Note 3 Supplement: Well Ordering Principle

Computer Science 70
University of California, Berkeley

Summer 2018

1 Introduction

Now that you have learned about mathematical induction to prove statements of the form $\forall n \in \mathbb{N},\ P(n)$, one question you may have is: "can we use induction to prove statements for any other sets besides $\mathbb{N}$?" To answer this question, we must examine what properties of $\mathbb{N}$ we are exploiting when we write an inductive proof.

The core of the proof by induction is the *inductive step*, which is the statement $\forall n \in \mathbb{N},\ [P(n) \implies P(n+1)]$. We can visualize the proof by imagining that we have a sequence of propositions $P(0), P(1), P(2), \ldots$, and the truth of each proposition implies the truth of the next proposition "in the line". Then, proving a base case, such as $P(0)$, proves the truth of all subsequent propositions, as if we are knocking down an infinite line of dominoes by knocking over the first one.

From the preceding discussion, it may appear that the method of induction can be carried out if we can arrange the propositions in a "line". For instance, the real numbers have a canonical ordering, so perhaps we can prove statements of the form $\forall x \in \mathbb{R},\ P(x)$ in a similar fashion. However, two issues quickly arise:

1. There is no analog of the base case for real numbers. The real numbers are a *doubly infinite* line, and therefore has no beginning.

2. We can ignore the previous issue by focusing our attention on statements of the form "for all $x \geq 0, \ldots$". The crucial difficulty, however, lies in the use of the word *next* when we seek to show that each proposition

implies the truth of the *next* proposition in line. Indeed, how can we move from one real number x to the "next" real number? If we try jumping from x to $x+1$, then we miss all of the real numbers in the interval $(x, x+1)$. Even if we take a smaller "step size", no matter what positive ε we choose, jumping from x to $x+\varepsilon$ will still miss many real numbers along the way.

The conclusion of the second point is that there is no way to move from a real number to a larger real number without skipping real numbers along the way. However, we do not have to give up hope. Instead, we can ask if there exists *another* ordering on $\mathbb{R}$ which makes induction possible.

2 The Well Ordering Principle

2.1 Total Orderings, Well Orderings

This leads us to define precisely what we mean by an ordering. Given a set S, a **total ordering** (sometimes called a **linear ordering**) $\lesssim$ on S is a subset of $S \times S$ satisfying some properties. If the pair (x, y) is in the ordering $S \times S$, then we write $x \lesssim y$. The properties we desire are:

- (Totality) For all $x, y \in S$, either $x \lesssim y$ or $y \lesssim x$ or both.
- (Reflexivity) For all $x \in S$, $x \lesssim x$.
- (Transitivity) For all $x, y, z \in S$, if $x \lesssim y$ and $y \lesssim z$, then $x \lesssim z$.
- (Antisymmetry) For all $x, y \in S$, if $x \lesssim y$ and $y \lesssim x$, then $x = y$.

The totality condition ensures that all pairs of elements can be compared (this property is what leads us to call it a *total* ordering, as opposed to a *partial* ordering). The reflexivity condition is a convention (when we speak of orderings, we choose to speak of "less than or equal to", rather than "strictly less than"). The transitivity condition is natural in order for the ordering to look like a "line", and the antisymmetry condition ensures that we cannot have two distinct elements both be larger than each other.

It turns out that these properties are not enough to allow us to perform induction. We say that $\lesssim$ is a **well ordering**[1] if $\lesssim$ is a total ordering, and in addition, the following property holds:

[1] Excuse the grammar.

Well Ordering Property: For any non-empty subset $R \subseteq S$, R has a least element.

A **least element** of R is an element $x \in R$ such that $x \lesssim y$ for all $y \in R$.

Example 1. The usual orderings on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are total orderings.

Example 2. The usual ordering on $\mathbb{Z}$ is not a well ordering. For example, $\mathbb{Z}$ itself does not have a least element.

Example 3. The usual ordering on $\mathbb{R}$ is not a well ordering, because it fails to have a least element. However, even if we restrict ourselves to the non-negative real numbers $\mathbb{R}_+ := \{x \in \mathbb{R} : x \geq 0\}$, we still do not have a well ordering. Indeed, the set $\{x \in \mathbb{R} : x > 0\}$ of strictly positive real numbers is a non-empty subset of $\mathbb{R}_+$ that fails to have a least element.

Example 4. Any total ordering on a finite set is a well ordering. (See if you can prove this.)

2.2 Well Ordering and Induction for $\mathbb{N}$

Our next example is actually a theorem.

Theorem 1 (Well Ordering Property for $\mathbb{N}$)**.** $\mathbb{N}$ *is well ordered under the usual ordering on* $\mathbb{N}$.

