Discrete

Sean Richardson

June 10, 2018

1 Combinatorics

Combinatorics studies methods of counting things.

Theorem 1.1. Addition Principle: Consider some task T. If T can be accomplished by methods $M_1, M_2, \ldots, M_n$ which can each be accomplished in $a_1, a_2, \ldots, a_n$ ways, then T can be accomplished in $\sum a_k$ ways.

Theorem 1.2. Multiplication Principle: Consider some task T. If T can be broken down into necessary subtasks $t_1, t_2, \ldots, t_n$ which can be accomplished in $b_1, b_2, \ldots, b_n$ ways, then T can be done in $\prod b_k$ ways.

Theorem 1.3. An arrangment of n objects is called a "permutaion". There are $n!$ possible permutations.

Theorem 1.4. An arrangment of r objects out of a collection of n objects is called an "r-permutation". This can be done in $P(n,r) = {}_nP_r = \frac{n!}{(n-r)!}$ ways.

Theorem 1.5. An r-combination is how many combinations of r objects (ignoring order) you can choose from n objects. There are $C(n,r) = {}_nC_r = \binom{n}{r} = \frac{n!}{r!(n-r)!}$ ways.

We will now try to determine how many ways n balls can be put in to r boxes. To see this, we use the following trick. Think of balls distributed into boxes in the following structure: $\circ\circ / \circ\circ\circ / \circ / \circ\circ$ where "$\circ$" represents balls and the "/" symbols divide the balls into categories or boxes. So, the amount of ways to divide n balls into r categories is the amount of ways we can the distribute the dividers among the characters. This is equivalent to "*characters* choose *dividers*". There are $n + r - 1$ characters and $r - 1$

dividers. So, we have $\binom{n+r-1}{r-1}$ ways to divide n identical things into r categories. Additionally, we have the following useful equivalency:

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

Theorem 1.6. The number of ways to distribute n identical balls into r distinct boxes is $\binom{n+r-1}{r-1}$ or $\binom{n+r-1}{n}$ ways.

2 Number Theory

Definition 2.1. Let k and n be integers with $k \neq 0$. If there exists integer q such that $kq = n$, we say k *divides* n, denoted $k|n$.

Theorem 2.1. Let a, b, c be integers. If $a|b$ and $b|c$, then $a|c$.

Theorem 2.2. Let a, b, c be integers. If $a|b$ and $a|c$, then $a|b + c$.

Theorem 2.3. (The Division Algorithm). Let m and n be integers, with $m > 0$. Then, there is a unique pair of integers q and r such that $n = mq+r$ where $0 \leq r < m$.

/*Irrational numbers and $\sqrt{2}$*/

Definition 2.2. Let $n > 0$ and $p > 1$ be integers. p is *prime* if "$n|p$" is only true if $n = p$ or $n = 1$.

There is a useful mathematical proof technique called *induction*. Induction operates in two parts. If you want to proove some statement involving an arbitrary n is true, you first proove it is true for the specific case $n = c$ where you choose c. Secondly, you show that if the statement holds for $n = k$, then it holds for $n = k + 1$. Then, you are done. By the first part, you have prooved the case $n = c$. Then, combining this with the second part of the prood, you know it holds for $n = c + 1$,$n = c + 2$,$n = \ldots$ A formal inductive proof has the following form:

Proof. *Sample Inductive Proof:*
We proceed by the method of Induction,
For the base case of $n = 0$, *prove the statement holds for* $n = 0$

Now we make the inductive hypotheseis that *the statement holds for arbitrary k.*
Now we proceed to proove the inductive step *proove that if statement holds for k, it holds for $k+1$.*
Thus by induction *the statement holds.* □

3 Logic

The symbols:

- $\neg$: Represents "not". $\neg A$ is read "not A" or "negation of A".
- $\wedge$: Represents "and". $A \rightarrow B$ is read "A and B".
- $\vee$: Represents "or". $A \vee B$ is read "A or B".
- $\rightarrow$: Represent "if". $A \wedge B$ is read "A implies B" or "if A then B".
- $\leftrightarrow$: Represent "necessary and sufficient condition". $A \leftrightarrow B$ is equivalet to $A \rightarrow B$ and $B \rightarrow A$.
- $\forall$: The universal quantifier; represents "for all". $\forall x \in D$ is read "for all x in D."
- $\exists$: The existential quantifier; represents "for some" or "there exists". $\exists x \in D$ is read "there exists an x in D".
- $\exists!$: Represent "there exists unique".

