COMPSCI 230: Discrete Mathematics for Computer Science January 14, 2019

Lecture 2

Lecturer: Debmalya Panigrahi *Scribe: Erin Taylor*

1 Overview

In this lecture, we continue to overview mathematical proofs. We explore types of statements we might wish to prove, and outline general proof techniques.

2 Implications

The goal of every proof is to show that a proposition is true. It is often the case that the proposition in question can be written in the form "P implies Q", where P and Q are statements. Propositions of this form are known as *implications*; we can think of them as "If . . ., then . . ." statements. The proposition "P implies Q" is equivalent to "If P, then Q."

Consider the following proposition:

Theorem 1. *If n is prime and even, then $n = 2$.*

We shall prove this proposition in two separate ways: a direct proof, and proving the contrapositive. In a direct proof, we assume that P is true, and then we show a sequence of implications and eventually conclude with Q.

Proof of Theorem 1. Start by assuming that n is prime and even. Now observe the following:

1. Since n is prime, n is not divisible by a number smaller than n (other than 1).
2. Since n is even, n is divisible by 2.

These two statements together imply that 2 is not smaller than n, or in other words, n is at most 2. Thus, n is either 1 or 2. However, since 1 is not divisible by 2, n must be equal to 2 as desired. □

Recall that the contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$. Thus, the contrapositive of the given proposition is the following:

If $n \neq 2$, then n is not prime or n is not even.

(The "or" here is inclusive, that is, it is possible for n to be both not prime and not even.) Since the contrapositive of an implication is logically equivalent to the original statement, a proof of the contrapositive is sufficient to prove the statement.

After stating the contrapositive, we then prove it by giving a direct proof (as we did in the previous proof).

Proof of Theorem 1. Assume $n \neq 2$. Observe that n must be either even or not even, but not both.

- If n is not even, then n satisfies the conclusion of the contrapositive, so we're done.

- If n is even, then n is divisible by 2. Since $n \neq 2$ by assumption, this implies that n is divisible by a number other than 1 and n. Thus, n is not prime.

Thus, regardless of whether n is even or not, we have shown that $n \neq 2$ implies n is not prime or n is not even. This proves the contrapositive, which proves the original implication. □

Notice that we used the fact that the negation of the predicate "n is prime and even" is "n is not prime or n is not even." This rule illustrates a general principle that we will discuss in future lectures. Consider another example of an implication:

Theorem 2. *If* $0 \leq x \leq 1$, *then* $-x^3 + x + 1 > 0$.

Before we write a formal proof of the theorem, we want to understand why this statement is true. Consider the expression $-x^3 + x + 1$:

$$-x^3 + x + 1 = x(1 - x^2) + 1 = x(1 + x)(1 - x) + 1$$

Consider only the product $x(1 + x)(1 - x)$. By definition, $x \geq 0$, so the first term of the product is non-negative. $x \geq 0$ also implies that $1 + x \geq 1 > 0$ so the second term is also non-negative. Finally, we know that $x \leq 1$ so $1 - x \geq 0$. Thus, the three terms of the product are all non-negative and the product must be non-negative. This implies $x(1 + x)(1 - x) + 1 = -x^3 + x + 1 > 0$. Note that this is not a formal proof, we were just doing some work to understand why the implication holds. We now formalize this work:

Proof of Theorem 2. Let x be a real number such that $x \geq 0$ and $x \leq 1$.

$$x \leq 1 \implies 1 - x \geq 0$$

$$x \geq 0 \implies 1 + x \geq 1 \implies 1 + x > 0$$

Therefore $x(1 - x)(1 + x) \geq 0$ since the product of non-negative terms is also non-negative. Thus, we have: $x(1 - x)(1 + x) \geq 0 \implies x(1 - x)(1 + x) + 1 > 0 \implies -x^3 + x + 1 > 0$. □

There are many ways of proving the same statement. Let's consider another proof of Theorem 2:

Proof of Theorem 2. Let $f(x) = -x^3 + x + 1$. Then:

$$f'(x) = -3x^2 + 1$$
$$f''(x) = -6x$$

For $0 \leq x \leq 1$, $f''(x) \leq 0$. This means $f'(x)$ is non-increasing on this domain. Thus, $-2 \leq f'(x) \leq 1$ since $f'(0) = 1$, $f'(1) = -2$, and $f'(x)$ is non-increasing for $0 \leq x \leq 1$. From $f'(x)$, we know that in the domain $0 \leq x \leq 1$, $f(x)$ increases and then decreases. Thus, the minimum value of this function in this domain must be realized at either $x = 0$ or $x = 1$. Therefore, $f(x) \geq \min\{f(0), f(1)\}$ for $0 \leq x \leq 1$. Since $f(0) = f(1) = 1$, this implies $f(x) \geq 1 \ \forall x$ such that $0 \leq x \leq 1$. □

Now, let's consider an example where proving the contrapositive of an implication is significantly more straightforward than proving the implication directly.

Theorem 3. *If r is irrational, then $\sqrt{r}$ is also irrational.*

Let's begin by making sure we understand the statement. What does $\sqrt{}$ mean?

