11 Learning How to Count

Definition 11.1: Finity.

finite Given an arbitrary set A, we say that A is *finite* if and only if $(\exists n \in \mathbb{N})(|A| \leqslant |n|)$. To be more explicit, this means that there exists a natural number $n \in \mathbb{N}$, and there exists a function $f : A \to \{w \in \mathbb{N} \mid w < n\}$, such that f is an *injection.*[1]

infinite Alternatively, we say that A is *infinite* if and only if A is *not finite;* this means that $(\forall n \in \mathbb{N})(|A| \not\leqslant |n|)$. Expanding this out: for *every* natural number $n \in \mathbb{N}$, and for *every* function $f : A \to \{w \in \mathbb{N} \mid w < n\}$, the function f is *not injective.* ⌟

[1] If we recall that $n = \{w \in \mathbb{N} \mid w < n\}$, we can abuse this set-theoretic implementation detail to simplify the notation and say that $f : A \to n$ is injective.

Lemma 11.1.

For any set X, if X is finite, then $(\exists! n \in \mathbb{N})(|n| = |X|)$. ⌟

Thanks to *Lemma 11.1*, all of the operations and concepts that we have defined recursively for natural numbers extend to arbitrary finite sets in natural ways. Fundamentally, this is because what *Lemma 11.1* really tells us is that finite sets can be lined up so that they look like an initial segment of the natural number line—finite sets can be *rearranged* so that some element is first, some other element is second, and so on until the last one. For example, if $\mathcal{I}$ is an arbitrary finite set—so that *Lemma 11.1* gives us a bijection $\eta : n \to \mathcal{I}$ for some $n \in \mathbb{N}$—and $f : \mathcal{I} \to \mathbb{N}$ is an arbitrary function associating elements of $\mathcal{I}$ to natural numbers, we can define what it means to take *the sum of $f(x)$ over all $x \in X$* by dealing with the composition $f \circ \eta : n \to \mathbb{N}$ as below.

$$\sum_{i \in \mathcal{I}} f(i) \coloneqq \sum_{i=0}^{n} (f \circ \eta)(i) = \sum_{i=0}^{n} f\big(\eta(i)\big)$$

The same idea generalizes to $\prod_{i \in \mathcal{I}} f(i)$ and other *"iterated"* operations.

Definition 11.2: Finite Cardinal Numbers.

When a set A is finite, we know there exists a unique natural number $n \in \mathbb{N}$ with the same cardinality as A, meaning $|n| = |A|$. In such situations, we often want to refer to and manipulate that number n that A is in bijection with directly. We therefore

$\#A$ introduce the notation $\#A$ to refer to *that unique natural number* bijective with A.

We refer to the number $\#A$ as the *cardinality of A.* Since $\#A$ is a number measuring the *"size"* of the set A, it is an example of what we call a *"(finite) cardinal number."*[2] Since every natural number $m \in \mathbb{N}$ measures the size of *some* finite set (*e.g.,* the set m itself), each of the natural numbers is a *"finite cardinal number."* Conversely, since every finite set is in bijection with a natural number, the set $\mathbb{N}$ is the set containing *all* of the *"finite cardinal numbers."* ⌟

[2] The idea of a *cardinal number* is that they are the numerical representatives of the *"sizes"* of collections of things. Because every thing in set theory has to be a set, we have to encode the cardinal numbers as sets if we want to reason about them in our framework. The most reasonable implementation for the finite cardinals is just the natural numbers that we already have; so, for example, the representative for the size of some set $\{a, b, c, d\}$ containing four distinct elements would be $\{0, 1, 2, 3\}$, which we have already conveniently associated with the concept of the *"arithmetical"* number 4.