Definition 3.1. A statement that is always false called is a *contradiction.* The classic contradiction is $p \wedge \neg p$.

Definition 3.2. A statement that is always true is called a *tautology.* The classic tautology is $p \vee \neg p$.

Theorem 3.1. DeMorgan's Law:
$\neg(p \wedge q) \iff \neg p \vee \neg q$ and $\neg(p \vee q) \iff \neg p \wedge \neg q$

Theorem 3.2. General DeMorgan's Law:
$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \iff (\neg p_1 \vee \neg p_2 \vee \cdots \vee p_n)$
$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \iff (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge p_n)$

Theorem 3.3. Reduction ad absurdum, $(p \rightarrow q) \iff ((p \wedge \neg q) \rightarrow c)$

Theorem 3.4. Modus ponens, $((p \leftarrow q) \wedge p) \implies q$

Theorem 3.5. Modus tollens, $((p \rightarrow q) \wedge \neg q)$

Theorem 3.6. Law of syllogism, $((p \rightarrow q) \wedge (q \rightarrow r)) \implies (p \rightarrow r)$

Theorem 3.7. Law of disjunctive syllogism, $((p \vee q) \wedge \neg p) \implies q$

Theorem 3.8. $\neg(\forall x \in D, p(x)) \iff \exists x \in D, \neg p(x)$

4 Set Theory

There exists objects. Objects can be "in", "belong to" or be an"element" of a set. If an object is in a set S, we say $a \in S$. If not, we say $a \notin S$. We can describe the elements of a set S in the folliwing notation. $S = \{f|\text{rule that } f \text{ must obey}\}$.

Definition 4.1. Let A and B be sets. If $\forall x \in A, x \in B$ then A is a *subset* of B, denoted $A \subseteq B$.

Definition 4.2. The set of everything in the relevant universe is denoted $\mathcal{U}$.

Definition 4.3. The set with nothing in it is the *empty set*, denoted $\emptyset$. $\emptyset = \{f|f \notin \mathcal{U}\}$.

Theorem 4.1. For any set A, $\emptyset \subseteq A$.

Definition 4.4. Let A and B be sets such that $A \subseteq B$ and $B \subseteq A$. Then, we say $A = B$.

Definition 4.5. Let A and B be sets. If $A \subseteq B$ but $A \neq B$ then A is a *proper subset* of B, denoted $A \subset B$.

Theorem 4.2. The empty set is unique.

Definition 4.6. Let n be a nonnegative integer. A set containing n distinct elements is called an *n-set*.

Definition 4.7. Let A be an n-set. n is called the *cardinality* of A or the *order* of A, denoted $|A| = n$

Definition 4.8. Let A and B be sets so that $B \in A$ and $|B| = r$. Then B is said to be an *r-subset* of A.

Theorem 4.3. There are $\binom{n}{r}$. r-subsets of and n-set.

Definition 4.9. Let A be a set. The set of all subsets of A is called the *power set of* A dentoted $\mathcal{P}(A)$.

Theorem 4.4. For any nonnegative integer n there are 2^n subsets of an n-set A. So $|\mathcal{P}(A)| = 2^n$

/*Note about summing over choose operators*/

Definition 4.10. Let A and B be sets. The *union* of A and B denoted $A \cup B$ is defined $A \cup B = \{x | x \in A \text{ or } x \in B\}$.

Definition 4.11. Let A and B be sets. The *intersection* of A and B denoted $A \cap B$ is defined $A \cap B = \{x | x \in A \text{ and } x \in B\}$.

Definition 4.12. Let A and B be sets. If $A \cap B = \emptyset$ then A and B are *disjoint*.

Theorem 4.5. Let A and B be sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.

Theorem 4.6. Let A and B be sets
Associative laws:
$(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
Distributive laws:
$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ and $(A \cap B) \cap C = (A \cup C) \cap (B \cup C)$

Definition 4.13. Let A and B be sets. The *relative complement* of B *in* A, denoted $A \setminus B$ or $A - B$. Its defined as $A \setminus B = \{x | x \in A \text{ and } x \notin B\}$.

Definition 4.14. Let A be a set. The *complement* of A, denoted $\overline{A}$ is defined as $\overline{A} = \{x \in \mathcal{U} | x \notin A\}$.

Definition 4.15. (DeMorgan's Laws) Let A and B be sets.
Then $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$