Hoofdstuk X

ARITHMETISCHE CODES

10.1. AN-CODES

Arithmetische codes zijn bestemd voor het controleren van rekenkundige bewerkingen, in het bijzonder optelling en aftrekking. De te bewerken getallen dient men zich hierbij voor te stellen als geschreven in het r-tallig stelsel, waar r een vast geheel getal ≥ 2 is. Het binaire (r=2) en het decimale (r=10) geval zijn van overwegend praktisch belang.

Arithmetische codes verschillen van de andere in deze syllabus behandelde codes door de keuze van de *afstandsfunctie*. Hamming-afstand is minder geschikt voor het doel: één enkele vergissing bij een optelling kan immers verscheidene foute cijfers in de uitkomst tot gevolg hebben, zodat de Hamming-afstand tussen het juiste antwoord en de verkregen uitkomst geen ondergrens is voor het aantal gemaakte fouten.

Een afstandsbegrip dat beter overeenkomt met het soort fouten dat men verwacht wordt als volgt verkregen. Het *arithmetische gewicht* w(x) van een geheel getal x is per definitie het kleinste getal $t \geq 0$ waarvoor er een representatie

$$x = \sum_{i=1}^{t} a_i r^{n(i)} \tag{10.1.1}$$

met

$$a_i,\ n(i) \in \mathbb{Z},\ |a_i| < r,\ n(i) \geq 0$$

(i=1,...,t) bestaat. De *arithmetische afstand* d(x,y) tussen twee gehele getallen x en y is gedefinieerd door

$$d(x,y) = w(x-y).$$

Men gaat gemakkelijk na dat d een metriek op $\mathbb{Z}$ is. Maakt men $\mathbb{Z}$ tot verzameling hoekpunten van een graph door x en x' te verbinden als

$$|x-x'| = c.r^i \text{ voor een } c \in \{1,2,\ldots, r-1\},\ i \in \mathbb{Z}_{\geq 0},$$

dan is de arithmetische afstand tussen twee gehele getallen gelijk aan hun afstand in deze graph. Arithmetische afstand is translatie-invariant: $d(x,y) = d(x+z,y+z)$ voor alle $x,y,z \in \mathbb{Z}$. Deze eigenschap heeft Hamming-afstand niet. Merk op dat de arithmetische afstand tussen twee niet-negatieve gehele getallen kleiner dan of gelijk aan hun Hamming-afstand is.

We zullen codes beschouwen van de vorm

$$C = \{AN \mid N \in \mathbb{Z}, 0 \leq N < B\}$$

waar A en B vaste positieve gehele getallen zijn; zulke codes heten *AN-codes*. Het gebruik van zo'n code moet men zich als volgt voorstellen. Om twee getallen N_1 en N_2 (niet negatief, en niet te groot t.o.v. B) op te tellen codeert men ze als AN_1 resp. AN_2. Vervolgens berekent men de som van AN_1 en AN_2; noem de uitkomst S. Als alles goed is gegaan is S een A-voud, en de som van N_1 en N_2 is dan S/A. Als S geen A-voud is, heeft men bij de optelling een vergissing gemaakt. Men bepaalt dan $AN_3 \in C$ met minimale $d(AN_3, S)$; het aantal gemaakte vergissingen is dan ten minste $d(AN_3,S)$, en de meest waarschijnlijke uitkomst voor $N_1 + N_2$ is N_3.

Opdat men op deze wijze alle ten hoogste e-voudige fouten kan corrigeren is nodig en voldoende dat geldt

$$d(AN,AN') \geq 2e + 1$$

voor alle $AN, AN' \in C$, $AN \neq AN'$. Dit is kennelijk hetzelfde als

$$w(AN) \geq 2e + 1 \text{ voor alle } AN \in C, AN \neq 0.$$

De tot nog toe gebruikte eigenschappen van C zijn voornamelijk te danken aan de gelijkenis van C met de ondergroep

$$H = \{AN \mid N \in \mathbb{Z}\};$$

vergelijk dit met de prominente plaats die *lineaire* codes in de codetheorie innemen. Het is helaas niet zinvol C = H te nemen, want er geldt

$$\min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\} \leq 2$$

voor alle $A \in \mathbb{Z}$ (zie (10.6.1)).

Dit ongemak omzeilen we door *modulaire* AN-codes te beschouwen. Zetten we, met A, B, C als boven,

$$m = AB,$$

dan kunnen we C opvatten als *ondergroep* van $\mathbb{Z}/m\mathbb{Z}$ (de gehele getallen modulo m). We moeten dan wel ons afstandsbegrip aanpassen. Hiertoe maken we $\mathbb{Z}/m\mathbb{Z}$ tot verzameling hoekpunten van een graph door (x mod m) en (x' mod m) te verbinden met een kant als

$$x - x' \equiv \pm c.r^j \pmod m$$

voor zekere $c,j \in \mathbb{Z}$, $0 < c < r$, $j \geq 0$. De *modulaire afstand* $d_m(\bar{x},\bar{y})$ tussen twee elementen $\bar{x},\bar{y}$ van $\mathbb{Z}/m\mathbb{Z}$ is dan de afstand tussen $\bar{x}$ en $\bar{y}$ in deze graph, en het *modulaire gewicht* $w_m(\bar{x})$ is gedefinieerd door $w_m(\bar{x}) = d_m(\bar{x},(0 \bmod m))$. Voor $x,y \in \mathbb{Z}$ schrijven we in plaats van $d_m((x \bmod m), (y \bmod m))$ en $w_m((x \bmod m))$ ook wel $d_m(x,y)$ en $w_m(x)$. Merk op dat geldt

$$w_m(x) = \min\{w(y) \mid y \in \mathbb{Z}, y \equiv x \pmod m\}$$

$$d_m(x,y) = w_m(x-y).$$

De code C kan nu gebruikt worden om twee getallen N_1 en N_2 modulo B op te tellen. Hierbij kunnen alle combinaties van ten hoogste e fouten hersteld worden dan en slechts dan als geldt

$$d_{min}(C) \geq 2e + 1$$

waar $d_{min}(C)$ de *minimum-afstand* van de code is:

$$d_{min}(C) = \min\{w_m(x) \mid x \in C, x \not\equiv (0 \bmod m)\}.$$

Niet iedere keuze voor m is zinvol. Als bijvoorbeeld m een priemgetal is waarvoor r een primitieve wortel is, dan geldt $w_m(x) \leq 1$ voor alle $x \in \mathbb{Z}$. Wij zullen ons in het vervolg beperken tot getallen van de vorm

$$m = r^n - 1, \; n \in \mathbb{Z}, \; n \geq 2.$$

Deze keuze is voor de praktijk van belang, aangezien vele computers modulo 2^n-1 rekenen.

Elk geheel getal x kan modulo r^n-1 eenduidig geschreven worden als

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{(r^n-1)}$$

met $c_i \in \{0,1,\ldots,r-1\}$ $(0 \le i < n)$, niet alle $c_i = 0$. Dus $\mathbb{Z}/(r^n-1)$ is op te vatten als de verzameling woorden ter lengte n gevormd uit r letters, met uitzondering van het woord 00...0.

Deze laatste uitzondering zou overbodig geweest zijn als we hadden genomen $m = r^n$; dit is voor de praktijk eveneens een zinvolle keuze, daar ook vele computers modulo 2^n rekenen. Goede codes zijn voor $r = 2$, $m = 2^n$ echter niet te verwachten: uit $AB = m = 2^n$ volgt immers $A = 2^k$ voor zekere k, en de code bestaat dan uit de getallen

$$\sum_{i=0}^{n-1} c_i 2^i, \quad c_i \in \{0,1\}$$

waarvoor $c_0 = \ldots = c_{k-1} = 0$; het coderen van een getal $\sum_{i=0}^{n-k-1} d_i 2^i$ modulo B $(=2^{n-k})$ $(d_i \in \{0,1\})$ bestaat dan uit het achterplaatsen van k nullen, die niet eens een parity-check functie vervullen! Analoge bezwaren zijn er voor algemene r.

