

Vorbereiding oefeningen les 10

Leen Van Houdt
Sander Mergan
Seppe Duwé
Willem Melis
Wouter Duyols
Xavier Dejager

April 27, 2016

1 Oefening 0.5

Met een tegenvoorbeeld kunnen we aantonen dat de bewering niet waar is. We stellen dat $x = 0$ en $z = 0$. Er geldt dat $xy = 0$ en $xz = 0$. Hieruit volgt dat $xy = xz$. We weten echter dat $y \neq z$. De bewering geldt dus enkel als $x = 1$.

We kunnen de bewering dus aanvullen met “gegeven dat $x = 1$ ”, en dit kan bewezen worden door x te vervangen door 1: $xy = xz \Rightarrow 1.y = 1.z \Rightarrow y = z$ maar dit is uiteraard triviaal.

Ook kunnen we de bewering omdraaien: “in de Booleaanse algebra volgt uit $y = z$ dat $xy = xz$ ”, en dit kan bewezen worden door y te vervangen door z in de 2^e vergelijking maar ook dit bewijs is triviaal.

2 Oefening 4.30

Deel 1 Met de exhaustieve methode (alle gevallen nagaan in de waarheidstabel) vinden we volgende oplossing:

N	x	y	z	t	v
0	0	0	0	0	1
1	0	0	0	1	0
2	0	0	1	0	0
3	0	0	1	1	1
4	0	1	0	0	0
5	0	1	0	1	1
6	0	1	1	0	1
7	0	1	1	1	0
8	1	0	0	0	0
9	1	0	0	1	1
10	1	0	1	0	1
11	1	0	1	1	0
12	1	1	0	0	1
13	1	1	0	1	0
14	1	1	1	0	0
15	1	1	1	1	1

De mintermnormaalkvorm wordt gevonden door te kijken naar de kolommen waar $f = 1$ is:

$$v = \bar{x}\bar{y}\bar{z}\bar{t} + \bar{x}\bar{y}zt + \bar{x}y\bar{z}t + \bar{x}yz\bar{t} + x\bar{y}\bar{z}t + x\bar{y}z\bar{t} + xyz\bar{t} + xyz\bar{t} \quad (1)$$

De maxtermnormaalkvorm wordt gevonden door te kijken naar de kolommen waar $f = 0$ is:

$$v = (x + y + z + \bar{t})(x + y + \bar{z} + t)(x + \bar{y} + z + t)(x + \bar{y} + \bar{z} + \bar{t})(\bar{x} + y + z + t)(\bar{x} + y + \bar{z} + \bar{t})(\bar{x} + \bar{y} + z + \bar{t})(\bar{x} + \bar{y} + \bar{z} + t) \quad (2)$$

De maxtermnormaalkvorm bijvoorbeeld kan gerealiseerd worden met volgend poorten-netwerk:

