COMPSCI 230: Discrete Mathematics for Computer Science January 16, 2019

Lecture 3

Lecturer: Debmalya Panigrahi *Scribe: Erin Taylor*

1 Overview

In this lecture, we will introduce an intuitive principle and illustrate how it can serve as a powerful technique in proving some non-obvious theorems.

2 Well-Ordering Principle

The well-ordering principle (*WOP*):

There is a smallest number in any set of positive integers.

While this may seem obvious, what if instead we had claimed there is a greatest number in any set of positive integers?

Example 1: Consider the set of even numbers. The smallest even number is 2, but there is no greatest even integer in this set.

Our sets may not have finite size. Here are a few more examples:

Example 2: The set of positive odd integers: The smallest element in this set is 1.
Example 3: The set of positive integers divisible by 3: The smallest element in this set is 3.

Example 4: The set of positive integers *not* divisible by 3: The smallest element in this set is 1.

We will consider a few theorems to demonstrate how we may use the *WOP* in a proof.

Theorem 1. *For any rational number q we can express it as a ratio of two integers, x and y such that $y \neq 0$ and x, y are coprime.*

Recall:

Definition 1. *Two integers x and y are coprime if $gcd(x, y) = 1$, i.e. they share no common factors other than 1.*

Theorem 1 seems apparent: any rational number can be represented as a ratio of two integers. Take one such ratio, and cancel common factors until you have a fraction in lowest terms. However, this intuition does not prove the statement. Let's prove the statement formally.

Proof of Theorem 1. Assume the theorem is false, that is assume there exist rational numbers that cannot be expressed as the ratio of two integers with *gcd* 1. Let q be such a rational number. Without loss of generality, assume $q > 0$. If $q < 0$, we can redefine q as $-q$. Consider all possible ratios q can be expressed as:

$$q = \frac{x_1}{y_1} = \frac{x_2}{y_2} = \dots$$

where $y_1 \neq 0, y_2 \neq 0, \dots$. Furthermore, $y_1 > 0, y_2 > 0, \dots$ and $x_1 > 0, x_2 > 0, \dots$ since $q > 0$. We define a set of positive integers by taking the numerators of the above fractions:

$$S = \{x_1, x_2, \dots\}$$

This set may be infinite, but it is a set of positive integers so we can apply the well-ordering principle. The *WOP* implies there exists a smallest integer in S. Call this integer x^*. Then, $q = \frac{x^*}{y^*}$ for some $y^* > 0$. By our original assumption, $gcd(x^*, y^*) \geq 2$ so x^* and y^* must share a factor greater than 1, call this factor p. We have:

$$q = \frac{x^*}{y^*} = \frac{x' \cdot p}{y' \cdot p} = \frac{x'}{y'}$$

$y' \neq 0$ because $y^* \neq 0$. Thus, x' is a numerator of a ratio of two integers equal to q, so by the definition of S, it must be that $x' \in S$. However, $x' < x^*$ because $p > 1$. This is a contradiction since we assumed x^* was the smallest element of S. Therefore, our original assumption was incorrect and the theorem holds. □

Consider another theorem you are familiar with:

Theorem 2. *Every positive integer can be written as the product of primes.*

Proof. We will proceed with a proof by contradiction. Assume there exists some positive integer that cannot be written as the product of primes. Let S be the set of positive integers that do not have a prime factorization. By the *WOP* on S, there is a smallest positive integer that cannot be written as the product of primes. Call this integer n^*. Consider the following cases:

- n^* is prime. In this case, the prime factorization of n^* is n^* itself. This is a contradiction, as $n^* \in S$ so by definition does not have a prime factorization.

- n^* is composite (not prime). Then $n^* = a \cdot b$ such that $a \neq n^*, a \neq 1$ and $b \neq n^*, b \neq 1$. This implies that $a < n^*$ and $b < n^*$. Since n^* is the smallest element of S, $a \notin S$ and $b \notin S$. Therefore, a, b have prime factorizations:

  $$a = p_1 \cdots p_k$$

  $$b = q_1 \cdots q_\ell$$

  for prime numbers $p_1, \dots, p_k, q_1, \dots, q_\ell$. But,

  $$n^* = a \cdot b = p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_\ell.$$

  This is a prime factorization of n^*. This is a contradiction of our original assumption.

