6 CARDINALITY OF SETS

We all have an idea of what it means to count a finite collection of objects, but we must be careful to define rigorously what it means for a set to have a given number of elements, not least because we must be able to apply the same ideas to infinite sets, where counting can get less intuitive. In this section we will encounter some familiar combinatorial results, but here we approach them in a rigorous way, giving proofs using our definition of the cardinality of a set.

Let \( n \in \mathbb{N} \). Define

\[
\mathbb{N}_n = \{1, 2, 3, \ldots, n\} = \{k \in \mathbb{N} : 1 \leq k \leq n\}.
\]

Let \( A \) be a set. We say \( A \) has cardinality \( n \) if there exists a bijection \( f : \mathbb{N}_n \to A \). In this case write \(|A| = n\).

Define \(|\emptyset| = 0\).

**Example:**

Let \( A = \{3, \pi, \sqrt{2}, 7\} \). Define \( f : \mathbb{N}_4 \to A \) by

\[
\begin{align*}
f(1) &= 3 \\
f(2) &= 7 \\
f(3) &= \pi \\
f(4) &= \sqrt{2}.
\end{align*}
\]

\( f \) is a bijection, so \(|A| = 4\).

Let \( A \) be a set. If \(|A| = n\) for some \( n \in \mathbb{N} \cup \{0\} \), then we say that \( A \) is finite. Otherwise we say \( A \) is infinite.

**Remarks:**

(i) Let \( A \) and \( B \) be sets. Then \(|A| = |B| \iff \exists \text{ bijection } f : A \to B\). It follows that our definition of the cardinality is well-defined (that is, it does not depend on the choice of bijection \( f \)).

(ii) If \( A \) and \( B \) are finite sets and \( A \subseteq B \), then \(|A| \leq |B|\). More generally, if there is a 1-1 map \( g : A \to B \), then \(|A| \leq |B|\). The contrapositive of this is the pigeonhole principle:

**Theorem 6.1 (Pigeonhole principle)** Let \( A \) and \( B \) be non-empty finite sets and let \( f : A \to B \). If \(|A| > |B|\), then there exist \( x_1, x_2 \in A \) with \( x_1 \neq x_2 \) and \( f(x_1) = f(x_2) \).
Example: In a group of 13 people, 2 will have a birthday in the same month.

Definition 6.2 Let $A$ be a set. We say that $A$ is countable if it is finite or if there exists a bijection $f : \mathbb{N} \rightarrow A$. In the latter case we say that $A$ is countable infinite.

Remark: An example of an uncountable set is $\mathbb{R}$, but that’s another story.

Example: $\mathbb{Z}$ is countable. To see this, take the bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$ defined as follows:

\[
\begin{align*}
f(1) &= 0 \\
f(2) &= 1 \\
f(3) &= -1 \\
f(4) &= 2 \\
f(5) &= -2 \\
f(6) &= 3 \\
f(7) &= -3 \\
f(8) &= 4 \\
f(9) &= -4 \\
&\text{etc.}
\end{align*}
\]

We will work towards the inclusion-exclusion principle for finding the size of a union of sets. We will do this in a number of stages.

Theorem 6.3 Let $X$ and $Y$ be finite sets such that $X \cap Y = \emptyset$ (we say that $X$ and $Y$ are disjoint).

Then $|X \cup Y| = |X| + |Y|$.

Proof. If $|X| = 0$, then $X = \emptyset$ and $X \cup Y = Y$, and the result holds. Similarly if $|Y| = 0$. Hence we may suppose that $|X| = m > 0$ and $|Y| = n > 0$. So there exist bijections $f : \mathbb{N}_m \rightarrow X$ and $g : \mathbb{N}_n \rightarrow Y$.

Define $h : \mathbb{N}_{m+n} \rightarrow X \cup Y$ by

\[
h(i) = \begin{cases} 
  f(i) & \text{if } 1 \leq i \leq m \\
  g(i-m) & \text{if } m+1 \leq i \leq m+n.
\end{cases}
\]

We claim that $h$ is a bijection.

$h$ is onto: Let $z \in X \cup Y$.

If $z \in X$, then $\exists j \in \mathbb{N}_m$ such that $f(j) = z$ (since $f$ is onto). So $h(j) = f(j) = z$.

