Hoofdstuk VIII

ARITHMETISCHE CODES

door

H.W. Lenstra Jr.

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

$$x = \sum_{i=1}^{t} a_i r^{n(i)} \tag{1.1}$$

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 net 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.

Wij 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 minstens $d(AN_3, S)$, 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 $A \in \mathbb{Z}$ (ga na) (*opgave*).

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

$$m = AB,$$

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

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

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 $\mathbb{Z}/m$ 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 $w_m((x \bmod m), (y \bmod m))$ en $w_m((x \bmod m))$ ook wel eenvoudig $d_m(x,y)$ en $w_m(x)$. Merk op dat geldt

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

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

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 en slechts dan als geldt

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

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

$$d_{min}(C) = \min\{w_m(x) \mid x \in C,\ x \neq (0 \bmod m)\}.$$

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

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

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

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

met $c_i \in \{0,1,\ldots, r-1\}$ $(0 \leq i < n)$, 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 $c_0 = c_1 = \ldots = c_{k-1} = 0$; 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 *cyklische AN-code* een ondergroep C van $\mathbb{Z}/(r^n-1)$; hier is 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

$$AB = r^n-1$$

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

We noemen A de *voortbrenger* van de code. We zijn primair geinteresseerd in

codes waarvan de *rate* $\frac{1}{n}.{}^{r}\log B$ en de minimum-afstand "groot" zijn.

Als abelse groep is C cyklisch van orde B. De benaming "cyklische AN-code" slaat echter op een andere eigenschap, die doet denken aan de cyklische codes over eindige lichamen: is $(x \bmod(r^n-1))$ een element van C,

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

dan geldt

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

(indices modulo n), en $(rx \bmod(r^n-1))$ is een element van C omdat C een ondergroep is. Dus de "cyklische opschuiving" van een codewoord behoort weer tot de code. De analogie met cyklische codes over eindige lichamen gaat verder: een cyklische AN-code is een ideaal van de ring $\mathbb{Z}/(r^n-1)$, een cyklische 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 *negacyklische* 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 §§ 2,3,4 voor het negacyklische geval te formuleren en te bewijzen.

Referenties voor deze paragraaf: PETERSON & WELDON [11], MASSEY & GARCIA [9], en de daar aangegeven literatuur. Deze auteurs beschouwen voornamelijk het binaire geval.

2. PERFECTE CYKLISCHE AN-CODES VAN ORDE 1.

Zij $C \subset \mathbb{Z}/(r^n-1)$ een cyklische 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

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

moet bijectief zijn. Hier geeft A de voortbrenger van de code aan, als in §1. Merk op dat een perfecte code van orde e alle hoogstens 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

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

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

De bijectie $S_1 \to \mathbb{Z}/A$ 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".

STELLING (2.1) [7]. *Stel* $C \subset \mathbb{Z}/(r^n-1)$ *is een perfecte cyklische 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* $H \subset (\mathbb{Z}/A)^*$ (= *multiplicatieve groep van het lichaam* $\mathbb{Z}/A$) *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* $(\mathbb{Z}/A)^*$.

Omgekeerd, als A *een priemgetal* $> r^2$ *is met de eigenschap dat de ondergroep* $H \subset (\mathbb{Z}/A)^*$ *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 cyklische AN-code van orde* 1.

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

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

Het beeld van $\{r^j \mid\ j = 0,1,\ldots,\ n-1\}$ is net de ondergroep 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 $(\mathbb{Z}/A)^*/H$. 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. □

GEVOLG (2.2) [11]. *Stel* p *is een priemgetal* $\equiv 3 \bmod 4$ *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 cyklische AN-code van orde 1. Bovendien is elke perfecte binaire cyklische AN-code van orde 1 van deze vorm.*

BEWIJS. Dit volgt direkt uit de stelling (2.1). De voorwaarde op p is slechts een vertaling van de eis dat $(2 \bmod p) \in (\mathbb{Z}/p)^*$ een ondergroep van index 2 voortbrengt waar $(-1 \bmod p)$ niet in zit. □

Priemgetallen p die aan de voorwaarden van 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 *negacyklische* codes, cf. [11]. Vergelijk dit met de cyklische 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.

GEVOLG (2.3) [18]. *Stel* p *is een priemgetal* $\equiv 5 \bmod 8$ *zodat* $(3 \bmod p) \in (\mathbb{Z}/p)^*$ *een ondergroep van index 4 voortbrengt. Dan brengt* (p mod $(3^{\frac{1}{4}(p-1)}-1)$) *een perfecte ternaire cyklische AN-code van orde 1 in* $\mathbb{Z}/(3^{\frac{1}{4}(p-1)}-1)$ *voort. Bovendien is elke perfecte ternaire cyklische AN-code van orde 1 van deze vorm.* □

Een priemgetal p dat aan de voorwaarden van dit gevolg voldoet is automatisch 13 mod 24; voorbeelden zijn p = 13, p = 109.