In het vervolg verstaan we onder een *cyclische AN-code* een ondergroep C van $\mathbb{Z}/(r^n-1)$; hieris n een geheel getal ≥ 2, de *woordlengte* van de code. Bij zo'n C is er steeds een eenduidig bepaald paar natuurlijke getallen A, B met

$$AB = r^n-1$$

$$C = \{(AN \bmod (r^n-1)) \mid N \in \mathbb{Z},\ 0 \le N < B\}.$$

We noemen A de *voortbrenger* van de code. We zijn primair geinteresseerd in codes waarvan de *rate* $\frac{1}{n} \cdot {}^r\log B$ en de minimum-afstand "groot" zijn.

Als abelse groep is C cyclisch van orde B. De benaming "cyclische AN-code" slaat echter op een andere eigenschap, die doet denken aan de cy-

clische codes over eindige lichamen: is $(x \bmod (r^n-1))$ een element van C,

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{(r^n-1)},$$

dan geldt

$$rx \equiv \sum_{i=0}^{n-1} c_{i-1} r^i \pmod{(r^n-1)}$$

(indices modulo n), en $(rx \bmod (r^n-1))$ is een element van C omdat C een ondergroep is. Dus de "cyclische opschuiving" van een codewoord behoort weer tot de code. De analogie met cyclische codes over eindige lichamen gaat verder: een cyclische AN-code is een ideaal van de ring $\mathbb{Z}/(r^n-1)$, een cyclische code over GF(q) is niets anders dan een ideaal in $GF(q)[x]/(x^n-1)$. Verder kan men r met x laten corresponderen, A met g(x) (= het voortbrengend polynoom van de code), en B met h(x) (het "check polynomial"). Op deze analogie komen we nog terug.

Men verkrijgt *negacyclische* AN-codes door $m = r^n + 1$ te nemen, en ondergroepen van $\mathbb{Z}/(r^n+1)$ te beschouwen. We laten het aan de lezer over, de resultaten van §§ 10.2 t/m 10.4 voor het negacyclische geval te formuleren en te bewijzen.

Referenties voor deze paragraaf: PETERSON & WELDON (1972), MASSEY & GARCIA (1972), RAO (1974) en de daar aangegeven literatuur. Deze auteurs beschouwen voornamelijk het binaire geval.

10.2. PERFECTE CYCLISCHE AN-CODES VAN ORDE 1

Zij $C \subset \mathbb{Z}/(r^n-1)$ een cyclische AN-code en e een geheel getal ≥ 1. We noemen C *perfect van orde e* als er voor elke $x \in \mathbb{Z}/(r^n-1)$ een eenduidig bepaald element $c \in C$ bestaat met $d_m(x,c) \leq e$; hier $m = r^n-1$. Zetten we

$$S_e = \{x \in \mathbb{Z}/(r^n-1) \mid w_m(x) \leq e\}$$

dan betekent dit dat elk element $x \in \mathbb{Z}/(r^n-1)$ een eenduidige voorstelling $x = c + y$, met $c \in C$, $y \in S_e$ heeft. Anders geformuleerd: de natuurlijke afbeelding

$$S_e \rightarrow (\mathbb{Z}/(r^n-1))/C \simeq \mathbb{Z}/A\mathbb{Z}$$

moet bijectief zijn. Hier geeft A de voorbrenger van de code aan, als in 10.1. Merk op dat een perfecte code van orde e alle ten hoogste e-voudige fouten kan corrigeren, dus $d_{min}(C) \geq 2e + 1$.

We beschouwen in deze paragraaf het geval e = 1. Dan geldt $d_{min}(C) \geq 3$. Heeft C meer dan één element, dan hebben we bovendien $d_{min}(C) \leq n$, dus we mogen ons beperken tot het geval $n \geq 3$. Het is eenvoudig na te gaan dat S_1 dan precies $1 + 2(r-1)n$ elementen heeft, namelijk

$$0 \bmod (r^n-1),$$

$$c.r^j \bmod (r^n-1),\ c,j \in \mathbb{Z},\ 0 < |c| < r,\ 0 \leq j < n.$$

De bijectie $S_1 \rightarrow \mathbb{Z}/A\mathbb{Z}$ levert dus $A = 1 + 2n(r-1)$, waaruit volgt dat $1 + 2n(r-1)$ een deler is van r^n-1 zodra er een perfecte code $C \subset \mathbb{Z}/(r^n-1)$ van orde 1 is: de "sphere packing condition".

(10.2.1) STELLING. (zie GOTO & FUKUMURA (1975)). *Stel* $C \subset \mathbb{Z}/(r^n-1)$ *is een perfecte cyclische AN-code van orde 1 met voortbrenger* A *en woordlengte* $n \geq 3$. *Dan is* A *een priemgetal* $> r^2$, *de woordlengte* n *is oneven, en de ondergroep* $H \subset (\mathbb{Z}/A\mathbb{Z})^*$ (= *multiplicatieve groep van het lichaam* $\mathbb{Z}/A\mathbb{Z}$) *voortgebracht door* (r mod A) *heeft orde* n *en index* 2(r-1). *Bovendien vormen de elementen* ($\pm$ c mod A), c = 1,2,..., r - 1, *een volledig representantensysteem voor de nevenklassen van* H *in* $(\mathbb{Z}/A\mathbb{Z})^*$.

Omgekeerd, als A *een priemgetal* $> r^2$ *is met de eigenschap dat de ondergroep* $H \subset (\mathbb{Z}/A\mathbb{Z})^*$ *voortgebracht door* r *index* 2(r-1) *heeft, met* $\{\pm$ c mod A$|$ c = 1,2,...,r-1$\}$ *als volledig representantensysteem voor de nevenklassen, dan is de orde* n *van* H *oneven, en de ondergroep* C *van* $\mathbb{Z}/(r^n-1)$ *voortgebracht door* A mod(r^n-1) *is een perfecte cyclische AN-code van orde* 1.

WIJS. Als $A = r^n-1$ dan is $A > r^2$ duidelijk. Als $A < r^n-1$ dan is (A mod -1) een element ongelijk aan nul van C, dus $d_{min}(C) \geq 3$ impliceert A) $\geq w_m(A) \geq 3$, waaruit volgt $A > r^2$. Is A niet priem, dan A = k.l met l > 1; we mogen aannemen k > r. Wegens de bijectie $S_1 \rightarrow \mathbb{Z}/A\mathbb{Z}$ is er ecies één geheel getal van de vorm $c.r^j$, $c,j \in \mathbb{Z}$, $|c| < r, j \geq 0$ met $c.r^j$ mod A. Kennelijk $c \neq 0$. Er volgt $k|c.r^j$. Ook $k|A|r^n-1$, dus (k,r) =

$= 1$ en $k|c$. Dit is in tegenspraak met $k > r$, $0 < |c| < r$. Dus A is priem.

