

Tentamen Toegepaste Algebra, TW2560
 vrijdag 15 april 2016, 13:30-16:30 uur.

Naam:

Cijfer :

Studienummer:

--	--	--	--	--	--	--

Dit werk bestaat uit twee delen: kort-antwoord-vragen en open vragen. Bij de open vragen dient elk antwoord te worden beargumenteerd. Er mogen geen hulpmiddelen als mobiele telefoons, laptops, formulebladen en dergelijke gebruikt worden. Alleen een eenvoudige niet-programmeerbare, niet-grafische rekenmachine (de TI-30 en de Casio FX-82, en de verschillende varianten van deze machines) is toegestaan. Het cijfer wordt bepaald door bij het aantal behaalde punten 5 op te tellen en vervolgens te delen door 5.

deel kort antwoord vragen

- (2) **K1.** (a) Geef een parity-check matrix voor een Ham(3, 3) code C .

- (2) (b) Wat zijn de parameters n , M en d van C ?

$n =$	$M =$	$d =$
-------	-------	-------

- (2) (c) Het syndroom van een ontvangen woord $\mathbf{x}$ blijkt gelijk te zijn aan $(2, 2, 1)^T$. De decoding naar het dichtstbijzijnde codewoord verkrijg je door bij positie i de waarde a op te tellen. Voor i en a geldt:

$i =$	$a =$
-------	-------

- (2) **K2.** Hoeveel deellichamen heeft het lichaam $F_{7^{10}}$? Tel hierbij $F_{7^{10}}$ ook mee!

- (2) **K3.** (a) Wat is q als F_q het splijtlichaam is van $x^{10} - 1$ over F_3 ?

- (2) (b) Uit hoeveel irreducibele polynomen bestaat de ontbinding van $x^{10} - 1$ over F_3 ?

- (2) (c) En wat zijn de graden van deze irreducibele polynomen?

- (2) (d) Hoeveel cyclische codes van lengte 10 zijn er over F_3 ?

K4. Haal bij elk van de volgende beweringen door wat niet van toepassing is:

- (1) (a) De binaire code $\{10110, 01011, 10101, 11010, 01101\}$ is cyclisch.

- (1) (b) De Hamming-code Ham(2, 5) (sus $q = 2$ en $r = 3$) heeft een cyclische verschijningsvorm.

- (1) (c) De binaire code $C = \{(x^4 + x + 1)f(x) \mid f(x) \in F_2[x], \deg f \leq 3\}$ is cyclisch.

1. C is de code over F_5 met parity-check matrix

$$H = \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}.$$

- (3) (a) Wat is de minimale afstand d van C ?
- (3) (b) Als je met deze code wilt decoderen is het voor de hand liggend om met een cosettabel te werken. Hierin staan de syndromen en de bijbehorende cosetleiders. Hoeveel van deze cosetleiders hebben gewicht twee of meer?

2. C_t is de binaire BCH code met parameters $n = 15$ en $\delta = 2t + 1$ ($0 < t < 8$) (en $b = 1$).

- (3) (a) Het generatorpolynoom van C_2 is het product van een aantal minimaalpolynomen. Bepaal één van deze minimaalpolynomen.

Het generatorpolynoom voor C_2 blijkt $g(x) = 1 + x + x^2 + x^4 + x^8$ te zijn.

- (2) (b) Wat is de minimale afstand van C_2 ?
- (3) (c) Bepaal voor alle $0 < t < 8$ de code rate van C_t .

3. Gegeven is de ring $R = F_3[x]/(x^2 + 1)$.

- (2) (a) Wat is de orde van $x + 1$ in R^* (dat is de groep die bestaat uit elementen van R die een multiplicatieve inverse hebben).
- (3) (b) Kun je uit je antwoord op (a) concluderen dat R een lichaam is?

4. Zij C een lineaire $[n, k]$ code over F_q die MDS is.

[HERINNER: Een code is MDS als de Singleton-bound gelijkheid geeft.]

- (3) (a) Definieer $\phi : C \rightarrow F_q$ door $\phi(\mathbf{c}) = c_i$ waarbij c_i de i^e coördinaat is van $\mathbf{c}$. Het is niet moeilijk om in te zien dat ϕ een lineaire afbeelding is (je hoeft dit niet aan te tonen). Bewijs dat ϕ surjectief is.
- (2) (b) Waarom is de dimensie van de kern van ϕ gelijk aan $k - 1$? Wat kun je zeggen over de woorden uit $\text{Ker } \phi$?

We maken de op de i^e coördinaat verkorte (engels: shortened) code C' van C als volgt: neem de woorden van C die op positie i een nul hebben en verwijder van al deze woorden de nul van die positie.

- (3) (c) Toon aan dat de zo verkregen code een $[n - 1, k - 1]$ MDS code is. [AANWIJZING: Gebruik (b).]