

TAI Examen juni 2008

1.) (6,4) Hamming code over $GF(5)$

parititsmatrix:

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

a.) Bepaal G

$$\tilde{H} = [-P^T | I]$$

$$\tilde{H} = \left[\begin{array}{cccc|cc} 3 & 4 & 1 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{array} \right]$$

$\underbrace{\hspace{1.5cm}}_{-P^T}$

wissel kolommen van H :

$$K_1 \leftrightarrow K_5$$

$$K_2 \leftrightarrow K_6$$

$$\tilde{G} = [I | P]$$

$$\tilde{G} = \left[\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & -3 & -1 \\ 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -4 & -1 \\ 0 & 0 & 0 & 1 & -2 & -1 \end{array} \right] = \left[\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 & 3 & 4 \end{array} \right]$$

$\underbrace{\hspace{1.5cm}}_{I_4} \quad \underbrace{\hspace{1.5cm}}_{P}$

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

Kolomwissels:

$$K_1 \leftrightarrow K_5$$

$$K_2 \leftrightarrow K_6$$

de generatormatrix

$$b.) \quad c = 1234$$

$$C = cG$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 \\ 4 & 4 & 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 28 & 10 & 3 & 4 & 12 \end{bmatrix} \pmod{5} = \begin{bmatrix} 3 & 0 & 3 & 4 & 2 \end{bmatrix}$$

$\begin{matrix} \text{"} \\ c \end{matrix}$
 $\begin{matrix} \text{"} \\ G \end{matrix}$
 $\begin{matrix} \text{"} \\ C \end{matrix}$

$$c = [3 \ 0 \ 3 \ 4 \ 2]$$

$$c.) \quad r = [2 \ 0 \ 2 \ 0 \ 4 \ 3]$$

Syndroomtabel:

Wat nodig is zelf, enkel voor te krijgen	Syndroom	Uitlegwoorden
	00	000000 (geen fout)
	10	100000
	01	010000
Kopieus	11	001000
betonnen	21	000100
uit H in	31	000010
volgorde	41	000001

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

Algemeen: De plaats in de volgorde n/d syndroom bepaalt welk teken fout is
(3^e syndroom → fout in 3^e teken)

$$s = rH^T$$

$$s = [2 \ 0 \ 2 \ 0 \ 4 \ 3] \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 28 & 9 \end{bmatrix} \pmod{5} = \begin{bmatrix} 3 & 4 \end{bmatrix}$$

$\begin{matrix} \text{"} \\ s \end{matrix}$

$$s = \begin{bmatrix} 3 & 4 \end{bmatrix} \rightarrow e = ?$$

$\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ komt niet voor als kolom van H

Maar wel een veelvoud van $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$!

$$4 \cdot \begin{bmatrix} 3 \\ 4 \end{bmatrix} \pmod{5} = \begin{bmatrix} 12 \\ 16 \end{bmatrix} \pmod{5}$$

(Herinner je dat de kolommen van H geen veelvouden van elkaar mochten zijn.)

$$= \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

En dit is de 4^e kolom uit H

$$e = 4 \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$e = \begin{bmatrix} 0 & 0 & 0 & 4 & 0 & 0 \end{bmatrix}$$

Fout op het 4^e karakter uit v

$$s = \begin{bmatrix} 3 & 4 \end{bmatrix} = 4 \begin{bmatrix} 2 & 1 \end{bmatrix}$$

des 4×4^e kolom van H

$$c = v - e$$

$$= \begin{bmatrix} 2 & 0 & 2 & 0 & 4 & 3 \end{bmatrix} - \begin{bmatrix} 0 & 0 & 0 & 4 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 & 2 & -4 & 4 & 3 \end{bmatrix} \pmod{5}$$

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

2.) $(10, 4)$ RS code over $GF(11)$

$$n = 10$$

$$q = 11$$

$$t = 3 \quad (\# \text{ fouten dat kan worden gecorrigeerd})$$

$5 + x$ primitieve veelterm over $GF(11)$

$\beta = \alpha$ is de primitieve 10^{e} wortel uit 1
(want: RS code)

$$\Lambda(x) = 2 + x^2 \quad \text{foutlocatorveelterm}$$

$$\text{Syndromen: } S_1 = 6 \quad S_6 = 7 \\ S_4 = 2$$

Bepaal overige syndromen:

$$\text{eig.: } \sum_{m=0}^r \Lambda_m S_{j+m} = 0 \quad \text{voor } j = 1, \dots, 2t-r$$

(eig (2) p 62)

met Λ_m de m^{e} coëff uit $\Lambda(x)$

merk op:

Λ_1 is altijd
gelijk aan 1

(hier: $\Lambda_2 = 1$)

$\Lambda(x)$ is monisch

$$\text{coëff van } \Lambda(x) \text{ zijn: } \begin{bmatrix} 2 & 0 & 1 \\ \Lambda_0 & \Lambda_1 & \Lambda_2 \end{bmatrix} \quad (\text{want } \Lambda(x) = 2 + x^2)$$

$$\text{Dus geldt: } 2S_i + S_{i+2} = 0 \quad \text{voor } i = 1, \dots, 2t-r$$

(met 1 aantal fouten in α)

