Chapter 4 notes

The reason we’ve been spending so much time learning the ins and outs of formal logic is that we can express many interesting things about CS using logic.

There exists c > 0, n0 > 0 forall x in R x > n0 -> f(x) < c\*g(x)

When creating new algorithms or data structures, we often want to prove things about how fast they are or how much memory they use.

Prove there is no sorting algorithm can can sort faster than n log n.

A binary tree if height h can store 2^h pieces of information.

P vs NP = If a solution to a problem can be verified quickly, can the solution be found quickly? Sudoku example: a sudoku puzzle is easy to verify that it solves the puzzle, but all algorithms to solve it run slowly.

PROOFS

* Most proofs involve proving a quantified statement (either an existentially quantified or universally quantified)
* You’ve already seen how to prove each of these sorts of statements.
* In your formal logic proofs, you had to only go one step at a time, and not combine steps, and everything had to be justified with a rule.
* Now, you’re going to be able to start combining steps, and occasionally leaving out justifications, for things that are very easy to understand.
  + Like things derived through algebra, like
* What this means is that now we’re building a bridge out of longer and stronger planks, with fewer supports in between.
* This lets us build the bridge quicker, but it’s easier for the bridge to break, because there are fewer supports. This is a trade-off we make when writing proofs because once we start proving more complicated things, if we did everything in formal logic it would take way too long.

**Definitions**

* + One of the ways we can build longer planks in our proof bridge is by using predicates that stand for long propositions.
  + These are called definitions.
  + Define even (exists k st n=2k)
  + Define odd (exists k st n=2k+1)
  + Definitions are logical equivalences, which means you can go back and forth between both sides. Whenever you do, the rule is “definition of \_\_\_”
  + Mini class exercises:
    - Is 7 odd?
    - Is 8 even?
    - If a is an integer, is 6a even?
    - If a is an integer, is 6a + 4 even?
    - If a is an integer, is 6a + 1 odd? What about 6a + 3?
* Laws of algebra
  + Most regular rules cite as “algebra”
  + Transitivity: a = b ^ b = c -> a = c.
  + Integers are closed under addition, subtraction, multiplication, and positive exponentiation.
* Key concepts to a proof:
  + Only true things can be stated in a proof
    - Things that are you are given to start off with (premises)
      * In “real” proofs, there are usually too many premises to write them all down, so we just assume you know them and can cite them when needed (like rules of algebra)
    - Things that you have proven to be true earlier in the proof.
  + Things that you WANT to be true, until you’ve proven them, should go in a scratch area.
  + HAVE/WANT lists
  + Example – proving equation to be true. Start with L, transform into R. or backwards. Or transform L and R into a common M.
  + ~~Def’n of prime~~ 
    - ~~N is prime <-> forall pos ints r & s, (n=rs -> (r=1 and s=n) or (s=1 and r=n))~~
    - ~~N is composite <-> not prime <-> exists pos ints r&s st n=rs and~~ 
      * ~~(1 < r < n) and (1 < s < n)~~

Proving Existential statements.

* Let’s prove that 7 is odd.
* Prove Odd(7).
  + Prove exists k in Z s.t. 7=2k + 1.
* How to prove an existential statement? The only rule that lets us add a exists sign is existential generalization.
  + There were two forms – one with a constant, and one with a variable that we obtained through existential instantiation.
* Here, we can use the one with a constant.
  + “Let k = 3.” Or “Define k = 3” or “Choose k=3”
  + Write: 7 = 2k+1. (algebra)
  + Write, therefore exists k in z s.t. 7=2k+1
  + Write, therefore, 7 is odd by def’n of odd.
* Could have used any variable name.

First way of proving existential: find an element of the domain that satisfies the predicate and show how it satisfies it.

How to prove a universal statement.

* Method of exhaustion.
  + Only works for universal statements where domain is finite.
  + Any even integer between 4 and 26 can be written as the sum of two primes.
  + Forall x in Z^even, exist y, z in Z^prime s.t. x = y + z.
  + All possibilities for x drawn from a finite set.
  + Therefore, we can enumerate all the possibilities.
    - If x = 4, then choose y = 2 and z = 2.
    - If x = 6, choose 3 and 3. Etc etc
    - See book
* Generalizing from the generic particular. Corresponds to beginning a proof with universal instantiation, and ending with universal generalization.

