Math 321: Induction, part II

Kameryn J Williams

University of Hawaiʻi at Mānoa

Fall 2020

Induction on $\mathbb{N}$

Last time, we talked about *Mathematical Induction*, and talked about the most important context in which it's formulated, namely with the natural numbers $\mathbb{N}$.

Mathematical Induction

To prove $\forall n \in \mathbb{N}\ P(n)$:

1. Prove $P(0)$.
2. Prove if $P(n)$ then $P(n+1)$.

Induction on $\mathbb{N}$

Last time, we talked about *Mathematical Induction*, and talked about the most important context in which it's formulated, namely with the natural numbers $\mathbb{N}$.

Mathematical Induction

To prove $\forall n \in \mathbb{N}\ P(n)$:

1. Prove $P(0)$.
2. Prove if $P(n)$ then $P(n+1)$.

For today, I want to talk about a different perspective on induction on $\mathbb{N}$, with a different explanation for why it's a valid proof technique.

Well-orders

One very nice property about $\mathbb{N}$ is that it is a well-order. There's two equivalent ways to formulate this property:

1. If you take any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.
2. If you take any descending sequence $a_0 \geq a_1 \geq \cdots \geq a_n \geq \cdots$ of natural numbers, then it is eventually constant.

Well-orders

One very nice property about $\mathbb{N}$ is that it is a well-order. There's two equivalent ways to formulate this property:

1. If you take any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.
2. If you take any descending sequence $a_0 \geq a_1 \geq \cdots \geq a_n \geq \cdots$ of natural numbers, then it is eventually constant.

Before we see what this has to do with induction, let's check that those two properties really are equivalent formulations of the same thing.

Characterizing being a well-order

Proposition

The following two properties are equivalent.

1. *If you take any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.*
2. *If you take any descending sequence $a_0 \geq a_1 \geq \cdots \geq a_n \geq \cdots$ from $\mathbb{N}$, then it is eventually constant.*

(In fact, this is true for more than just $\mathbb{N}$, and the equivalence holds for any linear order.)

Characterizing being a well-order

Proposition

The following two properties are equivalent.

1. *If you take any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.*
2. *If you take any descending sequence $a_0 \geq a_1 \geq \cdots \geq a_n \geq \cdots$ from $\mathbb{N}$, then it is eventually constant.*

(In fact, this is true for more than just $\mathbb{N}$, and the equivalence holds for any linear order.)

($\longrightarrow$) We check this by contrapositive. Suppose we have a decreasing sequence of natural numbers which is not eventually constant. By throwing out any repetitions, we can thin it down to a strictly decreasing sequence

$$a_0 > a_1 > \cdots > a_n > \cdots \qquad n \in \mathbb{N}.$$

Now consider $X = \{a_n : n \in \mathbb{N}\}$. Then X cannot have a smallest element.

Characterizing being a well-order

Proposition

The following two properties are equivalent.

1. *Any nonempty set* $X \subseteq \mathbb{N}$ *then* X *has a smallest element.*
2. *Any infinite descending sequence from* $\mathbb{N}$ *is eventually constant.*

Characterizing being a well-order

Proposition

The following two properties are equivalent.

1. *Any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.*
2. *Any infinite descending sequence from $\mathbb{N}$ is eventually constant.*

($\longleftarrow$) Also by contrapositive. Consider nonempty $X_0 \subseteq \mathbb{N}$ so that X_0 does not have a smallest element. So if we pick any $a_0 \in X_0$ then the set $X_1 = \{a \in X_0 : a < a_0\}$ is nonempty. Notice that X_1 cannot have a smallest element, as its smallest element would have to also be the smallest element of X. Pick any $a_1 \in X$.

Proposition

The following two properties are equivalent.

1. *Any nonempty set $X \subseteq \mathbb{N}$ then X has a smallest element.*
2. *Any infinite descending sequence from $\mathbb{N}$ is eventually constant.*

($\longleftarrow$) Also by contrapositive. Consider nonempty $X_0 \subseteq \mathbb{N}$ so that X_0 does not have a smallest element. So if we pick any $a_0 \in X_0$ then the set $X_1 = \{a \in X_0 : a < a_0\}$ is nonempty. Notice that X_1 cannot have a smallest element, as its smallest element would have to also be the smallest element of X. Pick any $a_1 \in X$.

