Voorbeelden van codes

Hoofdstuk II

VOORBEELDEN VAN CODES

In dit hoofdstuk noemen we een code C met M woorden van de lengte n en onderlinge afstand ≥ d een [n,M,d]-code.

2.1. DE (7,4)-HAMMING CODE

Beschouw de 7 vectoren die ontstaan door cyclische permutatie van (1,1,0,1,0,0,0). Dit zijn de rijen van de incidentiematrix van PG(2,2), het projectieve vlak van de orde 2 (zie (0.3.3)). Hieruit (of door eenvoudige inspectie) volgt dat deze 7 woorden onderling afstand 4 hebben. We voegen nu toe $\underline{0}$ = (0,0,...,0) en de 8 woorden die ontstaan door in alle woorden overal 0 door 1 en 1 door 0 te vervangen. Zo hebben we 16 woorden uit $\{0,1\}^7$. Het is eenvoudig in te zien dat deze code H *minimum afstand* 3 heeft. H is dus een [7,16,3]-code. Als we H *verlengen* tot de code $\overline{H}$ door ieder woord een achtste letter te geven en wel zó dat ieder woord van $\overline{H}$ een even aantal enen heeft, dan vinden we een code met minimumafstand 4, een [8,16,4]-code. $\overline{H}$ heeft de eigenschap dat als $\underline{a} \in \overline{H}$ en $\underline{b} \in \overline{H}$ dan ook $\underline{a} + \underline{b} \in \overline{H}$ (optelling modulo 2). (Zie Hoofdstuk III).

2.2. HADAMARD CODES EN GENERALISATIES

Zij H_n een Hadamard matrix van de orde n (zie (0.3.5)). Vervang in H_n en $-H_n$ overal -1 door 0. Dan ontstaan 2n rijen van n symbolen met onderlinge afstand $\geq \frac{1}{2}n$. Een Hadamard code is een $[n,2n,\frac{1}{2}n]$-code. Voor n = 8 vinden we de code $\overline{H}$ uit § 2.1. Voor n = 32 vinden we de code gebruikt door de Mariner '69 die in § 1.1 is genoemd.

Zij S een Paley matrix van de orde n. Beschouw de rijen van de matrices $\frac{1}{2}(S+I+J)$ en $\frac{1}{2}(-S+I+J)$ en voeg ook nog $\underline{0}$ en $\underline{1}$ toe. Uit stelling (0.3.7) volgt dat we nu een $[n,2(n+1),\frac{1}{2}(n-1)]$-code geconstrueerd hebben. Voor n = 9 vinden we de code bestaande uit de rijen van de matrix

$$\begin{pmatrix} 0\,0\,0 & 0\,0\,0 & 0\,0\,0 \\ J & P^2 & P \\ P & J & P^2 \\ P^2 & P & J \\ I & J-P^2 & J-P \\ J-P & I & J-P^2 \\ J-P^2 & J-P & I \\ 1\,1\,1 & 1\,1\,1 & 1\,1\,1 \end{pmatrix}$$

waarin I, J, en P orde 3 hebben.

De methode van § 2.1 wil ook wel eens lukken in meer ingewikkelde situaties. Beschouw de code C van lengte 8 die bestaat uit $\underline{0}$, $\underline{1}$, en alle cyclische permutaties van (1,1,0,1,0,0,0,0), (1,1,1,0,0,1,0,0), (1,0,1,0,1,0,1,0). Men ga zelf na dat dit een [8,20,3]-code is. Zo'n code krijgen we ook als we in de [9,20,4]-code in elk woord de laatste letter weglaten.

