Finite sets definition

Definition: A **finite** set is one whose distinct elements can be counted by a natural number.

Cardinality motivation

Motivating question: when can we say one set is *bigger than* another?

Which is bigger?

- The set $\{1, 2, 3\}$ or the set $\{0, 1, 2, 3\}$?
- The set $\{0, \pi, \sqrt{2}\}$ or the set $\{\mathbb{N}, \mathbb{R}, \emptyset\}$?
- The set $\mathbb{N}$ or the set $\mathbb{R}^+$?

Which of the sets above are finite? infinite?

Cardinality rationale for functions

Key idea for cardinality: Counting distinct elements is a way of labelling elements with natural numbers. This is a function! In general, functions let us associate elements of one set with those of another. If the association is "*good*", we get a correspondence between the elements of the subsets which can relate the sizes of the sets.

Cardinality power sets

Recall: When U is a set, $\mathcal{P}(U) = \{X \mid X \subseteq U\}$

Key idea: For finite sets, the power set of a set has strictly greater size than the set itself. Does this extend to infinite sets?

Definition: For two sets A, B, we use the notation $|A| < |B|$ to denote $(\; |A| \leq |B| \;) \land \neg(\; |A| = |B|)$.

$\emptyset = \{\}$	$\mathcal{P}(\emptyset) = \{\emptyset\}$	$\lvert\emptyset\rvert < \lvert\mathcal{P}(\emptyset)\rvert$
$\{1\}$	$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$	$\lvert\{1\}\rvert < \lvert\mathcal{P}(\{1\})\rvert$
$\{1, 2\}$	$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$	$\lvert\{1, 2\}\rvert < \lvert\mathcal{P}(\{1, 2\})\rvert$

$\mathbb{N}$ and its power set

Example elements of $\mathbb{N}$

Example elements of $\mathcal{P}(\mathbb{N})$

Claim: $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$

Claim: There is an uncountable set. Example: ________

Proof: By definition of countable, since ________ is not finite, **to show** is $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$.

Rewriting using the definition of cardinality, **to show** is

Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

To show: f is not a bijection. It's enough to show that f is not onto.

Rewriting using the definition of onto, **to show**:

$$\neg \forall B \in \mathcal{P}(\mathbb{N})\ \exists a \in \mathbb{N}\ (\ f(a) = B\ )$$

. By logical equivalence, we can write this as an existential statement:

____

In search of a witness, define the following collection of nonnegative integers:

$$D_f = \{n \in \mathbb{N} \mid n \notin f(n)\}$$

. By definition of power set, since all elements of D_f are in $\mathbb{N}$, $D_f \in \mathcal{P}(\mathbb{N})$. It's enough to prove the following Lemma:

Lemma: $\forall a \in \mathbb{N}\ (\ f(a) \neq D_f\ )$.

Proof of lemma:

By the Lemma, we have proved that f is not onto, and since f was arbitrary, there are no onto functions from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$. QED

Where does D_f come from? The idea is to build a set that would "disagree" with each of the images of f about some element.

$n \in \mathbb{N}$	$f(n) = X_n$	Is $0 \in X_n$?	Is $1 \in X_n$?	Is $2 \in X_n$?	Is $3 \in X_n$?	Is $4 \in X_n$?	...	Is $n \in D_f$?
0	$f(0) = X_0$	**Y / N**	Y / N	Y / N	Y / N	Y / N	...	**N / Y**
1	$f(1) = X_1$	Y / N	**Y / N**	Y / N	Y / N	Y / N	...	**N / Y**
2	$f(2) = X_2$	Y / N	Y / N	**Y / N**	Y / N	Y / N	...	**N / Y**
3	$f(3) = X_3$	Y / N	Y / N	Y / N	**Y / N**	Y / N	...	**N / Y**
4	$f(4) = X_4$	Y / N	Y / N	Y / N	Y / N	**Y / N**	...	**N / Y**
$\vdots$								

Cardinality rationals reals

Comparing $\mathbb{Q}$ and $\mathbb{R}$

Both $\mathbb{Q}$ and $\mathbb{R}$ have no greatest element.

Both $\mathbb{Q}$ and $\mathbb{R}$ have no least element.

