

Boole'i funktsioonid

Mati Tombak

Informaatika instituut
Tallinna Tehnikaülikool

0-muutuja ja 1-muutuja BF

Boole'i funktsioon on funktsioon, mille määramispiirkond ja muutumispiirkond on hulk $\{0, 1\}$.

0-muutujaga Boole'i funktsioonid on konstantsed funktsioonid – **0**, mille väärtus on alati 0 ning **1**, mille väärtus on alati 1.

1-muutuja Boole'i funktsioone on neli:

x	0	$\neg x$	x	1
0	0	1	0	1
1	0	0	1	1

Nagu tabelist näha, sisalduvad ühe muutuja Boole'i funktsioonide tabelis ka 0-muutuja funktsioonid.

1	1	0	0	x
1	0	1	0	y
0	0	0	0	0
0	0	0	1	$x \nabla y$
0	0	1	0	$x \not\leftarrow y$
0	0	1	1	$\bar{x}$
0	1	0	0	$x \not\rightarrow y$
0	1	0	1	$\bar{y}$
0	1	1	0	$x \oplus y$
0	1	1	1	$x \bar{\&} y$
1	0	0	0	$x \& y$
1	0	0	1	$x \equiv y$
1	0	1	0	y
1	0	1	1	$x \rightarrow y$
1	1	0	0	x
1	1	0	1	$x \leftarrow y$
1	1	1	0	$x \vee y$
1	1	1	1	1

Mõned kahe muutuja Boole'i funktsioonid.

konjunktsioon, AND

x	y	$x \& y$
0	0	0
0	1	0
1	0	0
1	1	1

disjunktsioon, OR

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

mitteekvivalents, XOR

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

implikatsioon

x	y	$x \rightarrow y$
0	0	1
0	1	1
1	0	0
1	1	1

ekvivalents

x	y	$x \equiv y$
0	0	1
0	1	0
1	0	0
1	1	1

eitus, NOT

x	$\neg x$
0	1
1	0

Boole'i valem (lausearvutuse valem).

Muutujad on x, y, z, w ja needsamad koos indeksitega, s.t. $x_1, x_2, \dots, y_1, \dots$

Boole'i valem defineeritakse induktiivselt:

1. Iga muutuja on Boole'i valem.
2. Kui A on Boole'i valem, siis on ka $(\neg A)$ Boole'i valem.
3. Kui A ja B on Boole'i valemid, siis on ka $(A \& B), (A \vee B), (A \rightarrow B)$ ja $(A \equiv B)$ Boole'i valemid. Tehete prioriteedid on kahanevalt $\neg, \&, \vee, \rightarrow, \equiv$.

Kui lepime kokku, et valem arvutatakse vasakult paremale, sooritades suurema prioriteediga tehted enne, kui sulud ei tekita teistsugust järjekorda, siis võib tarbetud sulud ära jätta.

Substitutsioon.

Olgu antud Boole'i valemid A ja B ning muutuja x . Valemi B *substitutsioon* valemisse A muutuja x asemele (tähistame $\mathcal{S}_x^B(A)$) on valem mille saame valemist A , asendades valemis A kõik muutuja x esinemised valemiga (B) .

$$\mathcal{S}_z^{x \rightarrow y}(w \vee \neg z) = w \vee \neg(x \rightarrow y)$$

$$\mathcal{S}_z^{x \rightarrow y}(y \oplus \neg z) = y \oplus \neg(x \rightarrow y)$$

$$\mathcal{S}_z^{x \rightarrow y}(z \rightarrow x \& z) = (x \rightarrow y) \rightarrow x \& (x \rightarrow y)$$

$$\mathcal{S}_x^{\neg x}(\neg \neg x \equiv x) = \neg \neg(\neg x) \equiv (\neg x)$$

Omadus: Kui valem A on samaselt tõene, siis on ka $\mathcal{S}_x^B(A)$ samaselt tõene. Seega kehtivad kõik harjutustundides tõestatud omadused ka juhul kui muutujate asemele on substitueeritud suvalised valemid.

0. Disjunksioon ja konjunksioon on assotsiatiivsed.

$$(A \vee B) \vee C \equiv A \vee (B \vee C)$$

$$(A \& B) \& C \equiv A \& (B \& C)$$

1. Konjunksioon on distributiivne disjunksiooni suhtes.

$$A \& (B \vee C) \equiv (A \& B) \vee (A \& C)$$

2. Disjunksioon on distributiivne konjunksiooni suhtes.

$$A \vee (B \& C) \equiv (A \vee B) \& (A \vee C)$$

3. Eituse viimine konjunksiooni alla muudab tehte disjunksiooniks.

$$\neg(A \& B) \equiv \neg A \vee \neg B$$

4. Eituse viimine disjunksiooni alla muudab tehte konjunksiooniks.

$$\neg(A \vee B) \equiv \neg A \& \neg B$$

5. Konjunktsioon on kommutatiivne.

$$A \& B \equiv B \& A$$

6. Disjunktsioon on kommutatiivne.

$$A \vee B \equiv B \vee A$$

7. Implikatsiooni semantika.

$$A \& (A \rightarrow B) \rightarrow B$$

8. Valemi lihtsustusreeglid.

$$(A \& B) \vee (\neg A \& B) \equiv B$$

$$(A \vee B) \& (\neg A \vee B) \equiv B$$

9. Ekvivalents ja implikatsioon.

$$(A \equiv B) \equiv ((A \rightarrow B) \& (B \rightarrow A))$$

10. Implikatsioon ja disjunktsioon.

$$(A \rightarrow B) \equiv (\neg A \vee B)$$

11. Implikatsioon ja konjunktsioon.

$$(A \rightarrow B) \equiv \neg(A \& \neg B)$$

12. Kahekordne eitus.

$$\neg\neg A \equiv A$$

Disjunktiiivne normaalkuju (DNF)

Definitsioon. Lausearvutuse valem F on *disjunktiiivsel normaalkujul*, kui ta on esitatav järgmiselt:

$$F(x_1, \dots, x_n) = \bigvee_{i=1}^p C_i,$$

kus C_i on *term*, mis on kujul

$$C_i = \bigwedge_{j=1}^{m_i} l_{ij},$$

kus l_{ij} on *literaal*. Literaal on muutuja või selle eitus.