If $z \in Y$, then $\exists j \in \mathbb{N}_n$ such that $g(j) = z$ (since $g$ is onto). So $h(m+j) = g(j) = z$.

In either case we have found an element mapping to $z$, so $h$ is onto.

$h$ is 1-1: Let $h(i) = h(j)$ for some $i, j \in \mathbb{N}_{m+n}$. Write $z = h(i) = h(j)$.

Since $z \in X \cup Y$ and $X \cap Y = \emptyset$, either $z \in X$ or $z \in Y$, but not both.

If $z \in X$ (i.e., $i, j \leq m$), then $h(i) = f(i)$ and $h(j) = f(j)$. Since $f$ is 1-1, we have $i = j$.

If $z \in Y$ (i.e., $i, j > m$), then $h(i) = g(i-m)$ and $h(j) = g(j-m)$. Since $g$ is 1-1, we have $i-m = j-m$, so $i = j$.

Hence $h$ is 1-1.

We have shown that $h$ is a bijection. So $|X \cup Y| = m + n = |X| + |Y|$. \qed
Corollary 6.4 Suppose that $X_1, \ldots, X_n$ are pairwise disjoint finite sets. Then $X_1 \cup \cdots \cup X_n = \bigcup_{i=1}^n X_i$ is a finite set and

$$|\bigcup_{i=1}^n X_i| = \sum_{i=1}^n |X_i|.$$ 

Proof. By induction on $n$, using Theorem 6.3. \hfill \Box

What if $X$ and $Y$ in Theorem 6.3 are not disjoint? We have the inclusion-exclusion principle, which turns out to be an application of Corollary 6.4.

Theorem 6.5 (Inclusion-exclusion principle) Let $X$ and $Y$ be finite sets. Then

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$ 

Proof. Note that $X \cup Y = (X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y)$, a union of pairwise disjoint sets.

By Corollary 6.4

$$|X \cup Y| = |X \setminus Y| + |Y \setminus X| + |X \cap Y|.$$ 

Now $X = (X \setminus Y) \cup (X \cap Y)$, a union of disjoint sets, so by Theorem 6.3

$$|X| = |X \setminus Y| + |X \cap Y|.$$ 

Similarly $|Y| = |Y \setminus X| + |X \cap Y|$. Substituting, we get

$$|X \cup Y| = (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| = |X| + |Y| - |X \cap Y|.$$

This can be generalized to more than two sets, as we will see later.

We now turn our attention to Cartesian products.

Theorem 6.6 Let $X$ and $Y$ be finite sets, with $|X| = m$ and $|Y| = n$. Then $X \times Y$ is a finite set and

$$|X \times Y| = mn.$$ 

Proof. Consider first the case $X = \emptyset$ or $Y = \emptyset$. Then $X \times Y = \emptyset$ and the result holds in this case.

Suppose that $X \neq \emptyset$ and $Y \neq \emptyset$.

Write $X = \{x_1, \ldots, x_m\}$. Then

$$X \times Y = \bigcup_{i=1}^m \{x_i\} \times Y.$$ 

Now $\forall \ i$, $|\{x_i\} \times Y| = |Y|$ (an easy exercise).

Note that the $\{x_i\} \times Y$ are pairwise disjoint (for distinct $x_i$), so the result follows by Corollary 6.4. \hfill \Box
Corollary 6.7 Let $X_1, \ldots, X_m$ be finite sets, where $|X_i| = n_i$ for each $i$. Then

$$|X_1 \times \cdots \times X_m| = n_1 n_2 \cdots n_m.$$ 

Proof. Use Theorem 6.6 and induction on $m$. \qed

We can now use these results to count functions.

Corollary 6.8 Let $X$ and $Y$ be non-empty finite sets, where $|X| = m$ and $|Y| = n$. Then the number of functions $X \to Y$ is $n^m$.

Proof. Write $X = \{x_1, \ldots, x_m\}$.

A function $f : X \to Y$ determines an element of $Y^m = Y \times \cdots \times Y$ by

$$(f(x_1), f(x_2), \ldots, f(x_m)).$$

Conversely, each element $(y_1, \ldots, y_m) \in Y^m$ determines an function $f : X \to Y$ by $\forall i, f(x_i) = y_i$. So (given our labelling $x_1, \ldots, x_m$) we have constructed a bijection $g : \{f : X \to Y \text{ is a function}\} \to Y^m$.

