Massachusetts Institute of Technology — Handout 10
6.042J/18.062J: Mathematics for Computer Science — September 14, 1995
Professors David Karger and Tom Leighton

Notes 3

What about those horses?

6 Other Kinds of Induction

6.1 Strong Induction

A variant of induction. To prove $(\forall n \in N)P(n)$

- prove $P(1)$
- prove $((\forall k < n)P(k))$ implies $P(n)$.

Definition 1 *We say a* divides *b if there exists an integer t such that $a = bt$. We write $a \mid b$.*

- $3 \mid 6$
- $3 \not\mid 7$

Definition 2 *p is* prime *if the only natural numbers dividing p are 1 and p.*

Thus, n is *composite* if $n = ab$ for natural numbers $a, b \neq 1, n$.

Theorem 1 *Every natural number has a prime divisor.*

Proof. BASE CASE: The theorem is true for $n = 2$.

INDUCTIVE STEP: Assuming the theorem true for all $2 \leq k < n$, consider the number n. We proceed by cases:

1. n is prime. Then n (a prime) divides n.

2. n is composite. Then $n = ab$ where $2 \leq a < n$. It follows from the inductive hypothesis that a has a prime divisor, ie that $a = pt$ for a prime t. Then $n = ptb$, meaning p divides n.

Since we proved the inductive step for both possible cases, we are done. ■

Note: we use a base case of 2. This is fine, as long as we never assume $n < 2$.

6.2 Well Ordering Principle

Theorem 2 *Every nonempty set of natural numbers contains a least element.*

Not true for integers, positive reals/rationals.

Theorem 3 *Every natural number can be factored as a product of primes.*

Proof. By well ordering. Let S be the set of all elements that cannot be factored as a product of primes. We assume $S \neq \emptyset$ and derive a contradiction. If S is not empty, it has a least element n by well ordering. If n is prime, then it is a product of primes, implying it shouldn't be in S. So n is composite—write $n = ab$ where $a, b < n$. It follows $a, b \notin S$. In other words, a can be written as a product of primes $p_1 p_2 \cdots p_k$ and b as a product of primes $q_1 \cdots q_l$. Therefore, $n = p_1 \cdots p_k q_1 \cdots q_l$ can be written as a product of primes, contradicting the claim that $n \in S$. Our assumption that $S \neq \emptyset$ must therefore false. ■

Here's a fallacious argument: every number can be factored uniquely into primes. Apply the same proof as before, adding "uniquely" to the inductive hypothesis. The problem is that even if $n = ab$ and a, b have unique factorizations, it is still possible that $n = cd$ for different c and d, producing a different factorization of n.

The argument is false, but the claim is true and is known as the fundamental theorem of arithmetic.

Theorem 4 *(The division algorithm.) Let a, b be naturals. $\exists! q, 0 \leq r < b$, such that $a = qb + r$.*

Proof. To prove this theorem, we need to prove both that some r exists and that this r is unique (this is typical of unique-existence proofs).

Existence: We use well ordering. Let $S = \{r \in \mathbb{N} \mid (\exists q) a = qb + r\}$.

- S is nonempty since $a = 0b + a$ implies $a \in S$. It follows by well ordering that S contains a least element r_0 such that $a = q_0 b + r_0$.
- Suppose $r_0 \geq b$. Then $a = (q_0+1)b+(r_0-b)$, and $r_0 - b \geq 0$, implying $r_0 - b \in S$, which contradicts the fact that r_0 is the least element of S. Thus $r_0 < b$.

Uniqueness: suppose $a = qb+r = q'b+r'$. Without loss of generality, suppose $r > r'$ (what we mean is, if $r < r'$, then we can swap (q, r) with (q', r') to make the assumption true). Then $(q - q')b = (r - r')$ By assumption, $r, r' < b$. Thus $0 \leq r - r' < b$, but $b \mid r - r'$, so $r - r' = 0$. Thus $q - q' = 0$.

∎

Definition 3 *In the theorem above, r is the* remainder *on dividing a by b and q is the* quotient*.*

We actually left a hole in our proof that $\sqrt{2}$ is irrational: we assumed that we could write a fraction in lowest terms. Here is how to actually prove that fact:

Theorem 5 *Every rational number can be written in lowest terms.*

Proof. Given a rational q, let $S = \{b \mid (\exists a) q = a/b\}$. S is nonempty by the definition of q being rational. Therefore S has a least element b and a corresponding a; a/b is the lowest-terms representation of q. ∎

6.3 Nim

The game of nim is defined as follows. A bunch of sticks are placed on the ground. Two players take turns removing one, two, or three sticks. The player to remove the last stick loses.

