MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S LECTURE NOTES

PART VII

Contents

17 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 an important example of a proof using well-ordering.

17.1 Statement of the well-ordering principle

17.1.1 The smallest member of a set of real numbers

In order to state the well-ordering principle, we first have to clarify what me mean by "smallest member" of a set of real numbers.

Definition 39. Let S be a subset of $\mathbb{R}$. (So in particular S could be a subset of $\mathbb{Q}$, or of $\mathbb{Z}$, or of $\mathbb{N}$, because every subset of $\mathbb{Q}$ or of $\mathbb{Z}$ or of $\mathbb{N}$ is a subset of $\mathbb{R}$). A smallest member of S is an object s such that

1. $s \in S$,
2. s is smaller than or equal to every member of S, that is,

$$(\forall t)(t \in S \Longrightarrow s \leq t)\,. \qquad \square$$

Remark 22. In Definition 39 I wrote ***a*** smallest member rather than ***the*** smallest member, because at this point we do not know yet that if a set has a smallest member then it has only one smallest member.

But we can prove that, indeed, if there is a smallest member then there is only one, and once we know this we will be able to talk about ***the*** smallest member. □

[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.

Proposition 1. *Let S be a subset of $\mathbb{R}$ that has a smallest member. Then the smallest member of S is unique.* □

Proof. To prove the uniqueness of the smallest member, we have to prove that if s_1 and s_2 are smallest members of S, then $s_1 = s_2$.

So let us assume that s_1 and s_2 are smallest members of S. Then the definition of "smallest member" tells us that

(i) $s_1 \in S$ (because s_1 is a smallest member of S),

and

(ii) If $t \in S$ then $s_2 \leq t$ (because s_1 is a smallest member of S).

Then, specializing (ii) to $t = s_1$, we find that

$$s_1 \leq s_2 \,. \tag{17.1}$$

A similar argument also shows that

$$s_2 \leq s_1 \,. \tag{17.2}$$

It follows from (17.1) and (17.2) that

$$s_1 = s_1 \,. \tag{17.3}$$

So the smallest member is unique. **Q.E.D.**

And then, ***now that we know that the smallest member of a subset S of $\mathbb{R}$, when it exists, is unique, we can talk about the smallest member of S.***

17.1.2 “A” vs. “the”

“A” vs. “the”

In English, we talk about “the” something when we know that there is only one something, and about “a” something if we don’t know that there is only one, so in principle there could be more than one. So, for example, we say

Paris is $\boxed{\text{the}}$ capital of France

because France has only one capital. But we say

Piscataway is $\boxed{\text{a}}$ town in New Jersey

because there are lots of towns in New Jersey.

Examples:

1. If you are asked to define “power set”, and you write “A power set of a set is . . .”, then this is wrong, because a set has only one power set, so you have to say “the power set”.

2. If you are asked to define “subset”, and you write “The subset of a set is . . .”, then this is wrong, because a set has lots of subsets, so you have to say “a subset”.

3. If you are asked to define “union”, and you write “A union of two sets is . . .”, then this is wrong, because given two sets there is only one set which is the union of those sets, so you have to say “the union”.

4. If you are asked to define “Cartesian product”, and you write “A Cartesian product of two sets is . . .”, then this is wrong, because given two sets there is only one set that is the Cartesian product of those two sets, so you have to say “a subset”.

5. If you are asked to define “function”, and you write “the function is. . . ”, then this is wrong, because there are lots of functions, “a function”.

17.1.3 The well-ordering principle (WOP)

Here, finally, is the well-ordering princple:

Theorem 58. *Every nonempty set of natural numbers has a smallest member.*

In formal language, the WOP says that

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

17.2 Proof of the well-ordering principle

First we prove a lemma[2]:

Lemma 5. *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

$$(\forall n \in \mathbb{N})(\forall S)\Big((S \subseteq \mathbb{N} \wedge n \in S) \Longrightarrow S \text{ has a smallest member}\Big)\,. \tag{17.4}$$

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.

