Lecture Notes for CSCI 311: Algorithms

Set 3-Proof Techniques

Professor Talmage

September 2, 2024

---

1 Overview

Before I ask you to write many of your own proofs, we will step back from algorithms and review some basic proof techniques. There is no possible set of precise guidelines that will tell you exactly how to write a proof, but your arguments will tend to use some of these patterns, so we will look at them individually. Note that the actual claims we will prove here are not particularly related to algorithms. These are just to demonstrate the proof techniques.

2 Techniques

- Direct Proof: Start with things you know are true (such as the preconditions of the claim you are proving) and derive more facts from those. Repeat until you reach the desired conclusion.

  Claim 1. *If m and n are perfect squares, then mn is a perfect square.*

  Proof. We know that m and n are perfect squares, which means, by definition, that $m = a^2$ and $n = b^2$ for some integers a, b. Since multiplication is commutative, $mn = a^2b^2 = (ab)(ab) = (ab^2)$. Since the integers are closed under multiplication, ab is an integer, so mn is the square of an integer and thus a perfect square. □

  Aside: It is **very** important that you only assume the precondition of the claim, not the desired conclusion. Assuming the conclusion is one of the most common errors I see in this class' homework. Once you have assumed the thing you are trying to prove, or something equivalent unrelated to the starting point of the claim, it becomes impossible to complete the proof, since you cannot prove an assumption. So, technically, no matter how good the rest of your work is, if you assume the conclusion, your proof is wrong.

  Exercise: Prove that if a and b are even, then $a + b$ is even.

- Proof by Contrapositive: If we want to prove something of the form A implies B (see above), recall that $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. This is the *contrapositive* of the desired claim. Since any implication is equivalent to its contrapositive, a proof by contrapositive is just a direct proof of the desired claim's contrapositive. Start from $\neg B$ and derive more facts until you reach $\neg A$.

  Exercise: Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

- Proof by Contradiction (a.k.a. Indirect Proof): Assume the desired statement is false. Follow the implications of that assumption to prove a contradiction (any contradiction!)–something which is simultaneously true and false. This means that the assumption was wrong, and the desired claim is true.
  - Watch out for multiple assumptions, a contradiction only disproves one!
  - We did this last time for `InsertionSort`: We assumed that it ever produced a non-sorted output, showed a contradiction, and concluded that it never produced a non-sorted output.

  Claim 2. *Given a set of 9 courses required for an (imaginary) CS major, at least two will fall in the same semester.*

  Proof. Assume not. Then there is at most one CS course per semester, for a total of 8 courses, since Bucknell degrees take 8 semesters. This contradicts the fact that there are 9 required courses, showing the assumption is incorrect and some semester will have two CS courses. □

  - We call this particular form of counting argument the *Pigeonhole Principle*: If there are n items to go in k boxes, some box will have at least $\lceil n/k \rceil$ items.
  - If you have 100 pigeons and only 49 pigeonholes, some hole will have 3 pigeons If that's overcrowding, you can conclude that you need at least 50 boxes.
  - This principle may seem obvious, but it shows up in odd places and is super useful.

  One final note: If you are proving a conditional (A implies B), we have to recall the negation of an if-then statement: $\neg(A \Rightarrow B) \equiv \neg(\neg A \vee B) \equiv (A \wedge \neg B)$. Thus, to assume the opposite of a desired implication $A \Rightarrow B$, we assume that A is true and B is false, then derive our contradiction.

  Exercise: Prove that if $5n + 6$ is odd, then n is odd.

- Proof by Construction: Show that something exists by giving an example.

  Claim 3. *There is no largest prime number*

  Proof. We will start with a proof by contradiction, then inside that proof construct a particular value to show that a value of that type exists.

  Assume in contradiction that there is a largest prime number. Any one number is finite, so there are finitely many prime numbers (recall that every prime is a positive integer). Multiply all the prime numbers and call the result P. Note that P is larger than the largest prime.

  Add 1 to P. $P+1$ is not divisible by 2, since it is odd, as 2 was a factor of P. Similarly, P is divisible by 3, so $P + 1$ is not. In fact, since P is divisible by *every* prime number, and every prime number is greater than 1, no prime divides $P + 1$. No other number greater than 1 can divide $P + 1$, as its prime factors would be able to, as well. Thus, $P + 1$ is prime, and larger than the largest prime, a contradiction. We can thus conclude that there is no largest prime number. □

  Exercise: Prove that there is an invertible function from every set to itself.