2.3. DE BINAIRE GOLAY CODE EN AFGELEIDEN

Beschouw de (7,4)-Hamming code H uit § 2.1. We vormen H^* door de woorden van H achterstevoren te schrijven. Daarna vormen we weer $\overline{H}^*$. Dit is een [8,16,4]-code met $\overline{H} \cap \overline{H}^* = \{\underline{0},\underline{1}\}$. We vormen nu een code $\overline{C}$ met woordlengte 24 door te definieren:

$$\overline{C} := \{(\underline{a}+\underline{x},\underline{b}+\underline{x},\underline{a}+\underline{b}+\underline{x}) \mid \underline{a} \in \overline{H},\ \underline{b} \in \overline{H},\ \underline{x} \in \overline{H}^*\}$$

Hierbij zijn de optellingen modulo 2. De code $\overline{C}$ bestaat uit 2^{12} woorden. Voor $\overline{C}$ geldt, evenals voor $\overline{H}$ en $\overline{H}^*$, dat de som van twee code woorden weer een codewoord is. Om de minimum afstand van $\overline{C}$ te bepalen moeten we dus de woorden van $\overline{C}\backslash\{\underline{0}\}$ zoeken met zo weinig mogelijk enen. Voor $\underline{x} \in \overline{C}$ noemt men $d_H(\underline{x},\underline{0}) =: w(\underline{x})$ het *gewicht* van $\underline{x}$, (zie (3.1.1),(3.3.1)). Is $\underline{c}$ = $= (\underline{a}+\underline{x},\underline{b}+\underline{x},\underline{a}+\underline{b}+\underline{x})$ en is tenminste één van de vectoren $\underline{a}$, $\underline{b}$, $\underline{a}+\underline{b}$, en $\underline{x}$ gelijk aan $\underline{0}$ of $\underline{1}$ dan zien we dat $\underline{c} = \underline{0}$ of $w(\underline{c}) \geq 8$. Uit de eigenschappen van $\overline{H}$ en uit $\overline{H} \cap \overline{H}^* = \{\underline{0},\underline{1}\}$ volgt dat als $\underline{a}$, $\underline{b}$, $\underline{a}+\underline{b}$ en $\underline{x}$ niet $\underline{0}$ of $\underline{1}$ zijn elk van de woorden $\underline{a}+\underline{x}$, $\underline{b}+\underline{x}$ en $\underline{a}+\underline{b}+\underline{x}$ een positief en even gewicht heeft. Was nu $w(\underline{c}) = 6$ dan zou moeten gelden $w(\underline{a}+\underline{x}+\underline{b}+\underline{x}+\underline{a}+\underline{b}+\underline{x}) =$

$= w(\underline{x}) = 6$ (ga na!). Daar $w(\underline{x}) = 4$ hebben we nu bewezen dat $w(\underline{c}) = 6$ niet kan. Dus heeft $\overline{C}$ minimum afstand 8. Dus $\overline{C}$ is een $[24,2^{12},8]$-code.

Laat nu uit alle woorden van $\overline{C}$ de laatste letter weg. We vinden een $[23,2^{12},7]$-code C, genaamde de *binaire Golay code*.

(2.3.1) DEFINITIE. Een code C met woordlengte n en minimum afstand 2e+1 heet *perfect* (en wel e-perfect) als ieder woord (van n letters) afstand $\leq$ e heeft tot een codewoord. Uit deze definitie en uit $|B_e(\underline{c})| = \sum_{i=0}^{e} \binom{n}{i}$ volgt dat een $(n,|C|,2e+1)$-code C e-perfect is als en alleen als

$$(2.3.2) \qquad |C| \sum_{i=0}^{e} \binom{n}{i} = 2^n.$$

Hieruit zien we dat de code H uit § 2.1 perfect is (daar $16(1+7) = 2^7$). De binaire Golay code C is ook perfect: C is een 3-error-correcting code en