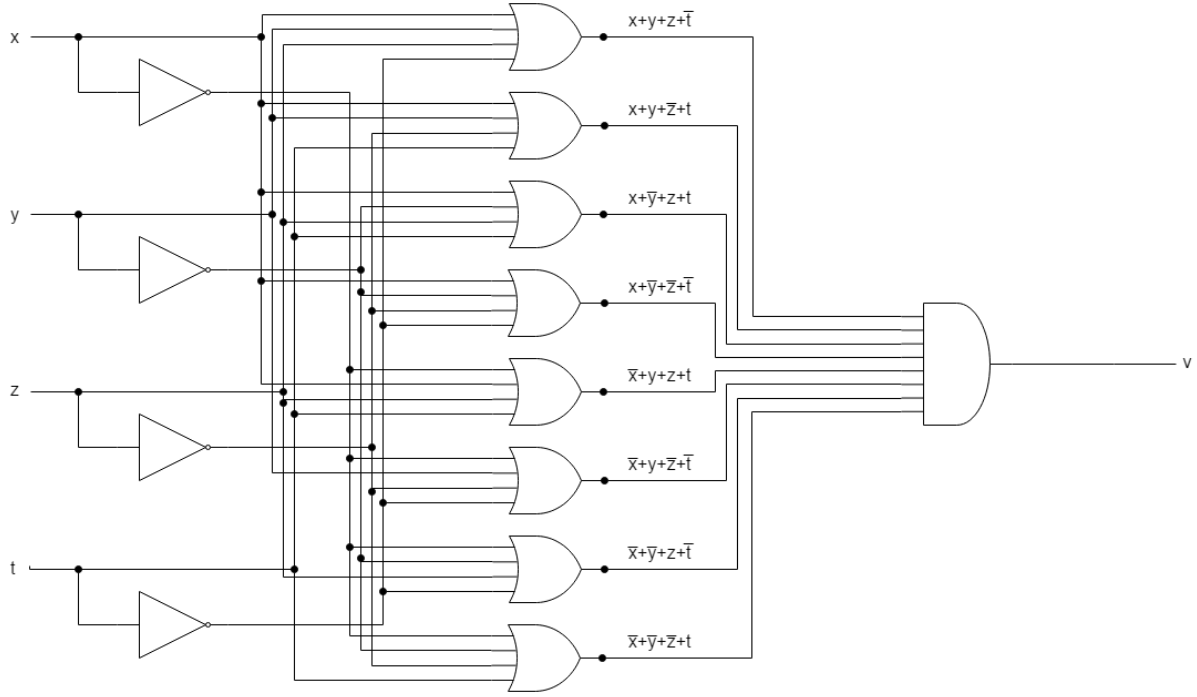


Figure 1: Poortnetwerk met maxtermen

Deel 2 Gevraagd is de vergelijking $v = 1$ op te lossen met de systematische methode. $v = 1$ als $\bar{v} = 0$.

\bar{v} kan makkelijk bekomen worden door de negatie van de maxtermnormaalvorm te nemen en deze vervolgens te vereenvoudigen met de wet van de Morgan:

$$\bar{v} = \neg((x + y + z + \bar{t})(x + y + \bar{z} + t)(x + \bar{y} + z + t)(x + \bar{y} + \bar{z} + \bar{t})(\bar{x} + y + z + t)(\bar{x} + y + \bar{z} + t)(\bar{x} + \bar{y} + z + t)(\bar{x} + \bar{y} + \bar{z} + t)) = 0 \quad (3)$$

$$\Leftrightarrow \bar{x}\bar{y}\bar{z}\bar{t} + \bar{x}\bar{y}z\bar{t} + \bar{x}y\bar{z}\bar{t} + \bar{x}yz\bar{t} + x\bar{y}\bar{z}\bar{t} + x\bar{y}z\bar{t} + xy\bar{z}\bar{t} + xyz\bar{t} = 0 \quad (4)$$

We beschouwen enkel x als veranderlijke en herschrijven de vergelijking:

$$x(\bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t}) + \bar{x}(\bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t}) = 0 \quad (5)$$

Met behulp van de wet van De Morgan kunnen we aantonen dat:

$$\neg(\bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t}) = (\bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t}) \quad (6)$$

Stel voor de leesbaarheid $q = (\bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t})$, dan volgt dat: $\bar{q} = \bar{y}\bar{z}\bar{t} + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yz\bar{t}$. De vergelijking wordt dan:

$$xq + \bar{x}\bar{q} = 0 \quad (7)$$

De oplossing voor x is:

$$x = \bar{q} + \bar{q}\lambda = \bar{q}(1 + \lambda) = \bar{q} = \bar{y}\bar{z}t + \bar{y}z\bar{t} + y\bar{z}\bar{t} + yzt = \bar{y}(\bar{z}t + z\bar{t}) + y(\bar{z}\bar{t} + zt) \quad (8)$$

De voorwaarde voor oplosbaarheid is:

$$q.\bar{q} = 0 \quad (9)$$

Dit geldt echter altijd dus deze voorwaarde is triviaal. y , z en t kunnen dus willekeurig gekozen worden. Stel $y = \lambda_1$, $z = \lambda_2$ en $t = \lambda_3$. We krijgen volgend stelsel:

$$\begin{cases} x &= \bar{\lambda}_1(\bar{\lambda}_2\lambda_3 + \lambda_2\bar{\lambda}_3) + \lambda_1(\bar{\lambda}_2\bar{\lambda}_3 + \lambda_2\lambda_3) \\ y &= \lambda_1 \\ z &= \lambda_2 \\ t &= \lambda_3 \end{cases} \quad (10)$$

Als we nu alle waarden doorlopen voor λ_1 , λ_2 en λ_3 krijgen we alle oplossingen voor $\bar{v} = 1$ en dus voor $v = 0$.

