noem het uitgezonden codewoord $c(X)$ en het ontvangen woord $y(X)$; dan is

$$y(X) - c(X) = e(X) = e_0 + e_1X + \ldots + e_{n-1}X^{n-1}$$

het foutenpatroon. Laat $M = \{i : 0 \le i \le n-1, e_i \ne 0\}$ de verzameling plaatsen zijn waar een fout is opgetreden en noteer voor het aantal fouten $\epsilon = \#M$.

We introduceren nu een polynoom waarvan de wortels de plaatsen van de fouten bepalen:

$$\sigma(Z) = \prod_{i\in M} (Z - \alpha^{-i}) =: \sum_{i=0}^{\epsilon} \sigma_i Z^i.$$

De graad van σ is ϵ. Als $\sigma(\alpha^{-i}) \neq 0$ dan is er op de i-de plaats geen fout opgetreden; als $\sigma(\alpha^{-i}) = 0$ dan is daar wel een fout opgetreden. De veelterm σ heet het *fouten-lokalisatie-polynoom*. Om de aard van de fouten te bepalen introduceren we ook nog het *fouten-evaluatie-polynoom*:

$$\omega(Z) = \sum_{i \in M} -e_i \prod_{j \in M - \{i\}} (Z - \alpha^{-j})$$

met graad$(\omega(Z)) < \epsilon$. Als de plaats i van een fout bekend is dan geldt

$$\omega(\alpha^{-i}) = -e_i \prod_{j \in M - \{i\}} (\alpha^{-i} - \alpha^{-j}) = -e_i \sigma'(\alpha^{-i})$$

zodat

$$e_i = -\frac{\omega(\alpha^{-i})}{\sigma'(\alpha^{-i})},$$

waarin σ' de afgeleide van σ is. Merk op dat de g.g.d.$(\sigma, \omega) = 1$.

De polynomen σ en ω bepalen plaats en aard van de fouten; een decodeerprocédé komt dus neer op de bepaling van σ en ω uit het ontvangen woord.

We gaan er van uit dat $\epsilon \leq t$. De eerste stap uit het decodeerproces bestaat uit de bepaling van het syndroom $S = Hy^t$ van het ontvangen woord $y = y(X)$:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2^{(n-1)}} \\ \vdots & & & & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} y(\alpha) \\ y(\alpha^2) \\ \vdots \\ y(\alpha^{2t}) \end{pmatrix} = \begin{pmatrix} e(\alpha) \\ \vdots \\ \vdots \\ e(\alpha^{2t}) \end{pmatrix}.$$

Hier kan S worden bepaald met $2t$ gekoppelde schuifregistercircuits gebaseerd op het minimumpolynoom van α.

Doel is nu om uit het syndroom de veeltermen σ en ω te bepalen. Daartoe beschouwen we

$$\frac{\omega}{\sigma} = \sum_{i \in M} \frac{-e_i}{Z - \alpha^{-i}} = \sum_{i \in M} e_i \alpha^i (\sum_{l=0}^{\infty} (\alpha^i Z)^l) =$$

$$= \sum_{l=0}^{\infty} (\sum_{i \in M} e_i \alpha^{(l+1)i}) Z^l = \sum_{l=0}^{\infty} e(\alpha^{l+1}) Z^l.$$

De eerste $2t$ termen van de machtreeks volgen uit het syndroom. Als we noteren

$$S(Z) = e(\alpha) + e(\alpha^2)Z + \ldots + e(\alpha^{2t}) Z^{2t-1}$$

dan vinden we de "*sleutelvergelijking*"

(1.8) Sleutelvergelijking:

$$S(Z)\sigma(Z) \equiv \omega(Z) (\mathrm{mod} Z^{2t}).$$

Decoderen komt neer op het bepalen van σ en $\omega \in \mathbb{F}_{q^m}[Z]$ met σ monisch,

$$\text{gr}(\omega(Z)) < \text{gr}(\sigma(Z)) \leq t$$

en g.g.d.$(\omega, \sigma) = 1$ die voldoen aan de sleutelvergelijking. (Hierbij is gr(f) de graad van een veelterm f.) Ga na dat het paar σ, ω eenduidig bepaald is.

Er blijkt dat de veeltermen σ en ω volgen uit de bepaling van de g.g.d. van $S(Z)$ en Z^{2t} met behulp van het euklidisch algoritme.

Zij K een lichaam en $A, B \in K[X]$ met gr$(A) \geq$ gr(B). Tijdens het euklidisch algoritme, dat de ggd van A en B bepaalt, worden ook polynomen S' en T' bepaald zodat geldt

$$\text{g.g.d.}(A, B) = S'A + T'B.$$

We beginnen met te schrijven

$$A = Q_1 B + R_1 \quad \text{met} \quad \text{gr}(R_1) < \text{gr}(B)$$

en vervolgen met

$$R_{i-2} = Q_i R_{i-1} + R_i \quad \text{met} \quad \text{gr}(R_i) < \text{gr}(R_{i-1})$$

waarbij $R_{-1} = A$ en $R_0 = B$. Als de laatste rest $\neq 0$ de rest R_n is dan is R_n de g.g.d. van A en B. We kunnen nu induktief de resten R_i ook schrijven als lineaire combinatie van A en B. De eerste rest voldoet aan

$$R_1 = A - Q_1 B = R_{-1} - Q_1 R_0.$$

We stellen dan

$$S_{-1} = 1, T_{-1} = 0, S_0 = 0, T_0 = 1$$

en vervolgen met

$$R_i = S_i A + T_i B \tag{1}$$

waarbij voor $1 \leq i \leq n+1$ de S_i en de T_i bepaald worden via

$$S_i = S_{i-2} - Q_i S_{i-1}, \quad T_i = T_{i-2} - Q_i T_{i-1}.$$

De polynomen S_i en T_i zijn onderling ondeelbaar; preciezer gezegd:

$$S_i T_{i-1} - T_i S_{i-1} = (-1)^{i+1} \qquad \text{voor} \quad 0 \leq i \leq n+1. \tag{2}$$

Verder geldt:

$$\begin{aligned} \text{gr}(R_i) + \text{gr}(S_{i+1}) &= \text{gr}(B) \qquad \text{voor} \quad 0 \leq i \leq n, \\ \text{gr}(R_i) + \text{gr}(T_{i+1}) &= \text{gr}(A) \qquad \text{voor} -1 \leq i \leq n. \end{aligned} \tag{3}$$

Deze feiten kan de lezer zelf bewijzen met volledige inductie naar i. Er geldt nu:

(1.9) Stelling. *Als T en R twee niet-triviale polynomen zijn waarvoor geldt*

$$TB \equiv R(\mathrm{mod}A) \quad \text{met } \mathrm{gr}(R) \leq s \ \text{ en } \mathrm{gr}(T) < \mathrm{gr}(A) - s$$

dan is er precies één index j met $0 \leq j \leq n$ en een veelterm $L \in K[X]$ met $T = LT_j$ en $R = LR_j$.

Bewijs. Laat j de kleinste index zijn zodat graad$(R_j) \leq s$. Merk hier op dat de graden van de R_i een strikt dalende functie van i zijn. Dan geldt wegens (3) $\mathrm{gr}(T_j) \leq \mathrm{gr}(A) - \mathrm{gr}(R) - 1$. Uit $R \equiv TB(\mathrm{mod}A)$ volgt

$$R = SA + TB \tag{4}$$

voor zekere $S \in K[X]$ zodat g.g.d.(A, B) deler is van R. Uit (1) en (4) leiden we af dat

$$\begin{aligned} TR_j &= TS_jA + TT_jB \\ T_jR &= T_jSA + TT_jB \end{aligned} \tag{5}$$

We zien hieruit dat A de uitdrukking $TR_j - RT_j$ deelt. Maar voor de graden geldt nu

$$\mathrm{gr}(TR_j) = \mathrm{gr}(T) + \mathrm{gr}(R_j) < \mathrm{gr}(A).$$

Zo ook

$$\mathrm{gr}(RT_j) = \mathrm{gr}(R) + \mathrm{gr}(T_j) < s + \mathrm{gr}(A) - s < \mathrm{gr}(A).$$

Hieruit volgt dat $TR_j = RT_j$ en met (5) ook dat $ST_j = S_jT$. Omdat we weten dat S_j en T_j onderling ondeelbaar zijn geldt $S = LS_j$ en $T = LT_j$. Dit geeft $R = LT_jB + LS_jA = LR_j$. Voor de eenduidigheid merken we op dat de graden van de T_i strikt stijgend zijn en die van de R_i strikt dalend. De lezer gaat hiermee gemakkelijk na dat de presentatie van R en T als boven eenduidig is. □

Uit deze stelling volgt het resultaat waarmee de sleutelvergelijking kan worden opgelost.

(1.10) Stelling. *Als σ en ω lokalisatie- en evaluatie-polynoom zijn bij een foutenpatroon van gewicht $\leq t$ dan geldt $\sigma = LT_j$ en $\omega = LR_j$, waarbij T_j en R_j ontstaan uit het euklidisch algoritme toegepast op $A = Z^{2t}$ en $B = S(Z)$ en j de kleinste index is waarvoor* $\mathrm{gr}(R_j) < t$. *Bovendien geldt $L \in \mathbb{F}_{q^m}$ en is zo dat LT_j kopcoëfficiënt 1 heeft.*

Deze bepaling van σ en ω is de tweede stap in het decodeerproces. Bij de derde stap worden de nulpunten van σ bepaald. Dit gebeurt door alle $\sigma(\alpha^{-i})$ te bepalen. De fouten e_i volgen dan uit $e_i = -\omega(\alpha^{-i})/\sigma'(\alpha^{-i})$.

Van belang is dat alle stappen kunnen worden gerealiseerd door middel van schuifregistercircuits.

§2 *Reed-Solomon Codes*

Reed-Solomon codes zijn codes van BCH-type die zowel van theoretisch als van practisch belang zijn. Ze zijn zeer geschikt om opeenhopingen (bursts) van fouten te corrigeren.

Hun theoretisch belang ligt in het feit dat deze codes belangrijke bouwstenen zijn bij de constructie van rijen asymptotisch goede codes zoals Justesen codes.

(2.1) Definitie. Een *Reed-Solomon* code (kortweg RS-code) over $\mathbb{F}_q$ van ontwerpafstand δ is een cyclische code van lengte $n = q-1$ met als voortbrengerpolynoom g het kleinste gemene veelvoud van de minimumpolynomen van de elementen α^i met $i = l, l+1, \ldots, l+\delta-2$, waarbij α een primitief element is van $\mathbb{F}_q$.

(2.2) Stelling. *Een RS-code C van lengte n en ontwerpafstand δ heeft dimensie $k = n-\delta+1$ en minimumafstand $d(C) = \delta = n-k+1$.*

Bewijs. Merk op dat het voortbrengerpolynoom van C gelijk is aan

$$g = (X-\alpha^l)(X-\alpha^{l+1})\ldots(X-\alpha^{l+\delta-2}).$$

Dit betekent dat $k = n - \mathrm{gr}(g) = n-\delta+1$. Voor de minimumafstand geldt $d(C) \geq \delta$ (BCH-grens), dus $k \geq n-d(C)+1$. Volgens de Singletongrens (II, 3.4) is $k \leq n-d(C)+1$. Dus $k = n-d(C)+1$, zodat $d(C) = \delta = n-k+1$. $\square$

In het algemeen neemt men $l = 1$.

Reed-Solomon codes zijn de natuurlijke keus wanneer een code moet worden gebruikt waarvan de lengte $<$ #{alfabet} $= q$. Omdat ze MDS zijn hebben ze de grootste minimumafstand.

Voorbeeld. Neem $q = 5$ en $\alpha = 2 \in \mathbb{F}_5$. De RS-code over $\mathbb{F}_5$ met $\delta = 3$ heeft voortbrengerpolynoom $g = (X-2)(X-4) = X^2 - X + 3 \in \mathbb{F}_5[X]$. Dit is een $(4,2,3)$-code over $\mathbb{F}_5$.

De oorspronkelijke benadering van RS-codes door Reed en Solomon (1960) was de volgende.

Laat $n = q-1$ en α een primitief element van $\mathbb{F}_q$. Identificeer $a = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_q^k$ (waarbij $k < n$) met het polynoom $a(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$. Reed en Solomon beschouwden de code

(2.3). $$C = \{c_a = (a(\alpha^0), a(\alpha), \ldots, a(\alpha^{n-1})) : a = \textstyle\sum_{i=0}^{k-1} a_iX^i \in \mathbb{F}_q[X]\}.$$

(2.4) Stelling. *De code C uit (2.3) is een RS-code met $\delta = n-k+1$.*

Bewijs. De code C heeft dimensie k en is cyclisch, want als $c_a \in C$ dan is het cyclisch verschoven woord c_b met $b(X) = a(\alpha^{-1}X)$. Verder geldt $c_a(\alpha^i) = 0$ voor $i = 1, \ldots, n-k$. Neem namelijk $a = X^t$ met $0 \leq t \leq k-1$. Dan geldt

$$c_a(\alpha^i) = \sum_{j=0}^{n-1} \alpha^{j(t+i)} = 0 \quad \text{voor} \quad i = 1, \ldots, n-k$$

want onder vermenigvuldiging met $\alpha^{t+i} \neq 1$ gaat de som over in zichzelf. De code is dus een $(n, k, n-k+1)$ RS-code. $\square$

Indien men de RS-codes op deze manier beschrijft is er een eenvoudig (niet-systematisch) codeerprocédé: evaluatie van polynomen over eindige lichamen (wat technisch efficiënt te realiseren is).

Een van de manieren waarop RS-codes gebruikt kunnen worden als bouwstenen voor nieuwe codes is het afbeelden van codes over $\mathbb{F}_q$ met $q = p^m$ naar codes over $\mathbb{F}_p$. Dit kan men bijvoorbeeld doen door een $\mathbb{F}_p$-basis van $\mathbb{F}_q$ te kiezen en elk element van $\mathbb{F}_q$ als m-tal uit $\mathbb{F}_p^m$ te representeren. Op deze manier gaat een (n, k, d)-code over $\mathbb{F}_q$ over in een (nm, km, d')-code over $\mathbb{F}_p$ met $d' \geq d$.

Voorbeeld. Ga uit van een RS-code over $\mathbb{F}_{2^m}$ met parameters (n, k, d). Vervang elke c_i uit een codewoord c door het corresponderende binaire m-tal en voeg nog per m-tal een controlesymbool toe via de totale toets. De binaire code die zo ontstaat heeft parameters

lengte $= (m+1)(2^m - 1)$,
dimensie $= mk$,
minimumafstand $\geq 2d = 2(2^m - k)$.

§3 *Kwadraatrest-codes*

De kwadraatrestcodes vormen een familie cyclische codes waarvan d vrij groot is in verhouding tot de lengte n (bij niet al te grote n). We gaan uit van codes waarvan de lengte n een oneven priemgetal is en die gedefineerd zijn over $\mathbb{F}_q$ met q een kwadraatrest modulo n.

Laat α een primitieve n-de machts eenheidswortel zijn in een uitbreiding van $\mathbb{F}_q$. We voeren nu enige notaties in:

$$R_0 = \{x^2 : x \in \mathbb{F}_n^*\}, \text{ de kwadraatresten modulo } n,$$

$$R_1 = \mathbb{F}_n^* - R_0, \text{ de niet-kwadraatresten modulo } n.$$

Verder stellen we

$$g_0 = \prod_{r \in R_0} (X - \alpha^r), \qquad g_1 = \prod_{r \in R_1} (X - \alpha^r).$$

Er geldt $g_0 \in \mathbb{F}_q[X]$ immers

$$(g_0(X))^q = \prod_{r \in R_0} (X^q - \alpha^{rq}) = g_0(X^q)$$

omdat $qr \in R_0$ als $q \in R_0$. Uit de relatie

$$(X-1) g_0 g_1 = X^n - 1$$

volgt nu dat ook $g_1 \in \mathbb{F}_q[X]$.

(3.1) Definitie. De cyclische codes van lengte n over $\mathbb{F}_q$ met voortbrengerpolynoom g_0 (resp. $(X-1)g_0$) heten *kwadraatrestcodes* (QR-codes).

Uit de definitie volgt:

(3.2). $\dim QR_{g_0} = (n+1)/2, \quad \dim QR_{(X-1)g_0} = (n-1)/2.$

(3.3) Stelling. *Als we in de definitie g_0 vervangen door g_1 dan ontstaan er equivalente codes.*

Bewijs. Laat $j \in R_1$. Beschouw de permutatie π van coördinaten geinduceerd door $X \to X^j$ in $\mathbb{F}_q[X]/(X^n-1)$. Een polynoom $q(X)g_0(X)$ dat correspondeert met een woord in QR_{g_0} gaat over in $q(X^j)g_0(X^j)$. Er geldt

$$g_0(X^j) = \prod_{r \in R_0} (X^j - \alpha^r) =: \hat{g}_0(X).$$

Laat $s \in R_1$. Dan zien we

$$\hat{g}_0(\alpha^s) = \prod_{r \in R_0} (\alpha^{js} - \alpha^r) = 0,$$

zodat g_1 deelt $\hat{g}_0$ en dus $g_0(X^j) \in QR_{g_1}$. Het beeld onder π van QR_{g_0} is bevat in QR_{g_1}. Omdat QR_{g_0} en QR_{g_1} dezelfde dimensie hebben volgt $\pi(QR_{g_0}) = QR_{g_1}$. Hieruit volgt de equivalentie.Op analoge wijze volgt de equivalentie van $QR_{(X-1)g_0}$ en $QR_{(X-1)g_1}$. □

(3.4) Stelling. *(Wortelgrens voor QR-codes) Voor het gewicht d van een woord $c(X) \in QR_{g_0}$ met $c(1) \neq 0$ geldt:*

i) $d^2 \geq n$,
ii) als $n = 4k-1$ dan $d^2 - d + 1 \geq n$,
iii) als $n = 8k-1$ en $q = 2$ dan is $d \equiv 3 (\mathrm{mod} 4)$.

Bewijs. i) Zij $c(X)$ een codewoord in QR_{g_0} van gewicht $w(c) = d$ en $c(1) \neq 0$. Als $j \in R_1$ dan $\hat{c}(X) = c(X^j) \in QR_{g_1}$ en $\hat{c}$ heeft ook gewicht d. Merk op dat $c \cdot \hat{c} \in QR_{g_0} \cap QR_{g_1}$. De code $QR_{g_0} \cap QR_{g_1}$ heeft voortbrengerpolynoom $g_0 g_1 = 1 + X + \ldots + X^{n-1}$ en heeft dimensie 1. Dus alle woorden $\neq 0$ in deze code hebben gewicht n. Omdat $c(1) \neq 0$ is $c \cdot \hat{c}$ niet het nulwoord.Uit $w(c) = w(\hat{c}) = d$ volgt $w(c \cdot \hat{c}) \leq d^2$, dus $n \leq d^2$.

ii) Als $n \equiv -1 (\mathrm{\ mod\ } 4)$ dan kan men nemen $j = -1$ en we vinden $c \cdot \hat{c} = c(X)c(X^{-1})$. In dit product gaan d termen aan de constante bijdragen, waarvan als bijdrage aan het gewicht hoogstens 1 overblijft: $n \leq d^2 - d + 1$.

iii) Als $n \equiv -1 (\mathrm{mod} 8)$ en $q = 2$ dan geldt

$$c(X)c(X^{-1}) = \sum_{i=1}^{d} X^{l_i} \sum_{j=1}^{d} X^{-l_j}.$$

De termen in het product zijn van de vorm $X^{l_i - l_j}$. Als twee termen elkaar annuleren, d.w.z. $l_i - l_j = l_s - l_t$ met $i \neq j$ dan ook $-l_i + l_j = -l_s + l_t$, zodat nog twee termen

elkaar annuleren. Dus $w(c(X)c(X^{-1})) = d^2 - d + 1 - 4-\text{voud} = n$. Dit betekent $d^2 - d + 1 \equiv -1(\text{mod}4)$ zodat $d \equiv 3(\text{mod}4)$. $\square$

We besteden tenslotte aandacht aan de automorfismen van uitgebreide kwadraatrestcodes.

We gaan uit van de binaire kwadraatrestcode QR_{g_0} van lengte n, waarbij n een priemgetal is van de vorm $n \equiv \pm 1(\text{mod}8)$ (zodat $q = 2$ een kwadraatrest mod$n$ is). Breid QR_{g_0} uit tot $\overline{QR}_{g_0}$ door middel van de totale toets (parity check) $\sum_{i=0}^{n} c_i = 0$. Indexeer de coördinaatplaatsen van de uitgebreide code met de punten van $\mathbb{P}^1(\mathbb{F}_n) = \{0, 1, 2, \ldots, n-1, \infty\}$. De speciale projectieve lineaire groep $PSL(2, \mathbb{F}_n)$ werkt op $\mathbb{P}^1(\mathbb{F}_n)$ en wel transitief door middel van gebroken lineaire transformaties:

$$x \mapsto \frac{ax + b}{cx + d}$$

voor $a, b, c, d \in \mathbb{F}_n$ met $ad - bc = 1$. Deze groep wordt voortgebracht door de transformaties $S : x \mapsto x + 1$ en $T : x \mapsto -1/x$. [Zie Serre: Cours d'Arithmétique.]

(3.5) Stelling. *De automorfismengroep $Aut(\overline{QR}_{g_0})$ bevat de transitieve permutatiegroep $PSL(2, \mathbb{F}_n)$.*

We bewijzen eerst een lemma.

(3.6) Lemma. *Het polynoom $e(X) = \sum_{r \in R_0} X^r$ is de idempotente voortbrenger van $QR_{(X-1)g_0}$ als $n \equiv 1(\text{mod}8)$ en van QR_{g_0} als $n \equiv -1(\text{mod}8)$.*

Bewijs. Omdat $(\frac{2}{n}) = 1$ geldt dat e idempotent is: $e(X)^2 = e(X)$. Dit betekent dat $e(\alpha) = 0$ of $e(\alpha) = 1$ als α een primitieve n-de machts eenheidswortel is. Verder geldt $e(\alpha^i) = e(\alpha)$ voor $i \in R_0$ en $e(\alpha^i) + e(\alpha) = 1$ voor $i \in R_1$.

Kies nu α zo dat $e(\alpha) = 0$; dan geldt $e(\alpha^i) = 0$ voor $i \in R_0$ en $e(\alpha^i) = 1$ voor $i \in R_1$. Omdat $e(1) = (n-1)/2$ geldt g.g.d.$(e(X), X^n - 1) = g_0(X)$ als $n \equiv -1(\text{mod}\,8)$ (resp. $(X-1)g_0(X)$ als $n \equiv 1(\text{mod}8)$). Hiermee is de bewering aangetoond. $\square$

Bewijs van Stelling (3.5). We construeren uitgaande van de idempotente voortbrenger e een $(n+1) \times (n+1)$-matrix die een voortbrengermatrix van $\overline{QR}_{g_0}$ bevat.

