Voorbereiding oefeningen les 10

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

April 28, 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 mintermnormaalvorm wordt gevonden door te kijken naar de kolommen waar $f = 1$ is:

$$v = \bar{x}\bar{y}\bar{z}\bar{t} + \bar{x}\bar{y}zt + \bar{x}y\bar{z}t + \bar{x}yz\bar{t} + x\bar{y}\bar{z}t + x\bar{y}z\bar{t} + xy\bar{z}\bar{t} + xyzt \tag{1}$$

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

$$\begin{aligned} v = (x+y+z+\bar{t})(x+y+\bar{z}+t)(x+\bar{y}+z+t)(x+\bar{y}+\bar{z}+\bar{t})(\bar{x}+y+z+t) \\ (\bar{x}+y+\bar{z}+\bar{t})(\bar{x}+\bar{y}+z+\bar{t})(\bar{x}+\bar{y}+\bar{z}+t) \end{aligned} \tag{2}$$

De maxtermnormaalvorm bijvoorbeeld kan gerealiseerd worden met volgend poortennetwerk:

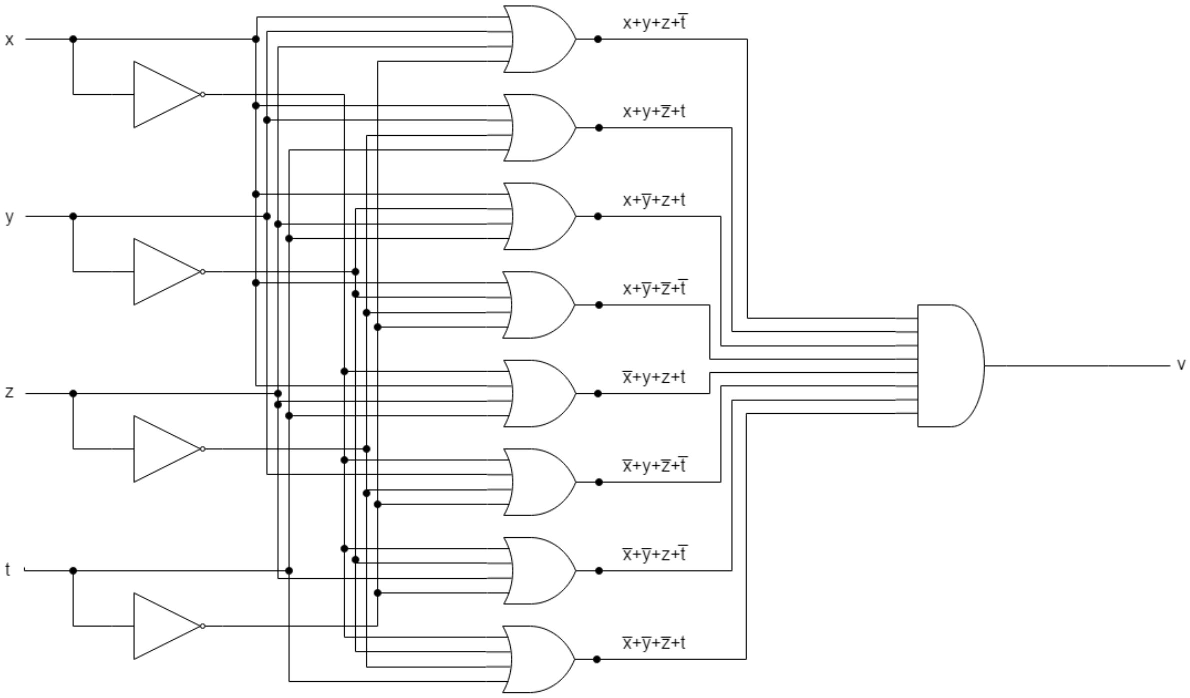

Figure 1: Poortnetwerk met maxtermen

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:

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

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

We beschouwen enkel x als veranderlijke en herschrijven de vergelijking:

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

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

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

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

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

De oplossing voor x is:

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

De voorwaarde voor oplosbaarheid is:

$$q.\bar{q} = 0 \tag{9}$$

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:

$$\begin{cases} x &= \bar{\lambda_1}(\bar{\lambda_2}\lambda_3 + \lambda_2\bar{\lambda_3}) + \lambda_1(\bar{\lambda_2}\bar{\lambda_3} + \lambda_2\lambda_3) \\ y &= \lambda_1 \\ z &= \lambda_2 \\ t &= \lambda_3 \end{cases} \tag{10}$$

