Samenvatting Math For IT

Rekenen in Boole algebra

Definitie Boole algebra

1. Een niet-ledige verzameling B vormt een Boole algebra als voldaan is aan volgende axioma's[1]:
2. Er bestaan in B twee bewerkingen: optelling en vermenivuldiging.
3. Beide bewerkingen zijn commutatief.
4. Elke bewerking is distributief t.o.v. de andere.
5. 0 is neutraal element voor optelling, 1 voor vermenigvuldiging.
6. Er bestaat in B een unaire[2] bewerking → complementering.

In symbolen zijn deze axioma's:

$B_{+,*,-}$ is een Boole algebra als voldaan is aan volgende voorwaarden: $\underline{x}$ = x complement

1.	$\forall x,y \in B$:	$x+y \in B$ $x*y \in B$	intern
2.	$\forall x,y \in B$:	$x+y = y+x$ $x*y = y*x$	commutatief
3.	$\forall x,y,z \in B$:	$x*(y+z) = x*y + x*z$ $x+y*z = (x+y)*(x+z)$	distributief
4.	$0 \in B, \forall x \in B$: $1 \in B, \forall x \in B$:	$x+0 = x$ $x*1 = x$	neutraal element
5.	$\forall x \in B: \exists \underline{x} \in B$:	$x*\underline{x} = 1$ x+x = 0	complementering

Prioriteitsregels

1. Haakjes uitwerken
2. Complement uitwerken
3. Vermenigvuldiging
4. Optelling

[1] stelling die geen bewijs hoeft
[2] bewerking waarvoor maar 1 parameter nodig is

Samenvatting Math For IT

Wat is de kleinst mogelijke Boole algebra?

+	0	1
0	0	1
1	1	1

*	0	1
0	0	0
1	0	1

0=1
1=0

0 neutraal elementvoor +
1 neutraal element voor *
+ commutatief
* commutatief

x+y*z = (x+y)*(x+z)
neem x=y=1 z=0
1+1*0 = (1+1)*(1+0)
1+0 = (1+1)*1
1 = 1+1

x*(y+z) = x*y+x*z
neem x=y=0 z=1
0(0+1) = 0*0+0*1
0*1 = 0*0+0
0 = 0*0

0+0=1 1+1=1
0*0=0 1*1=0

Dualiteitsprincipe

Elke stelling, elke uitdrukking of algebraïsche identiteit afgeleid uit de axioma´s blijft geldig wanneer men de bewerkingen + en * en ook de elementen 0 en 1 onderling verwisselt in de hele stelling of identieit.

vb. x*(x+y)= x*y Duale: x+(x*y) = x+y

Stellingen

Stelling 1: Het complement is uniek

Bewijs: Stel dat x 2 complementen a en b heeft

Definitie complement

x+a = 1
x*a = 0

x+b = 1
x*b = 0

a = a*1	1 neutraal element voor *	b = b*1
= a*(x+b)	definitie complement	= b*(x+a)
= a*x+a*b	* distributief t.o.v. +	= b*x+b*a
= x*a+a*b	* commutatief	= x*b+b*a
= 0+a*b	definitie complement	= 0+b*a
= a*b	0 neutraal element voor +	= b*a

Besluit

a = a*b en b = a*b
a = b

Stelling 2: Het complement is involutief $\forall x \in B: \underline{\underline{x}} = x$

Bewijs: $\underline{x}$ is het complement van $\underline{x}$

$x+\underline{x} = 1$	definitie complement
$x*\underline{x} = 0$	definitie complement

$\underline{x}$ is het complement van x

$x+\underline{x} = 1$	definitie complement	$\underline{x}+x = 1$	+ commutatief
$x*\underline{x} = 0$	definitie complement	$\underline{x}*x = 0$	* commutatief

Besluit

$\underline{\underline{x}} = x$ complement is immers uniek

Stelling 3: idempotentie $\forall x \in B: x+x = x \quad x*x = x$

Bewijs: Omwille van het dualiteitsprincipe volstaat aan te tonen dat x+x = x

$x+x = (x+x)*1$	1 neutraal element voor *
$= (\mathbf{x}+x)*(\mathbf{x}+\underline{x})$	definitie complement
$= \mathbf{x}+x*\underline{x}$	+ distributief t.o.v. *
$= x+0$	definitie complement
$= x$	0 neutraal element van +

