Hoofdstuk V

CYCLISCHE CODES

5.1. CYCLISCHE CODES

Een lineaire code V (ter lengte n over een eindig lichaam $\mathbb{F}$) werd gedefinieerd als een deelruimte van de n-dimensionale vectorruimte over $\mathbb{F}$, d.w.z. als $(a_0,\ldots,a_{n-1}) \in V$ en $(b_0,\ldots,b_{n-1}) \in V$, dan ook $(a_0+b_0,\ldots,a_{n-1}+b_{n-1}) \in V$, en als $(a_0,\ldots,a_{n-1}) \in V$ en $\lambda \in F$, dan $(\lambda a_0,\ldots,\lambda a_{n-1}) \in V$. Een lineaire code V heet een *cyclische code* als daarnaast ook geldt: als $(a_0,\ldots,a_{n-1}) \in V$ dan $(a_{n-1}, a_0,\ldots,a_{n-2}) \in V$.

Een triviaal voorbeeld van een cyclische code is de code V ter lengte 2k met: $(a_0,\ldots,a_{2k-1}) \in V \iff a_0=a_k,\ a_1=a_{k+1},\ldots,a_{k-1}=a_{2k-1}$. Zij $R^{(n)}$ de n-dimensionale vectorruimte over $\mathbb{F}$. Door $(a_0,\ldots,a_{n-1})$ te schrijven als $a_0+a_1x+\ldots a_{n-1}x^{n-1}$, is het mogelijk een vector uit $R^{(n)}$ voor te stellen als een element van (een volledig representantensysteem van) de restklassenring $\mathbb{F}[x]/(x^n-1)$. Het is duidelijk dat deze relatie een 1-1-correspondentie geeft tussen elementen van $R^{(n)}$ en elementen van $\mathbb{F}[x]/(x^n-1)$, en daarom maken we in het vervolg geen onderscheid meer tussen deze twee verzamelingen; beide noteren we met $R^{(n)}$ of R.

(5.1.1) STELLING. *Een lineaire code* V *in* $R^{(n)}$ *is cyclisch als en alleen als* V *een ideaal in* $\mathbb{F}[x]/(x^n-1)$ *is.*

BEWIJS. (i) Zij V cyclisch. Is $a(x) = a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ een codewoord dan $a_{n-1}+a_0x+a_1x^2+\ldots+a_{n-2}x^{n-1} = xa(x)$ ook. Daar V lineair is volgt hieruit dat voor ieder polynoom f(x) geldt dat f(x) a(x) $\in$ V. Dus V is een ideaal.

(ii) Is omgekeerd V een ideaal dan is met a(x) ook xa(x) in V. Dus is V cyclisch. □

Zij $q := |\mathbb{F}|$. We beperken ons in het vervolg tot de gevallen waarin (n,q) = 1. Verder zullen wij schrijven: $R := \mathbb{F}[x]$, $S := (x^n-1)$ (het ideaal in R voortgebracht door x^n-1) en $\mathcal{R}$ g(x) := het ideaal in $\mathcal{R}$ voortgebracht door g(x). Dus $\mathcal{R} = R/S$. Omdat R een hoofdideaalring is, is ook ieder ideaal in $\mathcal{R}$ een hoofdideaal, en ieder ideaal V in $\mathcal{R}$ wordt voortgebracht door een monisch polynoom g(x) met de laagste graad in V. Dit uniek bepaalde poly-

noom heet de *generator* van V. Steeds is deze g(x) een deler (in R) van x^n-1. Anders zou de g.g.d. (in R) van g(x) en x^n-1 een polynoom in V zijn met lagere graad dan g(x).

Zij $x^n-1 = f_1(x).\ \ldots\ .f_t(x)$ de ontbinding (in R) van x^n-1 in irreducibele polynomen. Een generator g(x) zal dan het product van een aantal faktoren f_i zijn. Omdat we hebben aangenomen dat (n,q) = 1, zijn $f_1,\ldots,f_t$ alle verschillend. Als een ideaal V als generator een der faktoren f_i heeft, d.w.z. $V = Rf_i(x)$, dan is V een maximaal ideaal in R en V heet dan een *maximale cyclische code*.

