Lecture 13 - The Well-Ordering Principle

6.042 - April 1, 2003

The well-ordering principle says that *every nonempty subset of the natural numbers contains a smallest element*. For example, the smallest element of the set $\{5, 11, 23, 24, 31\}$ is 5, and the smallest element of the set of prime numbers is 2. In logic notation, the well-ordering principle can be expressed as follows:

$$\forall S \subseteq \mathbb{N}\ (S \neq \emptyset \to \exists x \in S\ \forall y \in S\ x \leq y)$$

This restatement motivates a short digression on style. Logic notation should be used only in very limited circumstances. If there is great need for brevity or exactitude, use logic notation. But encrypting your ideas using funny symbols simply requires others to spend time decrypting them later. Stick to plain language where possible.

At first glance, the well-ordering principle may seem obvious and useless. On the "obvious" front, note that not every subset of the *integers* has a smallest element. And not every subset of the *nonnegative real numbers* has a smallest element either; for example, what is the smallest real number greater than 3? As for "useless", we shall see that the well-ordering prinicple is precisely as powerful as mathematical induction!

1 Elementary Examples

Let's use the well-ordering principle to prove some elementary results.

Theorem 1 *The following equation holds for all $n \in \mathbb{N}$:*

$$\sum_{i=1}^{n} i \quad = \quad \frac{n(n+1)}{2}$$

Proof. Suppose that the claim is false. Let S be the set of all $n \in \mathbb{N}$ for which the equation does not hold. By our supposition that the claim is false, the set S is nonempty. By the well-ordering principle, S has a smallest element. This smallest element can not be 0, because the equation holds for $n = 0$. Therefore, the smallest element of S must be some integer $s > 0$. Since $s - 1$ is in $\mathbb{N}$ and is not in S, the equation must hold for $n = s - 1$. Therefore, we have:

$$\begin{aligned}\sum_{i=1}^{s} i &= s + \sum_{i=1}^{s-1} i \\ &= s + \frac{(s-1)s}{2} \\ &= \frac{s(s+1)}{2}\end{aligned}$$

In the first step, we break out the last term of the summation. In the second step, we use the fact that the equation holds for $n = s - 1$. The third step uses only algebra. Overall, this implies that the original equation holds for $n = s$. This contradicts the definition of s. Therefore, our supposition must be wrong, and the claim is true. □

Theorem 2 *There is no natural number between 0 and 1.*

Proof. Suppose that there is at least one natural number between 0 and 1; we'll show that this leads to a contradiction. Let S be the set of all natural numbers between 0 and 1. By our supposition, S is nonempty. By the well-ordering principle, S contains a smallest element a. Since a is an element of S, it lies between 0 and 1; that is:

$$0 < a \qquad \text{and} \qquad a < 1$$

Squaring both sides of the left inequality gives $0 < a^2$. Squaring both sides of the right inequality gives $a^2 < 1$. Multiplying both sides of the right inequality by a gives $a^2 < a$. Finally, note that $a^2 = a \cdot a$ is a natural number, because it is the product of two natural numbers. Putting all this together, a^2 is a natural number between 0 and 1 that is strictly smaller than a. This contradicts the definition of a. Therefore, our supposition that there exists a natural number between 0 and 1 was false, and thus the claim is true. □

The second result is usually called the *division algorithm*. However, since there is no algorithm in sight, we'll break with tradition and call it the *division lemma*[1].

Lemma 3 *Let a and b be natural numbers such that $b > 0$. Then there exist natural numbers q and r such that $a = bq + r$ and $0 \leq r < b$.*

Note that q and r in the lemma are simply the quotient and remainder when one divides a by b. For example, dividing $a = 23$ by $b = 10$ gives quotient $q = 2$ and remainder $r = 3$. Sure enough, we have $a = bq + r$, since $23 = 10 \cdot 2 + 3$.

[1] Admittedly, this name change creates a slight risk that someone else might prove another division lemma and then refer to them collectively as the *division lemmata*. But if that happens, we'll deal with that someone. Oh yes.

Proof. Define the set S as follows:

$$S = \{r \in \mathbb{N} \mid r = a - bq \text{ for some } q \in \mathbb{N}\}$$

The set S is nonempty; in particular, it must contain a, since $a = a - bq$ when q is zero. Therefore, by the well-ordering principle, S contains a smallest element, r_0. Let q_0 be the corresponding value of q, so that $r_0 = a - bq_0$.

All that remains is to show that $0 \leq r_0 < b$. The left inequality is immediate, since S contains only natural numbers. Now suppose that the right inequality does not hold; that is, $r_0 \geq b$. We'll show that this leads to a contradiction. Let $r_1 = r_0 - b$. Then we have:

$$0 \leq r_1 < r_0$$

The left inequality follows from the supposition that $r_0 \geq b$. The right inequality comes from the fact that $b > 0$. Now we have:

$$\begin{aligned} r_1 &= r_0 - b \\ &= (a - bq_0) - b \\ &= a - b(q_0 + 1) \end{aligned}$$

The first step uses the definition of r_1. In the second, we substitute in an expression for r_0. The last step uses algebra. Since r_1 can be expressed in this way, r_1 is an element of S. Since r_1 is smaller than r_0, we have contradicted the definition of r_0. Thus, our supposition was wrong, and so $r_0 < b$. □

2 The Difference Game

The *Difference Game* begins with two positive integers on a chalkboard. There are two players, who alternate turns. On a player's turn, he or she must write a new positive number on the board which is the difference of two numbers that are already there. The first player who is unable to form a new number loses.