Konjunkttiivne normaalkuju (CNF)

Definitsioon. Lausearvutuse valem F on *konjunkttiivsel normaalkujul*, kui ta on esitatav kujul

$$F(x_1, \dots, x_n) = \bigwedge_{i=1}^p D_i$$

kus D_i on *lause*, mis on kujul $D_i = \bigvee_{j=1}^{m_i} l_{ij}$ kus l_{ij} on *literaal*. Literaal on muutuja või selle eitus.

Rakendused I. Skeemtehnoloogia.

Rakendused II. Matemaatika alused.

Leibnitz, Hilbert. Enamus matemaatikast tegeleb lõpmatute hulkadega (täisarvud, ratsionaalarvud, reaalarvud). Nende käsitlemiseks laiendatakse Boole'i loogikat predikaatarvutusega. Predikaat on funktsioon, mille määramispiirkond on suvaline hulk ja muutumispiirkond on hulk $\{0, 1\}$. Näiteks liitmisele vastab predikaat $+(x, y, z)$, mis defineeritakse:

$$+(x, y, z) = 1, \text{ kui } x + y = z; \quad +(x, y, z) = 0, \text{ kui } x + y \neq z.$$

Operatsioonidest lisanduvad *kvantorid*: $\forall xF(x)$ ja $\exists xF(x)$.

Tabelimeetod samaselt tõesuse näitamiseks ei ole rakendatav kuna me ei saa ehitada lõpmatuid tabeleid. Selle asemel antakse aksioomid ja tuletusreeglid, nii et süsteem on täielik (kõik samaselt tõesed predikaatarvutuse valemid on tuletatavad) ja mittevastuoluline (iga tuletatav valem on samaselt tõene).

Matemaatilise teooria kirjeldamiseks lisatakse vajalikud aksioomid.

Naturaalarvude aritmeetika aksioomid.

$$\forall x \in N(0 \neq S(x))$$

$$\forall x, y \in N(s(x) = s(y) \rightarrow x = y)$$

$$\forall x \in N(x + 0 = x)$$

$$\forall x, y \in N(x + s(y) = s(x + y))$$

$$\forall x \in N(x \cdot 0 = 0)$$

$$\forall x, y \in N(x \cdot s(y) = x \cdot y + x)$$

Neile lisandub täieliku induktsiooni aksioom.

$$\forall \bar{y}(\phi(0, \bar{y}) \& \forall x(\phi(x, \bar{y}) \rightarrow \phi(s(x), \bar{y}))) \rightarrow \forall x \phi(x, \bar{y})$$

ϕ on suvaline valem, mis sisaldab muutujat x .

Gödeli teoreem (Kurt Gödel, 1931). Ükski aksiomaatiline teooria, mis sisaldab eelmisel slaidil toodud naturaalarvude aritmeetika aksioome ei saa olla samaaegselt mittevastuoluline ja täielik.

Rakendused III. Automaattõestamine.

Teoreem. Ei leidu algoritmi, mis arvutaks suvalise predikaatarvutuse valemi järgi selle tõestuse. (Church, Kleene 1936.)

|Sellest sai alguse *algoritmiteooria* ja 35 aastat hiljem ka *keerukusteooria*.

Olemas on programmid, mis otsivad tõestust etteantud ajalimiidi piires Samuti on uuritud lahenduvaid valemite alamklasse ja programmeeritud vastavaid tõestajaid.

Rakendused IV. Programmi tõeestamine.

Seatakse tingimused programmi $P : X \implies Y$ algandmetele $pre(X)$ ja tulemusele $post(Y)$ ning otsitakse tõestust väitele

$$pre(X)[P]post(Y)$$

"Kui algandmete X jaoks on täidetud tingimused $pre(X)$, siis programmi rakendamise tulemus rahuldab tingimusi $post(Y)$ ".

Eestis tegeleb selle valdkonnaga akadeemik Tarmo Uustalu.

Rakendused V. Programmide süntees.

Siin kasutatakse intuitsionistlikku loogikat. See on antud predikaatarvutuse aksioomide alamhulgaga, millest on eemaldatud välistatud kolmanda seadusega seotud aksioomid (näit. $\neg\neg A \equiv A$).

Otsitakse tõestust valemile $pre(X) \rightarrow post(Y)$. Sellest tõestusest arvutatakse programm.

Eestis tegeleb selle valdkonnaga akadeemik Enn Tõugu.

Rakendused VI. Kitsendustega programmeerimine (Constraint programmeng)

Kasutatakse andmevoogude teisendamiseks. Sisendandmete jaoks antakse loogilised tihngimused ja neile vastavad arvutuseeskirjad, mis määravad väljundvoo. Rakendused on eriti statistilises andmetöötles.

Rakendused VII. Vastushulkadega programmeerimine

Valem sisaldab ainult tõkestatud kvantoreid, mis on defineeritud lõplikel hulkadel. Sellisel juhul on valem teisendatav lausearvutuse valemiks ja iga selle valemi mudel (tõene väärtustus) on vastuseks. Kasutatakse näiteks diskreetse matemaatika objektide ja nende omaduste uurimiseks.