[Vera Koponen 2009] ①

Boolesk algebra

Konnektiven $\neg$, $\wedge$, $\vee$ kallas ibland för <u>Booleska konnektiv</u> och är besläktade med så kallade "Booleska operationer" på ett sätt som kommer att framgå.

Låt L_2 beteckna mängden av alla formler som kan byggas upp från två atomära formler P_1, P_2 med hjälp av $\neg$, $\wedge$, $\vee$.

Det är inte svårt att inse att '$\overset{\text{taut}}{\Longleftrightarrow}$' är en ekvivalensrelation på L_2, dvs '$\overset{\text{taut}}{\Longleftrightarrow}$' uppfyller

<u>reflexivitet</u>: $A \overset{\text{taut}}{\Longleftrightarrow} A$ för alla $A \in L_2$.

<u>symmetri</u>: För alla $A, B \in L_2$, om $A \overset{\text{taut}}{\Longleftrightarrow} B$ så $B \overset{\text{taut}}{\Longleftrightarrow} A$.

<u>transitivitet</u>: För alla $A, B, C \in L_2$, om $A \overset{\text{taut}}{\Longleftrightarrow} B$ och $B \overset{\text{taut}}{\Longleftrightarrow} C$ så $A \overset{\text{taut}}{\Longleftrightarrow} C$.

För varje $A \in L_2$ så definierar vi nu $[A] = \{B \in L_2 : A \overset{taut}{\Longleftrightarrow} B\}$.

Det följer att $[A] = [B]$ om och endast om $A \overset{taut}{\Longleftrightarrow} B$. (Övning att verifiera detta.)

Låt $L_2^* = \{[A] : A \in L_2\}$.

Man kan nu definiera operationer $\oplus$, $\otimes$ och $\sim$ på L_2^* så här:

$$[A] \oplus [B] = [A \vee B]$$
$$[A] \otimes [B] = [A \wedge B]$$
$$\sim [A] = [\neg A]$$

Från faktumet att '$\overset{taut}{\Longleftrightarrow}$' är en ekvivalensrelation så följer att om

$[A] = [B]$ så $\sim[A] = [\neg A] = [\neg B] = \sim[B]$

så operationen $\sim$ är entydigt definierad på L_2^*. På liknande sätt så inser man att operationerna $\oplus$ och $\otimes$ är entydigt definierade på L_2^*.

På grund av välkända tautologiska ekvivalenser så får vi följande räkneregler för $\oplus$, $\otimes$ och $\sim$: Om a, b, c betecknar element i L_2^* så

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

$$a \oplus b = b \oplus a$$

$$a \otimes b = b \otimes a$$

$$a \oplus a = a$$

$$a \otimes a = a$$

$$\left.\begin{array}{l} a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c) \\ a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \end{array}\right\} \text{distributivitet}$$

$$\left.\begin{array}{l} \sim(a \oplus b) = (\sim a) \otimes (\sim b) \\ \sim(a \otimes b) = (\sim a) \oplus (\sim b) \end{array}\right\} \text{de Morgans lagar}$$

$$a \oplus (a \otimes b) = a \quad , \quad a \otimes (a \oplus b) = a.$$

Om $\underline{0}$ betecknar $[P_1 \wedge \neg P_1]$ och $\underline{1}$ betecknar $[P_1 \vee \neg P_1]$ så gäller även följande räkneregler:

$a \oplus \underline{0} = a$, $a \otimes \underline{0} = \underline{0}$

$a \oplus \underline{1} = \underline{1}$, $a \otimes \underline{1} = a$

$a \oplus (\sim a) = \underline{1}$.

Notera att om man byter ut a, b, c mot formler och

$\sim, \otimes, \oplus$ mot $\neg, \wedge, \vee$ (respektive),

'$=$' mot '$\overset{\text{taut}}{\Longleftrightarrow}$',

$\underline{0}$ mot $A \wedge \neg A$ och $\underline{1}$ mot $A \vee \neg A$,

så får man tautologiska ekvivalenser i samtliga fall (där A kan vara vilken formel som helst).

<u>Definition</u> En <u>Boolesk algebra</u> är en 6-tupel $(M, \oplus, \otimes, \sim, \underline{0}, \underline{1})$ där M är en mängd, $\underline{0}$ och $\underline{1}$ är olika element som tillhör M, och $\oplus$, $\otimes$ och $\sim$ är operationer som uppfyller alla räkneregler som angivits på denna och föregående sida.

Det följer att $(L_2^*, \oplus, \otimes, \sim, \underline{0}, \underline{1})$ med de tidigare givna definitionerna av $\oplus, \otimes, \sim, \underline{1}$ och $\underline{0}$ är en Boolesk algebra.

För varje (icke-tom) mängd N så kan en Boolesk algebra genereras på följande sätt. Låt

$$M = \{X : X \subseteq N\}$$ (så M består av alla delmängder av N).

För $X, Y \in M$ definieras sedan

$$X \oplus Y = X \cup Y$$
$$X \otimes Y = X \cap Y$$
$$\sim X = N \setminus X = \{x \in N : x \notin X\}$$

(så $\sim X$ är "komplementet till X i N").

Och slutligen låter vi $\underline{0} = \emptyset$ = "tomma mängden" och $\underline{1} = N$. På detta sätt blir $(M, \oplus, \otimes, \sim, \underline{0}, \underline{1})$ en Boolesk algebra. Verifikationen av de flesta räknereglerna är mer eller mindre trivial och distributiviteten samt de Morgans lagar fås från de välkända mängdteoretiska likheterna (som ofta benämns på samma sätt)

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$
$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

$$N \setminus (X \cup Y) = (N \setminus X) \cap (N \setminus Y)$$

$$N \setminus (X \cap Y) = (N \setminus X) \cup (N \setminus Y)$$

(där vi antar att $X, Y \subseteq N$).