Hypothetically, suppose that a game begins with the numbers 60 and 42 and that the players are Charles-Jean-Gustave-Nicholas de la Valleé-Poussin, who proved the celebrated Prime Number Theorem in 1896, and Bubba, the guy who picks up my trash on Friday mornings. The game might proceed as follows:

		60	
		42	
Poussin	→	18	$(= 60 - 42)$
Bubba	→	24	$(= 42 - 18)$
Poussin	→	6	$(= 24 - 18)$
Bubba	→	54	$(= 60 - 6)$
Poussin	→	36	$(= 54 - 18)$
Bubba	→	30	$(= 36 - 6)$
Poussin	→	12	$(= 36 - 24)$
Bubba	→	48	$(= 60 - 12)$
Poussin	→	LOSES!	

Notice that the numbers on the board are all the multiples of 6 less than or equal to 60. While Bubba prances about shouting "Booyah!", we'll prove that Charles-Jean-Gustave-Nicholas was doomed from the outset. The winner of the Difference Game is determined by the starting numbers and who goes first. The strategies of the two players are irrelevant!

First, we need a some definitions.

- Let a and b be natural numbers. We say a *divides* b if there exists an $m \in \mathbb{N}$ such that $am = b$. We indicate that a divides b in symbols by $a \mid b$. For example, $10 \mid 30$, but it is not true that $7 \mid 13$.

- If a divides b, then a is called a *divisor* of b, and b is called a *multiple* of a. For example, the divisors of 12 are 1, 2, 3, 4, 6, and 12, and the multiples of 12 are 0, 12, 24, 36, etc.

- If $d \in \mathbb{N}$ divides both a and b, then d is called a *common divisor* of a and b. The greatest common divisor of a and b is denoted $\gcd(a, b)$. For example, the common divisors of 60 and 42 are 1, 2, 3, and 6, and $\gcd(60, 42) = 6$.

Now we're ready to analyze the Difference Game! Not surprisingly, we use the well-ordering principle.

Theorem 4 *Suppose that the Difference Game begins with the numbers M and N where $M \geq N$. The numbers generated during the game are all of the positive multiples of $\gcd(M, N)$ up to M.*

The example game began with the numbers $M = 60$ and $N = 42$. The greatest common divisor of M and N is 6. Sure enough, the set of numbers generated consists of all multiples of 6 up to 60.

Proof. We begin by defining some variables:

$$\begin{aligned} S &= \text{The set of numbers generated during the game, including } M \text{ and } N. \\ d &= \text{The smallest element of } S. \\ g &= \gcd(M, N) \end{aligned}$$

Note that d exists by the well-ordering principle, since S is a nonempty subset of the natural numbers. We structure the remainder of the proof by stating and proving four claims.

1. Every number generated is a multiple of the gcd **of the starting numbers.**

In terms of our variables, we must show that every element of S is a multiple of g. Suppose not. Then, by the well-ordering principle, we can select the first-generated element of S that is not a multiple of g.[2] Call this x_0. Since M and N are both multiples of g, x_0 can not be a starting number. Therefore x_0 must be equal to $x_1 - x_2$, where x_1 and x_2 are previously-generated numbers. Since they were generated before x_0, both are x_1 and x_2 are multiples of g. But then $x_1 - x_2 = x_0$ is a multiple of g. This is a contradiction. Therefore, our supposition was wrong; every element of S is a multiple of g.

2. Every number generated is a multiple of the smallest number generated.

In other words, we must show that every element of S is a multiple of d. Suppose that x is an element of S, but not a multiple of d. Then, by the division lemma, $x = dq + r$ where $0 \leq r < d$. But then the number $r = x - dq$ can be generated by repeatedly subracting d from x, a total of q times. Therefore, r is an element of S that is smaller than d, which was defined to be the smallest element of S. This is a contradiction. Therefore, every element of S is a multiple of d.

3. The smallest number generated is the gcd **of the starting numbers.**

We must show that $d = g$. On one hand, $g \leq d$ because d is an element of S and g divides every element of S by claim 1. On the other hand, $d \leq g$, because d is a common factor of M and N by claim 2, and g is the greatest common factor of M and N. Therefore, $d = g$; that is, the smallest number generated is the gcd of the starting numbers.

4. The numbers generated are the positive multiples of $\gcd(M, N)$ **up to** M**.**

By claim 3, the smallest number generated is $g = \gcd(M, N)$. All remaining multiples of g up to M can be generated by repeatedly subtracting g from M. Claims 1 and 2 both imply that no other numbers less than M are generated. No numbers larger than M can be generated by taking differences. Therefore the set S of numbers generated is precisely the set of all positive multiples of g up to M. □

Corollary 5 *Suppose that the Difference Game begins with the numbers M and N where*

[2] The use of the well-ordering principle here is somewhat subtle. Let $s_1, s_2, \ldots$ be the sequence of numbers generated during the game, where $s_1 = M$ and $s_2 = N$. Let T be the set of all i such that s_i is not a multiple of g. By our supposition, T is nonempty. By well-ordering, it has a smallest element, j. Then s_j is the first-generated element of S that is not a multiple of g.