Theorem 6 *First player loses if the number of sticks n is $4k + 1$ for some k, and wins otherwise.*

Proof. By strong induction. In class, I forgot to do the base case.

BASE CASE: If $n = 1$, clearly the first player loses.

INDUCTIVE STEP: Assume the theorem for $m < n$. Suppose there are n sticks. We work by cases.

- Suppose $n = 4k + 1$. Then if the first player removes one stick, the remainder is $n - 1 = 4k + 0$. By the inductive hypothesis, the player who plays at this point should win. It follows that the player who played first will lose. Similarly, if the first player removes 2 sticks, then the remainder is $4(k-1)+3$, and he loses by the same reasoning. Same holds for removing 3 sticks. So however the first player moves, he loses by the inductive hypothesis. Note this is a *strong* induction, since we rely on the previous three cases.

- Suppose $n = 4k + 0$. Then if we remove 3 sticks, we get $4(k - 1) + 1$ sticks to the second player, who loses by the inductive hypothesis.

- The case $n = 4k + 2$ and $n = 4k + 3$ are handled the same way.

From the division algorithm, we know these are all the possible cases. ∎

6.4 Equivalence of the three techniques

6.4.1 Weak implies Strong:

In this case, we are allowed to assume weak induction. In other words, for any predicate P, $(P(0) \wedge ((\forall n)P(n) \Rightarrow P(n+1)))$ implies $(\forall n)P(n)$. We want to prove that for any predicate Q, if $Q(0)$ is true, and $(\forall n)((\forall k \leq n)Q(k)) \Rightarrow Q(n+1)$, then $(\forall n)Q(n)$ is true. So let $P(n)$ be the predicate $(\forall k \leq n)Q(k)$. If $Q(0)$ is true, then by definition $P(0)$ is true. Now suppose $(\forall n)((\forall k \leq n)Q(k)) \Rightarrow Q(n+1)$. This can be rewritten as $(\forall n)(P(n) \Rightarrow Q(n+1))$. But certainly $P(n) \Rightarrow P(n)$. Therefore, $(\forall n)(P(n) \Rightarrow (P(n) \wedge Q(n+1)))$. But $P(n) \wedge Q(n+1) \Rightarrow P(n+1)$. Therefore, $P(n) \Rightarrow P(n+1)$. Since $P(0)$ and $P(n) \Rightarrow P(n+1)$ hold, weak induction tells us that $P(n)$ holds for all n. But $P(n) \Rightarrow Q(n)$, so $Q(n)$ holds for all n.

6.4.2 Strong implies Well-Ordering

We wish to prove: every nonempty set contains a least element. We formulate the following inductive hypothesis $P(n)$: every nonempty set containing n contains a least element. If we prove this inductive hypothesis, then we have proven well ordering since a nonempty set must contain some element n for which $P(n)$ implies the claim. The base case of the inductive step is easy: if a set of natural numbers contains 0 then 0 is its least element. Now suppose $(\forall k \leq n)P(k)$, and let us prove $P(n+1)$. Consider a set containing $n+1$. If it contains no smaller element, then $n+1$ is the least element and we are done. If it contains a smaller element $k \leq n$ then, but the inductive hypothesis, it contains a least element and again we are done.

6.4.3 Well-Ordering implies Weak Induction

Suppose $P(0)$ is true and $P(n) \Rightarrow P(n+1)$ is true. Let

$$S = \{n \mid \neg P(n)\}.$$

Let us assume $S \neq \emptyset$ and derive a contradiction. If S is nonempty then, by well ordering, it contains a least element n. Clearly $n \neq 0$ since $P(0)$ is true. Therefore $n-1$ is a natural number not in S (otherwise n wouldn't be the least element), meaning $P(n-1)$ is true. It follows from the inductive hypothesis that $P(n)$ is true, which contradicts the claim that $n \in S$. We have derived a contradiction, meaning that our initial assumption, that S is nonempty, is false. But if S is empty, it must be that $(\forall n)P(n)$ is true, which is what we wished to prove.