Review:

Proving an existential statement:

* Constructive proof of existence.
  + To prove exists x in D P(x), explicitly find an x in D and demonstrate that it satisfies P.
    - [example, show exists k in Z 8=2k. Find k=4. Show 8=2k. ]
* Proving universal statement.
  + Method of exhaustion.
  + Generalizing from the generic particular.
* Do sum of two evens is even. **[HAS ANSWER HANDOUT**]
  + Forall x, y in Z, if x and y are even, then x + y is even.
  + Write “suppose x and y are arbitrary integers.” Or “Let x and y be arbitrary in Z” This is the word form of univ instantiation with a variable.
  + Assume x, y are even. [enter cond world ]
  + By def of even exists k, m such that x = 2k and y = 2m.
    - Exist inst always creates a new var, so we can’t reuse the same var
  + X + y = 2k + 2m = 2(k + m)
  + Let t = k + m. t is an int by closure of Z under addition.
  + Then x+y = 2t
  + X + y is even by the def’n of even.
  + Can combine starting statement to be “assume x,y is an arb even integer.”
* Do if x is even, then x + 5 is odd. [**HAS ANSWER HANDOUT]**  
  + Prove for all integers x, if x is even then x + 5 is odd.
  + Forall x in Z Even(x) -> Odd(x+5)
  + Write “Suppose x is an arbitrary integer.” “Let x be arbitrary in Z”. (This is the word form of universal instantiation with a variable [arb but specific])
  + Write “Assume x is even.” (enter cond world)
  + Exists k in Z st x = 2k (def’n of even)
    - Can leave out exist instantiaion.
  + X + 5 = 2k + 5 (alg)
  + Exists k in Z st x + 5 = 2k + 5 (exist gen)
  + X + 5 is odd by def’n of odd.
  + Therefore Even(x) -> Odd(x+5) CCW
  + Forall …. By univ gen.
* Can leave out ending with CCW and univ gen b/c so common.
* Can combine starting statement to be “assume x is an arb even integer.”
* Generalizing from GP usually involves things of the form for all x P(x) -> Q(x).
  + Prove all ripe bananas are tasty.
  + Prove if a banana is yellow and spotted, then it is ripe.
* Common mistakes
  + Arguing from examples – cannot use this to show a universal statement. An example only proves an existential statement, not universal.
  + Using same variable to mean two different things (exist inst needs diff var each time)
  + Combining steps (leaving out factoring above)
  + Begging the question (assuming what you want to prove)
  + Mixing up things you know with things you want to know.
* Class does: prove the product of two even #s is even.
  + Prove that if m is odd and n is even, then m + n is odd.

* Proving things false.
  + Equiv to proving negation true.
  + Prove forall a, b, in R, a < b implies a^2 < b^2.
    - Exists x, y, st x is even and x + y is not even.
    - Let x = 4 and y = 1. Therefore x + y = 5, which is = 2(2) + 1, and is therefore odd.
  + Prove there exists x, y, st x is even and y >= 1, and x^y is odd.
* 4.2 Direct Proof II
  + Def’n of rational
    - R is rational IFF exist a, b s.t. r = a/b and b neq 0.
  + Prove sum of rationals is rational.
    - a/b + c/d = ad/bd + bc/bd = (ad+bc)/bd
    - let p = ad+bc q = bd
  + **As class: suppose a, b, c, d are ints and a neq c. And suppose x is a real number and (ax+b)/(cx+d)=1. Prove x is a rational number.**
* 4.3 Divisiblity
  + Def’n of divides: a | b IFF exists k s.t. b = ak
    - B is a multiple of a/a is a factor of b.
    - Smaller number always on left (or equal). That’s how you can remember b=ak.
    - Handy reminders: 1 divides anything. Anything divides 0. Anything divides itself. Negatives OK.
  + Very similar to even. Even(x) <-> 2 | x
  + Simple ex: a|b and a|c, then a|bc
* 2nd day of divisibility:
  + Transitivity of divisibility.
  + Discuss idea of proving something false.
  + Disprove (a | b) and (b | a) 🡪 (a=b)
  + PROVE: Sum of 3 consec ints is divisible by 3.

