
Huiswerkopgaven III

♠ Huiswerk III-1. [Universal Product Code en International Standard Book Number]

- (i) Beschouw de UPC $(0, 7, 7, 7, 7, 8, 6, 6, 3, 5, 2, c)$ van een muziek-CD. Bepaal c .
- (ii) Ga na dat de UPC $(0, 1, 2, 9, 8, 1, 7, 0, 0, 1, 2, 6)$ verminkt is; geef twee verschillende correcties van 1 cijfer die tot een correcte UPC leiden.
- (iii) Bewijs dat de UPC 1 fout kan detecteren, maar niet kan corrigeren.
- (iv) Bepaal het check-digit d van het boek met ISBN $(9, 0, 6, 1, 6, 8, 3, 7, 9, d)$.
- (v) Bewijs dat ISBN 1 fout kan detecteren, maar niet kan corrigeren.
- (vi) Bewijs dat ISBN een andere veeloptredende typefout kan detecteren, namelijk de verwisseling van 2 cijfers die naast elkaar staan.
- (vii) Is de ISBN codering lineair in de zin dat zowel de nulvector als de som van elk tweetal codewoorden een codewoord is? (Let hierbij niet op de betekenis van cijfers als landenaanduiding etc)

♠ Huiswerk III-2. [Hamming afstand]

- (i) Bewijs dat $h(v, w)$ tussen twee vectoren v, w uit $\mathbb{F}_q^n$ gelijk is aan het gewicht van de vector $v - w$.
- (ii) Laat ook zien dat de minimumafstand van een code gelijk is aan het minimumgewicht van de code, dat wil zeggen, de kleinste positieve g waarvoor een codewoord van gewicht g bestaat.
- (iii) Bewijs dat de Hammingafstand een metriek definieert, dat wil zeggen, voor alle $u, v, w \in \mathbb{F}_q^n$ geldt:
 - a) $h(v, w) \geq 0$; en $[h(v, w) = 0 \iff v = w]$;
 - b) $h(v, w) = h(w, v)$;
 - c) $h(u, v) + h(v, w) \geq h(u, w)$.

♠ Huiswerk III-3. [Even gewicht code]

- (i) Laat zien dat de vectoren van even gewicht in $\mathbb{F}_2^n$ een code vormen.
- (ii) Wat is de minimumafstand van de code uit (i)?
- (iii) Vormen de even gewicht vectoren in $\mathbb{F}_3^n$ een code?

♠ Huiswerk III-4. [Hamming codes]

- (i) Schrijf de parity-check matrix H_2 en de generatormatrix G_2 op. Waaraan is de binaire Hamming code met $r = 2$ gelijk?
- (ii) Laat zien dat de r kolommen van parity-check matrix H_r onafhankelijk zijn. Omdat de codewoorden rijvectoren v ter lengte $2^r - 1$ zijn die voldoen aan $v \cdot H_r = 0$ volgt dat de dimensie van de code $2^r - 1 - r$ is.
- (iii) Een vector v uit $\mathbb{F}_2^7$ is een codewoord uit $\mathcal{C}_3$ wanneer geldt dat het product $v \cdot H_3$ precies de nulvector oplevert (in $\mathbb{F}_2^3$). Veronderstel nu dat v de som is van een codewoord c en de vector f_j met alleen op positie j een 1 en elders nullen. Wat is dan het product $v \cdot H_3$?
- (iv) Gebruik het vorige onderdeel om te bepalen in welke coördinaat van de vector $(1, 1, 0, 1, 1, 1, 0)$ een fout geslopen is.
- (v) Bewijs dat $\mathcal{C}_r$ altijd 1-foutverbeterend is.
- (vi) Laat voor $r = 2, 3$ zien dat de Hammingcode precies de Hamming grens bereikt voor $e = 1$, en bewijs dat tenslotte voor alle $r \geq 2$.