λ_1	λ_2	λ_3	x	y	z	t
0	0	0	0	0	0	0
0	0	1	1	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	1
1	0	0	1	1	0	0
1	0	1	0	1	0	1
1	1	0	0	1	1	0
1	1	1	1	1	1	1

Als we deze tabel vergelijken met de tabel van de exhaustieve methode (zie deel 1) dan zien we dat deze waarden voor x , y , z en t inderdaad overeenkomen met $v = 1$.

3 Oefening 4.41

Deeloefening 1 De inverse van $x^2 + 1 \pmod{x^3 + x^2 + 1}$ zoeken:

$$\begin{array}{r|l}
 \begin{array}{cccccc}
 x^3 & + & x^2 & + & 0x & + & 1 \\
 x^3 & + & 0x^2 & + & x & + & 1
 \end{array} & \begin{array}{c} x^2 + 1 \\ x + 1 \end{array} \\
 \hline
 \begin{array}{cccccc}
 & & x^2 & - & x & + & 1 \\
 & & x^2 & + & 0x & + & 1 \\
 \hline
 & & & & x & + & 0
 \end{array} &
 \end{array}$$

$$\begin{array}{r|l}
 \begin{array}{ccc}
 x^2 & + & 1 \\
 x^2 & &
 \end{array} & \begin{array}{c} x \\ x \end{array} \\
 \hline
 1 &
 \end{array}$$

$$x^3 + x^2 + 1 = (x + 1)(x^2 + 1) + x \quad (11)$$

$$x^2 + 1 = x \cdot x + 1 \quad (12)$$

$$1 = (x^2 + 1) - x \cdot x \quad (13)$$

$$= (x^2 + 1) - x(x^3 + x^2 + 1 - (x + 1)(x^2 + 1)) \quad (14)$$

$$= (1 + x + x^2)(x^2 + 1) - x(x^3 + x^2 + 1) \quad (15)$$

$$(16)$$

$$1 + x + x^2 = \text{gezochte inverse} \quad (17)$$

$$(x^2 + 1)y(x) = x^2 + x + 1 \pmod{x^3 + x^2 + 1} \quad (18)$$

$$\Leftrightarrow y(x) = (x^2 + 1)^{-1}(x^2 + x + 1) \pmod{x^3 + x^2 + 1} \quad (19)$$

$$= (x^2 + x + 1)(x^2 + x + 1) \pmod{x^3 + x^2 + 1} \quad (20)$$

$$= x^4 + x^2 + 1 \pmod{x^3 + x^2 + 1} \quad (21)$$

$$= x \pmod{x^3 + x^2 + 1} \quad (22)$$

$$\begin{array}{r|l}
 \begin{array}{cccccc}
 x^4 & + & 0x^3 & + & x^2 & + & 0x & + & 1 \\
 0x^4 & + & x^3 & + & 0x^2 & + & x & &
 \end{array} & \begin{array}{c} x^3 + x^2 + 1 \\ x - 1 \end{array} \\
 \hline
 \begin{array}{cccccc}
 0 & - & x^3 & + & x^2 & - & x & + & 1 \\
 & - & x^3 & - & x^2 & + & 0x & - & 1 \\
 \hline
 & & 0 & + & 0 & + & x & + & 0
 \end{array} &
 \end{array}$$

Deeloefening 2

$$\begin{cases} 2z + 4y = 1 & \textcircled{1} \\ 3z + 2y = 2 & \textcircled{2} \end{cases} \quad (23)$$

modulo 7:

$$\textcircled{1} + 2 \cdot \textcircled{2} \Rightarrow z = 5 \pmod{7} \quad (24)$$

$$\Rightarrow 3 + 4y = 1 \pmod{7} \quad (25)$$

$$\Leftrightarrow 4y = -2 = 5 \pmod{7} \quad (26)$$

$$\Leftrightarrow y = 5 \cdot 4^{-1} = 5 \cdot 2 = 3 \pmod{7} \quad (27)$$

modulo 6:

$$\textcircled{1} + 2 \cdot \textcircled{2} \Rightarrow z = 5 \pmod{6} \quad (28)$$

$$\Leftrightarrow z = 5 \cdot 2^{-1} \pmod{6} \quad (29)$$

De inverse van 2 bestaat echter niet in \mathbb{Z}_6 , dus het stelsel is niet eenduidig oplosbaar in \mathbb{Z}_6 .

