Massachusetts Institute of Technology
6.042J/18.062J: Mathematics for Computer Science
Professors David Karger and Tom Leighton

Handout 8
September 12, 1995

Notes 2

Books have arrived in the COOP. 18.062.

Typo in homework 2: reading is 3.1–3.3, not 3.4.

4 Definitions

Definitions are not necessary in a logical proof system, but they are very useful.

Definitions call attention to something interesting that we expect to encounter frequently:

- a *factor* of n is a positive integer that divides n without remainder.
- A *prime number* is one whose only factors are 1 and itself.
- A *K-number* is one that is divisible by 5 and by 7, but not by 13 or 43.

The first two definitions are useful, because they pin down a concept that we encounter frequently (and save us a lot of extra typing). The third definition is valid, but is not useful.

It is important for definitions to be *well defined.*

- $f(n)$ is the largest rational number less than n (sometimes no such number—how could we prove this?).
- $\sqrt{x}$ is the complex number y such that $y^2 = x$.

$$\begin{aligned} 1 &= \sqrt{1} \\ &= \sqrt{(-1)(-1)} \\ &= \sqrt{(-1)}\sqrt{(-1)} \\ &= -1 \end{aligned}$$

The problem is that $\sqrt{x}$ is not well defined, because it can take on two possible values.

4.1 Recursive Definitions

A *recursive definition* says how to build something from a simpler version of the same thing. Two parts:

- Base case(s) that don't depend on anything else
- Combinations cases that depend on simpler cases

Note the relationship to a *recursive algorithm.*

Examples:

- The *Factorial function*
  - $1! = 1$
  - $(n+1)! = (n+1)n!$ for $n \geq 1$.
- Prime numbers:
  - 2 is prime
  - $n > 2$ is prime if n is not divisible by any prime less than n.
- The *Fibonacci numbers*:
  - $f_0 = 0$
  - $f_1 = 1$
  - $f_{n+1} = f_n + f_{n-1}$

  Note: 2 base cases, since combination relies on previous two values.

  What is f_4? Well, $f_2 = f_0 + f_1 = 1$, $f_3 = f_1 + f_2 = 2$, so $f_4 = 3$.
- A *well formed arithmetic formula* is
  - A number
  - $(f+g)$, $(f-g)$, $(f*g)$, or (f/g) where f, g are well-formed arithmetic formulae.
- A *binary tree* is one of
  - a *node* with no children
  - a node with a left child that is a binary tree
  - a node with a right child that is a binary tree

  - a node with left and right binary-tree children.

We must take care that recursive definitions are well-defined:

- $f(n) = 2 + f(n-1)$. No base case.
- $f(1) = 1$ and $f(n) = 1 + f(n+1)$ still no base case.
-
  - $f(1) = 1$
  - If n is even, then $f(n) = f(n/2)$.
  - If n is odd, then $f(n) = f(3n+1)$.

  If f is well defined, then $f(1) = 1$ everywhere. But nobody knows if the recursion always terminates (though it's been checked for many numbers).

5 Proofs By Induction

Recall Peano's Induction Axiom:

Let $P(n)$ be a predicate, and suppose

- $P(0)$
- $(\forall n)\ (P(n) \Rightarrow P(n+1))$.

Then $P(n)$ is true for all natural numbers n.

Relation to recursive definitions. Think dominoes.

Note *not* a fallacious circular proof. We do *not* prove $P(n) \Rightarrow P(n)$.

Our universe of discourse will be $\mathbb{N}$.

If we replace $P(0)$ by $P(1)$ above, we have proven $P(n)$ for all $n \geq 1$.

Vital: write down P exactly!

5.0.1 A Sum

Theorem 1 $1 + 2 + 3 + \cdots + n = n(n+1)/2$

Proof. Let $P(n)$ be the proposition that the sum of the first n positive integers is $n(n+1)/2$.
BASIS STEP: $P(1)$ is true since $1 = 1(1+1)/2$.
INDUCTIVE STEP: Assumes that $P(n)$ holds, i.e.

$$1 + 2 + 3 + \cdots + n = n(n+1)/2.$$

Add $n+1$ to both sides to get that

$$1 + 2 + 3 + \cdots + n + (n+1) = n(n+1)/2 + (n+1) = (n+1)(n+2)/2.$$

Hence $P(n+1)$ is true. This completes the inductive step and the proof. ∎

Can also be proven without induction. How?