$$|C| \sum_{i=0}^{3} \binom{23}{i} = 2^{12}(1+23+253+1771) = 2^{23}.$$

Uit onze constructie van de Golay code kan men vrij eenvoudig inzien dat er 32 codewoorden $\underline{c} = (c_1,c_2,\ldots,c_{24})$ in $\overline{C}$ zijn die met 8 nullen beginnen. Kiezen we $c_8 = 1$ en precies één van de letters c_1 t/m c_7 ook 1 dan vinden we weer 32 woorden van $\overline{C}$. We hebben zo een collectie van $32(1+7) = 256$ woorden uit $\overline{C}$ waarvan we nu de eerste 8 letters weglaten. De code N die op deze manier onstaat heet de *Nordstrom-Robinson code*. Het is een $[16,2^8,6]$-code.
Uit N construeren we door verder af te breken nog enkele interessante codes. Eerst merken we op dat in N precies 64 woorden op (0,0) eindigen. We nemen deze woorden en laten daarvan de laatste drie letters weg. Zo ontstaat een [13,64,5]-code Y. Als we uit alle woorden van Y die op een 0 eindigen deze 0 weglaten vinden we een [12,32,5]-code die de *Nadler code* wordt genoemd (zie (2.7.4)).

2.4. DE TERNAIRE GOLAY CODE

Zij S_5 de Paley matrix

$$\begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix}$$

Laat C bestaan uit alle lineaire combinaties, met coefficienten in $\mathbb{F}_3$, van de rijen van

$$G:=\left(\begin{array}{c|c} I_6 & \begin{array}{c} 1\ 1\ 1\ 1\ 1 \\ \hline \multicolumn{1}{|c|}{S_5} \\ \hline \end{array} \end{array}\right)$$

Het is natuurlijk niet handig om alle 3^6 woorden (met letters 0,+1 of -1) die zo ontstaan op te schrijven en te vergelijken. In het volgende hoofdstuk leren we technieken die ons snel in staat stellen in te zien dat deze code minimum-afstand 5 heeft en dus perfect is (zie (3.8.14)). [Merk op dat vgl. (2.3.2) welke gold voor een alfabet van twee symbolen hier

$$|C| \sum_{i=0}^{2} \binom{11}{i} 2^i = 3^{11}$$

luidt.]

Het is wellicht nuttig voor de lezer om te proberen de eigenschappen van deze code nu af te leiden zonder te beschikken over de middelen van hoofdstuk III.

2.5. COMBINATIE VAN CODES

Een bekende manier om codes te construeren is het aan elkaar plakken van woorden uit verschillende codes zoals we ook in § 2.3 gedaan hebben. Beschouw bijv. de [12,24,6]-Hadamard code uit § 2.2. Hieruit nemen we 6 woorden die met (0,0) beginnen en vormen zo een [10,6,6]-code. We plakken nu twee zulke codes aan elkaar, d.w.z. achter ieder woord schrijven we hetzelfde woord nog een keer. Hierachter zetten we 6 woorden van de [7,8,4]-code die we krijgen door de woorden van even gewicht van de (7,4)-Hamming code code te beschouwen. Zo ontstaat een [27,6,16]-code. In hoofdstuk IV zullen we zien dat een [27,M,16]-code moet voldoen aan $M \leq 6$. Onze plak-techniek levert dus een optimaal resultaat!

We geven nog een voorbeeld. Laat C_1 een $[n,M_1,d_1]$-code zijn en C_2 een $[n,M_2,d_2]$-code. Definieer

$$C := \{(\underline{x}+\underline{y},\underline{y}) \mid \underline{x} \in C_1,\ \underline{y} \in C_2\}.$$

Dan is C een $[2n,M_1M_2,d]$-code met $d := \min\{d_1,2d_2\}$. Om dit in te zien beschouwen we $d((\underline{x}_1+\underline{y}_1,\underline{y}_1),(\underline{x}_2+\underline{y}_2,\underline{y}_2))$. Als $\underline{x}_1 = \underline{x}_2$ dan is deze afstand $2d(\underline{y}_1,\underline{y}_2)$. Is echter $x_{1i} \neq \underline{x}_{2i}$ dan kan de i-de letter van $\underline{x}_1 + \underline{y}_1$ alleen gelijk zijn aan de i-de letter van $\underline{x}_2 + \underline{y}_2$ als $\underline{y}_1$ en $\underline{y}_2$ ook verschillende i-de coordinaten hebben. Dan is dus $d(\underline{x}_1,\underline{x}_2) \geq d_1$. Nemen we bijvoorbeeld voor C_1 de [8,20,3]-code uit § 2.2 en voor C_2 de $[8,2^7,2]$-code bestaande uit alle woorden van even gewicht dan vinden we een $[16,5.2^9,3]$-code. Op het ogenblik is geen [16,M,3]-code bekend met $M > 5.2^9$.