Now repeat the process inductively. Suppose we have already picked $a_0 > a_1 > \cdots > a_n$, where $a_i \in X_i$ and $X_{i+1} = \{a \in X_i : a < a_i\}$. Just as before, X_{n+1} is nonempty and cannot have a smallest element. Pick any $a_{n+1} \in X_{n+1}$ and set $X_{n+2} = \{a \in X_{n+1} : a < a_{n+1}\}$.

So we have built an infinite strictly decreasing sequence $a_0 > a_1 > \cdots > a_n > \cdots$.

Remark on that proof

For the $\longleftarrow$ direction, we used an induction argument. The sets X_n were defined recursively, and then we inductively showed that each one had the property we needed—namely being nonempty and having no smallest element. In math we sometimes do this sort of argument where we interleave the building up of objects step by step with the inductive argument that the objects behave as we want.

But what does this have to do with induction?

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.
- Let's see why this gives us what we want, namely $P(n)$ for all n.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.
- Let's see why this gives us what we want, namely $P(n)$ for all n.
- Suppose toward a contradiction that there were $n \in \mathbb{N}$ so that $P(n)$ were false. Let $X = \{n \in \mathbb{N} : \neg P(n)\}$. Then X is nonempty.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.
- Let's see why this gives us what we want, namely $P(n)$ for all n.
- Suppose toward a contradiction that there were $n \in \mathbb{N}$ so that $P(n)$ were false. Let $X = \{n \in \mathbb{N} : \neg P(n)\}$. Then X is nonempty.
- By well-orderedness, X has a smallest element, call it m.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.
- Let's see why this gives us what we want, namely $P(n)$ for all n.
- Suppose toward a contradiction that there were $n \in \mathbb{N}$ so that $P(n)$ were false. Let $X = \{n \in \mathbb{N} : \neg P(n)\}$. Then X is nonempty.
- By well-orderedness, X has a smallest element, call it m.
- It cannot be that $m = 0$, since we checked that $P(0)$ and so $0 \notin X$.

But what does this have to do with induction?

We can use the property of being a well-order to justify why induction is a valid proof technique. Let's use the first characterization—every nonempty subset of $\mathbb{N}$ has a smallest element.

- We want to prove $\forall n \in \mathbb{N}\ P(n)$.
- We prove two things: $P(0)$ and, for all n, if $P(n)$ then $P(n+1)$.
- Let's see why this gives us what we want, namely $P(n)$ for all n.
- Suppose toward a contradiction that there were $n \in \mathbb{N}$ so that $P(n)$ were false. Let $X = \{n \in \mathbb{N} : \neg P(n)\}$. Then X is nonempty.
- By well-orderedness, X has a smallest element, call it m.
- It cannot be that $m = 0$, since we checked that $P(0)$ and so $0 \notin X$.
- So it must be that $m = n + 1$ for some n. but m is the smallest element of X, so $n \notin X$. That is, we have $P(n)$. By the inductive step we conclude $P(n+1)$, i.e. $P(m)$. This is a contradiction.

Well-orderedness implies induction is valid

The idea from the previous slide can be summarized as a slogan:

- Being a well-order implies that if you have a counterexample to $P(n)$ you have a smallest counterexample, but the induction argument says there cannot be a smallest counterexample.

Well-orderedness implies induction is valid

The idea from the previous slide can be summarized as a slogan:

- Being a well-order implies that if you have a counterexample to $P(n)$ you have a smallest counterexample, but the induction argument says there cannot be a smallest counterexample.

You can use this smallest counterexample idea to prove things. This technique, which is really just a form of induction, is known as proof by infinite descent.

An example of a proof by infinite descent

Theorem

$\sqrt{2}$ *is irrational.*

An example of a proof by infinite descent

Theorem

$\sqrt{2}$ *is irrational.*

We can reformulate our earlier proof as a proof by infinite descent.

An example of a proof by infinite descent

Theorem

$\sqrt{2}$ *is irrational.*

We can reformulate our earlier proof as a proof by infinite descent.

Proof.

