TOEPASSINGEN VAN ALGEBRA IN DE INFORMATICA

Woensdag 11 juni 2008

Informatica

- Het examen is volledig schriftelijk. Schrijf netjes en overzichtelijk en schrijf uw naam op elk blad. Geef voldoende tussenresultaten, zodat bij rekenfouten kan nagegaan worden of u het principe begrepen hebt.

- Het gebruik van (alle soorten) rekenmachines is toegestaan.

- Het examen bestaat uit 4 vragen en is opgesteld om opgelost te worden op **4 uur**. Een suggestie voor de tijdsverdeling:

  – 30 min. voor vraag 1,

  – 1u. voor vraag 2,

  – 1u. 30 min. voor vraag 3

  – 1u. voor vraag 4.

- Na het examen geeft u af :

  – de opgave,

  – de antwoorden op de vragen en

  – alle kladbladen en niet-beschreven bladen.

  Leg de netbladen op volgorde (vraag 1 eerst, enz). Steek de kladbladen achter de netbladen. Plooi de opgavebladen rond alle andere bladen en geef alles af in één stapeltje. De kladbladen worden normaal niet bekeken.

Veel succes
Ann Haegemans

Examenvragen

1. De pariteitstestmatrix van de (6,4) Hamming-code over GF(5) is de volgende:
   $$H = \begin{bmatrix} 1 & 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$
   (a) Bepaal de bijhorende generatormatrix.
   (b) Codeer het informatiewoord: $i = 1\ 2\ 3\ 4$.
   (c) Decodeer het ontvangen woord: $v = 2\ 0\ 2\ 0\ 4\ 3$. Wat is het bijhorende informatiewoord?

2. Gegeven een (10,4) RS-code over GF(11) die 3 fouten kan verbeteren. l werd gelijk aan 2 gekozen. De primitieve 10e wortel uit 1 werd geconstrueerd op basis van de primitieve veelterm $5 + x$ over GF(11). De foutlocatorveelterm van een ontvangen woord is $\Lambda(x) = 2 + x^2$ en enkele syndromen zijn $S_1 = 6$, $S_4 = 2$, $S_6 = 7$. Bepaal de overige syndromen en bepaal met het PGZ-algoritme (pag. 64) de plaats en de waarde van de fouten.

3. Beschouw een BCH-code van lengte 12 over GF(5) die 3 fouten kan verbeteren. l werd gelijk aan 0 gekozen.
   (a) Bepaal de generatorveelterm van de code.
   U mag de veelterm laten staan als een product van factoren met **coëfficiëenten in GF(5)**.
   (b) Wat is de dimensie van de code? Wat zou de dimensie geweest zijn als $l = 8$ werd gekozen? Is de keuze $l = 0$ een goede keuze?
   (**Let op**: voor het vervolg van de vraag is l steeds gelijk aan 0.)
   (c) Op bijgevoegd blad (pag. 5) vindt u tabellen met machten van een primitief element α van GF(25) over GF(5). In de tabel voor GF(25) ontbreken een aantal elementen (ook achteraan de tabel!). Vul de tabel (pag. 5) verder aan. Schrijf ook het antwoord op vraag 1.(d) op dit blad. Schrijf uw naam op dat blad en geef het aan de assistent. In ruil hiervoor krijgt u een volledig ingevulde tabel, een tabel met de 'omgekeerden' en een tabel met de juiste syndromen.
   (d) Van het ontvangen woord
   $v = 2\ 4\ 3\ 2\ 4\ 1\ 1\ 3\ 0\ 0\ 0\ 0$
   (**Let op**: laagstegraadscoëfficiënt staat links!)
   zijn enkele syndromen:
   $S_3 = \alpha^{12}$, $S_5 = \alpha^{21}$, $S_6 = \alpha^{23}$.
   Bepaal de ontbrekende syndromen. Schrijf deze ontbrekende syndromen (eventueel samen met de berekeningswijze) ook op het blad waar u 1.(c) beantwoord hebt (pag. 5). Wanneer u dit afgeeft krijgt u van de assistent een tabel met de juiste syndromen.

   Hint: Stelling 22 pag. 20 kan helpen; bekijk eens de cyclotomische nevenklassen die u in 1.(a) opgesteld hebt.
   Hint: $\alpha^6 = 3$.