De bijectie $S_1 \longrightarrow \mathbb{Z}/A\mathbb{Z}$ levert nu een bijectie

$$\{\pm\, c.r^j \mid c = 1,2,\ldots,r-1,\ j = 0,1,\ldots,n-1\} \longrightarrow (\mathbb{Z}/A\mathbb{Z})^*.$$

Het beeld van $\{r^j \mid j = 0,1,\ldots,n-1\}$ is net de ondergroep H voortgebracht door (r mod A), want $r^n \equiv 1 \bmod A$. Deze ondergroep heeft dus orde n, en kennelijk is $\{\pm\, c \bmod A \mid c = 1,2,\ldots,r-1\}$ een representantensysteem voor $(\mathbb{Z}/A\mathbb{Z})^*/H$. In het bijzonder geldt $(-1 \bmod A) \notin H$, dus de orde n van H is oneven. Dit bewijst de eerste helft van de stelling. De omkering laten we aan de lezer over. □

(10.2.2) GEVOLG (zie PETERSON & WELDON (1972)). *Stel* p *is een priemgetal* $\equiv 3 \pmod 4$ *waarvoor* -2 *een primitieve wortel is. Dan is de ondergroep* $C \subset \mathbb{Z}/(2^{\frac{1}{2}(p-1)}-1)$ *voortgebracht door* p mod $(2^{\frac{1}{2}(p-1)}-1)$ *een perfecte binaire cyclische AN-code van orde 1. Bovendien is elke perfecte binaire cyclische AN-code van orde 1 van deze vorm.*

BEWIJS. Dit volgt direkt uit (10.2.1). De voorwaarde op p is slechts een vertaling van de eis dat (2 mod p) $\in (\mathbb{Z}/p\mathbb{Z})^*$ een ondergroep van index 2 voortbrengt waar (-1 mod p) niet in zit. □

Priemgetallen p die aan de voorwaarden van (10.2.2) voldoen zijn bijvoorbeeld: p = 7 (levert een triviale code), p = 23, p = 47, p = 71, p = 79. Merk op dat p noodzakelijk 7 mod 8 is.

Priemgetallen p waarvoor 2 een primitieve wortel is geven aanleiding tot perfecte *negacyclische* codes, cf. PETERSON & WELDON (1972). Vergelijk dit met de cyclische beschrijving van binaire Hamming codes: is $g(x) \in GF(2)[x]$ een irreducibel polynoom zodat x een primitieve wortel mod g(x) is, dan brengt g(x) in $GF(2)[x]/(x^n-1)$, $n = 2^{\text{graad}(g)}-1$, een perfecte code van orde 1 voort.

Het volgende gevolg bewijst men als het vorige.

(10.2.3) GEVOLG (zie GRITSENKO (1969)). *Stel* p *is een priemgetal* $\equiv 5 \bmod 8$ *zodat* (3 mod p) $\in (\mathbb{Z}/p\mathbb{Z})^*$ *een ondergroep van index 4 voortbrengt. Dan brengt* (p mod $(3^{\frac{1}{4}(p-1)}-1)$) *een perfecte ternaire cyclische AN-code van orde 1 in* $\mathbb{Z}/(3^{\frac{1}{4}(p-1)}-1)$ *voort. Bovendien is elke perfecte ternaire cyclische AN-code van orde 1 van deze vorm.* □

Elk priemgetal p dat aan de voorwaarden van dit gevolg voldoet is congruent met 13 modulo 24; voorbeelden zijn p = 13, p = 109, p = 181.

Niet voor elke r bestaan er cyclische AN-codes van orde 1:

(10.2.4) GEVOLG (zie BOYARINOV & KABATYANSKY (1973)). *Er bestaat geen perfecte AN-code van orde 1 met* $r = 2^k$, $k \in \mathbb{Z}$, $k > 1$.

BEWIJS. Stel C is zo'n code, met voortbrenger A. Zij $H' \subset (\mathbb{Z}/A\mathbb{Z})^*$ voortgebracht door (r mod A) en (-1 mod A). Wegens de stelling heeft $(\mathbb{Z}/A\mathbb{Z})^*/H'$ orde $r - 1 = 2^k - 1$ en een volledig representantensysteem {(1 mod A), (2 mod A),...,(r-1 mod A)}. Hieruit ziet men dat de orde van het beeld van (2 mod A) in $(\mathbb{Z}/A\mathbb{Z})^*/H'$ gelijk is aan k. Omdat de orde van een element de orde van de groep deelt, volgt $k \mid 2^k - 1$. Zij nu q het kleinste priemgetal dat k deelt. Dan $2^k \equiv 1 \bmod q$, $2^{q-1} \equiv 1 \bmod q$ (Fermat), en $(k, q-1) = 1$, dus $2^1 \equiv 1 \bmod q$, tegenspraak. □

(10.2.5) GEVOLG (zie GOTO (1975)). *Er bestaat geen perfecte decimale cyclische AN-code van orde 1.*

BEWIJS. Brengt A zo'n code voort, en is $H' \subset (\mathbb{Z}/A\mathbb{Z})^*$ voortgebracht door de restklassen van 10 en -1, dan heeft $(\mathbb{Z}/A\mathbb{Z})^*/H'$ orde 9. Geven we het beeld van (i mod A) in deze groep aan met $\overline{i}$, dan

$$(\mathbb{Z}/A\mathbb{Z})^*/H' = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}.$$

Uit $\overline{2}^3 = \overline{8} \neq \overline{1}$ volgt orde $(\overline{2}) = 9$, dus $\overline{2}$ brengt de groep voort. Verder $\overline{2}.\overline{5} = \overline{10} = \overline{1}$ dus $\overline{5} = \overline{2}^8$. Zij $\overline{3} = \overline{2}^x$, met $0 \leq x < 9$. Als x = 0, 1, 2, 3 of 8, dan $\overline{3} = \overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{8}$ of $\overline{5}$, respectievelijk, een tegenspraak. Als x = 4, 5 of 6 dan $\overline{9} = \overline{2}^{2x} = \overline{5}$, $\overline{2}$ of $\overline{8}$, weer een tegenspraak. Tenslotte levert ook x = 7 een tegenspraak: $\overline{6} = \overline{2}^{x+1} = \overline{5}$. □

Meer non-existentiestellingen van dit type vindt men in GOTO & FUKUMURA (1975); hier worden ook negacyclische codes beschouwd. Perfecte codes van orde 1 met r = 4, 5, 8, 9 of 10 bestaan niet; voor r = 6 of 7 worden perfecte cyclische codes van orde 1 geleverd door:

r	A	n
6	18191	1819
6	20611	2061
7	19237	1603
7	30013	2501.

Voor hogere r zijn er geen voorbeelden bekend; deze bestaan echter waarschijnlijk wel, bijvoorbeeld voor r = 11, 12, 14, 15, 17, ... Deze verwachting is gebaseerd op overwegingen uit de algebraïsche getaltheorie, waar we hier niet verder op ingaan.

Voor niet-perfecte AN-codes die enkelvoudige fouten kunnen corrigeren zie men GRITSENKO (1969) en NEUMANN & RAO (1975).

10.3. BEREKENING VAN HET ARITHMETISCHE EN MODULAIRE GEWICHT

Voor het construeren van AN-codes die meer fouten kunnen corrigeren hebben we een goede manier nodig om het arithmetische of modulaire gewicht van een geheel getal te bepalen.

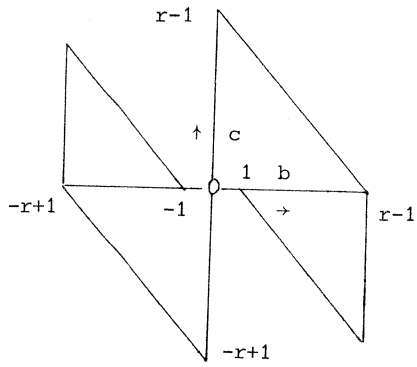
Elk geheel getal x kan, per definitie van w, geschreven worden als

$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)}$$

met a_i, $n(i) \in \mathbb{Z}$, $|a_i| < r$, $n(i) \geq 0$ $(i=1,\ldots,w(x))$. Aan de hand van voorbeelden ziet men gemakkelijk in dat deze schrijfwijze niet eenduidig hoeft te zijn. Er is echter één zo'n representatie die bijzonder eenvoudig te bepalen is; deze is als volgt gedefinieerd.