5.2. GENERATOR MATRIX EN CHECK POLYNOOM

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

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

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

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

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

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

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

Dan

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

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

Een parity-check matrix voor V kan als volgt worden verkregen. Omdat $g(x) \mid x^n-1$ bestaat er een $h(x)$ zo dat $g(x)h(x) = x^n-1$ (in R). Omdat $g(x)$ de graad n-k heeft, zal $h(x)$ de graad k hebben. Dus:

$$h(x) = h_0 + h_1x + \ldots + h_kx^k.$$

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

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

Als nu:

$$H = \begin{pmatrix}
0 & \cdots & 0 & h_k & \cdots & h_1 & h_0\\
0 & \cdots & 0 & h_k & \cdots & h_0 & 0\\
\vdots & & \ddots & & \ddots & 0 & 0\\
\vdots & \ddots & & \ddots & & \vdots & \vdots\\
\vdots & & \ddots & & \ddots & \vdots & \vdots\\
0 & \ddots & & \ddots & & \vdots & \vdots\\
h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0
\end{pmatrix}$$

dan geldt dus $G.H^T = 0$ (omdat $h_{k+1} = \ldots = h_{n-1} = 0$), d.w.z. H is de parity-check matrix van de code. Hieruit volgt ook dat de code $\mathcal{R}h(x)$ equivalent is met de duale code van $\mathcal{R}g(x)$. Het polynoom $h(x)$ heet het *check polynoom* van de code V. $v(x)$ zit in deze code als en slechts als $v(x)h(x) = 0$ (in $\mathcal{R}$).

Wij geven nu een voorbeeld van een cyclische code.

Zij $\mathbb{F} = \mathbb{F}_2$ en $n = 7$. De ontbinding van x^n-1 in irreducibele faktoren is:

$$x^n-1 = (x+1)(x^3+x^2+1)(x^3+x+1).$$

Als $g(x) = x^3+x+1$, dan

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

Nu is $h(x) = (x+1)(x^3+x^2+1) = x^4 + x^2 + 1$, dus:

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

d.w.z. $Rg(x)$ is equivalent met de (7,4)-Hamming-code.

De duale code van de maximale cyclische code $Rf_i(x)$ heeft $f_i(x)$ als check polynoom. Deze code heet een *minimale* cyclische code of *irreducibele* cyclische code. Een minimale cyclische code is een lichaam. Om dit in te zien is het voldoende om te bewijzen dat twee codewoorden a(x) en b(x) alleen product 0 kunnen hebben als een factor 0 is (zie (0.1.5)). Maar $a(x)b(x) = 0$ in R betekent dat in R een van de factoren bijv. a(x) door $f_i(x)$ deelbaar is. Daar ieder codewoord deelbaar is door $(x^n-1)/f_i(x)$ is $a(x) = 0$. Als eenvoudigste voorbeeld kiezen we $n = 2^k-1$ en nemen voor f(x) een irreducibel polynoom van de graad k. Laat $x^n-1 = g(x)f(x)$. De code $Rg(x)$ heeft dimensie k en bestaat dus uit 2^k woorden. Daarbij zijn $\underline{0}$ en de n cyclische permutaties van g(x) en dus blijkbaar geen andere woorden. Dit betekent dat ieder tweetal cyclische permutaties van g(x) als verschil weer een cyclische permutatie heeft! Deze code heeft dus de eigenaardige eigenschap dat ieder tweetal woorden dezelfde afstand heeft. Zo'n code heet *equidistant*. In het geval van ons voorbeeld moet de afstand dan 2^{k-1} zijn (zie § 2.2).

5.3. NULPUNTEN VAN EEN CYCLISCHE CODE

Zij β_i een nulpunt van f_i in een uitbreidingslichaam van IF. Dan is:

$$Rf_i(x) = \{v(x) \mid v(\beta_i) = 0\}$$

(want f_i is het minimaalpolynoom van β_i).
Algemeen kan een cyclische code V gespecifieerd worden door een aantal nulpunten voor te schrijven:

$$V = \{v(x) \mid v(\beta_1) = v(\beta_2) = \ldots = v(\beta_\ell) = 0\}$$

waarbij $\beta_1,\beta_2,\ldots,\beta_\ell$ n-de eenheidswortels zijn. De generator van V is nu het k.g.v. van de minimaalpolynomen van de β_j's. Omgekeerd, als g(x) de generator is van een cyclische code V en $g(x) = \prod_{i\in J} f_i(x)$ $(J \subset \{1,\ldots,t\})$ en β_i is een nulpunt van $f_i(x)$ $(i\in J)$, dan is $V = \{v(x) \mid v(\beta_i) = 0$ voor iedere $i \in J\}$.

Als we β uit het uitbreidingslichaam $GF(q^m)$ kiezen, dan kan β opgevat worden als kolomvector $\underline{\beta}$ ter hoogte m over GF(q) (uitgeschreven op een willekeurige basis). De eis $v(\beta) = 0$ wordt nu: $vH^T = 0$, met $H = (\underline{1}\ \underline{\beta}\ \underline{\beta}^2\ \ldots\ \underline{\beta}^{n-1})$. Bij meer β's, krijgen we meer rijen in H. Deze hoeven overigens niet lineair onafhankelijk te zijn.