(e) Voor het ontvangen woord waarvan de syndromen in 1.(d) gegeven en berekend werden is een gedeelte van de tabel voor het algoritme van Berlekamp-Massey gegeven op de volgende bladzijde. Vervolledig de tabel (d.w.z. vul de nodige lege hokjes in). Achteraan (pag. 6) vindt u een copie van deze tabel. Dat blad geeft u ingevuld mee af met het net (vergeet niet uw naam op dit blad te schrijven!).

s	Δ	n	d	$\Lambda(x)$	$\Lambda^\star(x)$
0	/				
1					
2					
3		1		$\alpha^5 x + x^2$	
4	α^1		2		α^5
5				$\alpha^{18} + \alpha^5 x + x^2$	
6	0	4			
7					

Hint: maak zoveel mogelijk gebruik van eigenschappen i.v.m. de veeltermen die in het algoritme van Berlekamp Massey voorkomen; als u uit de theorie b.v. weet dat een bepaald element 0 is hoeft u dat niet te berekenen (u kan dit natuurlijk steeds als controle doen).

(f) Wat zijn mogelijke $\phi^{(d)}(x)$, $d = 0, 1, 2, 3$?
Wat is μ_d, $d = 0, 1, 2, 3$?
(Voor de definitie van $\phi^{(d)}(x)$ en μ_d zie pag. 67).

(g) Construeer de matrix $R^{(3)}$ (definitie pag. 70, zie ook pag. 72). Haal de gegevens hiervoor uit de tabel van Berlekamp-Massey. Voor van nul verschillende elementen die u niet rechtstreeks uit de tabel kunt aflezen mag u 'X' invullen.

(h) Bepaal de plaats van alle fouten als u weet dat α^{22} een nulpunt is van $\Lambda(x)$.

(i) Bepaal met het algoritme van Forney de waarde van één van de fouten. U mag gebruik maken van de reeds gedeeltelijke berekende veelterm
$\Omega(x) = ... + \alpha^6 x + ...$

4. In de tekst over convolutionele codes wordt als voorbeeld meestal de convulutionele code met $k_0 = 1$, $n_0 = 2$ en $\nu = 2$ (zie notaties pag. 112) met generatorveeltermen $g^{(1)} = X^2 + X + 1 = (7)$ en $g^{(2)} = X^2 + 1 = (5)$ gebruikt. We noteren dit als de code (7,5) met minimale afstand $d_{\text{min}} = 3$ en vrije afstand $d_\infty = 5$ (zie pag. 116).
In de oefenzittingen hebben we een andere code met $k_0 = 1$, $n_0 = 2$ en $\nu = 2$ gebruikt: de code (7,3) met $d_{\text{min}} = 3$ en $d_\infty = 4$.

(a) Bepaal **alle** verschillende niet catastrofische codes (zie def. pag. 117-118) met $k_0 = 1$, $n_0 = 2$ en $\nu = 2$. (Codes zoals (7,5) en (5,7) waarbij we de twee uitvoerbits van plaats verwisselen noemen we niet verschillend!).

(b) Bepaal voor **een** onder (a) gevonden code (niet de (7,5) code van het boek en niet de (7,3) code van de oefeningen!) d_{min} en d_∞.
U kan eventueel gebruik maken van de tabellen en/of de trellis op pag. 7 en 8 respectievelijk.

Tabel met machten van α, primitief element van GF(25),
nulpunt van $3+3x+x^2$ over GF(5).
In de volgende tabel bedoelen we met [2 3]: $2+3\alpha=\alpha^9$ enz.

α^0	$=$	[1 0]	α^5	$=$	[2 4]	α^{10}	$=$		α^{15}	$=$	[1 4]	α^{20}	$=$	[4 4]
α^1	$=$	[0 1]	α^6	$=$	[3 0]	α^{11}	$=$		α^{16}	$=$	[3 4]	α^{21}	$=$	[3 2]
α^2	$=$		α^7	$=$	[0 3]	α^{12}	$=$	[4 0]	α^{17}	$=$	[3 1]			
α^3	$=$	[4 1]	α^8	$=$	[1 1]	α^{13}	$=$	[0 4]	α^{18}	$=$	[2 0]			
α^4	$=$	[2 1]	α^9	$=$	[2 3]	α^{14}	$=$	[3 3]	α^{19}	$=$	[0 2]			

Syndromen:

$S_1=$

$S_2=$

$S_4=$

k	1	2	3	4	5	6
S_k			α^{12}		α^{21}	α^{23}

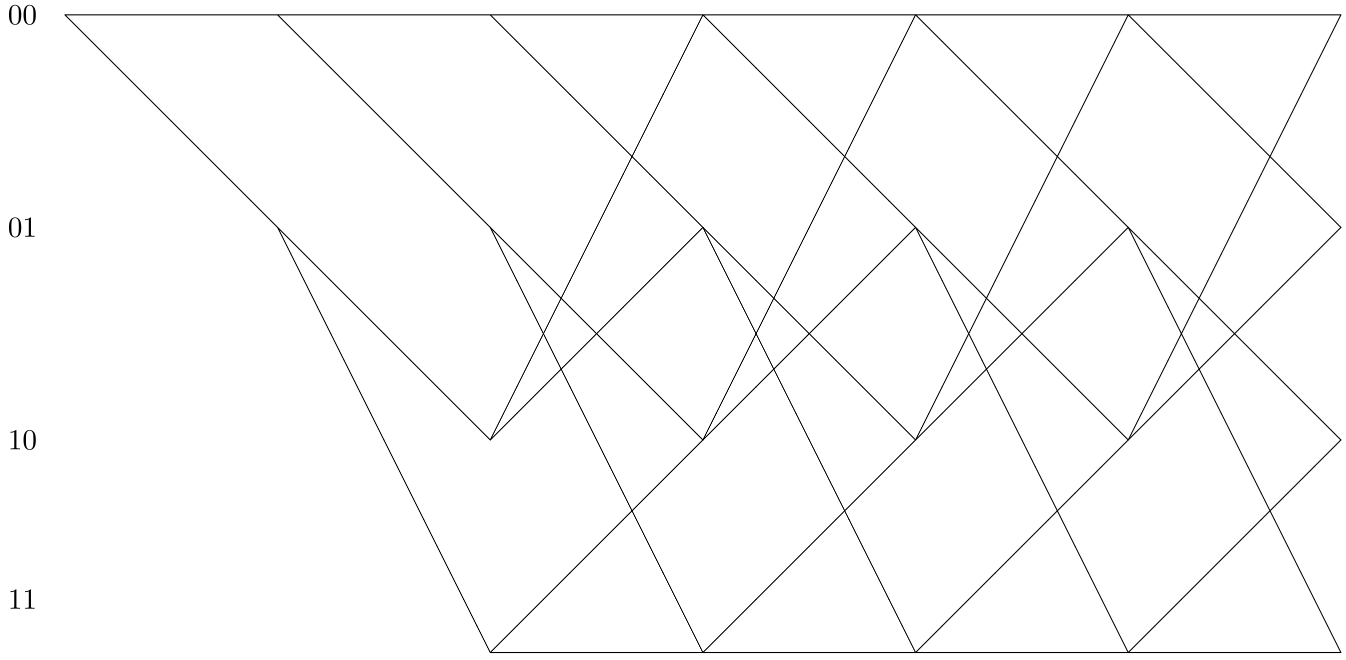
s	Δ	n	d	$\Lambda(x)$	$\Lambda^{\star}(x)$
0	/				
1					
2					
3		1		$\alpha^5 x + x^2$	
4	α^1		2		α^5
5				$\alpha^{18} + \alpha^5 x + x^2$	
6	0	4			
7					

