MATHEMATICS 300 — SPRING 2015

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

LECTURE ON WELL-ORDERING

Contents

1 The well ordering principle

The ***well ordering principle*** is a very powerful tool for proving results about the natural numbers. Every proof by induction can easily be transformed into a proof by well ordering, but there are many proofs by well ordering that cannot easily be turned into a proof by induction[1].

In this section we are going to

1. state the well ordering principle,
2. prove it,
3. give examples of proofs using well ordering.

1.1 Statement of the well ordering principle

Theorem 1. *Every nonempty set of natural numbers has a smallest member.*

In formal language, this says that

$$(\forall S)((S \subseteq \mathbb{N} \wedge S \neq \emptyset) \Longrightarrow (\exists \bar{s})(\bar{s} \in S \wedge (\forall s \in S)\bar{s} \leq s)) .$$

1.2 Proof of the well ordering principle

First we prove a lemma[2]:

Lemma 1. *If n is a natural number and S is a subset of $\mathbb{N}$ such that $n \in S$, then S has a smallest member.*

Proof. We want to prove that

$$(1.1)\ (\forall n \in \mathbb{N})(\forall S)\Big((S \subseteq \mathbb{N} \wedge n \in S) \Longrightarrow S \text{ has a smallest member}\Big) .$$

[1]The key word here is "easily". Every proof by well ordering can be reformulated as a proof by induction, but often this is rather complicated.

[2]Recall that a *lemma* is a result one proves as a preliminary towards proving a theorem.

Let $P(n)$ be the sentence

$$(\forall S)\Big((S \subseteq \mathbb{N} \wedge n \in S) \Longrightarrow S \text{ has a smallest member}\Big).$$

We want to prove that $(\forall n \in \mathbb{N})P(n)$. And we will do this by induction.

The base case. We want to prove that $P(1)$ is true. But $P(1)$ says that if S is a subset of $\mathbb{N}$ and $1 \in S$ then S has a smallest member. But this is obviously true because 1 is the smallest member of S, since 1 is less than or equal to every natural number, so in particular it is less than or equal to every member of S.

The inductive step. We want to prove that $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

Let n be an arbitrary natural number. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.

Now, $P(n+1)$ says that

$$(\forall S)\Big((S \subseteq \mathbb{N} \wedge n+1 \in S) \Longrightarrow S \text{ has a smallest member}\Big).$$

To prove this, let S be an arbitrary set.

Assume that $S \subseteq \mathbb{N}$ and $n+1 \in S$. We want to prove that S has a smallest member.

Clearly, either n belongs to S or it does not.

If $n \in S$ then it follows from the inductive hypothesis $P(n)$ that S has a smallest member. (Recall that $P(n)$ says that if a subset X of $\mathbb{N}$ is such that $n \in X$ then X has a smallest member.)

Next consider the case when $n \notin S$.

In that case, let us form a new set T by adding n to S. That is, let us introduce a set T defined by

$$T = \{x : x \in S \vee x = n\}.$$

Then $T \subseteq \mathbb{N}$ (because $S \subseteq \mathbb{N}$ and $n \in \mathbb{N}$) and $n \in T$.

So by the inductive hypothesis (which says that a subset X of $\mathbb{N}$ for which $n \in X$ has a smallest member), T has a smallest member. Call this smallest member $\bar{t}$.

Then $\bar{t} \in T$, and $\bar{t} \leq t$ for every $t \in T$.

In particular, $\bar{t} \leq s$ for every $s \in S$ (because every member of S is a member of T).

There are two possibilities: $\boxed{\bar{t} \in S}$ or $\boxed{\bar{t} \notin S}$.

Assume that $\boxed{\bar{t} \in S}$.

Then $\bar{t}$ is a member of S that is smaller than or equal to every member of S. So $\bar{t}$ is the smallest member of S. Hence $\boxed{S \text{ has a smallest member}}$.

Now consider the case when $\boxed{\bar{t} \notin S}$. Since $\bar{t} \in T$, and the only member of T that can possibly not be in S is n, it follows that $\bar{t} = n$.

Hence $n \leq s$ for every $s \in S$.

Let s be an arbitrary member of s.

Then $s \geq n$.

