Discrete Mathematics

7. Boolean Algebra

Boolean algebra

- *Definition:*
  - A ***Boolean lattice*** is a complemented and distributive lattice.
  - A ***Boolean algebra*** is an algebra with signature $<B, +, *, ', 0, 1>$, where + and * are binary operations and ′ is a unary operation called complementation, and the following axioms hold.

    1. $x*x=x$ and $x+x=x$ *(idempotent)*
    2. $(x*y)*z=x*(y*z)$ and $(x+y)+z=x+(y+z)$ *(associative)*
    3. $x*y=y*x$ and $x+y=y+x$ *(commutative)*
    4. $x*(x+y)=x$ and $x+(x*y)=x$ *(absorption)*
    5. $x*(y+z)=(x*y)+(x*z)$ and $x+(y*z)=(x+y)*(x+z)$ *(distributive)*
    6. Every element x has a (unique) complement x' such that $x*x'=0$ and $x+x'=1$ *(complemented)*

Huntington's postulates

- *Huntington's postulates for Boolean algebra*
  - An algebra $<B, *, +, ', 0, 1>$, where * and + are binary operations on the set B, is a *Boolean algebra*, if the followings are true.

    For every $x, y, z \in B$,

    1. $x*y=y*x$ and $x+y=y+x$ (*commutative*)
    2. $x*(y+z)=(x*y)+(x*z)$ and $x+(y*z)=(x+y)*(x+z)$ (*distributive*)
    3. There exist 0 and 1 in B such that $x+0=x$ and $x*1=x$
    4. For every x, there exist x' in B such that $x*x'=0$ and $x+x'=1$ *(complemented)*.

Lemma 1:

1. 0 is a unique element.
2. 1 is a unique element.

Lemma 2:

For every x in B,

1. $x*0=0$.
2. $x+1=1$.

Lemma 3:

For every x in B,

1. $x*x=x$.
2. $x+x=x$

Lemma 4:

For every x in B,

1. $x*(x+y)=x$
2. $x+(x*y)=x$

Lemma 5:

For every x in B,
there is a unique x' in B.

Lemma 6:

For every x in B, $(x')'=x$.

Lemma 7:

For every x and y in B,

1. $x*(x'*y)=0$
2. $x+(x'+y)=1$

Lemma 8:

For every x and y in B,

1. $(x*y)'=x'+y'$
2. $(x+y)'=x'*y'$

Lemma 9 (Associative law):

For every x, y and z in B,

1. $(x*y)*z=x*(y*z)$
2. $(x+y)+z=x+(y+z)$

Stone's Representation Theorem

- *Theorem:*
  - Let $<B, *, +, ', 0, 1>$ be a Boolean algebra. Then $<B, \leq>$ is a *Boolean lattice*, where x and y in B and $x \leq y$ iff $x*y=x$ and $x+y=y$
- *Theorem (Stone's Representation Theorem):*
  - For every *Boolean algebra* $<B, *, +, ', 0, 1>$, there exists a power set algebra $<\wp(A), \cap, \cup, \overline{}, \emptyset, A>$ which is isomorphic to $<B, *, +, ', 0, 1>$.
- *Definition:*
  - Given a *Boolean algebra* $<B, *, +, ', 0, 1>$, an *atom* is the element in B that covers 0.

Proof of Stone's representation theorem

Define $f : B \rightarrow \wp(A)$, where A is a set of atoms, such that for any x in B,
$f(x) = \{ a \mid (a \in A) \text{ and } (a \leq x) \}$.
Claim : f is isomorphism from $<B, *, +, ', 0, 1>$ to $<\wp(A), \cap, \cup, \overline{\ }, \varnothing, A>$.

Lemma 1:
For every $x \neq 0$ in $B, \exists a \in A$,
such that $a \leq x$

Lemma 2:
For every $x \neq 0$ in B and a in A,
one and only one of the following holds.

1. $a \leq x$
2. $a * x = 0 (a \leq x')$

Lemma 3: (homomorphism)

$$f(x') = \overline{f(x)}$$

Lemma 4: (homomorphism)

$f(x*y) = f(x) \cap f(y)$

$f(x+y) = f(x) \cup f(y)$

Lemma 5: (one-to-one)

$x = y$ if $f(x) = f(y)$

Lemma 6: (onto)

For any $\{a_1, a_2, \ldots, a_k\} \subseteq A$,
$\exists\ (a_1 + a_2 + \ldots + a_k) \in B$ such that
$f(a_1 + a_2 + \ldots + a_k) = \{a_1, a_2, \ldots, a_k\}$.

