Mathematical Proofs

Rajiv Raman

September 21, 2023

Abstract

These notes provide a quick background on basic Counting.

1 Introduction

Theorem 1

Let X and Y be two sets, where $|X| = n$ and $|Y| = m$. The number of functions $f : X \to Y$ is m^n.

Proof. We prove by induction on $|X|$. If $X = \emptyset$, then there is just one function, namely the empty function, which is $m^0 = 1$. Suppose for $|X| = n$ and any $m = |Y|$, the number of functions is m^n. Consider a set X of size $n+1$. Let $x_1, \ldots, x_{n+1}$ be the elements in X. For any function $f : X \to Y$, there are m functions $f' : X \setminus \{x_{n+1}\} \to Y$ for each available choice for the element x_{n+1}. By the inductive hypothesis, the number of function $f' : X \setminus \{x_{n+1}\} \to Y$ is m^n. Therefore, the number of functions $f : X \to Y$ is

$$m^n m = m^{n+1}$$

□

Exercise 1

How many distinct 7 letter words are there in the English alphabet?

Solution: Since there is a bijection between the number of functions from a set of size 7 to a set of size 26, the number of words is 26^7.

Exercise 2

There are 26 types of postcards at a store. You want to select 7 postcards to send to your friends. In how many different ways can you choose the postcards to send to your friends?

Solution: There is a bijection between the number of functions from a set of size 7 to a set of size 26 to the different ways in which you can select 26 types of postcards to your seven friends.

In both cases, we viewed the set X as the letters of the 7 letter word in the first case, and the 7 friends in the second case; the set Y is the 26 letters of the English alphabet. Each position of the word gets a single letter, and similarly each friend receives a single postcard. Since there are no other restrictions, it is easy to see that the numbers in both cases are equivalent to the number of functions between appropriately chosen sets.

The idea of obtaining a *bijection* is a central idea in counting. To count the number of elements in a set, obtain a bijection to a set whose cardinality is known.

Theorem 2

Any set X of size n has 2^n subsets.

Proof. Let $f : X \to \{0, 1\}$. By Theorem 1, the number of such functions is 2^n. Such a function is called a *characteristic function*. There is a bijection between the power set of X and functions $f : X \to \{0, 1\}$. For a function f, let $S = \{x : f(x) = 1\}$. In other words, let $\mathcal{F}$ denote the set of all functions from X to $\{0, 1\}$. Note that each element in $\mathcal{F}$ is a function. Let $\mathcal{P}(X)$ denote the power set of X.

Let $g : \mathcal{F} \to \mathcal{P}(X)$ be the following function:

$$g(f) = \{x \in X : f(x) = 1\}$$

That is, g maps a particular function f to the subset of X that it maps to 1. To see that this is a bijection, note that g is an injection, and g^{-1} is well defined; for $S \in \mathcal{P}(X)$, $g^{-1}(S) = \{f : X \to \{0, 1\} : f(x) = 1 \Leftrightarrow x \in S\}$. □

Theorem 3

Any non-empty set X has exactly 2^{n-1} sets of odd size and 2^{n-1} sets of even size.

Proof. Let $n = |X|$. Let $a \in X$, and consider the set $X' = X \setminus \{a\}$. Then, the number of functions from $X' \to \{0, 1\}$ is 2^{n-1} by Theorem 2. Let $A' \subseteq X'$. We associate a subset $A \subseteq X$ as follows: If A' is an odd-sized subset, then set $A = A'$. Otherwise, set $A = A \cup \{a\}$. Hence, we have established a bijection between the number of odd-sized subsets of X and all subsets of $X \setminus \{a\}$. Therefore, the number of odd-sized subsets of X is 2^{n-1}. □

We provide an alternate proof.