Er zijn $2t$
syndromen
(=6)

$$\begin{aligned} 2S_1 + S_3 &= 0 & 2S_3 + S_5 &= 0 \\ 2S_4 + S_6 &= 0 \\ 2S_2 + S_4 &= 0 \end{aligned}$$

We weten uit de generator veelterm ook al dat $v=2$ (het aantal fouten in r is 2)

$$2S_1 + S_3 = 0$$

$$12 + S_3 = 0$$

$$S_3 = -10 \pmod{11}$$

$$2S_2 + S_4 = 0$$

$$2S_2 = -2$$

$$6(2S_2) = 6(-2)$$

$$S_2 = 10 \pmod{11}$$

$$2S_3 + S_5 = 0$$

$$20 + S_5 = 0$$

$$S_5 = -20 \pmod{11}$$

Syndromen:

$$S_1 = 6$$

$$S_2 = 10$$

$$S_3 = 10$$

$$S_4 = 2$$

$$S_5 = 2$$

$$S_6 = 7$$

- Gebruik het PG-2 algoritme om de plaats en waarde v/d fouten te bepalen: (algoritme p 64)

Step 1 (bepalen v/d syndromen) reeds gedaan

Step 2: $r=t=3$

Fout: we weten dat $v=2$

Invertieerbare Hankelmatrix (als $v=3$ fouten leest)

$$H^v = H^3 = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} 6 & 10 & 10 \\ 10 & 10 & 2 \\ 10 & 2 & 2 \end{bmatrix}$$

We kunnen step 2 en 3 overslaan

Step 3:

$$\begin{aligned} \det(H^3) &= 6(10 \cdot 2 - 2 \cdot 2) - 10(10 \cdot 2 - 10 \cdot 2) \\ &\quad + 10(10 \cdot 2 - 10 \cdot 10) \\ &= -704 \\ &= 0 \pmod{11} \end{aligned}$$

Ok, we weten dat $v=3$ en moeten deze niet verkleinen

Het ontvanger woord v bevat dus 2 fouten

Stap 4:

Dere stap is
het bepalen
van $\Lambda(x)$,
maar die is
reeds gegeven
Zie dus over

$$H^{(3)} \begin{bmatrix} \Lambda_0 \\ \Lambda_1 \\ \Lambda_2 \end{bmatrix} = \begin{bmatrix} S_4 \\ S_5 \\ S_6 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 10 & 10 \\ 10 & 10 & 2 \\ 10 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$$

Maar we kennen Λ_0, Λ_1 en Λ_2
(in de $\Lambda(x)$) al, dus
slaan deze stap over.

→

Bepaal nulpunten van

$$\Lambda(x) = 2 + x^c = 0$$

We proberen alle machten van x in $\Lambda(x)$
in te vullen en kijken of die 0 geeft.

Vit prim. veld $x+5$ weten we dat

$$x+5=0$$

$$x = -5 = 6 \pmod{11}$$

Plaats:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

$$\alpha^0 = 1$$

$$\alpha^1 = 6$$

$$\alpha^2 = 6^2 = 36 \pmod{11} = 3$$

$$\alpha^3 = 7$$

$$\alpha^4 = 9$$

$$\alpha^5 = 10$$

$$\alpha^6 = 5$$

$$\alpha^7 = 8$$

$$\alpha^8 = 4$$

$$\alpha^9 = 2$$

$$(\alpha^{10} = \alpha^0 = 1)$$

$$\Lambda(1) = 3$$

$$\Lambda(6) = 5$$

$$\Lambda(3) = 0$$

$$\Lambda(7) = 7$$

$$\Lambda(9) = 6$$

$$\Lambda(10) = 3$$

$$\Lambda(5) = 5$$

$$\Lambda(8) = 0$$

$$\Lambda(4) \neq 0$$

$$\Lambda(2) \neq 0$$

Fouten :

$$X_1 = \alpha^c = 3$$

Gr plants 3

$$X_2 = \alpha^{\frac{7}{2}} = 8$$

Gr plants 8

"
Footwear side

"
Plants

3.) BCH - code

over $GF(5)$

$$q = 5$$

$$t = 3$$

(kan 3 fouten verbeteren)

$$l = 0$$

⚠ LET OP: Dit is een gegeven ontwerpparameters die bepaalt vanaf welke macht van β de generatorpolynomial $g(x)$ die de code genereert zal geconstrueerd worden.

$$n = 12$$

→

Dit is NIET de l uit pagina 30 van de cursus ($n - l$) die zegt dat $\beta = \alpha^l$

• Typical uitbreidingsveld:

$$GF(5)$$

$$q = 5$$

$$n = 12$$

$$q^k \pmod{n} = 1$$

$$5^k \pmod{12} = 1$$

Zoek k zo klein mogelijk

$$\boxed{k=2}$$

$$\rightarrow 5^2 = 25 \pmod{12} = 1$$

⚠ Zie p 30

• (zie ook opg. hierboven over l)

$$\text{en } 25 - 1 = l \cdot n$$

↳ Dit is de andere l van

↑ 30

$$= 2 \cdot 12$$

" l "

$$\underline{\underline{l=2}} \Rightarrow \underline{\underline{\beta = \alpha^l = \alpha^2}}$$