Neem de idempotent uit (3.6) en alle cyclische verschuivingen van dit codewoord. Dan ontstaat er een $n \times n$-matrix G. Voor $n \equiv 1(\text{mod}8)$ (resp. $n \equiv -1(\text{mod}8)$) bevat deze een voortbrengermatrix van $QR_{(X-1)g_0}$ (resp. van QR_{g_0}). Nu bevat de matrix

$$\begin{pmatrix} \underline{1} \\ G \end{pmatrix}$$

(met $\underline{1}$ de vector van lengte n met op alle plaatsen een 1) een voortbrengermatrix van QR_{g_0}.

Laat $c = (0, \ldots, 0)$ voor $n \equiv 1(\text{mod}8)$ en $c = (1, \ldots, 1)$ voor $n \equiv -1(\text{mod}8)$; dan bevat de matrix

$$\overline{G} = \begin{pmatrix} 1 & \ldots & 1 & 1 \\ & G & & c^t \end{pmatrix}$$

een voortbrengermatrix van $\overline{QR}_{g_0}$. Indexeer de coördinaatplaatsen van $\overline{QR}_{g_0}$ met de punten van $\mathbb{P}^1(\mathbb{F}_n)$ in de volgorde $0, 1, \ldots, n-1, \infty$. De voortbrenger $S : x \mapsto x+1$ laat ∞ vast en voert een rij van $\overline{G}$ over in een andere rij. De voortbrenger $T : x \mapsto -1/x$ verwisselt 0 en ∞. Verder kan men nagaan (bewerkelijk) dat T een rij van $\overline{G}$ overvoert in een lineaire combinatie van hoogstens drie rijen van $\overline{G}$. Hieruit volgt nu dat $PSL(2, \mathbb{F}_n)$ bevat is in $\mathrm{Aut}(\overline{QR}_{g_0})$. □

(3.7) Gevolg. *De binaire kwadraatrestcode QR_{g_0} heeft oneven minimumafstand d.*

§4. *De binaire Golay Code*

Deze code neemt een unieke plaats in binnen de coderingstheorie. Naast de triviale perfecte codes en de Hamming codes is de binaire Golay code de enige lineaire code over $\mathbb{F}_2$ die perfect is. Deze bizondere struktuur van de Golay code leidt tot nauwe banden met andere wiskundige onderwerpen als bolstapelingen, roosters en simpele groepen.

De code is ontdekt door Golay in 1949 naar aanleiding van de merkwaardige relatie:

$$2^{12}\left\{1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right\} = 2^{23}.$$

Dit betekent dat een binaire $(23, 12, 7)$-code perfect is. Vraag is of zo een code bestaat. We zoeken daarvoor tussen de cyclische codes van lengte 23.

Laat α een primitieve 23-ste eenheidswortel. De orde van $2 (\mathrm{mod} 23)$ is 11, dus het minimumpolynoom van α ten opzichte van $\mathbb{F}_2$ heeft graad 11; de wortels zijn

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^9, \alpha^{18}, \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}.$$

Dus de cyclische code met voortbrengerpolynoom het minimumpolynoom van α (waarvoor we nemen $g = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1$) is een BCH-code van lengte 23, dimensie 12 en ontwerpafstand 5, zodat $d \geq 5$. Merk op dat de exponenten van bovengenoemde machten van α juist de kwadraatresten $\mathrm{mod} 23$ zijn, dus de code is een kwadraatrestcode. Op grond van IV 3.7 en IV 3.4 weten we dan $d \equiv 3 (\mathrm{mod} 4)$. Dus $d \geq 7$, maar dan ook $d = 7$ omdat g gewicht 7 heeft.

(4.1) Stelling. *De cyclische code van lengte 23 met voortbrengerpolynoom $g = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1$ is een $(23, 12, 7)$-code , de binaire Golay code G_{23}.*

§5 *De ternaire Golay code*

Ook deze code is in 1949 ontdekt door Golay en wel naar aanleiding van de relatie

$$3^6\left\{1 + \binom{11}{1}2 + \binom{11}{2}2^2\right\} = 3^{11}.$$

Deze betrekking betekent dat een $(11, 6, 5)$-code over $\mathbb{F}_3$ perfect is. Om zo een code te vinden zoeken we tussen de ternaire cyclische codes van lengte 11.

Zij α een primitieve 11-de eenheidswortel. De orde van 3(mod11) is 5, dus het minimumpolynoom van α ten opzichte van $\mathbb{F}_3$ heeft graad 5; de wortels zijn $\alpha, \alpha^3, \alpha^9, \alpha^5$ en α^4. Dus de cyclische code met als voortbrengerpolynoom het minimumpolynoom van α (waarvoor we nemen $g = X^5 + X^4 - X^3 + X^2 - 1$) is een BCH-code van lengte 11, dimensie 6 en ontwerpafstand 4, zodat $d \geq 4$.

Merk op dat de voorkomende exponenten juist de kwadraten modulo 11 zijn. Noem deze ternaire kwadraatrestcode G_{11}.

Om aan te tonen dat $d = 5$ gaan we als volgt te werk. Beschouw de cyclische deelcode G'_{11} van G_{11} voortgebracht door het polynoom $(X-1)g$. Dan geldt

$$G'_{11} = \{c \in G_{11} : \sum_{i=0}^{10} c_i = 0\}.$$

Voor het toetspolynoom h van G'_{11} geldt h^* deelt $(X-1)g$, zodat $G'_{11} \subseteq (G'_{11})^{\perp}$.

Dus als $c \in G'_{11}$ dan vinden we $0 = (c,c) = \sum_{i=0}^{10} c_i^2$, waaruit volgt $w(c) \equiv 0(\text{mod } 3)$. Veronderstel nu dat G_{11} een woord c van gewicht 4 bevat. Twee mogelijkheden moeten nader bekeken worden.

i) Op equivalentie na is c van de vorm $c = (1,1,1,1,0,\ldots,0)$. Maar dan geldt $c + \underline{1} = (-1,-1,-1,-1,1,\ldots,1) \in G'_{11}$ echter van gewicht $w(c+\underline{1}) \not\equiv 0(\text{mod}3)$. (Hier is $\underline{1}$ de vector van lengte 11 met op alle plaatsen een 1.)

ii) Op equivalentie na is c van de vorm $(1,1,1,-1,0,\ldots,0)$. Maar nu is $c - \underline{1} = (0,0,0,1,-1,\ldots,-1) \in G'_{11}$ echter van gewicht $w(c-\underline{1}) \not\equiv 0(\text{mod}3)$.

Dus G_{11} bevat geen woorden van gewicht 4 zodat $d = 5$.

(5.1) Stelling. *De cyclische code van lengte* 11 *met voortbrengerpolynoom* $X^5 + X^4 - X^3 + X^2 - 1$ *is een* $(11,6,5)$*-code over* $\mathbb{F}_3$*, de ternaire Golay code* G_{11}*.*

Opgaven bij Hoofdstuk IV

1) i) Bepaal het voortbrengerpolynoom, de dimensie en de minimumafstand van de binaire BCH-code met $n = 15, \delta = 5$* gedefinieerd via een primitieve 15-de eenheidswortel α waarvoor geldt $\alpha^4 + \alpha + 1 = 0$.
ii) Wat is het voortbrengerpolynoom als men uitgaat van een α waarvoor geldt $\alpha^4 + \alpha^3 + 1 = 0$?
iii) Bepaal de dimensie van een BCH-code over $\mathbb{F}_4$ met $n = 15$ en $\delta = 5$.

2) Als Opgave 1.i) voor de BCH-code over $\mathbb{F}_3$ met $(n = 8, \delta = 3)$ uitgaande van de primitieve 8-ste eenheidswortel α waarvoor geldt: $\alpha^2 + \alpha + 2 = 0$.

3) Gegeven zijn de primitieve n-de machts eenheidswortels α en β. Bewijs dat de BCH-code van lengte n met ontwerpafstand δ gedefinieerd via α equivalent is met die gedefinieerd via β.

---

* Met BCH-codes worden hier steeds strikte BCH-codes bedoeld.

4) i) Bepaal de dimensie van de binaire BCH-code met $(n, \delta) = (31, 5), (31, 7)$ en $(31, 9)$.
ii) Bepaal de minimumafstand van $BCH(31, 9)$.

5) Bewijs dat voor een binaire BCH$-(n = 2^m - 1, \delta = 5)$ code geldt dat de dimensie gelijk is aan $2^m - 1 - 2m$ als $m \geq 3$.

6) i) Bewijs dat de binaire BCH-codes met $n = 17$ en $k = 9$ minimumafstand 5 hebben.
ii) Als 6i) voor $n = 65, k = 53$.

7)i) Bewijs dat voor een BCH-(n, δ)-code met δ deelt n geldt $d = \delta$.
ii) Bepaal de d van de binaire cyclische code van lengte 63 met $g = X^6 + X + 1 \in \mathbb{F}_2[X]$.

8) i) De binaire BCH -$(2^m - 1, 2t + 1)$-code heeft $d = 2t + 1$ als

$$\sum_{i=0}^{t+1} \binom{2^m - 1}{i} > 2^{mt}.$$

ii) Bepaal d voor de binaire BCH $(31, 5)$ en BCH $(31, 7)$-code.

9) Zij α een primitieve n-de machts eenheidswortel met $n = 2^m - 1$, waarin $m \geq 3$, m oneven. Bewijs dat de minimumafstand van een binaire cyclische code C, die lengte $n = 2^m - 1$ heeft en voortbrengerpolynoom g met $g(\alpha) = g(\alpha^{-1}) = 0$, minstens 5 is.

10) i) Bewijs dat alle cyklische codes over $\mathbb{F}_2$ van lengte $n = 2^m + 1$, met m even, voortgebracht door een primitieve n-de machts eenheidswortel minimumafstand 5 hebben.
ii) Toon aan dat de beide cyclische $(17, 8)$-codes over $\mathbb{F}_2$ minimumafstand 6 hebben.

11) Zij $n = 2^m - 1$ en α een primitieve n-de eenheidswortel met minimumpolynoom $f \in \mathbb{F}_2[X]$. Laat C een binaire cyklische code met voortbrengerpolynoom $(X^n - 1)/f$ zijn. Toon aan dat C de $(2^m - 1, m)$-simplex code is en laat met behulp van de BCH-grens zien dat $d = 2^{m-1}$.

12) Zij C een BCH-code met ontwerpafstand δ. Bewijs dat voor de uitgebreide code $\overline{C}$ geldt: $d \geq \delta + 1$.

13) Gegeven is de binaire BCH-$(n = 31, \delta = 5)$-code gedefinieerd via een primitieve 31-ste eenheidswortel waarvoor geldt $\alpha^5 + \alpha^2 + 1 = 0$. Wat kan worden geconcludeerd over het foutenpatroon als $S(Z) = \alpha^{19} + \alpha^7 Z + \alpha^{20} Z^2 + \alpha^{14} Z^3$?

14) Gegeven is de binaire BCH-code met $n = 15, \delta = 7$ gedefinieerd via α waarvoor $\alpha^4 + \alpha + 1 = 0$. Decodeer (111110101111000).

15) Gegeven is de code $RS(n = 7, \delta = 5)$ over $\mathbb{F}_8$. Decodeer $(\alpha^3, \alpha, 1\alpha^2, 0, \alpha^3, 1)$, waarin α een primitieve 7-de eenheidswortel is waarvoor geldt $\alpha^3 + \alpha + 1 = 0$.

16) Laat C een RS -code over $\mathbb{F}_4$ zijn met ontwerpafstand 2 gedefinieerd via een α met $\alpha^2 + \alpha + 1 = 0$.
i) Bepaal de parameters n, k en d van C.
ii) Geef een lijst van de codewoorden.
iii) Breid C uit tot $\overline{C}$ door middel van de totale toets $\sum c_i = 0$. Geef een lijst van de codewoorden van $\overline{C}$.
iv) Bepaal de parameters n, k en d van $\overline{C}$.
v) Bepaal de parameters n, k en d van de code die ontstaat door af te beelden naar $\mathbb{F}_2$.

17) Laat C een RS-code met parameters $(2^m - 1, k, d)$ zijn. Bewijs dat C de primitieve binaire BCH-code van lengte $2^m - 1$ en ontwerpafstand d bevat.

18) Laat C een Reed-Solomon-code zijn. i) Bewijs dat $C^\perp$ ook een RS-code is.
ii) Breid C uit tot $\overline{C}$ door middel van de totale toets $\sum c_i = 0$. Bewijs dat $\overline{C}$ een MDS-code is.

19) Bepaal k, d en de nulpunten van de binaire kwadraatrestcode QR_{g_0} van lengte $n = 17, 23, 31$ en 47.

20) Bewijs dat de kwadraatrestcodes over $\mathbb{F}_2$ van lengte n de volgende eigenschappen hebben.
i) Als $n \equiv -1(\text{mod}8)$ dan $QR_{(X-1)g_0} \subset QR^\perp_{(X-1)g_0}$, $QR^\perp_{g_0} = QR_{(X-1)g_0}$ en $\overline{QR}_{g_0}$ is zelf-duaal.
ii) Als $n \equiv 1(\text{mod}8)$ dan $QR_{(X-1)g_0} \subset QR^\perp_{(X-1)g_1}$, $QR^\perp_{g_0} = QR_{(X-1)g_1}$ en $(\overline{QR}_{g_0})^\perp = \overline{QR}_{g_1}$.

21) Toon aan dat de gewichtsverdeling van de uitgebreide $(48, 12)$ QR-code over $\mathbb{F}_2$ eenduidig wordt bepaald door de identiteiten van MacWilliams.

22)i) Bewijs dat de uitgebreide binaire Golay code $\overline{G}_{23}$ zelf-duaal is.
ii) Bepaal de gewichtsverdeling van $\overline{G}_{23}$ en van G_{23}.

23 i) Bewijs dat de uitgebreide Golay code $\overline{G}_{11}$ zelf-duaal is.
ii) Bepaal de gewichtsverdeling van $\overline{G}_{11}$ en die van G_{11}. Hierbij mag gebruik worden gemaakt van het feit dat $\overline{G}_{11}$ een transitieve code is.

Hoofdstuk V. Het corrigeren van blokken van fouten

Tot nu toe zijn we er bij de behandeling van codeertechnieken stilzwijgend van uitgegaan dat ze worden toegepast in situaties waar alle patronen van een zeker aantal fouten even waarschijnlijk zijn. Maar deze aanname is bij toepassingen vaak niet reëel. In veel communicatiesystemen doen zich opeenhopingen van fouten voor binnen een kort tijdsbestek. Als we van een code eisen dat slechts "opeenhopingen" van l fouten moeten worden gecorrigeerd en niet elk patroon van l fouten, is het vaak mogelijk efficiëntere codes te vinden. Zo een opeenhoping zullen we hier (fouten-)blok noemen; in het Engels wordt de term "burst" gebruikt.

(5.1) Definitie. De vector $x \in \mathbb{F}_q^n$ heet een *(cyclisch) foutenblok* van lengte l als de coördinaten van x die ongelijk nul zijn optreden in l (cyclisch gezien) opeenvolgende posities, waarbij op de eerste en laatste van deze l coördinaatplaatsen een coördinaat ongelijk aan nul staat.

Dus $(000010110100) \in \mathbb{F}_2^{12}$ is een foutenblok van lengte 6; $(010000010100) \in \mathbb{F}_2^{12}$ is een cyclisch foutenblok van lengte 7. Bij cyclische codes verstaan we onder foutenblok steeds een cyclisch foutenblok.

(5.2) Definitie. Een lineaire code die alle foutenblokken van lengte $\leq l$ kan corrigeren heet een *l-blok corrigerende code*.

Dit betekent dat alle foutenblokken van lengte $\leq l$ tot verschillende nevenklassen van $C \subset \mathbb{F}_q^n$ behoren. Het doel is nu om bij gegeven n en l zulke l-blok corrigerende codes te vinden waarvan de dimensie k maximaal is.

(5.3) Stelling. *(Reiger-grens) Voor een lineaire l-blok corrigerende (n,k)-code C geldt $n - k \geq 2l$.*

Bewijs. Omdat C alle blokken van lengte $\leq l$ kan corrigeren geldt voor verschillende foutenblokken x en y van lengte $\leq l$ dat $x - y \notin C$. Een foutenblok van lengte $\leq 2l$ is te schrijven als het verschil van twee foutenblokken van lengte $\leq l$, dus C bevat geen foutenblokken van lengte $\leq 2l$.

Beschouw de verzameling $\{z \in \mathbb{F}_q^n : z_i = 0 \quad \text{als} \quad i > 2l\}$ die bestaat uit q^{2l} elementen. Elke nevenklasse van C bevat hoogstens één zo'n element, dus $q^{n-k} \geq q^{2l}$, zodat $n - k \geq 2l$. □

(5.4) Definitie. Een l-blok corrigerende (n,k)-code heet *optimaal* als $n - k = 2l$.

Voorbeeld. De binaire cyclische code van lengte 15 met voortbrengerpolynoom $X^6 + X^5 + X^4 + X^3 + 1$ is 3-blok corrigerend optimaal.

We bekijken nu een aantal manieren om blok corrigerende codes te construeren.

I. Fire-codes

Dit zijn cyclische blok-corrigerende codes in 1959 ontdekt door Fire.

De veelterm $b \in \mathbb{F}_q[X]$ die correspondeert met een cyclisch foutenblok van lengte l is van de vorm $b = X^i B$, waarbij B een polynoom is van graad $l - 1$ met $B(0) \neq 0$. De veelterm B wordt *blokpatroon* genoemd en i het *beginpunt van het blok*.

(5.5) Definitie. Als $l \in \mathbb{Z}_{>1}$ en $f \in \mathbb{F}_q[X]$ is irreducibel van graad $m \geq l$ met g.g.d.$(X^{2l-1}-1, f) = 1$, dan heet de cyclische code C over $\mathbb{F}_q$ met voortbrenger-polynoom $g = (X^{2l-1}-1)f$ van lengte $n = \text{orde}(g)$ (zie hierna) een *Fire-code*.

Intermezzo De orde van een polynoom. Laat $f \in \mathbb{F}_q[X]$ een polynoom zijn met $\text{gr}(f) \geq 1$ en $f(0) \neq 0$. We beschouwen een eindig uitbreidingslichaam $\mathbb{F}$ van $\mathbb{F}_q$ waarin f volledig in lineaire factoren splitst, zeg $f = \prod_{i=1}^{n}(X - \alpha_i)$. De elementen α_i brengen een ondergroep van $\mathbb{F}^*$ voort. De orde van deze ondergroep is de *orde van* f. Merk op dat dit niet van de keuze van $\mathbb{F}$ afhangt. De orde van f is dan ook gelijk aan het k.g.v. van de ordes van de α_i.

Als f een irreducibel polynoom is dan geldt $\text{orde}(f) = \text{orde}(\alpha_i)$ voor $i = 1, \ldots, n$. □

(5.6) Stelling. *De Fire-code C over $\mathbb{F}_q$ heeft lengte $n =$ k.g.v.$(2l-1, \text{orde}(f))$ en is l-blok corrigerend.*

Bewijs. Uit de eigenschappen van $X^{2l-1}-1$ en f volgt dat de orde van g gelijk is aan k.g.v.$(2l-1, \text{orde}(f))$.
Vanaf nu is het bewijs tevens een decodeeralgoritme voor een foutenblok. Veronderstel dat het ontvangen woord $r = c + b$ is met $c \in C$ en b een foutenblok van lengte $t \leq l$. Bepaal veeltermen s_1 en s_2 gedefinieerd door

$$\begin{aligned} s_1 &\equiv r \equiv b(\text{mod}(X^{2l-1}-1)) \quad \text{met } \text{gr}(s_1) < 2l-1, \\ s_2 &\equiv r \equiv b(\text{mod}(f)) \quad \text{met } \text{gr}(s_2) < m. \end{aligned}$$

We noemen het paar (s_1, s_2) het *syndroom* van r; het is eenvoudig in te zien dat $s_1 = 0 \iff b = 0$. Neem aan dat $s_1 \neq 0$. Uit $b = X^i B$ volgt dat

$$s_1 \equiv X^{i'} B(\text{mod}(X^{2l-1}-1)),$$

met $i \equiv i'(\text{mod}(2l-1))$ en $0 \leq i' < 2l-1$.

De veelterm s_1 bepaalt eenduidig B en i'. Bekijkt men namelijk de exponenten die optreden in s_1 op een cirkel waarop achtereenvolgens $0, 1, \ldots, 2l-2$ zijn aangegeven, dan is er precies één gat tussen de optredende exponenten waarvan de lengte $\geq l-1$ is. Dit gat eindigt bij $X^{i'-1}$. Hiermee is i' bepaald en ook B, want $B = X^{-i'} s_1$, waarbij in het rechterlid de exponenten modulo $2l-1$ worden genomen.

Voor het beginpunt i geldt $i = i' + j(2l-1)$ met $0 \leq j < n/(2l-1)$. Dus

$$s_2 \equiv X^{i'+j(2l-1)} B(\text{mod}(f)).$$

Zij $\alpha \in \mathbb{F}_{q^m}$ een nulpunt van f zodat $\text{orde}(\alpha) = \text{orde}(f)$. Omdat f irreducibel is en $\text{gr}(B) < \text{gr}(f)$ geldt $B(\alpha) \neq 0$ terwijl

$$s_2(\alpha) = \alpha^{i'+j(2l-1)} B(\alpha),$$

ofwel

$$\alpha^{j(2l-1)} = s_2(\alpha)/(\alpha^{i'} B(\alpha)).$$

Hieruit volgt de waarde van j modulo de orde van α^{2l-1}, ofwel de waarde van j modulo

$$\frac{\text{orde}(f)}{\text{g.g.d.}(2l-1,\text{orde}(f))} = \frac{\text{k.g.v}(2l-1,\text{orde}(f))}{2l-1} = \frac{n}{2l-1}.$$

Dit legt j met $0 \leq j < n/(2l-1)$ vast, zodat ook het beginpunt van het foutenblok is vastgelegd.

Uit het voorgaande is duidelijk dat verschillende foutenblokken van lengte $\leq l$ verschillende syndromen hebben. Dus de Fire-code C is l-blok corrigerend. □

Merk op dat de redundantie van een l-blok corrigerende Fire-code minstens $3l-1$ is.

Voorbeeld. De binaire cyclische code voortgebracht door $g = (X^5-1)(X^3+X^2+1)$ is een Fire-code van lengte 35, die blokken van lengte ≤ 3 corrigeert. Als bijv. het syndroom van een ontvangen woord gelijk is aan $s_1 = X^4 + X$ en $s_2 = X$ dan $b = X^{19}(X^2+1)$. Ga deze beweringen na.

II. Vlechten

Deze methode is geschikt om uit korte blok-corrigerende codes langere te maken.