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 $x^2 + 1 \mod x^3 + x^2 + 1$ zoeken:

$$
\begin{array}{ccccccc|ccc}
x^3 & + & x^2 & + & 0x & + & 1 & x^2 & + & 1 \\ \cline{8-10}
x^3 & + & 0x^2 & + & x & + & 1 & x & + & 1 \\ \cline{1-7}
 & & x^2 & - & x & + & 1 & & & \\
 & & x^2 & + & 0x & + & 1 & & & \\ \cline{3-7}
 & & & & x & + & 0 & & &
\end{array}
$$

$$
\begin{array}{ccc|c}
x^2 & + & 1 & \text{x} \\ \cline{4-4}
x^2 & & & \text{x} \\ \cline{1-3}
 & & 1 &
\end{array}
$$

$$x^3 + x^2 + 1 = (x+1)(x^2+1) + x \tag{11}$$
$$x^2 + 1 = x \cdot x + 1 \tag{12}$$

$$1 = (x^2+1) - x \cdot x \tag{13}$$
$$= (x^2+1) - x(x^3 + x^2 + 1 - (x+1)(x^2+1)) \tag{14}$$
$$= (1 + x + x^2)(x^2+1) - x(x^3 + x^2 + 1) \tag{15}$$
$$\tag{16}$$

$$1 + x + x^2 = \text{gezochte inverse} \tag{17}$$

$$(x^2+1)y(x) = x^2 + x + 1 \mod (x^3 + x^2 + 1) \tag{18}$$
$$\Leftrightarrow y(x) = (x^2+1)^{-1}(x^2 + x + 1) \mod (x^3 + x^2 + 1) \tag{19}$$
$$= (x^2 + x + 1)(x^2 + x + 1) \mod (x^3 + x^2 + 1) \tag{20}$$
$$= x^4 + x^2 + 1 \mod (x^3 + x^2 + 1) \tag{21}$$
$$= x \mod (x^3 + x^2 + 1) \tag{22}$$

$$
\begin{array}{ccccccccc|ccccc}
x^4 & + & 0x^3 & + & x^2 & + & 0x & + & 1 & x^3 & + & x^2 & + & 1 \\ \cline{10-14}
0x^4 & + & x^3 & + & 0x^2 & + & x & & & x & - & 1 & & \\ \cline{1-9}
0 & - & x^3 & + & x^2 & - & x & + & 1 & & & & & \\
 & - & x^3 & - & x^2 & + & 0x & - & 1 & & & & & \\ \cline{2-9}
 & & 0 & + & 0 & + & x & + & 0 & & & & &
\end{array}
$$

Deeloefening 2

$$\begin{cases} 2z + 4y = 1 & \text{①} \\ 3z + 2y = 2 & \text{②} \end{cases} \tag{23}$$

$\boxed{\text{modulo 7:}}$

$$\begin{aligned}
2 \cdot \text{①} + 1 \cdot \text{②} \Rightarrow 3y &= 4 \mod 7 && (24)\\
y &= 3^{-1}4 \mod 7 && (25)\\
y &= 5 \cdot 4 \mod 7 && (26)\\
y &= 6 \mod 7 && (27)\\
& && (28)
\end{aligned}$$

$$\begin{aligned}
2z + 4y &= 1 \mod 7 && (29)\\
2z + 3 &= 1 \mod 7 && (30)\\
2z &= -2 = 5 \mod 7 && (31)\\
z &= 2^{-1} \cdot 5 \mod 7 && (32)\\
z &= 6 \mod 7 && (33)
\end{aligned}$$

$\boxed{\text{modulo 6:}}$

$$\begin{aligned}
1 \cdot \text{①} + 1 \cdot \text{②} \Rightarrow 5z &= 3 \mod 6 && (34)\\
z &= 5^{-1} \cdot 3 \mod 6 && (35)\\
z &= 5 \cdot 3 \mod 6 && (36)\\
z &= 3 \mod 6 && (37)\\
& && (38)
\end{aligned}$$

$$\begin{aligned}
2z + 4y &= 1 \mod 6 && (39)\\
4y &= 1 \mod 6 && (40)\\
y &= 4^{-1} \cdot 1 \mod 6 && (41)
\end{aligned}$$

De inverse van 4 bestaat echter niet in $\mathbb{Z}_6$, dus het stelsel is niet eenduidig oplosbaar in $\mathbb{Z}_6$.