Machten van β tot α

$$\beta^0 = 1$$

$$\beta^1 = \alpha^2$$

$$\beta^2 = \alpha^4$$

$$\beta^3 = \alpha^6$$

$$\beta^4 = \alpha^8$$

$$\beta^5 = \alpha^{10}$$

$$\beta^6 = \alpha^{12}$$

$$\beta^7 = \alpha^{14}$$

$$\beta^8 = \alpha^{16}$$

$$\beta^9 = \alpha^{18}$$

$$\beta^{10} = \alpha^{20}$$

$$\beta^{11} = \alpha^{22}$$

$$(\beta^{12} = \alpha^{24} = \alpha^0 = 1)$$



machten van β : van 0 tot $n-1$ ($=11$)

over $GF(25)$

$\rightarrow$ machten α moet 24

Vermits we geen primitieve wortelterm gekregen hebben kunnen we α niet bepalen als nulpunt daarvan en kunnen we voor de machten van α geen worteltermen in $GF(5)$ definiëren.

Hierdoor kunnen we ook de cyclotomische minimaalpolyn. n/d cyclotomische reekkenlassen niet nauwkeurig uitwerken.

~~$$x=0, t=3$$

$$g(x) = (x - \beta^0)(x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4)(x - \beta^5)(x - \beta^6)(x - \beta^7)(x - \beta^8)(x - \beta^9)(x - \beta^{10})(x - \beta^{11})$$~~

α is das von ~~effektiv~~ primitiv element
von $GF(25)$

$$\beta = \alpha^2 \quad (l=2)$$

Galois'sche Nebenklassen modulo n over $GF(q)$
von β

modulo 12 over $GF(5)$

$$C_i = \{i, q^2 i, q^4 i, \dots\}$$

$$C_0 = \{0\}$$

$$C_1 = \{1, 5\}$$

$$C_2 = \{2, 10\}$$

$$C_3 = \{3\}$$

$$C_4 = \{4\}$$

$$C_6 = \{6\}$$

$$C_7 = \{7, 11\}$$

$$C_8 = \{8\}$$

$$C_9 = \{9\}$$

$$m^{(0)}(x) = (x - \beta^0) = x - 1 \equiv x + 4 \pmod{5}$$

$$m^{(1)}(x) = m^{(5)}(x) = (x - \beta^1)(x - \beta^5) \\ = (x - \alpha^2)(x - \alpha^{10})$$

$$(x - \beta^2)(x - \beta^{10}) = (x - \alpha^4)(x - \alpha^{20})$$

$$(x - \beta^3) = (x - \alpha^6)$$

$$(x - \beta^4) = (x - \alpha^8)$$

$$(x - \beta^6) = (x - \alpha^{12})$$

$$(x - \beta^7)(x - \beta^{11}) = (x - \alpha^{14})(x - \alpha^{22})$$

$$(x - \beta^8) = (x - \alpha^{16})$$

$$(x - \beta^9) = (x - \alpha^{18})$$



Minimalpoltermen

• Bijnaal generatorpolynoom $g(x)$

moeten $n/8$

$\rightarrow \underline{l=0}$

we hebben er 2 t. $\frac{1}{6}$ gevolgende nodig

0, 1, 2, 3, 4, 5, 6

$$\text{dit zijn } g(x) = m^{(0)}(x) \cdot m^{(1)}(x) \cdot m^{(2)}(x) \cdot m^{(3)}(x) \cdot m^{(4)}(x) \cdot m^{(5)}(x)$$

Zie
↑ 58-59

$$g(x) = (x+4) \cdot (x-\alpha^2) \cdot (x-\alpha^{10}) \cdot (x-\alpha^4) \cdot (x-\alpha^{20})$$

$$(x-\alpha^6) \cdot (x-\alpha^8) \cdot (x-\alpha^{12})$$

$$= x^8 + \dots$$

$\rightarrow g(x)$ heeft graad 8

b.) De grootste n/d informatie in deze code
is $n-8 = \underline{4}$

(12, 4) - code

(4 is de lengte n/d het
informatiewoord)

$\rightarrow \underline{l=8}$

8, 9, 10, 11, 0, 1

$$g(x) = m^{(8)}(x) \cdot m^{(9)}(x) \cdot m^{(10)}(x) \cdot m^{(11)}(x) \cdot m^{(0)}(x) \cdot m^{(1)}(x)$$

$$= (x-\alpha^{16}) \cdot (x-\alpha^{18}) \cdot (x-\alpha^{14}) \cdot (x-\alpha^{22}) \cdot (x+4)$$

$$\cdot (x-\alpha^2) \cdot (x-\alpha^{20})$$

$$= x^7 + \dots$$

$\rightarrow g(x)$ heeft graad 7

nu hebben we een (12, 5) - code, dit is
beter (efficiënter)

(12-7)

volgens me is
 $\ell=0$

Met andere woorden $\ell=0$ is niet de beste keuze.

