ITCS 531: Counting - Cardinal numbers

Rob Egrot

What is a set?

- A **set** is a collection of objects.
- E.g. the natural numbers, the real numbers, the integers etc. are all sets.
- So is something like $\{1, 2, 5, 11, 6\}$.
- Sets don't just contain numbers.
- We can have e.g. the set of all students in this class, the set of all toasters made in Germany etc.
- We can also define sets arbitrarily, e.g. the set that contains my left shoe, the set of all prime numbers, and the current president of France.
- Notice that in the previous example a set contains another set as a member.

When are two sets the same?

- Sets are unordered collections that contain no duplicates.
- Two sets are the same (equal) if they have exactly the same members.
- So there may be multiple ways to define the same set.
- E.g. The set of all natural numbers greater than 1 is the same as the set of all possible products of prime numbers.
- There's a special set that contains nothing, the **empty set**, $\emptyset$.

Defining sets from other sets

- Given a set X we can define the powerset $\wp(X) = \{S : S \subseteq X\}$, the set of all subsets of X.
- Given sets X and Y we can define things like the union $X \cup Y$ and intersection $X \cap Y$.
- If I is an *indexing set*, that is, a set we use just to label things, and for each $i \in I$ there is a set X_i, then we can take the infinite union $\bigcup_I X_i$ and the infinite intersection $\bigcap_I X_i$.
- There are also other ways we can build sets from other sets. E.g. if X is a set, and each element $x \in X$ is associated with some other object, y_x say, then $\{y_x : x \in X\}$ is a set too.

Set theory as a foundation for mathematics

- Gottlob Frege and Bertrand Russell wanted to use the idea of a set to formalize mathematics.
- So the results of mathematics could be derived just by thinking hard enough about the logic of sets.
- They wanted to do this for philosophical reasons related to the work of the German idealist philosopher Immanuel Kant.
- They believed it is a fact of pure logic that every concept defines a set. I.e., if P is a property of objects, then I can define the set of all the things that P applies to (in symbols $\{x : P(x)\}$).

Russell's paradox

- The problem with this assumption is that it leads to a contradiction.
- Some sets are members of themselves, e.g. the set of all abstract ideas. Other sets are not, e.g. the set of all chocolate biscuits.
- So 'not being a member of itself' is a property of sets.
- Let X be the set of all sets that are not members of themselves.
- Suppose X is a member of itself. Then, by the definition of X, it must also not be a member of itself.
- On the other hand, if X is not a member of itself, then, again by definition of X, it must be a member of itself after all.
- This contradiction reveals that not all properties can define sets.

The consequences of Russell's paradox

- Russell's paradox tells us we can't naively assume that every property defines a set.
- So to be safe mathematicians must restrict the notion of 'set'. This gives us what we know as *ZFC* set theory, which we can define as a theory in first-order logic.
- This is a hack, but it produces enough sets for the (most of) the needs of mathematicians, and seems to block the paradoxes of naive set theory (Russell's paradox is just one of these).
- To avoid his paradox, Russell and others developed the foundations of mathematical logic in the early 20th century.

Comparing the sizes of sets

- If X, Y are sets, a function $f : X \to Y$ is:
  - *1-1 (injective)* if for all $y \in Y$ there is *at most* one $x \in X$ with $f(x) = y$.
  - *onto (surjective)* if for all $y \in Y$ there is *at least* one $x \in X$ with $f(x) = y$.
  - *bijective* if it is both 1-1 and onto.
- We say X is *at most as big* as Y if there is a 1-1 function $f : X \to Y$.
- We write $|X| \leq |Y|$.
- If X and Y are finite then $|X| \leq |Y|$ according to this definition if and only if X is actually at most as big as Y as we usually understand it.
  - Because if $X = \{x_1, \ldots, x_k\}$ and $Y = \{y_1, \ldots, y_n\}$ with $k \leq n$ we can define $f : X \to Y$ by $f(x_i) = y_i$ for $i \in \{1, \ldots, k\}$.

Defining cardinality

Fact 1

1. *$|X| \leq |Y| \iff$ there is an onto (surjective) function from Y to X.*
2. *(Cantor-Bernstein theorem). $|X| = |Y| \iff$ there is a bijection between X and Y.*
3. *Given two sets X and Y, either $|X| \leq |Y|$ or $|Y| \leq |X|$, or both.*

Definition 2 (cardinality)

We define the *cardinality* of X to be the equivalence class defined by $|X|$.

Why is this useful?

- This definition of cardinality agrees with the usual one for finite sets.
- I.e., if X and Y are finite then $|X| = |Y|$ if and only if X and Y have the same number of elements.
- So, for example, if X has 3 elements, then $|X|$ contains every set that has 3 elements.
- We can use this as a definition for the number 3.
- But this definition also applies to infinite sets, for example $\mathbb{N}$.
- $\mathbb{N}$ is obviously bigger than every finite set, but what about other infinite sets?

$\mathbb{N}$ and $\mathbb{Z}$

Theorem 3

$|\mathbb{N}| = |\mathbb{Z}|$.

Proof.

We define a bijection $f : \mathbb{Z} \to \mathbb{N}$ as follows.

$$f(z) = \begin{cases} 2z \text{ when } z \geq 0 \\ 2|z| - 1 \text{ when } z < 0 \end{cases}$$

$\square$

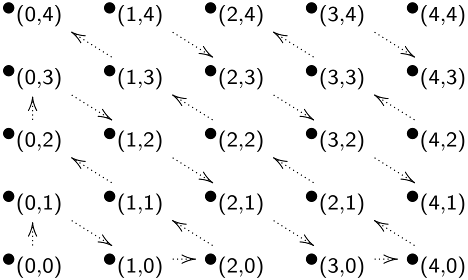
$\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$

Theorem 4

$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Proof.