Alternate proof: Let $\mathcal{O}_X, \mathcal{E}_X$ denote the odd-sized subsets and even-sized subsets, respectively of X. That is, $\mathcal{O}_X = \{S \in \mathcal{P}(X) : |S| \text{ is odd}\}$, and $\mathcal{E}_X = \{S \in \mathcal{P}(X) : |S| \text{ is even}\}$. Note that $\mathcal{O}_X$ and $\mathcal{E}_X$ form a *partition* of $\mathcal{P}(X)$, i.e.,

$$\mathcal{O}_X \cap \mathcal{E}_X = \emptyset$$
$$\mathcal{O}_X \cup \mathcal{E}_X = \mathcal{P}(X)$$

Thus, if we show that $|\mathcal{O}_X| = |\mathcal{E}_X|$, then it must be that $|\mathcal{O}_X| = |\mathcal{P}(X)|/2 = 2^{n-1}$. Let $X = \{x_1, \ldots, x_n\}$. Consider the function $f : \mathcal{O}_X \to \mathcal{E}_X$ defined as follows:

$$f(S) = \begin{cases} S \cup \{x_n\}, & x_n \notin S \\ S \setminus \{x_n\}, & x_n \in S \end{cases}$$

In other words, fix an element of X, say x_n. If a set $S \in \mathcal{O}_n$ contained x_n, it is mapped to the set $S \setminus \{x_n\}$, which has even cardinality and hence in $\mathcal{E}_n$. On the other hand, if $x_n \notin S$, we map S to the set $S \cup \{x_n\}$, which again is even; and hence in $\mathcal{E}_n$. It is easy to check that f is a bijection, which implies $|\mathcal{O}_n| = |\mathcal{E}_n|$ and we are done. □

Now we compute the number of injective functions from a finite set X to a set Y. Note that if there is an injective function, then necessarily $|X| \leq |Y|$.

Theorem 4

The number of injective functions from a set X of size n to a set Y of size m is

$$m^{\underline{n}} = m(m-1)\ldots(m-n+1)$$

If $m = n$, the number of functions is $m! = m(m-1)\ldots 1$.

Proof. We prove by induction on X. If $X = \emptyset$, then the empty function is injective. Suppose for $|X| = n-1$, the number of injective functions is as claimed. Consider a set $X = \{x_1, \ldots, x_n\}$ of size n. Let $X' = X \setminus \{x_n\}$. By the inductive hypothesis, the number of injective functions from X' to Y is $m^{\underline{n-1}} = m(m-1)\ldots(m-n+1)$. For each of the $m-1$ choices for x_n, we have by induction, $(m-1)^{\underline{n-1}}$ injective functions from X' to $Y \setminus \{f(x_n)\}$. Hence, the number of injective functions from X to Y is

$$\begin{aligned} m \cdot (m-1)^{\underline{n-1}} &= m(m-1)\ldots(m-n+1) \\ &= m^{\underline{n}} \end{aligned}$$

□

Exercise 3

How many 7 letter words with distinct letters can be formed with letters from the English alphabet?

Solution:
This is precisely the number of injective functions from a set of size 7 to a set of size 26, and is therefore given by $26^{\underline{7}} = 26(26-1)(26-2)\ldots(26-6)$.

Exercise 4

Determine the number of ordered pairs (A, B), where $A \subseteq B \subseteq X$, where $|X| = n$.

Exercise 5

Show that a natural number $n \geq 1$, has an odd number of divisors (including 1 and itself) if and only if $\sqrt{n}$ is an integer.

Exercise 6

Determine the number of surjective functions from a set X of size n to a set Y of size m.

2 Permutations

if $|X| = |Y|$, and $f : X \to Y$ is an injective function, it follows that f is a bijection. A bijective function $f : X \to X$ is called a *permutation*. By Theorem 4, the number of permutations of an n element set is $n!$.

We represent permutations in a two-row form as follows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

The first row consists of the elements of the set X and the second row lists $f(x)$ where f is the permutation. Sometimes, we use a shortened notation:

$$(2\ 1\ 4\ 3)$$

Another way of representing permutations is via their cycles. For example, if f is the permutation (4 5 3 2 9 0 1 7 6 8), which is represented in Figure 1. Using cycles, the permutation can also be represented as $((0, 4, 9, 8, 6, 1, 5)(2, 3)(7))$.

Exercise 7

How many permutations have a single cycle?

