

# Logic, Sets, Number Theory, and Counting

Walker Smith

November 23, 2012

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Propositional Logic</b>	<b>5</b>
2.1	Proposition . . . . .	5
2.2	Negation of $p$ . . . . .	5
2.3	Conjunction of $p$ and $q$ . . . . .	5
2.4	Disjunction of $p$ and $q$ . . . . .	5
2.5	Exclusive or of $p$ and $q$ . . . . .	5
2.6	Conditional statement . . . . .	5
2.7	Biconditional statement . . . . .	6
2.8	Logical Equivalence . . . . .	6
2.9	Propositional Function . . . . .	6
2.10	Propositional Multivariable Function . . . . .	6
2.11	Universal Quantification . . . . .	6
2.12	Existential Quantification . . . . .	6
2.13	Quantification Equivalences . . . . .	7
2.14	Quantification of Two Variables . . . . .	7
<b>3</b>	<b>Laws of Logical Equivalence</b>	<b>8</b>
3.1	De Morgan's Laws . . . . .	8
3.2	Identity Laws . . . . .	8
3.3	Domination Laws . . . . .	8
3.4	Idempotent Laws . . . . .	8
3.5	Double Negation . . . . .	8
3.6	Commutative Laws . . . . .	8
3.7	Associative Laws . . . . .	9
3.8	Distributive Laws . . . . .	9
3.9	Absorption Laws . . . . .	9
3.10	Absorption Laws . . . . .	9
<b>4</b>	<b>Sets</b>	<b>10</b>
4.1	Set . . . . .	10
4.2	Set Membership . . . . .	10
4.3	Set Membership . . . . .	10
4.4	Roster Notation . . . . .	10
4.5	Set Builder Notation . . . . .	10

4.6	Null Set . . . . .	10
4.7	Singleton Set . . . . .	11
4.8	Subset . . . . .	11
4.9	Proper Subset . . . . .	11
4.10	Set Equality . . . . .	11
4.11	Cardinality . . . . .	11
4.12	Power Set . . . . .	11
<b>5</b>	<b>Number Theory and Cryptography</b>	<b>12</b>
5.1	Coprime . . . . .	12
5.2	Euler's Theorem . . . . .	12

# 1 Introduction

L<sup>A</sup>T<sub>E</sub>X is a document preparation system for the T<sub>E</sub>X typesetting program.

## 2 Propositional Logic

### 2.1 Proposition

A proposition is a declarative sentence that is either true or false.

$$p \tag{1}$$

### 2.2 Negation of p

The negation of p has the opposite truth value of p.

$$\neg p \tag{2}$$

### 2.3 Conjunction of p and q

The conjunction of p and q is true when both p and q are true and false otherwise.

$$p \wedge q \tag{3}$$

### 2.4 Disjunction of p and q

The disjunction of p and q is false when both p and q are false and true otherwise.

$$p \vee q \tag{4}$$

### 2.5 Exclusive or of p and q

The exclusive or of p and q is true when exactly one of p and q are true and false otherwise.

$$p \oplus q \tag{5}$$

### 2.6 Conditional statement

The conditional statement if p then q is false when p is true and q is false and true otherwise.

$$p \rightarrow q \tag{6}$$

## 2.7 Biconditional statement

The biconditional statement  $p$  if and only if  $q$  is true when  $p$  and  $q$  have the same truth value and false otherwise.

$$p \leftrightarrow q \quad (7)$$

## 2.8 Logical Equivalence

compound propositions  $p$  and  $q$  are logically equivalent if  $p$  if and only if  $q$  is a tautology, that is the compound proposition is true no matter the truth values of the propositional variables.

$$p \equiv q \quad (8)$$

## 2.9 Propositional Function

Value of a propositional function  $P$  at  $x$ . Function defined by it's predicate,  $P$  and subject,  $x$  where  $x$  is the subject of the statement and  $P$  refers to a property that the subject has.

$$P(x) \quad (9)$$

## 2.10 Propositional Multivariable Function

Value of a propositional function  $P$  at the  $n$ -tuple  $(x_1, x_2, \dots, x_n)$ .

$$P(x_1, x_2, \dots, x_n) \quad (10)$$

## 2.11 Universal Quantification

Universal quantification of  $P(x)$  is true when  $P(x)$  is true for every  $x$  and false when there is an  $x$  for which  $P(x)$  is false.

$$\forall x P(x) \quad (11)$$

## 2.12 Existential Quantification

Existential quantification of  $P(x)$  is true when there exists an element  $x$  in the domain such that  $P(x)$  and false when  $P(x)$  is false for every  $x$ .

$$\exists x P(x) \quad (12)$$

## 2.13 Quantifaction Equivalences

Statement is true when there is an  $x$  for which  $P(x)$  is false and false when  $P(x)$  is true for every  $x$ .

$$\neg\forall xP(x) \equiv \exists x\neg P(x) \quad (13a)$$

Statement is true when for every  $x$   $P(x)$  is true and false when there is an  $x$  for which  $P(x)$  is true.