In all cases, we reached a contradiction. Thus, our original assumption was incorrect and every positive integer can be written as the product of primes. □

3 Well-Ordered Sets

Definition 2. *A* well-ordered set *is a set S such that each non-empty subset of S has a minimum element.*

In other words, the well-ordering principle states that the set of all positive integers is well-ordered. Consider the following claim:

Claim 3. *The set of integers that are $\geq -n$ for any integer n is well-ordered.*

Proof. Let S be a subset of integers such that $\forall s \in S, s \geq -n$. Define a new set as follows:

$$S' = \{s + n + 1 \ : \ s \in S\}$$

This notation means that for every element s in S add element $(s + n + 1)$ to set S'. For each $s \in S, s \geq -n$ implies that $s + n \geq 0$, so $s + n + 1 \geq 1$. Thus, S' is a set of positive integers. By the well-ordering principle there is a smallest integer in S'. Let this integer be x^*. Then, the smallest integer in S is $s = x^* - (n + 1)$ and the claim is true. □

Theorem 4. *Any set of integers with a lower bound is well-ordered.*

Before proving this theorem, let's define a lower bound:

Definition 3. *A* lower bound *of a set S is any real number y such that $y \leq s$ $\forall s \in S$.*

Observe that a lower bound is not unique. $0, 1$, and -100 are all lower bounds on the set of positive integers. For the set of all positive integers, 1 is the largest lower bound. We can similarly define an upper bound:

Definition 4. *A* upper bound *of a set S is any real number y such that $s \leq y$ $\forall s \in S$.*

We can now prove the theorem:

Proof of Theorem 4. Let S be a subset of integers with a lower bound. Let y be one such lower bound. Define a new set as follows:

$$S' = \{s - y + 1 | s \in S\}$$

Since y is a lower bound, $s \geq y$ $\forall s \in S$. This implies $s - y \geq 0$, and thus $s - y + 1 \geq 1$. Therefore, S' is a set of positive integers. By the well-ordering principle there is a smallest integer in S'. Let this integer be x^*. Then, the smallest integer in S is $s = x^* + y - 1$. □

Theorem 5. *Any set of integers with an upper bound has a maximum element.*

Proof. Let S be a subset of integers with an upper bound. Let y be one such upper bound. Define a new set as follows:

$$S' = \{y + 1 - s | s \in S\}$$

Since y is an upper bound, $s \leq y$ $\forall s \in S$. For all $s \in S$, this implies $y - s \geq 0$ and therefore $y + 1 - s \geq 1$. Thus, S' is a set of positive integers. By the well-ordering principle, S' has a smallest integer. Let this integer be x^*. Then, the largest integer in S is $s = y + 1 - x^*$. □

Why are these theorems not immediately obvious? Consider the following (false) claim:

Claim 6. *Any set of rational numbers with a lower bound is well-ordered.*

Counter Example: Define the following set of rational numbers:

$$S = \{1 + x \mid x \text{ is any rational number s.t. } 0 < x < 1\}$$

S has a lower bound of 1. For the claim to hold, we would need to show that every non-empty subset of S has a minimum element. In particular, this implies that S must have a minimum element. Let this be $x^* = 1 + \frac{p}{q}$ for some integers p, q where $p, q > 0$. Now define $x' = 1 + \frac{p}{q+1}$.

$0 < \frac{p}{q+1} < 1$ because $0 < \frac{p}{q} < 1$. Additionally $\frac{p}{q+1}$ is rational because $\frac{p}{q}$ is rational. Thus, $x' \in S$. However, $x' < x^*$, which contradicts our assumption that x^* was the smallest element of S. Thus, S is not well-ordered and the claim is false.

