1 The Well-Ordering Principle

Definition 1. A set of real numbers S is *well-ordered* if every nonempty subset of S has a least element.

There are some sets we can easily see are well-ordered: if S is finite, then it clearly has a least element, and so do its finite nonempty subsets, so any finite set of real numbers is clearly well-ordered. If we look at infinite sets, most of the ones that spring to mind are transparently *not* well-ordered: $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$ don't even have least elements themselves (any given element x of one of these sets is clearly not the least, since $x-1$ is smaller), so they can't be well-ordered (since $S \subseteq S$, it is clearly a necessary condition for well-ordering that S itself have a least element). However, even some sets which do have a least element aren't well-ordered: consider the closed interval $[0,1]$: it has a least element of zero, but its subset, the half-open interval $(0,1]$ doesn't have a least element (for any element x of $(0,1]$, $\frac{x}{2}$ is smaller).

There is of course one well-known, named infinite set of numbers which *is* well-ordered, and this will be the crux of what we do henceforth.

Axiom 1. *The set $\mathbb{N}$ is well-ordered.*

This is nice, but what we can do with it ends up being authentically excellent.

2 Inductive Proof

The well-ordering principle ends up givign us a very useful proof method. We start by proving something for the smallest positive integer, and then we premise the proof of successive cases on the proofs of earlier cases. This method is known as *induction*

Theorem 1 (Mathematical Induction)**.** *Let $P(n)$ be a statement qualified by a positive integer n. If $P(1)$ is true, and if $P(k)$ implies $P(k+1)$ for all positive integers k, then $P(n)$ is true for all positive integers n.*

Proof. We shall prove this by contradiction, so we start with the premise that $P(1)$ is true, that $P(k)$ implies $P(k+1)$ for all positive integers k, and that at $P(n)$ is *not true for all positive integers n*; in particular, this last element of the premise signifies that $P(n)$ is false for at least one positive integer n. Now, let $S = \{n \in \mathbb{N} : P(n) \text{ is false}\}$. From our premise, S is nonempty but $1 \notin S$. By definition, $S \subseteq \mathbb{N}$: since S is nonempty and $\mathbb{N}$ is well-ordered, S has a least element x; since $1 \notin S$, $x \geq 2$. Sicne $x-1 \in \mathbb{N}$ but $x-1 \notin S$, it follows by the definition of S that $P(x-1)$ is true; however, then the fact that $P(k)$ implies $P(k+1)$ when $k = x-1$ requires that $P(x)$ be true, in contradiciton to the definition of x as an element of S. □

Mathematical induction is a shorthand for what would otherwise be a tedious (and actually infinite) daisy-chain of implication. We would start by establishing $P(1)$; then having established $P(1)$ and $P(1) \Rightarrow P(2)$ to be true, we know $P(2)$ is true; then since $P(2)$ and $P(2) \Rightarrow P(3)$ is true, we know $P(3)$ is true, and so forth.

This is all a little rarified at present. How do we actually use this? We can prove a proposition P in general using a method called "proof by induction".

- State something which we wish to show is true for all natural numbers n as a qualified proposition $P(n)$.

- Demonstrate that $P(1)$ is true; this is known as the *base case*.
- For a specific but unspecified value of k, *assume* that $P(k)$ is true. This is called the *inductive hypothesis*
- Prove, based on that assumption, that $P(k+1)$ is true. This is the *inductive step*.

If we follow these four steps, then we have a proof that $P(n)$ is true for all positive integers N, by the power of induction! Step 2 demonstrates $P(1)$, and steps 3–4 are how one proves that $P(k) \Rightarrow P(k+1)$ for all k.

Let's see this in action:

Proposition 1. *If n is a positive integer, then $1+2+3+4+5+\cdots+n = \frac{n(n+1)}{2}$.*

Proof. We shall prove this by induction, defining the qualified statement $P(n)$ to be $1+2+\cdots+n = \frac{n(n+1)}{2}$.

For the base case, we note that $P(1)$ is merely the assertion $1 = \frac{1(1+1)}{2}$, which is easily verified arithmetically.