Laat $b, c \in \mathbb{Z}$, $|b|, |c| < r$. We noemen het paar (b,c) *toegelaten* als geldt:

als $bc > 0$ dan $|b+c| < r$,
als $bc < 0$ dan $|b| > |c|$.



Het toegelaten gebied.

Een schrijfwijze

$$(10.3.1) \qquad x = \sum_{i=0}^{\infty} c_i r^i$$

met $c_i \in \mathbb{Z}$, $|c_i| < r$ voor alle i, en $c_i = 0$ voor i groot genoeg, heet een NAF voor x als voor elke $i \geq 0$ het paar (c_{i+1}, c_i) toegelaten is. In het binaire geval betekent dit $c_{i+1} \cdot c_i = 0$ voor alle i, oftewel: twee naburige "cijfers" mogen niet allebei ongelijk aan nul zijn. De afkorting "NAF", aan het binaire geval ontleend, betekent dan ook "non-adjacent form".

(10.3.2) STELLING. *Elk geheel getal* x *heeft precies één NAF; bovendien, als* (10.3.1) *een NAF is voor* x, *dan is*

$$w(x) = |\{i \mid i \geq 0,\ c_i \neq 0\}|$$

Voor een (onnodig lang) bewijs van deze stelling verwijzen we naar CLARK & LIANG (1973). Daar vindt men ook een algoritme om een NAF voor x te berekenen uitgaande van een willekeurige representatie (10.1.1): men zorgt er eerst voor dat alle n(i) verschillend zijn, zodat de representatie de vorm $x = \sum_{i=0}^{\infty} b_i r^i$ heeft ($|b_i| < r$, en $b_i = 0$ voor i groot genoeg), en dan maakt men, te beginnen bij i = 0, achtereenvolgens alle paren (b_{i+1}, b_i) toegelaten, door zo nodig zo'n paar te vervangen door $(b_{i+1} \pm 1, b_i \mp r)$. We laten de details aan de lezer.

De volgende stelling geeft een andere manier om een NAF voor x te berekenen:

(10.3.3) STELLING. *Zij* $x \in \mathbb{Z}$, $x \geq 0$. *Schrijf* $(r+1).x$ *en* x *in het* r*-tallig stelsel:*

$$(r+1).x = \sum_{j=0}^{\infty} a_j r^j,$$

$$x = \sum_{j=0}^{\infty} b_j r^j$$

met $a_j, b_j \in \{0,1,\ldots,r-1\}$ *voor alle* j, *en* $a_j = b_j = 0$ *voor* j *groot genoeg. Dan wordt de NAF van* x *gegeven door*

$$x = \sum_{j=0}^{\infty} (a_{j+1} - b_{j+1}).\, r^j. \qquad \square$$

Definiëren we de *graad* $gr(x)$ van een geheel getal x door

$$gr(0) = -1$$

$$gr(x) = \max\{i \mid c_i \neq 0\},\ x \neq 0,$$

als (10.3.1) een NAF voor x is, dan kan men eenvoudig bewijzen:

(10.3.4) STELLING. *Zij* $k \in \mathbb{Z}$, $k \geq -1$, *en* $x \in \mathbb{Z}$. *Dan geldt*

$$gr(x) \leq k \iff |x| < \frac{r^{k+2}}{r+1}. \qquad \square$$

Vervolgens beschouwen we de analoge stellingen voor het *modulaire* gewicht w_m, met $m = r^n - 1$, $n \geq 2$.

We noemen een representatie

$$(10.3.5) \qquad x \equiv \sum_{i=0}^{n-1} c_i r^i \bmod m$$

met $c_i \in \mathbb{Z}$, $|c_i| < r$ een CNAF (= cyclische NAF) voor x modulo m, als (c_{i+1}, c_i) toegelaten is voor $i = 0,1,\ldots,n-1$; hier is $c_n = c_0$.

(10.3.6) STELLING. *Elk geheel getal* x *heeft een CNAF modulo* m; *deze CNAF is uniek behalve als*

$$(r+1)x \equiv 0 \not\equiv x \bmod m$$

in welk geval er twee CNAFs voor x *modulo* m *zijn. Is (10.3.5) een CNAF voor* x *modulo* m, *dan geldt*

$$w_m(x) = |\{i \mid 0 \le i < n,\ c_i \neq 0\}|. \qquad \square$$

(10.3.7) STELLING. *Als* $(r+1)x \equiv 0 \not\equiv x \bmod m$, *dan geldt* $w_m(x) = n$, *behalve als*

$$n \equiv 0 \bmod 2 \text{ en } x \equiv \pm \frac{m}{r+1} \bmod m,$$

in welk geval geldt $w_m(x) = \frac{1}{2}n$. $\square$

We verwijzen naar CLARK & LIANG (1974) voor meer over CNAF's o.a. voor een algoritme om een CNAF van een geheel getal te bepalen.

Stelling (10.3.4) impliceert gemakkelijk:

(10.3.8) STELLING. *Een geheel getal* x *heeft een CNAF (10.3.5) met* $c_{n-1} = 0$ *dan en slechts dan als er een* $y \in \mathbb{Z}$ *is met*

$$x \equiv y \bmod m,\ |y| \le \frac{m}{r+1}. \qquad \square$$

Heeft x een CNAF (10.3.5), dan wordt een CNAF voor rx gegeven door

$$rx \equiv \sum_{i=0}^{n-1} c_{i-1} r^i \pmod m \text{ (indices modulo n)}.$$

Uit stelling (10.3.6) volgt dus

(10.3.9) $$w_m(rx) = w_m(x),$$

hetgeen ook direct in te zien is.

Op dezelfde wijze ziet men dat de kopcoëfficiënt c'_{n-1} van de CNAF van $r^j.x$ gelijk is aan de n-1-j-de coëfficiënt c_{n-1-j} van de CNAF van x (aangenomen dat deze CNAF uniek is). Het al of niet nul zijn van c_{n-1-j} kan men dus bepalen door (10.3.8) op $r^j.x$ toe te passen, en men vindt:

(10.3.10) STELLING. *Voor* $x \in \mathbb{Z}$ *geldt*

$$w_m(x) = |\{j \mid 0 \le j < n, \text{ en er is een } y \in \mathbb{Z},$$

$$\frac{m}{r+1} < y \le \frac{mr}{r+1}, \text{ met } r^j x \equiv y \bmod m\}|. \qquad \square$$

10.4. MANDELBAUM-BARROWS CODES

(10.4.1) STELLING. *Zij* $C \subset \mathbb{Z}/(r^n-1)$ *een cyclische AN-code met voortbrenger* A, *en zij* $B = (r^n-1)/A = |C|$. *Dan geldt*

$$\sum_{x \in C} w_m(x) = n.\left(\left\lfloor \frac{rB}{r+1} \right\rfloor - \left\lfloor \frac{B}{r+1} \right\rfloor\right).$$

BEWIJS. Schrijf elke $x \in C$ in CNAF:

$$x = \left(\sum_{i=0}^{n-1} c_{i,x} r^i \bmod (r^n-1)\right),$$

dan moeten we het aantal coëfficiënten ongelijk aan nul van de matrix $(c_{i,x})_{0 \le i \le n-1,\ x \in C}$ bepalen.
Neem voor de eenvoud aan dat elke $x \in C$ een *unieke* CNAF heeft. Dan bevat elke kolom van de matrix $(c_{i,x})$ evenveel nullen, wegens het cyclische karakter van de code. Dus het gevraagde aantal is

$$n.\left|\{x \in C \mid c_{n-1,x} \neq 0\}\right|.$$

Bezit x een unieke CNAF, dan is wegens (10.3.8) de kopcoëfficiënt $c_{n-1,x}$ hiervan ongelijk aan nul dan en slechts dan als er een $y \in \mathbb{Z}$ is met

$$x = (y \bmod r^n-1),\ \frac{m}{r+1} < y \le \frac{mr}{r+1}.$$

Schrijven we $x = (AN \bmod r^n-1)$, $0 \le N < B$, dan betekent dit

$$\frac{B}{r+1} < N \le \frac{Br}{r+1}.$$

Het aantal van zulke N is kennelijk $\left\lfloor \frac{Br}{r+1} \right\rfloor - \left\lfloor \frac{B}{r+1} \right\rfloor$.