Als voorbeeld van een toepassing geven we de volgende stelling.

(5.3.1) STELLING. *Zij* $n = \frac{q^m-1}{q-1}$ *en zij* β *een primitieve* n*-de eenheidswortel in een uitbreidingslichaam van* GF(q). *Dan is de cyclische code* $V = \{v(x) \mid v(\beta) = 0\}$ *(equivalent met) de* (n,n-m)*-Hamming-code over* GF(q) *als en slechts als* (m,q-1) = 1.

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

BEWIJS VAN DE STELLING

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

$$\beta^1,\beta^2,\ldots,\beta^{n-1} \notin GF(q).$$

Nu geldt: $\beta^1,\beta^2,\ldots,\beta^{n-1} \notin GF(q) \iff (m,q-1) = 1$.
Immers, (m,q-1) = (n,q-1), want:

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

Verder zijn de volgende beweringen equivalent.

$\forall\ i \in \{1,\ldots,n-1\}$: $\beta^i \notin GF(q)$.

$\forall\ i \in \{1,\ldots,n-1\}$: $\beta^{i(q-1)} \neq 1$,

$\forall\ i \in \{1,\ldots,n-1\}$: $n \nmid i(q-1)$,

$(n,q-1) = (m,q-1) = 1$. □

5.4. DE IDEMPOTENT VAN EEN CYCLISCHE CODE

(5.4.1) STELLING. *Zij* V *een cyclische code. Dan bevat* V *een (uniek bepaald) codewoord* c(x) *dat een eenheidselement is voor* V, *d.w.z. als* $v(x) \in V$, *dan* $c(x)v(x) = v(x)$.

BEWIJS. Zij g(x) de generator en h(x) het check-polynoom voor V (d.w.z. $g(x)h(x) = x^n-1$). Omdat x^n-1 geen meervoudige wortels heeft geldt $(g(x),h(x)) = 1$. Dus zijn er polynomen a(x) en b(x) zo dat $a(x)g(x) + b(x)h(x) = 1$. Definieer nu: $c(x) := a(x)g(x) = 1 - b(x)h(x)$. Als $v(x) = k(x)g(x)$ een codewoord in V is dan volgt:

$$c(x)v(x) = k(x)g(x) - k(x)g(x)b(x)h(x) = k(x)g(x) = v(x) \text{ in } \mathcal{R}.$$

Dus c(x) is inderdaad een eenheidselement in V en daarom uniek bepaald. □

In het bijzonder geldt: $c^2(x) = c(x)$; daarom heet c(x) de *idempotent* van V. Ook geldt dat c(x) de code genereert, omdat iedere $v(x) \in V$ een veelvoud van c(x) is (want $v(x) = v(x)c(x)$).

5.5. BCH-CODES

Een klasse van cyclische codes vormen de zgn. BCH-codes, ontdekt door BOSE & RAY-CHAUDHURI en HOCQUENGHEM.

Zij $\mathcal{R} = \mathcal{R}^{(n)} = \mathbb{F}[x]/(x^n-1)$ en laat $(n,q) = 1$ en $\mathbb{F} = \mathbb{F}_q$. Zij m het kleinste positieve gehele getal zo dat $n \mid q^m-1$ en zij β een primitieve n-de eenheidswortel in $GF(q^m)$ (dit is het kleinste uitbreidingslichaam van GF(q) met een primitieve n-de eenheidswortel). Zij g(x) het k.g.v. van de

minimale polynomen van $\beta,\beta^2,\ldots,\beta^{d-1}$. Dan heet de cyclische code $\bar{R}$ g(x) een *BCH-code* met *ontwerp-afstand* d. Dit is dus de code:

$$\{v(x) \mid v(\beta) = v(\beta^2) = \ldots = v(\beta^{d-1}) = 0\} \text{ (zoals in § 5.3).}$$

Als $n = q^m-1$ dan heet de code een *primitieve BCH-code*.

De minimum afstand van een BCH-code behoeft niet gelijk te zijn aan de ontwerp-afstand, maar kan niet kleiner zijn:

(5.5.1) STELLING. *De minimum afstand van een* BCH-*code met ontwerp-afstand* d *is ten minste* d.