C.) α is het primitief element van $GF(25)$
en nulpunt van $3+3x+x^2$ over $GF(5)$

"primitieve veelterm"
 $= m^{(4)}(x)$ voor cyclot. reeklassen
van α

$$3+3\alpha+\alpha^2=0 \quad (\text{want } \alpha \text{ is nulpunt})$$

$$\alpha^2 = -3 - 3\alpha \quad (\text{mod } 5)$$

$$\alpha^2 = 2 + 2\alpha$$

• Inversen tabel

$$\alpha^2 = [2 \ 2]$$

$$\begin{aligned} \alpha^{10} &= \alpha^7 \cdot \alpha^3 \\ &= (3\alpha)(4+\alpha) \\ &= 12\alpha + 3\alpha^2 \\ &= 12\alpha + 3(2+2\alpha) \\ &= 12\alpha + 6 + 6\alpha \\ &= 18\alpha + 6 \\ &\quad (\text{mod } 5) \\ &= 3\alpha + 1 \\ &= [1 \ 3] \end{aligned}$$

$$\begin{aligned} \alpha^{22} &= \alpha^{12} \alpha^{10} \\ &= (1+3\alpha)4 \\ &= 4 + 12\alpha \quad (\text{mod } 5) \\ &= 4 + 2\alpha \\ &= [4 \ 2] \end{aligned}$$

$$\begin{aligned} \alpha^{11} &= \alpha^{10} \cdot \alpha^1 \\ &= (1+3\alpha)\alpha \\ &= \alpha + 3\alpha^2 \\ &= \alpha + 3(2+2\alpha) \\ &= 7\alpha + 6 \\ &\quad (\text{mod } 5) \\ &= 2\alpha + 1 \\ &= [1 \ 2] \end{aligned}$$

$$\begin{aligned} \alpha^{23} &= \alpha^{11} \alpha^{12} \\ &= (1+2\alpha) \cdot 4 \\ &= 4 + 8\alpha = 4 + 3\alpha \\ &= [4 \ 3] \end{aligned}$$

→ 24 machten α in de tabel $(= 9^2 - 1)$

!
Bij achteraan
tabel aanvullen

d.) Syndromen:

gegeven:

$$v = 2 \ 4 \ 3 \ 2 \ 4 \ 1 \ 1 \ 3 \ 0 \ 0 \ 0 \ 0$$

$$S_3 = \alpha^{12}$$

$$S_6 = \alpha^{23}$$

$$S_5 = \alpha^{27}$$

Formules:

$$S_1 = v(\beta^{l+1-1}) = v(\beta^l) \quad (l=0)$$

$$= v(\beta^0)$$

Gemiddeld
uit te
rekken

$$= v(1)$$

$$= 2 + 4 + 3 + 2 + 4 + 1 + 1 + 3$$

$$= 20 \quad (\text{mod } 5)$$

$$S_1 = 0$$

$$S_2 = v(\beta^{l+1})$$

$$= v(\beta^1)$$

$$C_1 = \{1, 5\}$$

$$(S_2)^4 = v(\beta^4)$$

$$S_2^5 = v(\beta^5)$$

in de orde van

→ 5 zit in zelfde cyclot.
nevenklasse

Geek is $(\beta^5)^5$
was gelijk
aan β^1

$$v(\beta^5) = S_6$$

$$\rightarrow \text{want } 5 = l + i - 1$$

$$i = 5 - 0 + 1$$

$$i = 0$$

(interpolatie n/ syndromen)

Stelling 22 p 20 rept

dat:

$$S_2 = (S_6)^5 = (\alpha^{23})^5 = \alpha^{5 \cdot 23} = \alpha^{115}$$

(mod 24)

$$S_2 = \alpha^{19}$$

$$S_4 = v(\beta^{l+3}) = v(\beta^3)$$

~~hier~~

$$C_3 = \{3\}$$

$$v(\beta^3) = v(\alpha^6)$$

Hier moeten we het
syndroom dus uitrekken, want
3 zit alleen in een nevenklasse.

$$v(x) = 2 + 4x + 3x^2 + 2x^3 + 4x^4 + x^5 + x^6 + 3x^7$$

machten
mod 24

$$v(\alpha^6) = 2 + 4\alpha^6 + 3\alpha^{12} + 2\alpha^{18} + 4\alpha^0 + \alpha^6 + \alpha^{12} + 3\alpha^{18}$$

$$= 2 + 4 \cdot 3 + 3 \cdot 4 + 2 \cdot 2 + 4 + 3 + 4 + 3 \cdot 2$$

$$= 47 \quad (\text{mod } 5)$$

$$= 2$$

$$= \alpha^{18}$$

achtewaards in tabel
gelezen

Er komen geen
machten van α
voor. Dat is dus
ook makkelijk
te berekenen!

$$S_4 = \alpha^{18}$$

Gpm: Het kan nog sneller!

$$\alpha^6 = 3 \quad (\text{volgens tabel})$$

$$v(\alpha^6) = v(3)$$

→ Dus je kan gewoon 3 invullen!

$$S_4 = v(3) = 2 = \alpha^{18}$$

2.) BM algoritme (p. 75)