For a permutation, let p^2 denote the composition of p with itself, i.e., $p^2 = p \circ p$. Note that p^2 is a permutation as the composition of bijections is a bijection. Similarly, we define

$$p^k = \underbrace{p \circ p \ldots p}_{k \text{ times}}$$

Let *id* denote the *identity permutation*, i.e., the permutation that maps each element to itself. For a permutation p on n elements, let the *order* of a permutation be the smallest k such that $p^k = id$.

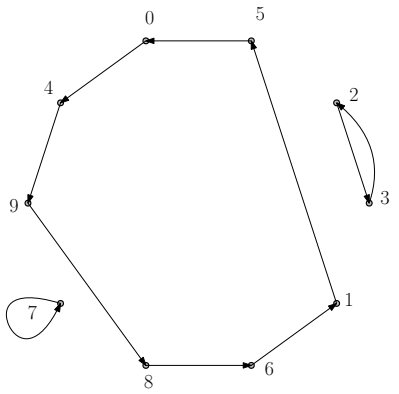

Figure 1: A cycle representation of the permutation (4 5 3 2 9 0 1 7 6 8)

Exercise 8

1. Prove that for any permutation on n elements, its order is finite.
2. If $p = C_1C_2 \dots C_\ell$ be a permutation written as a product of cycles $C_1C_2 \dots C_\ell$. What is the relation between $|C_i|$ and the order of a permutation?

2.1 Cyclic Permutations

In many settings, we are interested in counting the number of different ways we can place the elements of a set in a circular fashion. In this setting, any cyclic shift correspond to the same permutation.

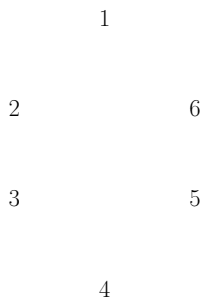

Figure 2: A cyclic permutation of $\{1, 2 \dots, 6\}$

For example, the set of permutations $123456, 234561, 345612, 456123, 561234, 612345$ all yield the same the of cyclic permutation in Figure 2. Thus, 6 permutations map to a single cyclic permutation. The number of cyclic permutations is therefore given as follows:

Theorem 5

The number of circular r-permutations of a set of n elements is given by

$$\frac{P(n,r)}{r} = \frac{n!}{r!(n-r)!}$$

In particular, the number of cyclic permutations of an n element set is $(n-1)!$

Exercise 9

In how many ways can ten students, two of whom do not wish to sit next to each other be seated around a round table?

Exercise 10

How many different necklaces can we make with 12 distinct beads? *Note: we could consider two cyclic sequences of beads to be identical if one can be obtained from the other by reflection, but we don't consider such operations. We only allow cyclic shifts.*

3 r-Permutations

An r-permutation of a set of n elements is a permutation of r elements of a set. The number of r permutations of a set of n elements is equal to the number of injective functions from an r element set to an n element set. Thus, the number of r-permutations of an n-element set, denoted $P(n,r)$ is given by

$$P(n,r) = n(n-1)\dots(n-r+1) = \frac{n!}{(n-r)!}$$

Exercise 11

In how many ways can we order the 26 letters of the English alphabet so that no two vowels, i.e., the letters $\{a,e,i,o,u\}$ appear consecutively?

Solution: The number of permutations of the 21 consonants is 21!. Since no two vowels are consecutive, they occupy the *gaps* between the consonants. There are 22 gaps between the consonants including the gap before the first consonant, or after the last consonant. The number of such permutations is given by

$$P(22,5) = \frac{22!}{(22-5)!} = \frac{22!}{17!}$$

Any permutation of the consonants and any choice of the permutation for the vowels yields a permutation such that no two vowels are consecutive. Therefore, the total number

of permutations is

$$21! \cdot \frac{22!}{17!}$$

Exercise 12

How many 7 digit numbers can be formed by using distinct digits such that the digits 5 or 6 do not appear consecutively?

Solution: Consider the set of all such numbers that can be formed: They can be classified into three types - those that don't contain either 5 or 6, those that contain exactly one of 5 or 6; and finally, those that contain both 5 and 6 but not consecutively. It will turn out to be easier to count these types separately.

The first type is easiest, there are 8 digits and since there is no restriction the number of 7 digit numbers that can be formed is $P(8,7) = 8!/(8-7)! = 8!$.