Stelling 4: Absorberende elementen $\forall x \in B: x+1 = 1 \quad x*0 = 0$

Bewijs: Omwille van het dualiteitsprincipe volstaat om aan te tonen dat x+1 = 1

$x+1 = (x+1)*1$	1 neutraal element voor *
$= (\mathbf{x}+1)*(\mathbf{x}+\underline{x})$	definitie complement
$= \mathbf{x}+1*\underline{x}$	+ distributief t.o.v. *
$= x+\underline{x}$	1 neutraal element van *
$= 1$	definitie complement

Stelling 5: Absorptiewetten

Bewijs niet kennen voor examen!

…

$x+x*y = x*(x+y) = x$

…

Stelling 6: Wetten van de Morgan $\forall x,y \in B: \overline{x+y} = \overline{x}*\overline{y}$ $\overline{x*y} = \overline{x}+\overline{y}$

Bewijs: Dualiteitsprincipe

$x+y+\overline{x+y}=1$ We tonen aan dat $x+y+\overline{x}*\overline{y} = 1$ 1

$(x+y)*\overline{x+y} = 0$ $(x+y)*\overline{x}*\overline{y} = 0$ 2

We hebben aangetoond dat $\overline{x+y} = \overline{x}*\overline{y}$ immers het complement is uniek.

1	$x+y+\overline{x}*\overline{y} = x+\overline{x}*\overline{y}+y$	+ commutatief
	$= (x+\overline{x})*(x+\overline{y})+y$	+ distributief t.o.v. *
	$= 1*(x+\overline{y})+y$	definitie complement
	$= x+\overline{y}+y$	1 neutraal element voor *
	$= x+1$	definitie complement
	$= 1$	1 absorberend element voor +
2	$(x+y)*\overline{x}*\overline{y} = x*\overline{xy}+y*\overline{xy}$	* distributief t.o.v. +
	$= x*\overline{xy}+y*\overline{yx}$	* commutatief
	$= 0*\overline{y}+0*\overline{x}$	definitie complement
	$= 0+0$	0 absorberend element voor *
	$= 0$	0 neutraal element voor +

Rekenen in Boole algebra

Stap 1: functie uitwerken m.b.v. prioriteitsregels en daarna vereenvoudigen.

Prioriteitsregels:

1. haakjes uitwerken
2. complement uitwerken
3. vermenigvuldigen
4. optellen

Vereenvoudigen:

1. $x*x=x$
2. $x+x=x$
3. $x*\overline{x}=0$
4. $x+\overline{x}=1$

Stap 2: gemeenschappelijke factoren

Zijn er gemeenschappelijke factoren die ik kan buitenzetten zodat datgene wat tussen haakjes overblijft vereenvoudigd kan worden?

vb. $x*y+x*\overline{y} = x*(y+\overline{y}) = x*1 = x$

$xyz+xy+x = x(yz+y+1) = x*1 = x$

Opm.: NIET bij $x*y+x*z = x*(y+z)$

Stap 3: distributiviteit van + t.o.v. *

x+x*y = (x+x)*(x+y)
= 1*(x+y)
= x+y

(x+y)*(x+y) = x+y*y
= x+0
= x

Stap 4: Dualiteitsprincipe

Als je een bepaalde uitdrukking hebt, kan je + en - verwisselen en bekom je een nieuwe geldige uitdrukking.

(x+y+z)*(x+y+z) = x+y

(**x+y**+z)*(**x+y**+z) = **x+y**+z*z
= x+y+0
= x+y

(**x*y***z)+(**x*y***z) = x*y

(**x*y***z)+(**x*y***z) = **x*y***(z+z)
= x*y*1
= x*y

DNV (Disjunctieve normaalvorm)

= som van minimale termen

vb. f(x,y) = xy+xy
f)x,y,z' ° xyz+xyz+xyz

Veitch/Karnaugh diagaram

n=1	1 variabele	1 vakje
n=2	product van 2 variabelen	1 vakje
	1 variabele	2 aanliggende vakjes
n=3	product van 3 variabelen	1 vakje
	product van 2 variabelen	2 aanliggende vakjes
	1 variabele	4 aanliggende vakjes
n=4	product van 4 variabelen	1 vakje
	product van 3 variabelen	2 aanliggende vakjes
	product van 2 variabelen	4 aanliggende vakjes
	1 variabele	8 aanliggende vakjes

Samenvatting Math For IT

Propositielogica

Vragende zinnen en gebiedende zinnen[3] zijn geen proposities.