Be careful to note that the above definition of $\#A$ only applies when the underlying set A is *finite!* More generally, there is a notion of *"cardinality"* for infinite sets as well, but these *"infinite cardinal numbers"* must obviously behave differently from natural numbers. As a prerequisite matter, we need to have a better understanding of infinite sets in general before we can hope to grasp what the *"infinite cardinal numbers"* are; we will discuss infinity in more detail later.

Theorem 11.1: The Set of Natural Numbers is Infinite.
$\mathbb{N}$ is an infinite set.

Proof. Towards a contradiction, suppose that $\mathbb{N}$ were *finite.* Using *Lemma 11.1*, this means that there exists a (unique) natural number $n \in \mathbb{N}$ and a function $f : n \to \mathbb{N}$ such that f is a bijection—in particular, f is a *surjection.* Now, thanks to the fact that $\mathfrak{dom}(f) = n = \{x \mid x \in \mathbb{N} \wedge x < n\}$ and $\mathfrak{cod}(f) = \mathbb{N}$, we can compute the sum of the outputs of f when evaluated over the points in its domain; we call this sum $\mathcal{S}$.

$$\mathcal{S} \coloneqq \sum_{i \in \mathfrak{dom}(f)} f(i) = \sum_{i=0}^{n-1} f(i)$$

Since $\mathcal{S} \in \mathbb{N}$, we also know that $\mathcal{S} + 1 \in \mathbb{N}$, and the surjectivity of f then tells us that there exists $k \in n$ such that $f(k) = \mathcal{S} + 1$. We can use this information to split the above sum at k, recognizing that any sum of natural numbers will be nonnegative.

$$\mathcal{S} = \sum_{i=0}^{n} f(i) = \underbrace{\left(\sum_{i=0}^{k-1} f(i) \right)}_{\geqslant 0} + f(k) + \underbrace{\left(\sum_{i=k+1}^{n-1} f(i) \right)}_{\geqslant 0} \geqslant 0 + f(k) + 0 = \mathcal{S} + 1$$

This shows that $\mathcal{S} \geqslant \mathcal{S} + 1$, contradicting the fact that $\mathcal{S} < \mathcal{S} + 1$. ↯
Therefore, $\mathbb{N}$ cannot be finite and must instead be infinite.

QED

11.1 Finite Combinatorics

Definition 11.3: Factorials.
$n!$ The *factorial function* is the recursively defined function $(\circlearrowleft)! : \mathbb{N} \to \mathbb{N}$ given below.

$$0! \coloneqq 1$$
$$\mathfrak{suc}(n)! \coloneqq \mathfrak{suc}(n) \cdot n!$$

Equivalently, we could write $n! = \prod_{i=1}^{n} i$ for $n \in \mathbb{N}$ if we recall $\prod_{i=1}^{0} i = 1$. ⌟

Theorem 11.2: Pigeonhole Principle.
Let A and B be arbitrary sets. The following three conditions then hold.

1. $|A| < |B|$ *iff* there *does not exist* a ***surjection*** $f : A \to B$.
2. $|A| > |B|$ *iff* there *does not exist* an ***injection*** $f : A \to B$.
3. If A and B are both finite, and $f : A \to B$ is an arbitrary function, then *there exists* an element of the codomain $b \in B$ with at least $\#(A)/\#(B)$ many preimages.

$$\#\Big\{a \;\Big|\; a \in A \wedge f(a) = b\Big\} \geqslant \left\lceil \frac{\#(A)}{\#(B)} \right\rceil = \left\lfloor \frac{\#(A) - 1}{\#(B)} \right\rfloor + 1$$

⌟

Lemma 11.2.
If A is a finite set and B is a set such that $B \subseteq A$, then B is also finite. ⌟

Corollary 11.1: Bounded Discrete Sets Are Finite.
For any $N \subseteq \mathbb{N}$, if $N \neq \varnothing$ and N is *bounded from above,*[1] then N is a finite set.
Similarly, for any $Z \subseteq \mathbb{Z}$, if $Z \neq \varnothing$ and Z is *bounded,*[2] then Z is finite. ⌟

[1] This means there exists some $u \in \mathbb{N}$ such that $(\forall n \in N)(n \leqslant u)$.

