

K1. (a) $\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}.$

(b) $n = 13$, $M = 3^{10}$, $d = 3$.

(c) Er geldt dat $(2, 2, 1)^T = 2(1, 1, 2)^T$. Volgens het decodeeralgoritme voor Hammingcodes moet (bij bovenstaand PC matrix) het symbool op de tiende positie veranderd worden. Van het tiende bit moet 2 worden afgetrokken (of -2 worden opgeteld of 1 worden opgeteld). De theoretische onderbouwing: Zij $\mathbf{c}$ het dichtst bij $\mathbf{x}$ gelegen codewoord en schrijf $\mathbf{x} = \mathbf{c} + \mathbf{e}$. Dan

$$S(\mathbf{x}) = H\mathbf{x}^T = H(\mathbf{c}^T + \mathbf{e}^T) = H(\mathbf{c}^T + \mathbf{e}^T) = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T$$

Voor $\mathbf{e} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0)$ geldt $H\mathbf{e}^T = (2, 2, 1)^T$. Dus $\mathbf{c} = \mathbf{x} - \mathbf{e}$.

K2. F_{7^n} is een deellichaam van $F_{7^{10}}$ als en slechts als n een deler is van 10. Er zijn dus 4 deellichamen.

K3. (a) $q = 3^4$

(b) De cyclotomische cosets voor 3 en 10 zijn $\{0\}$, $\{1, 3, 9, 7\}$, $\{2, 6, 8, 4\}$ en $\{5\}$. De ontbinding van $x^{10} - 1$ bestaat dus uit 4 irreducibele polynomen over F_3 .

(c) Uit de cyclotomische cosets volgt twee keer graad 1 en twee keer graad 4

(d) $2^4 = 16$.

K4. (a) Niet eens lineair, dus zeker niet cyclisch.

(b) Alle binaire Hamming-codes hebben een cyclische variant.

(c) $x^4 + x + 1$ is geen deler van $x^8 - 1$. De code is dus niet cyclisch.

1. (a) De kolomen 1, 2 en 5 zijn afhankelijk, want

$$2 \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} + 3 \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 8 \\ 6 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}.$$

Dat betekent dat $d \leq 3$. Verder is elk tweetal kolomen onafhankelijk (waaruit volgt dat $d \geq 3$): door de posities van de nullen in de eerste, tweede en vierde kolom is dat direct duidelijk voor elk tweetal waarvan tenminste één kolom de eerste, tweede of vierde is. Rest te checken dat de derde en vijfde kolom onafhankelijk zijn. Ga daarvoor na dat

$$\begin{bmatrix} 4 & 3 \\ 1 & 1 \\ 3 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 \\ 0 & 4 \\ 0 & 0 \end{bmatrix}$$

waaruit volgt dat de derde en vijfde kolom inderdaad onafhankelijk zijn. De minimale afstand is dus 3.

(b) Het syndroom van de codewoorden is $\mathbf{0}$ en de bijbehorende cosetleider is het nulwoord. Verder heeft de code $d = 3$ dus de code is één-fout verbeterend. Het gevolg is dat alle woorden van gewicht 1 cosetleider zijn. Er zijn twintig woorden met gewicht 1. Omdat er in totaal $5^3 = 125$ syndromen zijn zijn er ook 125 cosetleiders. Hiervan hebben er 21 gewicht nul of één. De resterende 104 cosetleiders hebben dus gewicht 2 of meer.

2. (a) Het generatorpolynoom is het kleinste gemene veelvoud van de minimaalpolynomen van α^1 , α^2 , α^3 en α^4 waarbij α een primitieve 15-de eenheidswortel is. Deze is te vinden in het splitslichaam van $x^{15} - 1$ en dat is F_{16} (immers: 4 is de eerste m waarvoor geldt dat 15 een deler is van $2^m - 1$). Blijkbaar is α tevens een primitief element van F_{16} .

De cyclotomische coset van 1 voor $n = 15$ en $p = 2$ is $\{1, 2, 4, 8\}$ en die van 3 is $\{3, 6, 12, 9\}$. De minimaalpolynomen van α^2 en van α^4 zijn dus hetzelfde als die van α en $g(x)$ is blijkbaar het product van twee irreducibele polynomen, elk van graad 4. Het minimaalpolynoom van α is eenvoudig te vinden, want het is het polynoom waarnaar is uitgedeeld, dus $x^4 + x^3 + 1$

(voor α geldt namelijk dat $\alpha^4 = \alpha^3 + 1$ en dus is α nulpunt van het irreducibele polynoom $x^4 + x^3 + 1$). Het minimaalpolynoom van α^3 is wat meer werk. Het is

$$\begin{aligned}
m_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\
&= x^4 - (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21})x^2 \\
&\quad - (\alpha^{18} + \alpha^{21} + \alpha^{24} + \alpha^{27})x + \alpha^{30} \\
&= x^4 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x^3 + (\alpha^9 + \alpha^{12} + \alpha^3 + \alpha^6)x^2 \\
&\quad + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12})x + 1 \\
&= x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