Before we proceed with the proof, it is worth pausing for a moment to think about how you would approach this proof. Since the statement is about the natural numbers, it is natural (excuse the pun) to proceed by induction—but on what? The statement to prove is that for all non-empty $R \subseteq \mathbb{N}$, the set R has a least element. It is tempting to try to prove the statement by induction on the size of the set R, but this approach *does not work*. Specifically, induction can prove the statement

$$\forall n \in \mathbb{N} \left([(|R| = n) \wedge (R \subseteq S) \wedge (R \neq \varnothing)] \implies \exists x \in R \, \forall y \in R \, x \leq y \right).$$

(*Exercise*: Decipher the above statement and explain why it does not imply the existence of a least element if R is an *infinite* subset of $\mathbb{N}$.)

Proof of Theorem 1. We prove the following statement by induction:

$$\forall n \in \mathbb{N}\, \forall R \subseteq S\, \big([(R \neq \varnothing) \wedge (\exists k \in R,\ k \leq n)] \implies \exists x \in R\, \forall y \in R\, x \leq y\big).$$

That is, for all $n \in \mathbb{N}$ and all non-empty subsets $R \subseteq S$, if R contains an element which is at most n, then R has a least element.

Base case: If $0 \in R$, then clearly 0 is the least element of R.

Inductive hypothesis: Let $n \in \mathbb{N}$. Assume that if R is a non-empty subset of $\mathbb{N}$ which contains an element which is at most n, then R has a least element.

Inductive step: Suppose that R contains an element k which is at most $n+1$. If R contains an element which is at most n, then by the inductive hypothesis, we are done. Otherwise, $k = n+1$, and since R does not contain any of the elements $0, 1, \ldots, n$, then $n+1$ is the least element of R. □

In fact, the Well Ordering Property for $\mathbb{N}$ is *equivalent* to the principle of induction, in the sense that if we assume that $\mathbb{N}$ is well ordered under $\leq$, then the principle of induction holds for $\mathbb{N}$. This is a bit more subtle to describe, since the set $\mathbb{N}$ is essentially *defined* by induction. We can formalize this by saying $\mathbb{N}$ is the smallest set S with the following property:

> **Inductive Property**: For all subsets $R \subseteq S$, if $0 \in R$ and for any $n \in R$ we have $n+1 \in R$, then $R = S$.

When we write a proof by induction, we are really using the Inductive Property for $\mathbb{N}$. To see this, for a statement $\forall n \in \mathbb{N},\ P(n)$, define the set $R := \{n \in \mathbb{N} : P(n) \text{ holds}\}$. In a proof by induction, we prove the base case $P(0)$, which shows that $0 \in R$, and we prove the inductive step $\forall n \in \mathbb{N},\ [P(n) \implies P(n+1)]$, which shows that for any $n \in R$, $n+1 \in R$ as well. By the Inductive Property for $\mathbb{N}$, we conclude that $R = \mathbb{N}$, i.e., the statement $P(n)$ holds for all $n \in \mathbb{N}$.

Theorem 2. *Assuming that $\mathbb{N}$ is well ordered under $\leq$, we can prove that $\mathbb{N}$ has the Inductive Property.*

Proof. Let $R \subseteq \mathbb{N}$ contain 0 and have the property that for any $n \in R$, we also have $n+1 \in R$. We must show that $R = \mathbb{N}$.

Consider the set $\mathbb{N} \setminus R := \{n \in \mathbb{N} : n \notin R\}$. If $\mathbb{N} \setminus R$ is non-empty, then by the assumption of well ordering, $\mathbb{N} \setminus R$ has a least element n_0. We know that $n_0 \neq 0$ because $0 \in R$. So, $n_0 - 1 \in \mathbb{N}$, and since n_0 is the *least* element of $\mathbb{N} \setminus R$, then $n_0 - 1$ must not be in $\mathbb{N} \setminus R$, i.e., $n_0 - 1 \in R$. This contradicts the fact that if $n_0 - 1 \in R$, then $n_0 \in R$ as well. Therefore, $\mathbb{N} \setminus R$ is empty, i.e., $R = \mathbb{N}$. □

2.3 Applications of the Well Ordering Property for $\mathbb{N}$

The Well Ordering Property for $\mathbb{N}$ allows us to write some inductive proofs more conveniently. To illustrate the idea, we will prove two theorems. The first theorem is a theorem we have already proven using induction. Compare and contrast the following proof with the proof you have already seen.