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

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

Iedere β^i hierin stelt een kolom ter hoogte m voor als beschreven in 5.3. Dan is $\underline{v} = (v_0,\ldots,v_{n-1})$ in de code als en alleen als $\underline{v}H^T = \underline{0}$. We bewijzen nu dat iedere d-1 kolommen lineair onafhankelijk zijn; dan heeft ieder codewoord $\underline{v} \neq \underline{0}$ een gewicht groter dan d-1.
Neem de kolommen met bovenaan resp. $\xi_1,\ldots,\xi_{d-1}$ (onderling verschillend). Dan is de submatrix bestaande uit deze kolommen:

$$\begin{pmatrix} \xi_1 & \ldots & \xi_{d-1} \\ \xi_1^2 & \ldots & \xi_{d-1}^2 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \xi_1^{d-1} & \ldots & \xi_{d-1}^{d-1} \end{pmatrix}$$

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

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

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

In het algemeen is het vinden van de feitelijke minimum afstand een moeilijk probleem. Niet altijd is de minimum afstand gelijk aan de ontwerp-afstand. Zij bijvoorbeeld $n = 31$, $m = 5$ $q = 2$ en $d = 8$. Zij β een primitieve n-de eenheidswortel in $GF(2^5)$. Dan hebben β, β^2, β^4, β^8 en β^{16} hetzelfde minimale polynoom. Evenzo hebben β^5, β^{10}, β^{20}, β^9, β^{18} hetzelfde minimale polynoom. Zij $g(x)$ het produkt (zonder faktor-herhaling) van de minimale polynomen van β, β^2, β^3, β^4, β^5, β^6, β^7. Dan is $\mathcal{R}g(x)$ de BCH-code met ontwerp-afstand 8. Maar ook is $g(x)$ het produkt (zonder faktor-herhaling) van de minimale polynomen van β, β^2, β^3, β^4, β^5, β^6, β^7, β^8, β^9, β^{10}; dus $\mathcal{R}g(x)$ is ook de BCH-code met ontwerp-afstand 11. D.w.z. de minimale afstand van de code is ten minste 11.

Men noemt (5.5.1) ook wel de BCH-*grens* voor de minimum afstand van een cyclische code. De stelling geldt onveranderd als de $d-1$ opeenvolgende machten van β niet bij β^1 beginnen. De volgende stelling van HARTMANN en TZENG (1972) is een uitbreiding.

(5.5.2) STELLING. *Zij* C *een cyclische code met woordlengte* n *over* $\mathbb{F}_q$ *en voortbrenger* $g(x)$. *Zij* β *een primitieve* n*-de eenheidswortel in* $GF(q^m)$. *Als* $(n,c_1) = (n,c_2) = 1$ *en* $g(\beta^{\ell+i_1c_1+i_2c_2}) = 0$ $(i_1 = 0,1,\ldots,d_0-2;\ i_2 = 0,1,\ldots,s)$ *dan geldt voor de minimum afstand* d *van* C

$$d \geq d_0 + s.$$

BEWIJS. Volgens de BCH-grens is $d \geq d_0$. Zij $d_0 \leq w < d_0 + s$. Neem aan dat

$$v(x) := 1 + \sum_{i=1}^{w-1} Y_i x^{a_i}$$

een codewoord van gewicht w is $(Y_i \in \mathbb{F}_q\setminus\{0\}, 1 \leq a_1 < a_2 < \ldots < n)$.
Zij $X_i := \beta^{a_i}$, $S_j := \sum_{i=1}^{w-1} Y_i X_i^j = -1 + v(\beta^j)$.

We definieren

$$\sigma_1(x) := \prod_{i_1=1}^{d_0-2} (x-X_{i_1}^{c_1}) = \sigma_0^{(1)} x^{d_0-2} + \sigma_1^{(1)} x^{d_0-3} + \ldots + \sigma_{d_0-3}^{(1)} x + \sigma_{d_0-2}^{(1)}$$

(met $\sigma_0^{(1)} = 1$), en

$$\sigma_2(x) := \prod_{i_2=d_0-1}^{w-1} (x-X_{i_2}^{c_2}) = \sigma_0^{(2)} x^{w-d_0+1} + \sigma_1^{(2)} x^{w-d_0} + \ldots + \sigma_{w-d_0}^{(2)} x + \sigma_{w-d_0+1}^{(2)}$$

(met $\sigma_0^{(2)} = 1$), en verder

$$\sigma(x) := \sigma_1(x)\sigma_2(x).$$

Daar $a_i \neq 0$, $(n,c_1) = (n,c_2) = 1$, is $X_i \neq 1$, $X_{i_1}^{c_1} \neq 1$ $(i_1=1,2,\ldots,d_0-2)$, $X_{i_2}^{c_2} \neq 1$ $(i_2=d_0-1,\ldots,w-1)$. Dus is $\sigma(1) \neq 0$. Nu is

$$\text{(5.5.3)} \qquad \sum_{j=0}^{w-d_0+1} \sigma_j^{(2)} \sum_{k=0}^{d_0-2} \sigma_k^{(1)} S_{\ell+(d_0-2-k)c_1+(w-d_0+1-j)c_2} = \sum_{i=1}^{w-1} Y_i X_i^{\ell} \sigma_1(X_i^{c_1})\sigma_2(X_i^{c_2}) = 0.$$