- (b) Er geldt $d \geq \delta$. Bij C_2 is δ gelijk aan 5, dus $d \geq 5$. Merk verder op dat de codewoorden van C_2 bekend zijn, ze bestaan immers uit de coëfficiënten van de polynomen uit $\{(1 + x + x^2 + x^4 + x^8)p(x) \mid \deg(p) < 7\}$. In het bijzonder vormen de coëfficiënten van $1 + x + x^2 + x^4 + x^8$, dus 111010001000000, een codewoord (neem maar $p(x) = 1$). Dit woord heeft gewicht 5 en dus is $d \leq 5$. Conclusie: $d = 5$.
- (c) Zie de volgende tabel. Herinner daarbij dat r de graad van het minimaalpolynoom is en dat $k = n - r$. Voor het bepalen van r (de graad van het generatorpolynoom) gebruik je de cyclotomische cosets. Die zijn $\{1, 2, 4, 8\}$, $\{3, 6, 12, 9\}$, $\{5, 10\}$ en $\{7, 14, 13, 11\}$

t	δ	n	r	k	rate
1	3	15	4	11	11/15
2	5	15	8	7	7/15
3	7	15	10	5	5/15
4	9	15	14	1	1/15
5	11	15	14	1	1/15
6	13	15	14	1	1/15
7	15	15	14	1	1/15

3. (a) Als we modulo $x^2 + 1$ rekenen volgt $(x + 1)^2 = x^2 + 2x + 1 = 2x$, $(x + 1)^4 = (2x)^2 = 4x^2 = -4 = 2$ en $(x + 1)^8 = 2^2 = 1$. Blijkbaar is de orde van $x + 1$ een deler van 8. De orde is dus 1, 2, 4 of 8. Omdat $x + 1$, $(x + 1)^2$ en $(x + 1)^4$ allemaal niet gelijk zijn aan 1 is de orde 8.
- (b) Merk op dat de ring R 9 elementen bevat, blijkbaar de 8 machten van $x + 1$ en 0.
Methode 1: Blijkbaar is $R \setminus \{0\}$ de cyclische groep voortgebracht door $x + 1$ en die is abels onder vermenigvuldiging. R is dan een lichaam! (slide 3.2.5)
Andere manier: R is een commutatieve ring met 1. Verder heeft het geen nuldelers. Stel namelijk dat $a \neq 0$ en $b \neq 0$. Dan $a = (x + 1)^{n_1}$ en $b = (x + 1)^{n_2}$. Dus $ab = (x + 1)^{n_1 + n_2}$, één van de elementen van $R \setminus \{0\}$. Dus $ab \neq 0$ en R is dus een (eindig!) integriteitsgebied. En dat is een lichaam (slide 3.2.6).
4. (a) Merk op dat $\text{Im } \phi$ een deelruimte is van de één-dimensionale ruimte F_q . $\text{Im } \phi$ is dus nul- of één-dimensionaal en in het tweede geval surjectief. Stel daarom dat $\dim \text{Im } \phi = 0$. Dat betekent dat ϕ de nulafbeelding is, wat op zijn beurt betekent dat alle codewoorden op positie i een nul hebben staan. Zij C' de code die uit C ontstaat door de i^e positie te verwijderen. Dan is C' een $[n', k', d']$ code met $n' = n - 1$, $k' = k$ (het aantal woorden is immers niet veranderd) en $d' = d$ (de bits die verwijderd zijn waren allemaal nul, zodat de afstand tussen de woorden niet is veranderd). Omdat C een MDS code is, is $k = n - 1 + d$, dus $k' = n' + d' > n' + d' - 1$ en dat kan niet volgens de Singleton bound. Conclusie: $\dim \text{Im } \phi = 1$ en ϕ is dus surjectief.
Andere methode: Bij de vorige uitwerking is al aangetoond dat we alleen maar hoeven te laten zien dat ϕ niet de nulafbeelding kan zijn. Stel het is wel de nulafbeelding. Dan betekent dit dat alle codewoorden op positie i een nul hebben staan. Maak dan de code C' uit C door bij alle codewoorden positie i te verwijderen. Voor C' geldt dat het aantal codewoorden M' gelijk is aan het aantal woorden M van C , dat de lengte n' gelijk is aan $n - 1$ is en dat de minimale afstand d' gelijk is aan d , de minimale afstand van C . De Singletonbound geeft dan $M' \leq q^{n' - d' + 1} = q^{n - d} < q^{n - d + 1} = M$. Tegenspraak. Hierbij gebruikte ik dat C een MDS-code is.

- (b) Dat zijn de woorden uit C die op positie i een nul hebben. Verder $\dim \text{Ker } \phi = \dim C - \dim \text{Im } \phi = k - 1$.
- (c) Het is duidelijk dat het aantal woorden in C' gelijk is aan het aantal woorden in $\text{Ker } \phi$. Dus $k' = \dim C' = k - 1$. Verder is de lengte van de woorden gelijk aan $n - 1$. Volgens de Singletonbound geldt dus dat

$$d' \leq n' - k' + 1 = (n - 1) - (k - 1) + 1 = n - k + 1 = d.$$

Verder is $d' \geq d$ want de afstand tussen de woorden van C' is gelijk aan de afstand tussen de oorspronkelijke woorden uit C en die was tenminste d . Dus $d' = d$ en de Singletonbound geeft gelijkheid. De code is dus MDS.