Discrete

Sean Richardson

October 13, 2018

Contents

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 arrangement of n objects is called a "permutation". There are $n!$ possible permutations.

Theorem 1.4. An arrangement 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.

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.

Proof. 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:

$$\begin{aligned}\binom{n+r-1}{r-1} &= \frac{(n+r-1)!}{(r-1)!(n+r-1-(r-1))} \\ &= \frac{(n+r-1)!}{(n+r-1-(n))!(n)!} = \binom{n+r-1}{n}\end{aligned}$$

□

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

Theorem 2.3. Let a, b, c be integers. If $a|b$ and $a|c$, then $a|b+c$.

Theorem 2.4 (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 2.5. 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 prove some statement involving an arbitrary n is true, you first prove 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 proved the case $n = c$. Then, combining this with the second part of the proof, you know it holds for $n = c + 1$,$n = c + 2$,$n = \ldots$ A formal inductive proof has the following form:
Inductive Proof Structure:
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 hypothesis that *the statement holds for arbitrary* k.
Now we proceed to prove the inductive step *prove 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". $A \to B$ is read "A and B".
- $\vee$: Represents "or". $A \vee B$ is read "A or B".
- $\to$: 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 equivalent to $A \to B$ and $B \to A$.
- $\forall$: 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 3.3 (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 3.4 (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 3.5 (Reduction ad absurdum)**.** $(p \to q) \iff ((p \wedge \neg q) \to c)$

Theorem 3.6 (Modus ponens)**.** $((p \leftarrow q) \wedge p) \implies q$

Theorem 3.7 (Modus tollens)**.** $((p \to q) \wedge \neg q)$

Theorem 3.8 (Law of syllogism)**.** $((p \to q) \wedge (q \to r)) \implies (p \to r)$

Theorem 3.9 (Law of disjunctive syllogism)**.** $((p \vee q) \wedge \neg p) \implies q$

Theorem 3.10. $\neg(\forall x \in D, p(x)) \iff \exists x \in D, \neg p(x)$

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 following 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 4.4. For any set A, $\emptyset \subseteq A$.

Definition 4.5. Let A and B be sets such that $A \subseteq B$ and $B \subseteq A$. Then, we say $A = B$.

Definition 4.6. 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 4.7. The empty set is unique.

Definition 4.8. Let n be a nonnegative integer. A set containing n distinct elements is called an *n-set*.

Definition 4.9. Let A be an n-set. n is called the *cardinality* of A or the *order* of A, denoted $|A| = n$

Definition 4.10. 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 4.11. There are $\binom{n}{r}$. r-subsets of and n-set.

Definition 4.12. Let A be a set. The set of all subsets of A is called the *power set of* A denoted $\mathcal{P}(A)$.

Theorem 4.13. 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 4.14. 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 4.15. 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 4.16. Let A and B be sets. If $A \cap B = \emptyset$ then A and B are *disjoint*.

Theorem 4.17. Let A and B be sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.

Theorem 4.18. 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 4.19. 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 4.20. 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 4.21. (DeMorgan's Laws) Let A and B be sets.
Then $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$

5 Pascal and Probability

5.1 Pascal's Triangle

This section is centered around the patterns of Pascal's Triangle and the related theorems. We will define Pascal's Triangle as the following pattern of choose functions:

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
\end{array}$$

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & &
\end{array}$$

First, we need some tools to further investigate Pascal's Triangle

Theorem 5.1 (Pascal's Identity)**.** Each entry in Pascal's Triangle is exactly equal to the sum of the entry up and to the right along with the entry up and to the left. This is due to the following equality, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Proof. The quantity $\binom{n+1}{k+1}$ represents the number of ways to make committees of size $k+1$ from $n+1$ people including you. Each committee either includes you or doesn't. $\binom{n}{k}$ include you and $\binom{n}{k+1}$ do not. Therefore, the equality holds. □

Theorem 5.2. Each entry in Pascal's Triangle describes precisely how many paths there is from the top of Pascal's Triangle there is to that entry.

Proof. /*Add inductive proof*/ □

Theorem 5.3 (The Biomial Theorem)**.** The nth row of Pascal's Triangle perfectly describes the coefficients of $(x+y)^n$. Or,

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

Proof 1. We proceed by induction on n,

We have the base case of $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0$

We make the inductive hypothesis that for some $m \geq 0$,

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

We will now make the inductive step in showing that

$$(x+y)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} x^{(m+1)-k} y^k$$

We begin,

$$(x+y)^{m+1} = (x+y)(x+y)^m = (x+y) \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k$$

$$= \sum_{k=0}^{m} \binom{m}{k} x^{(m+1)-k} y^k + \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^{k+1}$$

Make a change of variables to right sum

$$= \sum_{k=0}^{m} \binom{m}{k} x^{(m+1)-k} y^k + \sum_{k=1}^{m} +1 \binom{m}{k-1} x^{(m+1)-k} y^k$$

