CSC236H1Y **Summer 2024**

Lecture 1: Well-Ordering Principle

Date: May 16, 2024

TAs: The text in red is for your eyes only. This the suggested tutorial structure: First go over the definitions and Section 1.1 on the board. Then go through the first part of Section 1.2. Write down the questions and give the students some time to solve them before going over the solutions. Suggested times below.

1.1 Well-Ordering Principle is Equivalent to Induction

This should take about 20 minutes.

Well-Ordering A — on a set S is a *total ordering* (there is a relationship between *every* pair of elements) such that every *non-empty* subset of S has a *least element.*

Well-Ordering Principle. Every *nonempty* set of $\mathbb{N}$ has a *smallest* element.

You want the two above definitions somewhere that is visible at all times.

Induction. For a predicate $P(n)$ on $n \in \mathbb{N}$,

$$(P(0) \wedge \forall k, (P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)) \implies \forall n \in \mathbb{N}, P(n).$$

In-class we showed that Induction implies the Well-Ordering Principle. It turns out that the two are *equivalent.* To show this, we prove that that the Well-Ordering Principle implies Induction.

Claim 1.1 *The Well-Ordering Principle implies Induction.*

Proof: Suppose that $P(0)$ is true and we have the implication $\forall k, (P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$. Let $S \subseteq \mathbb{N}$ be defined as the set $S \coloneqq \{s \in \mathbb{N} : \neg P(s)\}$. For the sake of contradiction, assume S is non-empty. Then, by the Well-Ordering Principle, S has a smallest element, say z. Note that $z \neq 0$ since we are given $P(0)$. Further, since z is the smallest element in S, it must follow that $P(0)$, ..., $P(z-1)$ must all be true. Recall that we have the implication $\forall k, (P(0) \wedge \cdots \wedge P(k)) \implies P(k+1)$. Substitute $z-1$ in for k. Thus $P(z)$ must be true. This is a contradiction and S must be empty. ∎

1.2 Problem Solving

The Well-Ordering Principle (WOP) is a useful problem-solving tool in its own right. The general template to prove "$\forall n \in \mathbb{N}, P(n)$" using WOP is as follows.

1. Define a set S of *counterexamples* to P being true i.e.

$$S \coloneqq \{n \in \mathbb{N} : \neg P(n)\}.$$

2. Assume for a contradiction that S is non-empty.

3. By WOP, there must be a smallest element $k \in S$.
4. Reach a contradiction — this will typically involve showing that $P(k)$ is actually true or by showing that there exists another member of S which is even smaller than k. *This requires some creativity.*
5. Conclude that S must be empty and no counterexample can exist.

Now, write the problems on the board and give the students 20 minutes to solve them. Present the solutions in the last 10 minutes. Don't worry if you don't cover everything these notes will be posted.

1. For $n \in \mathbb{N}$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

   Proof: Let $P(n)$ be the predicate $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ and let S be the set of natural number where $s \in S$ if and only if $\neg P(s)$. For a contradiction suppose S is non-empty. By WOP, let k be the minimum element of S. Then we know that $1 + 2 + \cdots + k \neq \frac{k(k+1)}{2}$ but for all $i \in \mathbb{N}$ with $i < k$, $P(i)$ is true. Note that $k \neq 0$ as $0 = \frac{0(0+1)}{2}$. Thus, $k - 1 \in \mathbb{N}$ and since $k - 1 < k$, $P(k-1)$ must be true. Note

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

   This is a contradiction, as we assumed $\neg P(k)$. Thus S must be empty. ■

2. There are no positive integers $a, b, c \in \mathbb{Z}_+$ such that $4a^3 + 2b^3 = c^3$.

   For this question, remember to emphasize the importance of extending the Well-Ordering Principle to elements of $\mathbb{Z}_+^3$ (standard WOP only applies to $\mathbb{N}$).

   Proof: Let $S = \{(x, y, z) \in \mathbb{Z}_+^3 : 4x^3 + 2y^3 = z^3\}$. For a contradiction, assume that S is non-empty. Apply WOP with lexicographical order on the triples i.e. for triples (x_1, y_1, z_1) and (x_2, y_2, z_2), first we compare x_1 and x_2, if they are equal, we compare y_1 and y_2, if *they* are equal, we compare z_1 and z_2 (*it is left as an exercise to show that the standard "$<$" on $\mathbb{N}$ with lexicographical order is a well-ordering of all elements in $\mathbb{Z}_+^3$*).

   Let (x, y, z) be the smallest element of S. Note that z^3 must be even as it is the sum of two even numbers $4x^3$ and $2y^3$. Since z^3 is even, then z must be as well. Let w be the integer $z/2$. Plug $2w$ into the formula to get $4x^3 + 2y^3 = (2w)^3 = 8w^3$. Similar arguments show that x and y are even as well and we have integers $u = x/2$ and $v = y/2$ such that $32u^3 + 16v^3 = 8w^3$. But we can divide all terms by 8 to obtain $4u^3 + 2v^3 = w^3$. This implies that $(u, v, w) \in S$ with $(u, v, w) < (x, y, z)$. This contradicts the minimality of (x, y, z) so S must be empty. ■

3. **The Division Algorithm.** Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists $q, r \in \mathbb{Z}$ (q is quotient, r is remainder) so that $a = qb + r$ and $0 \leq r < b$.

   Proof: The key is to pay attention to which set you are applying WOP to. We consider $S = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}$. Note that $S \subseteq \mathbb{N}$.

   To see that S is non-empty, take $x = -|a| \in \mathbb{Z}$, so that $a - xb = a + |a|b \geq 0$. Note that b is a positive integer ($b \geq 1$) so $a + |a|b \in S$. By WOP on $\mathbb{N}$, S contains a least element which we will call r. Since $r \in S \subseteq \mathbb{N}$, $r \geq 0$ and $r = a - qb$ for some $q \in \mathbb{Z}$. It remains to prove that $r < b$. If $r \geq b$, then

   $$0 \leq r - b = (a - qb) - b = a - (q+1)b$$

   would imply $r - b \in S$, which contradicts the fact that r is *the smallest element of* S. ■

   This question is taken from Jingyi Chen's MATH 220 notes.

Notes adapted from Chapter 2.1 to 2.3 of the MIT 6.042J Course Textbook (available online).