5.1 Angles in A Polygon

Definition 1 *A* **convex polygon** *is a polygon such that any straight line between two polygon vertices does not leave the polygon.*

Lemma 2 *If we draw a line between two vertices of a convex polygon, it divides the polygon into two convex polygons.*

Proof. Sketch. It is clear the line divides the convex polygon into two polygons. Each piece is convex because any straight line between two vertices of a piece lies entirely on one side of the dividing line and since it did not leave the original polygon, it must not leave the piece it is in. ∎

Theorem 3 *The sum of angles in an n-sided convex polygon is $(n-2)180°$.*

Proof. By induction. The induction hypothesis $P(n)$ is the theorem statement. The base case, for $n = 3$, is true from Euclid. For the inductive step, assume $P(n)$. To prove $P(n+1)$, consider an $(n+1)$-sided polygon. Consider three vertices A, B, C that appear consecutively on the boundary of the polygon. Draw a line AC. This produces a triangle ABC and a polygon with n vertices (we've removed B). By the preceding lemma, the smaller polygon is convex and thus, by the induction hypothesis, contains $(n-2)180°$. We now add in the $180°$ contained in the angles of ABC to find that the total angle sum in the $(n+1)$-vertex polygon is $(n-2)180° + 180° = ((n+1)-2)180°$, which proves $P(n+1)$. ∎

5.2 Die Hard

In Die Hard III, Bruce Willis and Samuel Jackson have to disarm a bomb using the old boy-scout trick of measuring four gallons of water using a three-gallon jug and a five-gallon jug. (You can figure out how this goes.) They have access to a reservoir of water. They need to pour out four gallons into a special container. The only operations they are permitted are those of pouring water using the three-gallon jug and the five-gallon jug. Whenever they pour water using a jug they either have to pour all of the water in the jug or until the receptacle into which the water is being poured becomes full.

Theorem 4 *Using a* 3 *gallon jug and a* 6 *gallon jug and the operations above, it is not possible to measure* 4 *gallons.*

Proof. By induction on n the number of operations. Let $P(n)$ be the proposition that after n operations all containers contain a number of gallons of water which is divisible by 3.
BASE CASE: $P(1)$ is clearly true since the containers contain either 3 or 6 gallons.
INDUCTIVE STEP: Assume $P(n)$ is true. Consider $(n+1)$ operations. At the end of the first n operations, by the inductive hypothesis, all containers contain a number of gallons divisible by 3. The $(n+1)$th operation involves the 3 gallon jug or the 6 gallon jug and in either case the resulting number of gallons in all containers continues to be divisible by 3. This completes the proof by induction.

Since 4 is not divisible by 3 it is not possible to measure 4 gallons. ∎

5.3 Courtyard Tiling

Theorem 5 *Every* 2^k *by* 2^k *courtyard with central square filled in can be tiled with L shaped tiles.*

Proof. Refer to Example 12 on Pp 194 of Rosen. ∎

Two things can make an induction proof break:

- Inductive hypothesis might be too strong: e.g., can tile any square courtyard with L shaped tiles (what goes wrong)?
- Inductive hypothesis might be too weak: e.g., can tile any 2^k by 2^k courtyard with a center square missing. We need to strengthen the hypothesis to "can tile any 2^k by 2^k courtyard with any square missing.

5.4 Structural Induction on a Recursive Definition

Two steps:

- Prove for "base cases" of definition
- Prove for any combination rule, assuming it's true for parts.

Why does this work? Regular induction on number of formation steps.

Theorem 6 *A binary tree with n nodes has $n-1$ edges.*

Proof. The proof is by induction on n the number of applications of the "combination rules". Let $P(n)$ be the proposition that a binary tree formed by n applications of the combination rules has 1 fewer edge than nodes.
BASE CASE: $P(0)$ is true since a binary tree that is a node with no children has 0 edges.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k \leq n$. Consider a binary tree formed by $(n+1)$ applications of the combination rules. There are three cases.