[2] When we say a set Z is *"bounded"* without further qualification, this means that Z is bounded from both *above and below.* When $Z \subseteq \mathbb{Z}$, we formally say there exist $\ell \in \mathbb{Z}$ and $u \in \mathbb{Z}$ such that $(\forall z \in Z)(\ell \leqslant z \leqslant u)$.

Corollary 11.2.
Let A be a finite set and B be an arbitrary set. The following all hold.

1. $\#(A \setminus B) \leqslant \#A$.
2. If B is finite, then $\#(A \setminus B) \geqslant \#A - \#B$.
3. If $B \subseteq A$, then $\#(A \setminus B) = \#A - \#B$. ⌟

Theorem 11.3: The Inclusion-Exclusion Theorem.
Let $n \in \mathbb{N}$, and suppose $\mathcal{A} = \{A_i \mid i \in \mathbb{N} \wedge 0 \leqslant i < n\}$ is a finite set, where each A_i is itself a finite set for each $i \in n$.

$$\#(\cup\mathcal{A}) \;=\; \sum_{\substack{B \subseteq \mathcal{A} \\ B \neq \varnothing}} (-1)^{\#B+1} \cdot \#(\cap B) \;=\; \sum_{\substack{J \subseteq n \\ J \neq \varnothing}} (-1)^{\#J+1} \cdot \#\left(\bigcap_{j \in J} A_j\right)$$ ⌟

Corollary 11.3.
If A and B are both finite, then $A \cup B$ is also finite and satisfies the following identity.

$$\#(A \cup B) \;=\; \#(A) + \#(B) - \#(A \cap B)$$ ⌟

Combinations

Definition 11.4: Combination.
combination Given a set X and $k \in \mathbb{N}$, we call Y a *k-combination of X iff* $Y \subseteq X$ and $|Y| = |k|$. ⌟

Definition 11.5: Binomial Coefficients.
$\binom{n}{k}$ For any natural numbers $n \in \mathbb{N}$ and $k \in \mathbb{N}$, we define the *binomial coefficient* $\binom{n}{k}$ to be the number of subsets of cardinality k that can be taken from an ambient set of cardinality n. More concretely: since only the sizes of the sets matter (as opposed to the identities of the elements of the sets), we define $\binom{n}{k}$ to be the number of subsets N of the natural number $n = \{m \mid m \in \mathbb{N} \wedge m < n\}$ satisfying $|N| = |k|$.

$$\binom{n}{k} \coloneqq \left\{ N \;\middle|\; N \subseteq \left\{ m \in \mathbb{N} \;\middle|\; m < n \right\} \wedge \#N = k \right\}$$

The number $\binom{n}{k}$ counts precisely the number of k-combinations of $\{0, ..., n-1\}$.[1] ⌟

[1] *N.B.* Informal "…" notation used here for visual purposes only.

Lemma 11.3.
For any $n \in \mathbb{N}$ and for any $k \in \mathbb{Z}$, if $k < 0$ or $n < k$, then $\binom{n}{k} = 0$. ⌟

Lemma 11.4.
For any $n \in \mathbb{N}$ and for any $k \in \mathbb{N}$, we have $\binom{n}{k} = \binom{n}{n-k}$. ⌟

Theorem 11.4: Pascal's Recurrence.
For any $n \in \mathbb{N}$ and $k \in \mathbb{N}$, the binomial coefficient $\binom{n}{k}$ satisfies the recurrence below.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad\qquad \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$$ ⌟

Theorem 11.5: Binomial Theorem.
For any $x \in \mathbb{R}$ and $y \in \mathbb{R}$, and for any $n \in \mathbb{N}$, we have the following.