Bij vlechten wordt uit een (n,k)-code C een $(\lambda n, \lambda k)$-code C_λ gemaakt door λ (niet noodzakelijk verschillende) woorden uit C volgens het onderstaande diagram samen te stellen tot een woord van lengte λn; we schrijven λ woorden $c_i \in C$ als rijvectoren onder elkaar en lezen kolom voor kolom naar beneden zodat een woord van lengte λn ontstaat:

$$\begin{matrix} c_1 \to \\ \vdots \\ c_\lambda \to \end{matrix} \begin{pmatrix} \downarrow & \downarrow & \downarrow & \downarrow & \dots \\ & & \vdots & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \dots \end{pmatrix}.$$

We doen dit voor alle λ-tallen van woorden uit C en verkrijgen zo een code C_λ. We noemen de nieuwe code C_λ de code die uit C ontstaat door λ *keer te vlechten*.

Veronderstel dat C blokken van lengte $\leq l$ kan corrigeren. Een foutenblok van lengte $\leq \lambda l$ in C_λ wordt over hoogstens $l+1$ kolommen van het diagram verdeeld, waarbij per rijvector ($\in C$) een corrigeerbaar foutenblok van lengte $\leq l$ ontstaat. Dus C_λ kan blokken van lengte $\leq \lambda l$ corrigeren. Merk op dat een optimale C een optimale C_λ levert.

(5.7) Stelling. *Als C een cyclische (n,k)-code is met voortbrengerpolynoom g, dan is de cyclische $(\lambda n, \lambda k)$-code $\tilde{C}$ met voortbrengerpolynoom $g(X^\lambda)$ de λ maal gevlochten code C_λ.*

Bewijs. Als $c \in \tilde{C}$ dan is $c(X) = \sum_{i=0}^{\lambda n-1} c_i X^i$ deelbaar door $g(X^\lambda)$. Schrijf $c(X)$ in de volgende vorm, waarbij de exponenten in restklassen modulo λ worden verdeeld:

$$\begin{aligned} &c_0X^0 + c_\lambda X^\lambda + \ldots + c_{(n-1)\lambda}X^{(n-1)\lambda} + \\ &c_1X^1 + c_{\lambda+1}X^{\lambda+1} + \ldots + c_{(n-1)\lambda+1}X^{(n-1)\lambda+1} + \\ &\qquad\vdots \\ &c_{\lambda-1}X^{\lambda-1} + c_{\lambda+(\lambda-1)}X^{2\lambda-1} + \ldots + c_{(n-1)\lambda+\lambda-1}X^{(n-1)\lambda+\lambda-1}. \end{aligned}$$

Elke rij is deelbaar door $g(X^\lambda)$, ofwel voor $0 \leq i \leq \lambda - 1$ geldt

$$g(X^\lambda) \quad \text{deelt} \quad X^i(c_i + c_{\lambda+i}X^\lambda + \ldots + c_{(n-1)\lambda+i}X^{(n-1)\lambda}),$$

zodat er geldt

$$g(X^\lambda) \quad \text{deelt} \quad c_i + c_{\lambda+i}X^\lambda + \ldots + c_{(n-1)\lambda+i}X^{(n-1)\lambda}$$

waaruit weer volgt

$$g(X) \quad \text{deelt} \quad c_i + c_{\lambda+i}X + \ldots + c_{(n-1)\lambda+i}X^{(n-1)},$$

met andere woorden

$$(c_i, c_{\lambda+i}, \ldots, c_{(n-1)\lambda+i}) \in C.$$

De rijen van het diagram zijn dus op te vatten als woorden uit C. Dit betekent $\tilde{C} \subset C_\lambda$ zodat $\tilde{C} = C_\lambda$ omdat beide codes dimensie λk hebben. $\square$

III. Tensorproduct codes

Deze constructie levert codes die tegelijk blokken van fouten en toevallige fouten kunnen corrigeren. We beginnen met een intermezzo waarin de definitie van het tensorproduct wordt gegeven.

Intermezzo. *Het tensorproduct*

Laat k een lichaam zijn en V en W twee (eindig-dimensionale) vectorruimten over k. Beschouw nu de vectorruimte T over k waarvan de elementen de (eindige) uitdrukkingen van de vorm

$$\sum_{i \in I} c_i(v_i, w_i) \qquad \text{met } c_i \in k, v_i \in V, w_i \in W.$$

zijn. Hierbij wordt de indexverzameling I altijd eindig genomen. Beschouw nu in T de lineaire deelruimte N opgespannen door de uitdrukkingen van de vorm

$$\begin{array}{r} (v_1 + v_2, w) - (v_1, w) - (v_2, w), \\ (v, w_1 + w_2) - (v, w_1) - (v, w_2) \\ (cv, w) - c(v, w) \\ (v, cw) - c(v, w) \end{array} \qquad \text{voor alle } v, v_1, v_2 \in V, w, w_1, w_2 \in W, c \in k.$$

De quotiëntruimte T/N heet het *tensorproduct* van V en W. Deze wordt genoteerd als $V \otimes W$. We noteren de restklasse van (v, w) als $v \otimes w$. Zo een element heet een *zuivere tensor*. Een willekeurig element van $V \otimes W$ is van de vorm $\sum_{i \in I} c_i(v_i \otimes w_i)$ en heet een *tensor*. Er gelden dan de volgende rekenregels in $V \otimes W$:

$$\begin{aligned} (v_1 + v_2) \otimes w &= v_1 \otimes w + v_2 \otimes w, \\ v \otimes (w_1 + w_2) &= v \otimes w_1 + v \otimes w_2, \\ c(v \otimes w) &= (cv) \otimes w = v \otimes (cw). \end{aligned}$$

Als e_i met $1 \leq i \leq n$ een basis van V is en f_j met $1 \leq j \leq m$ een basis van W dan vormen de tensoren $e_i \otimes f_j$ met $1 \leq i \leq n$ en $1 \leq j \leq m$ een basis van $V \otimes W$. We zien dus

$$\dim(V \otimes W) = \dim(V) \dim(W).$$

□

Gegeven zijn een lineaire (n_1, k_1, d_1)-code C over $\mathbb{F}_q$ en een lineaire (n_2, k_2, d_2)-code D over $\mathbb{F}_q$. We beschouwen nu het tensorproduct $C \otimes D$. Als c_i met $1 \leq i \leq k_1$ en d_j met $1 \leq j \leq k_2$ bases van C en D vormen dan wordt een basis van $C \otimes D$ gegeven door $c_i \otimes d_j$ met $1 \leq i \leq k_1$, $1 \leq j \leq k_2$. We kunen $C \otimes D$ inbedden in $\mathbb{F}_q^{n_1 n_2}$ via

$$c_i \otimes d_j \mapsto (c_i^{(1)} d_j, c_i^{(2)} d_j, \ldots, c_i^{(n_1)} d_j),$$

waarbij $c_i = (c_i^{(1)}, \ldots, c_i^{(n_1)})$. Als $c = (c_1, \ldots, c_{n_1}) \in C$ en $(d_1, \ldots, d_{n_2}) \in D$ dan wordt $c \otimes d$ afgebeeld op

$$(c_1 d_1, \ldots, c_1 d_{n_2}, \ldots\ldots, c_{n_1} d_{n_2}) \in F_q^{n_1 n_2}.$$

We identificeren $c \otimes d$ met $(c_1 d_1, \ldots, c_{n_1} d_{n_2})$. Voor het gewicht geldt

$$w(c \otimes d) = w(c) w(d).$$

Men kan de elementen $c \otimes d$ ook in de vorm van een $n_1 \times n_2$-matrix noteren:

$$c \otimes d = \begin{pmatrix} c_1 d_1 & \ldots & \ldots & c_1 d_{n_2} \\ c_2 d_1 & \ldots & \ldots & c_2 d_{n_2} \\ \vdots & & & \vdots \\ c_{n_1} d_1 & \ldots & \ldots & c_{n_1} d_{n_2} \end{pmatrix}; \tag{1}$$

hierbij zijn de rijen in de matrix woorden van D en de kolommen zijn woorden van C.

(5.8) Definitie. De code $C \otimes D$ heet de *(tensor)product code* van C en D. Dit is een $(n_1 n_2, k_1 k_2)$-code.
In oudere terminologie heet de code $C \otimes D$ ook wel het Kronecker-product van C en D. Een element van $C \otimes D$ heeft de gedaante

$$\sum_{i,j} \lambda_{ij} (c_i \otimes d_j) \qquad \text{met} \quad \lambda_{ij} \in \mathbb{F}_q.$$

Zo een element kan men dan met (1) in matrixvorm schrijven; hierin zijn de rijen woorden van D terwijl de kolommen woorden van C zijn. Omgekeerd levert iedere $n_1 \times n_2$-matrix waarvan de rijen woorden uit D zijn en de kolommen woorden uit C een element van $C \otimes D$.

(5.9) Eigenschap. *Er geldt:* $d(C \otimes D) = d(C) \cdot d(D)$.

Bewijs. Neem een woord $\neq 0$ van $C \otimes D$ en schrijf dit in matrixvorm. Dan is er een rij van gewicht $\geq d(D)$. De kolommen horende bij de plaatsen $\neq 0$ in die rij hebben gewicht $\geq d(C)$. Dus we vinden een woord met gewicht $\geq d(C)d(D)$. Anderzijds volgt

uit $w(c \otimes d) = w(c)w(d)$ dat er minstens één woord van de vorm $c \otimes d$ is met gewicht $d(C)d(D)$. $\square$

Als G_C en G_D voortbrengermatrices zijn voor C en D dan is het tensorproduct

$$G_C \otimes G_D = \begin{pmatrix} g_{11}G_D & \dots & g_{1n_1}G_D \\ \vdots & & \vdots \\ g_{k_1 1}G_D & \dots & g_{k_1 n_1}G_D \end{pmatrix}$$

een voortbrengermatrix van $C \otimes D$.

Het vormen van de productcode is een generalisatie van het vlechten van een code C. We krijgen op equivalentie na de code C_λ door te nemen $E \otimes C$, waar E de triviale $(\lambda, \lambda, 1)$-code is. (Ga na.)

Het corrigerend vermogen van een tensorproduct code wordt gegeven in de volgende twee stellingen.

(5.10) Stelling. *Als C een l_1-blok corrigerende code is en D een l_2-blok corrigerende code, dan is $C \otimes D$ een $\max(n_1 l_2, n_2 l_1)$-blok corrigerende code.*

Bewijs. Stuur een woord van $C \otimes D$ rij voor rij over (in matrixvorm). Een foutenblok van lengte $\leq n_2 l_1$ beïnvloedt hoogstens $l_1 + 1$ opeenvolgende rijen. Dit leidt in de kolommen tot foutenblokken van lengte $\leq l_1$. Door kolom voor kolom te decoderen wordt het foutenblok van lengte $n_2 l_1$ gecorrigeerd.

Door de rol van rijen en kolommen te wisselen kan men ook foutenblokken van lengte $\leq n_1 l_2$ corrigeren. Dus de code $C \otimes D$ corrigeert blokken van lengte $\leq \max(n_1 l_2, n_2 l_1)$. $\square$

(5.11) Stelling. *De tensorproduct code $C \otimes D$ kan tegelijkertijd $\leq [(d_1 d_2 - 1)/2] = t$ toevallige fouten én foutenblokken van lengte $\leq \max(n_1 t_2, n_2 t_1)$ met $t_1 = [(d_1 - 1)/2]$ en $t_2 = [(d_2 - 1)/2]$ corrigeren.*

Toelichting. Dit betekent dat de in de stelling genoemde foutenpatronen in verschillende nevenklassen van $C \otimes D$ in $\mathbb{F}_q^{n_1 n_2}$ moeten liggen. In het bizonder mag een nevenklasse niet zowel een vector van gewicht $\leq t$ als een foutenblok van gewicht $> t$ en lengte $\leq \max(n_1 t_2, n_2 t_1)$ bevatten. In de standaardtabel kan men dan als nevenklassehoofden nemen de elementen van gewicht $\leq t$ en de foutenblokken van gewicht $> t$ en lengte $\leq \max(n_1 t_2, n_2 t_1)$, zodat deze foutenpatronen corrigeerbaar zijn.

Bewijs. Uit $d(C \otimes D) = d_1 d_2$ resp. uit (5.10) volgt dat een nevenklasse niet twee foutenpatronen van gewicht $\leq t$ resp. niet twee foutenblokken van gewicht $> t$ en lengte $\leq \max(n_1 t_2, n_2 t_1)$ bevat. Stel nu dat $n_1 t_2 \leq n_2 t_1$ en stuur het woord rij voor rij over. Indien een toevallige fout van gewicht $\leq t$ en een foutenblok van gewicht $> t$ en lengte $\leq n_2 t_1$ in één nevenklasse liggen dan is hun verschil c een codewoord in $C \otimes D$. Bekijk het gewicht van dit codewoord.

Het gewicht van een kolom $\neq 0$ is $\geq d_1$ en zo een kolom bevat hoogstens t_1 fouten uit het foutenblok, en dus minstens $d_1 - t_1$ toevallige fouten. De $\leq t$ toevallige fouten treden dus op in hoogstens $[t/(d_1 - t_1)]$ kolommen. Dit betekent dat er hoogstens $[t/(d_1 - t_1)]$

kolommen $\neq 0$ zijn, die elk hoogstens t_1 van de fouten van het blok bevatten. Het gewicht van het codewoord c is dus

$$\leq [t/(d_1 - t_1)]t_1 + t \leq t(1 + t_1/(d_1 - t_1)) < 2t < d_1 d_2 = d(C \otimes D),$$

wat onmogelijk is. $\square$

IV. Reed-Solomon codes.

De Reed-Solomon codes zijn bij uitstek geschikt om meerdere foutenblokken per ontvangen woord te corrigeren.

We hebben in Hoofdstuk IV, §2 gezien dat een $(q^m - 1, q^m - 1 - 2t)$-RS code over $\mathbb{F}_{q^m}$ met $d = 2t + 1$ een $((q^m - 1)m, (q^m - 1 - 2t)m)$-code over $\mathbb{F}_q$ levert. Deze laatste code kan elk foutenpatroon corrigeren waarin de fouten beperkt blijven tot $\leq t$ blokken van m symbolen ("m-bit bytes"). Immers, het ontvangen woord van lengte $m(q^m - 1)$ wordt verdeeld in $(q^m - 1)$ stukken ("bytes"), die worden omgezet in elementen van $\mathbb{F}_{q^m}$.

Zij r het maximale aantal beïnvloede bytes ten gevolge van een foutenblok van lengte l, dan geldt $l \geq (r-2)m + 2$, ofwel $r \leq [(l + 2m - 2)/m]$. Nu zijn s blokken van lengte l corrigeerbaar als het totale aantal beïnvloede bytes $\leq t$ is. Hieruit volgt dat een patroon van s blokken van lengte l met

$$s \leq \left[\frac{t}{[(l + 2m - 2)/m]} \right]$$

corrigeerbaar is.

V. Koppeling (of concatenatie).

Bij deze constructie, die in 1966 door Forney werd geïntroduceerd, worden twee of meer korte codes gecombineerd tot een lange code, die een grote foutcorrigerende capaciteit heeft en waarvan de decodeercomplexiteit beperkt blijft.

De codes die zo ontstaan zijn efficiënt bij het tegelijk corrigeren van toevallige fouten en blokken van fouten.

De twee codes die gekoppeld worden zijn de *inwendige code* C_1 met parameters (n, k, d) over $\mathbb{F}_q$ en de *uitwendige code* C_2 met parameters (N, K, D) over $\mathbb{F}_{q^k}$.

De codes C_1 en C_2 worden gekoppeld volgens het diagram

$$\rightarrow \text{[uitwendige codeerder]} \rightarrow \text{[uitwendig kanaal]} \rightarrow \text{[uitwendige decodeerder]} \rightarrow$$

waarbij het uitwendig kanaal zelf van de vorm is

$$\text{[inwendige codeerder]} \rightarrow \text{[kanaal]} \rightarrow \text{[inwendige decodeerder]}.$$

Het *uitwendig kanaal* brengt q-aire k-tallen over. Deze k-tallen beschouwt men via een basis van $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ als elementen van $\mathbb{F}_{q^k}$, zodat het uitwendige kanaal symbolen uit $\mathbb{F}_{q^k}$ overbrengt. De uitwendige code C_2 moet de fouten ontstaan in het uitwendig kanaal corrigeren. Als uitwendige codes zijn RS-codes uitermate geschikt.

De geschetste combinatie heet een *gekoppelde code*.

Codering bij een gekoppelde code.

Een blok van kK symbolen uit $\mathbb{F}_q$ wordt verdeeld in K k-tallen, die worden opgevat als K elementen uit $\mathbb{F}_{q^k}$. De uitwendige codeerder levert een codewoord $(c_0, \ldots, c_{N-1}) \in C_2 \subseteq \mathbb{F}_{q^k}^N$. Elke c_i wordt dan als k-tal over $\mathbb{F}_q$ door de inwendige codeerder omgezet in een n-tal over $\mathbb{F}_q$: een codewoord uit C_1. Zo ontstaat een codewoord van lengte nN (opgebouwd uit N woorden uit C_1) uit de gekoppelde code.

Conclusie. *De gekoppelde code is een lineaire code over $\mathbb{F}_q$ met parameters*

lengte nN,
dimensie kK,
minimumafstand $\geq dD$.

Voorbeeld. Laat C_1 de $(8, 4, 4)$ uitgebreide binaire Hamming code zijn; neem voor C_2 een $(12, 6, 7)$-RS code over $\mathbb{F}_{16}$. Dan is de gekopppelde code een binaire $(96, 24, \geq 28)$-code.

Decodering bij een gekoppelde code.

Een blok van nN ontvangen symbolen uit $\mathbb{F}_q$ wordt verdeeld in N n-tallen. De inwendige decodeerder maakt hier eerst N codewoorden uit C_1 van, die daarna worden omgezet in N k-tallen informatiesymbolen. Deze N k-tallen worden opgevat als een ontvangen woord over $\mathbb{F}_{q^k}$ van lengte N. De uitwendige decodeerder maakt hiervan eerst een woord uit C_2 en zet dit vervolgens om in K informatiesymbolen uit $\mathbb{F}_{q^k}$. Deze leveren kK informatiesymbolen uit $\mathbb{F}_q$.

Een foutenpatroon kan door de gekoppelde code juist dan niet worden gecorrigeerd als de niet corrigeerbare inwendige n-tallen een niet-corrigeerbaar patroon voor de uitwendige code vormen.

Bij gekoppelde codes wordt C_1 gebruikt om toevallige fouten te corrigeren, terwijl C_2 dient ter correctie van blokken van fouten.

Voorbeeld. Neem C_1 een binaire $(7, 4, 3)$-Hamming code. Voor C_2 kiezen we een $(15, 7, 9)$-RS-code over $\mathbb{F}_{16}$. De gekoppelde code is een binaire $(105, 28, \geq 27)$-code. Een element uit $\mathbb{F}_2^{105}$ wordt juist gedecodeerd als ≤ 4 van de 15 delen uit $\mathbb{F}_2^7$ meer dan 1 fout bevatten.

Opgaven bij Hoofdstuk V

1. i) Bewijs dat de binaire cyclische code van lengte 7 met voortbrengerpolynoom $X^4 + X^3 + X^2 + 1$ 2-blok corrigerend is.
ii) Beschrijf met behulp van i) een 4-blok corrigerende code.
iii) Bewijs dat de even gewichts deelcode van de binaire $(2^m - 1, 2^m - m - 1)$-Hamming code 2-blok corrigerend is.

2. i) Zij H de toetsmatrix van een (n, k)-code C met als kolommen $k_1, k_2, \ldots, k_n$. Beschrijf de toetsmatrix van C_λ in termen van H.
ii) Geef de toetsmatrix van een binaire $(25, 20)$-code die alle blokken van lengte ≤ 5 ontdekt.

3. i) Bewijs dat voor een lineaire code C die alle blokken van lengte $\leq l$ ontdekt geldt $n - k \geq l$.
ii) Bewijs dat een cyclische (n, k)-code alle blokken van lengte $\leq n - k$ ontdekt.

4. i) Ga na dat de binaire cyclische code C die wordt voortgebracht door de veelterm $g = (X^7 - 1)(X^4 + X + 1)$ een Fire-code is.
ii) Bepaal de lengte van C en de blok-corrigerende capaciteit.
iii) Bepaal het foutenblok als het syndroom van het ontvangen woord gelijk is aan $s_1 = X^6 + X^4 + 1$ en $s_2 = X$.

5. Vlecht een $(n = 15, k = 7)$-BCH-code over $\mathbb{F}_2$ zeven keer. Toon aan dat alle blokken van lengte ≤ 14 corrigeerbaar zijn.

6. Beschouw de $(n = 31, k = 15)$-RS-code over $\mathbb{F}_{2^5}$. Beschrijf de blok-corrigerende capaciteit van de bijbehorende binaire code.

7. i) Bewijs dat door verkorten van een code de blok-corrigerende capaciteit niet verandert.
ii) Gegeven is een binaire cyclische code $(135, 123)$-code die 5-blok corrigerend is. Construeer een binaire code van lengte 2040 met rendement 0.9, die blokken van lengte 85 kan corrigeren.
iii) Construeer via een RS-code een binaire code van lengte 2040 met rendement bijna 0.9, die blokken van lengte 90 corrigeren kan.

8. Bewijs dat het bij systematische codering van $C \otimes D$ niet uitmaakt of de controlesymbolen in het blok rechtsonder via C of via D worden gevormd.

9. Zij α een primitieve 63-ste eenheidswortel met minimumpolynoom $X^6 + X + 1 \in \mathbb{F}_2[X]$. Nu is $X^6 + X^4 + X^2 + X + 1 \in \mathbb{F}_2[X]$ het minimumpolynoom van α^3.
i) Bepaal de lengte en de blok-corrigerende capaciteit van de binaire Fire-code met voortbrengerpolynoom $g_1 = (X^9 - 1)(X^6 + X + 1)$.
ii) Bepaal het voortbrengerpolynoom g_2 van de binaire BCH-code van lengte 63 en ontwerpafstand 5.
iii) Bepaal lengte en dimensie van de cyclische code C met voortbrengerpolynoom k.g.v.(g_1, g_2).
iv) Bewijs dat C *tegelijk* alle blokken van lengte ≤ 5 en alle toevallige fouten van gewicht ≤ 2 kan corrigeren.

Hoofdstuk VI. Binaire Reed-Muller Codes

Deze codes zijn genoemd naar hun ontdekkers Reed (1954) en Muller (1954). Zij zijn eenvoudig te decoderen bij een weliswaar betrekkelijk laag rendement.

