Discrete Mathematics

Max Kasperowski

December 15, 2017

Contents

1 Logic

1.1 Propositional Logic—Zeroth Order Logic

In propositional logic, propositions are denoted by letters (p, q) and are formed by connecting other propositions using logical connectives. Propositions can either be true (T) or false (F).

Logical Connectives The logical connectives listed below are the basic connectives available in propositional logic in order of their precedence. Below are the truthtables corresponding to each of the connectives.

1. $\neg$, not
2. $\wedge$, and, $\bigwedge_{i=1}^{n} p_i$
3. $\vee$, or, $\bigvee_{i=1}^{n} p_i$
4. $\rightarrow$, $\Rightarrow$, implies (only if) defined as: $p \rightarrow q \equiv \neg p \vee q$
5. $\leftrightarrow$, $\Leftrightarrow$, is equivalent to (if and only if, iff) defined as: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Negation

p	¬ p	
T	F	T
F	T	F

Logical Or

p	q	p	∨	q
T	T	T	T	T
T	F	T	T	F
F	T	F	T	T
F	F	F	F	F

Equivalence

p	q	p	↔	q
T	T	T	T	T
T	F	T	F	F
F	T	F	F	T
F	F	F	T	F

Logical And

p	q	p	∧	q
T	T	T	T	T
T	F	T	F	F
F	T	F	F	T
F	F	F	F	F

Implication

p	q	p	→	q
T	T	T	T	T
T	F	T	F	F
F	T	F	T	T
F	F	F	T	F

1.1.1 Definitions

Converse, Contrapositive, Inverse When given the proposition $p \rightarrow q$, $q \rightarrow p$ is its converse, $\neg q \rightarrow \neg p$ is its contrapositive and $\neg p \rightarrow \neg q$ is its inverse. The contrapositive is equivalent to the original proposition and the converse and inverse are also equivalent.

Tautology A proposition that is always true ($p \vee \neg p$).

Contradiction A proposition that is always false ($p \wedge \neg p$).

Contingency A proposition that is neither a tautology nor a contradiction.

Logical Equivalence p and q are logically equivalent if $p \leftrightarrow q$ is a tautology. The notation for equivalence is typically $\equiv$.

1.1.2 Properties

De Morgan's Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

Identity Laws

$$p \wedge T \equiv p$$
$$p \vee F \equiv p$$

Domination Laws

$$p \wedge F \equiv F$$
$$p \vee T \equiv T$$

Idempotent Laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Negation Laws

$$p \wedge \neg p \equiv F$$
$$p \vee \neg p \equiv T$$

Commutative Laws

$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$

Associative Laws

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$

Distributive Laws

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

Absorption Laws

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

1.1.3 Equivalence Proof

This is an example of how to perform an equivalence proof. The aim is to show that $\neg(p \vee (\neg p \wedge q))$ is logically equivalent to $\neg p \wedge \neg q$. We can prove this by forming a series of logical equivalences.

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{2}^{\text{nd}} \text{ De Morgan's law} \\
\neg p \wedge \neg(\neg p \wedge q) &\equiv \neg p \wedge (p \vee \neg q) && \text{1}^{\text{st}} \text{ De Morgan's law} \\
\neg p \wedge (p \vee \neg q) &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{Associative law} \\
(\neg p \wedge p) \vee (\neg p \wedge \neg q) &\equiv F \vee (\neg p \wedge \neg q) && \text{Negation law} \\
F \vee (\neg p \wedge \neg q) &\equiv \neg p \wedge \neg q && \text{Identity law}
\end{aligned}$$

1.2 Predicate Logic —First Order Logic

Predicate logic uses quantified variables over non-logical objects and allows the use of sentences that contain variables. This allows a generalisation of propositions for a set of variables from a domain.

1.2.1 Definitions

Predicates A predicate is a generalisation of propositions when the variable x is replaced by a specific element from its domain. $P(x)$ becomes a proposition. When no other domain is specified the domain is U.