Het geval dat C een element met twee CNAFs bevat vereist enige extra zorg, die aan de lezer toevertrouwd kan worden. □

De uitdrukking in (10.4.1) is ongeveer gelijk aan

$$n.|C|.\frac{r-1}{r+1}.$$

Vergelijk hiermee het analoge resultaat voor cyclische codes over GF(q): is C zo'n code, met woordlengte n, dan

$$\sum_{x\in C} w_H(x) = n.\ |C|.\ \frac{q-1}{q} \qquad (w_H = \text{Hamming-gewicht}).$$

De volgende stelling beschrijft de gegeneraliseerde Mandelbaum-Barrows codes, zie MASSEY & GARCIA (1972) voor referenties voor het binaire geval. Een code heet *equidistant* als $d_m(x,x') = d_m(y,y')$ voor alle $x,x',y,y' \in C$, $x \neq x'$, $y \neq y'$.

(10.4.2) STELLING. *Zij* B *een priemgetal dat* r *niet deelt, met de eigenschap dat* $(\mathbb{Z}/B\mathbb{Z})^*$ *wordt voortgebracht door de restklassen van* r *en* -1. *Zij* n *een positief geheel getal met* $r^n \equiv 1$ *mod* B, *en laat* $A = (r^n-1)/B$. *Dan is de code* $C \subset \mathbb{Z}/(r^n-1)$ *voortgebracht door* A *equidistant met afstand*

$$\frac{n}{B-1}\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right).$$

BEWIJS. Zij $x \in C$, $x \neq 0$ willekeurig; dan geldt $x = (AN \bmod r^n-1)$, met $N \not\equiv 0 \bmod B$. De aannamen van de stelling impliceren dat $N \equiv \pm r^j \bmod B$ voor zekere j, dus $w_m(x) = w_m(\pm r^j A) = w_m(A)$ (wegens (10.3.9)). Hieruit blijkt dat alle elementen van C ongelijk nul hetzelfde modulaire gewicht hebben, dus C is equidistant. De afstand berekenen we met (10.4.1):

$$w_m(A) = \frac{1}{B-1}\sum_{x\in C,\ x\neq 0} w_m(x) = \frac{n}{B-1}\left(\left\lfloor\frac{rB}{r+1}\right\rfloor - \left\lfloor\frac{B}{r+1}\right\rfloor\right). \qquad \square$$

We merken op dat de woordlengte n in (10.4.2) ten minste $\frac{B-1}{2}$ is; dit is nogal groot ten opzichte van het aantal codewoorden, nl. B. Voor de praktijk lijken de Mandelbaum-Barrows codes dan ook niet belangrijk.

De Mandelbaum-Barrows codes corresponderen met de "maximum-length" codes over eindige lichamen. Dit zijn cyclische codes met woordlengte q^k-1 waarvan het check polynoom h(x) een primitief irreducibel polynoom van graad k is (*primitief* betekent dat de nulpunten van h(x) multiplicatieve orde q^k-1 hebben). Deze codes zijn equidistant met afstand $(q-1).q^{k-1}$. (Zie § 5.2).

Er bestaan generalisaties van (10.4.2) voor het geval B een natuurlijk getal, relatief priem met r, is, met de eigenschap dat de groep van eenheden $(\mathbb{Z}/B\mathbb{Z})^*$ van de ring $\mathbb{Z}/B\mathbb{Z}$ wordt voortgebracht door (r mod B) en (-1 mod B). In dit geval hoeft de verkregen AN-code C niet equidistant te zijn, maar wel is het zo dat het modulaire gewicht van een codewoord alleen van zijn orde in de groep C ($\cong \mathbb{Z}/B\mathbb{Z}$) afhangt. Door (10.4.1) op subcodes van C toe te passen kan men dan met Moebius-inversie de gewichtsenumerator van C opstellen; vergelijk TSAO-WU & CHANG (1969) voor het binaire geval. Voor deze codes geldt hetzelfde als voor de Mandelbaum-Barrows codes: een grote woordlengte en slechts weinig codewoorden.

Tenslotte noemen we een methode waarmee men de gewichten van een gegeven cyclische AN-code $C \subset \mathbb{Z}/(r^n-1)$ kan bepalen. Zij A de voortbrenger, en $AB = r^n - 1 = m$. Met H geven we de ondergroep van $(\mathbb{Z}/B\mathbb{Z})^*$ aan die wordt voortgebracht door de restklassen van r en -1. De groep H werkt op $\mathbb{Z}/B\mathbb{Z}$ door vermenigvuldiging; voor $N \in \mathbb{Z}$ geven we de baan van (N mod B) onder H met H.N aan:

$$H.N = \{\pm r^j N \bmod B \mid j = 0,1,2,\ldots\} \subset \mathbb{Z}/B\mathbb{Z}.$$

(10.4.3) STELLING. *Het modulaire gewicht* $w_m(AN)$ *hangt alleen van de baan* H.N *af; er geldt*

$$w_m(AN) = n.\frac{\left|HN \cap \{y \bmod B \mid \frac{B}{r+1} < y \leq \frac{Br}{r+1}\}\right|}{|HN|}$$

BEWIJS. Dit is in essentie een herformulering van (10.3.10). □

(10.4.4) VOORBEELD: r = 2, B = 109, n = 36. De groep $H \subset (\mathbb{Z}/109\ \mathbb{Z})^*$ heeft orde 36, en $\mathbb{Z}/109\ \mathbb{Z}$ valt onder H in vier banen uiteen:

H.0, H.1, H.3, H.9.

Doorsnijdt men deze banen met $\{y \bmod 109 \mid \frac{109}{3} < y \leq \frac{2.109}{3}\} =$
$= \{37, 38, \ldots, 72\}$, dan vindt men

$\emptyset$, $\{\pm 38, \pm 41, \pm 43, \pm 45, \pm 46, \pm 54\}$,

$\{\pm 40, \pm 48, \pm 51, \pm 52, \pm 53\}$, $\{\pm 37, \pm 39, \pm 42, \pm 44, \pm 47, \pm 49, \pm 50\}$,

dus de AN-code $C \subset \mathbb{Z}/(2^{36}-1)$ voortgebracht door $A = (2^{36}-1)/109$ heeft één element met gewicht 0 (het nul-element van C); 36 elementen met gewicht 12; 36 elementen met gewicht 10; en 36 elementen met gewicht 14. Er volgt $d_{min}(C) = 10$. Zie MASSEY & GARCIA (1972) § 3.6 voor meer voorbeelden.

In SEGUIN (1973) vindt men een manier om uit (10.4.3) een ondergrens voor $d_{min}(C)$ af te leiden.

10.5. CHEN-CHIEN-LIU CODES

De reeds vaker vermelde analogie met cyclische codes over een eindig lichaam heeft de gedachte in het leven geroepen dat er een klasse AN-codes bestaat die correspondeert met de klasse der BCH-codes. Voor een inmiddels weerlegd vermoeden hierover zie men MASSEY & GARCIA (1972) § 3.7.

De enige bekende klasse AN-codes die enigszins doet denken aan BCH-codes wordt beschreven door de volgende stelling, die men voor r = 2 kan vinden bij CHEN, CHIEN & LIU (1974).