§1 *Definitie en parameters van binaire Reed-Muller codes*

We zullen de binaire Reed-Muller codes definiëren via $\mathbb{F}_2$-waardige functies op $\mathbb{F}_2^m$. De $\mathbb{F}_2$-waardige functies op $\mathbb{F}_2^m$ vormen een ring met de bewerkingen gedefinieerd door optellen en vermenigvuldigen van de waarden van zulke functies. Deze ring heeft 2^{2^m} elementen en wordt genoteerd $\mathcal{F}(\mathbb{F}_2^m)$. Een polynoom F in $\mathbb{F}_2[X_1, \ldots, X_m]$ definieert een $\mathbb{F}_2$-waardige functie op $\mathbb{F}_2^m$. Deze afbeelding

$$\phi : \mathbb{F}_2[X_1, \ldots, X_m] \to \mathcal{F}(\mathbb{F}_2^m)$$

is een ringhomomorfisme. Omdat voor elk element van $\mathbb{F}_2$ geldt $x^2 = x$ definiëren de polynomen in het ideaal $I_m = (X_1^2 - X_1, \ldots, X_m^2 - X_m)$ de nulfunctie. Daarom factorizeert het homomorfisme ϕ via de ring

$$R_m = \mathbb{F}_2[X_1, \ldots, X_m]/(X_1^2 - X_1, \ldots, X_m^2 - X_m).$$

We vinden zo een homomorfisme $\psi : R_m \to \mathcal{F}(\mathbb{F}_2^m)$.

Er blijkt dat alle functies uit $\mathcal{F}(\mathbb{F}_2^m)$ afkomstig zijn van polynomen en dat het ideaal I_m precies de kern is van ϕ. Voor we dit aantonen bepalen we eerst het aantal elementen van R_m.

(1.1) Lemma. *De dimensie van R_m als $\mathbb{F}_2$-vectorruimte is 2^m.*

Bewijs. Met inductie naar m toont men aan dat ieder element van R_m een unieke representant heeft van de vorm

$$f = \sum_{\alpha} a_\alpha X_1^{\alpha_1} \cdots X_m^{\alpha_m}, \tag{1}$$

waarbij $\alpha = (\alpha_1, \ldots, \alpha_m)$ met α_i gelijk aan 0 of 1 en $a_\alpha \in \mathbb{F}_2$. De 2^m monomen $X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m}$ waarbij de exponenten α_i gelijk zijn aan 0 of 1 vormen een stelsel voortbrengers van R_m en zij zijn onafhankelijk. □

(1.2) Stelling. *Het homomorfisme $\psi : R_m \to \mathcal{F}(\mathbb{F}_2^m)$ is een isomorfisme van ringen.*

Bewijs. We bewijzen eerst de injectiviteit met inductie naar m. Voor $m = 1$ geldt de injectiviteit. Neem nu $m \geq 2$. Een element $f \in R_m$ met $f \neq 0$ kan geschreven worden als

$$f = X_m g(X_1, \ldots, X_{m-1}) + h(X_1, \ldots, X_{m-1}) \tag{2}$$

met $g, h \in R_{m-1}$. Stel $h \neq 0$. Vanwege de inductieveronderstelling levert h een niet-triviale functie op $\mathbb{F}_2^{m-1}$, m.a.w. er is een punt $(x_1, \ldots, x_{m-1}) \in \mathbb{F}_2^{m-1}$ waar de functie $\psi(h)$ niet verdwijnt. Maar dan geldt $\psi(f)(x_1, \ldots, x_{m-1}, 0) \neq 0$ zodat $\psi(f) \neq 0$ als functie. Het geval dat $h = 0$ gaat analoog gebruikmakend van het niet nul zijn van g. Dus de afbeelding ψ is injectief. Aangezien $\#(R_m) = \#(\mathcal{F}(\mathbb{F}_2^m)) = 2^{2^m}$ volgt dat ψ ook surjectief is. □

Gezien de bovenstaande Stelling zullen we in het vervolg $\psi(f)$ ook simpelweg noteren als f.

We kunnen nu de graad van een element van R_m en van $\mathcal{F}(\mathbb{F}_2^m)$ definiëren.

(1.3) Definitie De *graad* van een element $f \in R_m - \{0\}$ (resp. $\psi(f) \in \mathcal{F}(\mathbb{F}_2^m) - \{0\}$) is de graad van de unieke representant van f van de vorm (1).

Een affiene transformatie van de variabelen X_i, d.w.z. een transformatie gegeven door

$$\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{pmatrix} \mapsto A \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{pmatrix} + b,$$

met $A \in \mathrm{GL}(m, \mathbb{F}_2)$ en $b \in \mathbb{F}_2^m$ induceert een ringautomorfisme van $\mathbb{F}_2[X_1, \ldots, , X_m]$. De samenstelling met de kanonieke afbeelding $\mathbb{F}_2[X_1, \ldots, X_m] \to R_m$ factorizeert via R_m en induceert een automorfisme van R_m. De graad (in de zin van (1.3)) blijft hierbij behouden. (Ga na.)

(1.4) Definitie. De *binaire Reed-Muller code* $\mathcal{R}(r, m)$ van lengte 2^m en orde r (voor $0 \leq r \leq m$) is de lineaire code

$$\mathcal{R}(r, m) = \{c_f = (f(p))_{p \in \mathbb{F}_2^m} : f \in R_m \text{ met } \mathrm{gr}(f) \leq r\}.$$

We evalueren dus alle polynoomfuncties van graad $\leq r$ in m variabelen in de punten van $\mathbb{F}_2^m$. Gezien de factorisatie van ϕ via R_m kunnen we ons beperken tot de polynomen van de vorm (1). De coördinaatplaatsen van een woord laten we corresponderen met de punten van $\mathbb{F}_2^m$, die we ons daartoe op een bepaalde manier geordend denken. Merk op dat een woord in $\mathcal{R}(r, m)$ wordt vastgelegd door de nulpuntenverzameling van de bijbehorende functie (of het complement daarvan, namelijk de punten waar de functie waarde 1 heeft). We identificeren een woord in $\mathcal{R}(r, m)$ dan ook wel met de deelverzameling van $\mathbb{F}_2^m$ waar de bijbehorende functie 1 is.

(1.5) Propositie. *De binaire Reed-Muller code* $\mathcal{R}(r, m)$ *heeft dimensie* $1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$.

Bewijs. Uit (1.1) en (1.2) volgt dat de functies afkomstig van de monomen $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ met $w(\alpha_1, \ldots, \alpha_m) \leq r$ een basis vormen van $\mathcal{R}(r, m)$. Hun aantal is $1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$. $\square$

Voorbeelden.

i) $\mathcal{R}(0, m) = \{c_{f=0}, c_{f=1}\} = \{\underline{0}, \underline{1}\}$.

ii) $\mathcal{R}(m, m) = \mathbb{F}_2^{2^m}$.

iii) $\mathcal{R}(1, m) = \{c_f : f \in R_m \text{ met } \mathrm{gr}(f) \leq 1\}$.

Een basis van $\mathcal{R}(1, m)$ wordt gegeven door de functies $1, X_1, \ldots, X_m$. De woorden c_f met $\mathrm{gr}(f) = 1$ hebben gewicht 2^{m-1}.

(1.6) Opmerking. Als $p = (a_1, \ldots, a_m) \in \mathbb{F}_2^m$ dan is de functie

$$f_p = \prod_{i=1}^{m} (X_i + a_i + 1) = X_1 X_2 \cdots X_m + \text{ termen van lagere graad}$$

de karakteristieke functie van p want $f_p(p) = 1$ en $f_p(q) = 0$ voor $q \neq p$.

(1.7) Lemma. *De code $\mathcal{R}(m-1, m)$ bestaat uit de elementen van $\mathbb{F}_2^{2^m}$ van even gewicht.*

Bewijs. Neem $c = (c_1, \ldots, c_{2^m}) \in \mathbb{F}_2^{2^m}$ met $w(c)$ even. Hierbij correspondeert de i-de coördinaat met een punt p_i in $\mathbb{F}_2^m$. Met c correspondeert dan de deelverzameling $S = \{p_i \in \mathbb{F}_2^m : c_i = 1\}$. Omdat $\#(S)$ even is volgt op grond van (1.6) dat de graad van $f_S = \sum_{p \in S} f_p$ hoogstens $m-1$ is. De functie f_S is de karakteristieke functie van S, dus geldt $c = c_{f_S} \in \mathcal{R}(m-1, m)$. Daarmee bevat $\mathcal{R}(m-1, m)$ alle woorden van even gewicht. Omdat de deelruimte van elementen van even gewicht in $\mathbb{F}_2^{2^m}$ en $\mathcal{R}(m-1, m)$ beide dimensie $2^m - 1$ hebben volgt de beweerde gelijkheid. □

(1.8) Stelling. *De duale code $\mathcal{R}(r, m)^\perp$ van de Reed-Muller code van orde r en lengte 2^m is de Reed-Muller code $\mathcal{R}(m-r-1, m)$.*

Bewijs. Neem $c_f \in \mathcal{R}(r, m)$ en $c_g \in \mathcal{R}(m-r-1, m)$. Dan heeft $fg \in R_m$ graad $\leq m-1$. Dus $w(c_{fg})$ is even. Nu geldt

$$(c_f, c_g) = \sum_{p \in \mathbb{F}_2^m} f(p)g(p) = \sum_{p \in \mathbb{F}_2^m} fg(p) = 0$$

zodat $\mathcal{R}(m-r-1, m) \subseteq \mathcal{R}(r, m)^\perp$. Omdat de codes $\mathcal{R}(m-r-1, m)$ en $\mathcal{R}(r, m)^\perp$ dezelfde dimensie hebben geldt de stelling. □

Tenslotte bepalen we de minimumafstand van $\mathcal{R}(r, m)$. Met $f = X_1 X_2 \ldots X_r$ correspondeert het codewoord $c_f \in \mathcal{R}(r, m)$ van gewicht $w(c_f) = 2^{m-r}$. Namelijk c_f heeft een coordinaat 1 op de plaatsen horend bij de punten van de $(m-r)$-dimensionale affiene deelruimte van $\mathbb{F}_2^m$ gedefinieerd door het stelsel lineaire vergelijkingen $X_1 = 1, \ldots, X_r = 1$. Voor het bepalen van de minimumafstand moeten we het aantal nulpunten van een $f \in R_m$ afschatten. Merk op dat de nulpuntenverzameling $V(F) \subseteq \mathbb{F}_2^m$ van een $F \in \mathbb{F}_2[X_1, \ldots, X_m]$ alleen afhangt van de restklasse van F in R_m. Bij de afschatting spelen hypervlakken in $\mathbb{F}_2^m$ een belangrijke rol.

(1.9) Definitie. Een deelverzameling $H \subset \mathbb{F}_2^m$ heet een *hypervlak* als er een lineaire veelterm $h \in \mathbb{F}_2[X_1, \ldots, X_m]$ is met

$$H = \{(x_1, \ldots, x_m) \in \mathbb{F}_2^m : h(x_1, \ldots, x_m) = 0\}.$$

Een collectie hypervlakken heet *onafhankelijk* als de homogene lineaire delen van de definiërende lineaire vergelijkingen h onafhankelijke lineaire vormen zijn.

(1.10) Stelling. *Laat $f \in R_m$ met $f \neq 0$. Dan geldt:*

$$\#V(f) = \#\{p \in \mathbb{F}_2^m : f(p) = 0\} \leq 2^m - 2^{m-\mathrm{gr}(f)},$$

waarbij gelijkheid alleen optreedt als $V(f)$ te schrijven is als de vereniging van $\mathrm{gr}(f)$ lineair onafhankelijke hypervlakken.

Bewijs. We voeren het bewijs met inductie naar het aantal variabelen m. Voor $m = 1$ is de stelling evident. Neem nu $m \geq 2$ en laat de stelling bewezen zijn voor $\leq m-1$ variabelen.

Stel dat $V(f)$ een vereniging is van hypervlakken: $V = V(f) = \cup_{i=1}^{t} H_i$, waarbij de H_i worden gedefiniëerd door lineare polynomen $h_i \in \mathbb{F}_2[X_1, \ldots, X_m]$. Dan geldt voor het complement V^c van V :

$$V^c = \cap_{i=1}^{t} H_i^c$$

waarbij de H_i^c ook hypervlakken zijn (en wel gedefinieerd door $h_i + 1 = 0$). Omdat $V^c \neq \emptyset$ is het stelsel

$$h_1 + 1 = 0, \ldots, h_t + 1 = 0$$

oplosbaar. Neem hieruit een maximaal lineair onafhankelijk deelstelsel corresponderende met, zeg, de hypervlakken $H_1^c = 0, \ldots, H_s^c = 0$. Dan geldt $s \leq m$ en $V = \cup_{i=1}^{s} H_i$ zodat in R_m geldt $f = \prod_{i=1}^{s} h_i$. Via de affiene transformatie

$$(X_1, \ldots, X_m) \mapsto (h_1, \ldots, h_s, X_{s+1}, \ldots, X_m)$$

vinden we $\mathrm{gr}(f) = \mathrm{gr}(\prod_{i=1}^{s} h_i) = s$. Dus

$$\#V^c = 2^{m-s} \quad \text{zodat} \quad \#V = 2^m - 2^{m-s} = 2^m - 2^{m-\mathrm{gr}(f)}.$$

We zien dat V in dit geval te schrijven is als vereniging van $\mathrm{gr}(f)$ onafhankelijke hypervlakken.

Neem nu aan dat V geen vereniging is van hypervlakken. We kunnen dan een punt p van V vinden dat op geen enkel hypervlak bevat in V ligt. Beperken we nu f tot een hypervlak H door p gedefinieerd door $h = 0$, dan vinden we een functie f' in $m-1$ variabelen met $f' \neq 0$ (want $H \not\subseteq V$) en met $\mathrm{gr}(f') \leq \mathrm{gr}(f)$ (want f' wordt verkregen door de relatie $h = 0$ te substitueren in f). Passen we de inductieveronderstelling toe op H en f' dan krijgen we

$$\#(V \cap H) \leq 2^{m-1} - 2^{m-1-\mathrm{gr}(f')} \leq 2^{m-1} - 2^{m-1-\mathrm{gr}(f)}. \tag{3}$$

We tellen nu op twee manieren de verzameling

$$X = \{(q, H) : q \in V - \{p\}, \text{ en } H \text{ hypervlak door } p \text{ en } q\}.$$

Voor vaste q is het aantal hypervlakken door p en q gelijk aan $2^{m-1} - 1$. Dus:

$$\#(X) = (\#(V) - 1)(2^{m-1} - 1) \tag{4}$$

Anderzijds geldt dat er $2^m - 1$ hypervlakken H door p zijn terwijl voor vaste H door p het aantal punten q met $q \in (V - \{p\}) \cap H$ gelijk is aan $\#(V \cap H) - 1$. Uit (3) volgt dan

$$\#(X) \leq (2^{m-1} - 2^{m-1-\mathrm{gr}(f)} - 1)(2^m - 1) \tag{5}$$

Combinatie van (3) en (4) levert

$$\begin{aligned}\#(V) \leq & \big[(2^{m-1} - 2^{m-1-\mathrm{gr}(f)} - 1)(\frac{2^m - 1}{2^{m-1} - 1})\big] + 1 = \\ = & 2^m - 2^{m-\mathrm{gr}(f)} - 1.\end{aligned}$$

De laatste ongelijkheid toont aan dat gelijkheid alleen wordt aangenomen als V vereniging van $\mathrm{gr}(f)$ onafhankelijke hypervlakken is. $\square$

(1.11) Gevolg. *De minimumafstand van $\mathcal{R}(r,m)$ is 2^{m-r} en de woorden van minimumgewicht in $\mathcal{R}(r,m)$ corresponderen met $f \in R_m$ die te schrijven zijn als product van r onafhankelijke lineaire factoren.*

Bewijs. Uit Stelling (1.10) volgt voor $c_f \in \mathcal{R}(r,m) - \{0\}$ met $f \in R_m$ van graad $\leq r$ dat

$$w(c_f) \geq 2^m - (2^m - 2^{m-\mathrm{gr}(f)}) \geq 2^{m-r}$$

terwijl $w(c_{X_1 \cdots X_r}) = 2^{m-r}$. Tevens volgt uit Stelling (1.10) dat een woord van minimumgewicht in $\mathcal{R}(r,m)$ afkomstig is van $f \in R_m$ met $\mathrm{gr}(f) = r$ en $V(f) = \cup_{i=1}^{r} H_i$, waarin $\{H_i\}$ een collectie onafhankelijke hypervlakken is gedefinieerd door onafhankelijke lineaire h_i. In R_m geldt dan $f = \prod_{i=1}^{r} h_i$. $\square$

§2 *Democratisch decoderen ("Majority logic decoderen").*

Deze decodeermethode, die zeer efficiënt is, wordt gebruikt bij Reed-Muller codes. Alvorens in te gaan op de specifieke situatie bij Reed-Muller codes bekijken we deze decodeermethode eerst in het algemeen. Zij C een (n,k,d)-code over $\mathbb{F}_q$. Elk element $c \neq 0 \in C^{\perp}$ bepaalt een toetssom (parity check som): als $c = (c_1, ..., c_n) \in C^{\perp}$ en $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$ dan hoort bij c de toetssom

$$(c,y) = c_1 y_1 + c_2 y_2 + ... + c_n y_n.$$

Als $x \in C$ wordt uitgezonden en y wordt ontvangen dan $y = x + e$ zodat $(c,y) = (c,e)$ dus $c_1 y_1 + ... + c_n y_n = c_1 e_1 + ... + c_n e_n$. Een toetssom levert dus een controle op de fouten. Het aantal toetssommen is q^{n-k}. Bij democratisch decoderen gaat het erom een zo gunstig mogelijke collectie toetssommen te kiezen.

(2.1) Definitie. Een collectie toetssommen $(c^{(i)}, y) = (c^{(i)}, e)$ met $i = 1, 2, ..., J$ heet *orthogonaal op de j-de positie* (of op e_j) als
i) de coëfficiënt van e_j is 1 in elke som,
ii) de coëfficiënt van $e_k (k \neq j)$ is $\neq 0$ in hoogstens één som.

Veronderstel nu dat we J toetssommen hebben die orthogonaal zijn op e_1 en neem verder aan dat er in de ontvangen y hoogstens $[J/2]$ fouten zitten.
i) Als $e_1 = \alpha \neq 0$ dan komen de bij de fouten horende $e_i (i \neq 1)$ in hoogstens $[J/2] - 1$ sommen voor. Er zijn dus minstens $[J/2] + 1$ sommen waarvan de waarde $e_1 = \alpha$ is. Een echte meerderheid van de waarden der sommen is $\alpha = e_1$.
ii) Als $e_1 = 0$ dan komen de bij de fouten horende e_i in hoogstens $[J/2]$ sommen voor, dus minstens $J - [J/2]$ sommen leveren $0 = e_1$ op. Ook dit is weer een echte meerderheid, behalve als J even is, dan kan er een gelijkspel optreden.

(2.2) Decodeerregel. Als hoogstens $[J/2]$ fouten zijn opgetreden dan is e_1 de waarde van de (echte) meerderheid van de sommen; bij gelijke stand decoderen we $e_1 = 0$.

Als er per positie J toetssommen bestaan die orthogonaal zijn op die positie dan kunnen we op deze manier $\leq [J/2]$ fouten corrigeren. Deze decodeermethode heet *1-traps democratisch decoderen.* Als $J \approx d - 1$ verliest men niet al te veel van het corrigerend vermogen van de code bij gebruik van deze decodeermethode. Als $J = d - 1$ dan heet C *volledig 1-traps orthogonaliseerbaar.* Merk nog op dat bij cyclische codes

een orthogonale collectie op één positie door successieve verschuiving een orthogonale collectie op alle posities levert.

Voorbeeld. De binaire $(15, 7, 5)$-BCH code met generatorpolynoom $g(X) = X^8 + X^7 + X^6 + X^4 + 1$ heeft de volgende collectie toetssommen die orthogonaal is op de laatste positie:

$$\begin{array}{cccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} .$$

Deze code is volledig orthogonaliseerbaar.

(2.3) Stelling. *Voor het aantal fouten t dat door middel van 1-traps democratisch decoderen kan worden gecorrigeerd geldt $t \leq (n-1)/2(d(C^\perp) - 1)$.*

Bewijs. De coëfficiëntenvector van een toetssom uit een stelsel dat orthogonaal is op de eerste positie is van de vorm

$$(1,\ \text{coördinaten}\ \neq 0,\ \ \text{coördinaten}\ = 0)\ \in C^\perp.$$

Op minstens $(d(C^\perp) - 1)$ posities staan er coëfficiënten $\neq 0$ die in de overige sommen op die posities nul moeten zijn. Dus $J \leq (n-1)/(d(C^\perp) - 1)$ zodat voor het aantal fouten t dat gecorrigeerd kan worden geldt $t \leq [J/2] \leq (n-1)/2(d(C^\perp) - 1)$. $\square$

Men kan de beschreven decodeermethode verfijnen tot L-traps democratisch decoderen.

(2.4) Definitie. Een collectie van J toetssommen heet *orthogonaal op de verzameling posities* $P = \{i_1, i_2, ..., i_M\}$ als
i) $e_{i_1} + e_{i_2} + ... + e_{i_M}$ optreedt in elke som uit de collectie,
ii) voor e_{i_j} met $i_j \notin P$ treedt e_{i_j} met coëfficiënt $\neq 0$ op in hoogstens één som.

Bij $t \leq [J/2]$ fouten kan uit deze collectie de waarde van $e_{i_1} + e_{i_2} + ... + e_{i_M}$ worden bepaald. Deze uitdrukking doet dan dienst als extra toetssom en kan in combinatie met de overige toetssommen worden gebruikt bij het verder decoderen.

Veronderstel nu dat men een aantal verzamelingen posities $P_1^{(1)}, P_1^{(2)}...$ heeft en voor elk van deze een orthogonaal stelsel van J toetssommen. Via democratisch decoderen volgen de waarden van de toetssommen $S(P_1^{(1)}), S(P_1^{(2)}), ...$. Zoek nu kleinere verzamelingen posities $P_2^{(1)}, P_2^{(2)}, ...$ waarvoor de nieuwe en de oude toetssommen orthogonale stelsels van J sommen leveren. Nu ontstaan weer nieuwe toetssommen $S(P_2^{(1)}), S(P_2^{(2)}), ...$ enz. Dit proces van het bepalen van steeds kleinere sommen van fouten heet *orthogonaliseren van de code* C.