Deeloefening 3

$$\begin{cases} zy + \bar{y} = y + \bar{z} \\ \bar{z} + zy = 1 \end{cases} \tag{42}$$

$$\boxed{f = g \Rightarrow f\bar{g} + \bar{g}f = 0}$$

$$\begin{cases} (zy + \bar{y})\overline{(y + \bar{z})} + \overline{(zy + \bar{y})}(y + \bar{z}) = 0 \\ \overline{(\bar{z} + zy)} = 0 \end{cases} \tag{43}$$

$$\begin{cases} (zy + \bar{y})(\bar{y} + z) + ((\bar{z} + \bar{y})y)(y + \bar{z}) = 0 \\ z(\bar{z} + \bar{y}) = 0 \end{cases} \tag{44}$$

$$\begin{cases} \bar{y}z + \bar{z}y + \bar{z}y = 0 \\ z\bar{y} = 0 \end{cases} \tag{45}$$

$$\begin{cases} y\bar{z} = 0 \\ z\bar{y} = 0 \end{cases} \tag{46}$$

$$\begin{cases} y\bar{z} + \bar{y}z = 0 \qquad \text{(xor)} \\ y = z \end{cases} \tag{47}$$

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:

$$\begin{cases} 3V = 2 \mod 5 \\ 2V = 2 \mod 7 \\ 4V = 0 \mod 11 \end{cases} \tag{48}$$

We zetten nu de opgave om in de vorm van vergelijking 49.

$$\begin{cases} V = a_1 \mod m_1 \\ V = a_2 \mod m_2 \\ V = a_3 \mod m_3 \end{cases} \tag{49}$$

$$\begin{cases} V = 4 \mod 5 \\ V = 8 \mod 7 \\ V = 0 \mod 11 \end{cases} \tag{50}$$

$$\begin{cases} V = 4 \mod 5 \\ V = 1 \mod 7 \\ V = 0 \mod 11 \end{cases} \tag{51}$$

We zien in vergelijking 51 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.)

$$M = 5 \cdot 7 \cdot 11 \tag{52}$$

$$M1 = \frac{M}{m_1} = \frac{5 \cdot 7 \cdot 11}{5} = 7 \cdot 11 = 77 \tag{53}$$

$$M2 = \frac{M}{m_2} = \frac{5 \cdot 7 \cdot 11}{7} = 5 \cdot 11 = 55 \tag{54}$$

$$M3 = \frac{M}{m_3} = \frac{5 \cdot 7 \cdot 11}{11} = 5 \cdot 7 = 35 \tag{55}$$

$$N_1 \cdot M_1 = 1 \mod m_1 \tag{56}$$

$$N_1 \cdot 77 = 1 \mod 5 \tag{57}$$

$\boxed{N_1 = 3}$

$$N_2 \cdot M_2 = 1 \mod m_2 \tag{58}$$

$$N_2 \cdot 55 = 1 \mod 7 \tag{59}$$

$\boxed{N_2 = 6}$

$$N_3 \cdot M_3 = 1 \mod m_3 \tag{60}$$

$$N_3 \cdot 35 = 1 \mod 11 \tag{61}$$

$\boxed{N_3 = 6}$

$$x = \sum_{i=1}^{r} = a_i \cdot N_i \cdot M_i = 4 \cdot 3 \cdot 77 + 1 \cdot 6 \cdot 55 + 0 \cdot 6 \cdot 11 = 1254 \tag{62}$$

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

$$x \mod m1 \cdot m2 \cdot m3 \tag{63}$$

$$1254 \mod 5 \cdot 7 \cdot 11 \tag{64}$$

$$1254 \mod 5 \cdot 7 \cdot 11 \tag{65}$$

En we vereenvoudigen dit tot:

$$99 \mod 385 \tag{66}$$

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

Modulo $g(x) = x^3+x^2+1$. Dit kan niet ontbonden worden, waardoor er geen nuldelers zijn en de vergelijking oplosbaar is. De 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.)

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

$x^4 = x * x^3 = x^3 + x = x^2 + x + 1$, 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 $x^3 = x^2 + 1 = x^{10 \mod 7} = x^{5^2}$. Dit is tevens de enige oplossing. x^{5+7k} met $k \in \mathbb{Z}$.