Sets, Logic and Boolean Algebra

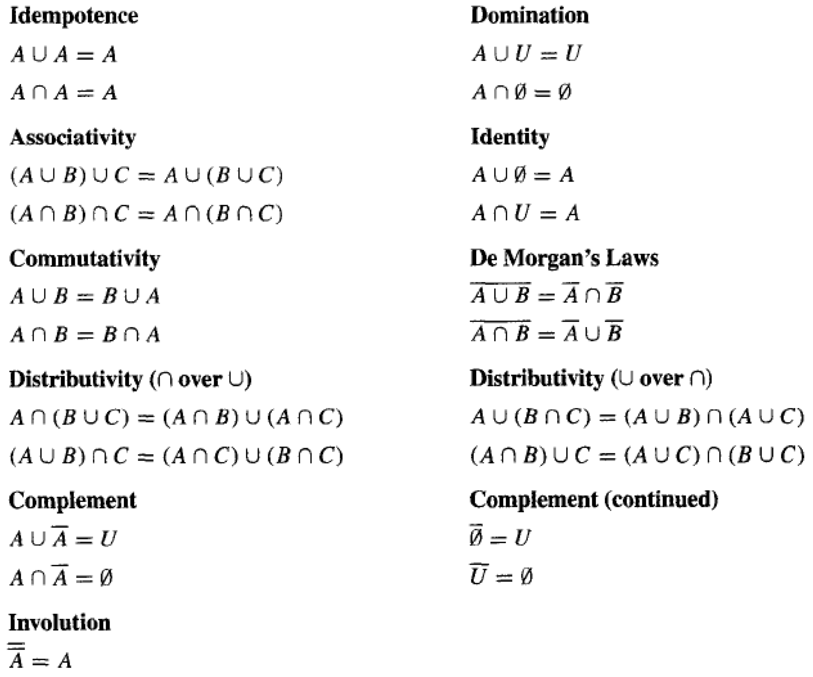
Xiaoyi Cui

This is just a brief summary of the contents of the three lectures. Please note: most of the calculations and demonstrations are neglected. Also, I will be brief about things which are well-explained in the textbook.

Set Theory

Definition 1
- *set, elements, universal set*
- *subset, proper subset, set equality*
- *cardinality, infinite set*
- *complement, intersection, union, difference*
- *covering, partition, Cartesian product*[1]*, power set*

Fundamental properties of sets:[2]



Idempotence

$A \cup A = A$

$A \cap A = A$

Associativity

$(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

Commutativity

$A \cup B = B \cup A$

$A \cap B = B \cap A$

Distributivity (∩ over ∪)

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Complement

$A \cup \overline{A} = U$

$A \cap \overline{A} = \emptyset$

Involution

$\overline{\overline{A}} = A$

Domination

$A \cup U = U$

$A \cap \emptyset = \emptyset$

Identity

$A \cup \emptyset = A$

$A \cap U = A$

De Morgan's Laws

$\overline{A \cup B} = \overline{A} \cap \overline{B}$

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

Distributivity (∪ over ∩)

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Complement (continued)

$\overline{\emptyset} = U$

$\overline{U} = \emptyset$

Figure 1: Fundamental properties of sets

Exercise 1 *Prove all the above statements.*

Exercise 2 *Work on the compatibility between Cartisian product and ∩, ∪ and* $\overline{()}$.

[1] Note that strictly speaking Cartesian product is not associative, due to the definition using ordered pairs; but in general you could assume the associativity using the canonical isomorphism.

[2] The notation for complement, $\overline{A}$ will be a bit confusing; alternatively we could use $\sim A$, or $\neg A$.

Propositional Logic

Definition 2 *A statement is an assertion that could be labeled true or false.*

Consider the set of statements S, as well as the set $\{\text{true} \equiv 1, \text{false} \equiv 0\}$, the valuation of the statement can be viewed as a map $S \to \{0, 1\}$.

The value is an incomplete description of the statements.