$M \geq N$. The first player wins if and only if $M/\gcd(M, N)$ is odd.

Proof. According to the theorem, the set of all numbers generated during the game has size $M/\gcd(M, N)$. The number of player turns is 2 less, because M and N are in this set at the beginning. Thus, if this fraction is odd, the number of turns is odd, and so the first player gets the last turn and wins. If this fraction is even, the second player gets the last turn, and the first player loses. □

3 Weak Induction, Strong Induction, and the Well-Ordering Principle

Remarkably, weak induction, strong induction, and the well-ordering principle all amount to the same thing. In particular, if you adopt any one as an exiom, the other two can be proved as theorems.

Theorem 6 *The following are equivalent:*

1. *Strong induction: if $P(0)$ is true and for all $n \in \mathbb{N}$, $P(0) \wedge \ldots \wedge P(n)$ implies $P(n+1)$, then $P(n)$ is true for all $n \in \mathbb{N}$.*

2. *Weak induction: if $P(0)$ is true and $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.*

3. *Well-ordering principle: every nonempty subset of the natural numbers has a smallest element.*

Many theorems are similar to this one in overall structure; that is, they assert that several different statements $S_1, S_2, \ldots, S_n$ are all equivalent. This means that each statement logically implies all the others; that is $S_i \rightarrow S_j$ for all i and j.

There is a trick to proving theorems with this structure. It is sufficient to prove a *cycle* of implications, such as $S_1 \rightarrow S_2$, $S_2 \rightarrow S_3$, and $S_3 \rightarrow S_1$. Then transitivity gives all the other possible implications for free. For example, $S_1 \rightarrow S_2$ and $S_2 \rightarrow S_3$ together imply that $S_1 \rightarrow S_3$, so we don't have to prove that one explicitly. This observation saves a lot of work!

Proof. We show that 1 implies 2, 2 implies 3, and 3 implies 1.

$\underline{1 \rightarrow 2}$ First, we assume that strong induction is valid, and prove that weak induction follows as a consequence.

We begin with the assumptions of weak induction; namely, $P(0)$ is true and $P(n) \rightarrow P(n+1)$ for all $n \in \mathbb{N}$. It follows that $P(0) \wedge \ldots \wedge P(n) \rightarrow P(n+1)$ for all $n \in \mathbb{N}$. (Here we are using the general fact that, if $B \to C$, then $A \wedge B \to C$.) Therefore, the conclusion of weak induction, that $P(n)$ is true for all $n \in \mathbb{N}$, follows by strong induction.

<u>$2 \to 3$</u> Next, we assume weak induction in order to prove the well-ordering principle.

Let S be a nonempty subset of the natural numbers. "Nonempty" means that S contains at least one natural number $n \in \mathbb{N}$. Below, we use weak induction to prove that for all $n \in \mathbb{N}$, every set of natural numbers that contains at least one number between 0 and n has a smallest element. This implies that the set S contains a smallest element, as desired.

All that remains is to complete the inductive argument. Let $P(n)$ be the hypothesis that every set $S \subseteq \mathbb{N}$ that contains a number between 0 and n has a smallest element. First, note that $P(0)$ is true; if S contains 0, then 0 must be the smallest element of S, since there is no smaller natural number at all. Now suppose that $P(n)$ is true and consider a set $S \subseteq \mathbb{N}$ that contains a number between 0 and $n+1$. There are two cases to consider. If S contains a number between 0 and n, then $P(n)$ implies that S contains a smallest element. Otherwise, S contains $n+1$ and contains none of the numbers from 0 to n. In this case, $n+1$ is the smallest element of S. Thus, $P(n)$ implies $P(n+1)$, and so $P(n)$ is true for all $n \in \mathbb{N}$ by weak induction.

<u>$3 \to 1$</u> Finally, we assume the well-ordering principle in order to prove strong induction.

We begin with the assumptions of strong induction; namely, $P(0)$ is true and $P(0) \wedge \ldots \wedge P(n) \to P(n+1)$ for all $n \in \mathbb{N}$. We use well-ordering to reach the conclusion of strong induction; that is, that $P(n)$ is true for all $n \in \mathbb{N}$.

Let S be the set of natural numbers for which $P(n)$ is false. Suppose that S is nonempty. Then, by the well-ordering principle, S contains a smallest element n_0. We must have $n_0 > 0$, since $P(0)$ is true by assumption. Furthermore, since n_0 is the smallest element of S, $P(0) \wedge \ldots \wedge P(n_0 - 1)$ must be true. But this implies that $P(n_0)$ is true as well, contradicting the fact that n_0 is an element of S. Therefore, our supposition must be wrong; actually, the set S is empty, which means that $P(n)$ is true for all $n \in \mathbb{N}$. □