Basis step. We want to prove that $P(1)$ is true.

Clearly, $P(1)$ 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.

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

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. So if $n \in S$ then S hasa 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

$$T = S \cup \{n\},$$

that is,

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

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 t.

Then $t \in T$, and $t \leq u$ for every $u \in T$.

In particular, if $s \in S$ then $s \in T$, so $t \leq s$.

This shows that t is smaller than or equal to every member of S, that is

$$(\forall s)(s \in S \Longrightarrow t \leq s). \qquad (17.5)$$

Does that prove that t is the smallest member of S?

No, it does not, because it may happen that t is not in S.

How could this happen? We know that t is in T, and that n is the only member of T that is not in S.

On the other hand, either $t \neq n$ or $t = n$.

Let us consider the case when $\boxed{t \neq n}$.

Then t must be in S. So (17.5) tells us that t is the smallest member of S, so $\boxed{S \text{ has a smallest member}}$.

Now consider the case when $\boxed{t = n}$.

Since (17.5) holds, it follows that $n \leq s$ for every $s \in S$.

Does this prove that n is the smallest member of S? No, because n is not in S.

But we can prove that $n + 1$ is the smallest member of S, as follows:

> 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 47 on page 166 of these notes. Remember that Theorem 47 says: *If $n \in \mathbb{Z}$ then there is no integer m such that $n < m < n + 1$.*)
> 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 $t \neq n$ and $t = n$. It then follows, using the Proof by Cases Rule, that $\boxed{\boxed{S \text{ has a smallest member}}}$.

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

$$(S \subseteq \mathbb{N} \wedge n{+}1) \in S \Longrightarrow S \text{ has a smallest member}\,. \qquad (17.6)$$

We have proved (17.6) under the assumption that S was an arbitrary set. Hence

$$(\forall S)\Big((S \subseteq \mathbb{N} \wedge n{+}1 \in S) \Longrightarrow S \text{ has a smallest member}\Big)\,. \qquad (17.7)$$

But (17.7) 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 58. 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.**

17.3 An example of a proof using well-ordering; the existence part of the fundamental theorem of arithmetic

In this section we prove the existence part of the ***fundamental theorem of arithmetic (FTA).*** This theorem is one of the most important results in integer arithmetic. It says that every natural number n such that $n \geq 2$ 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 will prove 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.

The proof of uniqueness requires more sophisticated tools, and will be done later.

Theorem 59. *Every natural number n such that $n \geq 2$ is a product of primes.*

Before we prove the theorem, let us explain what it says.

17.3.1 Clarification: What is a "product of primes"?

Like all mathematical ideas, even something as simple as "product of primes" requires a precise definition. Without a precise definition, it would not be clear, for example, whether a single prime such as 2 or 3 or 5 is a "product of primes".

Definition 40. A natural number n is a product of primes if there exist

1. a natural number k,

and

2. a list $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers,

such that

$$n = \prod_{i=1}^{k} p_i \,. \tag{17.8}$$

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.*** □

Definition 41. If n is a natural number, then a list $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers such that (17.8) holds is called a prime factorization of n. □

Example 28. The following natural numbers are products of primes:

- 7 (because 7 is prime),
- 24 (because $24 = 2 \times 2 \times 2 \times 3$),
- 309 (because $309 = 3 \times 103$ and both 3 and 103 are prime).
- $3,895,207,331,689$. Here it would really take a lot of work to find the primes $p_1, p_2, \ldots, p_k$ such that $3,895,207,331,689 = \prod_{i=1}^{k} p_i$. But the theorem that we are going to prove tell us that $3,895,207,331,689$ is a product of primes. □

17.3.2 Outline of the strategy for proving the theorem

Call a natural number n "bad" if $n > 1$ and n is not a product of primes.

What we want is to prove is that there are no bad natural numbers.