On the set of statements, we can have many operations. Operations are maps between (Cartesian product of) sets of statements. Examples are as follows.

Example 1 • *NOT* $\neg$*: "Roses are red."*$\mapsto$*"Roses are not red."*

- *AND* $\wedge$*: ("Roses are red.", "Violets are blue.")* $\mapsto$ *"Roses are red, and violets are blue."*
- *OR* $\vee$*: ("Roses are red.", "Violets are blue.")* $\mapsto$ *"Roses are red, or violets are blue."*

To understand the nature of those operations, we look into the truth table of those operations. Note that the tables are useful to distinguish different operations. I.e., if the trube tables are different, the corresponding operations are not equivalent.

Example 2 *The non-associativity* $A \wedge (B \vee C)$ *versus* $(A \wedge B) \vee C$.

Operations can act on operations to produce new ones. [3]

Example 3

Implication $\rightarrow$*: ("Roses are red.", "Violets are blue.")* $\mapsto$ *"If Roses are red, violets are blue."*

Biconditonal $\leftrightarrow$*: ("Roses are red.", "Violets are blue.")* $\mapsto$ *"Roses are red if and only violets are blue.".*

The truth table for operations imposes logical equivalence between two operations. Note: equivalence relation does not mean being identical — it is entirely possible to have two operations that give rise to different compound statements for the same input. Consider for example $(P \to Q) \wedge (Q \to P)$ vs $P \leftrightarrow Q$. We denote the logical equivalence by $\Leftrightarrow$.

Exercise 3 *Verify the following logic equivalences.*

- $P \to Q \Leftrightarrow \neg P \vee Q$,
- $P \leftrightarrow Q \Leftrightarrow \neg(P \vee Q) \vee (P \wedge Q)$.

Exercise 4 *Verify the following logic equivalences.*

- $[(P \to S_1) \wedge (S_1 \to S_2) \wedge \cdots \wedge (S_n \to Q)] \Rightarrow (P \to Q)$,
- $[(P \leftrightarrow S_1) \wedge (S_1 \leftrightarrow S_2) \wedge \cdots \wedge (S_n \leftrightarrow Q)] \Rightarrow (P \leftrightarrow Q)$.

[3] You should probably consider functions on the reals, which compose to make new functions.

There are operations whose every truth value is true, which we call tautologies. Likewise, there are operations whose every truth value is false, which we call contradictions.

Example 4
- $P \vee \neg P$
- $P \wedge \neg P$

Definition 3 *If for operations A, B, we have that $(A \rightarrow B) \Leftrightarrow \mathbf{T}$, we say that A infers B, and denote by $A \Rightarrow B$.*

Theorem 1 (The substitution principles)
- *Substituting an Equivalent Statement: If $A \Leftrightarrow B$, and A is a component of an operation, C, then B may be substituted for A without changing the T/F value of C.*
- *Replacing a Logic Variable in a Tautology: If B is a logic variable in a tautology, C, and A is any operation, then A may be substituted for every occurrence of B in C and C will still be a tautology.*
- *Using a Rule of Inference: If $A \Rightarrow B$, A evaluates to $\mathbf{T}$, and A is a component of a statement, C, then B may be substituted for A without changing the T/F value of C C.*

Example 5
- *Let $A = \neg(P \wedge Q)$ and let $B = [(\neg P) \vee (\neg Q)]$, let $C = [(\neg P) \vee (\neg Q)] \wedge R$. The first substitution principle asserts that $C \Leftrightarrow [[\neg(P \wedge Q)]] \wedge R$.*
- *Let $C = B \vee (\neg B)$. Let $A = P \vee Q$. Then replacing B with A leads to another tautology: $[P \vee Q] \vee [\neg(P \vee Q)]$.*
- *Let $A = [\neg P \wedge (P \vee Q)]$ and let $B = Q$. Let $C = Q \wedge [\neg P \wedge (P \vee Q)]$. Since $A \Rightarrow B$, the third substitution principle asserts that C can be replaced by $Q \wedge Q$ when $[\neg P \wedge (P \vee Q)]$ is known to be true. However, if A is false, the substitution is not necessarily valid.*