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

Permutations

Definition 11.6: Permutation.
permutation Given a set X, a function $f : X \to X$ is called a *permutation on X iff f* is a bijection. ⌟

Lemma 11.5.
If A and B are finite sets, then $\#(A \times B) = \#A \cdot \#B$. ⌟

Theorem 11.6.
Let X and Y be arbitrary finite sets. There are $\#Y^{\#X}$ many functions from X to Y.

$$\#\Big\{f \;\Big|\; f : X \to Y\Big\} = \#Y^{\#X}$$

In particular, there are $\#X!$ many *permutations on X—i.e., bijections from X to X.*

$$\#\Big\{f \;\Big|\; f : X \to X \wedge f \text{ is a bijection}\Big\} = \#X!$$

⌟

Theorem 11.7.
The power set $\mathbb{P}(X)$ of any set X is bijective with the set of functions from X to $\{0, 1\}$.

$$\big|\mathbb{P}(X)\big| = \Big|\Big\{f \;\Big|\; f : X \to \{0, 1\}\Big\}\Big|$$

In particular, when X is finite, we have $\#\mathbb{P}(X) = 2^{\#X}$ thanks to *Theorem 11.6*. ⌟

Given a set $\mathcal{N}$ of cardinality $\#\mathcal{N} = n$, and given $k \in \mathbb{N}$, consider a subset $\mathcal{K} \subseteq \mathcal{N}$ of cardinality $\#\mathcal{K} = k$. We can associate $\mathcal{K}$ with those permutations on $\mathcal{N}$ that *split over* $\mathcal{K}$ as follows. Given a permutation $p : \mathcal{N} \to \mathcal{N}$, if it is possible to decompose p into two maps $p_k : \mathcal{K} \to \mathcal{K}$ and $p_{n\setminus k} : \mathcal{N} \setminus \mathcal{K} \to \mathcal{N} \setminus \mathcal{K}$ such that…

1. p_k is a bijection—meaning p_k is a permutation on $\mathcal{K}$,
2. $p_{n\setminus k}$ is a bijection—meaning $p_{n\setminus k}$ is a permutation on $\mathcal{N} \setminus \mathcal{K}$,
3. for $x \in \mathcal{N}$, both $\big(x \in \mathcal{K} \;\Rightarrow\; p(x) = p_k(x)\big)$ and $\Big(x \in \mathcal{N} \setminus \mathcal{K} \;\Rightarrow\; p(x) = p_{n\setminus k}(x)\Big)$

…then we will say that p *"splits,"* or *"factors,"* over the subset $\mathcal{K}$. When p splits over $\mathcal{K}$, this means we can represent the permutation p on $\mathcal{N}$ by stitching together a permutation p_k on $\mathcal{K}$ together with another, completely independent, permutation $p_{n\setminus k}$ on $\mathcal{N} \setminus \mathcal{K}$. There are precisely $k!$ many permutations on $\mathcal{K}$, and there are exactly $(n-k)!$ permutations on $\mathcal{N} \setminus \mathcal{K}$.[1] Each permutation on $f : \mathcal{K} \to \mathcal{K}$ can be thought of as *extending* to a permutation on all of $\mathcal{N}$ by stitching f together with one of the permutations $g : \mathcal{N} \setminus \mathcal{K} \to \mathcal{N} \setminus \mathcal{K}$.

[1] Therefore, there should be $k!(n-k)!$ permutations of $\mathcal{N}$ that split over $\mathcal{K}$.

This should begin to give you an idea as to how we could define an equivalence relation on the set of permutations on $\mathcal{N}$; the equivalence classes with respect to this equivalence relation are in bijection with the set of subsets of $\mathcal{N}$ that have cardinality equal to that of $\mathcal{K}$. While the generalizing this idea requires care, the following famous result makes this association more explicit when the sets involved are finite.

Theorem 11.8: Combinations Are Quotients of Permutations.
The identity below relates combinations and permutaitons for any $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

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

⌟