Lecture 9: Principle of Mathematical Induction

1 Properties of Natural Numbers

Most fundamental property of natural numbers is ability to do proof by induction. The set of natural numbers is denoted by the set $\mathbb{N}$. The set $\mathbb{N}$ consists of a distinguished element denoted by 1 considered to be starting point for the induction. A unique property for the set of natural numbers is that, there is a function s which maps the elements of $\mathbb{N}$ to its successor in $\mathbb{N}$. Any rigorous treatment of the natural numbers must ultimately rely upon some axioms. There are two standard axiomatic approaches to developing the natural numbers. One approach, involving the minimal axiomatic assumptions and the most effort deducing facts from the axioms, is to assume the Peano Postulates for the natural numbers, which are stated as follows.

Axiom 1.1 (Peano Postulates). There exists a set $\mathbb{N}$ with an element $1 \in N$ and a function $s : \mathbb{N} \to \mathbb{N}$, that satisfy the following three properties.

- There is no $n \in \mathbb{N}$ such that $s(n) = 1$.
- The function s is injective.
- Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.

If we think intuitively of the function s in the Peano Postulates as taking each natural number to its successor, then first postulate says that 1 is the first number in $\mathbb{N}$, because it is not a successor of anything.

Definition 1.2 (Natural numbers). The set of **natural numbers** is the set $\mathbb{N}$, the existence of which is given in the Peano Postulates.

How do we know that there is a set, and an element of the set, and a function of the set to itself, that satisfy the Peano Postulates? There are two approaches to resolving this matter. When we do mathematics, we have to take something as axiomatic, which we use as the basis upon which we prove all our other results.

Hence, one approach to the Peano Postulates is to recognize their very reasonable and minimal nature, and to be satisfied with taking them axiomatically. Alternatively, if one takes the Zermelo-Fraenkel Axioms as the basis for set theory, then it is not necessary to assume additionally that the Peano Postulates hold, because the existence of something satisfying the Peano Postulates can be derived from the Zermelo-Fraenkel Axioms.

If one goes through the full development of the natural numbers starting from the Peano Postulates, the first major theorem one encounters is the one which will be stated shortly. This theorem is used in particular in the definition of addition and multiplication of the natural numbers.This theorem, called Definition by Recursion.

Theorem 1.3 (Defintion by Recursion). *Let A be a set, $b \in A$, and $k : A \to A$ be a function. Then there exists a unique function $f : \mathbb{N} \to A$ such that $f(1) = b$ and $f \circ s = k \circ f$.*

Remark 1. We make following observations about definition by recursion.

1. The equation $f \circ s = k \circ f$ means that $f(s(n)) = k(f(n))$ for all $n \in \mathbb{N}$.
2. If $s(n)$ were to be interpreted as $n + 1$, that it will turn out to be once addition for $\mathbb{N}$ is rigorously defined, then $f(s(n)) = k(f(n))$ would mean that $f(n + 1) = k(f(n))$, which looks more familiar intuitively.
3. It's easier to understand this definition by the commutative diagram in Figure 1.

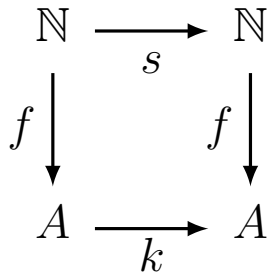

Figure 1: Commutative diagram for recursive function $k : A \to A$.

Theorem 1.4. *Let $a, b, c, d \in \mathbb{N}$. Then the following hold.*

1. *If $a + c = b + c$, then $a = b$. (Additive inverse)*
2. *$(a + b) + c = a + (b + c)$. (Additive associativity)*

3. $s(a) = a + 1$. *(Additive increment)*

4. $a + b = b + a$. *(Additive commutativity)*

5. $a \cdot 1 = a = 1 \cdot a$. *(Product identity)*

6. $(a + b)c = ac + bc$. *(Multiplicative distributivity)*

7. $ab = ba$. *(Multiplicative commutativity)*

8. $c(a + b) = ca + cb$. *(Multiplicative distributivity)*

9. $(ab)c = a(bc)$. *(Multiplicative associativity)*

10. *If* $ac = bc$ *then* $a = b$. *(Multiplicative inverse)*

11. $a \geq a$, *and* $a \not> a$, *and* $a + 1 > a$.

12. $a \geq 1$, *and if* $a \neq 1$ *then* $a > 1$.

13. *If* $a < b$ *and* $b < c$, *then* $a < c$; *if* $a \leq b$ *and* $b < c$, *then* $a < c$. *If* $a < b$ *and* $b \leq c$, *then* $a < c$; *if* $a \leq b$ *and* $b \leq c$, *then* $a \leq c$.

14. $a < b$ *if and only if* $a + c < b + c$.

15. $a < b$ *if and only if* $ac < bc$.

16. *Precisely one of the following holds:* $a < b$, *or* $a = b$, *or* $a > b$. *(Trichotomy Law)*

17. $a \leq b$ *or* $b \leq a$. *(Comparability)*

18. *If* $a \leq b$ *and* $b \leq a$, *then* $a = b$. *(Equality)*

19. *It cannot be that* $b < a < b + 1$.