An intuitive idea about the well-ordered property is as follows: You start with some number in the set and you consider smaller and smaller elements. Eventually, there will not be a smaller element left to consider. For the set of positive integers you may start at 5 and begin counting down to 1, where you stop. This idea captures the fact that there can be no infinite length decreasing sequence from a fixed starting point in a well-ordered set. Otherwise, there would always exist a smaller element in the set and there would be no minimum. Recall some examples of familiar infinite decreasing sequences:

Example 5: The negative integers: $-1, -2, -3, \ldots$

Example 6:

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots \frac{1}{x}, \frac{1}{x+1}, \ldots$$

Although a well-ordered set does not have a decreasing sequence of infinite length, we will shortly see that a well-ordered set *can* have decreasing sequences of arbitrarily large finite length.

Using the definition of well-ordered sets, we can prove the following observation:

Observation 7. *A well-ordered set cannot contain a decreasing sequence of infinite length.*

Proof. Let S be any well-ordered set, and for contradiction, suppose S contains a sequence A of decreasing numbers with infinite length. Thus, A is of the form $(a_1, a_2, a_3, \ldots)$ where $a_1 > a_2 > a_3 > \cdots$. Since each term of A is smaller than the preceding term and A has infinite length, A does not contain a minimum element. However, since A is a subset of S and S is well-ordered, the set A *does* have a minimum element. Since no set cannot simultaneously contain and *not* contain a minimum element, we conclude that S does not contain a decreasing sequence of infinite length. □

However, it is possible for a well-ordered set to contain decreasing sequences that are *arbitrarily long*. More precisely, there are well well-ordered sets that satisfy the following property: for any positive integer k, there exists a decreasing sequence of length k in the set. (Note that the set of positive integers is such a set: simply take the sequence $(k, k-1, \ldots, 2, 1)$.)

Now let us consider the following subset of rational numbers:

$$S = \left\{ \frac{n}{n+1} : n \text{ is a positive integer} \right\} = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots \right\}.$$

Theorem 8. *The set S, defined above, is well-ordered.*

To prove Theorem 8, we will first prove a useful lemma that allows us to order the elements of S by simply looking at their numerators.

Lemma 9. *If n_1 and n_2 are positive integers such that $n_1 < n_2$, then $\frac{n_1}{n_1+1} < \frac{n_2}{n_2+1}$.*

Proof. Let n_1 and n_2 be positive integers such that $n_1 < n_2$. Adding $n_1 n_2$ to both sides gives us

$$n_1 n_2 + n_1 < n_1 n_2 + n_2.$$

Factoring n_1 from the left and n_2 from the right yields

$$n_1(n_2 + 1) < n_2(n_1 + 1).$$

Finally, dividing the left by $(n_1 + 1)$ and the right by $(n_2 + 1)$ yields

$$\frac{n_1}{n_1 + 1} < \frac{n_2}{n_2 + 1},$$

as desired. □

(Note that starting with the conclusion, cross-multiplying, simplifying, and stating that all steps are reversible is an equally valid proof of Lemma 9). We now use Lemma 9, combined with the fact that the set of positive integers is well-ordered, to prove that S is well-ordered.

Proof of Theorem 8. To prove that S is well-ordered, we need to show that any subset of S contains a minimum element. Thus, let A be a subset of S, and define the set B as follows:

$$B = \left\{ k : \frac{k}{k+1} \in A \right\}.$$

In other words, B is the set of numerators that appear in the fractions of A. Since B is a subset of the set of positive integers (which is well-ordered), B contains a minimum element which we denote by b. Since b is the smallest numerator appearing in A, by Lemma 9 we have

$$\frac{b}{b+1} < \frac{a}{a+1}$$

where a is any integer larger than b. In particular, a can be any other numerator that appears in A, so this means $\frac{b}{b+1}$ is the the minimum element of A. □

Recall that we denote the set of positive integers by the symbol $\mathbb{Z}^+$, and this set is well-ordered. Now consider the the following set:

$$\mathbb{Z}^+ + S = \left\{ n + s : n \in \mathbb{Z}^+, s \in S \right\}.$$

In other words, this set is formed by adding all possible (n, s) pairs, where n is a positive integer and s is an element of S (as defined above). For example, $1 + \frac{1}{2}$ and $5 + \frac{8}{9}$ are elements of this set. Both $\mathbb{Z}^+$ and S are well-ordered; we now show that their sum is also well-ordered.