1. The tree is a node with a left child that is a binary tree. Since the left child is a binary tree formed by n applications of the combination rules, by the inductive hypothesis, it has 1 fewer edge than nodes. Hence the whole tree has 1 fewer edge than nodes, too.
2. The tree is a node with a right child that is a binary tree. This case is identical to the previous case.
3. The tree is a node with left and right binary-tree children. Let the left tree be formed by k nodes and the right tree $n-k$ nodes. By the inductive hypothesis they have $k-1$ and $n-k-1$ applications of the combination rules respectively. Then, since they each have 1 fewer edge than nodes the whole tree which has 1 node and 2 more edges has 1 fewer edge than nodes, too.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n.

∎

Theorem 7 *Well formed formulae always have the same number of left and right parentheses.*

Proof. The proof is by induction on n the number of applications of the "combination rules". Let $P(n)$ be the proposition that a well formed formula formed by n applications of

the combination rules has the same number of left and right parentheses.
BASE CASE: If the formula is just a number then the above proposition is obviously true since there are 0 left and right parentheses. Hence, $P(0)$ is true.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k \leq n$. Consider a well formed formula formed by $(n+1)$ applications of the combination rules. There are four cases.

1. The formula is of the form $(f+g)$, where f and g are well formed. Since f and g are well-formed and are formed by at most n applications of the combination rules, by the inductive hypothesis, they have an equal number of left and right parentheses and hence so does $(f+g)$.
2. The formula is of the form $(f-g)$. This case is similar to the first.
3. The formula is of the form $(f*g)$. This case is similar to the first.
4. The formula is of the form (f/g). This case is similar to the first.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n. ■

5.5 Fallacies

The biggest fallacy is forgetting to prove the base case.

It's also possible to switch an n for an $n+1$ at an inconvenient time.

False Theorem 1 *Every Fibonacci number is even.*

Proof. The proof is by induction. Let $P(n)$ be the proposition that F_n is even.
BASE CASE: $P(O)$ is true since $F_0 = 0$ is even.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k \leq n$. Consider $F_{n+1} = F_n + F_{n-1}$. Since F_n and F_{n-1} are even, by the inductive hypothesis, it follows that F_{n+1} is even too. Hence P_{n+1} is true.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n.
■

The above proof is faulty because the base case is insufficient. The base case should have proved that F_0 and F_1 are both even.

The following is a true theorem but with a fallacious proof whose inductive hypothesis is too weak.

Theorem 8 *All regular convex polygons with n sides have angles summing to $(n-2)180°$.*

Proof. False proof. The proof is by induction. Let $P(n)$ be the proposition that all regular convex polygons with n sides have angles summing to $(n-2)180°$.
BASE CASE: $P(3)$ is true since an equilateral triangle has angles summing to $(3-2)180°$.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k \leq n$. Consider a regular convex polygons with $n+1$ sides. Consider three vertices A, B, C that appear consecutively on the boundary of the polygon. Draw a line AC. This produces a triangle ABC and a polygon with n vertices (we've removed B). By lemma 2, the smaller polygon is convex and thus, by the induction hypothesis, contains $(n-2)180°$. We now add in the $180°$ contained in the angles of ABC to find that the total angle sum in the $(n+1)$-vertex polygon is $(n-2)180° + 180° = ((n+1)-2)180°$, which proves $P(n+1)$.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n.

■

The above proof is wrong because the inductive hypothesis has been invoked wrongly. The smaller polygon created by line AC is not *regular*. But it is almost the same proof as the right one.

False Theorem 2 *All men are created equal (or, all horses are brown).*

Proof. Let $P(n)$ be the proposition that all men in a set of n men are equal. Clearly, $P(1)$ is true. Now assume that $P(n)$ is true. Consider any $n+1$ men; number these as men $1, 2, 3, \ldots, n+1$. Now the first n of these men are equal and the last n are equal too. Since the set of the first n men and the last n men overlap all men must be equal. This shows that $P(n+1)$ is true and finishes the proof by induction.

■

The above proof is wrong because the inductive step does not work for $n=1$, i.e. the truth of $P(1)$ does not imply the truth of $P(2)$.