Step 1 Syndromen berekenen (reeds gedaan)

$$t=3$$

s	Δ	n	d	$\Lambda(x)$	$\Lambda^*(x)$
0	1	0	0	1	0
1	0	1	0	1	0
2	α^{19}	0	2	x^2	α^5
3	α^{12}	1	2	$\alpha^5 x + x^2$	α^5
4	α^1	2	2	$x^2 + \alpha^5 x + \alpha^{12}$	α^5
5	0	3	2	$\alpha^{18} + \alpha^5 x + x^2$	α^5
6	0	4	2	$\alpha^{18} + \alpha^5 x + x^2$	α^5
7					

Step 2 $\Lambda = 1$ (Init)

$$d=0$$

$$n=0$$

$$\Lambda^*=0$$

Step 3 $0 < 6$

① $\Delta = 1S_0 + 0S_1 = S_1 = 0$

$\Delta = 0 \Rightarrow n++$ ($n=1$)

② $1 < 6$

$\Delta = 1S_2 = \alpha^{19}$

$\Delta \neq 0$ en $n < d$

$\Rightarrow$ ~~update~~

$$\begin{bmatrix} \Lambda \\ \Lambda^* \end{bmatrix} \leftarrow \begin{bmatrix} x^2 \cdot 1 - \alpha^{19} \cdot 0 \\ 1/\alpha^{19} \cdot 1 \end{bmatrix}$$

$\Lambda = x^2$

$\Lambda^* = \alpha^{-19} \pmod{24}$
 $= \alpha^5$

$$\begin{bmatrix} n \\ d \end{bmatrix} \leftarrow \begin{bmatrix} d \\ n+1 \end{bmatrix}$$

$n=0$
 $d=2$

③ $2 < 6$

$\Delta = 0 \cdot S_1 + 0S_2 + 1S_3 = S_3 = \alpha^{12}$

$\Delta \neq 0$ en $n < d$

$\Rightarrow$ ~~update~~

$\Lambda \leftarrow x^2 - \alpha^{12} \cdot x \cdot \alpha^5$

$\Lambda = x^2 - \alpha^{17} x = x^2 - (3+\alpha)x$ (graaf in tabel)

$n++$ ($n=1$)

$= x^2 + (-3-\alpha)x \pmod{5}$

$= x^2 + (2+4\alpha)x$

$= x^2 + \alpha^5 x$ (omgekeerd graaf in tabel)

④ $3 < 6$

$\Delta = 0 \cdot S_2 + \alpha^5 S_3 + S_4 = \alpha^5 (\alpha^{12}) + \alpha^{18}$

$= \alpha^{17} + \alpha^{18}$

$= (3+\alpha) + (2) \pmod{5}$

$= \alpha \pmod{5}$

$\Delta \neq 0$ en $n < d \Rightarrow \Lambda = \alpha^5 x + x^2 - \alpha \cdot x^0 \cdot \alpha^5$

$= x^2 + \alpha^5 x - \alpha^6$

$= x^2 + \alpha^5 x + 2 = x^2 + \alpha^5 x + \alpha^{18}$

$n++$ ($n=2$)

$$\lambda = 5$$

$$4 < 6$$

$$\begin{aligned}\Delta &= \alpha^{18} S_3 + \alpha^5 S_4 + 1 \cdot S_5 \\ &= \alpha^{18} \cdot \alpha^{12} + \alpha^5 \cdot \alpha^{18} + \alpha^{21} \\ &= \alpha^{30} + \alpha^{23} + \alpha^{21} \quad (\text{mod } 24) \\ &= \alpha^6 + \alpha^{23} + \alpha^{21} \\ &= 3 + (4 + 3\alpha) + (3 + 2\alpha) \\ &= 10 + 5\alpha \quad (\text{mod } 5) \\ &= 0\end{aligned}$$

$$\Delta = 0$$

$$\Rightarrow n++ \quad (n=3)$$

$$\lambda = 6$$

$$5 < 6$$

$$\begin{aligned}\Delta &= \alpha^{18} S_4 + \alpha^5 S_5 + 1 S_6 \\ &= \alpha^{18} \alpha^{18} + \alpha^5 \alpha^{21} + \alpha^{23} \\ &= \alpha^{12} + \alpha^2 + \alpha^{23} \quad (\text{mod } 24) \\ &= 4 + (2 + 2\alpha) + (4 + 3\alpha) \\ &= 10 + 5\alpha \quad (\text{mod } 5) \\ &= 0\end{aligned}$$

$$\Delta = 0$$

$$\Rightarrow n++ \quad (n=4)$$

$$\lambda = 7$$

$$6 \not< 6$$

Stopconditie !

f.) mogelijke $\phi^{(d)}(x)$ voor $d=0, 1, 2, 3$

In het algoritme ~~we~~ proberen we steeds n te verhoggen en de coëff van $\Lambda(x)$ aan te passen om $\mu_d(\Lambda(x))$ maximaal

||
 μ_d te maken

Wanneer we μ_d bereikt hebben ~~we~~ verhoggen we d . Op dat moment is $\Lambda(x)$ een mogelijke $\phi^{(d)}(x)$ (dus net voor het verhoggen van d)