Apply Pascal's Identity

$$= \binom{m}{0} x^{m+1} + \sum_{k=1}^{m} \binom{m+1}{k} x^{(m+1)-k} y^k + \binom{m+1}{m+1} y^{m+1}$$

$$= \sum_{k=0}^{m+1} \binom{m+1}{k} x^{(m+1)-k} y^k$$

We have shown our inductive step and thus conclude our proof by induction. □

Proof 2. A more intuitive proof of the Binomial Theorem.
Consider $(x+y)^n = (x+y)(x+y)\cdots(x+y)$ Multiplying this out is of the form $(xx\cdots xx) + (xx\cdots xy) + \cdots + (yy\cdots yy)$ iterating through all orderings of x's and y's. Every ordering with k amount of y's contributes 1 to the $x^{n-k}y^k$ coefficient. There are $\binom{n}{k}$ ways to contribute to $x^{n-k}y^k$ terms, so the coefficient of this term is $\binom{n}{k}$. It follows that the full expansion is $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$. Proving the Binomial Theorem.

Corollary 5.4. The case $x = y = 1$ in the binomial theorem shows

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n$$

And the case of $x = -1$, $y = 1$ in the binomial theorem shows that

Corollary 5.5. And the case of $x = -1$, $y = 1$ in the binomial theorem shows that

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$$

□

Add Intuitive proof

Theorem 5.6. The sum of some diagonal down and to the right on Pascal's Triangle is described by the term down and to the left of the lowest term in the diagonal. Or,

$$\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \cdots + \binom{k+r}{r} = \binom{k+r+1}{r}$$

Add Figure

Proof. /*Do this, (inductive)*/ □

/*After stuff*/

Definition 5.7. We define the notation

$$\binom{n}{a_1, a_2, \cdots, a_k} = \frac{n}{a_1! a_2! \ldots a_k!}$$

Theorem 5.8 (The Multinomial Theorem)**.** For $n \geq 0 \in Z$,

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{a_1, a_2, \cdots, a_k \geq 0 \\ a_1 + a_2 + \cdots + a_k = n}} \binom{n}{a_1, a_2, \cdots, a_k} x_1^{a_1} + x_2^{a_2} + \cdots x_k^{a_k}$$

Proof. Consider $(x_1 + x_2 + \cdots + x_k)^n$, which expands to the sum of every ordering of x_1's, x_2's, ..., x_k's. The amount of orderings that contribute to an arbitrary $x_1^{a_1} + x_2^{a_2} + \cdots x_k^{a_k}$ is $\binom{n!}{a_1!}\binom{(n-a_1)!}{a_2}\binom{n-(a_1+\cdots+a_{k-1})}{a_k} = \binom{n}{a_1, a_2, \cdots, a_k}$. It then follows that,
$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{a_1, a_2, \cdots, a_k \geq 0 \\ a_1 + a_2 + \cdots + a_k = n}} \binom{n}{a_1, a_2, \cdots, a_k} x_1^{a_1} + x_2^{a_2} + \cdots x_k^{a_k}$ which proves the Multinomial Theorem. □

5.2 Probability

Definition 5.9. An *experiment* is an action whose result is one of a finite number of equally likely outcomes.

Definition 5.10. The set of outcomes of an experiment is called the *sample space* of the experiment, denoted S.

Definition 5.11. An *event* is a subspace of the sample space.

Definition 5.12. Let E be an event in S. Then, the *probability* of E is $P(E) = \frac{|E|}{|S|}$.

6

6.1 Relations

Definition 6.1. Let A and B be sets. The *Cartesian product* or the *cross product* of A and B, is defined $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

multiplication table

Definition 6.2. Let A and B be sets. A subset of $A \times B$ is a *relation* from A to B

Theorem 6.3. Let A and B be finite sets. $|A \times B| = |A||B|$.

Justification. The set $A \times B$ is created in a matrix of (a, b) pairs. The matrix is $|A|$ by $|B|$, so it has $|A||B|$ elements.

Theorem 6.4. Let A and B be finite sets. The number of relations from A to B is $2^{|A||B|}$.

Proof. Let A and B be sets. By Definition 6.2, a relation is a subset any $A \times B$. The number of relations is the number of ways to create a relation, which is the number of subsets of $A \times B$. By Theorem 4.13, this is equivalent to $2^{|A \times B|} = 2^{|A||B|}$. □

Definition 6.5. Let R be a relation from A to B. Then the set $R^{-1} = \{(b, a) \mid (a, b) \in R\}$ is the *inverse relation* of R.

Definition 6.6. Let A be a set. A subset R of $A \times A$ is a *(binary) relation* on A. If $(a, b) \in R$, we say aRb, read "a is related to b".

Definition 6.7. Let R be a relation on A. If aRa for $\forall a \in A$, R is *reflexive*.

Definition 6.8. Let R be a relation on A. If aRb implies bRa, R is *symmetric*.

Definition 6.9. Let R be a relation on A. R is *transitive* if aRb and bRc implies aRc.