Exercise 5
- *Show that $[(R \vee P) \rightarrow (R \vee Q)] \leftrightarrow [R \vee (P \rightarrow Q)]$ is tautological.*
- *Show that $(P \rightarrow Q) \Leftrightarrow [(P \wedge \neg Q) \rightarrow \neg P]$.*

Exercise 6 *Write down and prove properties of the operations $\wedge$, $\vee$ and $\neg$, compare with the corresponding properties for $\cap$, $\cup$ and $\overline{()}$ in Figure 1.*

Remark 1 *If you like, m-nary operations can be visualized as trees — they takes m input, and produce one output. This point of view allows us to view statements also as 0-nary operations by generalizing the definition to the case with 0 input and 1 output*[4].

[4] There are even more freedom — any m-nary operations can be viewed as $m + k$-nary operations for positive k. Think about why.

Remark 2 *As the operations over the reals, there are precedences of operations. The brackets have the highest precedence. For m-nary operations, the smaller m is, the higher the precedence is. For binary operations we have introduced, $\rightarrow$ has the lowest precedence, since it can be viewed as a composite operation.*

Boolean algebra

Definition 4 *A Boolean algebra is a set B together with binary operations $+$ and $\cdot$ together with an unary operation $\neg$, such that the following axioms hold:*

- *identity: there exists two distinguished elements 0 and 1, such that $x + 0 = x$ and $x \cdot 1 = x$, for all $x \in B$.*
- *complement: $x + \neg x = 1$ and $x \cdot \neg x = 0$.*
- *commutativity: $\forall x, y \in B$, $x + y = y + x$, $x \cdot y = y \cdot x$.*
- *distributivity: $\forall x, y, z \in B$, $x + (y \cdot z) = (x + y) \cdot (x + z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$.*

Definition 5 *A boolean expression on a Boolean algebra $(B, +, \cdot, \neg)$ is an algebraic experession that is composed using elements from B, those operations, and variables whose possible values are in B.*[5]

Example 6

- $(\mathcal{S}, \cup, \cap, \sim)$.
- $(Propositions, \vee, \wedge, \neg)$.

Theorem 2 (Stone's representation theorem, finite case) *Every finite Boolean algebra A is isomorphic to the Boolean algebra $(\mathcal{P}(S), \cup, \cap, \overline{()})$ for some finite set S.*

Example 7 *Show that the Boolean algebra $(\{0, 1\}, +, \cdot, \neg)$ is isomorphic to $(\mathcal{P}(S), \cup, \cap, \sim)$ for some finite set S.*

The Boolean algebra in the propositional calculus is the minimum, nontrivial one.

Proposition 1 *Let x and y be elements of a Boolean algebra. Then*

- $x \cdot y = x \Leftrightarrow x \cdot \neg y = 0$,
- $x = y \Leftrightarrow x \cdot \neg y + y \cdot \neg x = 0$.

Hint on the $\Leftarrow$ direction of the second statement: in Boolean algebra, $x + x = \neg(\neg x \cdot \neg x) = \neg(\neg x \cdot (x + \neg x)) = \neg\neg x = x$, so we have that $x \cdot \neg y + x \cdot \neg y + \neg x \cdot y = x \cdot \neg y + \neg x \cdot y = (x \cdot \neg y + \neg x \cdot y) + \neg x \cdot y$.

The duality principle for Boolean algebras holds: Let T be a theorem that is valid over a Boolean algebra. Then if all Os and 1s are exchanged (with a suitable change in parentheses), and if all $+$ and $\cdot$ are exchanged, the result is also a theorem that is valid over the Boolean algebra.

[5] Compare the notion in p261 of the textbook.

Exercise 7 *Show that a general Boolean algebra satisfies the same properties as in Figure 1 from its axiomatic definition.*

Predicate Logic

Propositional logic is not capable to deal with statements with multiple objects. So we need a more powerful way. Predicate Logic = predicates + set of objects.

