Discrete Math Cram Sheet

October 6, 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
$p \barwedge q$ / $p \overline{\vee} q$	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
$p \overline{\wedge} q$	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
$p \to q$	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

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

Involving Conditional Statements

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

1.3 Rules of Inference

Modus Ponens	$\begin{array}{l} p \to q \\ p \\ \hline q \end{array}$
Modus Tollens	$\begin{array}{l} \neg q \\ p \to q \\ \hline \neg p \end{array}$
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	$\begin{array}{l} p \to q \\ q \to p \\ \hline p \leftrightarrow q \end{array}$
Exportation	$\begin{array}{l} (p \wedge q) \to r \\ \hline p \to (q \to r) \end{array}$
Contraposition	$\begin{array}{l} p \to q \\ \hline \neg q \to \neg p \end{array}$
Hypothetical Syllogism	$\begin{array}{l} p \to q \\ q \to r \\ \hline p \to r \end{array}$
Material Implication	$\begin{array}{l} p \to q \\ \hline \neg p \vee q \end{array}$
Distributive	$\begin{array}{l} (p \vee q) \wedge r \\ \hline (p \wedge r) \vee (q \wedge r) \end{array}$
Absorption	$\begin{array}{l} p \to q \\ \hline p \to (p \wedge q) \end{array}$
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...)

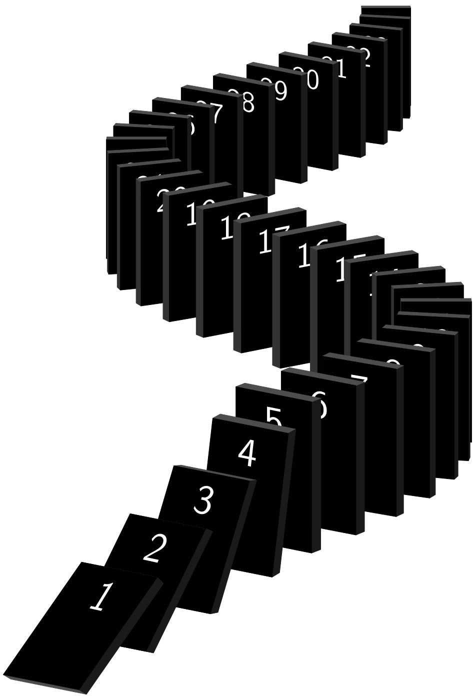
2 Proofs

2.1 Well-Ordering Principle

Every non-empty subset of the natural numbers has a smallest element.

2.2 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.

2.3 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

Properties

$a|b \rightarrow a|bc \quad \forall c$
$(a|b \wedge b|c) \rightarrow a|c$
$(a|b \wedge a|c) \rightarrow a|sb + tc \quad \forall s, t$
$\forall c \neq 0\, (a|b \leftrightarrow ca|cb)$

4.2 Primes and Factors

Prime Numbers

OEIS A000040: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, . . .

4.3 Divisors

Greatest Common Divisor

This can be defined by the following recurrence relation:

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

Bézout's Identity

Let a and b be nonzero integers (i.e., $a, b \in \mathbb{R}^*$) and let $d = \gcd(a, b)$. Then:

$$\exists x, y \in \mathbb{Z}\, (ax + by = d)$$

In addition,

- the greatest common divisor d is the smallest positive integer that can be written as $ax + by$
- every integer of the form $ax + by$ is a multiple of the greatest common divisor d.

Extended Euclidean Algorithm

4.4 Modular Arithmetic

Basic Rules

(to follow...)

Fermat's Little Theorem

If p is a prime number and a is a natural number, then

$$a^p \equiv a \pmod{p}$$

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

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

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

5.1 Notation

Fundamental Notation

G	graph	E	edge set
V	vertex set		

Graph Invariants

$c(G)$	circumference	$\chi'(G)$	chromatic index
$d(u,v)$	distance between two vertices	$\delta(G)$	minimum degree
$\deg(v)$	degree of a vertex	$\Delta(G)$	maximum degree
$\mathrm{gir}(G)$	girth	$\kappa(G)$	vertex connectivity
$\chi(G)$	chromatic number	$\lambda(G)$	edge connectivity

5.2 Definitions

graph an ordered pair (V, E) where V is the set of vertices and E is the set of edges

simple a graph having neither loops nor multiple edges

multigraph a graph with multiple edges but no loops

pseudograph a graph having both loops and multiple edges

digraph a directed graph in which each edge has a direction

adjacency two distinct vertices v and w in a graph are adjacent if the pair $\{v, w\}$ is an edge

incidence a vertex v and an edge e are incident with one another if $v \in e$

degree (of a vertex v, in symbols $\deg(v)$) the number of vertices adjacent to v

walk an alternating sequence $v_0, e_1, v_1, \ldots, e_k, v_k$ of vertices v_i and edges e_i for which e_i is incident with v_{i-1} and with v_i for each i

path a walk whose vertices are distinct

trail a walk whose edges are distinct

circuit a trail whose first and last vertices are identical

cycle a circuit where each pair of whose vertices other than the first and the last are distinct