- $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $f(n) = (n, n)$ is clearly 1-1.
- If we define a 1-1 function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ then fact 1(2) says $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. We get g by listing the elements of $\mathbb{N} \times \mathbb{N}$:



□

$\mathbb{N}$ and $\mathbb{Q}$

Corollary 5

$|\mathbb{N}| = |\mathbb{Q}|$.

Proof.

- Since $\mathbb{N} \subset \mathbb{Q}$ the inclusion function is an injection from $\mathbb{N}$ to $\mathbb{Q}$, so we just need to find a 1-1 function $\mathbb{Q} \to \mathbb{N}$.
- Let $h : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ be defined by

$$h(q) = \begin{cases} (0,0) \text{ when } q = 0 \\ (a,b) \text{ when } \frac{a}{b} \text{ is the most reduced form of } q \end{cases}$$

- Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function from theorem 4.
- Let $f_1, f_2 : \mathbb{Z} \to \mathbb{N}$ be copies of the function f from theorem 3.
- Then $g \circ (f_1, f_2) \circ h : \mathbb{Q} \to \mathbb{N}$ is 1-1 as g, f and h are.

$$\mathbb{Q} \xrightarrow{h} \mathbb{Z} \times \mathbb{Z} \xrightarrow{(f_1,f_2)} \mathbb{N} \times \mathbb{N} \xrightarrow{g} \mathbb{N}$$

□

$\mathbb{N}$ and $\mathbb{R}$

Theorem 6

$|\mathbb{N}| < |\mathbb{R}|$.

Proof:

- Since $\mathbb{N} \subset \mathbb{R}$ we know that $|\mathbb{N}| \leq |\mathbb{R}|$ as the inclusion function is 1-1.
- We will show that $|\mathbb{N}| \neq |\mathbb{R}|$ by proving that there is no onto function from $\mathbb{N}$ to $\mathbb{R}$.
- Let f be a function from $\mathbb{N}$ to the interval $(0, 1) \subset \mathbb{R}$.
- We will show that there is an $x \in (0, 1)$ such that $f(n) \neq x$ for all $n \in \mathbb{N}$.
- This proof technique is known as *Cantor's diagonal argument*, or just *the diagonal argument*.

Theorem 6 proof continued

- Every number in $(0, 1)$ can be expressed as an infinite decimal expansion, e.g. $0.x_1x_2x_3\ldots$, where x_n is the nth digit.
- Define $y = 0.y_1y_2y_3\ldots$ by defining the digits as follows:

$$y_n = \begin{cases} 7 \text{ if the } n\text{th digit of } f(n) \text{ is not } 7 \\ 3 \text{ if the } n\text{th digit of } f(n) \text{ is } 7 \end{cases}$$

- Then, by definition, the nth digit of y is different from the nth digit of $f(n)$ for all n, and so $y \neq f(n)$ for all $n \in \mathbb{N}$.
- So f cannot be onto.
- Since there's no onto function $\mathbb{N} \to (0, 1)$, there's no onto function $\mathbb{N} \to \mathbb{R}$ either.
- So $|\mathbb{N}| < |\mathbb{R}|$.

Countable and uncountable sets

- We have seen there's at least one set bigger than $\mathbb{N}$.

Definition 7 (countable)

A set X is *countable* if $|X| \leq |\mathbb{N}|$. Otherwise it is *uncountable*.

- It turns out that there's a never ending increasing hierarchy of uncountable cardinals.
- You'll see a justification for this by thinking about powersets in the exercises.
- This is just the tip of the iceberg.
- Understanding this hierarchy is part of the work of modern set theorists.

Cardinal arithmetic

- Given disjoint sets X and Y, we extend the familiar arithmetic operations as follows:
  - $|X| + |Y| = |X \cup Y|$.
  - $|X| \times |Y| = |X \times Y|$.
  - $|X|^{|Y|} = |X^Y|$ (here X^Y stands for the set of functions from Y to X).
- You'll see in the exercises that these operations agree with the usual ones for finite sets.

Powersets and exponentials

Proposition 8

If X is a set, then $|\wp(X)| = |2^X|$, where 2 is the two element set $\{0,1\}$.

Proof.

- We define a bijection g from $\wp(X)$ to 2^X by $g(S) = f_S$, where $f_S : X \to \{0,1\}$ is defined by setting

$$f_S(x) = \begin{cases} 1 \text{ when } x \in S \\ 0 \text{ otherwise.} \end{cases}$$

- f_S is known as the *characteristic function* of S.
- g is well defined because every set $S \subseteq X$ defines a unique f_S.
- It is clearly 1-1, and it is onto because given $f : X \to 2$ we can define $S_f = \{x \in X : f(x) = 1\}$, and then $g(S_f) = f$.

$\square$

The continuum hypothesis

Fact 9
$|\mathbb{R}| = |2^{\mathbb{N}}|$.

- We know that $|\mathbb{N}| < |\mathbb{R}| = |2^{\mathbb{N}}|$.
- Is there a set Y such that $|\mathbb{N}| < |Y| < |\mathbb{R}|$?.
- Cantor, the founder of set theory, believed the answer is no.
- This idea that there is no such Y is the *continuum hypothesis*.
- It turns out that the continuum hypothesis (CH) can neither be proved nor disproved using the ZFC axioms.
- Gödel showed that it can not be disproved in 1940, and, in 1963, Cohen showed that it can not be proved either.
- The basic idea is that there are models of ZFC where CH is true, and others where it is false.