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

GEVOLG (24) [2]. *Er bestaat geen perfecte cyklische 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 $H' \subset (\mathbb{Z}/A)^*$ voortgebracht door (r mod A) en (-1 mod A). Wegens de stelling heeft $(\mathbb{Z}/A)^*/H'$ 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 $(\mathbb{Z}/A)^*/H'$ 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. □

GEVOLG (2.5) [6]. *Er bestaat geen perfecte decimale cyklische AN-code van orde 1.*

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

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

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

Meer non-existentiestellingen van dit type vindt men in [7]; hier worden ook negacyklische codes beschouwd. Perfecte codes van orde 1 met r = 4, 5, 8, 9 of 10 bestaan niet; voor r = 6 of 7 worden perfecte cyklische 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 [8] en [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

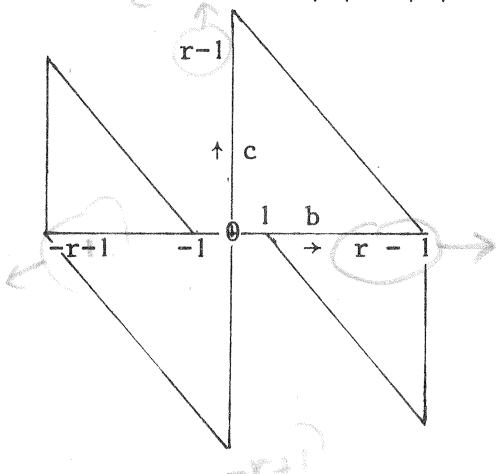
$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)}$$

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 b c ≥ 0 dan $|b+c| < r$,

als b c < 0 dan $|b| > |c|$.



Het toegelaten gebied.

Een schrijfwijze

$$(3.1) \qquad x = \sum_{i=0}^{\infty} c_i r^i$$

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".

STELLING (3.2) [4]. *Elk geheel getal* x *heeft precies één NAF; bovendien, is* (3.1) *een* NAF *voor* x, *dan*

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

Voor een (onnodig lang) bewijs van deze stelling verwijzen we naar [4]. Daar vindt men ook een algoritme om een NAF voor x te berekenen uitgaande van een willekeurige representatie (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:

STELLING (3.3) [4]. *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*

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

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

STELLING (3.4) [5]. *Zij* $k \in \mathbb{Z}$, $k \geq -1$, *en* $x \in \mathbb{Z}$. *Dan geldt*

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

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

We noemen een representatie

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \bmod m \tag{3.5}$$

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

STELLING (3.6) [5]. *Elke geheel getal* x *heeft een CNAF modulo* m; *deze CNAF is uniek behalve als*

$$(r+1)x \equiv 0 \neq x \bmod m$$

in welk geval er twee CNAFs voor x *modulo* m *zijn. Is (3.5) een CNAF voor* x *modulo* m, *dan geldt*

$$w_m(x) = \#\{i \mid 0 \leq i < n,\ c_i \neq 0\}. \quad \square$$

STELLING (3.7) *Als* $(r+1)x \equiv 0 \neq x$ *mod* 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 [5] voor een algoritme om een CNAF van een geheel getal te bepalen.

Stelling (3.4) impliceert gemakkelijk:

STELLING (3.8). *Een geheel getal* x *heeft een CNAF (3.5) met* $c_{n-1} = 0$ *dan en slechts dan als er een* $y \in \mathbb{Z}$ *is met*

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

Heeft x een CNAF (3.5), dan wordt een CNAF voor rx gegeven door

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

Uit stelling (3.6) volgt dus

$$w_m(rx) = w_m(x), \tag{3.9}$$

hetgeen ook direct in te zien is.

Op dezelfde wijze ziet men dat de kopcoëfficient 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 (3.8) op $r^j.x$ toe te passen, en men vindt:

STELLING (3.10) [5]. *Voor* $x \in \mathbb{Z}$ *geldt*

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

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

4. MANDELBAUM-BARROWS CODES

STELLING (4.1). *Zij* $C \subset \mathbb{Z}/(r^n-1)$ *een cyklische AN-code met voortbrenger* A, *en zij* $B = (r^n-1)/A = \#\, C$. *Dan geldt*

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

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 $(c_{i,x})$ $0 \leq i \leq n-1$, $x \in C$ 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 cyklische karakter van de code. Dus het gevraagde aantal is

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

Bezit x een unieke CNAF, dan is wegens (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

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

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

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

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

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

De uitdrukking in (4.1) is ongeveer gelijk aan

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

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

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

De volgende stelling beschrijft de gegeneraliseerde Mandelbaum-Barrows codes, zie [9] voor referenties voor het binaire geval. Een code C heet *equidistant* als $d_m(x,x') = d_m(y,y')$ voor alle $x,x', y,y' \in C$, $x \neq x'$, $y \neq y'$.