- $d=0 \rightarrow \phi^{(0)}(x) = 1 \quad \mu_0 = 1$
- $d=1 \rightarrow \phi^{(1)}(x) = x \quad \mu_1 = \mu_0$
 Voor $d=1$ kan geen optimale oplossing gevonden worden, we gaan maken naar $d=2$
 (Zie p. 73, eerste bolletje)
 Omdat n niet noodzakelijk stijgt als d stijgt
- $d=2 \rightarrow \phi^{(2)}(x) = x^{10} + x^5 x + x^2$
 $\mu_2 = 4$
 (dit is n op het eind van het algoritme)
- Het algoritme heeft geen $\phi^{(3)}$ berekend ($d=3$)

Merkt ook op dat μ_d gelijk is aan n uit de tabel, net voor graad d verhoogd wordt.

h.) De introes van het BM algoritme was foutlocatorverterm:

$$\Lambda(x) = x^2 + \alpha^5 x + \alpha^{18}$$

nulpunten:

$$x^2 + \alpha^5 x + \alpha^{18} = 0$$

$$X_1 = \alpha^{22} \quad (\text{gegeven})$$

dan:

$$\Lambda(x) = (x - \alpha^{22})(x - X_2)$$

$$= x^2 - X_2 x - \alpha^{22} x + X_2 \alpha^{22}$$

$$= x^2 + (-X_2 - \alpha^{22}) x + (X_2 \alpha^{22})$$

omdat $\Lambda(x) = x^2 + \alpha^5 x + \alpha^{18}$

met

$$\begin{cases} -X_2 - \alpha^{22} = \alpha^5 \\ X_2 \alpha^{22} = \alpha^{18} \end{cases} \quad \text{waar zijn}$$

$$X_2 = \frac{\alpha^{18}}{\alpha^{22}} = \alpha^{18-22}$$

$$= \alpha^{-4} \quad (\text{mod } 24)$$

$$= \alpha^{20}$$

Dit dient enkel
nog te
verificatie

$$-\alpha^{20} - \alpha^{22} = \alpha^5$$

$$-4 - 4\alpha - 4 - 2\alpha = \alpha^5 \quad (\text{mod } 5)$$

$$1 + \alpha + 1 + 3\alpha = \alpha^5$$

$$2 + 4\alpha = \alpha^5$$

$$[2 \ 4] = \alpha^5$$

ok/

fout op:

$$\begin{array}{ll} \text{Dus: } X_1 = \alpha^{22} & \rightarrow \text{Plaats 23} \\ X_2 = \alpha^{20} & \rightarrow \text{Plaats 21} \end{array}$$

(α^0 is plaats 1)

i.) Forney gebruiken om foutwoorden te bepalen

geg.: deel w/d veelterm

$$\Omega(x) = \dots + \alpha^6 x + \dots$$

Forney

a.) Stel $S(x)$ op

$$S(x) = \sum_{k=0}^{2t-1} S_{2t-k} x^k$$

$$t=3$$

$$\begin{aligned} S(x) &= S_6 x^0 + S_5 x^1 + S_4 x^2 + S_3 x^3 \\ &\quad + S_2 x^4 + S_1 x^5 \\ &= \alpha^{23} + \alpha^{21} x + \alpha^{18} x^2 + \alpha^{12} x^3 \\ &\quad + \alpha^{19} x^4 + 0 x^5 \end{aligned}$$

b.) Stel $\Omega(x)$ op

$$\Omega(x) = R_{x^{20}}(S(x), 1(x))$$

$$= R_{x^6} \left(\left(\alpha^{23} + \alpha^{21} x + \alpha^{18} x^2 + \alpha^{12} x^3 + \alpha^{19} x^4 \right) \cdot \left(\alpha^{18} + \alpha^5 x + x^2 \right) \right)$$

$$= R_{x^6} \left(\right)$$

~~$$R_{25} = \alpha^{23} + \alpha^{18} + \alpha^{13} + \alpha^8 + \alpha^3 + \alpha^{-2}$$~~

Alle stukken
met x^2
in zijn weglaten
omdat we de
coëff. van x
als nieten

$$= R_{25} \left(\alpha^{23+18} + \alpha^{23+5} x + \alpha^{23} x^2 + \alpha^{21+18} x^3 + \alpha^{16+18} x^4 + \alpha^{12+18} x^5 + \alpha^{12+5} x^6 + \alpha^{12} x^7 + \alpha^{19+18} x^8 + \alpha^{19+5} x^9 + \alpha^{19} x^{10} \right)$$

$$= R_{25} \left(\alpha^{17} + \alpha^6 x + (\alpha^{12} + \alpha^{23}) x^2 + (\alpha^{23} + \alpha^6) x^3 + (\alpha^{18} + \alpha^{17} + \alpha^{13}) x^4 + (\alpha^{12} + \alpha^0) x^5 + \alpha^{19} x^6 \right)$$

verpomp
dat laat alle
stukken met
 $x^{n \geq 6}$ weg

$$\begin{aligned} &= \alpha^{17} + \alpha^6 x + (4 + 4 + 3\alpha) x^2 \\ &+ (4 + 3\alpha + 3) x^3 + (2 + 3 + \alpha + 4\alpha) x^4 \\ &+ (4 + 1) x^5 \end{aligned}$$