The result follows since $|Y^m| = |Y|^m = n^m$ by Corollary 6.7. \qed

Notation: For $n \in \mathbb{N}$, define $n! = n(n - 1) \ldots 2.1$. Define $0! = 1$

Theorem 6.9 Let $A$ and $B$ be finite sets with $|A| = |B| = n$. Then there are precisely $n!$ bijections $A \to B$. In particular, there are precisely $n!$ permutations of $A$.

Proof. We use induction on $n$. The result is clear for $n = 1$. Suppose that the result is true for $n = k$.

Suppose that $|A| = |B| = k + 1$. Fix $a \in A$. For each $b \in B$, count bijections $f : A \to B$ for which $f(a) = b$. By our assumption, there are $k!$ bijections $A \setminus \{a\} \to B \setminus \{b\}$. So there are $k!$ bijections $f : A \to B$ satisfying $f(a) = b$.

There are $k + 1$ choices for $b$, so the total number of bijections is $(k + 1)! = (k + 1)!$.

So by induction the result is true for all $n$. \qed

6.1 Counting subsets and the binomial theorem

Let $A$ be a set and $k \in \mathbb{N} \cup \{0\}$.

A $k$-subset of $A$ is a subset $X \subseteq A$ with $|X| = k$.

Write $P_k(A) = \{X \subseteq A : |X| = k\}$.

Consequently, if $|A| = n$, then

$$P(A) = \bigcup_{k=0}^{n} P_k(A).$$
We define \( \binom{n}{k} \) to be the cardinality \(|\mathcal{P}_k(\mathbb{N}_n)|\) of \( \mathcal{P}_k(\mathbb{N}_n) \).

\( \binom{n}{k} \) is called a binomial coefficient, or “\( n \) choose \( k \)”.

**WARNING:** This is the definition used in this course - we will see later that it is equivalent to a more familiar one.

**Remark:** If \( A \) is a set with \(|A| = n\), then \(|\mathcal{P}_k(A)| = |\mathcal{P}_k(\mathbb{N}_n)|\). Hence \( \binom{n}{k} \) is the number of \( k \)-element subsets of \( A \).

**Example:**
Let \( A = \{a, b, c\} \).
- \( \mathcal{P}_0(A) = \{\emptyset\} \) (so \( \binom{3}{0} = 1 \)).
- \( \mathcal{P}_1(A) = \{\{a\}, \{b\}, \{c\}\} \) (so \( \binom{3}{1} = 3 \)).
- \( \mathcal{P}_2(A) = \{\{a, b\}, \{b, c\}, \{a, c\}\} \) (so \( \binom{3}{2} = 3 \)).
- \( \mathcal{P}_3(A) = \{A\} \) (so \( \binom{3}{3} = 1 \)).

We collect some facts about \( \binom{n}{k} \):

**Lemma 6.10** Let \( n, k \in \mathbb{N} \cup \{0\} \). Then

(i) \( \binom{n}{k} = 0 \) if \( k > n \),

(ii) \( \binom{n}{0} = \binom{n}{n} = 1 \) and \( \binom{n}{1} = n \),

(iii) \( \binom{n}{k} = \binom{n}{n-k} \),

(iv) if \( 0 < k \leq n \), then

\[ \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \cdot \]

**Proof.** (i) and (ii) are clear.

(iii) \( f : \mathcal{P}_k(A) \to \mathcal{P}_{n-k}(A) \), \( f(X) = A \setminus X \) defines a bijection.

(iv) See exercises. \( \square \)

**Theorem 6.11** Let \( n, k \in \mathbb{N} \cup \{0\} \) with \( k \leq n \). Then

\[ \binom{n}{k} = \frac{n!}{k!(n-k)!} \]
**Proof.** Uses Lemma 6.10 and induction on $n$. See [IMR, 12.2.10].

If $n = 0$, then $k = 0$ and

$$\binom{0}{0} = 1 = \frac{0!}{0!0!},$$

so the result is true for $n = 0$.