Boolean expression

- *Definition :*
  - A ***Boolean expression*** in *n* variables, $x_1, x_2, \ldots, x_n$, is a finite string of symbols formed by the following manner;
    1. *0* and *1* are *Boolean expressions*.
    2. $x_1, x_2, \ldots, x_n$ are *Boolean expressions*.
    3. If α and β are *Boolean expressions,* the $(\alpha*\beta)$, $(\alpha+\beta)$ are *Boolean expressions*.
    4. If α is a *Boolean expression*, then α' is a *Boolean expression*.
    5. No String of symbols except those formed by steps 1,2,3, and 4 is a *Boolean expression*.

Equivalence

- *Definition:*
  - Two *Boolean expression* $\alpha(x_1, x_2,\ldots, x_n)$ and $\beta(x_1, x_2,\ldots, x_n)$ are ***equivalent*** if one can be obtained from the other by a finite number of applications of identities of a *Boolean algebra*.
- *Definition:*
  - Let $\alpha(x_1, x_2,\ldots, x_n)$ be a *Boolean expression* in *n* variables and $<B, *, +, ', 0,1>$ be any *Boolean algebra* whose elements are denoted by $a_1, a_2,\ldots, a_n$. Let $<a_1, a_2,\ldots, a_n>$ be an *n*-tuple of B^n. Then the ***value*** of the *Boolean expression* $\alpha(x_1, x_2,\ldots, x_n)$ for the *n*-tuple $<a_1, a_2,\ldots, a_n> \in B^n$ is given by $\alpha(a_1, a_2,\ldots, a_n)$ which is obtained by replacing x_1 by a_1, x_2 by a_2,…, and x_n by a_n in the $\alpha(x_1, x_2,\ldots, x_n)$.

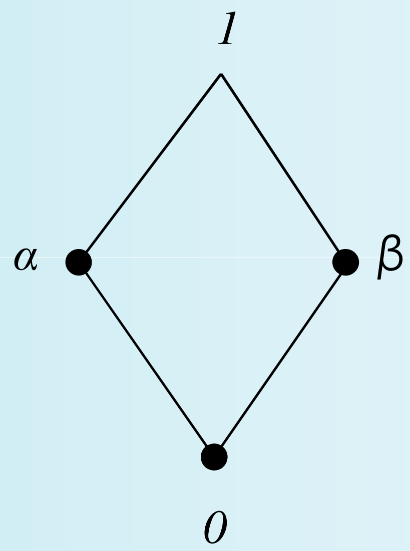
Boolean function

- *Definition:*
  - Let $f{:}B^n \to B$ be a function. If a *Boolean expression* $g(x_1, x_2, \ldots, x_n)$ matches to a function *f,* then we say *g* is ***associated with*** function *f*.

- *Definition:*
  - Let <*B*, *, +, ', *0*, *1*> be a *Boolean algebra*. A function $f{:}B^n \to B$ which is associated with a *Boolean expression* in *n* variables is called a ***Boolean function***. A *Boolean function* defined on a switching algebra is called a ***switching function***.

Example

- Which of f_1, f_2, and f_3 are *Boolean functions* ? (f_i: $B^2 \rightarrow B$, $i=1,2,3$)



<B, *, +, ', 0, 1>

where $B = \{ 0, 1, \alpha, \beta \}$

$f_1 = x_1'x_2 + x_1x_2'$

x_1, x_2	f_1	f_2	f_3
0, 0	0	1	0
0, α	α	β	β
0, β	β	α	β
0, 1	1	0	α
α, 0	α	β	0
α, α	0	β	1
α, β	1	0	α
α, 1	β	0	0
β, 0	β	β	α
β, α	1	0	0
β, β	0	α	β
β, 1	α	β	α
1, 0	1	0	β
1, α	β	α	α
1, β	α	β	β
1, 1	0	0	1

Exercise

1. Let $<B, \leq_1>$ be a *Boolean lattice* where $B=\{1,2,3,5,6,10,15,30\}$ and $\leq_1$ is defined to be "$x \leq_1 y$ if and only if x divides y".

   By *Stone Representation Theorem*, there exists a power set *Boolean lattice*, $<\wp(A), \leq_2>$, which is isomorphic to $<B, \leq_1>$.

   Answer each of the following:

   (a) Define set A.

   (b) Show that $f{:}B\rightarrow\wp(A)$ is a homomorphism from $<B, \leq_1>$ to $<\wp(\mathrm{A}), \leq_2>$.

Exercise (cont.)

2. Let <*B, +, *, ′, 0, 1*> be a *Boolean algebra*. Show that the complement x' of each element x in B is unique (All identity properties used in your proof should be proven except those given by the definition of Boolean algebra).