$$\neg\exists xP(x) \equiv \forall x\neg P(x) \quad (13b)$$

## 2.14 Quantification of Two Variables

$P(x,y)$  is true for every pair  $x,y$  and false when there is a pair  $x,y$  for which  $P(x,y)$  is false.

$$\forall x\forall yP(x,y) \quad (14a)$$

$$\forall y\forall xP(x,y) \quad (14b)$$

For every  $x$  there is a  $y$  for which  $P(x,y)$  is true. There is an  $x$  such that  $P(x,y)$  is false for every  $y$ .

$$\forall x\exists yP(x,y) \quad (14c)$$

There is an  $x$  for which  $P(x,y)$  is true for every  $y$ . For every  $x$  there is a  $y$  for which  $P(x,y)$  is false.

$$\exists x\forall yP(x,y) \quad (14d)$$

There is a pair  $x,y$  for which  $P(x,y)$  is true.  $P(x,y)$  is false for every pair  $x,y$ .

$$\exists x\exists yP(x,y) \quad (14e)$$

$$\exists y\exists xP(x,y) \quad (14f)$$

### 3 Laws of Logical Equivalence

#### 3.1 De Morgan's Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad (1a)$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad (1b)$$

#### 3.2 Identity Laws

$$p \wedge T \equiv p \quad (2a)$$

$$p \vee F \equiv p \quad (2b)$$

#### 3.3 Domination Laws

$$p \vee T \equiv T \quad (3a)$$

$$p \wedge F \equiv F \quad (3b)$$

#### 3.4 Idempotent Laws

$$p \vee p \equiv p \quad (4a)$$

$$p \wedge p \equiv p \quad (4b)$$

#### 3.5 Double Negation

$$\neg(\neg p) \equiv p \quad (5)$$

#### 3.6 Communative Laws

$$p \vee q \equiv q \vee p \quad (6a)$$

$$p \wedge q \equiv q \wedge p \quad (6b)$$



### 3.7 Associative Laws

$$(p \vee q) \vee r \equiv p \vee (q \vee r) \quad (7a)$$

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \quad (7b)$$

### 3.8 Distributive Laws

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \quad (8a)$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad (8b)$$

### 3.9 Absorption Laws

$$p \vee (p \wedge q) \equiv p \quad (9a)$$

$$p \wedge (p \vee q) \equiv p \quad (9b)$$

### 3.10 Absorption Laws

$$p \vee \neg p \equiv T \quad (10a)$$

$$p \wedge \neg p \equiv F \quad (10b)$$

## 4 Sets

### 4.1 Set

A set is an unordered collection of elements where elements are referred to as members of the set.

$$S \tag{1}$$

### 4.2 Set Membership

s is a member of the set S.

$$s \in S \tag{2}$$

### 4.3 Set Membership

s is not a member of the set S.

$$s \notin S \tag{3}$$

### 4.4 Roster Notation

Roster notation describes a set by listing the set's elements

$$S = \{s_1, \dots, s_n\} \tag{4}$$

### 4.5 Set Builder Notation

Set builder notation determines membership of an element s in a set S based on a property or properties, P(s)

$$S = \{s | P(s)\} \tag{5}$$

### 4.6 Null Set

The null set,  $\emptyset$ , contains no elements

$$\{\} \tag{6}$$

## 4.7 Singleton Set

The singleton set contains exactly one element, the null set

$$\{\emptyset\} \quad (7)$$

## 4.8 Subset

The set A is a subset of set B, denoted  $A \subseteq B$ , is true if all members of A are also members of B and false if there is a single  $a \in A$  such that  $a \notin B$

$$\forall x(x \in A \rightarrow x \in B) \quad (8)$$

## 4.9 Proper Subset

The set A is a proper subset of a set B, denoted  $A \subset B$ , is true if A is a subset of B and there exists an x of B that is not an element of A

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A) \quad (9)$$

## 4.10 Set Equality

Two sets are equal, denoted  $A = B$ , if and only if they have the same elements

$$\forall x(x \in A \leftrightarrow x \in B) \quad (10)$$

## 4.11 Cardinality

The set A with n distinct elements, where n is a non negative integer, has a cardinality or size of n.

$$|A| \quad (11)$$

## 4.12 Power Set

Given a set A, the power set of A is the set of all subsets of the set A

$$\mathcal{P}(S) \quad (12)$$

## 5 Number Theory and Cryptography

### 5.1 Coprime

Integers  $m$  and  $n$  are relatively prime if

$$\gcd(m, n) = 1 \tag{1}$$

### 5.2 Euler's Theorem

If  $n$  and  $m$  are relatively prime for some  $m, n \in \mathbb{Z}^+$

$$n^{\Phi(m)} \equiv 1 \pmod{m} \tag{2a}$$

$$n^{\Phi(m)} - 1 \equiv 0 \pmod{m} \tag{2b}$$