Quantifiers Quatifiers are used to express that a proposition is true for all elements of the domain and that there exists some element in the domain for which it is true. They also have the highest precedence among the logical operators.

Universal quantifier	$\forall x P(x)$	$P(x)$ is true for every x in U
Existential quantifier	$\exists x P(x)$	$P(x)$ is true for some x in U

1.2.2 Properties

Uniqueness Quantifier The uniqueness quantifier is a commonly used quantifier to express that there is only one x for which $P(x)$ is true. It is usually written as $\exists!$ or $\exists_1$.

$$\exists_1 x P(x) \equiv \exists x(P(x) \land \forall y(P(y) \to y = x))$$

De Morgan's Laws De Morgan's laws for quantifiers state that $P(x)$ is not true for all x if and only if there exists an x for which $P(x)$ is false and furthermore that if $P(x)$ is false for all x if and only if there does not exist an x for which $P(x)$ is true.

$$\neg\forall x P(x) \equiv \exists x \neg P(x)$$
$$\forall x \neg P(x) \equiv \neg\exists x P(x)$$

1.3 Logical Proofs

Using logical inference it is possible to build an argument given a set of premises to reach a logical conclusion. An argument is valid if truth of all premises p_i implies that the conclusion q is also true.

$$\left(\bigwedge_{i=1}^{n} p_i\right) \rightarrow q \equiv T$$

1.3.1 Rules of Inference

Modus Ponens

$$\begin{array}{ll} & p \rightarrow q \\ & \underline{p \qquad\quad} \\ \therefore & q \end{array}$$

Modus Tollens

$$\begin{array}{ll} & p \rightarrow q \\ & \underline{\neg q \qquad\quad} \\ \therefore & \neg p \end{array}$$

Hypothetical Syllogism

$$\begin{array}{ll} & p \rightarrow q \\ & \underline{q \rightarrow r} \\ \therefore & p \rightarrow r \end{array}$$

Disjunctive Syllogism

$$\begin{array}{ll} & p \vee q \\ & \underline{\neg p \qquad} \\ \therefore & q \end{array}$$

Addition

$$\begin{array}{ll} & \underline{p \qquad} \\ \therefore & p \vee q \end{array}$$

Simplification

$$\begin{array}{ll} & \underline{p \wedge q} \\ \therefore & p \end{array} \qquad \begin{array}{ll} & \underline{p \wedge q} \\ \therefore & q \end{array}$$

Conjunction

$$\begin{array}{ll} & p \\ & \underline{q \qquad} \\ \therefore & p \wedge q \end{array}$$

Resolution

$$\begin{array}{ll} & \neg p \vee r \\ & \underline{p \vee q \quad} \\ \therefore & q \vee r \end{array}$$

Universal Instantiation

$$\begin{array}{ll} & \underline{\forall x P(x)} \\ \therefore & P(c) \end{array}$$

Universal Generalisation

$$\begin{array}{ll} & \underline{P(c) \text{ for an arbitrary } c} \\ \therefore & \forall x P(x) \end{array}$$

Existential Instantiation

$$\begin{array}{ll} & \underline{\exists x P(x) \qquad\qquad\qquad\quad} \\ \therefore & P(c) \text{ for some element } c \end{array}$$

Existential Generalisation

$$\begin{array}{ll} & \underline{P(c) \text{ for some element } c} \\ \therefore & \exists x P(x) \end{array}$$

Universal Modus Ponens

$$\begin{array}{ll} & \forall x (P(x) \rightarrow Q(x)) \\ & \underline{P(a) \text{ for a particular element } a} \\ \therefore & Q(a) \end{array}$$

1.3.2 Inference Proof

All men are mortal. Socrates is a man. Prove that Socrates is mortal.

$P(x) \equiv T$ means that x is a person. $M(x) \equiv T$ means that x is mortal. s is the particular element Socrates.

