Discrete Math Cram Sheet

August 20, 2016

Contents

1 Propositional Logic

1.1 Truth Tables

p	T	T	F	F	
q	T	F	T	F	
F	F	F	F	F	contradiction
$p \veebar q$	F	F	F	T	joint denial
$p \nleftarrow q$	F	F	T	F	converse nonimplication
$\neg p$	F	F	T	T	left negation
$p \nrightarrow q$	F	T	F	F	nonimplication
$\neg q$	F	T	F	T	right negation
$p \oplus q$	F	T	T	F	exclusive disjunction
$p \barwedge q$	F	T	T	T	alternative denial
$p \wedge q$	T	F	F	F	conjunction
$p \leftrightarrow q$	T	F	F	T	biconditional/equivalence
q	T	F	T	F	right projection
$p \rightarrow q$	T	F	T	T	implication
p	T	T	F	F	left projection
$p \leftarrow q$	T	T	F	T	converse implication
$p \vee q$	T	T	T	F	disjunction
T	T	T	T	T	tautology

1.2 Logical Equivalences

Identity	$p \wedge \mathrm{T} \equiv p$ $p \vee \mathrm{F} \equiv p$
Domination	$p \vee \mathrm{T} \equiv \mathrm{T}$ $p \wedge \mathrm{F} \equiv \mathrm{F}$
Idempotent	$p \wedge p \equiv p$ $p \vee p \equiv p$
Commutative	$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$
Associative	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ $p \vee (q \vee r) \equiv (p \vee q) \vee r$
Distributive	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
De Morgan's	$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$
Absorption	$p \wedge (p \vee q) \equiv p$ $p \vee (p \wedge q) \equiv p$
Negation	$p \vee \neg p \equiv \mathrm{T}$ $p \wedge \neg p \equiv \mathrm{F}$
Double Negation	$\neg(\neg p) \equiv p$

Involving Biconditionals

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

Involving Conditional Statements

$p \rightarrow q \equiv \neg p \vee q$ $\quad$ $p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$ $\quad$ $p \wedge q \equiv \neg(p \rightarrow \neg q)$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

1.3 Rules of Inference

Modus Ponens	$\begin{array}{l} p \rightarrow q \\ p \\ \hline q \end{array}$
Modus Tollens	$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \neg p \end{array}$
Associative	$\begin{array}{l} (p \vee q) \vee r \\ \hline p \vee (q \vee r) \end{array}$
Commutative	$\begin{array}{l} p \wedge q \\ \hline q \wedge p \end{array}$
Biconditional	$\begin{array}{l} p \rightarrow q \\ q \rightarrow p \\ \hline p \leftrightarrow q \end{array}$
Exportation	$\begin{array}{l} (p \wedge q) \rightarrow r \\ \hline p \rightarrow (q \rightarrow r) \end{array}$
Contraposition	$\begin{array}{l} p \rightarrow q \\ \hline \neg q \rightarrow \neg p \end{array}$
Hypothetical Syllogism	$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$
Material Implication	$\begin{array}{l} p \rightarrow q \\ \hline \neg p \vee q \end{array}$
Distributive	$\begin{array}{l} (p \vee q) \wedge r \\ \hline (p \wedge r) \vee (q \wedge r) \end{array}$
Absorption	$\begin{array}{l} p \rightarrow q \\ \hline p \rightarrow (p \wedge q) \end{array}$
Disjunctive Syllogism	$\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}$
Addition	$\begin{array}{l} p \\ \hline p \vee q \end{array}$
Simplification	$\begin{array}{l} p \wedge q \\ \hline p \end{array}$
Conjunction	$\begin{array}{l} p \\ q \\ \hline p \wedge q \end{array}$
Double Negation	$\begin{array}{l} p \\ \hline \neg\neg p \end{array}$
Disjunctive Simplification	$\begin{array}{l} p \vee p \\ \hline p \end{array}$
Resolution	$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$

1.4 Satisfiability

A proposition is *satisfiable* if some setting of the variables makes the proposition true. For example, $p \wedge \neg q$ is satisfiable because the expression is true if p is true or q is false. On the other hand, $p \wedge \neg p$ is not satisfiable because the expression as a whole is false for both settings of p.