If $n = 1$, then $k = 0$ or $k = 1$. In either case

$$\binom{1}{k} = 1 = \frac{1!}{1!0!}.$$

Suppose that the result is true for $n = m$ (and all $k$). We will show that it is true for $n = m + 1$.

Let $k \in \mathbb{N} \cup \{0\}$ with $0 \leq k \leq m + 1$.

If $k = 0$ or $k = m + 1$, then

$$\binom{m + 1}{k} = 1 = \frac{(m + 1)!}{0!(m + 1)!},$$

so we may assume that $1 \leq k \leq m$.

By Lemma 6.10

$$\binom{m + 1}{k} = \binom{m}{k} + \binom{m}{k - 1}$$

$$= \frac{m!}{k!(m-k)!} + \frac{m!}{(k-1)!(m-(k-1))!}$$

(since true for $m$)

$$= \frac{m!(m+1-k)}{k!(m+1-k)!} + \frac{m!k}{k!(m+1-k)!}$$

$$= \frac{(m+1)!}{k!(m+1-k)!}$$

So the result is true for $m + 1$. Hence by induction the result is true for all $n$. 

\[\square\]

An application of this is:

**Theorem 6.12 (Binomial theorem)** Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{R}$. Then

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$ 

**Sketch proof.**

$$(a + b)^n = \underbrace{(a + b) \ldots (a + b)}_{n \text{ times}}.$$ 

Label the factors on the right hand side $1, \ldots, n$.

$(a + b)^n$ is obtained as a sum of $2^n$ products, each of which is a product of $n$ $a$’s and $b$’s.

Each product corresponds to a subset $X$ of $\mathbb{N}_n = \{1, \ldots, n\}$ defined by $i \in X$ if and only if the product involves $a$ from factor $i$. 

6
Let $k \in \mathbb{Z}$ with $0 \leq k \leq n$. Then $X \in \mathcal{P}_k(\mathbb{N}_n)$ if and only if the corresponding product is $a^k b^{n-k}$.

So the number of times that $a^k b^{n-k}$ occurs in $(a+b)^n$ is $|\mathcal{P}_k(\mathbb{N}_n)| = \binom{n}{k}$. \qed

### 6.2 Bonus nonexaminable material

Recall that a set $A$ is countable if either $A$ is finite or there is a bijection $\mathbb{N} \to A$.

(i) There is a bijection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

The bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is given by

\[
\begin{align*}
 f(1) &= (1, 1), \\
 f(2) &= (2, 1), \\
 f(3) &= (1, 2), \\
 f(4) &= (1, 3), \\
 f(5) &= (2, 2), \\
 f(6) &= (3, 1), \\
 f(7) &= (4, 1), \\
 f(8) &= (3, 2), \\
 f(9) &= (2, 3), \\
 f(10) &= (1, 4), \\
 &\text{etc.}
\end{align*}
\]

By induction, for all $n \in \mathbb{N}$, there is a bijection $\mathbb{N} \to \mathbb{N}^n$, i.e., $\mathbb{N}^n$ is countable.

More generally, a finite Cartesian product of countable sets is countable.

(ii) Existence of non-countable sets

**Theorem 6.13 (Cantor)** Let $A$ be a set. Then there is no onto map $A \to \mathcal{P}(A)$.

**Proof.** Suppose that $f : A \to \mathcal{P}(A)$ is onto.

Let $x \in A$. Note that $f(x) \subseteq A$, and so either $x \in f(x)$ or $x \notin f(x)$. This allows us to define a subset

\[ S = \{ x \in A : x \notin f(x) \} \subseteq A. \]

Now since $f$ is onto, there is $a \in A$ such that $f(a) = S$.

Suppose that $a \in f(a)$. Then $a \in S$ since $f(a) = S$, so by definition of $S$ we have $a \notin f(a)$, a contradiction.

Hence $a \notin f(a)$. But then $a \in S$ by definition of $S$, and so $a \in f(a)$ since $S = f(a)$, a contradiction. \qed

**Corollary 6.14** $\mathcal{P}(\mathbb{N})$ is not countable.

**Proof.** Suppose that $\mathcal{P}(\mathbb{N})$ is countable.

Then there is a bijection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

Then $f$ is onto, a contradiction by the Theorem. \qed