- Proof by Cases: *Partition* the space of possibilities into subsets and prove separately that the desired claim holds for each subset.
  - We did this for the intermediate claim in the correctness proof of `InsertionSort`, considering the possible orders in which certain values could have been *key*.

- The most important thing is that you must consider every possible case. If you skip any, then you have no proof at all.

Claim 4. $|x| * |y| = |xy|$

Proof. Consider whether each of x and y is positive or negative:

1. $x > 0, y > 0$
2. $x > 0, y < 0$
3. $x < 0, y > 0$
4. $x < 0, y < 0$
5. One or both of $x, y = 0$

Note that we can reduce cases 2 and 3 to the same case (one positive, one negative), since $(-a)(b) = (a)(-b)$. Whenever possible, once you have set out all cases, combine those for which the argument will be identical.

Exercise: Prove each case.

□

- Induction: A technique for proving an infinite number of cases, most often that a claim is true for all positive integers.
  - Induction is one of the strongest frameworks for a proof. That is, inductive proofs lay out a pattern for you to follow. Use this to your benefit, as you can tell whether you have completed the proof by whether you have completed the pattern.
  - The general outline of an inductive proof is:
    - Claim: For all $x \in \mathbb{Z}^+, P(x)$.
    - Proof:

    BC Show $P(1)$ is true.

    IH Assume that for an arbitrary $k \geq 1$, $P(k)$ is true.

    IS Using $P(k)$, show that $P(k+1)$ is also true.
  - The logic built into the inductive hypothesis/inductive step is that $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, $P(3) \Rightarrow P(4)$, and so on to infinity. Thus, since $P(1)$ is true, $P(x)$ is true for every positive integer x.

Claim 5. $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$

Proof. Proceed by induction on n:

BC This is the case when $n = 1$: $1 = \frac{1(2)}{2}$, so the base case holds.

IH Assume that the claim holds for an arbitrary value of n. That is, for an arbitrary $k \geq 1$, assume $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$.

IS We now need to show the $k+1$ case. $1+2+\cdots+(k+1) = (1+2+\cdots+k)+(k+1)$. By the inductive hypothesis, we can substitute for the first part: $= \frac{k(k+1)}{2} + (k+1)$. Then we just need to manipulate the expression to the desired final form:

$$\begin{aligned} 1+2+\cdots+(k+1) &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k^2+k}{2} + \frac{2k+2}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2} \end{aligned}$$

Thus, by mathematical induction, the claim holds for all $n \geq 1$. □

– Sometimes you will not be able to prove $P(k+1)$ using only $P(k)$, typically when it is defined in terms of more or farther previous values. In this case, we use *strong induction*. The only difference is that we change the inductive hypothesis to assume *all* previous cases $P(1), \ldots, P(k)$, not just the one immediately prior.

Exercise: Prove that any postage amount of at least 12 cents can be evenly reached using only 4- and 5-cent stamps.

Proof. Proceed by strong induction on the amount of postage.

BC We need several base cases:

* $P(12)$: three 4-cent stamps
* $P(13)$: two 4-cent stamps, one 5-cent stamp
* $P(14)$: one 4-cent stamps, two 5-cent stamps
* $P(15)$: three 5-cent stamps

IH Assume that for an arbitrary $12 \leq k$, we can make exact postage of any value $12 \leq m \leq k$ cents using only 4- and 5-cent stamps.

IS We need to show that we can make exact postage of $k+1$ cents. By assumption, we can make exact postage for $(k+1)-4$ cents. Add a 4-cent stamp and we have exact postage for $(k+1)$ cents.

Thus, by strong induction, we can make exact postage for any postage amount of at least 12 cents. □

Exercise: Prove that every positive integer greater than 1 is the product of one or more primes

– Base case is 2.

– Consider cases: If n is prime, you are done. Otherwise, $n = k * \ell$, where k and ℓ are smaller than n, and thus the inductive hypothesis assumes they are products of primes.