The quantified statement

$$\forall x \forall y (x < y \to \exists z (x < z < y))$$

is true about both $\mathbb{Q}$ and $\mathbb{R}$.

Both $\mathbb{Q}$ and $\mathbb{R}$ are infinite. But, $\mathbb{Q}$ is countably infinite whereas $\mathbb{R}$ is uncountable.

The set of real numbers

$\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$

Order axioms (Rosen Appendix 1):

Reflexivity	$\forall a \in \mathbb{R} (a \leq a)$
Antisymmetry	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ (\ (a \leq b\ \wedge\ b \leq a) \to (a = b)\ )$
Transitivity	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ \forall c \in \mathbb{R}\ (\ (a \leq b \wedge b \leq c)\ \to\ (a \leq c)\ )$
Trichotomy	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ (\ (a = b\ \vee\ b > a\ \vee\ a < b)$

Completeness axioms (Rosen Appendix 1):

Least upper bound	Every nonempty set of real numbers that is bounded above has a least upper bound
Nested intervals	For each sequence of intervals $[a_n, b_n]$ where, for each n, $a_n < a_{n+1} < b_{n+1} < b_n$, there is at least one real number x such that, for all n, $a_n \leq x \leq b_n$.

Each real number $r \in \mathbb{R}$ is described by a function to give better and better approximations

$$x_r : \mathbb{Z}^+ \to \{0,1\} \qquad \text{where } x_r(n) = n^{th} \text{ bit in binary expansion of } r$$

r	Binary expansion	x_r
0.1	$0.00011001\ldots$	$x_{0.1}(n) = \begin{cases} 0 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 2 \\ 0 & \text{if } n = 1 \text{ or if } n > 1 \text{ and } (n \textbf{ mod } 4) = 3 \\ 1 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 0 \\ 1 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 1 \end{cases}$
$\sqrt{2} - 1 = 0.4142135\ldots$	$0.01101010\ldots$	Use linear approximations (tangent lines from calculus) to get algorithm for bounding error of successive operations. Define $x_{\sqrt{2}-1}(n)$ to be n^{th} bit in approximation that has error less than $2^{-(n+1)}$.

Claim: $\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is uncountable.

Approach 1: Mimic proof that $\mathcal{P}(\mathbb{Z}^+)$ is uncountable.

Proof: By definition of countable, since $\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is not finite, **to show** is $|\mathbb{N}| \neq |\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}|$.

To show is $\forall f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\} \ (f \text{ is not a bijection})$. Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$. **To show**: f is not a bijection. It's enough to show that f is not onto. Rewriting using the definition of onto, **to show**:

$$\exists x \in \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\} \ \forall a \in \mathbb{N} \ (\ f(a) \neq x \ )$$

In search of a witness, define the following real number by defining its binary expansion

$$d_f = 0.b_1 b_2 b_3 \cdots$$

where $b_i = 1 - b_{ii}$ where b_{jk} is the coefficient of 2^{-k} in the binary expansion of $f(j)$. Since[1] $d_f \neq f(a)$ for any positive integer a, f is not onto.

Approach 2: Nested closed interval property

To show $f : \mathbb{N} \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is not onto. **Strategy**: Build a sequence of nested closed intervals that each avoid some $f(n)$. Then the real number that is in all of the intervals can't be $f(n)$ for any n. Hence, f is not onto.

Consider the function $f : \mathbb{N} \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ with $f(n) = \frac{1+\sin(n)}{2}$

n	$f(n)$	Interval that avoids $f(n)$
0	0.5	
1	0.920735...	
2	0.954649...	
3	0.570560...	
4	0.121599...	
$\vdots$		

Cardinality uncountable examples

- The power set of any countably infinite set is uncountable. For example:

$$\mathcal{P}(\mathbb{N}), \mathcal{P}(\mathbb{Z}^+), \mathcal{P}(\mathbb{Z})$$

  are each uncountable.

- The closed interval $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$, any other nonempty closed interval of real numbers whose endpoints are unequal, as well as the related intervals that exclude one or both of the endpoints.

- The set of all real numbers $\mathbb{R}$ is uncountable and the set of irrational real numbers $\overline{\mathbb{Q}}$ is uncountable.

[1] There's a subtle imprecision in this part of the proof as presented, but it can be fixed.