5.3 Properties

Handshaking Lemma

In any graph the sum of the vertex degrees is equal to twice the number of edges.

$$\sum_{v \in V} \deg(v) = 2|E|$$

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.
The number of permutations of length k from n distinct objects where repetition is not allowed is

$${}_nP_k = (n)_k = \frac{n!}{(n-k)!}$$

where $(n)_k$ denotes the falling factorial.

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.
The number of different combinations of k objects taken from a collection of n distinct objects without repetition is

$${}_nC_k = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

7.2 Binomial Coefficients

The binomial coefficient $\binom{n}{k}$ can be defined as the coefficient of the x^k term in the polynomial expansion of $(x+1)^n$, which occurs in the binomial formula

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

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

Pascal's Triangle

Row 0:	1
Row 1:	1 1
Row 2:	1 2 1
Row 3:	1 3 3 1
Row 4:	1 4 6 4 1
Row 5:	1 5 10 10 5 1
Row 6:	1 6 15 20 15 6 1
Row 7:	1 7 21 35 35 21 7 1
Row 8:	1 8 28 56 70 56 28 8 1
Row 9:	1 9 36 84 126 126 84 36 9 1
Row 10:	1 10 45 120 210 252 210 120 45 10 1

7.3 Generalized Permutations and Combinations

Permutations with Repetitions

The number of permutations of length k from n distinct objects where repetition is allowed is n^k.

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 (Stars and Bars)

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

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

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:

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

7.5 Derangements

A derangement is a permutation of the elements of a set, such that no element appears in its original position. The number of derangements of n elements can be determined as follows:

$$!n = (n-1)\,(!\,(n-1) + !\,(n-2)) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

OEIS A000166: 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570, 176214841, 2290792932, . . .

7.6 Catalan Numbers

$$
\begin{aligned}
C_n &= \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!\,n!} = \prod_{k=2}^{n}\frac{n+k}{k} \qquad \text{for } n \geq 0 \\
&= \binom{2n}{n} - \binom{2n}{n+1} = \sum_{i=0}^{n-1} C_i C_{n-i-1}
\end{aligned}
$$

OEIS A000108: 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, 2674440, 9694845, 35357670, ...

Applications

1. number of expressions containing n pairs of parentheses which are correctly matched
2. number of different ways $n+1$ factors can be completely parenthesized
3. number of full binary trees with $n+1$ leaves
4. number of monotonic lattice paths along the edges of a grid with $n \times n$ square cells, which do not pass above the diagonal
5. number of triangulations of a convex polygon with $n+2$ sides
6. number of permutations of $\{1, \ldots, n\}$ that avoid the pattern 123 (or any of the other patterns of length 3)
7. number of noncrossing partitions of the set $\{1, \ldots, n\}$
8. number of ways to tile a stairstep shape of height n with n rectangles
9. number of ways to form a “mountain range” with n upstrokes and n downstrokes that all stay above the original line
10. number of semiorders on n unlabeled items

7.7 Partitions

The function $p(n,k)$ denotes the number of ways of writing n as a sum of exactly k terms.

$$
p(n,k) = \begin{cases} 1 & \text{if } n = k = 0 \\ 0 & \text{if } n < k \\ p(n-1,k-1) + p(n-k,k) & \text{if } n \geq k \end{cases}
$$

7.8 Stirling Numbers

First Kind (Cycles)

Counts number of permutations of n elements with k disjoint cycles.

$$
\left[{n \atop k}\right] = \begin{cases} 1 & \text{if } n = k = 0 \\ 0 & \text{if } n \neq k \wedge k = 0 \\ (n-1)\left[{n-1 \atop k}\right] + \left[{n-1 \atop k-1}\right] & \text{if } n,k > 0 \end{cases}
$$

Second Kind (Subsets)

Counts the number of ways to partition a set of n objects into k non-empty subsets.

$$
\left\{{n \atop k}\right\} = \begin{cases} 1 & \text{if } n = k = 0 \\ 0 & \text{if } n \neq k \wedge k = 0 \\ (k-1)\left\{{n-1 \atop k}\right\} + \left\{{n-1 \atop k-1}\right\} & \text{if } n,k > 0 \end{cases}
$$

8 Probability