Så vi har stora likheter mellan $\vee, \wedge, \neg$ och Booleska operationer $\oplus, \otimes, \sim$ och mängdoperationerna $\cup, \cap$, "komplement".

Mera om $(L_2^*, \oplus, \otimes, \sim, \underline{0}, \underline{1})$

där $\oplus, \otimes, \sim, \underline{1}$ och $\underline{0}$ är definierade som beskrivits tidigare.

Låt oss först fundera på hur många element som L_2^* innehåller.
L_2 är oändlig, för L_2 innehåller $P_1, P_1 \wedge P_1, P_1 \wedge P_1 \wedge P_1, \ldots$ osv...

På så sätt som förklaras i en annan stencil, om Booleska funktioner och konnektiv,[1] så ger varje formel $A \in L_2$ upphov till en binär Boolesk funktion F_A, och om $A, B \in L_2$ så gäller att

$$A \overset{taut}{\iff} B \text{ om och endast om } F_A = F_B.$$

Därför motsvarar (eller "representerar") varje $[A] \in L_2^*$ (exakt) en binär Boolesk funktion. Eftersom det finns (exakt) 16 binära Booleska funktioner så har L_2^* högst 16 element. Enligt en sats i ovan nämnda stencil så finns för varje binär Boolesk funktion G en formel $A \in L_2$ sådan att $F_A = G$.

---

[1] Läs den stencilen först.

Därmed följer att L_2^* har exakt 16 element.

Vi påpekade ovan att varje $[A] \in L_2^*$ motsvarar en Boolesk funktion, nämligen F_A.

Operationerna $\oplus, \otimes, \sim$ motsvarar i sin tur särskilda sammansättningar av binära Booleska funktioner, på följande vis:

Operationerna

$$[A] \oplus [B], \quad [A] \otimes [B], \quad \sim[A]$$

motsvarar sammansättningarna

$$F_{P_1 \vee P_2}(F_A(x_1, x_2), F_B(x_1, x_2)), \quad F_{P_1 \wedge P_2}(F_A(x_1, x_2), F_B(x_1, x_2))$$

och $F_{\neg P_1}(F_A(x_1, x_2))$, respektive.

Innan vi går vidare kan nämnas att binära Booleska funktioner är i princip detsamma som logiska kretsar/grindar. (Skillnaden är bara en fråga om formulering.)

En sak som kanske har bekymrat vissa läsare är att en del formler i L_2, som tex. P_1, bara har en av P_1 och P_2 som delformel, och frågan är hur en binär Boolesk funktion F_{P_1} associeras med tex. P_1. Svaret är att F_{P_1} som binär funktion bara beror på sitt första argument, som motsvar P_1: $F_{P_1}(s,s)=s$, $F_{P_1}(s,f)=s$, $F_{P_1}(f,s)=f$, $F_{P_1}(f,f)=f$.

Om man i stället (för P_1, P_2) startar med n stycken atomära formler $P_1, \ldots, P_n$ så kan man på samma vis konstruera en Boolesk algebra $(L_n^*, \oplus, \otimes, \sim, \underline{0}, \underline{1})$ med $2^{(2^n)}$ element. Sådana Booleska algebror kallas för Lindenbaum-algebror. (Det går också att börja med en oändlig mängd av atomära formler och i detta fall blir Lindenbaum-algebran oändlig.)

Ett till exempel: Låt

$$M = \{ (b_1, \ldots, b_n) : b_i \in \{0,1\},\ i = 1, \ldots, n \},$$

så M består av alla "bitsträngar" av längd n.

Definiera

$$\sim(b_1, \ldots, b_n) = (c_1, \ldots, c_n) \text{ där } c_i = \begin{cases} 0 \text{ om } b_i = 1 \\ 1 \text{ om } b_i = 0. \end{cases}$$

$$(b_1, \ldots, b_n) \oplus (c_1, \ldots, c_n) = (d_1, \ldots, d_n)$$

där $d_i = \begin{cases} 0 & \text{om } b_i = 0 \text{ och } c_i = 0 \\ 1 & \text{annars} \end{cases}$

$$(b_1, \ldots, b_n) \otimes (c_1, \ldots, c_n) = (d_1, \ldots, d_n)$$

där $d_i = \begin{cases} 1 & \text{om } b_i = 1 \text{ och } c_i = 1 \\ 0 & \text{annars} \end{cases}$

$\underline{0} = (0, \ldots, 0)$, $\underline{1} = (1, \ldots, 1)$.

Även i detta fall blir $(M, \oplus, \otimes, \sim, \underline{0}, \underline{1})$ en Boolesk algebra.

Mera om $(L_n^*, \oplus, \otimes, \sim, \underline{0}, \underline{1})$:

Man kan notera att om man definierar $[A] \leq [B]$ till att betyda att $A \overset{\text{taut}}{\Longrightarrow} B$ så blir '$\leq$' en <u>partiell ordning</u> på L_n^*, vilket betyder att '$\leq$' har de tre egenskaperna

reflexivitet: $a \leq a$ för alla a.

transitivitet: för alla a, b, c, om $a \leq b$ och $b \leq c$ så $a \leq c$.

antisymmetri: för alla a, b, om $a \leq b$ och $b \leq a$ så $a = b$.