(10.5.1) STELLING. *Laten* a *en* b *twee onderling ondeelbare getallen* ≥ 2 *zijn. Dan heeft de cyclische AN-code* $C \subset \mathbb{Z}/(r^{ab}-1)$ *voortgebracht door*

$$A = \frac{(r^{ab}-1)\,(r-1)}{(r^{a}-1)\,(r^{b}-1)}$$

minimum-afstand gelijk aan min {a,b}.

Dat de minimumafstand van C ten hoogste min{a,b} is blijkt uit de aanwezigheid van de codewoorden $(r^{ab}-1)/(r^{a}-1) = \sum_{i=0}^{b-1} r^{ia}$ en $(r^{ab}-1)/(r^{b}-1) = \sum_{j=0}^{a-1} r^{jb}$. De andere ongelijkheid is minder evident. Beneden schetsen we een bewijs voor het binaire geval, uitgaande van de onvolledige argumentatie van CHEN, CHIEN & LIU (1974), § 4. Het algemene geval laten we aan de lezer over, zie (10.6.3).

De analogie met BCH-codes is als volgt. Is q een priemmacht, en zijn a, b twee onderling ondeelbare getallen ≥ 2 met (ab,q) = 1, dan heeft het polynoom

$$g(x) = \frac{(x^{ab}-1)\,(x-1)}{(x^{a}-1)\,(x^{b}-1)} \in GF(q)[x]$$

min {a,b} - 1 "opeenvolgende" nulpunten

$$\alpha,\ \alpha^2,\ \ldots\ ,\ \alpha^{\min\{a,b\}-1}$$

waar α een primitieve ab-de eenheidswortel in een uitbreiding van GF(q) voorstelt. De BCH-grens impliceert dan dat de code

$$(g(x)) \subset GF(q)[x]/(x^{ab}-1)$$

minimum-afstand $\geq \min\{a,b\}$ heeft. In feite is de minimum-afstand *gelijk* aan $\min\{a,b\}$, want $(g(x))$ bevat de codewoorden $\sum_{i=0}^{b-1} x^{ia}$ en $\sum_{j=0}^{a-1} x^{jb}$.

We merken op dat de voorwaarde (ab,q) = 1 overbodig is: dit blijkt te volgen uit de methode waarmee (10.5.1) bewezen wordt.

BEWIJS van (10.5.1) voor r = 2. Zij $m = 2^{ab}-1$, en $y = AN \in C$, $y \neq (0 \bmod m)$. We moeten bewijzen dat $w_m(y) \geq \min\{a,b\}$.

Zetten we $x = (2^a-1).y = 2^a.y-y$, dan geldt wegens (10.3.9):

$$w_m(x) \leq w_m(2^a.y) + w_m(y) = 2.w_m(y). \tag{10.5.2}$$

Verder $x = N.(2^{ab}-1)/(2^b-1)$, dus

$$2^b.x \equiv x \bmod m.$$

Dit betekent dat we, door de cijfers van een CNAF van x modulo m over b plaatsen op te schuiven, opnieuw een CNAF van x modulo m krijgen. Heeft x een unieke CNAF modulo m, dan kan dit alleen als deze CNAF periode b heeft:

$$x \equiv \sum_{i=0}^{ab-1} c_i 2^i \quad \bmod m, \qquad c_i = c_{i+b} \text{ als } 0 \leq i < ab-b.$$

In het uitzonderlijke geval dat x twee CNAF's modulo m bezit blijkt deze periodiciteit voor beide te gelden. Dus

$$w_m(x) = a.\left|\{i \mid 0 \leq i < b,\ c_i \neq 0\}\right|$$

en dit is deelbaar door a. Als $w_m(x) \geq 2a$, dan $w_m(y) \geq a$ wegens (10.5.2), en we zijn klaar. Als $w_m(x) = 0$, dan $x \equiv 0 \bmod m$, dus $2^a y \equiv y \bmod m$, en hieruit volgt op analoge wijze dat $w_m(y)$ deelbaar is door b, dus inderdaad $w_m(y) \geq b \geq \min\{a,b\}$ als $w_m(y) \neq 0$. We concluderen dat we alleen blijven zitten met het geval $w_m(x) = a$.
Dan

$$x \equiv \varepsilon \cdot \sum_{\ell=0}^{a-1} 2^{i+\ell b} = \varepsilon \cdot 2^i \cdot \frac{2^{ab}-1}{2^b-1} \bmod m$$

voor een $\varepsilon \in \{\pm 1\}$ en een $i \in \{0,1,\ldots,b-1\}$. Wegens $x = N \cdot (2^{ab}-1)/(2^b-1)$ impliceert dit

$$N \equiv \varepsilon \cdot 2^i \bmod (2^b-1).$$

Verwisseling van a en b toont aan dat we ook mogen aannemen

$$N \equiv \eta \cdot 2^j \bmod (2^a-1)$$

voor een $\eta \in \{\pm 1\}$ en een $j \in \{0,1,\ldots,a-1\}$. Kies nu $k \in \{0,1,\ldots,ab-1\}$ met $k \equiv -i \bmod b$ en $k \equiv -j \bmod a$, en vervang N door $\varepsilon \cdot r^k \cdot N$. Dit verandert $w_m(NA)$ niet, en we krijgen

$$N \equiv 1 \bmod (2^b-1), \qquad N \equiv \pm 1 \bmod (2^a-1).$$

Wegens $(2^a-1, 2^b-1) = 1$ blijven er voor N dan slechts 2 waarden over modulo $(2^a-1)(2^b-1)$; en omdat (NA mod m) alleen afhangt van (N mod $(2^a-1)(2^b-1)$), zien we dat we nog slechts met twee codewoorden y te maken hebben. Het eerste correspondeert met N = 1, en is de voortbrenger van de code: y = A. Het tweede noemen we A'; het is bepaald door

(10.5.3) $\quad A' \equiv A \bmod (2^{ab}-1)/(2^a-1)$

(10.5.4) $\quad A' \equiv -A \bmod (2^{ab}-1)/(2^b-1).$

We moeten bewijzen

$$w_m(A) \geq \min\{a,b\}, \qquad w_m(A') \geq \min\{a,b\}.$$

(10.5.5) LEMMA. Stel $x \equiv \sum_{i=0}^{ab-1} \varepsilon_i 2^i \bmod m$, met $\varepsilon_i \in \{0,1,-1\}$ voor alle i, en $\varepsilon_i = 0$ voor ten minste één i, zodanig dat

(10.5.6) er is geen i met $\varepsilon_i = \varepsilon_{i+1} \neq 0$

(indices modulo ab). Dan geldt

$$w_m(x) \geq \left|\{i \mid \varepsilon_i = 1\}\right|.$$

BEWIJS (schets): roteer x zó, dat $\varepsilon_{ab-1} = 0$, en bereken de NAF van $\sum \varepsilon_i 2^i$ volgens de algoritme gegeven na (10.3.2); dit blijkt een CNAF $\sum c_i 2^i$ voor x mod m te leveren met de eigenschap $\varepsilon_i = 1 \Rightarrow c_i \neq 0$ of $c_{i-1} \neq 0$. □

Kies gehele getallen λ en μ met

$$\lambda a \equiv 1 \bmod b, \quad 1 \leq \lambda \leq b,$$
$$\mu b \equiv 1 \bmod a, \quad 1 \leq \mu \leq a.$$

Eenvoudig bewijst men

$$\lambda a + \mu b = 1 + ab$$

(10.5.7) $\lambda \cdot \mu \geq \min\{a,b\}$.

