CS 6363.005.19S Lecture 2—January 17, 2019

Main topics are #asymptotic_notation and #induction.

Prelude

- Please fill out the prerequisite form if you haven't already. Thank you!

Introduction

- We'll start today by discussing the asymptotic notation used for analyzing algorithms.
- Then, we're going to discuss induction, a method for proving universally quantified propositions, and the most useful tool we have available for reasoning about, proving correctness for, and analyzing algorithms.

Asymptotic Notation

- **[See LaTeX notes on asymptotic notation.]**

Prime Divisors

- To get to induction, we're going to iterate over successively better proofs concerning prime divisors of positive integers.
- A *divisor* of a positive integer n is a positive integer p such that n / p is an integer.
- A positive integer is *prime* if it has exactly two divisors, itself and 1.
- It is *composite* if it has more than two divisors.
- 1 is neither prime nor composite.
- Theorem: Every integer greater than 1 has a prime divisor.
- This is a universally quantified statement. We need to prove it about *all* the integers greater than one. And there's only two ways to do that.
  - Direct proof: Let n be an arbitrary integer greater than 1.
    - **BLAH BLAH BLAH**
    - Thus, n has at least one prime divisor.
  - Proof by contradiction:
    - For the sake of argument, assume there is an integer greater than 1 with no prime divisor.
    - Let n be an arbitrary integer greater than 1 with no prime divisor.
    - **BLAH BLAH BLAH WITH LOTS OF SPACE**
    - But that's just silly. Our assumption must be incorrect.
- Proofs by contradiction are usually easier to discover, so let's start there.

- And to make things easier, we're going to pick a very specific counterexample. The smallest one.
- Proof by contradiction:
  - For the sake of argument, assume there is an integer greater than 1 with no prime divisor.
  - Let n be **the smallest** integer greater than 1 with no prime divisor.
    - Since n is a divisor of n and n has no prime divisors, n cannot be prime.
    - Thus, n must have at least one divisor d such that 1 < d < n.
  - Let d be an arbitrary divisor of n such that 1 < d < n.
    - **Because n is the smallest counterexample, d has a prime divisor.**
  - Let **p** be a prime divisor of d.
    - Because d / p is an integer, n / p = (n / d) * (d / p) is also an integer.
    - Thus, p is also a divisor of n.
    - But this contradicts our assumption that n has no prime divisors!
  - So our assumption must be incorrect.
- Great, we have a proof!

- But we can do better. Contradiction proofs are easy to write, but direct proofs are much easier to read. And when your readers include the people grading your homework, you probably want to make things easy to read.
- There's one thing we can take from the previous proof, though, that makes it all work. When we assumed n was the smallest counterexample, what we were also doing is assuming there were no *smaller* counterexamples.
- This is exactly what you do in a proof by induction.
- Proof by **induction**: Let n be an arbitrary integer greater than 1.
  - **Assume that every integer k such that 1 < k < n has a prime divisor.**
  - There are two cases to consider: Either n is prime, or n is composite.
  - Suppose n is prime.
    - Then n is a prime divisor of n.
  - Suppose n is composite.
    - Then n has a divisor d such that 1 < d < n.
    - Let d be a divisor of n such that 1 < d < n.
    - By assumption (i.e. there are no smaller counterexamples), d has a prime divisor.
    - Let p be a prime divisor of d.
    - Because d / p is an integer, n / p = (n / d) * (d / p) is also an integer.
    - Thus, p is also a divisor of n.
  - In each case, we conclude that n has a prime divisor.
- This is called *proof by induction*.
- The assumption that there are no counterexamples smaller than n is called the *induction*

hypothesis.

- The case we argued directly is called a *base case*. Yes, every prime number is a base case. No, base cases are not always small.
- The other case was the *inductive case*.
- Maybe you want to label the inductive hypothesis, the base case, and the inductive case. That's up to you and how comfortable you feel doing these proofs.
- But until you're very comfortable doing these proofs, you do need to explicitly write out your inductive hypothesis and make the case analysis obviously exhaustive.
- Again, I want to emphasize there is very little difference between this proof by induction and a proof by smallest counterexample except in readability.
- Originally, we relied on the observation that "n has no prime divisor => some number smaller than n has no prime divisor"
- The direct proof just relies on the contrapositive, "every number smaller than n has a prime divisor => n has a prime divisor"

Proofs by Induction

- So what's the recipe here?
    1. **Write down the boilerplate.** Write down the universal invocation "Let n be an arbitrary…", the induction hypothesis, the conclusion, and leave blank space for the remaining details. **This is the easy part.**
    2. **Think big.** DO NOT think how to solve the problem all the way down to the ground. Don't think about small numbers like 1 or 5 or 10^100. Think about how to reduce proofs about gigantic numbers (the inductive case) to proofs about some other smaller number or numbers. **This is the hard part.**
    3. **Look for holes.** Look for cases where your inductive argument breaks down (the base cases) and solve them directly. Don't be clever; be stupid but thorough.
    4. **Rewrite everything.** You probably didn't leave the correct amount of space. Rewrite the proof so the argument is easier for someone (the grader) to follow.
- Cases in inductive proofs are either inductive cases or base cases. Base cases are *usually* a few small values of n, but they may be other things like all prime numbers. Induction proofs are usually easier to read if they describe the base cases first, but I find it easier to discover the inductive cases first so you know which gaps need to be filled in with base cases.