Uit de definitie van S_1 en het gegeven volgt echter dat $S_{\ell+i_1c_1+i_2c_2} = -1$ voor $i_1 = 0,1,\ldots,d_0-2$ en $i_2 = 0,1,\ldots,s$. Dan staat in (5.5.3) echter $\sigma(1) = 0$, een tegenspraak. De aanname was dus onjuist. □

VOORBEELD. Zij $n = 51$, $g(x) := m_1(x)m_9(x)$. De nulpunten β^i van $g(x)$ hebben resp. $i = 1,2,4,8,16,32,13,26$ en $9,18,36,21,42,33,15,30$. De dimensie van de code is 35. Volgens (5.5.1) is $d \geq 3$. Volgens (5.5.2) is echter $d \geq 5$ omdat we met $i = 1,2,8,9,15,16$ blijkbaar $\ell = 1$, $c_1 = 1$, $c_2 = 7$ kunnen nemen in stelling (5.5.2).

5.6. EEN PROCEDURE VOOR HET CORRIGEREN VAN FOUTEN BIJ BCH-CODES

Stel dat een codewoord $C(x)$ van een BCH-code (met ontwerp-afstand $d \geq 2t + 1$, ter lengte n, over het lichaam $GF(q)$, en m en β als in § 5.5) wordt verzonden en een woord: $R(x) = R_0 + R_1x + \ldots + R_{n-1}x^{n-1}$ wordt ontvangen. Zij $E(x) = R(x) - C(x) = E_0 + E_1x + \ldots + E_{n-1}x^{n-1}$ het foutenpatroon. Definieer voorts:

$M := \{i \mid E_i \neq 0\}$, de verzameling posities waar een fout is gemaakt;

$e := |M|$, het aantal fouten;

$\sigma(z) := \prod_{i\in M} (1-\beta^i z)$; dit polynoom heet het "error-locator polynomial";

$$\omega(z) := \sum_{i\in M} E_i\beta^i z \prod_{j\in M\setminus i} (1-\beta^j z).$$

Kennelijk is kennis van $\sigma(z)$ en $\omega(z)$ voldoende om fouten te verbeteren:

als $\sigma(\beta^{-i}) \neq 0$, dan is op de i-plaats geen fout gemaakt;

als $\sigma(\beta^{-i}) = 0$, dan is de fout $E_i = \dfrac{-\omega(\beta^{-i})}{\sigma'(\beta^{-i})} \cdot \beta^i$.

Natuurlijk kunnen we alleen voor $e \leq t$ verwachten dat $E(x)$ bepaald kan worden (en daarmee $C(x)$). Neem dus aan dat $e \leq t$, dan zal blijken hoe $E(x)$ gevonden kan worden m.b.v. relatief eenvoudige operaties (het oplossen van een stelsel lineaire vergelijkingen over $GF(q)$).

We berekenen hiertoe:

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

$$= \sum_{\ell=1}^{\infty} z^\ell E(\beta^\ell).$$

Voor $1 \leq \ell \leq 2t$ is $E(\beta^\ell) = R(\beta^\ell)$, dus aan de ontvanger van het codewoord bekend. D.w.z. $\dfrac{\omega(z)}{\sigma(z)}$ is bekend modulo z^{2t+1}. De kunst is nu om polynomen $\sigma(z)$ en $\omega(z)$ met graad $\omega(z) \leq$ graad $\sigma(z)$ en graad $\sigma(z)$ minimaal te vinden, zó dat:

$$\frac{\omega(z)}{\sigma(z)} = \sum_{\ell=1}^{2t} z^\ell R(\beta^\ell) \pmod{z^{2t+1}}.$$

Zij $S_\ell = E(\beta^\ell) = R(\beta^\ell)$ voor $\ell = 1,\ldots,2t$, en zij $\sigma(z) = \sum_{i=0}^{e} \sigma_i z^i$. Dan is:

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

Daar $\omega(z)$ de graad e heeft, volgt:
$\sum_{i+\ell=k} S_\ell \sigma_i = 0$ voor $e + 1 \le k \le 2t$. Dit zijn 2t-e vergelijkingen voor de e onbekenden $\sigma_1,\ldots,\sigma_e$ (want $\sigma_0 = 1$ is bekend). Als $e \le t$ dan heeft dit stelsel hooguit één oplossing: stel $\tilde{\sigma}(z) = \sum_{i=0}^{e} \tilde{\sigma}_i z^i$ is een oplossing (met $\tilde{\sigma}_0 = 1$); dan volgt voor $e + 1 \le k \le 2t$:

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

Dit zijn 2t-e vergelijkingen voor de e onbekenden $E_i\tilde{\sigma}(\beta^{-i})$. Vanwege Vandermonde is de oplossing uniek, d.w.z. $\forall\, i \in M$ geldt: $E_i\tilde{\sigma}(\beta^{-i}) = 0$. Nu is $E_i \neq 0$, d.w.z. $\tilde{\sigma}(x)$ heeft als nulpunten: β^{-i} $(i\in M)$; dus $\tilde{\sigma} = \sigma$.
Dus als we polynomen $\omega(z)$ en $\sigma(z)$ van zo laag mogelijke graad gevonden hebben, dan zijn dit de gevraagde $\omega(z)$ en $\sigma(z)$.

5.7. REED-SOLOMON CODES

Een *Reed-Solomon code* of *RS-code* is een primitieve BCH-code waarbij $m = 1$, $n = q-1$. De code wordt voortgebracht door het polynoom $g(x) = \prod_{i=1}^{d-1} (x-\alpha^i)$ uit GF(q)[x]. Op grond van (5.5.1) is de minimum afstand van de code ten minste d. De code heeft dimensie $k = n-d+1$ en dus op grond van (4.3.2) een minimum afstand ten hoogste d. We zien dus dat d de minimum afstand is en dat de code optimaal is (vgl. (4.1.1)).

De RS-codes worden o.a. gebruikt voor de verbetering van zgn. "burst-errors", dat zijn intervallen uit de ontvangen rij symbolen met veel fouten er in (veroorzaakt door een storing op het kanaal). Een RS-code met $q = 2^r$ kunnen we opvatten als binaire code met woordlengte $r(2^r-1)$ en dimensie rk. Als een burst-error fouten veroorzaakt op een traject ter lengte $b \le ([d/2]-1)r + 1$ dan worden van de oorspronkelijke RS-code niet meer dan $[d/2]$ symbolen veranderd. De fout kan dus gecorrigeerd worden. Dezelfde gedachte is de basis van de zgn. *concatenated codes* (cf. Hfdst. IX).

5.8. KWADRAATREST-CODES

Zij n een oneven priemgetal, zódat q een kwadraatrest modulo n is, d.w.z. $\exists x$: $x^2 \equiv q \pmod{n}$. Dit is hetzelfde als: $q^{\frac{1}{2}(n-1)} \equiv 1 \pmod{n}$ (zie § 0.2). Zij α een primitieve n-de eenheidswortel in een uitbreidingslichaam van GF(q). Zij R_0 de verzameling van alle kwadraatresten modulo n:

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

en R_1 de verzameling van alle niet-kwadraatresten modulo n:

$$R_1 = GF(n) \setminus \{0\} \setminus R_0.$$

Definieer verder:

$$g_0(x) := \prod_{r \in R_0} (x-\alpha^r) \text{ en } g_1(x) := \prod_{r \in R_1} (x-\alpha^r).$$

Dan geldt:

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

Merk op dat de eis dat q een kwadraatrest modulo n is equivalent is met de eis dat g_0 en g_1 polynomen over GF(q) zijn.

(5.8.1) DEFINITIE. De cyclische codes van lengte n over GF(q) met generatoren $g_0(x)$ en $(x-1)g_0(x)$ heten *kwadraatrest-codes* of *QR-codes*. De verlengde *QR-code* van lengte n+1 over GF(q) wordt verkregen door aan de code met generator $g_0(x)$ een extra parity-check symbool toe te voegen (zie (3.4.3)).

De code met generator $(x-1)g_0(x)$ bestaat uit alle woorden $(v_0,\ldots,v_{n-1})$ uit de code met generator $g_0(x)$ waarvoor geldt: $v_0+\ldots+v_{n-1} = 0$.
Door in de definitie g_0 door g_1 te vervangen krijgen we codes equivalent met de oorspronkelijke. Want zij j een niet-kwadraatrest modulo n. Dan definieert:

$$\pi_j(\ell) := j\ell \pmod{n},\ 0 \leq \pi_j(\ell) < n,$$

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

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

en: $R_0 = jR_1$, zijn de volgende beweringen equivalent:

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

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

Evenzo:

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

Over de gewichten van de woorden kan het volgende gezegd worden.