Verder zetten we

$$f = \frac{(X^{ab}-1)(X-1)}{(X^a-1)(X^b-1)}.$$

(10.5.8) LEMMA. (a) Er geldt

$$f = \sum_{i=0}^{\lambda-1} \sum_{j=0}^{\mu-1} X^{ia+jb} - \sum_{i=\lambda}^{b-1} \sum_{j=\mu}^{a-1} X^{ia+jb-ab}.$$

(b) Als $V = \{sa+tb \mid s,t \in \mathbb{Z}_{\geq 0}\}$, dan

$$f = (1-X) \cdot \sum_{v \in V} X^v.$$

(c) f is een polynoom van de graad (a-1)(b-1), en de coëfficiënten van f die ongelijk aan nul zijn, zijn afwisselend +1 en -1.

BEWIJS: overgelaten aan de lezer; de laatste bewering van (c) volgt uit (b). □

Het bewijs van $w_m(A) \geq \min\{a,b\}$ is nu niet lastig meer: we hebben $A = f(2)$, en wegens (10.5.8)(c) geeft dit een representatie van A waarop we lemma (10.5.5) kunnen toepassen. Met behulp van (10.5.8)(a) en (10.5.7) vinden we dan

$$w_m(A) \geq \lambda \cdot \mu \geq \min\{a,b\},$$

zoals verlangd.

Om A' te kunnen behandelen voeren we een nieuwe notatie in. We zeggen dat een b×a-matrix $(e_{ij})_{0\leq i<b,\ 0\leq j<a}$ met gehele coëfficiënten een geheel getal x representeert als

$$x \equiv \sum_{i=0}^{b-1} \sum_{j=0}^{a-1} e_{ij} 2^{ia+jb} \mod (2^{ab}-1).$$

Omdat elk geheel getal k modulo ab eenduidig te schrijven is als ia + jb, met $0 \leq i < b$ en $0 \leq j < a$, kunnen we elke "gewone" ontwikkeling $x \equiv \sum_{k=0}^{ab-1} e_k 2^k \mod (2^{ab}-1)$ in matrix-vorm brengen, en omgekeerd. Het getal $A = f(2)$ kunnen we wegens (10.5.8)(a) bijvoorbeeld representeren door de matrix

(10.5.9)

$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & -1 \end{array}\right] \begin{array}{l} \} \lambda \\ \} b-\lambda \end{array}$$

μ $\quad$ $a-\mu$.

(de "1" linksboven slaat hier op een $\lambda \times \mu$-matrix vol met enen, etc.). De congruentie $2 \equiv 2^{\lambda a+\mu b} \bmod (2^{ab}-1)$ toont dat het "cyclisch opschuiven" van een schrijfwijze $\sum e_k 2^k$er in matrix-notatie op neerkomt dat de rijen over een verticale afstand λ cyclisch worden opgeschoven, en de kolommen over een horizontale afstand μ. Bovenstaand voorbeeld geeft dan

0	1	0	$2\lambda-b$
-1	0	-1	$b-\lambda$
0	1	0	$b-\lambda$
μ	μ	$a-2\mu$	

We zien dat deze matrix en matrix (10.5.9) op geen enkele plaats dezelfde coëfficiënt $\neq 0$ hebben staan. Dit bewijst opnieuw dat de representatie (10.5.9) voor A voldoet aan conditie (10.5.6) van lemma (10.5.5). Ter rechtvaardiging van het plaatje merken we op dat we zonder verlies van algemeenheid mogen aannemen

$$\lambda > \tfrac{1}{2} b, \qquad \mu \leq \tfrac{1}{2} a,$$

zoals de lezer eenvoudig nagaat.

Het blijkt dat deze techniek zich ook laat toepassen op A'. We kunnen A' laten representeren door

(10.5.10)

0	1	λ
-1	0	$b-\lambda$
μ	$a-\mu$	

Immers, trekken we deze matrix af van (10.5.9), dan vinden we een matrix waarvan alle rijen gelijk zijn, en die dus een getal representeert dat deelbaar is door $(2^{ab}-1)/(2^{a}-1)$, in overeenstemming met (10.5.3). Evenzo controleert men (10.5.4) door beide matrices op te tellen.

De bovenbeschreven cyclische opschuiving geeft ons de volgende representatie voor 2.A':

(10.5.11)

1	0	1	$2\lambda-b$
0	-1	0	$b-\lambda$
1	0	1	$b-\lambda$
μ	μ	$a-2\mu$	

De 1 rechtsboven laat evenwel zien, dat (ingeval $\mu<\frac{1}{2}a$) de representatie (10.5.10) niet aan conditie (10.5.6) voldoet. Trekken we (10.5.10) af van (10.5.11) dan krijgen we de matrix

1	-1	0
0	-2	-1
2	0	1

die het getal 2A'-A' = A' representeert. De 2 linksonder valt gelukkigerwijze weg tegen de helft van de -2 in het midden, dus A' wordt ook gerepresenteerd door

(10.5.12)

1	-1	0	$\}\ \lambda$
0	-1	-1	$\}$
0	0	1	
	$\underbrace{\quad}_{\mu}$		

tatie voor A' inderdaad aan (10.5.6) voldoet. Passen we dus (10.5.5) toe/ Een ogenblik staren op deze matrix voert tot het inzicht dat deze representatie voor A' inderdaad aan (10.5.6) voldoet. Passen we dus (10.5.5) toe (met x = -A') dan vinden we dat $w_m(A')$ ten minste gelijk is aan het aantal

coëfficiënten -1 in (10.5.12), en dat is $\geq \lambda \cdot \mu \geq \min\{a,b\}$, wegens (10.5.7). □

10.6. OPGAVEN

(10.6.1) Bewijs dat

$$\min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\} \leq 2$$

voor alle $A \in \mathbb{Z}$.

(10.6.2) Generaliseer de resultaten van §§ 10.2 t/m 10.4 voor het negacyclische geval.

(10.6.3) Voer het bewijs van (10.5.1) door voor $r > 2$.

LITERATUUR

AX, J., *Zeroes of polynomials over finite fields*, Am.J.Math. 86 (1964), 255-261.

BAUMERT, L.D. & R.J. McELIECE, *A note on the Griesmer bound*, IEEE Trans. Inform. Theory 19 (1973) 134-135.

BERLEKAMP, E.R., *Algebraic Coding Theory*, McGraw Hill, New York (1968).

BERLEKAMP, E.R. and O. MORENO, *Extended double-error-correcting binary Goppa codes are cyclic*, IEEE Trans. Inform. Theory 19 (1973) 817-818.

BEST, M.R. & A.E. BROUWER, *The triply shortened Hamming code is optimal*, Discr. Math., to appear.

BEST, M.R., A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than 25*, to appear.

BLAKE, I.F. & R.C. MULLIN, *The mathematical theory of coding*, Academic Press, New York (1975).

BOYARINOV, I.M. & G.A. KABATYANSKY, *On perfect arithmetic AN-codes*, Int. Symp. Inf. Theory Talin, SSSR, (1973), pp. 41-43 (Russisch).

CAMERON, P.J. & J.H. VAN LINT, *Graph Theory, Coding Theory and Block Designs*, London Math. Soc. Lecture Note Series 19, Cambr. Univ. Press, (1975).

CHEN, C.L., R.T. CHIEN & C.K. LIU, *On the binary representation form of certain integers*, SIAM J. Appl. Math. 26 (1974), 285-293.

CHEVALLEY, C., *Demonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Hamburg 11 (1936), 73-75.

CHIEN, R.T. & D.M. CHOY, *Algebraic generalization of BCH-Goppa-Helgert codes*, IEEE Trans. Inform. Theory (1975), pp. 70-79.

CLARK, W.E. & J.J. LIANG, *On arithmetic weight for a general radix representation of integers*, IEEE Trans. Inform. Theory IT-19 (1973), 823-826.

—— *On modular weight and cyclic nonadjacent forms for arithmetic codes*, IEEE Trans. Inform. Theory IT-20 (1974), 767-770.

DELSARTE, P., *Bounds for unrestricted codes, by linear programming*, Philips Res. Repts. 27 (1972), 272-289.