1.	$\forall x P(x) \rightarrow M(x)$	premise
2.	$P(s)$	premise
3.	$P(s) \rightarrow M(s)$	UI (1)
4.	$M(s)$	Modus Ponens, (2) & (3)

2 Set Theory

A set is a collection of distinct elements without duplicates and the order of elements is unimportant.

2.1 Notation

Containment $a \in A$ denotes that a is an element of the set A, whereas $a \notin A$ denotes that a is not contained in A. A set may contain other sets.

2.1.1 Describing Sets

Roster Method List all elements contained in the set. $S = \{a, b, c, d\}$ is equivalent to both $S = \{d, c, a, b\}$ and also $S = \{a, a, b, c, d, d\}$. When the pattern is clear, (...) may be used as in $S = \{a, b, c, \ldots, z\}$.

Set-Builder Method Specify the proposition that all members must satisfy. $S = \{x|P(x)\}$ denotes that all elements x in S must satisfy the proposition $P(x)$.

Interval Notation The elements in a set can be constrained by an open or closed interval. $[a, b] = \{x|a \leq x \leq b\}$ represents the closed interval between a and b. $(a, b) = \{x|a < x < b\}$ represents the open interval between a and b. Additionally combinations like $[a, b)$ and $(a, b]$ are possible.

2.1.2 Special Sets

Universal Set The universal set, denoted by U, contains everything currently under consideration.

Empty Set The empty set is the set that contains no elements. It is denoted by $\varnothing$. It is important to note that $\varnothing = \{\}$, but $\varnothing \neq \{\varnothing\}$. A set containing the empty set is not the equal to the empty set.

Singleton A singleton is a set containing exactly one element.

2.1.3 Set Equality

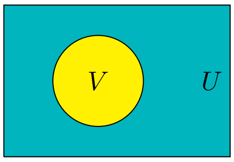
Two sets are equal if they contain the same elements. If A and B are sets then their equality is denoted as $A = B$.

$$\forall x(x \in A \equiv x \in B) \rightarrow A = B$$

.

2.1.4 Venn Diagram

Venn diagrams use circles to represent sets and their relation to other sets through their positioning and overlapping. The below diagram shows the set V contained in the universal set U.



2.1.5 Subsets

Set A is a subset of B if all elements in A are also in B. This relation is denoted as $A \subseteq B$.

$$\forall x(x \in A \rightarrow x \in B) \equiv A \subseteq B$$

Every set is always a subset of itself and the empty set $\varnothing$ is a subset of every other set.

Proper Subset When $A \subseteq B$, but $A \neq B$ then A is a proper subset of B, which is denoted as $A \subset B$.

$$\forall x(x \in A \rightarrow x \in B) \land \exists x(x \in B \land x \notin A) \equiv A \subset B$$

.

2.1.6 Set Cardinality

For finite sets the set cardinality describes the number of distinct elements in a set. It is denoted as $|S|$. The cardinality of the empty set is zero ($|\varnothing| = 0$). If A is the set containing all the letters of the english alphabet, then $|A| = 26$.

2.1.7 Power Sets

The set of all subsets of a set A is called the power set of A and is denoted as $\mathcal{P}(A)$. If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$. For example, given the set $A = a, b$ we get the power set $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

2.2 Tuples

Tuples are a collection of ordered elements. An n-tuple is written as $(a_1, a_2, a_3, \ldots, a_n)$. Two n-tuples are equal if and only if all of their corresponding elements are equal.

$$(a, b) = (c, d) \equiv (a = c) \land (b = d)$$

A subset R of $A \times B$ is called a relation from the set A to the set B.

2.2.1 Cartesian Product

The cartesian product $A \times B$ is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) | a \in A \land b \in B\}$$

The cartesian product of n sets is the set of tuples containing all possible combinations of elements as tuples.

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$$

The cardinality of the cartesian product is equal to the product of the cardinalities of the individual sets.

$$|A_1 \times A_2 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|$$