INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

9. Uncountable sets and power sets

Definition. A set X is called uncountable if it is infinite but not countable.

We want to show that $\mathbb{R}$ is uncountable. To do this we will show that the interval $(0,1) = \{x \in \mathbb{R} : \ 0 < x < 1 \ \}$ is uncountable; as an exercise one shows that there is a bijection between the interval $(0,1)$ and $\mathbb{R}$.

We assume that every real number between 0 and 1 has a decimal expansion of the form

$$0.a_1a_2a_3\cdots = \sum_{k\in\mathbb{Z}_+} a_k 10^{-k}$$

where $a_k \in \{0,1,2,3,4,5,6,7,8,9\}$ for each $k \in \mathbb{Z}_+$. Note that

$$\begin{aligned} 0.999\cdots &= \sum_{k\in\mathbb{Z}_+} 9\cdot 10^{-k} \\ &= 9\cdot \frac{1/10}{1-1/10} \\ &= 1 \end{aligned}$$

(recall that $\sum_{k\in\mathbb{Z}_+} 10^{-k}$ is a convergent geometric series). Consequently if there is some $N \in \mathbb{Z}_+$ so that $a_N \neq 9$ and $a_n = 9$ for all $n \in \mathbb{Z}_+$ with $n > N$, then $0.a_1a_2a_3\cdots = 0.a_1a_2\cdots a_{N-1}b_N$ where $b_N = a_N + 1$. We will assume the result that for every $\alpha \in \mathbb{R}$ with $0 < \alpha < 1$, there is a unique way to write α as $0.a_1a_2a_3\cdots$ so that $a_k \in \{0,1,2,3,4,5,6,7,8,9\}$ for all $k \in \mathbb{Z}_+$ and $\neg(\exists N \in \mathbb{Z}_+$ so that $\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9)$.

Theorem 9.1. *The interval* $(0,1) = \{x \in \mathbb{R} : \ 0 < x < 1 \ \}$ *is uncountable.*

Proof. (Cantor's diagonalisation argument) We know the interval $(0,1)$ is infinite, since $f : \mathbb{Z}_+ \to (0,1)$ defined by $f(k) = 10^{-k}$ is easily shown to be injective. For the sake of contradiction, suppose $(0,1)$ is countable. Thus we can enumerate the elements of $(0,1)$ as $\alpha_1, \alpha_2, \alpha_3, \ldots$. Write each α_k as a decimal expansion as described above:

$$\alpha_k = 0.a_{k1}a_{k2}a_{k3}\cdots$$

where $a_{ki} \in \{0,1,2,3,4,5,6,7,8,9\}$ and $\neg(\exists N \in \mathbb{Z}_+$ so that $\forall n \in \mathbb{Z}_+,\ n > N \implies a_{kn} = 9)$. For each $k \in \mathbb{Z}_+$, set

$$b_k = \begin{cases} 1 & \text{if } a_{kk} \neq 1, \\ 2 & \text{if } a_{kk} = 1. \end{cases}$$

Set $\beta = 0.b_1b_2b_3\cdots$. Thus $\beta \in \mathbb{R}$ with $0 < \beta < 1$ and $\neg(\exists N \in \mathbb{Z}_+$ so that $\forall n \in \mathbb{Z}_+,\ n > N \implies b_n = 9)$. Hence by assumption, $\beta = \alpha_m$ for some $m \in \mathbb{Z}_+$. But $b_m \neq a_{mm}$, contradicting the uniqueness of the representation of β as

a decimal expansion not ending in an infinite sequence of 9s. Thus the assumption that the interval $(0,1)$ is countable leads to a contradiction, so $(0,1)$ must be uncountable. $\square$

Remark: Suppose we have $m \in \mathbb{Z}_+$ and $a_1, a_2, \ldots, a_m \in \{0,1,2,3,4,5,6,7,8,9\}$ (not all 0), and

$$\alpha = 0.a_1a_2\cdots a_m a_1a_2\cdots a_m a_1a_2\cdots a_m\cdots = 0.\overline{a_1a_2\cdots a_m}.$$