So $s > n$, because if s was equal to n then n would be in S, and we are assuming that $n \notin S$.

But then $s \geq n+1$. Reason: Suppose not. Then $s < n+1$. But we have shown that $s > n$. So $n < s < n+1$. But we know that there do not exist any natural numbers that lie between n and $n+1$. (This was proved in Theorem 3 of the Notes on the Feb. 26 lecture, page 2.)

So we have shown that $s \geq n+1$ for every member s of S.

In addition, we are assuming that $n+1 \in S$. Hence $n+1$ is the smallest member of S.

So $\boxed{S \text{ has a smallest member}}$.

We have proved that S has a smallest member in each of the two cases $\bar{t} \in S$ and $\bar{t} \notin S$. It then follows, using the Proof by Cases Rule, that $\boxed{S \text{ has a smallest member}}$.

We have proved that S has a smallest member assuming that $S \subseteq \mathbb{N}$ and $n+1 \in S$. Hence

(1.2) $(S \subseteq \mathbb{N} \wedge n+1) \in S \Longrightarrow S$ has a smallest member.

We have proved (1.2) under the assumption that S was an arbitrary set. Hence

$$(\forall S)\Big((S \subseteq \mathbb{N} \wedge n+1 \in S) \Longrightarrow S \text{ has a smallest member}\Big). \tag{1.3}$$

But (1.3) is exactly statement $P(n+1)$. So we have proved $P(n+1)$.

We have proved $P(n+1)$ assuming $P(n)$. It then follows that $P(n) \Longrightarrow P(n+1)$.

We have proved that $P(n) \Longrightarrow P(n+1)$ for an arbitrary $n \in \mathbb{N}$.

Hence $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$. This completes the inductive step.

It follows from the PMI that $(\forall n \in \mathbb{N})P(n)$. **Q.E.D.**

Having proved the lemma, the proof of the well ordering principle is easy.

Proof of Theorem 1. Let S be a nonempty subset of $\mathbb{N}$. Then we may pick a member of S and call it n. Then n is a natural number and $n \in S$. So by the lemma S has a smallest member. **Q.E.D.**

1.3 An example of a proof using well-ordering

Theorem 2. *Every natural number n such that $n \geq 2$ is a product of primes.*

Clarification: What is a "product of primes"? A natural number n is a product of primes if there exist

1. a natural number k,

and

2. prime numbers $p_1, \ldots, p_k$

such that $n = \prod_{i=1}^{k} p_i$. Notice that k *can be equal to one.* That is, *a single prime, such as* 2, *or* 3, *or* 23, *is a product of primes in the sense of our definition.*

So the following natural numbers are products of primes: 7 (because it is prime), 24 (because $24 = 2 \times 2 \times 2 \times 3$).

Proof of the theorem. Let B be the set of all natural numbers n such that $n \geq 2$ and n is not a product of primes. (Think of the members of B as "bad" numbers, in the sense that we don't want them to be there at all; we want to prove that there are no bad numbers.)

We want to prove that the set B is empty. For this purpose, we assume that B is not empty and try to get a contradiction.

So assume that $B \neq \emptyset$. By the well-ordering principle, B has a smallest member b. Then $b \in B$, so

a. b is a natural number,

b. $b \geq 2$,

c. $\boxed{b \text{ is not a product of primes}}$.

And, in addition,

d. b is the smallest member of B, that is,

$$(\forall m)(m \in B \Longrightarrow m \geq b)\,.$$

Since b is not a product of primes, it follows in particular that b is not prime. (Reason: if b was prime, then b would be a product of primes according to our definition.) Then we can pick natural numbers j, k such that

$$b = jk\,, \qquad j > 1\,, \qquad \text{and} \quad k > 1\,.$$

Then $j < b$, because $b = jk$ and $k > 1$. So $j \notin B$ (because b is the smallest member of B, and $j < b$). And $j \geq 2$ (because $j > 1$). This means that j is a product of primes (because if j wasn't a product of primes it would be in S).

Similarly, k is a product of primes. So we can write $j = \prod_{i=1}^{m} p_i$ and $k = \prod_{\ell=1}^{\mu} q_\ell$, where the p_i and the q_ℓ are primes. But then

$$b = \Big(\prod_{i=1}^{m} p_i\Big) \times \Big(\prod_{\ell=1}^{\mu} q_\ell\Big)\,,$$

so $\boxed{b \text{ is a product of primes}}$. But $\boxed{b \text{ is not a product of primes}}$. So we got two contradictory statements.