(mod 5)

$$= \alpha^{17} + \alpha^6 x + (3 + 3\alpha) x^2 + (2 + 3\alpha) x^3 + 0 x^4 + 0 x^5$$

$$\Omega(x) = \alpha^{17} + \alpha^6 x + \alpha^{14} x^2 + \alpha^9 x^3$$

c.) Bepaal afgeleide van $\Lambda(x)$

$$\Lambda(x) = 2x + x^5$$

d.) Bepaal fontwaarden

$$Y_k = - \frac{\Omega(X_k)}{X_k^{2L+1} \Lambda'(X_k)} \quad k=1, \dots, v$$

$$2L=6$$

$$v=2$$

$$L=0$$

$$Y_1 = - \frac{\Omega(x^{22})}{(x^{22})^6 \Lambda'(x^{22})}$$

$$= - \frac{\alpha^9 \alpha^{22 \cdot 3} + \alpha^{19} \alpha^{22 \cdot 2} + \alpha^6 \alpha^{22} + \alpha^{17}}{\alpha^{22 \cdot 6} (2 \alpha^{22} + \alpha^{22 \cdot 5})}$$

$$= - \frac{\alpha^3 + \alpha^{10} + \alpha^4 + \alpha^{17}}{\alpha^{12} (2 \alpha^{22} + \alpha^{14})}$$

$$= - \frac{4 + \alpha + 1 + 3\alpha + 2 + \alpha + 3 + \alpha}{4 (2(4 + 2\alpha) + 3 + 3\alpha)}$$

$$= - \frac{\alpha}{2 + \alpha + 2 + 2\alpha}$$

$$= - \frac{\alpha}{4 + 3\alpha}$$

$$= - \frac{\alpha^1}{\alpha^{23}} = - \alpha^{1-23} = - \alpha^{22}$$

$$= -2 - 2\alpha$$

$$= 3 + 3\alpha$$

$$= \alpha^{14}$$

$$\begin{aligned}
Y_2 &= - \frac{\Omega(\alpha^{20})}{\alpha^{20.6} \Pi'(\alpha^{20})} \\
&= - \frac{\alpha^9 \alpha^{20.3} + \alpha^{14} \alpha^{20.2} + \alpha^6 \alpha^{20.17}}{\alpha^{20.6} \cdot (2\alpha^{20} + \alpha^{20.5})} \\
&= - \frac{\alpha^{29} + \alpha^6 + \alpha^2 + \alpha^{17}}{1(2\alpha^{20} + \alpha^4)} \\
&= - \frac{3+2\alpha + 3+2+2\alpha + 3+\alpha}{2(4+4\alpha) + 2+\alpha} \\
&= - \frac{14}{8+8\alpha+2+\alpha} \\
&= - \frac{1}{4\alpha} \\
&= - \frac{1}{\alpha^{13}} \\
&= - \alpha^{-13} \\
&= - \alpha^{11} \\
&= -(1+2\alpha) \\
&= -1-2\alpha \quad (\text{mod } 5) \\
&= 4+3\alpha \\
&= \alpha^{23} \\
&= \underline{\underline{\alpha^{23}}}
\end{aligned}$$

$$\begin{array}{l}
Y_1 = \alpha^{14} \\
Y_2 = \alpha^{23}
\end{array}$$

Volgens de opgave moet je er wel maar één berekenen.

4.) Convolutionele codes

a.) We zoeken alle generatorvallen
van graad 2 die niet deelbaar
door elkaar zijn (niet-catastrofale codes)

Codes uit de
les en
opdracht

$$\begin{cases} g^{(1)} = X^2 + X + 1 & (7,5) \text{ code} \\ g^{(2)} = X^2 + 1 \end{cases} \quad \begin{cases} g^{(1)} = X^2 + X + 1 & (7,3) \text{ code} \\ g^{(2)} = X + 1 \end{cases}$$

→ Elk register kan 2 waarden (0 of 1) innemen, wat in
elke $X=2$ in onze rijtje de code beschrijving

$$k_0 = 1$$

aantal bits in input frame

$$m_0 = 2$$

aantal output bits

$$v = 2 \quad (= m_0 \text{ bit per cel}) \quad \text{Het aantal shift registers}$$

(ook wel het totaal aantal,
sinds er maar 1 input
bit is)

⇒ 2 generatorvallen

$$(k_0, n_0)$$

maximaal graad 2

$$(v)$$

mogen niet onderling deelbaar zijn

!!!