STELLING (4.2) [5]. *Zij* B *een priemgetal dat* r *niet deelt, met de eigenschap dat* $(\mathbb{Z}/B)^*$ *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*

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

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(3.9)). Hieruit blijkt dat alle elementen van C ongelijk nul hetzelfde modulaire gewicht hebben, dus C is equidistant. De afstand berekenen we met (4.1):

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

We merken op dat de woordlengte n in (4.2) minstens $\frac{B-1}{2}$ 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 [1, p. 48/49]. Dit zijn cyklische codes met woordlengte q^k-1 waarvan het "check polynomis1" h(x) een primitief irreducibel polynoom van graad m is (*primitief* betekent dat de nulpunten van h(x) multiplicatieve orde $q^k - 1$ hebben). Deze codes zijn equidistant met afstand $(q-1).\ q^{k-1}$.

Er bestaan generalisaties van (4.2) voor het geval B een natuurlijk getal, relatief priem met r, is, met de eigenschap dat de groep van eenheden $(\mathbb{Z}/B)^*$ van de ring $\mathbb{Z}/B$ 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 ($\cong \mathbb{Z}/B$) afhangt. Door (4.1) op subcodes van C toe te passen kan men dan met Moebius-inversie de gewichtsenumerator van C opstellen; vergelijk [13] 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 cyklische AN-code $C \subset \mathbb{Z}/(r^n-1)$ kan bepalen. Zij A de voortbrenger, en $AB = r^n - 1 = m$. Met H geven de de ondergroep van $(\mathbb{Z}/B)^*$ aan die wordt voortgebracht door de restklassen van r en -1. De groep H werkt op $\mathbb{Z}/B$ door vermenigvuldiging; voor $N \in \mathbb{Z}$ geven we de baan van (N mod B) onder H met H.N aan:

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

STELLING (4.3). *Het modulaire gewicht* $w_m(AN)$ *hangt alleen van de baan* H.N *af; er geldt*

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

BEWIJS. Dit is in essentie een herformulering van (3.10). □

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

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

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

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 [9, §3.6] voor meer voorbeelden.

In [12] vindt men een manier om uit (4.3) een ondergrens voor $d_{min}(C)$ af te leiden.

5. CHEN-CHIEN-LIU CODES.

De reeds vaker vermelde analogie met cyklische codes over een eindig lichaam heeft voedsel gegeven aan de gedachte dat er een klasse AN-codes bestaat die correspondeert met de klasse der BCH-codes. Voor een onbewezen vermoeden hierover zie men [9, §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 [3]:

STELLING (5.1). *Laten* a *en* b *twee relatief prieme getallen* ≥ 2 *zijn. Dan heeft de cyklische 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).

Het bewijs van (5.1) geven we hier niet. Dat de minimumafstand hoogstens 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 echter minder evident. Een aanzet tot bewijs in het binaire geval vindt men in [3, §4]; de daar gegeven argumenten zijn evenwel niet volledig.

De analogie met BCH-codes is als volgt. Is q een priemmacht, en zijn a, b twee relatief prieme 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 [11, §9.1] impliceert dan dat de code

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

minimum-afstand ≥ 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 (5.1) bewezen wordt.

LITERATUUR.

[1] I.F. BLAKE & R.C. MULLIN, *The mathematical theory of coding*, Academic Press 1975.

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

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

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

[5] W. E. CLARK & J.J. LIANG, *On modular weight and cyclic nonadjacent forms for arithmetic codes*, IEEE Trans. Information Theory IT-20 (1974), 767-770.

[6] M. GOTO, *A note on decimal perfect AN-codes*, the Research Reports of Gifu University 25 (1975), 24-26.

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

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

[9] J.L. MASSEY & 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.

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

[11] W.W. PETERSON & E.J. WELDON, JR., *Error-correcting codes*, Second edition, the MIT Press, 1972.

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

[13] N.T. TSAO-WU & S.-H. CHANG, *On the evaluation of minimum distance of binary arithmetic cyclic codes*, IEEE trans. Information theory IT-15 (1969), 628-631.