This contradiction was derived by assuming that $B \neq \emptyset$. So $B = \emptyset$, and this proves that every natural number n such that $n \geq 2$ is a product of primes, which is our desired conclusion. **Q.E.D.**

Remark 1. ***The fundamental theorem of arithmetic (FTA).*** This theorem is one of the most important results in integer arithmetic. It says that every natural number greater than 2 can be written as a product of primes in a unique way. (That is, not only is the number equal to a product of primes, but there is only one way to write it as a product of primes.) We have proved a part of the FTA, namely, the assertion that if $n \in \mathbb{N}$ and $n \geq 2$ then n can be written as a product of primes. What have not proved is the uniqueness of the factorization. This is much more delicate, and we will prove it later. At this point, just notice that even *defining* what "uniqueness" of the factorization of n into primes means is not a trivial question. For example, we can write the number 6 as a product of primes in this way:

$$6 = 2 \times 3\,,$$

but we can also write it as

$$6 = 3 \times 2\,.$$

Are these two expressions different ways of factoring 6 as aproduct of primes, or are they "the same"? Obviously, they must be "the same". because if they were different then the factorization of 6 as a product of primes would not be unique, and the FTA would not be true.

This means that we will have to be very precise, and define very carefully what "writing a number as a product of primes in a unique way" means. And this will be done later. □

1.4 Two theorems about the Fibonacci numbers

The Fibonacci numbers f_n (for $n \in \mathbb{N}$) are defined as follows:

$$\begin{aligned} f_1 &= 1\,, \\ f_2 &= 1\,, \\ f_{n+2} &= f_n + f_{n+1} \qquad \text{for } n \in \mathbb{N}\,. \end{aligned}$$

Remark 2. The definition of the Fibonacci numbers looks very much like an inductive definition, except that, instead of defining each Fibonacci number in terms of the previous one, we define each Fibonacci number in terms of the two preceding ones. For this reason, the definition of the Fibonacci numbers is said to be a *two-step inductive definition*. □

Example 1. Here are the first twelve Fibonacci numbers:

$$\begin{array}{llll} f_1 = 1\,, & f_2 = 1\,, & f_3 = 2\,, & f_4 = 3\,, \\ f_5 = 5\,, & f_6 = 8\,, & f_7 = 13\,, & f_8 = 21\,, \\ f_9 = 34\,, & f_{10} = 55\,, & f_{11} = 89\,, & f_{12} = 144\,. \end{array}$$

We now prove an upper bound and an identity for the Fibonacci numbers. In these results, there appears a very famous number, the "golden ratio". So we first define this number.

Definition 1. The golden ratio is the real number φ given by

$$\varphi = \frac{1+\sqrt{5}}{2}\,.$$

Remark 3. The golden ratio also has several other names: the golden mean, the golden section, the divine proportion, the divine section, and also the golden proportion.

If you want to find out why this number is so important and so famous, you should read something about it:

Strongly recommended reading: The Wikipedia article entitled "golden ratio".

In these notes, I will just give you two results showing that the golden ratio is closely related to the Fibonacci numbers, and I will prove one of these results, leaving the other one for you to prove.

Theorem 3. *The Fibonacci numbers f_n satisfy the bound*

$$f_n \le \varphi^{n-1} \qquad \text{for every} \quad n \in \mathbb{N}\,, \tag{1.4}$$

where φ is the golden ratio, that is, $\varphi = \frac{1+\sqrt{5}}{2}$.

Theorem 4. *(Binet's formula) The Fibonacci numbers f_n satisfy the identity*

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \qquad \text{for every} \quad n \in \mathbb{N}\,, \tag{1.5}$$

where φ is the golden ratio, that is, $\varphi = \frac{1+\sqrt{5}}{2}$, and ψ is the number given by

$$\psi = \frac{1-\sqrt{5}}{2}\,.$$

Proof of Theorem 3. First, we observe that

$$\varphi^2 = \varphi + 1\,. \tag{1.6}$$

(This is a simple calculation: $\varphi^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \varphi$.)

