Logic, Sets, Number Theory, and Counting

Walker Smith

November 24, 2012

Contents

1 Introduction **4**

2 Propositional Logic **5**
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 Converse 6
2.8 Contrapositive 6
2.9 Inverse 6
2.10 Biconditional statement 6
2.11 Logical Equivalence 6
2.12 Propositional Function 6
2.13 Propositional Multivariable Function 7
2.14 Universal Quantification 7
2.15 Existential Quanification 7
2.16 Quantifaction Equivalences 7
2.17 Quantification of Two Variables 7

3 Laws of Logical Equivalence **9**
3.1 De Morgan's Laws 9
3.2 Identity Laws 9
3.3 Domination Laws 9
3.4 Idempotent Laws 9
3.5 Double Negation 9
3.6 Communative Laws 9
3.7 Associative Laws 10
3.8 Distributive Laws 10
3.9 Absorption Laws 10
3.10 Absorption Laws 10

4 Sets **11**
4.1 Set 11
4.2 Set Membership 11

4.3 Set Membership . . . 11
4.4 Roster Notation . . . 11
4.5 Set Builder Notation . . . 11
4.6 Null Set . . . 11
4.7 Singleton Set . . . 12
4.8 Subset . . . 12
4.9 Proper Subset . . . 12
4.10 Set Equality . . . 12
4.11 Cardinality . . . 12
4.12 Power Set . . . 12
4.13 Ordered n-tuples . . . 13
4.14 Ordered n-tuples Equality . . . 13
4.15 Ordered n-tuples Equality . . . 13
4.16 Union . . . 13
4.17 Intersect . . . 13
4.18 Disjoint Sets . . . 14
4.19 Difference . . . 14

5 Relations **15**
5.1 Reflexive . . . 15
5.2 Symmetric . . . 15
5.3 Anti-Symmetric . . . 15
5.4 Transative . . . 15

6 Number Theory and Cryptography **16**
6.1 Coprime . . . 16
6.2 Euler's Theorm . . . 16

7 Graph Theory **17**

1 Introduction

LaTeX is a document preparation system for the TeX typesetting program.

2 Propositional Logic

2.1 Proposition

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

$$\mathrm{p} \tag{1}$$

2.2 Negation of p

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

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

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.

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

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.

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

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.

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

2.6 Conditional statement

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

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

2.7 Converse

The converse of p $\rightarrow$ q is the conditional statement

$$\mathrm{q} \rightarrow \mathrm{p} \tag{7}$$

2.8 Contrapositive

The contrapositive of p $\rightarrow$ q is the conditional statement

$$\neg \mathrm{q} \rightarrow \neg \mathrm{p} \tag{8}$$

2.9 Inverse

The inverse of p $\rightarrow$ q is the conditional statement

$$\neg \mathrm{p} \rightarrow \neg \mathrm{q} \tag{9}$$

2.10 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.

$$\mathrm{p} \leftrightarrow \mathrm{q} \tag{10}$$

2.11 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.

$$\mathrm{p} \equiv \mathrm{q} \tag{11}$$

2.12 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.

$$P(x) \tag{12}$$

2.13 Propositional Multivariable Function

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

$$P(x_1, x_2, \ldots, x_n) \tag{13}$$

2.14 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.

$$\forall x P(x) \tag{14}$$

2.15 Existential Quanification

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.

$$\exists x P(x) \tag{15}$$

2.16 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.

$$\neg \forall x P(x) \equiv \exists x \neg P(x) \tag{16a}$$

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

$$\neg \exists x P(x) \equiv \forall x \neg P(x) \tag{16b}$$

2.17 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.

$$\forall x \forall y P(x, y) \tag{17a}$$
$$\forall y \forall x P(x, y) \tag{17b}$$

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.

$$\forall x \exists y P(x, y) \tag{17c}$$

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.

$$\exists x \forall y P(x, y) \tag{17d}$$

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

$$\exists x \exists y P(x, y) \tag{17e}$$

$$\exists y \exists x P(x, y) \tag{17f}$$

3 Laws of Logical Equivalence

3.1 De Morgan's Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \tag{1a}$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q \tag{1b}$$