Deeloefening 3

Deeloefening 4 Voor deze oefening werd gebruik gemaakt van de chinese reststelling. Er wordt naar een oplossing gezocht, indien deze bestaat natuurlijk.

We vereenvoudigen het systeem:

$$\begin{cases} 3V = 2 \pmod{5} \\ 2V = 2 \pmod{7} \\ 4V = 0 \pmod{11} \end{cases} \quad (30)$$

We zetten nu de opgave om in de vorm van vergelijking 31.

$$\begin{cases} V = a_1 \pmod{m_1} \\ V = a_2 \pmod{m_2} \\ V = a_3 \pmod{m_3} \end{cases} \quad (31)$$

$$\begin{cases} V = 4 \pmod{5} \\ V = 8 \pmod{7} \\ V = 0 \pmod{11} \end{cases} \quad (32)$$

$$\begin{cases} V = 4 \pmod{5} \\ V = 1 \pmod{7} \\ V = 0 \pmod{11} \end{cases} \quad (33)$$

We zien in vergelijking 33 dat m_1 tot en met m_3 relatief priem zijn met elkaar. (Het zijn zelfs priemgetallen, maar dit hoeft niet, relatief priem zijn is genoeg.)

$$M = 5.7.11 \quad (34)$$

$$M1 = \frac{M}{m_1} = \frac{5.7.11}{5} = 7.11 = 77 \quad (35)$$

$$M2 = \frac{M}{m_2} = \frac{5.7.11}{7} = 5.11 = 55 \quad (36)$$

$$M3 = \frac{M}{m_3} = \frac{5.7.11}{11} = 5.7 = 35 \quad (37)$$

$$N_1.M_1 = 1 \pmod{m_1} \quad (38)$$

$$N_1.77 = 1 \pmod{5} \quad (39)$$

$$\boxed{N_1 = 3}$$

$$N_2.M_2 = 1 \pmod{m_2} \quad (40)$$

$$N_2.55 = 1 \pmod{7} \quad (41)$$

$$\boxed{N_2 = 6}$$

$$N_3.M_3 = 1 \pmod{m_3} \quad (42)$$

$$N_3.35 = 1 \pmod{11} \quad (43)$$

$$\boxed{N_3 = 6}$$

$$x = \sum_{i=1}^r a_i.N_i.M_i = 4.3.77 + 1.6.55 + 0.6.11 = 1254 \quad (44)$$

We zien nu duidelijk dat er wel degelijk een oplossing is. Alle oplossingen die bestaan zijn:

$$x \pmod{m_1.m_2.m_3} \quad (45)$$

$$1254 \pmod{5.7.11} \quad (46)$$

$$1254 \pmod{5.7.11} \quad (47)$$

En we vereenvoudigen dit tot:

$$99 \pmod{385} \quad (48)$$

Deeloefening 5 $[y(x)]^2 = x^2 + 1 \pmod{(x^3 + x^2 + 1)}$ met $y(x)$ een veelterm in x over het veld $\{0,1\}$.

Modulo $g(x) = x^3 + x^2 + 1$. Indien kan ontbinden geen nuldelers zijn en kan vergelijking worden opgelost. constante term $\rightarrow g(0) \neq 0$ en oneven aantal termen $\rightarrow g(1) \neq 0$. De veelterm $g(x)$ is dus irreduceerbaar. De veelterm met coëfficiënten over het veld $\mathbb{Z}_2 = \{0,1\}$, $x + y = 0 \leftrightarrow x = y$. (Geen minteken nodig om naar het ander lid om te brengen.)

Stellen de logaritme-tabel voor de vermenigvuldiging op. X is een generator van de groep $F_8 \setminus \{0\}$.

$x^4 = x * x^3 = x^3 + x = x^2 + x + 1$, x^5 en x^6 analoog.

i		x^i			x^{i^2}	
0			1			1
1		x		x^2		
2	x^2			x^2	x	1
3	x^2		1	x^2	x	
4	x^2	x	1		x	
5		x	1	x^2		1
6	x^2	x			x	1

Uit de tabel $x^3 = x^2 + 1 = x^{10 \pmod 7} = x^{5^2}$. Dit is tevens de enige oplossing. x^{5+7k} met $k \in \mathbb{Z}$.