Als na L stappen op deze wijze per e_i orthogonale stelsels van J toetssommen zijn ontstaan dan heet de code *L-traps orthogonaliseerbaar* en kunnen $\leq [J/2]$ fouten door herhaald democratisch decoderen worden bepaald. We spreken dan van *L-traps democratisch decoderen.*

(2.5) Stelling. *Voor het aantal fouten t dat door middel van L-traps democratisch decoderen kan worden gecorrigeerd geldt $t \leq n/d(C^{\perp}) - 1/2$.*

Bewijs. Ga uit van een collectie van J toetssommen, orthogonaal op de posities $P = \{i_1, i_2, ..., i_M\}$. Hoogstens één van de sommen verbruikt buiten de posities van P minder dan $d(C^{\perp})/2$ plaatsen. Het aantal sommen moet dan i.v.m. het aantal beschikbare plaatsen voldoen aan: $(J-1)d(C^{\perp})/2 + d(C^{\perp}) \leq n$. Hieruit volgt voor het aantal fouten t dat gecorrigeerd kan worden $t \leq [J/2] \leq J/2 \leq n/d(C^{\perp}) - 1/2$. □

§3 *Democratisch decoderen van Reed-Muller-codes.*

Bij codes die orthogonaliseerbaar zijn is de constructie van de orthogonale stelsels meestal gebaseerd op de meetkundige structuur van de betreffende codes. In het decodeerprocédé van Reed-Muller-codes gebruiken we het volgende feit uit de eindige meetkunde.

(3.1) Eigenschap. *Als W een r-dimensionale affiene deelruimte is van $\mathbb{F}_2^m$ dan zijn er $2^{m-r} - 1$ affiene deelruimten van dimensie $r+1$ die W omvatten.*

Bewijs. We kunnen aannemen dat W een r-dimensionale lineaire deelruimte is van $\mathbb{F}_2^m$. Een $(r+1)$-dimensionale deelruimte W' om W, wordt bepaald door een punt a buiten W : $W' = W \cup (a + W)$, terwijl 2^r punten buiten W dezelfde W' bepalen. Het aantal W' is dus: $(2^m - 2^r)/2^r = 2^{m-r} - 1$. □

(3.2) Stelling. *De Reed-Muller code $\mathcal{R}(r, m)$ is $(r+1)$-traps orthogonaliseerbaar waarbij alle patronen van hoogstens $2^{m-r-1} - 1$ fouten kunnen worden gecorrigeerd.*

Bewijs. De code $\mathcal{R}(m-r-1, m)$ bevat alle $(r+1)$-dimensionale affiene deelruimten van $\mathbb{F}_2^m$. Elk van hen levert een toetssom voor $\mathcal{R}(r, m)$ want $\mathcal{R}(m-r-1,\ m) = \mathcal{R}(r, m)^{\perp}$. Neem een r-dimensionale affiene deelruimte W. Voor de $2^{m-r}-1$ affiene deelruimten van dimensie $r+1$ om W geldt dat elk punt $\notin W$ tot precies één zo een $(r+1)$-dimensionale affiene deelruimte behoort. Deze leveren dus een stelsel van $J = 2^{m-r} - 1$ toetssommen dat orthogonaal is op de bij W horende 2^r posities. Dus bij $t \leq [J/2]$ fouten kan men voor alle r-dimensionale affiene deelruimten W de toetssom $\sum_{p \in W} e_p$ bepalen.

Neem nu een $(r-1)$-dimensionale affiene deelruimte Z. Deze wordt omvat door $2^{m-r+1} - 1$ affiene deelruimten W van dimensie r waarvoor $\sum_{p \in W} e_p$ bekend is. Op dezelfde wijze als boven heeft men zo $2^{m-r+1} - 1 (> J)$ toetssommen, orthogonaal op de bij Z horende 2^{r-1} posities. Hieruit volgt $\sum_{p \in Z} e_p$ voor alle $(r-1)$-dimensionale affiene deelruimten Z.

Na $r+1$ stappen komt men zo op meer dan J toetssommen, orthogonaal op 0-dimensionale affiene deelruimten (d.w.z. punten) waaruit de e_p zelf kunnen worden bepaald. Via $(r+1)$-traps democratisch decoderen kunnen zo $t \leq [J/2] = 2^{m-r-1} - 1 = [(d(\mathcal{R}(r, m)) - 1)/2]$ fouten worden gecorrigeerd. □

Opgaven bij Hoofdstuk VI

1. Geef een generatormatrix en een toetsmatrix voor $\mathcal{R}(1,4)$ en voor $\mathcal{R}(2,4)$.
2. Bewijs dat $\mathcal{R}(r+1,\ m+1) = \{(u|u+v)|u \in \mathcal{R}(r+1,m) \text{ en } v \in \mathcal{R}(r,m)\}$.
3. Bepaal de gewichtsverdeling van $\mathcal{R}(0,m), \mathcal{R}(1,m), \mathcal{R}(m-2,m), \mathcal{R}(m-1,m)$ en $\mathcal{R}(m,m)$.
4. Toon aan dat $\mathcal{R}(m-2,m)$ de uitgebreide $(n, n-m-1)$-Hamming code is.
5. i) Bewijs dat de groep van de affiene transformaties van $\mathbb{F}_2^m$ bevat is in de groep $\mathrm{Aut}(\mathcal{R}(r,m))$.
   ii) Bewijs dat $\mathrm{Aut}(\mathcal{R}(r,m) = S_{2^m}$ (de symmetrische groep op 2^m elementen) voor $r = 0, m-1, m$.
6. i) Zij $\mathcal{R}(r,m)^*$ de code die ontstaat door $\mathcal{R}(r,m)$ te puncteren op de plaats die correspondeert met de coördinatenoorsprong van $\mathbb{F}_{2^m}$. Bewijs dat $\mathcal{R}(r,m)^*$ cyclisch is.
   ii) Bewijs dat een code die ontstaat door $\mathcal{R}(r,m)$ te puncteren equivalent is met een cyclische code.
7. Geef een stelsel van 3 toetssommen van de binaire $(7,3,4)$-simplex code dat orthogonaal is op de eerste positie.
8. Beschrijf een volledig 2-traps democratisch decodeerprocédé voor $\mathcal{R}(1,3)$.
9. Bewijs dat een (n,d) RS-code met $2 < d < n$ niet volledig 1-traps democratisch decodeerbaar is.

Hoofdstuk VII. Goppa Codes

Omstreeks 1980 stuitte V. Goppa bij zijn pogingen tot generalisatie van de constructie van klassieke codes, zoals de Reed-Solomon codes, BCH-codes en de rond 1970 door hem ontdekte klassieke Goppa codes, op algebraïsch meetkundige methoden om codes te maken. De klassieke codes worden dan verkregen door rationale functies op de affiene (of projectieve) lijn te evalueren of residuen van zogenaamde differentiaalvormen te nemen. Het algemene geval gebruikt in plaats van de projectieve lijn, waarvan het zogeheten geslacht nul is, ook krommen van hoger geslacht. Daarmee zijn krachtige methoden uit de algebraïsche meetkunde ter beschikking van de coderingstheorie gekomen. Dit heeft geleid tot opmerkelijke resultaten.

Wij beschrijven eerst de constructies voor de projectieve rechte en bestuderen dan de klassieke Goppa codes vanuit dit nieuwe gezichtspunt.

§1. *Meetkundige Goppa codes op de projectieve rechte.*

We beschouwen de affiene en de projectieve lijn $\mathbb{A}^1 = \mathbb{A}^1_{\mathbb{F}_p}$ en $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_p}$ over $\mathbb{F}_p$. We vatten het symbool $\mathbb{A}^1$ op als een voorschrift dat aan ieder uitbreidingslichaam k van $\mathbb{F}_p$ de verzameling $\mathbb{A}^1(k) = k$ toevoegt. Zo ook beschouwen we $\mathbb{P}^1$ als een voorschrift dat aan k de verzameling

$$\mathbb{P}^1(k) = \{(x_0, x_1) \in k \times k : (x_0, x_1) \neq (0,0)\}/\sim,$$

toevoegt, waar de equivalentierelatie $\sim$ gegeven is door

$$(x_0, x_1) \sim (\lambda x_0, \lambda x_1) \qquad \text{voor alle } \lambda \in k, \lambda \neq 0.$$

De equivalentieklasse van $(x_0, x_1) \neq (0,0)$ wordt genoteerd met $(x_0 : x_1)$. We kunnen $\mathbb{A}^1(k)$ opvatten als deelverzameling van $\mathbb{P}^1(k)$ via:

$$\mathbb{A}^1(k) = k \overset{1-1}{\longleftrightarrow} \{(x : 1) \in \mathbb{P}^1(k)\} = \mathbb{P}^1(k) - (1 : 0).$$

Het punt $(1 : 0)$ noemen we het punt op oneindig in $\mathbb{P}^1(k)$ en wordt genoteerd P_∞. Als $k_1 \subseteq k_2$ dan hebben we een natuurlijke inclusie $\mathbb{P}^1(k_1) \subseteq \mathbb{P}^1(k_2)$.

De polynoomring $\mathbb{F}_p[X]$ en het quotiëntenlichaam $\mathbb{F}_p(X)$ van $\mathbb{F}_p[X]$ (en algemener $k[X]$ en $k(X)$) zullen een belangrijke rol spelen in het vervolg.

Een matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, k)$$

definieert een automorfisme van $k(X)$ via $X \mapsto (aX + b)/(cX + d)$ en een bijectie van $\mathbb{P}^1(k)$ op zichzelf via:

$$(x_0 : x_1) \mapsto (ax_0 + bx_1 : cx_0 + dx_1).$$

De elementen van $\mathbb{F}_p[X]$ (resp. van $k[X]$) definiëren functies $\mathbb{A}^1(\mathbb{F}_p) \to \mathbb{F}_p$ (resp. $\mathbb{A}^1(k) \to k$) via $\alpha \mapsto f(\alpha)$.

Rationale functies f/g met $f, g \in k[X]$ en $g \neq 0 \in k[X]$ definiëren functies op $\mathbb{A}^1(k) - S$ met $S = \{\alpha \in k : g(\alpha) = 0\}$.

Aan een punt $\alpha \in \mathbb{A}^1(k)$ kunnen we een *discrete valuatie* op het lichaam $k(X)$ toevoegen die triviaal is op k. Dat is een surjectief homomorfisme

$$v : k(X)^* \to \mathbb{Z}$$

met de eigenschap dat

$$v(f+g) \geq \min(v(f), v(g))$$

en $v(c) = 0$ voor elke $c \in k^*$. We doen dit als volgt: het ideaal $(X-\alpha)$ van $k[X]$ is een hoofdideaal en tegelijk een maximaal ideaal (want het quotient $k[X]/(X-\alpha) \cong k$ is een lichaam). Dit betekent dat $X-\alpha$ een priemelement is en dat ieder element $f \in k[X]$ geschreven kan worden als $f = (X-\alpha)^m g$, waarbij $g \in k[X]$ niet door $X-\alpha$ deelbaar is. Definiëren we nu v voor een polynoom f als $v(f) = m$ en voor een quotiënt $f = f_1/f_2$ met $f_1, f_2 \in k[X], f_2 \neq 0$ als $v(f_1/f_2) = v(f_1) - v(f_2)$ dan levert dit een discrete valuatie op. Een punt van $\mathbb{A}^1(k) \subset \mathbb{P}^1(k)$ bepaalt zo een discrete valuatie. Ook het punt $P_\infty \in \mathbb{P}^1(k)$ bepaalt een discrete valuatie op $k(X)$ als we definiëren $v(f_1/f_2) = -\text{graad}(f_1/f_2) = \text{gr}(f_2) - \text{gr}(f_1)$. Dit komt overeen met de eerdere definitie in de zin dat X een enkelvoudige pool heeft in P_∞.

Op deze manier levert dus elk punt $P \in \mathbb{P}^1(k)$ (corresponderend met $\alpha \in k$ of met P_∞) een discrete valuatie op $k(X)$, die we noteren als $f \mapsto \text{ord}_P(f)$. Als $\text{ord}_P(f) \geq 0$ (resp. als $\text{ord}_P(f) < 0$) kunnen we $\text{ord}_P(f)$ opvatten als de multipliciteit waarmee $f \in k(X)$ een nulpunt (resp. een pool) in P heeft.

Als $\text{ord}_{P_\infty}(f_1/f_2) = 0$ definiëren we $(f_1/f_2)(P_\infty) =$ kopcoëfficiënt van f_1 / kopcoëfficiënt van f_2.

Laat nu $K = \overline{\mathbb{F}}_p$ een algebraische afsluiting van $\mathbb{F}_p$ zijn, bijv. $K = \cup_{n=1}^{\infty} \mathbb{F}_{p^n}$. Op K werkt een lichaamsautomorfisme $F : \alpha \mapsto \alpha^p$. De vaste punten van F^j zijn

$$\{\alpha \in K : \alpha^{p^j} = \alpha\}$$

en vormen precies het lichaam $\mathbb{F}_{p^j}$. Omdat $\mathbb{A}^1(K) = K$ levert F een bijectie van $\mathbb{A}^1(K)$. We kunnen dit uitbreiden tot een bijectie van $\mathbb{P}^1(K)$ met $F(P_\infty) = P_\infty$.

(1.1) Definitie. Een *divisor* D op $\mathbb{P}^1$ is een formele som

$$D = \sum_{P \in \mathbb{P}^1(K)} n_P P, \qquad n_P \in \mathbb{Z}, \quad n_P = 0 \text{ voor bijna alle } P.$$

Met andere woorden zo een divisor is een eindige formele som van punten P van $\mathbb{P}^1(K)$ met multipliciteiten n_P. We definiëren de *graad van* D als $\sum_P n_P$. We zeggen dat de divisor D *over* $\mathbb{F}_{p^j}$ *gedefinieerd is* als $F^j(D) = D$.

Voorbeeld. We beschouwen $\mathbb{P}^1_{\mathbb{F}_2}$. Voor $\alpha \in \mathbb{F}_4 - \mathbb{F}_2$ is de divisor $P+Q$ met $P = (\alpha : 1)$ en $Q = (\alpha^2 : 1)$ gedefinieerd over $\mathbb{F}_2$.

Een element $f \in K(X), f \neq 0$ definieert een divisor (f) op $\mathbb{P}^1$ als volgt:

$$(f) = \sum_{P \in \mathbb{P}^1(K)} \text{ord}_P(f) P.$$

We kunnen dit opvatten als de formele som van de nulpunten minus de som van de polen van f (geteld met multipliciteiten). Als we f in $K(X)$ in lineaire factoren ontbinden

$$f = \frac{\prod_{i=1}^{s}(X-\alpha_i)}{\prod_{j=1}^{t}(X-\beta_j)}$$

met $\alpha_i, \beta_j \in K$ dan geldt

$$(f) = \sum \alpha_i - \sum \beta_j + (t-s)P_\infty. \tag{1}$$

Als $f \in k(X)$ dan is de divisor (f) van f over k gedefinieerd.

(1.2) Lemma. *De graad van de divisor (f) van een rationale functie f op $\mathbb{P}^1$ is nul.*

Bewijs. Dit volgt direct uit (1): $\mathrm{gr}((f)) = s - t + (t-s) = 0$. $\square$

Laat $D = \sum_P n_P P$ een divisor zijn. We zeggen dat D *effektief* is als voor alle coëfficiënten n_P geldt $n_P \geq 0$. Notatie: $D \geq 0$. Voor twee divisoren D_1 en D_2 schrijven we $D_1 \geq D_2$ dan en slechts dan als $D_1 - D_2 \geq 0$.

We beschouwen nu een divisor $D = \sum n_P P$ op $\mathbb{P}^1$ gedefinieerd over k en definiëren een k-vectorruimte

$$L(D) = \{f \in k(X)^* : (f) + D \geq 0\} \cup \{0\}.$$

Opmerking. De conditie in de definitie zegt dus dat we voor alle $P \in \mathbb{P}^1(K)$ de conditie

$$\mathrm{ord}_P(f) + n_P \geq 0$$

moeten controleren, en niet alleen voor de punten $P \in \mathbb{P}^1(k)$.

Als we $D = \sum n_i P_i - \sum m_j Q_j$ schrijven als verschil van positieve divisoren (dwz. $n_i > 0, m_i > 0$ en $P_i \neq Q_j$) dan bestaat $L(D)$ uit de functies die in Q_j een nulpunt van orde tenminste m_j hebben en in P_i een pool van orde hoogstens n_i.

(1.3) Lemma. *De verzameling $L(D)$ is een k-deelvectorruimte van $k(X)$.*

Bewijs. Er geldt $(cf) = (f)$ voor alle $c \neq 0$ in k. Verder geldt voor alle $P \in \mathbb{P}^1(K)$ dat $\mathrm{ord}_P(f+g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}$, dus als $f, g \in L(D)$ dan ook $f + g \in L(D)$. $\square$

(1.4) Lemma. *Zij D een divisor op $\mathbb{P}^1$ gedefinieerd over k. Als $\mathrm{gr}(D) < 0$ dan geldt $L(D) = \{0\}$. Als $\mathrm{gr}(D) \geq 0$ dan geldt $\dim_k(L(D)) = \mathrm{gr}(D) + 1$.*

Bewijs. Laat $f \in L(D)$ met $f \neq 0$. Dan geldt $(f) + D \geq 0$. Dit impliceert dat $\mathrm{gr}((f)) + \mathrm{gr}(D) \geq 0$. Maar aangezien $\mathrm{gr}((f)) = 0$ betekent dit dat $\mathrm{gr}(D) \geq 0$.

Neem nu aan dat $\mathrm{gr}(D) \geq 0$. Laat dan $D = \sum \alpha_i - \sum \beta_j + tP_\infty$. Neem een element $f \in L(D)$. Dan moet

$$g = f \cdot \prod (X - \alpha_i) \in k[X]$$

nulpunten hebben in β_j, dus $\prod(X - \beta_j) \in k[X]$ deelt g. Dan is f van de vorm

$$f = \frac{\prod(X-\beta_j)}{\prod(X-\alpha_i)} h \tag{2}$$

met $h \in k[X]$. Verder moet $\mathrm{ord}_{P_\infty}(f) + t \geq 0$. Dit betekent $\mathrm{gr}(h) \leq \mathrm{gr}(D)$ zodat h in de $d+1$-dimensionale k-vectorruimte van polynomen van graad $\leq d = \mathrm{gr}(D)$ in $k[X]$ moet liggen. Omgekeerd, ieder element van de vorm (2) met h in de zojuist aangegeven k-vectorruimte van polynomen ligt in $L(D)$. $\square$

We gaan nu de meetkundige Goppa codes of kortweg meetkundige codes definiëren. We kiezen een lichaam $k = \mathbb{F}_q$ en fixeren dit. Neem verschillende punten $P_1, \ldots, P_n \in \mathbb{P}^1(k)$ en stel $D = \sum_{i=1}^n P_i$. Verder kiezen we een divisor G die gedefinieerd is over k met $\mathrm{drager}(G) \cap \mathrm{drager}(D) = \emptyset$ (dwz. de coëfficiënt van P_i in G is nul). Dan hebben de functies $f \in L(G)$ geen pool in P_i $(i = 1, \ldots, n)$ zodat voor elke $f \in L(G)$ en elk punt P_i de waarde $f(P_i) \in \mathbb{F}_q$ welgedefinieerd is.

(1.5) Definitie. De meetkundige code $C(D, G)$ over $\mathbb{F}_q$ is de lineaire code

$$C(D, G) = \{c_f = (f(P_1), \ldots, f(P_n)) : f \in L(G)\} \subseteq \mathbb{F}_q^n.$$

Voorbeeld. Neem $k = \mathbb{F}_q$, $D = \sum_{P \in \mathbb{F}_q^*} P$ en $G = sP_\infty$ met $1 \leq s \leq q-1$. Nu geldt

$$L(G) = \{f \in \mathbb{F}_q[X] : \mathrm{gr}(f) \leq s\}$$

en $C(D, G)$ is de Reed-Solomon code over $\mathbb{F}_q$ van lengte $q-1$ en ontwerpafstand $\delta = q - 1 - s$. Dus $C(D, G)$ is een $(q-1, s+1, q-1-s)$-code (zie Hfdstk. IV, §2).

(1.6) Stelling. *Voor de code $C(D, G)$ geldt:*

i) $C(D, G) \cong L(G)/L(G - D)$,
ii) als $0 \leq \mathrm{gr}(G) < n$ dan $\dim_k(C(D, G)) = \mathrm{gr}(G) + 1$,
iii) de minimumafstand voldoet aan $d(C(D, G)) \geq n - \mathrm{gr}(G)$ als $\mathrm{gr}(G) \geq 0$.

Bewijs. Beschouw de surjectieve lineaire afbeelding

$$\phi : L(G) \to C(D, G), \quad f \mapsto c_f = (f(P_1), \ldots, f(P_n)).$$

De kern bestaat uit de functies $f \in L(G)$ met $f(P_i) = 0$ voor $i = 1, \ldots, n$ zodat $\ker(\phi) = L(G - D)$. Dit bewijst i). Voor het bewijs van ii) merken we op dat uit $\mathrm{gr}(G - D) < 0$ volgt $\dim_k(L(G - D)) = 0$ zodat $\dim_k(C(D, G)) = \dim_k(L(G))$. Nu volgt ii) uit (1.4). Voor iii) nemen we een $c_f \neq 0$ in $C(D, G)$. Stel het gewicht van c_f is w. Dan heeft $f \in L(G)$ in de punten P_i precies $n - w$ nulpunten, zeg $P_1, \ldots, P_{n-w}$. Voor de divisor (f) van f geldt dan

$$(f) \geq P_1 + \ldots P_{n-w} - G.$$

Nemen we de graad van beide divisoren in deze ongelijkheid dan vinden we

$$0 \geq n - w - \mathrm{gr}(G), \quad \text{i.e. } w \geq n - \mathrm{gr}(G).$$

Dit bewijst iii). $\square$

Naast rationale functies (elementen van $k(X)$) kunnen we ook rationale differentiaalvormen op $\mathbb{P}^1$ beschouwen. Dit zijn uitdrukkingen van de vorm $\omega = f dX$ met $f \in k(X)$. Deze vormen een k-vectorruimte Ω_k (via $f dX + g dX = (f+g) dX$ en

$c(fdX) = (cf)dX$ voor $c \in k$). We definiëren de divisor van een differentiaalvorm als volgt:

(1.7) Definitie. De divisor van de differentiaalvorm $\omega = fdX \in \Omega_k$ is

$$(\omega) = (f) - 2P_\infty. \tag{3}$$

Dus in het bizonder $(dX) = -2P_\infty$. Dit wordt gemotiveerd door over te gaan op $1/X$. Volgens de bekende rekenregels geldt dan $d(1/X) = -(1/X^2)dX$ zodat $dX = -X^2 d(1/X)$ een tweevoudige pool in P_∞ heeft. [Wij hebben dit feit niet nodig, we definiëren gewoon de divisor van een differentiaal met (3).]

We stellen nu

$$\Omega_k(D) = \{\omega \in \Omega_k : (\omega) - D \geq 0\} \cup \{0\}.$$

Dit is weer een k-vectorruimte.

(1.8) Lemma. *Er geldt* $\Omega_k(D) \cong L(-D - 2P_\infty)$ *en* $\dim_k(L(D)) - \dim_k(\Omega_k(D)) = \mathrm{gr}(D) + 1$.