Suppose toward a contradiction that $\sqrt{2}$ can be written as a ratio of two integers. Since $\sqrt{2}$ is positive, we may take both integers to be positive. Thus there must be a smallest natural number p so that there is some $q \in \mathbb{N}$ with $\sqrt{2} = p/q$.

An example of a proof by infinite descent

Theorem

$\sqrt{2}$ is irrational.

We can reformulate our earlier proof as a proof by infinite descent.

Proof.

Suppose toward a contradiction that $\sqrt{2}$ can be written as a ratio of two integers. Since $\sqrt{2}$ is positive, we may take both integers to be positive. Thus there must be a smallest natural number p so that there is some $q \in \mathbb{N}$ with $\sqrt{2} = p/q$.

Now some algebra yields that $p^2 = 2q^2$, whence both p^2 and p are even. But then, if $p = 2k$, we get that $q^2 = 2k^2$, whence both q^2 and q are even. So we get that $\sqrt{2} = \frac{p/2}{q/2}$ is a ratio of natural numbers. This contradicts that p was supposed to be the smallest natural number we could put in the numerator. □

More about well-orders

While $\mathbb{N}$ is a well-order, it is not the only well-order.

More about well-orders

While $\mathbb{N}$ is a well-order, it is not the only well-order.

You can formulate induction to apply to any well-order, but we won't do so in this class.

Another way to formulate induction

This "no smallest counterexample" way of thinking about induction gives us an alternative way to formulate it. This version is sometimes called "strong induction". It's a terrible name, since this is the correct way to formulate induction in the general context, but math is full of terrible names :shrug:

Another way to formulate induction

This "no smallest counterexample" way of thinking about induction gives us an alternative way to formulate it. This version is sometimes called "strong induction". It's a terrible name, since this is the correct way to formulate induction in the general context, but math is full of terrible names :shrug:

- To prove $\forall n \in \mathbb{N}\ P(n)$:
- Prove: "for all n, if $P(m)$ holds for all $m < n$ then $P(n)$ holds". That is, assume $P(m)$ for all $m < n$ and try to prove $P(n)$.

Another way to formulate induction

This "no smallest counterexample" way of thinking about induction gives us an alternative way to formulate it. This version is sometimes called "strong induction". It's a terrible name, since this is the correct way to formulate induction in the general context, but math is full of terrible names :shrug:

- To prove $\forall n \in \mathbb{N}\ P(n)$:
- Prove: "for all n, if $P(m)$ holds for all $m < n$ then $P(n)$ holds". That is, assume $P(m)$ for all $m < n$ and try to prove $P(n)$.

Two comments:

- This handles the case $n = 0$, since "$P(m)$ for all $m < 0$" is vacuously true.
- For the earlier formulation of the induction step, we only assumed that the immediate predecessor of $n + 1$ satisfies P. For this formulation, we get to assume the stronger assumption that all predecessors satisfy P. Sometimes this stronger assumption is useful in proofs.

An example

Proposition

Every natural number > 1 *is a product of one or more primes.*

An example

Proposition

Every natural number > 1 *is a product of one or more primes.*

Proof.

We prove this by (strong) induction. Suppose $n > 1$ and that each $m < n$ is a product of primes. There are two cases to consider.

An example

Proposition

Every natural number > 1 *is a product of one or more primes.*

Proof.

We prove this by (strong) induction. Suppose $n > 1$ and that each $m < n$ is a product of primes. There are two cases to consider.
Case 1 (n is prime): Then trivially n is the product of the single prime n.

An example

Proposition

Every natural number > 1 *is a product of one or more primes.*

Proof.

We prove this by (strong) induction. Suppose $n > 1$ and that each $m < n$ is a product of primes. There are two cases to consider.
Case 1 (n is prime): Then trivially n is the product of the single prime n.
Case 2 (n is not prime). Then, by definition, n is the product of two smaller numbers a and b. By the inductive hypothesis, a and b are both products of primes, say

$$a = p_1 \cdots p_k, \qquad b = q_1 \cdots q_\ell.$$

But then

$$n = ab = p_1 \cdots p_k q_1 \cdots q_\ell$$

is also a prodct of primes. □

Remark on the example

Note that if you try to prove this by the other formulation of induction it's not clear how to proceed. How do you write $n + 1$ as a product of primes just from knowing you can do it for n?