Het negatieteken ¬ (niet)

p = zij is ziek ¬p = zij is niet ziek

Het disjunctieteken ∨ (∨ = + = of)

'Jan wast af of droogt de vaat' wordt p ∨ q

p = Jan wast af
q = Jan droogt de vaat

Waarheidstabel:

p	q	p∨q
0	0	0
0	1	1
1	0	1
1	1	1

		q	
	∨	0	1
p	0	0	1
	1	1	1

Het conjunctieteken ∧ (∧ = * = en)

'Jan studeert en hij is verstandig' wordt p ∧ q

p = Jan studeert
q = hij is verstandig

Waarheidstabel:

p	q	p∧q
0	0	0
0	1	0
1	0	0
1	1	1

		q	
	∧	0	1
p	0	0	0
	1	0	1

[3] zinnen met een ? en een !

Samenvatting Math For IT

Het implicatieteken ⇒ (als … dan …)

'Als ik slaag in 1TIN, dan krijg ik een auto'

p = ik slaag in 1TIN

q = krijg een auto

p	q	p⇒q	
0	0	1	$\underline{p}\underline{q}$
0	1	1	$\underline{p}\underline{q}$
1	0	0	
1	1	1	pq

Verder vereenvoudigen

$p \Rightarrow q = \underline{p}\underline{q}+\underline{p}q+pq$
$= \underline{p}(\underline{q}+q)+pq$
$= \underline{p}*1+pq$
$= p+pq$
$= (\underline{p}+p)*(\underline{p}+q)$
$= \underline{p}+q$

OF

		p
	X	
q	X	X

p+q

Het equivalentieteken ⇔ ('als en slechts als', 'enkel en alleen als', 'dan en slechts dan als')

'Ik open een paraplu enkel en alleen als het regent' wordt p⇔q

p = ik open een paraplu
q = het regent

Waarheidstabel:

p	q	p⇔q	
0	0	1	$\underline{p}\underline{q}$
0	1	0	
1	0	0	
1	1	1	pq

DNV: $p \Leftrightarrow q = \underline{p}\underline{q}+pq$

		p
	X	
q		X

Er kan niks samengenomen worden, dit is dus de meest eenvoudige vorm.

Samenvatting Math For IT

Het exclusieve disjunctieteken ⊕ of XOR (ofwel... ofwel...)

'Ofwel krijg je een auto ofwel mag je op kot' wordt p⊕q

p = je krijgt een auto
q = je mag op kot

Waarheidstabel:

p	q	p⊕q	
0	0	0	
0	1	1	$\underline{p}q$
1	0	1	$p\underline{q}$
1	1	0	

DNV: $p \oplus q = \underline{p}q + p\underline{q}$

		p
		X
q	X	

Er kan niks samengenomen worden, dit is dus de meest eenvoudige vorm.

Schakelalgebra

p1-33, in het boek nakijken, kan de poorten hier niet tekenen!

Werken met EuMathT

Ieder voor zich, fuck EuMathT en zijn vriendin Maxima.

Deel 3: Inleiding tot cryptografie

Hoofdstuk 1: Inleiding

Sleutel: informatie die iemand nodig heeft om een boodschap te encrypteren/decrypteren (getal, paswoord of sleutelzin).

Soorten cryptosystemen

Symmetrische cryptosystemen

Zender en ontvanger hebben dezelfde sleutel.

bv. typische geheim schrift

Cryptosystemen met openbare sleutel

De sleutel waarmee vercijferd wordt is openbaar.

De sleutel waarmee ontcijferd wordt is privé.

bv. duizenden mensen kunnen berichten vercijferen met dezelfde openbare sleutel (jouw openbare sleutel), jij kan jouw privésleutel gebruiken om te ontcijferen.

Hoofdstuk 2: Symmetrische cryptosystemen

Transpositie: verwisselen van letters van het bericht op een vooraf afgesproken manier.

Substitutie: de letters vervangen door andere letters op een vooraf afgesproken manier.

Wij gaan gebruik maken van de substitutiemethode.