20. $a < b$ *if and only if* $a + 1 \leq b$.

21. *If* $a < b$, *there is a unique* $p \in \mathbb{N}$ *such that* $a + p = b$.

Theorem 1.5 (Well-ordering principle). *Let* $A \subseteq \mathbb{N}$ *be a set. If* A *is non-empty, then there is a unique* $m \in A$ *such that* $m \leq a$ *for all* $a \in A$.

Remark 2. Uniqueness is easy to see from Thm 1.4, but existence is hard to show.

Definition 1.6. Let $a, b \in \mathbb{N}$. The sets $\{a, \ldots, b\}$ and $\{a, \ldots\}$ are defined by $\{a, \ldots, b\} = \{x \in \mathbb{N} : a \leq x \leq b\}$ and $\{a, \ldots\} = \{x \in \mathbb{N} : a \leq x\}$ respectively.

2 Mathematical Induction

Mathematical induction is a method to prove statements of the form $(\forall n \in \mathbb{N})(P(n))$. Informally, we show that $P(1)$ is true, and if $P(1)$ is true then $P(2)$ is true, and so on. It suffices to show that $P(1)$ holds, and if $P(n)$ holds then $P(n+1)$ holds for any arbitrary natural number n.

Theorem 2.1 (Principle of mathematical induction (PMI)). *Let $G \subseteq \mathbb{N}$. Suppose that*

1. *$1 \in G$,*
2. *if $n \in G$, then $n+1 \in G$.*

Then, $G = \mathbb{N}$.

Remark 3. Notice second assumption is called inductive step and $n \in G$ is called inductive hypothesis.

Example 2.2. If $n \in \mathbb{N}$, then $8^n - 3^n$ is divisible by 5.

Proof. Let

$$G = \{n \in \mathbb{N} : 8^n - 3^n \text{ divisible by } 5\},$$

and we'll show $G = \mathbb{N}$. Notice that $G \subseteq \mathbb{N}$. Further, we have $1 \in G$, since $8^1 - 3^1 = 5$ is divisible by 5. Let $n \in G$, then $8^n - 3^n$ is divisible by 5. Further,

$$8^{n+1} - 5^{n+1} = 8 \cdot 8^n - 3 \cdot 5^n = 5 \cdot 8^n + 3(8^n - 3^n).$$

Hence, $8^{n+1} - 5^{n+1}$ is divisible by 5 and hence $n+1 \in G$. □

Theorem 2.3 (PMI-Variant 1). *Let $G \subseteq \mathbb{N}$ and $k_0 \in \mathbb{N}$. Suppose that*

1. *$k_0 \in G$,*
2. *if $n \in \{k_0, \ldots\}$ and $n \in G$, then $n+1 \in G$.*

Then, $\{k_0, \ldots\} \subseteq G$.

Theorem 2.4 (PMI-Variant 2). *Let $G \subseteq \mathbb{N}$. Suppose that*

1. *$1 \in G$,*
2. *if $n \in \mathbb{N}$ and $\{1, \ldots, n\} \in G$, then $n+1 \in G$.*

Then, $G = \mathbb{N}$.

Proof. Suppose $G \neq \mathbb{N}$, we'll derive a contradiction. Let $H = \mathbb{N} \setminus G \neq \emptyset$. Since, $H \subseteq \mathbb{N}$, we have some $m \in H$ such that $m \leq h$ for all $h \in H$ by well-ordering principle. We have $m > 1$ since $1 \in G$. Therefore, $m = 1 + b$ for some $b \in \mathbb{N}$. Let $p \in \{1, 2, \ldots, b\}$, then $p \leq b < b + 1 = m$. That is, $p \notin H$ and hence $p \in G$. By second hypothesis of the theorem, we have $m = b + 1 \in G$. Therefore, we have a contradiction. □

Theorem 2.5 (PMI-Variant 3). *Let $G \subseteq \mathbb{N}$ and $k_0 \in \mathbb{N}$. Suppose that*

1. *$k_0 \in G$,*
2. *if $n \in \{k_0, \ldots\}$ and $\{k_0, \ldots, n\} \in G$, then $n + 1 \in G$.*

Then, $\{k_0, \ldots\} \subseteq G$.

Definition 2.6. Set $\{1, 2, \ldots, n\}$ is also denoted by $[n]$.

Example 2.7. Let $n \in \mathbb{N}$. Suppose that $n \geq 2$. Then n is either a prime number or a product of finitely many prime numbers.

Theorem 2.8. *Let $n, k \in \mathbb{N}$. Then the following are true.*

1. *Let $f : [n] \to \mathbb{N}$ be a function. Then, there is a $q \in [n]$ such that $f(q) \geq f(i)$ for all $i \in [n]$.*
2. *Let $S \in [n]$ be a non-empty subset. Then, there is a bijective function $g : [n] \to [n]$ such that $g(S) = [r]$ for some $r \in \mathbb{N}$ such that $r \leq n$. If $S \subset [n]$, then $r < n$.*
3. *Let $f : [n] \to [k]$ be a function. If f is bijective, then $n = k$. If f is injective but not surjective, then $n < k$.*