(5.8.2) STELLING. *Zij* $c(x)$ *een codewoord van* $Rg_0(x)$, *zo dat* $c(x) \notin R\cdot(x-1)g_0(x)$. *Zij* d *het gewicht van* $c(x)$. *Dan:*

(i) $d^2 \geq n$;
(ii) *als* $n \equiv -1 \pmod 4$, *dan* $d^2-d+1 \geq n$;
(iii) *als* $n \equiv -1 \pmod 8$, *en* $q = 2$, *dan* $d \equiv 3 \pmod 4$.

BEWIJS.
(i) Omdat $c(x) \in R\, g_0(x) \backslash R\,(x-1)g_0(x)$, geldt ook:

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

Dan:

$$g_0(x)g_1(x) \mid c(x)\pi_j c(x), \text{ en } (x-1) \nmid c(x)\pi_j c(x).$$

Dus:

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

Maar dan:

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

(ii) als $n \equiv -1 \pmod 4$ dan is -1 een niet-kwadraatrest, dus dan kunnen we $j = -1$ nemen. Maar dan dragen in het produkt $c(x)\pi_j c(x)$ de termen x en x^{-1}, resp. x^2 en x^{-2},..., resp. x^{n-1} en x^{-n+1}, alle bij tot dezelfde term. Dus dan:

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

(iii) Zij $c(x) = \sum_{i=1}^{d} x^{e_i}$. Dan
$c(x)\pi_{-1}c(x) = d + \sum_{i\neq j} x^{e_i - e_j}$. Als $e_i - e_j = e_k - e_\ell$ dan vallen de twee termen $x^{e_i-e_j}$ en $x^{e_k-e_\ell}$ tegen elkaar weg. Maar dan vallen ook $x^{e_j-e_i}$ en $x^{e_\ell-e_k}$ tegen elkaar weg. Dus het aantal wegvallende termen is een viervoud, zeg $4b$.

Dan:

$d^2-d+1-4b = n$, of: $d \equiv 3 \pmod 4$ (d is oneven, omdat $c(x) \notin R\,(x-1)g_0(x)$). □

Het kan bewezen worden dat elke verlengde binaire QR-code met woordlengte $n + 1$ en posities geindiceerd met $PG(1,n) = \mathbb{F}_n \cup \{\infty\}$ invariant is onder de werking op de posities van de 2-voudig transitieve groep $PSL(2,n) := \{x \mapsto \frac{ax+b}{cx+d} \mid ad-bc = 1\}$ (zie VAN LINT 1971)). Hieruit volgt eenvoudig dat een binaire QR-code oneven minimum gewicht heeft, zodat de bovenstaande stelling gebruikt kan worden om ondergrenzen voor de minimum afstand van een QR-code te vinden.

VOORBEELDEN

(5.8.3) Neem $q = 2$, $n = 7$ en generator $g_0(x)$ (zodat $k = 4$). Stelling (5.8.2) levert $d \geq 3$ maar $(1+7)\cdot 2^4 = 2^7$ dus de QR-code met deze parameters is 1-perfect. (In feite is het natuurlijk de (7,4)-Hamming code, zie § 2.1 en § 2.4).

In dit voorbeeld was $g(x) = x + x^2 + x^4$ en $h(x) = 1 + x + x^2 + x^4 = 1 + g(x)$. Dit verschijnsel is algemeen in het binaire geval:

Bekijk $g(x) = \sum_{r\in R_0} x^2$. Er geldt $g(x^i) = g(x) \pmod{x^n-1}$ als $i \in R_0$, en in het bijzonder $g(x)^2 = g(x) \pmod{x^n-1}$. Voorts is voor $j \in R_1$: $g(x^j) + g(x) = \sum_{r=1}^{n-1} x^r \pmod{x^n-1}$. Als dus α een primitieve n-de eenheidswortel is (in een uitbreidingslichaam van GF(2)) dan is $g(\alpha^i) \in GF(2)$ en de afbeelding $i \mapsto g(\alpha^i)$ is constant op R_0 en op R_1 d.w.z. òf $g_0(x) \mid g(x)$ òf $g_1(x) \mid g(x)$. Bij passende keuze van α volgt $g_0(x) \mid g(x)$ zodat $g(x)$ een idempotent van de code $Rg_0(x)$ is. Aangezien $x^n-1 = (x-1)g_0(x)g_1(x)$ en $(g_1(x), g(x)) = 1$ is de cyclische code met generator $g(x)$ òf $Rg_0(x)$ òf $Rg_0(x)(x-1)$. Nu is $g(1) = \frac{n-1}{2}$ dus het eerste geval treedt op als $n \equiv -1 \pmod 8$ en het tweede als $n \equiv 1 \pmod 8$. [Merk op dat de eis dat 2 een kwadraatrest mod n is impliceert dat $n \equiv \pm 1 \pmod 8$.] Tenslotte volgt $g(x)\cdot(1+g(x)) = 0 \pmod{x^n-1}$ zodat $h(x) = 1 + g(x)$.