Theorem 3. *For all $n \in \mathbb{N}$, $\sum_{i=0}^{n} i = n(n+1)/2$.*

Proof. If the statement of the theorem is false, then by the Well Ordering Property for $\mathbb{N}$ there exists a least $n_0 \in \mathbb{N}$ such that $\sum_{i=0}^{n_0} i \neq n_0(n_0+1)/2$. Since the statement of the theorem holds trivially when $n = 0$, we know that $n_0 \neq 0$. Because n_0 is the least element for which the theorem fails, we know that $\sum_{i=0}^{n_0-1} i = (n_0-1)n_0/2$. However,

$$\sum_{i=0}^{n_0} i = \sum_{i=0}^{n_0-1} i + n_0 = \frac{(n_0-1)n_0}{2} + n_0 = \frac{n_0(n_0+1)}{2},$$

which is a contradiction. Hence, the theorem is true. □

The proof we have just given is essentially the same as the argument in the ordinary proof by induction, but using the Well Ordering Principle for $\mathbb{N}$ makes the proof more indirect and harder to read. The lesson here is that the Well Ordering Principle for $\mathbb{N}$ can be used to write proofs which are equivalent to proofs by induction, but they are not necessarily easier.

On the other hand, the Well Ordering Principle for $\mathbb{N}$ provides an elegant proof of the following theorem, which will be useful in our study of modular arithmetic.

Theorem 4 (Division Algorithm)**.** *For any $a, b \in \mathbb{Z}$, where $b > 0$, there exist unique integers $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ such that $a = qb + r$.*

Proof. Consider the set $R = \{a - qb : q \in \mathbb{Z},\ a - qb \geq 0\}$. Then, $R \subseteq \mathbb{N}$ and by choosing q to be a negative integer, we can see that $R \neq \varnothing$. By the Well Ordering Principle for $\mathbb{N}$, R has a least element r.

Since $r \in R$, we can write $a = qb + r$ for some $q \in \mathbb{Z}$. We claim that $r \in \{0, 1, \ldots, b-1\}$. Indeed, if $r \geq b$, then $a-(q+1)b \geq 0$ so $a-(q+1)b \in R$, and $a - (q+1)b$ is smaller than $a - qb = r$, which contradicts the fact that r is the least element of R.

Finally, for uniqueness, suppose that $a = q_1 b + r_1 = q_2 b + r_2$ where $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \{0, 1, \ldots, b-1\}$. We may assume (without loss of generality) that $r_2 - r_1 \geq 0$. Then, subtracting, we have $(q_1 - q_2)b = r_2 - r_1$, where $r_2 - r_1 \in \{0, 1, \ldots, b-1\}$. Since $(q_1 - q_2)b$ is divisible by b, then $r_2 - r_1$ is divisible by b, from which it follows that $r_2 - r_1 = 0$, i.e., $r_1 = r_2$. So, $(q_1 - q_2)b = 0$, and dividing by b, we get $q_1 = q_2$ as well. □

3 What Sets Are Well Ordered? (Optional)

This section is optional. Read on if you are interested.

To connect the concept of well orderings back to our discussion of induction, observe that well orderings solve the problem that we encountered at the beginning of this note, namely that for sets such as $\mathbb{R}$, we do not know how to reach the "next" element. If $\mathbb{R}$ has a well ordering $\lesssim$, then we can carry out the following procedure:

- Since $\mathbb{R}$ is well ordered under $\lesssim$, there is a least element x_0. We add x_0 to a set X of elements considered thus far.
- As long as $X \neq \mathbb{R}$, then $\mathbb{R} \setminus X$ is non-empty, so it has a least element x. We can add x to the set X and keep going.

The full details are more complicated than the simplified version we have presented, but the essential idea is there. If we have a well ordering on a set, then we can perform a version of induction on the set, called *transfinite induction*. However, any well ordering of $\mathbb{R}$ will be very bizarre; it will certainly not resemble anything like the usual ordering $\leq$ on $\mathbb{R}$.

In fact, since any well ordering on $\mathbb{R}$ will be incompatible with the usual ordering on $\mathbb{R}$, then any proof by transfinite induction on $\mathbb{R}$ will only use the *set-theoretic* nature of $\mathbb{R}$. That is, the proof will only view $\mathbb{R}$ as a *set* and ignore the other properties of $\mathbb{R}$ that make $\mathbb{R}$ familiar to us (e.g., the property that real numbers can be added and multiplied). Consequently, transfinite induction is typically only useful for proving statements in *set theory* (as opposed to, e.g., calculus).

Finally, there is one important question we have not yet answered: *which sets can be well ordered?* According to the standard axioms of set theory[2],

[2]The standard axioms are called **ZFC**. See: https://en.wikipedia.org/wiki/Zermelo%E2%80%93Fraenkel_set_theory.

every set can be well ordered. The proof is highly non-constructive, however, so no one has written down an explicit well ordering on $\mathbb{R}$. "Sure," you may say, "the existence of a well ordering on $\mathbb{R}$ may follow from the axioms, but in what sense does the well ordering actually *exist* if we cannot write it down?" In fact, there are many mathematicians who study logic, set theory, and *metamathematics* (roughly speaking, the study of the foundations of mathematics). If these sorts of questions interest you, then you may want to give some courses in these areas a try.