DELSARTE, P., *An algebraic approach to the association schemes of coding theory*, Philips Res. Repts. Suppl. (1973) no. 10.

DELSARTE, P., J.M. GOETHALS and F.J. MAC WILLIAMS, *On generalized Reed-Muller codes and their relatives*, Inf. and Control 16 (1970), 403-442.

DICKSON, L.E., *Theory of Numbers*, Vol. I, p. 271, Chelsea (1952).

FORNEY, Jr. G.D., *Concatenated Codes*, M.I.T. Press, Cambridge, Mass. (1966).

GILBERT, E.N., *A comparison of signalling alphabets*, Bell Syst. Tech. J. 31 (1952), 504-522.

GOETHALS, J.M., *On the Golay perfect binary code*, J. Comb. Theory 11 (1971), 178-186.

GOETHALS, J.M. & H.C.A. VAN TILBORG, *Uniformly packed codes*, Philips Res. Repts. 30 (1975), 9-36.

GOLAY, M.J.E., *Notes on digital coding*, Proc. IRE. 37 (1949), 657.

GOPPA, V.D., *A new class of linear error-correcting codes*. Problems of Information Transmission (1973), pp. 207-212 = Problemy Peredachi Informatsii 1970, Vol. 6, No. 3, pp. 24-30.

-- *A rational representation of codes and* (L,g)*-codes*. Ibid (1973), pp. 223-229 (1971, Vol. 7, No. 3, pp. 41-49).

-- *Codes constructed on the base of* (L,g) *codes*. Ibid (1974), pp. 165-166 (1972, Vol. 8, No. 2, pp. 107-109).

GOTO, M., *A note on perfect decimal AN codes*, Inform. & Control 29 (1975) 385-387.

GOTO, M. & T. FUKUMURA, *Perfect nonbinary AN codes with distance three*, Information and Control 27 (1975), 336-348.

GRIESMER, J.H., *A bound for error correcting codes*, IBM J. Res. & Dev. 4 (1960), 532-542.

GRITSENKO, V.M., *Nonbinary arithmetic correcting codes*, Problems of Information Transmission 5 (1969), 15-22.

HALL, Jr, M., *Combinatorial Theory*, Blaisdell, Waltham, Mass. (1967).

HAMMING, R.W., *Error detecting and error correcting codes*, Bell Syst. Tech. J. 29 (1950), 147-160.

HARTMANN, C.R.P. & K.K. TZENG, *Generalization of the* BCH *bound*, Inf. & Control 20 (1972) 489-498.

HELGERT, H.J. & R.D. STINAFF, *Minimum-distance bounds for binary linear codes*, IEEE Trans. Inform. Theory 19, no. 3 (1973), 344-356.

JOHNSON, S.M., *A new upper bound for error correcting codes*, IRE Trans. Inform. Theory 8 (1962), 203-207.

-- *Improved asymptotic bounds for error correcting codes*, IEEE Trans. Inform. Theory 9 (1963), 193-205.

-- *On upper bounds for unrestricted binary error-correcting codes*, IEEE Trans. Inform. Theory 17 (1971), 466-478.

JOLY, J.R., *Equations et variétés algebriques sur un corps fini*, Enseign. Math. 19 (1973)

JUSTESEN, J., *A Class of Constructive Asymptotically Good Algebraic Codes*, IEEE Trans. on Inform. Theory, IT 18, 1972, 652-656.

KASAMI, T., *An upper bound on* k/n *for affine invariant codes with fixed* d/n, IEEE Trans. Inform. Theory 15 (1969), 171-176.

LEVENSHTEIN, V.I., *On the Minimal Redundancy of Binary Error-Correcting Codes*, Inf. and Control 28 (1975), 268-291.

LIN, S. & E.J. WELDON, *Long* BCH *codes are bad*, Inf. and Control 11 (1967), 455-451.

LINDSTRÖM, K., *The nonexistence of unknown nearly perfect binary codes*, Ann. Univ. Turku A 169 (1975).

VAN LINT, J.H., *Coding Theory*, Lecture Notes in Math. 201, Springer Verlag, Berlin etc. (1971).

-- *Recent results on perfect codes and related topics*, Combinatorics Part 1, Math. Centre Tracts 55 (1974), 158-178.

-- *A survey of perfect codes*, Rocky Mount. J. of Math. 5 (1975), 199-224.

LLOYD, S.P., *Binary block coding*, Bell System Tech. J. 36 (1957), 517-535.

McELIECE, R.J., E.R. RODEMICH, H.C. RUMSEY jr. & L.R. WELCH, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, to appear.

MacWILLIAMS, F.J., *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. 42 (1963), 79-94.

MASSEY, J.L., *Threshold Decoding*, M.I.T. Press, Cambridge, Mass. (1963).

MASSEY, J.L., D.J. COSTELLO & J. JUSTESEN, *Polynomial Weights and Code Construction*, IEEE Trans. on Inform. Theory, IT-19 (1973), 101-110.

MASSEY, J.L. & O.N. GARCIA, *Error-correcting codes in computer arithmetic*, Advances in Information Systems Science (J.T. Tou, ed.), 4, Ch. 5 (273-326), Plenum Press, (1972).

NEUMANN, P.G. & T.R.N. RAO, *Error-correcting codes for byte-organized arithmetic processors*, IEEE Trans. Computers C-24 (1975), 226-232.

NORDSTROM, A.W. & J.P. ROBINSON, *An optimal nonlinear code*, Inform. Contr. 11 (1967), 613-616.

PETERSON, W.W. & E.J. WELDON, JR., *Error-correcting codes*, Second edition, The MIT Press, (1972).

PLOTKIN, M., *Binary codes with specified minimum distance*, IEEE Trans. Inform. Theory 6 (1960), 445-450.

POSNER, E.C., *Combinatorial Structures in Planetary Reconnaissance*, p. 15-46 in H.B. MANN, Error correcting codes, Wiley, New York, 1968.

RAO, T.R.N., *Error coding for arithmetic processors*, Academic Press, New York-London, (1974).

RETTER, C.T., *Decoding Goppa codes with a* BCH *decoder*, IEEE Trans. Inform. Theory 21 (1975), 112.

SEGUIN, G., *Bounds for certain cyclic AN-codes*, Information and Control 23 (1973), 41-47.

SHANNON, C.E., *Mathematical Theory of Communication*, Bell System Tech. J. 27 (1948) 379-423.

SIDELNIKOV, V.M., *Upper Bounds on the Cardinality of a Binary Code with a Given Minimum Distance*, Inf. and Control 28 (1975), 292-303.

SLOANE, N.J.A., *A survey of constructive coding theory, and a table of binary codes of highest known rate*, Discrete Math. 3 (1972), 265-294.

SLOANE, N.J.A., S.M. REDDY & C.L. CHEN, *New binary codes*, IEEE Trans. Inform. Theory IT-18 (1972), 503-510.

SLOANE, N.J.A. & D.S. WHITEHEAD, *A new family of single-error-correcting codes*, IEEE Trans. Inform. Theory, IT-16 (1970), 717-719.

SZEGÖ, G., *Orthogonal polynomials*, A.M.S. Coll. Publ. 23 (1959).

VAN TILBORG, H.C.A., *All binary* (n,e,r)*-uniformly packed codes are known*, Memorandum 1975-08, T.H. Eindhoven (1975).

TSAO-WU, N.T. & S.-H. CHANG, *On the evaluation of minimum distance of binary arithmetic cyclic codes*, IEEE Trans. Inform. Theory IT-15 (1969), 628-631.

TZENG K.K. and K. ZIMMERMAN, *On extending Goppa codes to cyclic codes*, IEEE Trans. Inform. Theory 21 (1975), 712-715.

WARNING, E., *Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Hamburg 11 (1936), 76-83.