Bewijs. De afbeelding gegeven door $fdX \mapsto f$ is een isomorfisme tussen de k-vectorruimten $\Omega_k(D)$ en $L(-D - 2P_\infty)$. De linkerkant van de gegeven formule is in verband met het isomorfisme gelijk aan

$$\dim_k(L(D)) - \dim_k(L(-2P_\infty - D))$$

en dit is op grond van (1.4) gelijk aan $\mathrm{gr}(D) + 1$. □

We definiëren nu voor een rationale differentiaalvorm het residu in een punt. Laat $\omega = fdX \in \Omega_k$. Voor een punt $\alpha \in \mathbb{A}^1(k)$ kunnen we f in een Taylorreeks ontwikkelen:

$$f = \frac{c_{-n}}{(X-\alpha)^n} + \ldots + \frac{c_{-1}}{(X-\alpha)} + c_0 + c_1(X-\alpha) + \ldots$$

waaarin $-n = \mathrm{ord}_{P=\alpha}(f)$. We definiëren dan het residu van ω in $P = \alpha$ als

$$\mathrm{res}_P(\omega) = c_{-1}.$$

Voor $P = P_\infty$ gaan we over op de nieuwe variabele $U = 1/X$ en schrijven we $f(X)$ als Taylorreeks $g(U)$ in U

$$g(U) = c_{-n}U^{-n} + \ldots + c_0 + c_1 U + \ldots.$$

We definiëren nu

$$\mathrm{res}_{P_\infty}(\omega) = -c_1.$$

Dit wordt weer gemotiveerd door de formele manipulatie

$$fdX = -g(U)dU/U^2.$$

Ook met behulp van differentiaalvormen kan men meetkundige codes definiëren over $k = \mathbb{F}_q$. We nemen divisoren D en G als in Definitie (1.5) .

(1.9) Definitie. De meetkundige code $C^*(D,G)$ is de code

$$C^*(D,G) = \{c_\omega = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) : \omega \in \Omega_k(G-D)\} \subseteq \mathbb{F}_q^n.$$

(1.10) Stelling. *Voor de code $C^*(D,G)$ geldt:*

i) $C^*(D,G) \cong \Omega_k(G-D)/\Omega_k(G)$,
ii) als $-2 < \mathrm{gr}(G) < n$ dan $\dim_k(C^*(D,G)) = n - 1 - \mathrm{gr}(G)$,
iii) de minimumafstand van $C^*(D,G)$ voldoet aan $d(C^*(D,G)) \geq \mathrm{gr}(G) + 2$ als $\mathrm{gr}(G) \leq n-2$.

Bewijs. i) De lineaire afbeelding $\phi : \Omega_k(G-D) \to C^*(D,G)$ gegeven door $\omega \mapsto c_\omega$ is surjectief en heeft als kern de ruimte van differentiaalvormen in $\Omega_k(G-D)$ die geen pool hebben in de punten P_i. Dit betekent $\ker(\phi) = \Omega_k(G)$. ii) Merk op dat $\ker(\phi) = \Omega_k(G) = L(-G-2P_\infty) = 0$ als $\mathrm{gr}(G) > -2$. De dimensie volgt nu uit de formule in (1.8). iii) Stel het gewicht van c_ω is w. Dan heeft $\omega \in \Omega_k(G-D)$ een residu $\neq 0$ in w punten P_i, zeg $P_1, \ldots, P_w$, zodat

$$(\omega) + P_1 + \ldots + P_w \geq G.$$

Nemen we van beide zijden de graad dan krijgen we

$$-2 + w \geq \mathrm{gr}(G).$$

□

(1.11) Stelling. *De codes $C(D,G)$ en $C^*(D,G)$ zijn elkaars duale: $C^*(D,G) = (C(D,G))^\perp$.*

Bewijs. We bewijzen eerst dat $C(D,G)$ en $C^*(D,G)$ orthogonaal zijn. Neem een element $c_f \in C(D,G)$ en een element $d_\omega \in C^*(D,G)$. Dan geldt

$$(f\omega) = (f) + (\omega) \geq -G + G - D = -D,$$

dus kan de rationale differentiaalvorm $f\omega$ alleen (enkelvoudige) polen in punten P_i hebben. Nu geldt

$$\sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\omega) = \sum_{P \in \mathbb{P}^1(K)} \mathrm{res}_P(f\omega) = 0$$

vanwege de residuenstelling (zie het Lemma hierna) zodat $C^*(D,G) \subseteq C(D,G)^\perp$. Op grond van (1.6.i), (1.8) en (1.10.i) geldt

$$\dim(C(D,G)) + \dim(C^*(D,G)) = n,$$

daarom volgt $C(D,G) = C^*(D,G)^\perp$. □

In het volgende gebruiken we de interpolatieformule van Lagrange (1736-1813). Deze formule levert een oplossing voor het probleem een polynoom $f \in K[X]$ te vinden van

graad $\leq n-1$ dat in n verschillende punten $\alpha_1, \ldots, \alpha_n$ van K voorgeschreven waarden $f(\alpha_1), \ldots, f(\alpha_n)$ heeft. De oplossing van Lagrange is:

$$f = \sum_{i=1}^{n} f(\alpha_i) \frac{\prod_{j=1, j\neq i}^{n} (X - \alpha_j)}{\prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j)}. \tag{4}$$

(Het bewijs van de formule volgt door op te merken dat beide kanten polynomen geven van graad $\leq n-1$ die dezelfde waarde in de n punten α_i voor $i = 1, \ldots, n$ aannemen.)

Als we stellen $F(X) = \prod_{j=1}^{n} (X - \alpha_j)$ dan kunnen we (4) ook schrijven

$$f = \sum_{i=1}^{n} \frac{F(X)}{X - \alpha_i} \cdot \frac{f(\alpha_i)}{F'(\alpha_i)}. \tag{5}$$

Een gevolg van (5) is de formule van Euler (1707-1783):

$$\sum_{i=1}^{n} \frac{f(\alpha_i)}{F'(\alpha_i)} = 0 \qquad \text{als } \operatorname{gr}(f) \leq n-2.$$

(Orden het rechterlid van (5) naar machten van X en bekijk de coëfficiënt van X^{n-1}.)

(1.12) Lemma. *Zij $\omega = f dX$ een rationale differentiaalvorm op $\mathbb{P}^1$ die alleen polen heeft in de n punten $P_i \in \mathbb{P}^1(K)$ en wel met orde ≤ 1. Dan geldt*

$$\sum_{i=1}^{n} \operatorname{res}_{P_i}(\omega) = 0.$$

Bewijs. Na eventueel toepassen van een automorfisme van $K(X)$ mogen we aannemen dat geen der P_i gelijk is aan P_∞. Dus nemen we aan dat $P_i = (\alpha_i : 1)$ met $\alpha_i \in K$. We kunnen ω schrijven als

$$\omega = \frac{g}{\prod_{j=1}^{n} (X - \alpha_j)} dX = \frac{g}{F} dX$$

met $g \in K[X]$ van graad $\leq n-2$. Het residu in een punt α_i is dan

$$\operatorname{res}_{P_i = \alpha_i}(\omega) = \frac{g(\alpha_i)}{\prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j)} = \frac{g(\alpha_i)}{F'(\alpha_i)}.$$

Uit de formule van Euler volgt nu

$$\sum_{i=1}^{n} \operatorname{res}_{P_i}(\omega) = \sum_{i=1}^{n} \frac{g(\alpha_i)}{F'(\alpha_i)} = 0. \qquad \square$$

Opmerking. Algemener geldt de stelling dat de som van de residuen van een rationale differentiaalvorm op $\mathbb{P}^1$ gelijk is aan 0 ('residuenstelling').

§2 *Klassieke Goppa codes*

Deze codes werden omstreeks 1970 door Goppa geconstrueerd als generalisatie van BCH-codes. Behalve dat Goppa codes zich efficiënt laten decoderen, hebben ze de interessante eigenschap dat er asymptotisch goede rijen Goppa codes zijn over $\mathbb{F}_q$. Dat wil zeggen, er zijn rijen $(C_i)_{i=1,2,\ldots}$ van zulke Goppa codes met parameters (n_i, k_i, d_i) die voldoen aan $\lim_{i\to\infty} n_i = \infty$, $\lim_{i\to\infty} k_i/n_i > 0$ en $\lim_{i\to\infty} d_i/n_i > 0$. We zullen nu de klassieke Goppa codes definiëren via een constructie uit §1.

Neem n verschillende elementen $\gamma_1, \ldots, \gamma_n$ in $\mathbb{F}_{q^m}$. Laat P_i het punt van $\mathbb{P}^1(\mathbb{F}_{q^m})$ zijn dat gegeven wordt door $(\gamma_i : 1)$. Kies verder een polynoom $g \in \mathbb{F}_{q^m}[Z]$ met $1 \leq \mathrm{gr}(g) \leq n-1$ en $g(\gamma_i) \neq 0$ voor $i = 1, \ldots, n$. Laat

$$D = \sum_{i=1}^{n} P_i \qquad \text{en } G = (g)_0 - P_\infty.$$

Hierbij is $(g)_0$ de divisor van de nulpunten van g. Omdat alle punten P_i in D met multipliciteit 1 optreden noteren we D ook wel met $D = \{\gamma_1, \ldots, \gamma_n\}$.

(2.1) Definitie. De klassieke Goppa code $\Gamma(D, g)$ met Goppa-polynoom g is de $\mathbb{F}_q$-code $C^*(D, G) \cap \mathbb{F}_q^n$.

Uit (1.10 iii) volgt direct:

(2.2) Eigenschap. *Voor de minimumafstand d van $\Gamma(D, g)$ geldt:* $d \geq \mathrm{gr}(g) + 1$.

We beschouwen nu eerst de code $C^*(D, G)$. Laat $k = \mathbb{F}_{q^m}$. Dan kunnen we $\Omega_k(G - D)$ met behulp van (1.8) en het bewijs van (1.4) beschrijven als

$$\Omega_k(G-D) = \{\omega = \frac{hg}{\prod_{i=1}^{n}(Z-\gamma_i)} dZ : h \in k[Z], \mathrm{gr}(h) < n - \mathrm{gr}(g)\}.$$

Neem $\omega = f\,dZ$ in $\Omega_k(G - D)$. Dan schrijven we $f = hg/(\prod_{i=1}^{n}(Z - \gamma_i))$ via breuksplitsing als

$$f = \sum_{i=1}^{n} \frac{c_i}{Z - \gamma_i} \text{ met } c_i \in k \text{ zodat } \mathrm{res}_{P_i}(\omega) = c_i.$$

Een codewoord $(c_1, \ldots, c_n) \in C^*(D, G)$ correspondeert dus met de relatie in $\mathbb{F}_{q^m}(Z)$

$$\frac{hg}{\prod_{i=1}^{n}(Z-\gamma_i)} = \sum_{i=1}^{n} \frac{c_i}{Z-\gamma_i}. \tag{6}$$

Dit levert de oorspronkelijke definitie van Goppa: bij D en g als boven is $\Gamma(D, g)$ de code:

$$\{c \in \mathbb{F}_q^n : \text{ er is een } h \in \mathbb{F}_{q^m}[Z] \text{ met } \mathrm{gr}(h) < n - \mathrm{gr}(g) \text{ zodat (6) geldt}\}$$

$$= \{c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{Z-\gamma_i} = 0 \text{ in } \mathbb{F}_{q^m}[Z]/(g)\}. \tag{7}$$

Op grond van deze beschrijving kunnen we (2.2) voor binaire $\Gamma(D,g)$ in bepaalde gevallen verscherpen.

(2.3) Stelling. *Als $q=2$ en als het Goppa polynoom g geen meervoudige wortels heeft dan $d(\Gamma(D,g)) \geq 2\mathrm{gr}(g)+1$.*

Bewijs: Definieer voor $c=(c_1,...,c_n) \neq 0 \in \Gamma(D,g)$ de veelterm $f \in \mathbb{F}_{2^m}[Z]$ door $f(Z)=\prod_{i=1}^{n}(Z-\gamma_i)^{c_i}$. Omdat $f(Z)$ een eenheid is in $\mathbb{F}_{2^m}[Z]/(g(Z))$ bevat deze ring $f'(Z)/f(Z)=\sum_{i=1}^{n}(c_i/(Z-\gamma_i))$. Dus $f'/f=0$ aangezien $c \in \Gamma(D,g)$. Dit betekent $f' \equiv 0(\bmod g)$. Daar $q=2$ treden in f' slechts even machten op, zodat f' een kwadraat is in $\mathbb{F}_{2^m}[Z]$. Omdat g geen meervoudige wortels heeft volgt hieruit: $f' \equiv 0(\mathrm{mod} g^2)$. Dit betekent $2\ \mathrm{gr}(g) \leq \mathrm{gr}(f') \leq \mathrm{gr}(f)-1 = w(c)-1$. Dus $d(\Gamma(D,g)) \geq 2\mathrm{gr}(g)+1$. $\square$

Via een toetsmatrix van $C^*(D,G)$ willen we een ondergrens voor de dimensie van $\Gamma(D,g)$ bepalen. Dit is een voortbrengermatrix van $C^*(D,G)^{\perp}=C(D,G)$ met $G=(g)_0-P_\infty$. Een basis van de bijbehorende functieruimte $L(G)$ wordt gevormd door de functies Z^i/g met $0 \leq i \leq \mathrm{gr}(g)-1=t-1$. Dus $C^*(D,G)$ heeft toetsmatrix:

$$H = \begin{pmatrix} g(\gamma_1)^{-1} & g(\gamma_2)^{-1} & ... & g(\gamma_n)^{-1} \\ \gamma_1 g(\gamma_1)^{-1} & \gamma_2 g(\gamma_2)^{-1} & ... & \gamma_n g(\gamma_n)^{-1} \\ \vdots & \vdots & & \vdots \\ \gamma_1^{t-1} g(\gamma_1)^{-1} & \gamma_2^{t-1} g(\gamma_2)^{-1} & ... & \gamma_n^{t-1} g(\gamma_n)^{-1} \end{pmatrix} \tag{8}$$

(2.4) Eigenschap. *Als $\mathrm{gr}(g)=t$ dan $\dim(\Gamma(D,g)) \geq n-mt$*

Bewijs. De toetsmatrix (8) over $\mathbb{F}_{q^m}$ van rang t levert een toetsmatrix van $\Gamma(D,g)$ over $\mathbb{F}_q$ van rang $\leq mt$. $\square$

Voorbeeld. Neem $g(Z)=Z^3+Z+1 \in \mathbb{F}_{2^5}[Z]$ en $D=\{\gamma_1,\gamma_2,...,\gamma_{32}\}=\mathbb{F}_{2^5}$. De nulpunten van g zijn voortbrengers van $\mathbb{F}_{2^3}$. Omdat $3 \nmid 5$ volgt $\mathbb{F}_{2^3} \not\subset \mathbb{F}_{2^5}$ zodat $g(\gamma_i) \neq 0$. Nu

$$\Gamma(D,g)=\{c=(c_1,c_2,...,c_{32}) \in \mathbb{F}_2^{32} \Big| \sum_{\gamma_i \in \mathbb{F}_{2^5}} \frac{c_i}{Z-\gamma_i}=0 \text{ in } \mathbb{F}_{2^5}[Z]/(g)\}.$$

Uit (2.4) volgt $\dim \Gamma(D,g) \geq 32-3\cdot 5=17$ en omdat Z^3+Z+1 geen meervoudige wortels heeft volgt uit (2.3) dat $d(\Gamma(D,g)) \geq 2\cdot 3+1=7$. Neem nu $\gamma_1=0$ en $\gamma_i=\alpha^{i-2}$ voor $i=2,\ldots,32$ met α een primitieve 31^{ste}-eenheidswortel waarvoor $\alpha^5+\alpha^2+1=0$. De toetsmatrix (8) wordt nu :

$$H = \begin{pmatrix} g(0)^{-1} & g(1)^{-1} & g(\alpha)^{-1} & ... & g(\alpha^{30})^{-1} \\ 0 & g(1)^{-1} & \alpha g(\alpha)^{-1} & ... & \alpha^{30} g(\alpha^{30})^{-1} \\ 0 & g(1)^{-1} & \alpha^2 g(\alpha)^{-1} & ... & \alpha^{60} g(\alpha^{30})^{-1} \end{pmatrix}.$$

Met behulp van de tabel voor $\mathbb{F}_{32}$ wordt dit:

$$H = \begin{pmatrix} 1 & 1 & \alpha^4 & \alpha^8 & ... & \alpha^{26} \\ 0 & 1 & \alpha^5 & \alpha^{10} & ... & \alpha^{25} \\ 0 & 1 & \alpha^6 & \alpha^{12} & ... & \alpha^{24} \end{pmatrix}.$$

Er geldt: $c \in \Gamma(D,g) \Longleftrightarrow Hc^t = 0$. Door de elementen van H te schrijven als kolomvectoren t.o.v. de $\mathbb{F}_2$-basis $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ van $\mathbb{F}_{2^5}$ ontstaat een 15×32 matrix over $\mathbb{F}_2$ waarvan de rang 15 is. Dus $\dim \Gamma(D,g) = 17$. Ter controle: de vierde kolom van deze matrix is: $(101101000101110)^t$. Verder blijkt $d(\Gamma(D,g)) = 7$.

§3 *Het decoderen van klassieke Goppa codes.*

Eerst construeren we een toetsmatrix van $\Gamma(D,g)$ op basis van (7):

$$c = (c_1, \ldots, c_n) \in \Gamma(D,g) \iff \left(\frac{1}{Z-\gamma_1}, \frac{1}{Z-\gamma_2}, \ldots, \frac{1}{Z-\gamma_n} \right) \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

Omdat $g(\gamma) \neq 0$ geldt in de restklassenring $\mathbb{F}_{q^m}[Z]/(g)$:

$$\frac{1}{Z-\gamma} = -\frac{1}{g(\gamma)} \cdot \frac{g(Z)-g(\gamma)}{Z-\gamma}.$$

Als $g(Z) = \sum_{j=0}^{t} g_j Z^j$ met $g_t \neq 0$ dan zijn de termen in $\dfrac{g(Z)-g(\gamma)}{Z-\gamma}$ van de vorm

$$g_j \frac{Z^j - \gamma^j}{Z-\gamma} = g_j \Big(Z^{j-1} + \gamma Z^{j-2} + ... + \gamma^{j-1} \Big).$$

Dus

$$\frac{g(Z)-g(\gamma)}{Z-\gamma} = g_t Z^{t-1} + (\gamma g_t + g_{t-1}) Z^{t-2} + (\gamma^2 g_t + \gamma g_{t-1} + g_{t-2}) Z^{t-3} + ... \\ ... + (g_t \gamma^{t-1} + g_{t-1} \gamma^{t-2} + ... + g_1).$$

Nu levert de relatie $c = (c_1, ..., c_n) \in \Gamma(D,g) \Longleftrightarrow \sum_{i=1}^{n} \dfrac{c_i}{Z-\gamma_i} = 0$ ofwel

$$\sum_{i=1}^{n} c_i \frac{-1}{g(\gamma_i)} \frac{g(Z)-g(\gamma_i)}{Z-\gamma_i} = 0,$$

door vergelijking van coëfficiënten, t toetsvergelijkingen op met als coëfficiëntenmatrix een matrix $\tilde{H}$ gelijk aan:

$$- \begin{pmatrix} g_t g(\gamma_1)^{-1} & g_t g(\gamma_2)^{-1} ... & g_t g(\gamma_n)^{-1} \\ (\gamma_1 g_t + g_{t-1}) g(\gamma_1)^{-1} & (\gamma_2 g_t + g_{t-1}) g(\gamma_2)^{-1} & (\gamma_n g_t + g_{t-1}) g(\gamma_n)^{-1} \\ \vdots & \vdots & \vdots \\ \frac{1}{g(\gamma_1)} \sum_{j=1}^{t} \gamma_1^{j-1} g_j & \frac{1}{g(\gamma_2)} \sum_{j=1}^{t} \gamma_2^{j-1} g_j & \frac{1}{g(\gamma_n)} \sum_{j=1}^{t} \gamma_n^{j-1} g_j \end{pmatrix}$$

Deze toetsmatrix zullen we gebruiken voor de syndroombepaling bij het decoderen.

De decodeerprocedure is analoog aan die van BCH-codes. Ga uit van een Goppa code $\Gamma(D,g)$ met D en g als in definitie (2.1). Zij $c \in \Gamma(D,g)$ een uitgezonden codewoord en $y \in \mathbb{F}_q^n$ het ontvangen woord. Voor de foutenvector $e = (e_1,...,e_n) = y - c$ stellen we $M = \{i: 1 \leq i \leq n \text{ met } e_i \neq 0\}$ en $|M| = \epsilon$. Het fouten-localisatie-polynoom is de veelterm $\sigma(Z) = \prod_{i\in M}(Z-\gamma_i) \in \mathbb{F}_{q^m}[Z]$ en het fouten-evaluatie polynoom is de veelterm $\omega(Z) = \sum_{i\in M} e_i \prod_{j\in M-\{i\}}(Z-\gamma_j) \in \mathbb{F}_{q^m}[Z]$. Merk op dat g.g.d. $(\sigma,\omega) = 1$. De polynomen σ en ω bepalen weer de plaats en de aard van de fouten:

$$e_i = 0 \quad \text{als} \quad \sigma(\gamma_i) \neq 0,$$
$$e_i = \frac{\omega(\gamma_i)}{\sigma'(\gamma_i)} \quad \text{als} \quad \sigma(\gamma_i) = 0.$$

Decoderen komt neer op het bepalen van σ en ω uit het ontvangen woord. Neem aan dat het aantal fouten $\epsilon \leq \text{gr}(g)/2$. De eerste stap in het decodeerprocédé is weer de bepaling van een syndroom van y. Hiervoor nemen we $\tilde{H}y^t$. Dit komt neer op het bepalen van de coëfficiënten in het unieke polynoom $S = S(Z)$ van graad $< t = \text{gr}(g)$ dat modulo g de rationale functie

$$\left(\frac{1}{Z-\gamma_1}, \frac{1}{Z-\gamma_2}, ..., \frac{1}{Z-\gamma_n}\right) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} =$$
$$= \left(\frac{1}{Z-\gamma_1}, ..., \frac{1}{Z-\gamma_n}\right) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \text{ representeert.}$$

Het polynoom S van graad $\leq \text{gr}(g) - 1$ heet het syndroompolynoom en er geldt:

$$S \equiv \sum_{i\in M} \frac{e_i}{Z-\gamma_i} \pmod{g}.$$

Nu hebben we

$$S\sigma \equiv \left(\sum_{i\in M} \frac{e_i}{Z-\gamma_i}\right)\left(\prod_{j\in M}(Z-\gamma_j)\right) =$$
$$\sum_{i\in M} e_i \prod_{j\in M-\{i\}} \left(Z-\gamma_j\right) = \omega \pmod{g}$$

Aldus vinden we als sleutelvergelijking:

$$S\sigma \equiv \omega (\text{mod} g).$$

We moeten dus weer $\sigma, \omega \in \mathbb{F}_{q^m}[Z]$ bepalen met $\text{gr}(\omega) < \text{gr}(\sigma) \leq \text{gr}(g)/2$ en g.g.d. $(\omega,\ \sigma) = 1$, die voldoen aan de sleutelvergelijking. Op dezelfde manier als bij de BCH-codes volgen σ en ω uit de bepaling van de g.g.d. van S en g met behulp van het euklidisch algoritme. De laatste stap in het decodeerproces bestaat uit de bepaling van de nulpunten van σ en daaruit de e_i.

