Introduction to Discrete Mathematics

from 93APM3 Applied Mathematics 3

AY25/26 Sem 2

This set of notes is based on the lectures as delivered in AY25/26 by Dr Li Zhongqiang, with reference to *Discrete Mathematics and Its Applications* (Rosen, 2019).

Contents

Sets

1.1 Basic Set Notation

notation	definition
$\in$	is an element of.
$\notin$	is not an element of.
$A = \{x_1, x_2, ...\}$	list of elements of A.
$A = \{x : x \in \mathbb{R}\}$	rule by which elements of A are determined.
$A \subset B$	A is a subset of B.
$A \subseteq B$	A is a proper subset of B. $A \subset B$, $A \neq B$.
U	Universal set of all elements of interest.
$\emptyset$	The empty set.
$\overline{A}$ or $A^{\complement}$	$\overline{A} = \{x, x \in U, x \notin A\}$.
$A \cup B$	set of **all** the elements of A and B.
$A \cap B$	set of the **common** elements of A and B.

A disjointed set is the set of A and B such that

$$A \cap B = \emptyset.$$

1.2 Algebra of Sets

Commutative law: $A \cup B \equiv B \cup A$, $A \cap B \equiv B \cap A$
Idempotent law: $A \cup A = A$, $A \cap A = A$
Identity law: $A \cup \emptyset = A$, $A \cap U = A$
Complementary law: $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$
Associative law: $A \cup (B \cup C) = (A \cup B) \cup C$
Distributive law: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
De Morgen laws: $\overline{A \cup B} = \overline{A} \cap \overline{B}, \overline{A \cap B} = \overline{A} \cup \overline{B}$

Logic and Proofs

2.1 Propositional Logic

Definition 2.1.1. The proposition p is a statement which declares a fact, and which is immediately discernible as either true or false.

Remarks. Compound propositions can be created through the application of logical operators on a proposition.

Definition 2.1.2. The *negation* of p, $\tilde{p}$ is the statement "it is not the case that p".

Remarks. $\tilde{p}$ can also be written $\overline{p}$ or $\neg p$

Definition 2.1.3. The *conjunction* of p and q, $p \wedge q$ is the statement "p and q".

Definition 2.1.4. The *disjunction* of p and q, $p \lor q$ is the statement "p or q".

Definition 2.1.5. The *exclusive or* of p and q, $p \oplus q$ is the statement which is true when, and only when, either p or q is true, but not both.

Definition 2.1.6. The *implication* $p \Rightarrow q$ is the statement "p *implies* q".

Remarks. The statement $p \to r$ is the *hypothesis*. q is the conclusion. Remember that just because q is true, this does **not** mean that p is true. This relation is not reversible.

Definition 2.1.7. The *converse* of the statement $p \Rightarrow q$ is the statement $q \Rightarrow q$.

Definition 2.1.8. The *contrapositive* of $p \Rightarrow q$ is $\neg p \Rightarrow \neg q$.

Definition 2.1.9. The *bi-conditional* statement $p \iff q$ is the proposition "p if and only if q".

Remarks. The bi-conditional is the compound proposition of $p \Rightarrow q$ and $q \Rightarrow p$. A true result is returned only when both p and q have the same truth table values, and is false otherwise. It has the same truth table values as $(p \Rightarrow q) \land (q \Rightarrow q)$.

2.2 Propositional Equivalences

Definition 2.2.1. The *contradiction* is a statement which is always false.

Remarks. For example, the statement $s \equiv p \land \tilde{p}$ is always false. It is thus a contradiction.

Definition 2.2.2. The *tautology* is a statement which is always true.

Remarks. For example, the statement $t \equiv p \lor \tilde{p}$ is always true. It is thus a tautology.

Definition 2.2.3. The compound propositions p and q are called *logically equivalent* if $p \iff q$ is a tautology (always true). This is also denoted with $p \equiv q$.