Antwoorden III

♠ Uitwerking III-1. [Universal Product Code en International Standard Book Number]

- (i) Het inproduct van $(3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ en $(0, 7, 7, 7, 7, 8, 6, 6, 3, 5, 2, c)$ is $8 + c \in \mathbb{Z}/10\mathbb{Z}$, en dat moet 0 worden, dus $c \equiv -8 \equiv 2 \pmod{10}$, dat wil zeggen, $c = 2$.
- (ii) Het inproduct van $(3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ en $(0, 1, 2, 9, 8, 1, 7, 0, 0, 1, 2, 6)$ is $5 \in \mathbb{Z}/10\mathbb{Z}$. Je kunt één van de cijfers op even posities ophogen met 5 om een correcte UPC te krijgen, of één van de cijfers op oneven posities met 5 verhogen (want dat telt er $15 \equiv 5 \pmod{10}$ bij op). Dus bijvoorbeeld $(5, 1, 2, 9, 8, 1, 7, 0, 0, 1, 2, 6)$ of $(0, 6, 2, 9, 8, 1, 7, 0, 0, 1, 2, 6)$, etc.
- (iii) Zodra een coëfficiënt mis is van de vector, scheelt het inproduct een veelvoud van 1 of van 3 modulo 10 met het juiste antwoord 0; maar zo'n veelvoud is nooit 0 mod 10 omdat 1 en 3 allebei geen factor met 10 gemeen hebben: $3 \cdot x \equiv 0 \pmod{10}$ dan en slechts dan als x deelbaar door 10 is, dat wil zeggen, x is 0 mod 10. Als in het vorige voorbeeld kan een gemaakte fout op elke plaats 'verbeterd' worden.
- (iv) Het inproduct van $(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ en $(9, 0, 6, 1, 6, 8, 3, 7, 9, d)$ is $8 + d$, dus $d = 3$.
- (v) Op elke plaats waar een fout wordt gemaakt wordt vermenigvuldigd met een factor die onderling ondeelbaar is met de modulus 11; dat betekent weer dat op elke plaats elke fout kan ontstaan (en worden verbeterd).
- (vi) Als v_i en v_{i+1} verwisseld worden, met $1 \leq 9$, dan verschilt het nieuwe van het oude inproduct met

$$((11 - i) \cdot v_{i+1} + (11 - (i + 1)) \cdot v_i) - ((11 - i) \cdot v_i + (11 - (i + 1)) \cdot v_{i+1}) = v_{i+1} - v_i$$

en dat is alleen 0 mod 11 wanneer $v_{i+1} \equiv v_i \pmod{11}$, dat wil zeggen, wanneer beide cijfers gelijk zijn!

- (vii) Ja (want het inproduct is lineair in het tweede argument).

♠ Uitwerking III-2. [Hamming afstand]

- (i) $v_i = w_i$ dan en slechts dan als $v_i - w_i = 0$, dus het aantal posities waar v en w verschillen is gelijk aan het aantal posities waar $v - w$ ongelijk aan 0 is, en dat is het gewicht van $v - w$.
- (ii) Vanwege het vorige onderdeel is de afstand tussen v en w gelijk aan a dan en slechts dan als de vector $v - w$ gewicht a heeft, dus het minimumgewicht is hoogstens de minimumafstand. Maar als er een vector z van gewicht $b > 0$ is, dan is de afstand van z tot 0 gelijk aan b dus de minimumafstand is ook hoogstens het minimumgewicht.
- (iii) Bewijs dat de Hammingafstand op $\mathbb{F}_q^n$ voor elke n een metriek definieert: a) het is duidelijk dat het aantal posities waar twee vectoren verschillen groter of gelijk 0 is, en alleen gelijk 0 wanneer ze geheel gelijk zijn; b) het aantal posities waarop vectoren verschillen hangt natuurlijk niet af van de volgorde waarin je de vectoren neemt; c) als u en w op een positie verschillen moeten u en v dat doen of v en w (of beide), dus u en w kunnen nooit op meer plaatsen verschillen dan de som van het aantal posities waarop u en v en waarop v en w verschillen.