§4 Het decoderen van binaire irreducibele Goppa codes

Zij $q = 2^m$ en $\Gamma(D, g)$ een Goppa code met $g \in \mathbb{F}_q[Z]$ irreducibel van graad t en D zó dat drager$(D) \cap$ drager$((g)_0) = \emptyset$. De decodeermethode uit §3 verbetert $\leq t/2$ fouten. Volgens Stelling (2.3) is echter $d(\Gamma(D, g)) \geq 2t + 1$. We zullen nu de decodeermethode zo aanpassen dat alle foutenpatronen van gewicht $\leq t$ verbeterd worden. In het binaire geval geldt voor het foutenevaluatiepolynoom $\omega = \sigma'$. De sleutelvergelijking wordt nu:

$$S\sigma \equiv \sigma' \ (\mathrm{mod} g).$$

Als g geen meervoudige wortels heeft (wat voor irreducibele g het geval is), geldt dat de sleutelvergelijking precies één monische oplossing σ heeft met graad $\sigma \leq t$ en σ slechts enkelvoudige wortels. Merk op dat we σ kunnen schrijven als $\sigma = \alpha^2 + Z\beta^2$ met $\alpha, \beta \in \mathbb{F}_q[Z]$, waarbij $\mathrm{gr}(\alpha) \leq t/2$, $\mathrm{gr}(\beta) < t/2$ en g.g.d.$(\alpha, \beta) = 1$. Om de sleutelvergelijking op te lossen gaan we als volgt te werk.

a) Bepaal via het Euklidisch algoritme $T \in \mathbb{F}_q[Z]$ met $\mathrm{gr}(T) < t$ zó dat

$$ST \equiv 1 \ (\mathrm{mod}\ g).$$

Aangezien g irreducibel is, volgt uit g.g.d.$(S,\ g) = 1$ dat precies één zo'n T bestaat.

b) Als $T = Z$ zet dan $\sigma = Z$ en decodeer.

c) Als $T \neq Z$ bepaal dan $R \in \mathbb{F}_q[Z]$ met $\mathrm{gr}(R) < t$ zó dat

$$R^2 \equiv T + Z \ (\ \mathrm{mod}\ g). \tag{9}$$

Ga na dat R uniek is. Het polynoom R is als volgt te bepalen.

c1) Schrijf $g = G_1^2 + ZG_2^2$ met g.g.d.$(G_1, G_2) = 1$.

c2) Laat $\tilde{T}(Z) = T + Z$ en schrijf $\tilde{T} = T_1^2 + ZT_2^2$ met $T_1, T_2 \in \mathbb{F}_q[Z]$.

Aangezien g.g.d.$(G_1, G_2) = 1$ bestaan $F_1, F_2 \in \mathbb{F}_q[Z]$ met $\mathrm{gr}(F_i) < \mathrm{gr}(G_i)$ voor $i = 1, 2$, zó dat $T_2 = F_1G_2 + F_2G_1$ (via het Euklidisch algoritme).

c3) Nu voldoet $R = T_1 + F_1G_1 + ZF_2G_2$ aan (9) met $\mathrm{gr}(R) < t$. Controleer dit.

d) Los vervolgens op de congruentie

$$R\beta \equiv \alpha \ (\mathrm{mod} g),$$

met $\alpha, \beta \in \mathbb{F}_q[Z]$, met $\mathrm{gr}(\alpha) \leq t/2$, $\mathrm{gr}(\beta) < t/2$ en g.g.d.$(\alpha, \beta) = 1$. Dit gebeurt op de manier zoals beschreven in Hoofdstuk IV, 1.19. Daaruit blijkt dat α en β vastliggen op een constante L in $\mathbb{F}_q$ na.

e) Kies $L \in \mathbb{F}_q$ zó dat $\alpha^2 + Z\beta^2$ monisch is.

f) Het foutenlocalisatie polynoom is nu

$$\sigma = \alpha^2 + Z\beta^2.$$

Ga na dat σ voldoet aan de sleutelvergelijking.

Na bepaling van de nulpunten van σ kan het ontvangen woord worden gedecodeerd.

Opgaven bij Hoofdstuk VII

1 i) Zij $g = Z^2 + Z + \alpha^3$ met α primitieve 15^e-eenheids wortel in $\mathbb{F}_{16}$ die voldoet aan $\alpha^4 + \alpha + 1 = 0$ en $D = \mathbb{F}_{16} = \{0, 1, \alpha, ..., \alpha^{14}\}$. Geef een voortbrengermatrix en een toetsmatrix voor $\Gamma(D, g)$ over $\mathbb{F}_2$. Bepaal lengte, dimensie en minimumafstand van $\Gamma(D, g)$.

ii) Decodeer met het decodeeralgoritme uit §4:

$$(1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0).$$

2) Als 1^i) met $g = Z^2 + 1$ en $D = \mathbb{F}_{16}^*$.

3) Laat $n = q^m - 1,\ D = \mathbb{F}_{q^m}^*$ en α een primitieve n^{de}-eenheidswortel.
De code C_1 is de BCH-code van lengte n over $\mathbb{F}_q$ met nulpunten $1, \alpha, ..., \alpha^{d_1 - 2}$.
De code C_2 is de Goppa code $\Gamma(D, g)$ over $\mathbb{F}_q$ voor zekere $g \in \mathbb{F}_{q^m}[Z]$.
Bewijs: $d(C_1 \cap C_2) \geq d(C_1) + d(C_2) - 1$.

4) Gegeven is de cyclische code C over $\mathbb{F}_2$ van lengte 15 met voortbrengerpolynoom $X^2 + X + 1$. Bewijs dat C geen Goppa code is.

5) Gegeven is een binaire Goppa code $\Gamma(D, g)$ met $g \in \mathbb{F}_q[Z]$ en $D \subset \mathbb{F}_q$. Het Goppa polynoom g is eenduidig te schrijven als $g = g_1^2 g_2$ met $g_1,\ g_2 \in \mathbb{F}_q[Z], g_2$ kwadraatvrij. Bewijs: $d(\Gamma(D, g)) \geq 2(\mathrm{gr}(g_1) + \mathrm{gr}(g_2)) + 1$.

6) Bewijs dat de codes $C(D, G)$ en $C^*(D, G)$ uit §1 MDS-codes zijn als $0 \leq \mathrm{gr}(G) \leq n - 2$.

Hoofdstuk VIII. Asymptotische grenzen voor codes.

De coderingstheorie is mede ontwikkeld naar aanleiding van de stelling van Shannon: Gegeven is een communicatiekanaal met capaciteit K. Nu bestaat er voor alle $\epsilon_1 > 0,\ \epsilon_2 > 0$ bij voldoend grote n een (lineaire) code over $\mathbb{F}_q$ van lengte n, rendement $R > K - \epsilon_1$ en kans op een decodeerfout $< \epsilon_2$.

Voor een binair symmetrisch kanaal met kans op een kanaalfout $\epsilon \leq \frac{1}{2}$ is de capaciteit $K_2(\epsilon) = 1 - H_2(\epsilon)$ waarin $H_2(\epsilon)$ de *binaire entropie functie* is, gedefinieerd door:

$$H_2(0) = 0, \quad H_2(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)$$

voor $0 < \epsilon \leq 1/2$.

In de coderingstheorie gaat het erom de (lineaire) codes uit de stelling van Shannon in concreto aan te geven. Omdat de kans op een decodeerfout een moeilijk te bepalen grootheid is, nemen we als maat voor het corrigerend vermogen van een code C van lengte n de *relatieve minimumafstand* $\delta(C) = d(C)/n$. De code C kan dus $\leq t = [(\delta n - 1)/2]$ fouten corrigeren.

Het wezenlijke probleem van de coderingstheorie is een optimaliseringsprobleem. Beperken we ons tot lineaire codes dan zoeken we bij vaste n naar codes waarvan de parameters k en d zo groot mogelijk zijn (en waarvoor een eenvoudig decodeeralgoritme bestaat). Om grenzen aan te geven van wat haalbaar is bestuderen we asymptotische eigenschappen van codes. Daartoe voegen we aan elke lineaire (n,k,d)-code over $\mathbb{F}_q$ het (code)punt

$$(\delta(C),\ R(C)) = \left(\frac{d}{n},\ \frac{k}{n}\right) \in [0,1] \times [0,1] \ \text{ toe.}$$

Noem de deelverzameling van het eenheidsvierkant die zo ontstaat V_q^{lin} en laat U_q^{lin} de verzameling ophopingspunten van V_q^{lin} zijn. Men ziet onmiddellijk in dat de zijden van het eenheidsvierkant op de assen tot U_q^{lin} behoren. Als (δ, R) met $\delta > 0, R > 0$ in U_q^{lin} ligt dan is er een rij (n_i, k_i, d_i) -codes C_i over $\mathbb{F}_q$ met

$$\lim_{i\to\infty} n_i = \infty, \lim_{i\to\infty} R_i = \lim_{i\to\infty} k_i/n_i = R > 0 \ \text{ en } \ \lim_{i\to\infty} \delta_i = \lim_{i\to\infty} d_i/n_i = \delta > 0.$$

Zo een rij codes heet *een asymptotisch goede rij*. Justesen slaagde er rond 1970 in als eerste een concrete asymptotisch goede rij codes aan te geven. De bepaling van de verzameling $U_q^{\text{lin}} \subset [0,1] \times [0,1]$ is het fundamentele (onopgeloste) asymptotische probleem van de theorie van lineaire codes. Men gaat na dat als $(\delta, R) \in U_q^{\text{lin}}$ dan ook (δ, R') met $0 \leq R' \leq R$. (Controleer.) Het "gebied" U_q^{lin} wordt behalve door de zijden van het eenheidsvierkant begrensd door de grafiek van de functie

$$a_q^{\text{lin}} : [0,1] \to [0,1]$$

gedefinieerd door

$$a_q^{\text{lin}}(\delta) = \sup\{R : (\delta, R) \in U_q^{\text{lin}}\}.$$

Er geldt:

$$U_q^{\text{lin}} = \{(\delta, R) : 0 \leq \delta \leq 1 \quad \text{en} \quad 0 \leq R \leq a_q^{\text{lin}}(\delta)\}.$$

Op basis van de in hoofdstuk II afgeleide grenzen voor lineaire codes zullen we eerst grenzen voor $a_q^{\text{lin}}(\delta)$ aangegeven. Daarna tonen we aan dat $a_q^{\text{lin}}(\delta)$ een continue functie van δ is. Laat men de restrictie lineair vallen dan kan men op dezelfde wijze als boven, U_q, V_q en $a_q(\delta)$ definiëren voor (algemene) codes over $\mathbb{F}_q$. Natuurlijk geldt $a_q^{\text{lin}}(\delta) \leq a_q(\delta)$; of er gelijkheid geldt is een onopgelost probleem.

(1.1) Stelling. *(Asymptotische Singleton grens) Er geldt:* $a_q^{\text{lin}}(\delta) \leq 1 - \delta$.

Bewijs. Voor een (n, k, d)-code C over $\mathbb{F}_q$ geldt de Singletongrens (II, (3.4)) : $k + d \leq n + 1$. Dus $R(C) + \delta(C) \leq 1 + 1/n$ en dit heeft 1 als limiet voor $n \to \infty$. Hieruit volgt dat voor $(\delta, R) \in U_q^{\text{lin}}$ geldt $\delta + R \leq 1$ ofwel $a_q^{\text{lin}}(\delta) \leq 1 - \delta$. $\square$

(1.2) Stelling. *(Asymptotische Plotkin grens) De functie* $a_q^{\text{lin}}(\delta)$ *voldoet aan de ongelijkheid:* $a_q^{\text{lin}}(\delta) \leq \max(1 - \delta/(1 - q^{-1}), 0)$.

Bewijs. Neem $(\delta, R) \in U_q^{\text{lin}}$. Zij $(C_i)_{i=1,2,\ldots}$ een rij verschillende (n_i, k_i, d_i)-codes over $\mathbb{F}_q$ met $\lim_{i\to\infty} d_i/n_i = \delta$ en $\lim_{i\to\infty} k_i/n_i = R$.

Bekijk eerst het geval waarbij δ voldoet aan $1 - 1/q < \delta \leq 1$. Vanaf zekere i geldt $d_i/n_i > 1 - 1/q$ en uit de Plotkingrens (II,(3.5)) volgt dan:

$$q^{k_i} \leq \frac{d_i/n_i}{(d_i/n_i) - (1 - q^{-1})}. \tag{1}$$

Het rechterlid van (1) is begrensd, dus de k_i zijn begrensd zodat $\lim_{i\to\infty} k_i/n_i = 0$. We zien dat $a_q^{\text{lin}}(\delta) = 0$ als δ voldoet aan $1 - 1/q < \delta \leq 1$.

Beschouw nu de situatie waarbij $0 \leq \delta < 1 - 1/q$. Vanaf zekere i geldt $d_i/n_i < 1 - 1/q$. Om de Plotkingrens te kunnen gebruiken verkorten we de (n_i, k_i, d_i)-code C_i tot een (n_i', k_i', d_i)-code met $n_i' < d_i/(1 - q^{-1})$. Neem $n_i' = [(d_i - 1)/(1 - q^{-1})]$, dan geldt

$$q^{k_i'} \leq \frac{d_i}{d_i - (1 - q^{-1})n_i'} \leq d_i$$

zodat $q^{k_i} \leq d_i q^{n_i - n_i'}$ ofwel

$$k_i/n_i \leq (1/n_i)\log_q(d_i/n_i) + 1 - (n_i'/n_i).$$

Als $i \to \infty$ dan $n_i'/n_i \to \delta/(1 - q^{-1})$ zodat $R = \lim_{i\to\infty}(k_i/n_i) \leq 1 - \delta/(1 - q^{-1})$. Dus voor $0 \leq \delta < 1 - 1/q$ geldt $a_q^{\text{lin}}(\delta) \leq 1 - \delta/(1 - q^{-1})$. Ga zelf na dat voor $(\delta, R) \in U_q^{\text{lin}}$ met $\delta = 1 - 1/q$ de gelijkheid $R = 0$ geldt. $\square$

Ook de Hamming grens (II, (3.3)) heeft een asymptotische variant. Voor we deze formuleren voeren we eerst de *entropie-functie* in:

$$H_q(\delta) = \begin{cases} 0 \quad \text{voor} \quad \delta = 0, \\ \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta) \quad \text{voor} \quad 0 < \delta \leq 1 - 1/q. \end{cases}$$

(1.3) Lemma. *Voor $t \in \mathbb{Z}_{>0}$ met $t/n \leq 1 - 1/q$ geldt*

$$\frac{1}{n+1} q^{nH_q(t/n)} < \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{nH_q(t/n)}. \tag{2}$$

Bewijs. Voor $0 < x \leq 1$ geldt

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq \sum_{i=0}^{n} \binom{n}{i} (q-1)^i x^{i-t} = x^{-t}(1 + (q-1)x)^n.$$

De functie $x^{-t}(1 + (q-1)x)^n$ heeft in $x_0 = \frac{1}{q-1}\frac{t}{n-t}$ een minimum. De waarde van dit minumum is $q^{nH_q(t/n)}$. Hieruit volgt de bovengrens in (2).

Voor de ondergrens merken we op dat

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i > \binom{n}{t} (q-1)^t > \frac{1}{n+1} \tilde{x}^{-t}(1 + (q-1)\tilde{x})^n \quad \text{met} \quad \tilde{x} = \frac{1}{q-1}\frac{t}{n-t}. \tag{3}$$

Beschouw namelijk de ontwikkeling

$$(1 + (q-1)\tilde{x})^n = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i \tilde{x}^i = \sum_{i=0}^{n} a_i \tilde{x}^i.$$

Dan geldt voor $i < t$

$$\frac{a_{i-1}}{a_i} < \frac{a_{t-1}}{a_t} = \frac{1}{q-1} \cdot \frac{t}{n-t+1}$$

en voor $i \geq t$

$$\frac{1}{q-1} \cdot \frac{t+1}{n-t} = \frac{a_t}{a_{t+1}} \leq \frac{a_i}{a_{i+1}}.$$

Aangezien $(a_{t-1}/a_t) < \tilde{x} < (a_t/a_{t+1})$ volgt dat de term $a_t \tilde{x}^t = \binom{n}{t}(q-1)^t \tilde{x}^t$ maximaal is in $\sum_{i=0}^{n} a_i \tilde{x}^i$. Dus

$$(1 + (q-1)\tilde{x})^n < (n+1)\binom{n}{t}(q-1)^t \tilde{x}^t.$$

Dit levert de ondergrens in (3), welke gelijk is aan $q^{nH_q(t/n)}/(n+1)$. □

(1.4) Eigenschap. *Als $\lim_{n\to\infty} t_n/n = \delta$ met $0 \leq \delta < 1 - 1/q$ dan geldt*

$$\lim_{n\to\infty} \frac{1}{n} \log_q \sum_{i=0}^{t_n} \binom{n}{i} (q-1)^i = H_q(\delta).$$

(1.5) Stelling. *(Asymptotische Hamming grens) Er geldt*

$$a_q^{\rm lin}(\delta) \leq 1 - H_q(\delta/2) \quad \text{voor} \quad 0 \leq \delta \leq 1.$$

Bewijs. Neem $(\delta, R) \in U_q^{\rm lin}$ met $0 < \delta < 1$. Voor (n_i, k_i, d_i)-codes C_i met de eigenschap $\lim_{i\to\infty} d_i/n_i = \delta$ en $\lim_{i\to\infty} k_i/n_i = R$ geldt de Hamming grens:

$$q^{n_i - k_i} \geq \sum_{j=0}^{[(d_i-1)/2]} \binom{n_i}{j} (q-1)^j.$$

Aangezien $\lim_{i\to\infty}[(d_i-1)/2]/n_i = \delta/2$ en $0 < \delta/2 < 1 - 1/q$ volgt uit Eigenschap (1.4) dat $\lim_{i\to\infty}(1 - k_i/n_i) = 1 - R \geq H_q(\delta/2)$. Dus $a_q^{\rm lin} \leq 1 - H_q(\delta/2)$. □

Na de bovengrenzen leiden we nu een ondergrens af voor $a_q^{\rm lin}$.

(1.6) Stelling. *(Asymptotische Gilbert-Varshamov grens) Er geldt:* $a_q^{\rm lin}(\delta) \geq 1 - H_q(\delta)$ *voor* $0 \leq \delta \leq 1 - 1/q$.

Bewijs: Uit de Gilbert-Varshamov grens, versie van Gilbert (II, (3.7a)), volgt dat voor gegeven n en d de dimensie van een maximale (n, d)-code voldoet aan:

$$k_{\max} \geq n - \log_q \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i.$$

Neem nu $0 \leq \delta < 1 - 1/q$ dan geldt voor n en $d = [\delta n]$ dat

$$k_{\max} \geq n - \log_q \sum_{i=0}^{[\delta n]} \binom{n}{i} (q-1)^i$$

zodat voor het bijbehorende rendement geldt

$$R_n = \frac{k_{\max}}{n} \geq 1 - \frac{1}{n} \log_q \sum_{i=0}^{[\delta n]} \binom{n}{i} (q-1)^i.$$

Als $n \to \infty$ ontstaat een rij lineaire codes met parameters $(n, k_{\max}, [\delta n])$ waarvoor $\lim_{n\to\infty}[\delta n]/n = \delta$ en $R_n \geq 1 - H_q(\delta) - \epsilon$ voor elke $\epsilon > 0$ (bij voldoend grote n). Deze rij levert dus een ophopingspunt $(\delta, \geq 1 - H_q(\delta))$. Voor $0 \leq \delta < 1 - 1/q$ geldt nu $a_q^{\rm lin}(\delta) \geq 1 - H_q(\delta)$. □

(1.7) Stelling. *De functie* $a_q^{\rm lin}(\delta)$ *is continu op het interval* $[0, 1]$ *en strikt monotoon dalend op* $[0, 1 - 1/q]$ *met* $a_q^{\rm lin}(0) = 1$. *Op* $[1 - 1/q, 1]$ *geldt* $a_q^{\rm lin}(\delta) = 0$.

Goppa codes blijken asymptotisch bijzonder goede codes te zijn: "Goppa codes halen de Gilbert-Varshamov grens".

(1.8) Stelling. *Voor elke δ_0 met $0 < \delta_0 < 1 - 1/q$ is er een rij klassieke Goppa codes over $\mathbb{F}_q$ met ophopingspunt $(\geq \delta_0, \geq 1 - H_q(\delta_0))$.*

Bewijs. Voor $m \geq 1$ nemen we $D_m = \mathbb{F}_{q^m}$ en $n_m = q^m$. Kies δ_0 met $0 < \delta_0 < 1 - 1/q$ en $\epsilon > 0$ zodat $\delta_0 - \epsilon > 0$. Zij $t_m = [(n_m/m)H_q(\delta_0)]$ en G_m de verzameling van monische irreducibele veeltermen van graad t_m over $\mathbb{F}_{q^m}$. We willen een rij verschillende Goppa codes $\Gamma(D_m, g_m)$ over $\mathbb{F}_q$ maken met $g_m \in G_m$, met minimumgewicht $\geq d_m = [(\delta_0 - \epsilon)n_m]$ en rendement $R(\Gamma(D_m, g_m)) \geq 1 - H_q(\delta_0)$.