3.2 Identity Laws

$$p \wedge T \equiv p \tag{2a}$$
$$p \vee F \equiv p \tag{2b}$$

3.3 Domination Laws

$$p \vee T \equiv T \tag{3a}$$
$$p \wedge F \equiv F \tag{3b}$$

3.4 Idempotent Laws

$$p \vee p \equiv p \tag{4a}$$
$$p \wedge p \equiv p \tag{4b}$$

3.5 Double Negation

$$\neg(\neg p) \equiv p \tag{5}$$

3.6 Communative Laws

$$p \vee q \equiv q \vee p \tag{6a}$$
$$p \wedge p \equiv q \wedge p \tag{6b}$$

3.7 Associative Laws

$$(p \vee q) \vee r \equiv p \vee (q \vee r) \tag{7a}$$

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \tag{7b}$$

3.8 Distributive Laws

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \tag{8a}$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \tag{8b}$$

3.9 Absorption Laws

$$p \vee (p \wedge q) \equiv p \tag{9a}$$

$$p \wedge (p \vee q) \equiv p \tag{9b}$$

3.10 Absorption Laws

$$p \vee \neg p \equiv T \tag{10a}$$

$$p \wedge \neg p \equiv F \tag{10b}$$

4 Sets

4.1 Set

A set is an unordered collection of elements where elements are refered 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 desribes a set by listing the set's elements

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

4.5 Set Builder Notation

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

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

4.6 Null Set

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

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

4.7 Singleton Set

The singleton set contains exaclty one element, the null set

$$\{\emptyset\} \tag{7}$$

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 $x \notin B$

$$\forall x(x \in A \rightarrow x \in B) \tag{8}$$

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

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A) \tag{9}$$

4.10 Set Equality

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

$$\forall x(x \in A \leftrightarrow x \in B) \tag{10}$$

4.11 Cardinality

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

$$|A| \tag{11}$$

4.12 Power Set

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

$$\mathcal{P}\left(S\right) \tag{12}$$

4.13 Ordered n-tuples

An ordered collection $(a_1, a_2, \ldots, a_n)$ has a_1 as its first element, a_2 as its second element, ..., and a_n as its last element.

$$(a_1, a_2, \ldots, a_n) \tag{13}$$

4.14 Ordered n-tuples Equality

Two ordered n-tuples, $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if and only if $a_i = b_i$ for $i = 1, 2, \ldots, n$

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \tag{14}$$

4.15 Ordered n-tuples Equality

The cartesian product is the set of all ordered pairs (a,b), where a ∈ A and b ∈ B

$$A \times B = \{(a, b) \mid \mathrm{a} \in \mathrm{A} \wedge \mathrm{b} \in \mathrm{B}\} \tag{15}$$

4.16 Union

The of union of set A and B , denoted is the set containing members of the set A or B

$$\mathrm{A} \cup \mathrm{B} = \{s \mid \mathrm{s} \in \mathrm{A} \vee \mathrm{s} \in \mathrm{B}\} \tag{16}$$

4.17 Intersect

The of intersect of set A and B is the set containing members of sets A and B

$$\mathrm{A} \cap \mathrm{B} = \{s \mid \mathrm{s} \in \mathrm{A} \wedge \mathrm{s} \in \mathrm{B}\} \tag{17}$$

4.18 Disjoint Sets

Two sets are disjoint if their intersect is the set containing no elements

$$\mathrm{A} \cap \mathrm{B} = \emptyset \tag{18}$$

4.19 Difference

The of difference of set A and B is the set containing members of sets A that are members of B

$$\mathrm{A} - \mathrm{B} = \{s \in A \mid \mathrm{s} \notin \mathrm{B}\} \tag{19}$$

5 Relations

5.1 Reflexive

The relation R on a set A is reflexive if a ordered pair (a,a) ∈ R for every a ∈ A

$$\forall a \in A((a,a) \in R) \tag{1}$$

5.2 Symmetric

The relation R on a set A is symmetric if the ordered pairs (a,b) ∈ R then (b,a) ∈ R

$$\forall a \forall b \, ((a,b) \in R \to (b,a) \in R) \tag{2}$$

5.3 Anti-Symmetric

The relation R on a set A is antisymmetric if the ordered pairs (a,b) ∈ R and (b,a) ∈ R then a = b

$$\forall a \forall b \, (((a,b) \in R \wedge (b,a) \in R \to (a = b)) \tag{3}$$

5.4 Transative

The relation R on a set A is transative if the ordered pairs (a,b) ∈ R and (b,c) ∈ R then (a,c) ∈ R

$$\forall a \forall b \forall c \, (((a,b) \in R \wedge (b,c) \in R \to (a,c) \in R) \tag{4}$$

6 Number Theory and Cryptography

6.1 Coprime

Integers m and n are relatively prime if

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

6.2 Euler's Theorm

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

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

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

7 Graph Theory