PROOFS BY INDUCTION AND CONTRADICTION, AND WELL-ORDERING OF $\mathbb{N}$

1. Induction

One of the most important properties (usually taken to be an axiom) of the set

$$\mathbb{N} = \{1, 2, \ldots\}$$

of natural numbers is the *principle of mathematical induction*:

Principle of Induction. *If $S \subseteq \mathbb{N}$ is a subset of the natural numbers such that*

(i) $1 \in S$*, and*
(ii) *whenever $k \in S$, then $k+1 \in S$,*

then $S = \mathbb{N}$.

Proofs which utilize this property are called 'proofs by induction,' and usually have a common form. The goal is to prove that some property or statement $\mathcal{P}(k)$, holds for all $k \in \mathbb{N}$, where the property itself depends on k. First one proves the *base case*, that $\mathcal{P}(1)$ holds (or sometimes $\mathcal{P}(0)$ if one takes $\mathbb{N} = \{0, 1, \ldots\}$). Then one shows the *inductive case* (also called the *inductive step*), which is to prove that *if* $\mathcal{P}(k)$ holds, *then* $\mathcal{P}(k+1)$ must hold as well. Once these two things have been shown, the proof is complete, since then the set

$$S = \{k \in \mathbb{N} : \mathcal{P}(k) \text{ holds}\}$$

must be all of $\mathbb{N}$ by the principle of induction. While proving the inductive step, one often refers to the assumption that $\mathcal{P}(k)$ is true as the *inductive hypothesis.*

Here is an example.

Proposition. *For all $k \in \mathbb{N}$,*

$$1 + \cdots + k = \frac{k(k+1)}{2}.$$

Proof. In this example $\mathcal{P}(k)$ is the statement that the equation

$$1 + \cdots + k = \frac{k(k+1)}{2} \tag{1}$$

is true. We prove the base case by hand, which is easy enough:

$$\mathcal{P}(1): \quad 1 = \frac{1(1+1)}{2} = 1$$

is indeed true.

To prove the inductive step, we now assume that the equation (1) holds, and use this to try and prove $\mathcal{P}(k+1)$. So consider the sum

$$1 + \cdots + (k+1) = (1 + \cdots + k) + (k+1).$$

By the inductive hypothesis (1), it follows that this is equal to

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

so the inductive step has been proved. □

1.1. **Strong induction.** We can use the principle of induction to prove a similar result, variously called the 'principle of *complete* induction' or the 'principle of *strong* induction.'

Proposition (Principle of strong induction)**.** *If $S \subset \mathbb{N}$ is a subset of the natural numbers such that*

(i) $1 \in S$, *and*
(ii) *whenever* $\{1, \ldots, k\} \subset S$, *then* $k+1 \in S$,

then $S = \mathbb{N}$.

Remark. Note the difference from the principle of induction above. In the second property we require the stronger assumption that not only is k in S but that in fact $n \in S$ for all of the numbers $1 \le n \le k$.

Proof. Instead of the set S, we will consider the set

$$S_0 = \{k \in \mathbb{N} : \{1, \ldots, k\} \subset S\}$$

of those numbers which, along with all of their preceding numbers, lie in S. Note that S_0 is a subset of S, so if we show that $S_0 = \mathbb{N}$, then we must have $S = \mathbb{N}$ also.

Proceeding by induction, we have $1 \in S_0$ by the assumption that $1 \in S$, which furnishes the base case.

For the inductive step, assume that $k \in S_0$. Observe that this is equivalent to the assumption that $\{1, \ldots, k\} \subset S$, so that by the second hypothesis on S it follows that $\{1, \ldots, k+1\} \subset S$. But this is equivalent to the statement that $k+1 \in S_0$, so it follows by induction that $S_0 = \mathbb{N}$. □

We can now use this alternate principle of strong induction for proofs. To prove a statement of the form "$\mathcal{P}(k)$ holds for all $k \in \mathbb{N}$" by strong induction, you prove the base case as before, but in the inductive step you are then allowed to make the stronger assumption that, not only does $\mathcal{P}(k)$ hold, but $\mathcal{P}(n)$ holds as well for all $1 \le n \le k$. We demonstrate such a proof below, which combines another technique — proof by contradiction.

2. Contradiction

Proof by contradiction is based on the following bit of logic. Suppose $\mathcal{A}$ and $\mathcal{B}$ are mathematical statements, either true or false. Then the statement

$$\mathcal{A} \implies \mathcal{B}, \tag{2}$$

which is read "if $\mathcal{A}$ is true, then $\mathcal{B}$ is true", is logically equivalent to the *contrapositive* statement

$$\text{not } \mathcal{B} \implies \text{not } \mathcal{A}, \tag{3}$$

i.e. "if $\mathcal{B}$ is false, then $\mathcal{A}$ is false." (Note that neither of (2) or (3) is equivalent to either of the statements '$\mathcal{B} \implies \mathcal{A}$' or 'not $\mathcal{A} \implies$ not $\mathcal{B}$'.)

Thus if $\mathcal{A}$ is a set of assumptions and $\mathcal{B}$ is a conclusion we are trying to prove, we may as well make the assumption that $\mathcal{B}$ is *false*, and try and prove that one of the assumptions in $\mathcal{A}$ must fail[1].

We now combine these proof techniques to prove that $\mathbb{N}$ is well-ordered.

Proposition (Well-ordering of $\mathbb{N}$)**.** *$\mathbb{N}$ has the 'well-ordering property', which means that every nonempty subset has a smallest element. In other words, if $S \subset \mathbb{N}$ is a nonempty subset, then there exists an $s_0 \in S$ such that*

$$s_0 \leq x, \ \text{for every } x \in S. \tag{4}$$

Remark. Our collection of assumptions is that $S \subset \mathbb{N}$ and $S \neq \emptyset$. Our conclusion is that there exists $s_0 \in S$ with the property (4).

Proof. Proceeding by contradiction, suppose that S has no smallest element. Let

$$T = \mathbb{N} \setminus S = \{x \in \mathbb{N} : x \notin S\}$$

be the set of numbers not in S. We will show, by strong induction, that $T = \mathbb{N}$, so that $S = \emptyset$, which contradicts the assumption that S is not empty.

For the base case of the induction, note that $1 \in T$, for if 1 was in S then it would function as a least element[2].

For the inductitve step, we may assume the strong induction hypothesis that $n \in T$ for all $1 \leq n \leq k$. In other words, *none* of the numbers $1, \ldots, k$ lie in S. Now if $k+1$ was in S, it would be a least element, so we must have $k+1 \in T$ instead, which completes the inductive step. We conclude, based on strong induction, that $T = \mathbb{N}$, which contradicts the assumption that S is non-empty as noted above. □

[1]Sometimes $\mathcal{A}$ may include not only the explicit assumptions made in the statement of the theorem, but all of the other axioms and theorems that we have developed prior to this point — in other words, it is enough to show that 'not $\mathcal{B}$', along with the given assumptions, implies that something you know to be true would have to be false.

[2]Note that this sentance itself is a self-contained example of reasoning by contradiction!