(5.8.4) Neem $q = 2$, $n = 23$ en generator $g_0(x)$ (zodat $k = 12$). Stelling (5.8.2) levert tezamen met de wetenschap dat d oneven is dat $d \geq 7$. Echter $(1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3})\cdot 2^{12} = 2^{23}$ dus de QR-code met deze parameters is 3-perfect. (In feite is het natuurlijk de (23,12)-binaire Golay code, zie § 2.3.)

(5.8.5) Neem $q = 3$, $n = 11$ en generator $g_0(x)$ (zodat $k = 6$). Nu vinden we de 2-perfecte (11,6)-ternaire Golay code (zie § 2.4).

Deze voorbeelden zouden de indruk kunnen wekken dat alle QR-codes perfect zijn, maar dat is natuurlijk geenszins het geval (zie opgave (5.10.5)); algemeen geldt dat QR-codes vaak goed zijn, maar moeilijk te decoderen.

5.9. COMMENTAAR

Het idee van cyclische codes kan gegeneraliseerd worden. Men kan bijvoorbeeld bij vaste ξ eisen dat met $(a_0, a_1, \ldots, a_{n-1})$ uit C ook $(\xi a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ in de code zit. Men noemt zo'n code *constacyclisch* (als $\xi = -1$ ook wel *negacyclisch*). De theorie is geheel analoog (zie BERLEKAMP (1968)). Voor een toepassing van idempotenten verwijzen we naar VAN LINT (1971) § 3.3. De procedure uit § 5.6 is een generalisatie van een door BERLEKAMP bedacht algorithme dat reeds practische toepassing vindt.

Voor meer theorie over QR-codes en diverse toepassingen in de combi-

natoriek verwijzen we naar CAMERON & VAN LINT (1975) en de twee hierboven genoemde boeken.

5.10. OPGAVEN

(5.10.1) Construeer een ternaire BCH-code met lengte 26 en ontwerp-afstand 5.

(5.10.2) Bepaal de idempotent van de (15.11)-Hamming code.

(5.10.3) Zij α een primitief element van $GF(2^5)$ met $\alpha^5 = \alpha^2 + 1$. Bij gebruik van een BCH-code met ontwerp afstand 5 ontvangen we

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

Bepaal met de algorithme van 5.6 het verzonden codewoord.

(5.10.4) Bepaal de ternaire QR-code met lengte 11 en toon aan dat dit een perfecte code is! Laat zien dat deze code equivalent is met de in § 2.4 geconstrueerde.

(5.10.5) Behalve de onder (5.8.3) - (5.8.5) genoemde QR-codes is er nog een perfecte QR-code. Welke?

(5.10.6) Zij $n = 4$, $q = 5$, $d = 3$. Kies $\alpha = 2$ als primitief element van $GF(5)$. Construeer de RS-code C met minimum afstand d voor deze parameters. Bewijs dat de matrices A en B gedefinieerd door $(i,j,a_{ij},b_{ij}) \in C$ orthogonale latijnse vierkanten zijn.

(5.10.7) Generaliseer de resultaten uit § 5.8 zoveel mogelijk tot e-de graads resten; de voorwaarden worden nu: n priem, $e \mid n-1$, $q^{\frac{n-1}{e}} \equiv 1 \pmod{n}$.

(a) Bewijs als generalisatie van (5.8.2) (i) dat $d^e > n$.

(b) Bepaal de generator en de minimum afstand van de kubische rest code voor $n = 31$.

(5.10.8) Bepaal de minimum afstand van de binaire kwadraatrest code met $n = 47$.

(5.10.9) Zij m oneven, $n = 2^m-1$, α primitief element van $GF(2^m)$. Zij $g(x)$ een deler van x^n-1 en $g(\alpha) = g(\alpha^5) = 0$. Bewijs dat de cyclische

code voortgebracht door $g(x)$ minimum afstand ≥ 4 heeft en wel

(a) door aan te tonen dat $1 + \xi + \eta = 0$ en $1 + \xi^5 + \eta^5 = 0$ met ξ en η in $GF(2^m)$ niet mogelijk is.

(b) door toepassing van een stelling.

(5.10.10) Zij C een BCH-code met ontwerpafstand d. Bewijs dat de minimum afstand van de verlengde code $\overline{C}$ tenminste d + 1 is.