For the second type, we can again split into two types - those that contain only 5 and those that contain only 6. Their cardinalities are the same, and the number of each is $P(9,7) = 9!/2!$. Therefore, the total number of digits containing exactly one of 5 or 6 is $2 \cdot 9!/2!$.

Finally, for the third type, the argument is similar to the one in the problem above. There are $P(8,5) = 8!/3!$ permutations of 5 digits from the digits $\{0,\ldots,9\}\setminus\{5,6\}$. Since 5 and 6 do not appear consecutively, they occupy the 6 gaps between these digits. The number of ways in which we can place 5 and 6 so that they don't appear consecutively is therefore $P(6,2) = 6!/4!$. Hence, the total number of the third type is $8!/3!6!/4!$.

The total number of digits is therefore, the number of digits of each of the three types which is

$$8! + 2\frac{9!}{2!} + \frac{8!6!}{3!4!} = 8! + 9! + \frac{8!6!}{3!4!}$$

Exercise 13

How many orderings of a deck of 52 cards can we form if all cards of the same suit are together?

Exercise 14

How many distinct positive divisors do the following numbers have?

1. $3^4 \times 5^2 \times 7^6 \times 11$
2. 620

3. 10^10

Exercise 15

Determine the largest power of 10 that is a factor of the following numbers:

1. 50!
2. 1000!

4 r-Combinations

The number of unordered subsets of size r a set X of size n is called an r-combination. The number of r-combinations is given by the following argument. The number of r-permutations is $P(n,r)$. For any subset or r elements of X, they yield $r!$ distinct permutations. Therefore, the number of r combinations is $P(n,r)/r!$. The number of r-combinations, denoted $C(n,r)$, or more popularly as $\binom{n}{r}$ is given by:

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}$$

By symmetry, we can readily observe that the number of r-combinations of a set of size n is identical to the number of $n-r$-combinations. One way to see this is that there is a bijection between sets of size r and sets of size $n-r$ - for a set S of size r, we map it to the unique set $X \setminus S$ of size $n-r$. Alternately, this follows immediately from the symmetry of the function $C(n,r)$.

Proposition 1.

$$\binom{n}{r} = \binom{n}{n-r}$$

Proposition 2.

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

Proof. The number of subsets of a set of size n is 2^n as we proved earlier. We can partition the subsets by their size, and for size, their number is given by the number of r-combinations, i.e., $\binom{n}{i}$. □

We now prove a very useful identity that we'll see many times.

Theorem 6 (Pascal's identity)

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

Proof. The LHS counts the number of subsets of size r of a set X of size n. Fix a particular element $x \in X$. The subsets of size r can be partitioned into two types: those that contain x and those that don't. The number of subsets is therefore the sum of the cardinalities of the two types of subsets The number of the first type is $\binom{n-1}{r}$ as we are not allowed to choose the element x. The number of the second type is $\binom{n-1}{r-1}$, as we choose x into a subset, and then choose the remaining $r-1$ elements from the remaining $n-1$ elements. □

Of course, we can also prove the identity by painful algebraic manipulation. The proof given above is an example of a *combinatorial proof*, and to prove binomial identities, when we ask to show a binomial identity via a combinatorial argument, we mean an argument like the one above.

5 Multisets

A *multiset* is a generalization of a set, where we allow *multiplicites* of the elements. For example $\{2 \cdot a, 3 \cdot b, 1 \cdot c\}$ is a multiset containing two as, 3 bs and one c. Likewise $\{\infty \cdot a, \infty \cdot b\}$ is a multiset containing infinitely many as and infinitely many bs. When we say infinitely many, we always mean countably infinite. The elements a, b, c are called the *types*.

Theorem 7

Let S be a multiset with k types of objects, each of infinite multiplicity. The number of r-permutations of S is k^r.

Theorem 8

Let S be a multiset with objects of k different types with multiplicities $n_1, \ldots, n_k$. Let the set S be $n = n_1 + \ldots + n_k$. The number of permutations of S is given by

$$\frac{n!}{n_1! n_2! \ldots n_k!}$$