Discuss “has the form of”/”can be written as”

New pseudo-definition: “Has the form”:

* The language, “n has the form [blah blah] for some integer k” what they mean is: “There exists an integer k such that n = [blah blah].”
* Example: Odd(x) === x has the form 2k+1 for some integer k.
* Even(x) === x has the form 2k for some integer k.
* PerfectSquare(x) === x has the form k^2 for some integer k.
  + If a number n can be written as 6k+3 for some int k, then n^2-1 can be written as 3s+2 for some int s.
  + TRUE: if ab|c, then a|b or a|c.
  + FALSE: if a|(b+c), then a|b or a|c. ctrex: 2|(3+3), but 2 does not divide 3.
  + UPFT
  + Def of prime: Prime(n) for all r,s in Z^pos, (n = rs) -> [(r = 1 and s = n) OR [r = n and s = 1])
  + Forall int n > 1, exists pos int k, distinct primes p1 through pk, and pos ints e1 through ek such that n = p1^e1 \* p2^e2 … pk ^ ek.
  + Use. Prove that if 5m = 17n, then 17|m.
* 4.4 Quotient-remainder thm
  + go over idea of counter examples.
    - For all a, b, a|b -> b|a
    - Negation is exists a, b, st a|b and b/| a
    - How to prove a |\ b? (forall k in Z, b neq ak)
      * Not equals is hard to work with
      * Alternate definition b/a is not an integer
      * Ok for explicit integers, not ok for complicated expressions
  + Given any integer n and positive integer d, there exist unique integers r and s s.t. n = dq+r and 0 leq r < d.
    - This is not a definition, this is a theorem, so it can be proven (we don’t have to take it as a given, like the definition of even). The proof is in a later part of the book.
    - Formalization of the division process you learned in elementary school.
      * Says that when you divide n by d, you get a quotient q, and some remainder that is always between 0 and d.
    - Another way to look at it means that because the multiples of d occur every d spaces on the number line, for any number n, you pick, you never have to move more than d spaces to the left to get to a multiple of d.
  + What the “unique” part means.
    - Consider what happens when d=2.
    - N = 2q + r, 0 leq r < 2.
      * What are possibilities for r: r=0 and r=1.
      * Expand to get n=2q+0 or n=2q+1.
    - So this means every integer is even or odd. Now because or is inclusive, this statement means something could be even and odd. But because r is unique, that means that if n=2q+0, (r=0) then we can’t also have the statement work when r=1.
  + Use of q-r theorem in a proof.
    - Often combined with the propositional logic rule dilemma or “proof by div into cases.”
    - Show “expanded” dilemma.
  + **Do proof:** product of consec 3 ints divisible by 3. (did before with sum)[**HAS HANDOUT**]
    - X(x+1)(x+2) = x(x^2 + 3x + 2) = x^3 + 3x^2 + 2.
    - Write x as 3q, 3q+1, or 3q+2.
  + **Do proof:** Square of any odd integer has the form 8m+1 for some integer m.[**HANDOUT**]
    - Works with 2 cases, if you use QRT on the k from odd.
    - 4 cases if you use on the number itself.
    - (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k)+1.
    - To get 8, consider x = 4q or 4q+1 or 4q+2 or 4q+3
  + **Do proof**: Square of any integer has the form 3s or 3s+1.[**HAS HANDOUT**]
    - Use qrt with d=3.
* 4.5
  + proof by contradiction.
  + Using CCW with contradiction
    - There is no greatest integer.
    - Give def
    - Prove for all integers m, 7m + 4 is not divisible by 7.
    - Assume 7 divides 7m+4.
    - 7k = 7m+4
    - 7k-7m = 4
    - 7(k-m)=4
    - k-m = 4/7 contradiction: one side is int and one is not.
  + Contraposition: if n^2 is even, then n is even.
* 4.5, 4.6, unique prime factorization
  + Proof by contrapositition.
  + Forall x P(x) -> Q(x).
    - Can also prove contrapositive.