♠ Uitwerking III-3. [Even gewicht code]

- (i) Het is voldoende te laten zien volgens Definitie (2.4) (zeg niet: "je moet laten zien"!): dat de nulvector in de code zit (dat is duidelijk want 0 is even), dat elk $\mathbb{F}_2$ -veelvoud van een vector die in de code zit er weer in zit (ook duidelijk want dat is de nulvector of de oorspronkelijke vector zelf) en met twee vectoren ook hun som. Dat laatste is waar omdat het gewicht van $u_1 + u_2$ gelijk is aan de $w_1 + w_2 - 2p$, waar w_1 en w_2 de gewichten zijn en het aantal posities p waarop beide een 1 hebben (want daar verdwijnen twee enen); de w_1 en w_2 waren even en ook $2p$: klaar.

- (ii) Twee natuurlijk, mits $n \geq 2$.
- (iii) Nee, niet voor $n \geq 2$, want $(1, 1, 0, \dots) + (1, 2, 0, \dots) = (2, 0, 0, \dots)$ heeft oneven gewicht.

♠ **Uitwerking III-4. [Hamming codes]**

- (i) De parity-check matrix is $H_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ en daarom is de generatormatrix $G_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, dus de codewoorden zijn alleen $(0, 0, 0)$ en $(1, 1, 1)$ (want de eerste kolom van de parity check zegt dat eerste en derde coëfficiënt gelijk moeten zijn, de tweede zegt dat tweede en derde gelijk moeten zijn). De code is dus de repetitiecodel van lengte 3.
- (ii) De r kolommen zijn onafhankelijk omdat de rijen $1, 0, \dots, 0$, en $0, 1, 0, \dots, 0$ tot en met $0, 0, \dots, 1$ allemaal voorkomen. De code bestaat dus uit de deelruimte van de $2^r - 1$ -dimensionale ruimte die wordt bepaald door r onafhankelijke lineaire vergelijkingen, en dat heeft dimensie $2^r - 1 - r$.
- (iii) $(c + f_j) \cdot H_3 = c \cdot H_3 + f_j \cdot H_3 = 0 + f_j \cdot H_3$ en omdat f_j alleen een 1 heeft op positie j , is het resultaat precies de j -de rij van H_3 , en dat is weer de vector die de binaire representatie van het getal j geeft (achterstevoren).
- (iv) Het product $(1, 1, 0, 1, 1, 1, 0) \cdot H_3$ is $(0, 0, 1)$, de binaire schrijfwijze van 4 (achterstevoren), dus er zit een fout op positie 4: het codewoord was dan $(1, 1, 0, 0, 1, 1, 0)$.
- (v) Altijd is $(c + f_j) \cdot H_r$ de j -de rij uit H_r ; dus als de ontvangen vector v van de vorm $c + f_j$ is, kunnen we de enkele fout op positie j vaststellen omdat $v \cdot H_r$ gelijk is aan de binaire representatie van j (achterstevoren) en repareren door het j -de bit dan te veranderen.
- (vi) Voor $r = 2$ is $k = 2^2 - 1 - 2 = 1$ dus het aantal codewoorden is $2k = 2$, terwijl de Hamminggrens gelijk is aan $2^3/(1+3) = 2$ want $n = 2^2 - 1 = 3$. Voor $r = 3$ is $n = 2^3 - 1 = 7$ en $k = 2^3 - 1 - 3 = 4$ dus er zijn 2^4 codewoorden, terwijl de Hamminggrens gelijk aan $2^7/(1+7) = 2^4$. Voor algemene $r \geq 2$ is $n = 2^r - 1$ en $k = 2^r - 1 - r$ zodat er dus 2^{2^r-1-r} codewoorden zijn. De Hamminggrens is

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1}} = \frac{2^n}{1+n} = \frac{2^n}{1+2^r-1} = 2^{n-r} = 2^{2^r-1-r}.$$

Steeds gelijkheid dus.