Definition 6 *Let S be the set of objects. A predicate P with n variables is a map*

$$P : S^{\times n} \to \{Propositions\} : (s_1, \cdots, s_n) \mapsto P(s_1, \cdots, s_n).$$

Sometimes operations over the statements can be transferred to quantifiers.

Let $P_2(x, y)$ be a predicate with two variables, if we only specify the variable x to the object a, then $P_2(a, y)$ needs not to be a proposition. This is because, with the free variable y, it might not be possible to determine the T/F value. On the other hand, if you agree that a proposition is a special kind of predicate, then we can always say that $P_2(a, y)$ is a predicate.

Example 8

- $P(x_1) \vee \cdots \vee P(x_n) \Leftrightarrow (\exists x \in \{x_1, \cdots, x_n\})P(x);$
- $P(x_1) \wedge \cdots \wedge P(x_n) \Leftrightarrow (\forall x \in \{x_1, \cdots, x_n\})P(x)$

From the above example, we can see that $\exists$ has the property inherited from $\vee$ while $\forall$ from $\wedge$ in the finite case. Then it is immediate that under negation, those two interchanges. For example, $\neg((\exists x)P(x) \wedge Q(x)) \Leftrightarrow (\forall x)\neg P(x) \vee \neg Q(x)$.

Besides, the operations for propositional calculus applies here as well. The only new thing, is the domain of the quantifier $\exists$ and $\forall$.

Consider $(\forall x)(P_2(x, y))$, y is called free variable. Since we assigned a quantifier for x, it is thus a bounded variable as opposed to a free one. Similar to the previous case, this needs not to be a proposition.

Exercise 8 *Which of the following is true?*

- $(\exists x)((\forall y)P(x, y)) \Rightarrow (\forall y)((\exists x)P(x, y));$
- $(\forall x)((\exists y)P(x, y)) \Rightarrow (\exists y)((\forall x)P(x, y)).$

More Examples and Applications

Islands and Inhabitants

An island has two kinds of inhabitants, knights, who always tell the truth, and their opposites, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types?"

Let p and q be the statements that A is a knight and B is a knight, respectively, so that $\neg p$ and $\neg q$ are the statements that A is a knave and B is a knave, respectively.

If A is a knight; this is the statement that p is true. Then he is telling the truth when he says that B is a knight, so that q is true.

And if p is false, so is q. So we have that $(p \wedge q) \vee (\neg p \wedge \neg q) \Leftrightarrow \mathbb{T}$, which is $p \Leftrightarrow q$. If q is true, B is a knight, then B's statement that A and B are of opposite types, the statement $(p \wedge \neg q) \vee (\neg p \wedge q)$, would have to be true. On the other hand, if q is false, then the statement $(p \wedge \neg q) \vee (\neg p \wedge q)$ would have to be false. So we have that $q \Leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$. Replace, in the rhs, whereever p by q, we have that $q \Leftrightarrow (q \wedge \neg q) \vee (\neg q \wedge q) \Leftrightarrow \mathbb{F}$. So we conclude that both A and B are knaves.

Logic circuit

This is a realization of the "tree" structure in a concrete form, if you look from the left. There are three types of nodes that are frequently used, see pp 48, Figure 1-9.1, top row.

Exercise 9 • *Read Sec. 1-9 (pp 47 - 52) in the textbook.*

- *Describe the approach to build a logic circuit for voting system, assume that the total voting number is odd.*

Sudoku puzzle

To encode a Sudoku puzzle, let $p(i, j, n)$ denote the proposition that is true when the number n is in the cell in the i-th row and j-th column. There are $9^3 = 729$ such propositions, for $i, j, k \in \{1, 2, \cdots, 9\}$. How to show the assertion that every row contains every number?

The assertion reads, for each number n and each i-th row, there exists a column j such that the number on the i, j cell is n. In turn, this means $(\forall n)(\forall i)(\exists j)P(i, j, n)$.