Alle mogelijkheden:

$$\begin{cases} X^2 + X & 1 \\ X^2 & 1 \end{cases}$$

$$\begin{cases} X^2 + X + 1 \\ X + 1 \end{cases}$$

$$\begin{cases} X^2 + X + 1 \\ X^2 + X \end{cases}$$

$$\begin{cases} X + 1 \\ X \end{cases}$$

$$\begin{cases} X^2 + 1 \\ X + 1 \end{cases}$$

~~$$\begin{cases} X^2 + X \\ X + 1 \end{cases}$$~~ want $(X+1)X = X^2 + X$

$$\begin{cases} X + 1 \\ X^2 \end{cases}$$

$$\begin{cases} X^2 + X + 1 \\ X^2 \end{cases}$$

$$\begin{cases} X^2 + X & 1 \\ X & \end{cases}$$

~~$$\begin{cases} X^2 + X \\ 1 \end{cases}$$~~ want $1 \cdot (X^2 + X) = X^2 + X$

~~$$\begin{cases} X^2 + X \\ X \end{cases}$$~~

want $X(1+X) = X^2 + X$

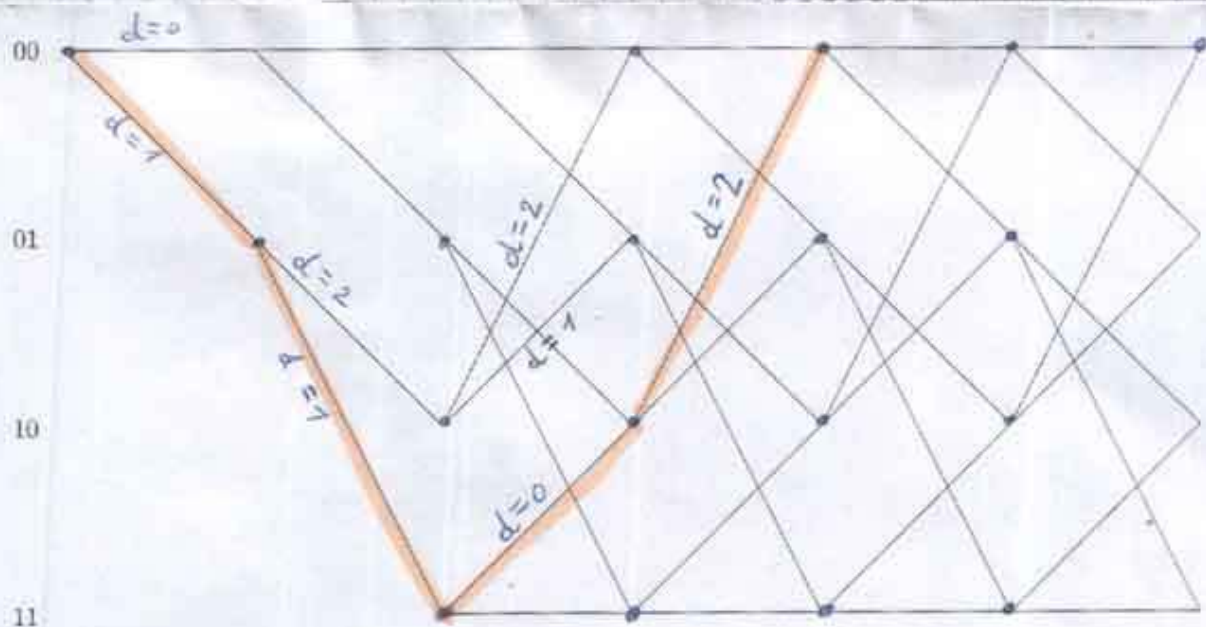
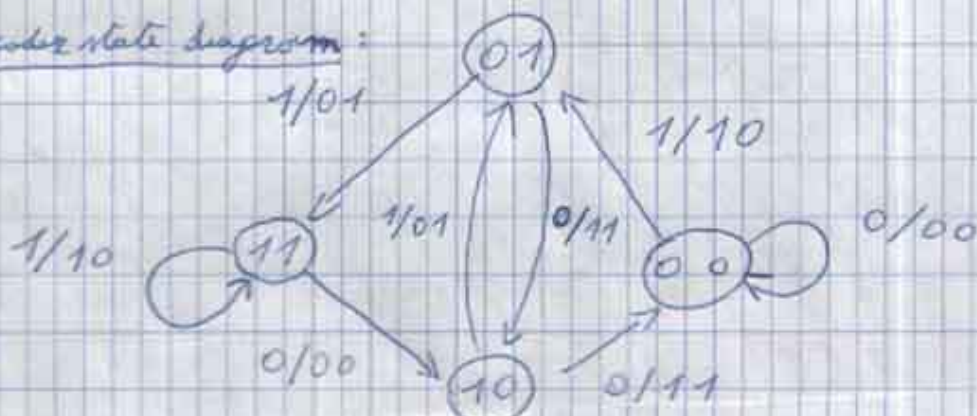
$\Rightarrow$ bijgewerkte
alle combinaties
met een
vulterm $g(X) = 1$

b.) Ik koos voor de (7,6)-code

$$g^{(1)}(x) = x^2 + x + 1$$

$$g^{(2)}(x) = x^2 + x$$

Encoder state diagram:



$$d_{\infty} = 1 + 1 + 0 + 2 = 4$$

$$d_{\min} = 1 + 1 + 0 = 2$$

Dit is het pad met kleinste gewicht
(met triviaal pad) van ingang $m+1$
(met $m=2$)

de ingang
in de shift
registers

* d is het aantal
enen in de output
verschillend van 0

$$d(00) = 0$$

$$d(01) = 1$$

$$d(10) = 1$$

$$d(11) = 2$$