De Caesarrotatie (=Caesarsubstitutiemethode)

Methode

Elke letter wordt cyclisch over k plaatsen verschoven.

- Met k=1 wordt de a een b, de b een c… en de z wordt weer een a.
- Met k=4 en de boodschap TIN krijg je dan TIN → XMR
- Met k=8 en de boodschap HALLO krijg je dan HALLO → OHSSV

Sleutel: de waarde k die we kunnen wijzigen. Ontvanger moet vooraf weten wat de sleutel is om het te kunnen ontcijferen.

Samenvatting Math For IT

De Caesarrotatie op computer

Coderen

Stap 1: Aan elke letter van het alfabet wordt een getal toegekend.
bv. a=0, b=1 … z=25

Stap 2: Het getal vermeerderen met de sleutelwaarde.

Stap 3: Als het bekomen getal >= 26 is, modulo 26 rekenen.

Stap 4: Bekomen getal terug omzetten naar een letter.

Decoderen

Stap 1: aan elke letter van het alfabet wordt een getal toegekend.
bv. a=0, b=1 … z=25

Stap 2: De getallen verminderen met de sleutelwaarde.

Stap 3: Wanneer het bekomen getal < 0, tel 26 op bij het bekomen getal totdat het bekomen getal >= 0, modulo 26 rekenen.

Stap 4: Het bekomen getal terug omzetten naar een letter.

Oefening

Vercijfer de boodschap 'bart' met behulp van de Caesarrotatie met als sleutel k=9 en decodeer vervolgens.

Coderen	b	a	r	t
Stap 1	2	1	17	19
	+9	+9	+9	+9
Stap 2	11	10	26	28
	modulo 26 rekenen			
Stap 3	11	10	0	2
Stap 4	l	k	a	c

Decoderen	l	k	a	c
Stap 1	11	10	0	2
	-9	-9	-9	-9
Stap 2	2	1	-9	-7
	modulo 26 rekenen			
Stap 3	2	1	17	19
Stap 4	b	a	r	t

Samenvatting Math For IT

Eenvoudige substitutiemethode met de computer

Coderen	b	a	r	t	Decoderen	k	t	{	}
	ascii("letter")					ascii("letter")			
Stap 1	98	97	114	116	**Stap 1**	107	116	123	125
	+9	+9	+9	+9		-9	-9	-9	-9
Stap 2	107	116	123	125	**Stap 2**	98	97	114	116
	mod(cijfer,256)					mod(cijfer,256)			
Stap 3	107	116	123	125	**Stap 3**	98	97	114	116
	char(cijfer)					char(cijfer)			
Stap 4	k	t	{	}	**Stap 4**	b	a	r	t

Substitutiemethode met behulp van de bitoperator XOR

//dit kwam niet op de PE, misschien wel op het examen: p3-8

Kraken van substitutiemethoden

//dit kwam niet op de PE, misschien wel op het examen: p3-11

Blokcijfersystemen

Blokcijfersystemen op basis van de Caesarrotatie

Coderen:

Boodschap:	I	N	F	O	R	M	A	T	I	C	A
Sleutel:	T	I	N	T	I	N	T	I	N	T	I
Numeriek:	8	13	5	14	17	12	0	19	8	2	0
	19	8	13	19	8	13	19	8	13	19	8
Optellen:	27	21	18	33	25	25	19	1	21	21	8
Modulo 26:	1	21	18	7	25	25	19	1	21	21	8
Tekst:	B	V	S	H	Z	Z	T	B	V	V	I

Decoderen:

Identiek aan coderen, maar dan Aftrekken in plaats van Optellen.

Blokcijfersystemen op basis van de XOR-methode

//dit kwam niet op de PE, misschien wel op het examen: p3-14

DES (Data Encryption Standard)

//dit kwam niet op de PE, misschien wel op het examen: p3-15

Samenvatting Math For IT

Enkele nadelen symmetrische cryptosystemen

Zender en ontvanger moeten een sleutel afspreken.

In een netwerk zal je veel meer sleutels moeten creëren dan er mensen op het netwerk zijn.