  + If n^2 is even, then n is even.
  + Proof by contradiction.
    - For all ints n, 3 does not divide 9n-4.
  + Primes:
    - Prime(n) <-> n>1 and forall r,s, n=rs -> r=1 and s=n or r=n and s=1
    - Prime(n) <-> n>1 and forall d in Z+, d | n -> d=1 or d=n.
  + Prove for any prime number p>3, p cannot be written as 9k+6 for any int k.
  + UPFT: (fundamental theorem of arithmetic)
    - Given any int n>1, there exist int k in Z+, distinct prime #s p1 through pk, and positive ints e1 through ek such that n=p1 e1 p2 e2 .. pk ek.
    - AND any other expression for which n is the product of prime numbers is identical to this one, except for the order in which the factors are permitted.
    - Meaning: there is exactly one way to write any integer >1 as the product of prime numbers.
    - Standard factored form p1 < p2 …
  + Ex: Prove for all ints a, b, if 12a = 25b, then 12|b.
    - By UPFT, the standard factored forms of 12a and 25b are identical.
    - 12a = (2 \* 2 \* 3)a
    - 25b = (5 \* 5)b
    - So 25b contains the factors 2 \* 2 \* 3. But since none of those factors are in the 5 \* 5 part, they must all be factors of b. So 12|b.
  + 2 indirect proofs.
    - Pf of sqrt(2) is irrational. (proofs of irrationality are usually done by contradiction)
    - Assume sqrt(2) is rational.
      * Exist a,b b neq 0 st sqrt(2) = a/b
      * assume that a and b have no factors in common (in lowest terms).
      * Square both sides to get 2 = a^2/b^2.
      * A^2 = 2b^2.
      * So a^2 is even. We know from before that a is also even.
      * So a = 2k
      * Substitute in: a^2 = (2k)^2 = 4k^2 = 2b^2.
      * Take 4k^2 = 2b^2 divide both sides by 2 to get 2k^2 = b^2.
      * B^2 is even. B is even. CONTRA!
  + Prove there are an infinite # of primes.
    - Lemma: for any int a and prime p, if p | a then p /| (a+1).
    - Suppose not. Assume there is a and p such that p | a and p|a+1.
    - Then there exist r, s, (divisibility) such that a=pr and a+1=ps.
    - (a+1) – a = 1
    - = ps – pr = p(s-r)
    - 1 = p(s-r), so p | 1.
    - But any prime is bigger than 1, and the only things that divide 1 are 1 and -1. CONTRA.
  + Prove there are an infinite # of primes.
    - Suppose not. Suppose finite # of primes. List them: 2, 3, 5, … up to some max p.
    - Let N = the product of all the primes + 1.
    - By UPFT, N can be written as the product of primes, so there is some prime that divides N. Call that prime q.
    - Q | N.
    - However, because Q is a prime, Q must be one of the primes listed , so Q | N-1.
    - However, by previous lemma, b/c Q | n-1, q /| n. Contra.
  + Prove there exist irrational numbers a, b, such that a^b is rational.
* Indeed, if √2√2 is rational, then take *a* = *b* = √2. Otherwise, take *a* to be the irrational number √2√2 and *b* = √2. Then *ab* = (√2√2)√2 = √2√2·√2 = √22 = 2, which is rational.
  + - (turns out sqrt(2) ^ sqrt(2) is irrational).

REVIEW FOR TEST: (covers up through 4.3, no QRT)

Prove: if a+b is odd, then a-b is odd.

Prove: if n can be written as 3k+2 for some ODD integer k, then n+1 is divisible by 6.

Prove: The difference of squares of any two consec ints is odd.

Prove: If a and b are both positive integers > 1 that are also perfect squares with a<b, then their difference is not a prime number.

Prove: If n can be written as 3k+1 for some integer k, then n^2-2n+1 is divisible by 9.

Prove: If n can be written as 3k+1 for some integer k, then n^2+2n is divisible by 3.

Prove: If n can be written as 3k+1 for some integer k and m can be written as 3p+2 for some integer p, then 3|k+m. OR …. 3 | (k-m+1) OR …. 3 | (k^2-m^2) OR …. K –m can be written as 3h+2 for some int h.