Eerst bekijken we voor $g_m \in G_m$ de codes $\Gamma(D_m, g_m)$ die een woord $c \neq 0$ van gewicht $< d_m$ bevatten. We hebben gezien:

$$c \in \Gamma(D_m, g_m) \iff \sum_{\gamma \in \mathbb{F}_{q^m}} \frac{c_\gamma}{Z - \gamma} = 0 \text{ in } \mathbb{F}_{q^m}[Z]/(g_m).$$

De teller van $\sum_{\gamma \in \mathbb{F}_{q^m}} c_\gamma/(Z - \gamma)$ moet dus deelbaar zijn door g_m en heeft graad $\leq w(c) - 1$. Het aantal g_m met $c \in \Gamma(D_m, g_m)$ is dus hoogstens $[(w(c) - 1)/t_m]$. Dus het aantal g_m zodat in $\Gamma(D_m, g_m)$ niet-triviale woorden van gewicht $< d_m$ optreden is hoogstens

$$\sum_{j=1}^{d_m - 1} [\frac{j-1}{t_m}] \binom{n_m}{j} (q-1)^j \leq \frac{d_m}{t_m} \sum_{j=0}^{d_m} \binom{n_m}{j} (q-1)^j. \tag{4}$$

Anderzijds is het aantal polynomen in G_m:

$$\frac{1}{t_m} \sum_{b | t_m} \mu(b) q^{m t_m / b} > \frac{n_m^{t_m}}{t_m}(1 - n_m^{-(t_m/2)+1}). \tag{5}$$

(Ga dit na.) Dus bestaan er codes $\Gamma(D_m, g_m)$ met minimumafstand $\geq d_m$ als

$$\text{rechterkant (4)} < \text{ rechterkant (5)}.$$

Nu blijkt

$$\lim_{m \to \infty} \frac{d_m \sum_{j=0}^{d_m} \binom{n_m}{j} (q-1)^j}{n_m^{t_m}(1 - n_m^{-(t_m/2)+1})} = 0.$$

Bewijs dit zelf door gebruik te maken van Eigenschap (1.4) en op te merken dat

$$\lim_{t \to \infty} \frac{m t_m}{n_m} = H_q(\delta_0).$$

Dus vanaf zekere m bestaan er $\Gamma(D_m, g_m)$ met minimumafstand $\geq d_m$ en dimensie $\geq n_m - m t_m$ (zie Hfdst. VII, Eig. (2.4)). Voor deze codes geldt

$$\delta(\Gamma(D_m, g_m)), R(\Gamma(D_m, g_m)) = (\geq \frac{d_m}{n_m}, \geq \frac{n_m - m t_m}{n_m}).$$

Omdat $\lim_{m \to \infty}(d_m/n_m) = \delta_0 - \epsilon$ en $(n_m - m t_m)/n_m \geq 1 - H_q(\delta_0)$ vinden we zo voor alle $\epsilon > 0$ een rij klassieke Goppa codes met ophopingspunt

$$(\geq \delta_0 - \epsilon, \geq 1 - H_q(\delta_0)).$$

Dit leidt tot een ophopingspunt $(\geq \delta_0, \geq 1 - H_q(\delta_0))$. $\square$

Gedurende meer dan 25 jaar was het hoofdvermoeden van de coderingstheorie:

$$a_q(\delta) = 1 - H_q(\delta) \quad \text{voor} \quad 0 < \delta < 1 - 1/q.$$

Echter rond 1980 ontdekte Goppa nauwe verbanden tussen de theorie van algebraische krommen over $\mathbb{F}_q$ en lineaire codes over $\mathbb{F}_q$. Dit leidde o.a. tot meetkundige Goppa codes. Op basis van de ideeën van Goppa werd in 1982 door Tsfasman, Vladut en Zink bewezen dat het hoofdvermoeden onjuist was:

(1.9) Stelling. *Voor $q = p^{2t} \geq 49$ bestaan er oneindige rijen meetkundige Goppa codes over $\mathbb{F}_q$ die ophopingspunten echt boven de asymptotische Gilbert-Varshamov grens hebben.*

Toelichting. Zij $N_q(g)$ het maximale aantal $\mathbb{F}_q$-rationale punten op een projectieve gladde irreducibele kromme van geslacht g over $\mathbb{F}_q$ en stel $A(q) = \limsup_{g\to\infty} N_q(g)/g$. Via meetkundige codes op krommen kan men aantonen dat

$$a_q^{\text{lin}} \geq 1 - \frac{1}{A(q)} - \delta.$$

Er geldt $A(q) \leq \sqrt{q} - 1$ en $A(q) = \sqrt{q} - 1$ als q een kwadraat is. Dus als $q = p^{2t}$ dan ligt de lijn (I)

$$R + \delta = 1 - 1/(\sqrt{q} - 1) \tag{6}$$

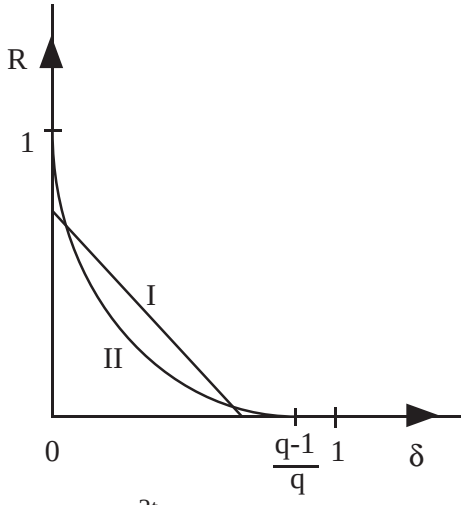
voor $0 \leq \delta \leq 1$ in U_q^{lin}. De raaklijn met richtingscoëfficiënt -1 aan de Gilbert-Varshamov-grens heeft vergelijking

$$R + \delta = 1 - \log_q((2q-1)/q).$$

Omdat de Gilbert-Varshamovgrens (II) concaaf is ligt een segment van (6) boven deze grens als

$$1 - 1/(\sqrt{q} - 1) > 1 - \log_q((2q-1)/q).$$

Dit is het geval als $q \geq 49$.



$q=p^{2t}$ 49

Aanhangsel I. Eindige Lichamen

Als $\mathbb{F}$ een eindig lichaam is dan is het priemlichaam van de vorm $\mathbb{Z}/p\mathbb{Z}$ en p heet de karakteristiek van $\mathbb{F}$. We kunnen dan $\mathbb{F}$ opvatten als een vectorruimte over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, zeg van dimensie r. Er geldt dan $\#\mathbb{F} = p^r$ en $\mathbb{F}$ heet een uitbreiding van graad r van $\mathbb{F}_p$. Het quotient $\mathbb{F}_p[X]/f$ met f een irreducibel polynoom van graad r in $\mathbb{F}_p[X]$ is een eindig lichaam met p^r elementen. Omdat men voor elk priemgetal p en elk positief geheel getal r een irreducibel polynoom van graad r in $\mathbb{F}_p[X]$ vinden kan, bestaat er voor iedere positieve priemmacht p^r een lichaam met p^r elementen.

Laat $\mathbb{F}$ een lichaam zijn met p^r elementen. Omdat de karakteristiek p is geldt $(a+b)^p = a^p+b^p$ en door herhaald toepassen $(a+b)^{p^t} = a^{p^t}+b^{p^t}$. Dus de afbeelding $\alpha \to \alpha^p$ definieert een $\mathbb{F}_p$-automorfisme van $\mathbb{F}$. Dit automorfisme heeft orde r en wordt het Frobenius-automorfisme genoemd. Er geldt dat de automorfismengroep van $\mathbb{F}$ cyclisch is en wordt voortgebracht door dit automorfisme.

Zij $\mathbb{F}'$ een uitbreidingslichaam van $\mathbb{F}_p$ waarin het polynoom $X^{p^r} - X$ volledig in lineaire factoren kan worden ontbonden, bijv. het ontbindingslichaam van dit polynoom t.o.v. $\mathbb{F}$. Dan gaat men gemakkelijk na dat

$$\mathbb{F}_{p^r} = \{\alpha \in \mathbb{F}' : \alpha^{p^r} = \alpha\}$$

een deellichaam van $\mathbb{F}'$ is met p^r elementen. Dit levert dus een lichaam $\mathbb{F}_{p^r}$ met p^r elementen. Verder volgt ook dat ieder lichaam K met p^r elementen isomorf is met $\mathbb{F}_{p^r}$. Immers, omdat iedere eindige ondergroep van een lichaam cyclisch is, is K^* cyclisch van orde $p^r - 1$ en ieder element van K^* voldoet dus aan $X^{p^r-1} - 1 = 0$. Hieruit volgt dat alle elementen van K voldoen aan $X^{p^r} - X = 0$. Het sturen van een voortbrenger van de cyclische group van K^* naar een voortbrenger van $\mathbb{F}^*_{p^r}$ levert nu een isomorfisme. We vatten samen:

Stelling. *Het aantal elementen van een eindig lichaam is een macht van een priemgetal. Voor elke positieve macht p^r van een priemgetal is er op isomorfie na precies een lichaam met p^r elementen.*

Laat $\mathbb{F}$ weer een lichaam met $q = p^r$ elementen zijn. Stel dat α in een uitbreidingslichaam K een nulpunt is van een irreducibel polynoom g van graad m in $\mathbb{F}[X]$. Laat $\mathbb{F}(\alpha)$ het kleinste deellichaam van K zijn dat $\mathbb{F}$ en α bevat. Dan geldt $\mathbb{F}(\alpha) \cong \mathbb{F}[X]/(g)$ en de elementen

$$1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$$

vormen een basis voor de $\mathbb{F}$-vectorruimte $\mathbb{F}(\alpha)$; we noemen $\mathbb{F}(\alpha)$ het lichaam dat ontstaat door adjunctie van α aan $\mathbb{F}$.

Laat $\mathbb{F}$ een eindig lichaam zijn dat een lichaamsuitbreiding van $\mathbb{F}_q$ is. Als $\beta \in \mathbb{F}$ dan is het ideaal

$$\{h \in \mathbb{F}_q[X] : h(\beta) = 0\}$$

een hoofdideaal. Als we van een voortbrenger, die van minimale graad is, eisen dat hij monisch is ligt deze eenduidig vast. Dit polynoom heet het minimumpolynoom $f^{\beta}_{F_q}$ van β (t.o.v. $\mathbb{F}_q$). Voor elke ander polynoom $h \in \mathbb{F}_q[X]$ met $h(\beta) = 0$ geldt: $f^{\beta}_{\mathbb{F}_q}$ deelt h.

De graad van dit minimumpolynoom is gelijk aan de graad van de lichaamsuitbreiding $\mathbb{F}_q(\beta)$ van $\mathbb{F}_q$.

Als $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s}$ een lichaamsuitbreiding is van eindige lichamen dan is $\mathbb{F}_{q^r}^*$ een ondergroep van de cyclische groep $\mathbb{F}_{q^s}^*$; i.h.b. $q^r - 1$ deelt $q^s - 1$. Daaruit volgt:

$$\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s} \iff r|s.$$

Aanhangsel II. De Projectieve Ruimte

Laat V een eindig-dimensionale vectorruimte van dimensie $n+1$ zijn over het lichaam k. We definieren een equivalentierelatie $\sim$ op $V - \{0\}$:

$$v_1 \sim v_2 \iff \text{ er bestaat een } \lambda \in k^* \text{ met } \lambda v_1 = v_2.$$

De equivalentieklassen zijn dus de lijnen door de oorsprong in V (waarbij de oorsprong zelf buiten beschouwing blijft). De verzameling van equivalentieklassen noteren we $\mathbb{P}(V)$ en heet de *projectieve ruimte* van V. Als in V een basis gegeven is en we dus een isomorfisme $V \cong k^{n+1}$ hebben noteren we $\mathbb{P}(V)$ als $\mathbb{P}^n$ (of $\mathbb{P}^n_k$ als we het lichaam ook in de notatie tot uitdrukking willen brengen). In dat geval noteren we de equivalentieklasse van een element $(v_0, v_1, \ldots, v_n) \in k^{n+1} - \{0\}$ met $(v_0 : v_1 : \ldots : v_n)$. Er geldt dan

$$(\lambda v_0 : \lambda v_1 : \ldots : \lambda v_n) = (v_0 : v_1 : \ldots : v_n).$$

In deze schrijfwijze heet een representant van een element van $\mathbb{P}(V)$ een stel *homogene coördinaten* van dat element. Verandering van een basis in V voert tot nieuwe homogene coördinaten in $\mathbb{P}(V)$.

Als $(v_0 : v_1 : \ldots : v_n) \in \mathbb{P}^n$ de eerste coördinaat ongelijk nul heeft kunnen we door vermenigvuldiging met v_0^{-1} bereiken dat de eerste coördinaat gelijk aan 1 is. We zien zo

$$\mathbb{P}^n = \{(1 : v_1 : \ldots : v_n) : (v_1, v_2, \ldots, v_n) \in k^n\} \cup \{(0 : v_1 : v_2 : \ldots : v_n) \in \mathbb{P}^n\}.$$

Daarmee kunnen we $\mathbb{P}^n$ schrijven als disjuncte som

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}, \tag{1}$$

met $\mathbb{A}^n = k^n$ de affiene n-dimensionale ruimte. Met inductie volgt nu

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \ldots \cup \mathbb{A}^0. \tag{2}$$

Als $W \subseteq V$ een lineaire deelruimte is dan vinden we $\mathbb{P}(W) \subseteq \mathbb{P}(V)$. Zo een deelverzameling heet een projectief-lineaire deelruimte. Als de codimensie van W (dat is $\dim(V) - \dim(W)$) gelijk is aan 1 dan heet zo een $\mathbb{P}(W)$ een hypervlak. Als in V een basis gegeven is dan wordt een lineaire deelruimte gegeven door lineaire vergelijkingen $\sum_{i=0}^n a_i x_i = 0$ met $a_i \in k$. Deze vergelijkingen definiëren ook de projectief-lineaire deelruimten in $\mathbb{P}^n$. Een punt $(v_0 : v_1 : \ldots : v_n) \in \mathbb{P}^n$ ligt in deze lineaire deelruimte als ze voldoet aan genoemde (homogene) lineaire vergelijkingen .

In het geval waarin k een eindig lichaam $\mathbb{F}_q$ is vinden we (met (2) of met de definitie)

$$\#\mathbb{P}^n_{\mathbb{F}_q} = q^n + q^{n-1} + \ldots + q + 1 = \frac{q^{n+1} - 1}{q - 1}.$$

Een hypervlak kan geïdentificeerd worden met $\mathbb{P}^{n-1}$ en bezit dus $(q^n - 1)/(q - 1)$ punten.

Aanhangsel III. Kwadraatresten

Zij p een oneven priemgetal en beschouw het lichaam $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. De multiplicatieve groep $\mathbb{F}_p^*$ is cyclisch van orde $p-1$. Laat α een voortbrenger zijn van $\mathbb{F}_p^*$. De kwadraten in $\mathbb{F}_p^*$ vormen een ondergroep van orde $(p-1)/2$:

$$(\mathbb{F}_p^*)^2 = \{\alpha^2, \alpha^4, \ldots, \alpha^{p-1}\}.$$

De overige elementen van $\mathbb{F}_p^*$ vormen een nevenklasse van $(\mathbb{F}_p^*)^2$ in $\mathbb{F}_p^*$: de niet-kwadraten

$$\alpha \cdot (\mathbb{F}_p^*)^2 = \{\alpha, \alpha^3, \ldots, \alpha^{p-2}\}.$$

Voor een geheel getal $a \in \mathbb{Z}$ noteren we de restklasse van a modulo p als $\bar{a}$.

Definitie. Een $a \in \mathbb{Z}$ met g.g.d. $(a, p) = 1$ heet een *kwadraatrest modulo p* als $\bar{a} \in (\mathbb{F}_p^*)^2$ en een *niet-kwadraatrest modulo p* als $\bar{a} \notin (\mathbb{F}_p^*)^2$.

Merk op dat a een kwadraatrest respectievelijk een niet-kwadraatrest modulo p is als $x^2 \equiv a (\mathrm{mod} p)$ oplosbaar respectievelijk niet oplosbaar is in $\mathbb{Z}$. Al of niet kwadraatrest zijn is een eigenschap van restklassen.

Rekenregels.

$$\begin{aligned} \text{rest} \times \text{rest} &= \text{rest}, \\ \text{niet-rest} \times \text{niet-rest} &= \text{rest}, \\ \text{rest} \times \text{niet-rest} &= \text{niet-rest}. \end{aligned}$$

Definitie. Voor $a \in \mathbb{Z}$ wordt het *Legendre-symbool* gedefinieerd als

$$(\frac{a}{p}) = \begin{cases} 1 & \text{als } a \text{ kwadraatrest modulo } p, \\ -1 & \text{als } a \text{ niet-kwadraatrest modulo } p, \\ 0 & \text{als } p \text{ deler is van } a. \end{cases}$$

Merk op dat het Legendre-symbool multiplicatief is en constant op restklassen modulo p.

Rekenregels voor het Legendre-symbool.
Voor verschillende oneven priemgetallen p en q geldt:

$$\begin{aligned} (\frac{-1}{p}) &= (-1)^{(p-1)/2}, \\ (\frac{2}{p}) &= (-1)^{(p^2-1)/8}, \\ (\frac{p}{q})(\frac{q}{p}) &= (-1)^{(p-1)(q-1)/4}. \end{aligned}$$

De laatste rekenregel geniet bekendheid als *kwadratische wederkerigheidswet*.

Tabel

1) Representatie van $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ met $\alpha^2 + \alpha + 1 = 0$ door middel van machten van α.

α^i	$a + b\alpha$	minimumpol. van $\alpha^i/\mathbb{F}_2$
0	$(0,0)$	X
1	$(1,0)$	$X+1$
α	$(0,1)$	X^2+X+1
α^2	$(1,1)$	X^2+X+1

2) Representatie van $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ met $\alpha^3 + \alpha + 1 = 0$ door middel van machten van α.

α^i	$a + b\alpha + c\alpha^2$	minimumpol. van $\alpha^i/\mathbb{F}_2$
0	$(0,0,0))$	X
1	$(1,0,0))$	$X+1$
α	$(0,1,0)$	X^3+X+1
α^2	$(0,0,1)$	X^3+X+1
α^3	$(1,1,0)$	X^3+X^2+1
α^4	$(0,1,1)$	X^3+X+1
α^5	$(1,1,1)$	X^3+X^2+1
α^6	$(1,0,1)$	X^3+X^2+1

3) Representatie van $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ met $\alpha^4 + \alpha + 1 = 0$ door middel van machten van α.

α^i	$a + b\alpha + c\alpha^2 + d\alpha^3$	minimumpol. van $\alpha^i/\mathbb{F}_2$
0	$(0,0,0,0)$	X
1	$(1,0,0,0)$	$X+1$
α	$(0,1,0,0)$	X^4+X+1
α^2	$(0,0,1,0)$	X^4+X+1
α^3	$(0,0,0,1)$	$X^4+X^3+X^2+X+1$
α^4	$(1,1,0,0)$	X^4+X+1
α^5	$(0,1,1,0)$	X^2+X+1
α^6	$(0,0,1,1)$	$X^4+X^3+X^2+X+1$
α^7	$(1,1,0,1)$	X^4+X^3+1
α^8	$(1,0,1,0)$	X^4+X+1
α^9	$(0,1,0,1)$	$X^4+X^3+X^2+X+1$
α^{10}	$(1,1,1,0)$	X^2+X+1
α^{11}	$(0,1,1,1)$	X^4+X^3+1
α^{12}	$(1,1,1,1)$	$X^4+X^3+X^2+X+1$
α^{13}	$(1,0,1,1)$	X^4+X^3+1
α^{14}	$(1,0,0,1)$	X^4+X^3+1

4) Representatie van $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$ met $\alpha^5 + \alpha^2 + 1 = 0$ door middel van machten van α.

α^i	$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$	minimumpol. van $\alpha^i/\mathbb{F}_2$
0	$(0,0,0,0,0)$	X
1	$(1,0,0,0,0)$	$X+1$
α	$(0,1,0,0,0)$	X^5+X^2+1
α^2	$(0,0,1,0,0)$	X^5+X^2+1
α^3	$(0,0,0,1,0)$	$X^5+X^4+X^3+X^2+1$
α^4	$(0,0,0,0,1)$	X^5+X^2+1
α^5	$(1,0,1,0,0)$	$X^5+X^4+X^2+X+1$
α^6	$(0,1,0,1,0)$	$X^5+X^4+X^3+X^2+1$
α^7	$(0,0,1,0,1)$	$X^5+X^3+X^2+X+1$
α^8	$(1,0,1,1,0)$	X^5+X^2+1
α^9	$(0,1,0,1,1)$	$X^5+X^4+X^2+X+1$
α^{10}	$(1,0,0,0,1)$	$X^5+X^4+X^2+X+1$
α^{11}	$(1,1,1,0,0)$	$X^5+X^4+X^3+X+1$
α^{12}	$(0,1,1,1,0)$	$X^5+X^4+X^3+X^2+1$
α^{13}	$(0,0,1,1,1)$	$X^5+X^4+X^3+X+1$
α^{14}	$(1,0,1,1,1)$	$X^5+X^3+X^2+X+1$
α^{15}	$(1,1,1,1,1)$	X^5+X^3+1
α^{16}	$(1,1,0,1,1)$	X^5+X^2+1
α^{17}	$(1,1,0,0,1)$	$X^5+X^4+X^3+X^2+1$
α^{18}	$(1,1,0,0,0)$	$X^5+X^4+X^2+X+1$
α^{19}	$(0,1,1,0,0)$	$X^5+X^3+X^2+X+1$
α^{20}	$(0,0,1,1,0)$	$X^5+X^4+X^2+X+1$
α^{21}	$(0,0,0,1,1)$	$X^5+X^4+X^3+X+1$
α^{22}	$(1,0,1,0,1)$	$X^5+X^4+X^3+X+1$
α^{23}	$(1,1,1,1,0)$	X^5+X^3+1
α^{24}	$(0,1,1,1,1)$	$X^5+X^4+X^3+X^2+1$
α^{25}	$(1,0,0,1,1)$	$X^5+X^3+X^2+X+1$
α^{26}	$(1,1,1,0,1)$	$X^5+X^4+X^3+X+1$
α^{27}	$(1,1,0,1,0)$	X^5+X^3+1
α^{28}	$(0,1,1,0,1)$	$X^5+X^3+X^2+X+1$
α^{29}	$(1,0,0,1,0)$	X^5+X^3+1
α^{30}	$(0,1,0,0,1)$	X^5+X^3+1

Literatuur

1. J. van Lint e.a.: Inleiding in de Coderingstheorie. MC Syllabus 31, CWI Amsterdam, 90-6196-136-X.

2. J. van Lint: Introduction to Coding Theory. Springer Verlag, 0-387-11284-7.

3. J. van Lint & G. van der Geer: Introduction to Coding Theory and Algebraic Geometry. Birkhäuser Verlag, 0-8176-2230-6.

4. F.J. MacWilliams & N.J.A. Sloane: The Theory of Error Correcting Codes. North Holland Publ. Co., 0-444-85009-0 & 0-444-85010-4.

5. R.J. McEliece: The Theory of Information and Coding. Addison-Wesley, 0-201-13502-7.

6. T. Rao & E. Fujiwara: Error-control Coding for Computer Systems. Prentice Hall, 0-13-284068-5.

7. H. Stichtenoth: Algebraic Function Fields and Codes. Springer Verlag, 3-540-56489-6.

8. T. Thompson: From Error-correcting Codes through Sphere Packings to Simple Groups. Math. Ass. of America, 0-88385-023-0.

9. M. Tsfasman & S. Vladut: Algebraic-Geometric Codes. Kluwer Acad. Publ., 0-7923-0727-5.

10. S. VanStone & P. van Oorschot: An Introduction to Error-correcting Codes with Applications. Kluwer Acad. Publ., 0-7923-9017-2.