Theorem 10. *The set $\mathbb{Z}^+ + S$ is well-ordered.*

The basic idea of the proof is fairly simple: the elements of $\mathbb{Z}^+ + S$ each have an integer component and a fractional component. To be the minimum element of some subset, the integer component should first be minimized, and then the fractional component should be minimized. We formalize this idea in the following proof.

Proof. Let A be any subset of $\mathbb{Z}^+ + S$. Define a set B as follows:

$$B = \{k : k + s \in A \text{ for some } s \in S\}.$$

In other words, B is the set of integers that appear in the "n" position in the definition of $\mathbb{Z}^+ + S$. Since B is a subset of positive integers, B contains a minimum element which we denote by n^*. Now consider the set A_{n^*}, defined as follows:

$$A_{n^*} = \{s \in S : n^* + s \in A\}.$$

In other words, A_{n^*} contains the elements of S that are paired with n^* as part of an element of A. Since A_{n^*} is a subset of S (which is well-ordered, by Theorem 8), A_{n^*} contains a minimum element which we denote by s^*.

Finally, we claim that $n^* + s^*$ is the minimum element of A. From the definitions of B and A_{n^*}, it should be clear that $n^* + s^*$ is an element of A. Now consider any other element of A; suppose it is $x + y$ where $x \in \mathbb{Z}^+$ and $y \in S$. We will show $n^* + s^* < x + y$ by considering two cases:

1. If $n^* = x$, then by definition of s^*, we have $s^* < y$. This means $n^* + s^* < x + y$.

2. If $n^* < x$, then $n^* + s^* < n^* + 1 \leq x + y$ because n^* and x are integers, and every element of S is less than 1.

In either case, we have $n^* + s^* < x + y$, so $n^* + s^*$ is the minimum element of A, as desired. □

To better understand the proof, we now illustrate its main idea with an example. Suppose the given subset of $\mathbb{Z}^+ + S$ is the following:

$$A = \left\{5 + \frac{1}{2}, 3 + \frac{3}{4}, 6 + \frac{8}{9}, 3 + \frac{2}{3}, 10 + \frac{10}{11}, 3 + \frac{99}{100}\right\}.$$

Then following the definitions given in the proof above, we have

$$B = \{5, 3, 6, 10\}.$$

The minimum element of B is 3, so we have $n^* = 3$. Continuing, we have

$$A_{n^*} = A_3 = \left\{\frac{3}{4}, \frac{2}{3}, \frac{99}{100}\right\}.$$

The minimum element of A_3 is $\frac{2}{3}$, so we have $s^* = \frac{2}{3}$. To conclude, $n^* + s^* = 3 + \frac{2}{3}$ is the minimum element of A. Note that in this example, Theorem 10 is easy to verify because A is a finite set, but in general, A can be any subset of $\mathbb{Z}^+ + S$ (even one with infinitely many elements).

Finally, we conclude with an observation that illustrates the difference between "infinite length" and "arbitrarily long."

Observation 11. *For any positive integers n, k where $n \geq 2$, there exists a decreasing sequence of length k in the set $\mathbb{Z}^+ + S$, such that every element of the sequence is less than n.*

For example, if $n = 3$ and $k = 5$, we can use the sequence

$$\left(2 + \frac{5}{6}, 2 + \frac{4}{5}, 2 + \frac{3}{4}, 2 + \frac{2}{3}, 2 + \frac{1}{2}\right).$$

Since a similar sequence can be exhibited for any value of k (which can be extremely large), we can conclude $\mathbb{Z}^+ + S$ contains decreasing sequences that are arbitrarily long. However, recall that Observation 7 states that a well-ordered set cannot contain a decreasing sequence of infinite length (which we showed earlier). These two observations illustrate the difference between "arbitrarily long" and "infinite."

4 Summary

In this lecture, we considered the well-ordering principle and discussed well-ordered sets. We used the well-ordering principle to formally prove familiar theorems. We also showed that this principle can be used to show that various sets are well-ordered. Finally, we saw a well-ordered set that contains arbitrarily long decreasing sequences.