Definition 6.10. Let R be a relation on A. If R is reflexive, symmetric, and transitive, then R is said to be an *equivalence relation*.

There will end up being some number of "bags" containing elements that are related within a relation. bags figure

Definition 6.11. Let R be an equivalence relation on a set A. Let $a \in A$. The set $R_a = \{x \in A \mid aRx\}$ is called the *equivalence class* of a.

Theorem 6.12. Let R be an equivalence relation on A and let $a, b \in A$. Then either $R_a = R_b$ or $R_a \cap R_b = \emptyset$.

Justification. If an equivalence relation represents a bunch of "bags". This is saying that an element cannot be in two bags. If an element were in to bags, the transitivity would imply that the bags are actually the same or they are not bags that define equivalence relations.

Definition 6.13. Let A be a nonempty set. We define $P = \{A_1, A_2, \ldots, A_n\}$, where each $A_i \subseteq A, A_i \neq \emptyset$ for $1 \leq i \leq n$, $A_i \cap A_j = \emptyset$ for $i \neq j$, and $A_1 \cup A_2 \cup \ldots A_n = A$. Then, P is a *partition* of A.

Translation. A *partition* splits all elements of something into smaller pieces.

Theorem 6.14. Let $P = \{A_1, A_2, \ldots, A_n\}$ be a partition on the set A. If we define a relation R on A by aRb iff $(a \in A_i) \leftrightarrow (b \in A_i)$ for some i, then R is an equivalence relation.

Translation. The pieces a partition splits a set A into can describe the "bags" of an equivalence relation.

Proof. We will show the relation R is reflexive, symmetric, transitive.

- Consider an arbitrary $a \in A$. Assume $\neg aRa$. This implies $\neg(a \in A_i \leftrightarrow a \in A_i) \Rightarrow (a \in A) \wedge (a \notin A)$, a contradiction. So, we conclude aRa. Because a is arbitrary, we have $\forall a \in A, aRa$. And we have thus concluded reflexivity.
- Assume aRb. This implies $(a \in A_i) \leftrightarrow (b \in A_i) \Rightarrow (b \in A_i) \leftrightarrow (a \in A_i) \Rightarrow bRa$. So, we conclude $aRb \rightarrow bRa$, confirming symmetry.

- Assume $aRb \wedge aRc$. This implies $(a \in A_i \leftrightarrow b \in A_i) \wedge (a \in A_i \leftrightarrow c \in A_i) \Rightarrow a \in A_i \leftrightarrow c \in A_i \Rightarrow aRc$, confirming transitivity.

R is reflexive, symmetric, and transitive. So, R is an equivalence relation. □

6.2 Functions

Definition 6.15 (Function)**.** Let F be a relation from a set A to a set B. If each first coordinate appears exactly once in the set of ordered pairs, then F is a *function* from A to B.

A function F that maps each element in A to a corresponding element in B is often notated by $F : A \to B$.

show mapping of F from every element of one set to some of other set

Theorem 6.16. Let A and B be finite sets. There are $|B|^{|A|}$ functions from A to B.

Definition 6.17 (Domain and Range)**.** Let F be a function from a set A to a set B. The set of all first coordinates of ordered pairs in F is the *domain* of F. (A is the domain). The set of all second coordinate ordered pairs in F is called the *range*. The set B is the *codomain* of F. If $F(a) = b$, we say b is the *image* of a under F and a is the *pre-image* of b.

Definition 6.18 (one-to-one)**.** Let A and B be sets and $F : A \to B$ a function. If $\forall x_1, x_2 \in A$ we have $x_1 \neq x_2 \implies F(x_1) \neq F(x_2)$, then F is a *one-to-one* function or an *injection*.

Theorem 6.19. Let A and B be finite sets. There are $\frac{|B|!}{(\|B\|-\|A\|)!}$ one-to-one functions from A to B.

Definition 6.20 (Onto function)**.** Let A and B be sets and $f : A \to B$ a function. If $\forall b \in B, \exists a \in A$ such that $f(a) = b$, then f is an *onto* function or a *surjection*.

Definition 6.21 (Bijection)**.** Let A and B be sets and $f : A \to B$ a function. If f is 1-1 and onto, f is a *bijection*. If a bijection exists from A to B, we say there is a *one-to-one correspondence* between A and B.

Definition 6.22 (Cardinality)**.** If there exists a bijection $f : \{1, 2, \ldots, n\} \to A$ then we say the *cardinality* of A is n, denoted $|A| = n$.

Definition 6.23 (Composition)**.** Let $F : A \to B$ and $G : B \to C$. Then the *composition* of G with F, denoted $G \circ F : A \to C$ is a function defined by

$$G \circ F : a \mapsto G(F(a)) \quad \forall a \in A$$

Definition 6.24 (The Pigeonhole Principle)**.** Let A be an n-set and B an m-set with $n > m$. Then $f : A \to B$ cannot be 1–1.