2.6. COMMENTAAR

Om didactische redenen hebben we dit hoofdstuk vóór het volgende geplaatst. Het is aan te nemen dat vele van bovenstaande voorbeelden duidelijker worden na lezing van Hoofdstuk III. We raden de lezer aan Hoofdstuk II na Hoofdstuk III te herlezen.

De Hamming code uit § 2.1 is een speciaal geval van de serie uit § 3.5. Hadamard codes komen terug in hoofdstuk VI als 1^e orde RM-codes. De beide Golay codes komen terug in de hoofdstukken V en VII. Deze codes zijn in 1949 geconstrueerd door M.J.E. Golay (zie GOLAY (1949)).

Perfecte codes behandelen we in hoofdstuk VII. De Nordstrom-Robinson code is een speciaal geval van de Preparata codes uit hoofdstuk VII. Veel meer over de Golay codes vindt men in CAMERON & VAN LINT (1975), GOETHALS (1971) en VAN LINT (1971). Over het onderwerp van § 2.5 raadplege men vooral SLOANE, REDDY & CHEN (1972) en SLOANE & WHITEHEAD (1970).

2.7. OPGAVEN

(2.7.1) Zij A_i het aantal woorden van gewicht i uit de binaire Golay code. Bewijs dat uit het feit dat deze code perfect is (met e = 3) volgt dat: $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$, en alle andere $A_i = 0$. De woorden van gewicht 7 vormen een Steiner systeem met $v = 23$, $k = 7$, $t = 4$, $\lambda = 1$. Bewijs dit.

(2.7.2) Zij S een Paley matrix van de orde 11. Beschouw de matrix A = $= \frac{1}{2}(S+I+J)$. De 11 rijen van A en alle sommen (mod 2) van twee verschillende rijen van A vormen een verzameling van 66 woorden van de lengte 11. Hieraan voegen we toe alle woorden die we krijgen door alle nullen in enen te veranderen en omgekeerd. Bewijs dat dit een [11,132,3]-code C is. Nu voegen we aan ieder woord C een letter toe zó dat de nieuwe code $\overline{C}$ alleen even gewichten heeft. Permuteer de letters zo dat (111 111 000 000) een codewoord is. Voeg nu toe (1,1,0,0,...,0), (0,0,1,1,0,0,...,0), ...,(0,0,...,0,1,1), en de zes woorden die hieruit ontstaan door weer 0 en 1 te verwisselen. Bewijs dat de nieuwe code een [12,144,4]-code is. Deze code bevat 38 woorden $\underline{c}$ met $c_{10} = 0$, $c_{12} = 1$. Deze 38 woorden vormen (na weglating van de genoemde coordinaten) een [10,38,4]-code. Bewijs dit. Tot nu toe is dit de beste code met n = 10, d = 4 die bekend is.

(2.7.3) Bewijs dat met een geschikte Paley matrix een [17,36,8]-code is te construeren.

(2.7.4) Beschouw I, J en P van de orde 3. Definieer

$$A = \begin{pmatrix} J-I & I & I & I \\ I & J-I & I & I \\ I & I & J-I & I \\ I & I & I & J-I \end{pmatrix}, \quad B = \begin{pmatrix} J & P & I & P^2 \\ P & J & P^2 & I \\ I & P^2 & J & P \\ P^2 & I & P & J \end{pmatrix},$$

$$C = (J-I \quad J-I \quad J-I \quad J-I), \qquad D = \begin{pmatrix} 000 & 111 & 111 & 111 \\ 111 & 000 & 111 & 111 \\ 111 & 111 & 000 & 111 \\ 111 & 111 & 111 & 000 \end{pmatrix}$$

Bewijs dat $\underline{0}$ en de rijen van A, B, C en D een [12,32,5]-code vormen.