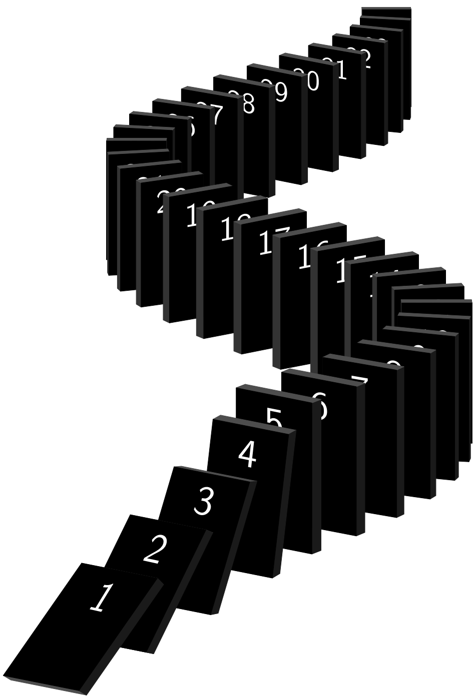
2-SAT Problem

(to follow...)

2 Proofs

2.1 Mathematical Induction

A statement $P(n)$ involving the positive integer n is true for all positive integer values of n is true if $P(1)$ is true and if $P(k)$ is true for any arbitrary positive integer k, then $P(k+1)$ is true.



The base case need not be for $n = 1$. It can be adjusted to whatever the smallest integer value n assumes.

2.2 Strong Induction

Let $P(n)$ be a predicate defined over all integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. Base cases: $P(a), P(a+1), \ldots, P(b)$ are all true.
2. Inductive step: For any integer $k > b$, if $P(i)$ is true for all integers i with $a \leq i < k$, then $P(k)$ is true.

Then the statement $P(n)$ is true for all integers $n \geq a$.

3 Recurrence Relations

4 Number Theory

4.1 Divisibility

4.2 Primes and Factors

4.3 Divisors

Greatest Common Divisor

This can be defined by the following recurrence relation:

$$\gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ \gcd(b, a \bmod b) & \text{else} \end{cases}$$

4.4 Modular Arithmetic

Basic Rules

(to follow...)

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers, and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$, where $x = \sum_{k=1}^{n} a_k M_k y_k$, $M_k = \frac{m}{m_k}$, and y_k is the modular inverse of M_k modulo m_k, i.e. $M_k y_k \equiv 1 \pmod{m_k}$.

5 Graph Theory

6 Linear Algebra

7 Combinatorics

7.1 Permutations and Combinations

Permutation

A permutation or ranking of n objects is a listing of them in a certain order from first to last.

Combination

A combination of k objects taken from a collection of n objects is simply a selection of k of those distinct objects without regard to order.

7.2 Binomial Coefficients

7.3 Generalized Permutations and Combinations

Permutations with Duplicate Objects

The number of permutations of a multiset of n objects made up of k distinct objects can be expressed as follows:

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}$$

where n_i represents the multiplicity of a distinct object i in the multiset.

Combinations with Repetition (Dashes and Dividers)

The number of combinations of length n using k different kinds of objects is

$${}_nR_k = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = \frac{(n+k-1)!}{n!\,(k-1)!}$$

Number of Non-negative Integer Solutions The number of solutions of the equation $x_1 + x_2 + \cdots + x_k = n$ in non-negative integers is $\binom{n+k-1}{k-1}$.

Number of Positive Integer Solutions The number of solutions of the equation $x_1 + x_2 + \cdots + x_k = n$ in positive integers is $\binom{n-1}{k-1}$.

7.4 Principle of Inclusion-Exclusion

This provides an organized method/formula to find the number of elements in the union of a given group of sets, the size of each set, and the size of all possible intersections among the sets.

Two/Three Sets

Suppose that A,B, and C are finite sets. Then:

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

General Form

For finite sets $A_1, \ldots, A_n$, one has the identity:

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\ &\quad + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \\ &\quad - \ldots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n| \\ &= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right)\end{aligned}$$

8 Probability