1 Well-Ordering

Definition 1.1. An *order set* (or *partially ordered set*) S is **well-ordered** if every nonempty subset of S has a smallest element.

e.g. If ordered by value, $\mathbb{N}$ is well-ordered, while $\mathbb{Z}$ and $\mathbb{Q}$ are not. However, if $\mathbb{Z}$ is ordered by absolute value and then by value, then $\mathbb{Z}$ is well-ordered. Similarly, if $\mathbb{Q}^+$ is considered with all the elements in the reduced form, then ordering first by a denominator and then by a numerator induces well-ordering. Another well-ordering $\mathbb{Q}^+$ is induced by taking $\max \text{numerator}, \text{denominator}$ in reduced form and then ordering by value, which is a construction used in Cantor's diagonal argument.

The proposition $\forall e \in S.P(e)$ can be proved using the well-ordering principle for any well-ordered set S with ordering $\prec$.

L1 To obtain a contradiction, suppose that $\forall e \in S.P(e)$ is false.

L2 Let $C = \{e \in S \mid P(e) \text{ is false}\}$ be the set of counterexamples to P.

L3 $C \neq \emptyset$ by L1 and L2

L4 Let e be the smallest element of C; well ordering principle, L3.

L5 Let $e' = \ldots$

L6 $e' \in C$

L7 $e' \prec e$

L8 This is a contradiction to L4, L5, L6

L9 $\forall e \in S.P(e)$; proof by contradiction, L1 - L7

2 Diagonalization

Definition 2.1. A function $f : A \to B$ is said to be *surjective* or *onto* if $\forall y \in B.\exists x \in A.f(x) = y$.

From the existence of a surjective function, if A and B are finite sets, we can conclude that $|B| \geq |A|$.

Definition 2.2. A nonempty set C is countable if there is a surjective function from $\mathbb{N}$ to $\mathbb{C}$. By convention, an empty set is countable.

Note that, by definition, every finite set is countable.

Suppose $C = \{c_0, \ldots, c_{n-1}\}$ is a nonempty finite set of n elements. Define $f : \mathbb{N} \to \mathbb{C}$ such that

$$f(i) = \begin{cases} c_i, \text{ for } i = 0, \ldots, n-1 \\ c_{n-1}, \text{ for } i \geq n \end{cases} . \tag{1}$$

Then f is surjective and hence C is countable.

Moreover, $\mathbb{Z}$ is countable. Then

$$g(x) = \begin{cases} \frac{-x-1}{2}, \text{ if } x \text{ is odd} \\ \frac{x}{2} \text{if } x \text{ is even} \end{cases} \tag{2}$$

is surjective, and hence $\mathbb{Z}$ is countable.

Furthermore, if A and B are countable, then so is $A \cup B$. To prove this, we need the following lemma.

Lemma 2.3

If A is countable and there is a surjective function $f : A \to B$, then B is countable.

Proof. Since A is countable, then there exists a surjective function $g : \mathbb{N} \to A$. Consider the function $h : \mathbb{N} \to B$ defined by $h(i) = f(g(i))$ for all $i \in \mathbb{N}$.

To prove that h is surjective, consider any $z \in B$. Since f is surjective, there exists $y \in A$ such that $f(y) = z$. Since g is surjectiv, then there exists $x \in \mathbb{N}$ such that $g(x) = y$. Hence, $f(g(x)) = z$, and by construction h is surjective. □

Consider the function $f(m, n) = 2^m \cdot 3^n \in \mathbb{N}$ for any $m, n \in \mathbb{N}$.

Definition 2.4. For any set A, the power set of A is the set of all subsets of A. Thus, $P(A) = \{S \mid S \subseteq A\}$.

Note that if $|A| = n$, then $\left|P(A)\right| = 2^n$.

Theorem 2.5

$P(\mathbb{N})$ is uncountable.

Proof.

Suppose $P(\mathbb{N})$ is countable. Then there is a surjective function $f : \mathbb{N} \to P(\mathbb{N})$.

Let $D = \{i \in \mathbb{N} \mid i \notin f(i)\} \in P(\mathbb{N})$.

Since f is surjective, there exists $j \in \mathbb{N}$ such that $f(j) = D$. Then for all $i \in \mathbb{N}$, $i \in f(j)$ IFF $i \in D$, since $f(j) = D$. This is true if $i \notin f(i)$ by definition of D. Since $j \in \mathbb{N}$, by specialisation $j \in f(j)$ IFF $j \notin f(j)$. This is a contradiction, and therefore $P(\mathbb{N})$ is uncountable. □