CSC236 Week 04: Well-Ordering, Induction Pitfalls

Hisbaan Noorani

September 30 – October 6, 2021

Contents

1 Principle of well-ordering

Every non-empty subset of $\mathbb{N}$ has a smallest element

- How would you prove this for some $S \subseteq \mathbb{N}$?

  Since $\mathbb{N}$ is bounded below by 0 and $0 \in \mathbb{N}$, we know that any subset S of $\mathbb{N}$ is also bounded below by 0. Since it is bounded below, we can say that there is a smallest element.

- Is there something similar for $\mathbb{Q}$ or $\mathbb{R}$?

  No. For example, $(0, 1) \subseteq \mathbb{Q}$, $\left\{\frac{1}{n} : n \in \mathbb{N}^+\right\}$.

- Here is the main part of proving the existence of a unique quotient and remainder

  $$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}^+, \exists q, r \in \mathbb{N} \text{ s.t. } m = qn + r \wedge 0 \leq r < n$$

  The course notes use Mathematical Induction. Well-ordering seems shorter and clearer.

2 Well-ordering example

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}^i, let R(m,n) = \{r \in \mathbb{N} : \exists q \in \mathbb{N} \text{ s.t. } m = qn + r\}$ has a smallest element

For a given pair natural numbers $m, n \neq 0$ does the set $R(m,n)$ satisfy the conditions for well-ordering?

$$R(m,n) = \{r \in \mathbb{N} : \exists q \in \mathbb{N} \text{ s.t. } m = qn + r\}$$

If so, we still need to be sure that the smallest element, r' has

1. $0 \leq r' < n$
2. That q' and r' are unique — no other pari of natural numbers would work

... in order to have

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}^+, \exists! q', r' \text{ s.t. } m = q'n + r' \wedge 0 \leq r < n$$

Proof. Let $m \in \mathbb{N}, n \in \mathbb{N}^+$. The $R(m,n)$ is a non-empty set of natural numbers. Then there is a smallest element of $R(m,n)$, let it be r', with corresponding q' such that $m = q'n + r'$.

- Case $r' < n$: This automatically satisfies our requirements.
- Case $r' \geq n$: Then we can show that there is another r'' such that $r'' < r'$ and r' is not the smallest element of the set.

  $$\begin{aligned} m &= q'n + r' && \text{(by choice of } r'\text{)} \\ &= \left(q' + 1\right) n + \left(r' - n\right) \end{aligned}$$

  Let $r'' = r' - n, q'' = q' - 1$. Then $r'' \in R(m,n)$, since $m = q''n + r''$

  Then $r'' < r'$ which is a contradiction, and thus the inital asusmption that $r' \geq n$ is false.

  So we have a pair of natural number (r', q') such that $m = q'n + r'$ and $0 \leq r' < n$. ■

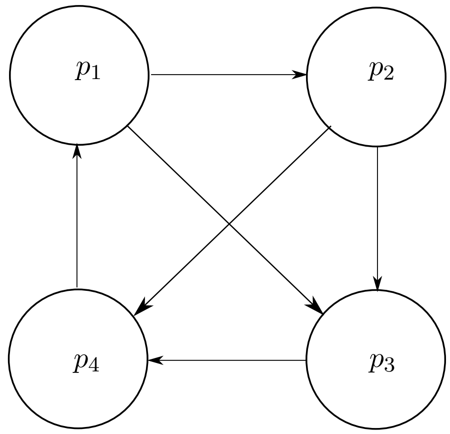
3 $P(n)$: Every round-robin tournament with n players with a cycle has a 3-cycle.

Use: every non-empty subset of $\mathbb{N}$ has a smallest element

Think of a round-robin as a complete oriented graph $G = (V,E)$, where $V = \{p_1, \ldots, p_n\}$ and every pair of distinct vertices has a uniquely directed edge between them.

If there is a cycle $p_1 \to p_2 \to p_3 \to \cdots \to p_n \to p_1$, can you find a shorter one? Can you add another directed edge without creating a 3-cycle? No, you can't.

Claim: $\forall n \in \mathbb{N}^{\geq 3}, P(n)$



Let T be a tournament with $n \geq 3$ contestants. Assume T has at least one cycle. Since there are no 1-cycles or 2-cycles (why?), T has a cycle of length at least 3. Let $C = \left\{c\ in \mathbb{N}^{\geq 3} : c \text{ is the length of a cycle in } T\right\}$. So C is a non-empty set of natural numbers, so it must have a smallest element c'.

Then, either $c' = 3$, in which case we are done, or $c' > 3$.

If $c' > 3$, there are some sub-cases to consider:

We want to show that this cycle cannot be: $p_1 \to p_2 \to p_3 \to \ldots_{c'} \to p_1$. To do this, we can find a smaller 3-cycle that contradicts this is the smallest cycle.

- Case $p_3 \to p_1$: Then there is a shorter cycle, $p_1 \to_2 \to p_3 \to p_1$, contradicting c' being the shortest cycle length.
- Case $p_1 \to p_3$: Then there is a shorter cycle, $p_1 \to p_3 \to \cdots \to p_{c'} \to_1$ has length $c' - 1$, contradicting c' being the shortest cycle length.

4 No basis?

$\forall n \in \mathbb{N}, \displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1}$ (!?)

Let $n \in \mathbb{N}$. Assume $\sum_{i=0}^{n} 2^i = 2^{n+1}$ (IH). I will show that $\sum_{i=0}^{n+1} 2^i = 2^{n+2}$.

$$\begin{aligned}
\sum_{i=0}^{n+1} 2^i &= \left[\sum_{i=0}^{n} 2^i\right] + 2^{n+1} \\
&= 2^{n+1} + 2^{n+1} && \text{(by the IH)} \\
&= 2 \cdot 2^{n+1} \\
&= 2^{n+2}
\end{aligned}$$

However, there is no verified base case!! This means that while we can prove the induction step, there is no basis to start the "infinite loop" of induction. For example, Let $n = 0, \displaystyle\sum_{i=0}^{n} 2^i = \sum_{i=0}^{0} 2^i = 2^0 = 1 \neq 2^1 = 2^n$.

5 Zero pair free binary strings, again but with well-ordering

$$f(n) = \begin{cases} 1, & n = 0 \\ 2, & n = 1 \\ f(n-1) + f(n+2), & n > 1 \end{cases}$$

$P(n)$ can follow simply from n being a natural number. You do not need to assume to $P(n-1)$ and $P(n-2)$ in order to prove this. Since the function is defined recursively, it is tempting to use induction, but you do not always need to.

6 How not to do simple induction

Does a graph $G = (V, E)$ with $|V| > 0$ have $|E| = |V| - 1$?

- Base case: Easy
- Inductive step: What happens if you try to extend an arbitrary graph with $|V| = n$ to one with $|V| = n + 1$? The claim breaks.
- Variations: What happens if you restrict the claim to connected graphs? If we make the graph cyclic, then the statement breaks again. What about acyclic connected graphs? In this final case, it becomes true.
- Take-home: Decompose rather than construct. . . except in structural induction. You never want to take an object of size n and extend it to size $n + 1$. Instead, you want to take an object of size $n + 1$, and find something related to n (and thus your inductive hypothesis) inside of it.