Then α is a rational number: Let $b = \sum_{k=1}^{m} a_k \cdot 10^{m-k}$. Then $b \in \mathbb{Z}_+$ and

$$\begin{aligned}\alpha &= \sum_{n\in\mathbb{Z}_+} b\cdot 10^{-mn}\\ &= b\cdot\frac{10^{-m}}{1-10^{-m}}\\ &= \frac{b}{10^m-1}.\end{aligned}$$

Note that the map $g : (0,1) \to \mathbb{R}$ given by $g(x) = x$ is injective, so $|(0,1)| \le |\mathbb{R}|$. Since $|\mathbb{Z}_+| < |(0,1)|$, we get $|\mathbb{Z}_+| < |\mathbb{R}|$, meaning $\mathbb{R}$ is uncountable. In the following corollary, we show $|(0,1)| = |\mathbb{R}|$, which is another way to argue that $\mathbb{R}$ is uncountable.

Corollary 9.2. *There is a bijection between the interval* $(0,1)$ *and* $\mathbb{R}$ *(and hence* $\mathbb{R}$ *is uncountable).*

Definition. For A a set, we let

$$\mathcal{P}(A) = \{C : \ C \subseteq A\ \}.$$

We call $\mathcal{P}(A)$ the power set of A.

Examples:

(a) $\mathcal{P}(\emptyset) = \{\emptyset\}$, so $|\mathcal{P}(\emptyset)| = 1$.

(b) For any nonempty set X, we know $\emptyset, X$ are distinct subsets of X, and hence $|\mathcal{P}(X)| \ge 2$.

(c) $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$, so $|\mathcal{P}(\{1,2\})| = 4 = 2^2$.

(d) $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. So $|\mathcal{P}(\{1,2,3\})| = 8 = 2^3$.

As an exercise, one proves the following.

Theorem 9.3. *Suppose* A *is a finite set with* $|A| = n$ *for some* $n \in \mathbb{Z}$ *with* $n \ge 0$. *Then* $|\mathcal{P}(A)| = 2^n$.

Remark: Suppose A is a finite set with n elements; enumerate these elements as $a_1, a_2, \ldots, a_n$. Let $Y = \{(c_1, c_2, \ldots, c_n) : \ c_i = 0 \text{ or } 1\ \forall i \in \mathbb{Z} \text{ with } 1 \le i \le n\ \}$. Define $f : Y \to \mathcal{P}(A)$ by

$$f((c_1, c_2, \ldots, c_n)) = \{a_i \in A : \ c_i = 1 \text{ for some } i \in \mathbb{Z} \text{ with } 1 \le i \le n\ \}.$$

Thus $f((c_1, c_2, \ldots, c_n))$ is a subset of A; one can show that f is bijective.

As exercises, one proves the following.

Proposition 9.4. *Let* A, B *be sets.*

(a) $(A \subseteq B) \iff (\mathcal{P}(A) \subseteq \mathcal{P}(B))$.

(b) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
(c) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Theorem 9.5. *(Cantor's Theorem) Let X be a set. Then $|X| < |\mathcal{P}(X)|$.*

Proof. When $X = \emptyset$, then we know $|X| = 0 < 1 = |\mathcal{P}(X)|$. So suppose $X \neq \emptyset$, and define $f : X \to \mathcal{P}(X)$ by $f(x) = \{x\}$. We show f is injective: Suppose $x_1, x_2 \in X$ so that $f(x_1) = f(x_2)$. Thus $\{x_1\} = \{x_2\}$, and hence $x_1 = x_2$. Therefore f is injective, so $|X| \leq |\mathcal{P}(X)|$.

Now we want to show there is no bijection between X and $\mathcal{P}(X)$. For the sake of contradiction, suppose there is a bijection $g : X \to \mathcal{P}(X)$. (So for each $x \in X$, $g(x)$ is a subset of X.) Define $A = \{x \in X : \ x \notin g(x) \ \}$. Then A is a subset of X, so $A \in \mathcal{P}(X)$. Also, since we have assumed g is bijective, there is some $z \in X$ so that $g(z) = A$. By the definition of g, $z \in A$ if and only if $z \notin g(z) = A$. Thus we have a contradiction (namely that $z \in A \iff z \notin A$). Hence our assumption that there is a bijective function $g : X \to \mathcal{P}(X)$ must be false. So $|X| < |\mathcal{P}(X)|$. $\square$