CS1200 Module-3: Counting & Algebraic Structures

Let's begin with an easy counting problem:

Question: How many subsets are there for a set S of cardinality n? (that is, $|S| = n$).

In other words, if $|S| = n$ then what is $|\mathcal{P}(S)|$?

$\downarrow$

(power set of S: collection of all subsets of S)

Perhaps, you already know the answer. It's okay. We will solve using bijections.

Plan: We will establish a bijection between $\mathcal{P}(S)$ and 0-1 vectors of length n.

$n := |S|$.

Let us label the elements of S as $s_1, s_2, \ldots, s_n$.

Let X denote the set of all 0-1 vectors of length n.

means vector whose each component is 0 or 1.

We define $f: \mathcal{P}(S) \to X$ as follows:

$$f(T) := (a_1, a_2, \ldots, a_n)$$

$$\text{where } a_i := \begin{cases} 1 & \text{if } s_i \in T \\ 0 & \text{if } s_i \notin T \end{cases}$$

DIY: Prove that f is indeed a bijection.

It follows from our discussion (in Module-1) that $|\mathcal{P}(S)| = |X|$.

Counting $|X|$ is quite easy.

$\downarrow$

set of all 0-1 vectors of length n

$\downarrow$

Each vector in this set has n components, and each component is either 0 or 1. So, for each component, we have 2 choices.

(where $|S|=n$).

Thus, $|X| = 2^n$. Thus, $|\mathcal{P}(S)| = 2^n$.

One may argue that counting $|\mathcal{P}(S)|$ is equally easy.

Sure.

We will see more interesting examples...

Notation: In fact, many authors/books use the notation 2^S for power set of S, and this is also why it is called power set!

(S is a set!)

We will use $\mathcal{P}(S)$.

So, we have proved the following theorem.

Theorem: For $n \in \mathbb{N}$, the number of subsets of an n-element set is 2^n. $\blacksquare$

Now, let's ask a more difficult question:

Question: For $n \in \mathbb{N} - \{0\}$, how many subsets of odd cardinality are there for an n-element set?

If you try some examples, or even otherwise, you may be tempted to guess that the answer is 2^{n-1}, and this turns out to be true. We will prove this by establishing a bijection between 2 sets A & $\mathbb{B}$.

the set we want to count

some set we already know how to count.

Note that 2^{n-1} is the # of subsets of a set of cardinality $n-1$. This gives us some hint for the definition of set $\mathbb{B}$.

Let S be a set of cardinality n where $n \geq 1$, and let $x \in S$ denote a fixed element of S (chosen arbitrarily).

We define $\mathbb{B}$ to be the set of all subsets of $S-x$.
(By previous theorem, $|\mathbb{B}| = 2^{n-1}$ since $|S-x| = n-1$.)

We define A to be the set of all subsets of S of odd cardinality. Thus,

$$A := \{T \in \mathcal{P}(S) : |T| \text{ is odd}\}$$

the set we want to count!

We define a function $f : \mathcal{B} \to \mathcal{A}$ as follows:

For $B \in \mathcal{B}$: (set of all subsets of $S - x$)

$$f(B) := \begin{cases} B & \text{if } |B| \text{ is odd} \\ B \cup \{x\} & \text{if } |B| \text{ is even} \end{cases}$$

Observe that, in both cases, $f(B)$ is an element of $\mathcal{A}$

(set of all subsets of S of odd cardinality)

Next Goal: To prove that f is indeed a bijection.

How do we do this?

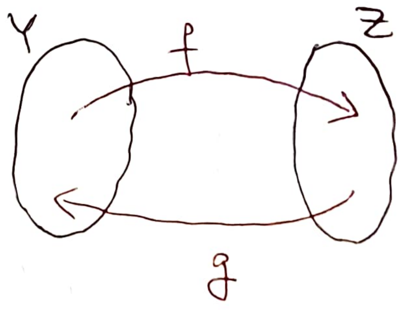
There are many ways to show that a function $f : Y \to Z$ (where Y & Z are finite sets) is a bijection. One way is to argue that f is 1-to-1 and onto. (DIY: what are some other ways?)

We will use a different approach this time.

such a function is called an inverse of f.

Invertible Functions: A function $f : Y \to Z$ is said to be $\boxed{\text{invertible}}$ if $\exists$ a function $g : Z \to Y$ such that f & g satisfy the following:

$$g(f(y)) = y \quad \forall y \in Y$$
$$f(g(z)) = z \quad \forall z \in Z$$



CS1200 Module -3: Counting & Algebraic Structures

DIY:
1. Prove that a function is a bijection if and only if it is invertible.
2. Prove that, for a function f, if an inverse of f exists then it is unique!

Caution: when proving that a function f is invertible, you should NOT use notation f^{-1}! This is misleading.

Due to this, it is customary AND okay to use f^{-1} to denote $\boxed{\text{the}}$ inverse of f when it exists.

First you need to show that the function f is invertible or a bijection. ONLY after that, you may use the notation f^{-1}!

We will show that $f : \mathcal{B} \to \mathcal{A}$ (defined on previous page) is invertible by defining a function g as follows:

$g : \mathcal{A} \to \mathcal{B}$ is defined as:

For $A \in \mathcal{A}$: → set of all subsets of S of odd cardinality

$$g(A) := \begin{cases} A & \text{if } x \notin A \\ A - x & \text{if } x \in A \end{cases}$$

Observe that, in both cases, $g(A)$ is an element of $\mathcal{B}$

(set of all subsets of $S - x$)

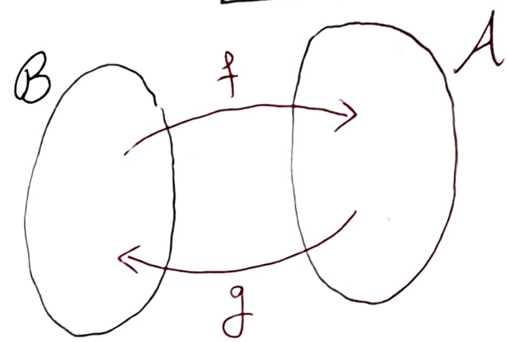
CS1200 Module-3: Counting & Algebraic Structures

Next goal: To prove that f & g satisfy the following:

1. $g(f(B)) = B \quad \forall B \in \mathcal{B}$
2. $f(g(A)) = A \quad \forall A \in \mathcal{A}$

$f : \mathcal{B} \to \mathcal{A}$
$g : \mathcal{A} \to \mathcal{B}$

We will prove that f & g satisfy 1:



Let $B \in \mathcal{B}$.

Case 1: $|B|$ is odd.

$f(B) = B$ (by defn of f)

Since $x \notin B$ (why?), $g(f(B)) = B$. (by defn of g)

Case 2: $|B|$ is even.

$f(B) = B \cup \{x\}$ (by defn of f)

Since $x \in f(B)$ and $f(B) = B \cup \{x\}$, $g(f(B)) = f(B) - x$ (by defn of g)

$= (B \cup \{x\}) - x$

$= B$

Thus, in all cases, $g(f(B)) = B$.

DIY: Prove that f & g satisfy 2.

This proves that f is invertible.

By DIY Theorem, f is a bijection. Thus, $|\mathcal{A}| = |\mathcal{B}|$.

However, $|\mathcal{B}| = 2^{n-1}$. Thus, $|\mathcal{A}| = 2^{n-1}$. This proves the following theorem.

Theorem: For $n \in \mathbb{N} - \{0\}$, the number of subsets of odd cardinality (of an n-element set) equals 2^{n-1}.