Math 347 - Lecture 16

Examples:

**Proposition:** All horses have the same colour.

**Well-ordering**

False. Then: All horses have the same colour.

False proof. For any \( n \in \mathbb{N} \), we consider the proposition

\[ P(n) : \text{any set of } n \text{ horses all have the same colour.} \]

We prove that \( P(n) \) is true for \( n \in \mathbb{N} \) by induction.

**Base case:** When \( n = 1 \), the proposition is trivially true, for in any set of 1 horse, any horse in that set has the same colour.

**Inductive step:** Fix some \( n \geq 1 \) and assume that any set of \( n \) horses all have the same colour. Let \( H \) be a set of \( n+1 \) horses. Write

\[ H = \{ h_1, h_2, \ldots, h_{n+1} \} \]

By the inductive hypothesis, \( \{ h_2, \ldots, h_{n+1} \} \) all have the same colour. Also, by the inductive hypothesis, \( \{ h_2, \ldots, h_{n+1} \} \) and \( \{ h_1 \} \) have the same colour. Then

\[ \text{colour}(h_1) = \text{colour}(h_2) = \cdots = \text{colour}(h_{n+1}) \]

This proves the inductive step. Thus, by induction, all horses are the same colour.

**Rubbish.** For a more "math-y" version, you could change this to “All natural numbers have the same parity.” (a and b have the same parity if they are either both even or both odd.)

**Question:** What’s wrong with the proof?

**Answer:** The inductive step is only valid when \( n = 3 \), i.e. \( n = 2 \), since we need at least 1 element in common among the sets \( \{ h_1, \ldots, h_3 \} \) and \( \{ h_2, \ldots, h_{n+1} \} \) to conclude

\[ \text{colour}(h_1) = \cdots = \text{colour}(h_{n+1}). \]
When \( n=1 \), \( H=\{h_1,h_2\} \), and it's certainly true that \( h_1,h_2 \) all have the same colour and \( h_1,h_2 \) all have the same colour but may have colour \( \text{colour}(h_1) \neq \text{colour}(h_2) \).

So in this example, because the proof of the inductive step requires \( n=2 \), we would need to establish two base cases: \( n=1 \) and \( n=2 \).

But the \( n=2 \) base case isn't true!

---

Why is induction true?

De: We say a subset \( A \subseteq \mathbb{R} \) is well-ordered if every nonempty subset of \( A \) contains a minimum element.

Ex: Any finite subset \( A \) of \( \mathbb{R} \) is well-ordered.

No: \( \mathbb{Z} \) is not well-ordered since it does not contain a minimum element.

- \([0,1]\) is not well-ordered since, for example, the subset \((0,1) \subseteq [0,1]\) does not contain a minimum element.

Indeed: For any \( x \in (0,1) \), we have \( 0 < x < 1 \). We can then find \( y \in \mathbb{R} \) with \( 0 < y < x \) and thus \( y \in (0,1) \) and \( y < x \).

Rub: In general, it is hard to show a set is well-ordered because it is a condition on all of its subsets. But we have

Then \( \mathbb{N} \) is well-ordered. More generally, for any \( n \in \mathbb{Z} \), the set

\[ \mathbb{Z}_{\geq n} = \{ n \in \mathbb{Z} : n \geq n \} \]

is well ordered.
Before proving this, let's use it to prove (weak/regular) induction.

Theorem. Let $n \in \mathbb{Z}$, and for each $n \geq no$, let $P(n)$ be a proposition. Suppose

1. $P(n_0)$ is true
2. $\forall n > n_0, P(n) \Rightarrow P(n+1)$

Then $P(n)$ is true for all $n \geq n_0$.

Proof. Assume for a contradiction that $P(n)$ is false for some $n \geq n_0$. Then the set

$$S = \{ n \in \mathbb{Z}_{\geq n_0} : P(n) \text{ is false} \} \subseteq \mathbb{Z}_{\geq n_0}$$

is non-empty. Since $\mathbb{Z}_{\geq n_0}$ is well-ordered, $S$ has a minimum element, call it $m$.

Assumption 1 $\Rightarrow n \in S$, so $m > n_0$.

Then $m-1 \not\in S$, and since $m$ is the minimum element of $S$, $m-1 < S$, i.e. $P(m-1)$ is true. Then assumption

2 $\Rightarrow P(m)$ is true, a contradiction.

Thus $P(n)$ is true $\forall n \geq n_0$. \qed

How do you prove $\mathbb{N}$ (or $\mathbb{Z}_{\geq n_0}$) is well-ordered?

What is $\mathbb{N}$?

$\mathbb{N} = \{1, 2, 3, \ldots \}$, duh!

\[\text{What do you mean ...?}\]

Umm... what do you mean $\ldots$?

This is circular!

---

Well, I'll investigate more detail next week.

Let $\mathbb{N}$ be the intersection of all subsets $A \subseteq \mathbb{R}$ satisfying the following two properties:

1. $1 \in A$
2. For any $a \in A$, $a+1 \in A$

Consequence: If $A \subseteq \mathbb{R}$ satisfies properties 1 and 2 above, then $\forall a \in A$.
Proof that $\mathbb{N}$ is well-ordered. Let $B \subseteq \mathbb{N}$ that has no minimum element. We want to show $B = \emptyset$.

Let $A = \{ n \in \mathbb{N} : \forall b \in B, n < b \}$. Note that for any $b \in B$, $b \notin A$, so $B \subseteq \mathbb{N} \setminus A$.

In particular, to show $B = \emptyset$, it is enough to show $A = \mathbb{N}$, which is what we'll do.

As $B$ has no minimum element, $1 \notin B$. Thus $1 < b$ for all $b \in B$, i.e., $1 \in A$.

Now take any $a \in A$. So $a < b$ for all $b \in B$.

Then if we had $a + 1 \in B$, it would be a minimum element of $B$, a contradiction. So for all $b \in B$, $a + 1 < b$.

We just showed $1 \in A$ and $\forall a \in A$, $a + 1 \in A$.

This shows $\mathbb{N} \subseteq A$. Thus $A = \mathbb{N}$ and $B = \emptyset$. $\square$

Aside (You don't need to know this!) You may complain that I used $\mathbb{R}$ to define $\mathbb{N}$, as $\mathbb{N}$ seems more basic than $\mathbb{R}$. You're right! In fact to define the $\mathbb{R}$ properly (not done in this course), you need to have defined $\mathbb{N}$ first, so our above definition of $\mathbb{N}$ is circular. However, the correct definition of $\mathbb{N}$ is very similar to above.

It is an axiom (called the axiom of infinity) that there exists a set $S$ that contains something like 1 and is stable under something like $\cdot +$. We then define $\mathbb{N}$ as a subset of this $S$ in the same way as above.

The proof that $\mathbb{N}$ is well-ordered is then the same.