The strategy is going to be this: we let B be the set of all bad numbers, so our goal is to prove that B is empty. For this purpose, we assume it is nonempty, and use the well-ordering Principle to conclude that it has a smallest member b. Then b is bad, and in addition b is the smallest bad natural number. But then b cannot be prime, because if it is prime then it is a product of primes, so b would not be bad. Since $b > 1$, and b is not prime, b must be a product cd of two smaller natural numbers. But then c and d cannot be bad. So c is a product $p_1 \times p_2 \times \cdots \times p_k$ of primes, and d is a product $q_1 \times q_2 \times \cdots \times q_j$ of primes. So

$$b = cd = p_1 \times p_2 \times \cdots \times p_k \times q_1 \times q_2 \times \cdots \times q_j \,.$$

But then b is a product of primes, so b is not bad. But b is bad, and we got a contradiction. Hence B is empty, and that means that there are no bad numbers.

17.3.3 The proof

Let B be the set of all natural numbers n such that $n \geq 2$ and n is not a product of primes.

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.)

Since b is not prime, there are two possibilities: either $b = 1$ or b has a factor k which is a natural number such that $k \neq 1$ and $k \neq b$.

But the fist possibility ($b = 1$) cannot arise, because $b \geq 2$.

Hence the second possibility occurs. That is, we can pick a natural number k such that k divides b, $k \neq 1$, and $k \neq b$.

Since $k|b$, we can pick an integer j such that

$$b = jk\,.$$

And then j has to be a natural number. (Reason: we know that $k \in \mathbb{N}$, so $k > 0$. If j was ≤ 0, it would follow that $kj \leq 0$. But $kj - b$ and $b > 0$.)

Then $j \neq 1$ and $j \neq b$. (Reason: j cannot be 1 because if $j = 1$ then it would folows from $b = jk$ that $k = b$, and we know that $k \neq b$. And j cannot be b because if $j = b$ then it would folows from $b = jk$ that $k = 1$, and we know that $k \neq 1$.)

Then $j < b$ and $k < b$. (Reason: $k \geq 1$, because $k \in \mathbb{N}$; so $k > 1$, because $k \neq 1$; so[3] $k \geq 2$; and then if j was $\geq b$ it would follow that $jk \geq 2j > j > b$, but $jk = b$. The proof that $k < b$ is exactly the same.)

Hence $j \notin B$ (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 B).

Similarly, k is a product of primes. So we can write

$$j = \prod_{i=1}^{m} p_i \qquad \text{and} \qquad k = \prod_{\ell=1}^{\mu} q_\ell\,,$$

where $m \in \mathbb{N}$, $\mu \in \mathbb{N}$, and the p_i and the q_ℓ are primes. But then

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

[3] Notice that here we are using again Theorem 47: "there is no integer between 1 and 2", so the fact that $k > 1$ implies $k \geq 2$ because if $k < 2$ then we would have $1 < k < 2$, contradicting Theorm 47.

so $\boxed{b \text{ is a product of primes}}$. (Precisely: define u_j, for $j \in \mathbb{N}$, $1 \le j \le m+\mu$, by the formula

$$u_j = \begin{cases} p_j & \text{if} \quad 1 \le j \le m \\ q_{j-m} & \text{if} \quad m+1 \le j \le m+\mu \end{cases} .$$

Then

$$b = \prod_{i=1}^{m+\mu} u_j \, .$$

And the u_j are prime, because each u_j is either one of the p_is or one of the q_ℓs.)

So $\boxed{b \text{ is a product of primes}}$.

But we know that $\boxed{b \text{ is not a product of primes}}$. 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 $n \ge 2$ is a product of primes, which is our desired conclusion. **Q.E.D.**

Remark 23. The ***fundamental theorem of arithmetic (FTA)*** 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.) Theorem 59 is a part of the FTA, namely, the assertion that if $n \in \mathbb{N}$ and $n \ge 2$ then n can be written as a product of primes.

What we 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
bf*defining* what "uniqueness" of the factorization of a natural number 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 a product 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. □