Hoofdstuk 4: Asymmetrische Cryptosystemen

De RSA-methode (uit 1977) behandelt de te vercijferen tekst door puur wiskundige methoden toe te passen op elke individuele letter of groepjes letters van het bericht.

e: encrypteren
m: multiplication
M: message
d: decryption
S(M): sent message

bv.:

Coderen
Openbare sleutel Piet: e=989, m=1073

Boodschap: bart is leuk

in ascii → 98 97 114 116 32 105 115 32 108 101 117 107

Iemand die een boodschap voor Piet wilt vercijferen (per letter):
M^e(mod m) → asciiwaarde_van_letter^{989}(mod1073) = vercijferde letter in ascii

Decoderen
Privésleutel Piet: d=53, m=1073

Ontvangen boodschap: 98 97 114 116 32 105 115 32 108 101 117 107

Ontcijferen (per letter**): S(M)^d(mod m)** → asciiwaarde_van_vercijferde_letter^{53}(mod1073)

De RSA-methode

blablabla

Bekijk pagina 3-22 + 3-29, een soortgelijke oefening moet je kunnen oplossen!

Bekijk ook pagina 3-30 (de juiste versie vind je op blackboard, deze heb je zojuist ook in de FB-chat ontvangen).

Bekijk ook de oefening die Frankie in de Facebookgroep heeft gezet.

Deel 4: Lineaire algebra

Hoodstuk 1: Matrices

Bewerkingen met matrices

Matrix transponeren: A → A^T = rijen en kolommen met elkaar verwisselen

Matrices optellen/aftrekken: A en B moeten van dezelfde orde zijn (bv. A = 2x3 en B = 2x3), vervolgens alle elementen met elkaar optellen.

- Eigenschappen:
  - Commutativiteit: A+B = B+A
  - Associativiteit: (A+B) + C = A + (B+C)
  - 0 neutraal element van +: A+0 = A = A+0

Scalaire vermenigvuldiging: matrix vermenigvuldigen met een getal: Elk element vermenigvuldigen met het getal.

Matrixvermenigvuldiging: matrices vermenigvuldigen met elkaar: 3x3 met 3x2 vermenigvuldigen, dit gaat want 3x**3 3**x2 zijn gelijk, het resultaat is een 3x2 (laat de vetgedrukte 3's wegvallen). Je bekomt het element van de uitkomst op rij 1, kolom 1 door het product van elk element van de eerste rij uit de eerste matrix en elk element van de eerste kolom uit de tweede matrix op te tellen met elkaar.

zie p 4-6 voor een duidelijk voorbeeld

Machten van matrices: zelfde als matrixvermenigvuldigen, maar nu met gelijke matrices.

- Eigenschappen:
  - Associativiteit: (A*B) * C = A * (B*C)
  - Neutraal element: A * I_n = A = I_n * A
  - NIET COMMUTATIEF

Matrices in Euler

(p 4-8 tot en met p 4-10, op p 4-11 staat de samenvatting)

Hoofdstuk 2: Toepassingen van matrixrekening

Overgangsmatrices

Lees eens door in het boek: p4-13

Populatiematrices of Lesliematrices

Lees eens door in het boek: p4-16

Let op: een periode kan 1 maand zijn, maar ook 3maanden of 2 jaar of …!

Samenvatting Math For IT

Verbindingsmatrices

Wel kennen

verbindingsmatrix V (p4-19)

directe wegenmatrix W (p4-20)

tweestapswegen W^2 (p4-20)

$W + W^2$ = matrix met het aantal tussenstations (p4-20)

n-stapswegen W^n (p4-20)

Codematrices

//dit kwam niet op de PE, misschien wel op het examen: p4-21

2D-computergrafieken

- Verschuivingen/translatie in het vlak R^2(p4-24)
- Lineaire transformaties in het vlak R^2 (p4-26)
    - Rotaties rond de oorsprong (p4-30)
    - Samenstelling van 2 lineaire transformaties (p4-33)
- Affiene transformaties in het vlak R^2 (p4-36)
    - Rotatie rond een punt verschillend van de oorpsrong (p4-37)
    - Spiegeling t.o.v. een willekeurige rechte y=ax+b (p4-39)

Hoofdstuk 3: Stelsels van lineaire vergelijkingen

Geen zin meer om dit samen te vatten, have fun!

Hoofdstuk 4: Inverse van een matrix

Moest ik niet kennen, enkel voor die het wel gehad hebben!

Succes iedereen!