The table below illustrates a number of such logical equivalences.

name	equivalence
identity laws	$p \wedge t \equiv p$
	$p \vee s \equiv p$
domination laws	$p \vee t \equiv t$
	$p \wedge s \equiv s$
idempotent laws	$p \vee p \equiv p$
	$p \wedge p \equiv p$
double negation law	$\neg(\tilde{p}) \equiv p$
associative law	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
distributive law	$p \vee (p \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
	$p \wedge (p \vee r) \equiv (p \wedge q) \vee (p \wedge q)$
De Morgen's laws	$\overline{(p \vee q)} \equiv \tilde{p} \wedge \tilde{q}$
	$\overline{(p \wedge q)} \equiv \tilde{p} \vee \tilde{q}$
absorption laws	$p \wedge (p \vee q) \equiv p$
	$p \vee (p \wedge q) \equiv p$
complementary(negation) law	$p \vee \tilde{p} \equiv t$
	$p \wedge \tilde{p} \equiv s$

2.3   Predicates and Quantifiers

Definition 2.3.1. The *Propositional Function* $P(x)$ refers to a statement which becomes a proposition when a value is assigned to its *variable(s) $a, b, ...z$*. The *predicate* is the condition to be fulfilled.

Exercise. Take $x > 3$. This propositional function only becomes a proposition when we give x a value, such that we can determine the function's truth table.

2.4   Proofs, Methods for Proofs

2.4.1   Terminology

word	definition
theorem	a statement that can be shown to be true (also: facts, results).
proposition	a less important theorem.
proof	demonstration that a theorem is true.
axioms	statements we assume to be true (also: postulates).
lemma	a less important theorem useful in the proof of other results.
corollary	theorem that can be directly established from a theorem that has been proved.
conjecture	a statement which is proposed to be a true statement.

2.5 Methods of Proof

2.5.1 Direct Proof

The *direct proof* of the proposition $p \to q$ is one which begins with the assumption that p is true, before the usage of a series of axioms, definitions, and proved theories, to show that q is also true. Direct proofs are the most straightforward of the proofs.

Definition 2.5.1. An integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$. Two integers are said to have the same *parity* when both are even or both are odd; they have the opposite parity when one is even and the other is odd.

Exercise. If n is odd, prove that n^2 is odd.

$$n = 2k + 1, \, k \in \mathbb{Z} \tag{1}$$
$$n^2 = (2k + 1)^2 \tag{2}$$
$$= 2\left(2k^2 + 2k\right) + 1] \tag{3}$$

therefore, by definition, n^2 is odd.

2.5.2 Indirect Proof

An *indirect proof* is one which does not start with the premise and end with the conclusion.

Proof by contraposition: We utilise the fact that the implication $p \to q$ is equivalent to its contrapositive $\tilde{p} \to \tilde{q}$. Taking $\tilde{p}$ as the premise, we use axioms, definitions and proven theorems to show that $\tilde{q}$ must follow. This indirectly proves that $p \implies q$.

Vacuous proof: Given that p is false, then it follows that $p \to q$ must be true. Therefore, if we can prove that p is false, we can then establish the *vacuous proof.*

Trivial proof: Given that q is true, then it follows that $p \implies q$ is also true. Such a proof is known as the *trivial proof.*

2.5.3 Proof by Contradiction

A type of indirect proof. We prove the statement p is true when we prove that $\tilde{p} \to (r \wedge \tilde{r})$, or $\tilde{p} \to$ false.

Exercise. Prove $\sqrt{2}$ is irrational.

If $\sqrt{2}$ is rational, then

$$\sqrt{2} = \frac{m}{n}. \tag{4}$$

where m, n have no common factors. Squaring both sides, we get

$$2n^2 = m^2, \tag{5}$$

which implies
$$m = 2k.$$

Thus,
$$m^2 = 4k^2 \tag{6}$$

However, from 5,
$$n^2 = \frac{1}{2}m^2 = 2k^2 \rightarrow n^2 \text{ is odd.}$$

Since both m and n are odd, they therefore have a common factor of 2. We have proven that $\sqrt{2}$ is irrational by contradiction.

2.5.4   Proof by Induction

Suppose we have the statements $p_1, p_2 p_3, ..., p_n, n \in \mathbb{N}$. If we prove that p_1 is true (the basis for induction), then we assume p_k is true. This is the induction hypothesis. We then show that $p_{k+!}$ is true, which proves that p_n is true by induction.