We now prove that

$$(\forall n \in \mathbb{N})\, f_n \leq \varphi^{n-1}\,. \tag{1.7}$$

We define B to be the set of all natural numbers n for which the inequality "$f_n \leq \varphi^{n-1}$" is not true. That is, we let

$$B = \{n \in \mathbb{N} : f_n > \varphi^{n-1}\}\,.$$

(Think of B as the set of all "bad" numbers, that is, the numbers that we want to prove don't exist at all.)

We want to prove that B is the empty set. We do this by contradiction: we assume that $B \neq \emptyset$, and will try to derive a contradiction.

Since B is nonempty, the well-ordering principle implies that B has a smallest member b. Then

1. $b \in B$, so

   a. $b \in \mathbb{N}$,

   and

   b. $f_b > \varphi^{b-1}$.

Furthermore, b is the smallest member of B, so

2. If $n \in \mathbb{N}$ and $n < b$, then $f_n \leq \varphi^{n-1}$.

Next, we observe that if $b \geq 3$ then f_b is given as the sum of the two preceding Fibonacci numbers, but if $b = 1$ or $b = 2$ then b is not given in that way. So it is natural to consider separately the cases $b = 1$, $b = 2$, and $b \geq 3$.

First, consider the case when $\boxed{b = 1}$. Then $f_b = 1$, and $\varphi^{b-1} = \varphi^0 = 1$. (Recall that $a^0 = 1$ for all real numbers a.) So the inequality $\boxed{f_b \leq \varphi^{b-1}}$ is true.

Next, consider the case when $\boxed{b = 2}$. Then $f_b = 1$, and $\varphi^{b-1} = \varphi = \frac{1+\sqrt{5}}{2}$. Clearly, $\frac{1+\sqrt{5}}{2} \geq 1$ (because $\sqrt{5} \geq 1$, so $1 + \sqrt{5} \geq 2$ and then $\frac{1+\sqrt{5}}{2} \geq 1$). So the inequality $\boxed{f_b \leq \varphi^{b-1}}$ is true in this case as well.

Finally, consider the casde when $\boxed{b \geq 3}$. In this case, we know that

$$f_b = f_{b-2} + f_{b-1}\,.$$

And we also know that the inequalities

$$f_{b-1} \leq \varphi^{b-2}\,, \tag{1.8}$$

$$f_{b-2} \leq \varphi^{b-3}\,, \tag{1.9}$$

hold, because $b-1$ and $b-2$ are smaller than b, so $b-1$ and $b-2$ do not belong to B.

If we add (1.8) and (1.9), we get

$$f_{b-2} + f_{b-1} \leq \varphi^{b-2} + \varphi^{b-3}\,. \tag{1.10}$$

But

$$f_{b-2} + f_{b-1} = f_b\,,$$

and

$$\varphi^{b-2} + \varphi^{b-3} = (\varphi+1)\varphi^{b-3} = \varphi^2\varphi^{b-3} = \varphi^{b-1}\,,$$

(using the fact that $\varphi + 1 = \varphi^2$), so (1.10) implies that $\boxed{f_b \leq \varphi^{b-1}}$.

So we have proved that the inequality $f_b \leq \varphi^{b-1}$ holds in all three cases ($b = 1$, $b = 2$, and $b \geq 3$). It follows (using the Proof by Cases Rule) that

$$f_b \leq \varphi^{b-1}\,. \tag{1.11}$$

But, as we established before,

$$f_b > \varphi^{b-1}\,. \tag{1.12}$$

Inequalities (1.11) and (1.12) contradict each other. This contradiction arose from assuming that $B \neq \emptyset$. So B is empty, and this proves out desired conclusion. **Q.E.D.**

Proof of Theorem 4. **YOU DO THIS PROOF.**

Important observation, that will play a crucial role in your proof: We already pointed out before that

$$\varphi^2 = 1 + \varphi\,.$$

It turns out that the number ψ also satisfies

$$\psi^2 = 1 + \psi\,.$$

(You can verify this by a simple computation.)

In other words, *the numbers φ, ψ are the two sokutions of the equation* $x^2 = x + 1$.

Problem 1. *Prove Theorem 4.*