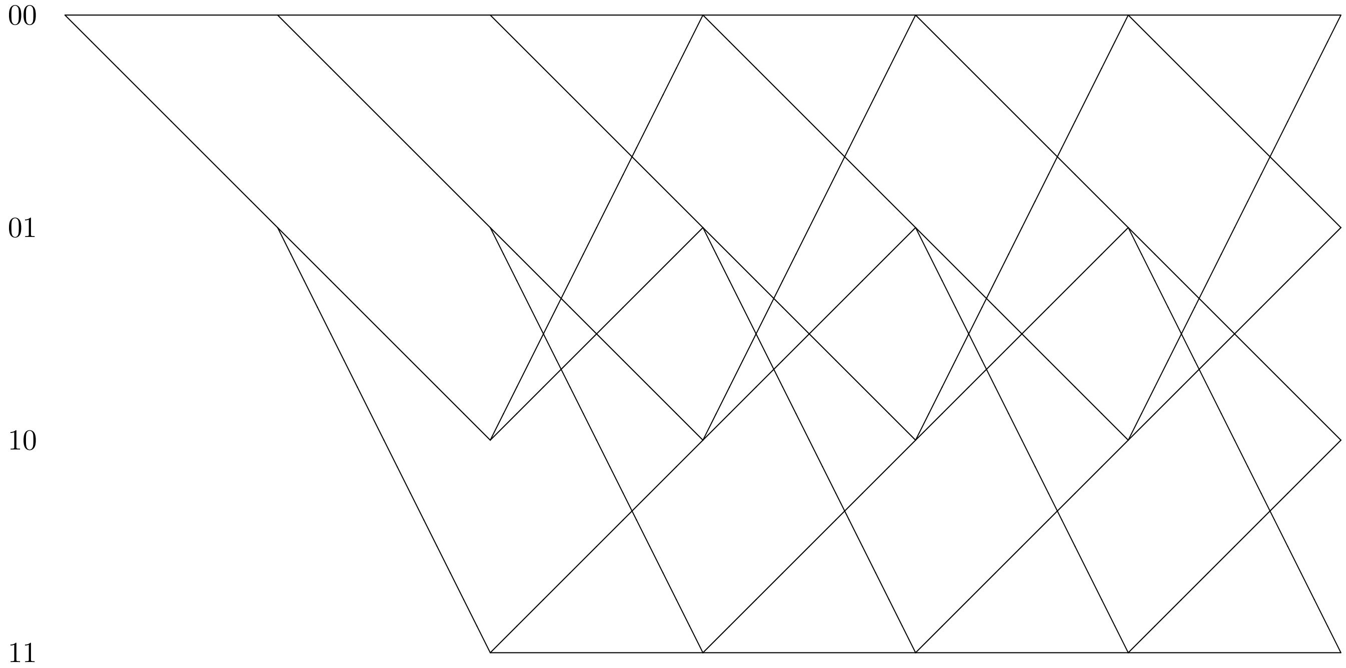
E.T. = eindtoestand B.T. = beingtoestand uitv. = uitvoer tak
F-tak = fout tak B-tak = fout bij begin v.d. tak E-tak = fout bij einde v.d. tak

E.T.	B.T.	uitv.	F-tak	B-tak	E-tak	Kies
00	00					
00	10					
01	00					
01	10					
10	01					
10	11					
11	01					
11	11					

E.T.	B.T.	uitv.	F-tak	B-tak	E-tak	Kies
00	00					
00	10					
01	00					
01	10					
10	01					
10	11					
11	01					
11	11					

E.T.	B.T.	uitv.	F-tak	B-tak	E-tak	Kies
00	00					
00	10					
01	00					
01	10					
10	01					
10	11					
11	01					
11	11					


00
01
10
11


00
01
10
11

Tabel met machten van α, primitief element van GF(25),
nulpunt van $3 + 3x + x^2$ over GF(5).
In de volgende tabel bedoelen we met [2 3]: $2 + 3\alpha = \alpha^9$ enz.

α^0	=	[1 0]	α^5	=	[2 4]	α^{10}	=	[1 3]	α^{15}	=	[1 4]	α^{20}	=	[4 4]
α^1	=	[0 1]	α^6	=	[3 0]	α^{11}	=	[1 2]	α^{16}	=	[3 4]	α^{21}	=	[3 2]
α^2	=	[2 2]	α^7	=	[0 3]	α^{12}	=	[4 0]	α^{17}	=	[3 1]	α^{22}	=	[4 2]
α^3	=	[4 1]	α^8	=	[1 1]	α^{13}	=	[0 4]	α^{18}	=	[2 0]	α^{23}	=	[4 3]
α^4	=	[2 1]	α^9	=	[2 3]	α^{14}	=	[3 3]	α^{19}	=	[0 2]			

Tabel met 'omgekeerden':

			[1 0]	=	α^0	[2 0]	=	α^{18}	[3 0]	=	α^6	[4 0]	=	α^{12}
[0 1]	=	α^1	[1 1]	=	α^8	[2 1]	=	α^4	[3 1]	=	α^{17}	[4 1]	=	α^3
[0 2]	=	α^{19}	[1 2]	=	α^{11}	[2 2]	=	α^2	[3 2]	=	α^{21}	[4 2]	=	α^{22}
[0 3]	=	α^7	[1 3]	=	α^{10}	[2 3]	=	α^9	[3 3]	=	α^{14}	[4 3]	=	α^{23}
[0 4]	=	α^{13}	[1 4]	=	α^{15}	[2 4]	=	α^5	[3 4]	=	α^{16}	[4 4]	=	α^{20}

Syndromen:

k	1	2	3	4	5	6
S_k	0	α^{19}	α^{12}	α^{18}	α^{21}	α^{23}