For the inductive step, we start by assuming $P(k)$ for a an integer k, so we may henceforth make use of the fact

$$1+2+3+4+5+\cdots+k = \frac{k(k+1)}{2}$$

and based on this knowledge, we can evaluate

$$\begin{aligned} 1+2+3+4+5+\cdots+k+(k+1) &= (1+2+3+4+5+\cdots+k)+(k+1) \\ &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ 1+2+3+4+5+\cdots+k+(k+1) &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

which is identically the statement of $P(k+1)$, so our inductive proof is completed. □

Maybe we can try another example:

Proposition 2. *For any nonnegative integer n, $7 \mid 2^{6n}-1$.*

Proof. We shall prove this by induction. In the base case $n=0$, this can easily be shown arithmetically: $2^{6\cdot 0}-1 = 0$, which is divisible by 7.

We now assume the inductive hypothesis $7 \mid 2^{6k}-1$, and attept to prove that $7 \mid 2^{6(k+1)}-1$; we thus know from the inductive hypothesis that $2^{6k}-1 = 7s$ for some integer s, or $2^{6k} = 7s+1$. Then:

$$2^{6(k+1)}-1 = 2^{6k+6}-1 = 64\cdot 2^{6k}-1 = 64(7s+1)-1 = 64\cdot 7s+63 = 7(64s+9$$

and thus $7 \mid 2^{6(k+1)}-1$, completing the inductive step. □

Note that in that case we used the set of non-negative integers (starting at zero), rather than the traditional starting point of 1; in fact, we can start our proof at any integer value, as dictated by the actual statement to be proven. For instance, some results are only true for "sufficiently large numbers" but can be shown to be true henceforth:

Proposition 3. *If n is an integer greater than or equal to 2500, then $n^3 < (1.01)^n$.*

Proof. We will prove this by induction, with the base case $n = 2500$: we can show with a calculator that $2500^3 = 15625000000$, while $1.01^{2500} \approx 63596681796$ (we could actually use a lower base case for a stronger result, but this one's fine).

Now we will prove the inductive step. Our inductive hypothesis is that $k^3 < (1.01)^k$ for some specific $k \geq 2500$, and we shall try to prove that $(k+1)^3 < (1.01)^{k+1}$. Starting from our inductive hypothesis, we can derive an inequality with the correct right side:

$$k^3 < (1.01)^k(1.01)k^3 \qquad\qquad < (1.01)^{k+1}$$

so now we need to show that $(1.01)k^3 \geq (k+1)^3$. using the fact that $k \geq 2500$, this is pretty easy:

$$\begin{aligned}(k+1)^3 &= k^3 + 3k^2 + 3k + 1 \\ &\leq k^3 + 3k^2 + 3k^2 + k^2 \text{ (since } k \geq 1) \\ &\leq k^3 + 7k^2 \qquad\qquad \leq k^3 + (0.01k)\cdot k^2 \text{ (since } k \geq 700) \\ &\leq 1.01k^3\end{aligned}$$

and thus $(1.01)^{k+1} > (1.01)k^3 \geq (k+1)^3$, completing our inductive argument. □

Induction is most at home, though, dealing with sums:

Proposition 4. *For any nonnegative integer n, the sum*

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n}$$

is at least $\frac{n+2}{2}$.

Proof. We prove this by induction on n: the base case $n = 0$ is the assertion $\frac{1}{1} \geq \frac{0+2}{2}$, which is indeed true.

For the inductive step, we shall assume that for a particular integer $k \geq 0$,

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \geq \frac{n+2}{2}$$

and now we are interested in placing a bound on $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}}$ Now, we may note that

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} + \frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}} \geq \frac{n+2}{2} + \frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}$$

so now we simply need to place a bound (preferably $\frac{1}{2}$) on $\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}$. Npte that this is a sum of the reciprocals of several numbers less than or equal to 2^{n+1}; thus each term in this sum is at least $\frac{1}{2^{n+1}}$, so

$$\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}} \geq \underbrace{\frac{1}{2^{n+1}} + \cdots + \frac{1}{2^{n+1}}}_{2^n \text{ times}}$$

so $\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}} \geq 2^n \cdot \frac{1}{2^{n+1}} = \frac{1}{2}$. And so:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} \geq \frac{n+2}{2} + \frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}} \geq \frac{n+2}{2} + \frac{1}{2} \geq \frac{(n+1)+2}{2}$$

completing our inductive proof. □