Definition 1. *The symbol* $\sqrt{}$ *always refers to the positive square root.*

Take $\sqrt{4}$. You might be tempted to say that $\sqrt{4}$ is either 2 or -2, but this is incorrect. The $\sqrt{.}$ refers only to the positive square root (in this case, 2). On the other hand, if we asked for the solution to $x^2 = 4$, it would be both 2 and -2. Theorem 3 also refers to irrational numbers. What are irrational numbers?

Definition 2. Irrationals *are real numbers which are not rational.*

Definition 3. *A real number r is* rational *if there exist two integers, p, q where $q \neq 0$ such that*

$$r = \frac{p}{q}$$

In this instance, it is difficult to work with irrational numbers due to their indirect definition. Consider the contrapositive to Theorem 3: If $\sqrt{r}$ is rational, then r is also rational.

Proof of Theorem 3. Since $\sqrt{r}$ is rational we know

$$\sqrt{r} = \frac{p}{q}$$

for some integers p, q where $q \neq 0$. Then, $r = \frac{p^2}{q^2}$. p^2, q^2 are integers because p, q were integers. Furthermore, $q^2 \neq 0$ since $q \neq 0$. Thus, r is rational. □

This proof was straightforward. Thinking about proving the original statement, we would have to show that if r is *not* a ratio of integers, then $\sqrt{r}$ is *also not* a ratio of integers. It is not clear how one would proceed in a direct proof.

3 Equivalences

Definition 4. *Two statements are logically* equivalent *provided one holds if and only if the other also holds.*

We will say an equivalence is an "if and only if" (abbreviated *iff*) statement, and denote it by '$\iff$'. "A $\iff$ B" means that A holds only if B holds and B holds only if A holds. It is the same as saying $A \implies B$ **and** $B \implies A$. To prove an equivalence holds, you could prove these two implications separately.

Another way to prove an equivalence is to construct a string of logically equivalent statements: $A \iff C_1 \iff C_2 \iff ... \iff C_n \iff B$. We will see an example of this technique, but first we recall some definitions:

Definition 5. *The* mean *of a set of integers $x_1, x_2, \ldots, x_n$, often denoted μ, is the following:*

$$\mu = \frac{x_1 + x_2 + \cdots + x_n}{n}.$$

Definition 6. *The* standard deviation *of a set of integers $x_1, x_2, \ldots, x_n$, often denoted σ, is the following:*

$$\sigma = \sqrt{\frac{(x_1 - \mu)^2 + \cdots + (x_n - \mu)^2}{n}}.$$

Theorem 4. *The standard deviation of a set of integers is* 0 *if and only if each integer is equal to their mean.*

Let us introduce some notation. We will use Σ to denote a sum of numbers. For example, $x_1 + x_2 + \cdots + x_n = \sum_{i=1}^{n} x_i$. The subscript and superscript denote the range of the sum, in this case $1, \ldots, n$. We will now prove Theorem 4.

Proof of Theorem 4. Let $x_1, \ldots, x_n$ be a set of integers whose standard deviation is 0.

$$\begin{aligned}
\sigma = \sqrt{\frac{(x_1 - \mu)^2 + \cdots + (x_n - \mu)^2}{n}} = 0 & \qquad \text{by assumption} \\
\iff (x_1 - \mu)^2 + \cdots + (x_n - \mu)^2 = 0 & \qquad \text{by squaring and multiplying by } n \\
\iff (x_i - \mu)^2 = 0 \; \forall i & \qquad \text{since the terms are non-negative and sum to 0} \\
\iff x_i - \mu = 0 \; \forall i & \qquad \text{by taking the square root} \\
\iff x_i = \mu \; \forall i &
\end{aligned}$$

Therefore, the standard deviation of a set of integers is 0 if and only if each integer is equal to their mean. □

4 Proof Techniques

We will introduce two common patterns which proofs often follow.

4.1 Proof by Contradiction

In a proof by contradiction, we assume the proposition we wish to prove is false. If we wish to prove proposition P, we assume $\neg P$. Using this assumption, we make logical deductions to derive a false fact. Since this false fact cannot by true by definition, it must be that our original assumption was false, implying that the original proposition is true. Here is an example:

Theorem 5. $\sqrt{2}$ *is irrational.*

Before we begin, recall that a rational number is the ratio of two integers. Consider any ratio of integers: $\frac{p}{q}$. If p and q share any factors, we could reduce this fraction. We can continue cancelling common factors until the fraction is in lowest terms. The greatest common divisor (gcd) of the resulting two integers is 1. (Two numbers whose $gcd = 1$ are 'coprime').

Proof of Theorem 5. We proceed via proof by contradiction. Suppose the claim is false, and $\sqrt{2}$ is rational.

$$\implies \sqrt{2} = \frac{p}{q}$$

for some integers $p, q \neq 0$. We may assume that $gcd(p, q) = 1$ (this fraction is in lowest terms, if not redefine p and q so that this holds). Squaring both sides:

$$2 = \frac{p^2}{q^2} \implies p^2 = 2q^2$$

the last equality holds since $q \neq 0$. Since p^2 is even, p must be even. This implies $p = 2r$ for some r and $p^2 = 4r^2$. Plugging this back in:

$$4r^2 = 2q^2 \implies 2r^2 = q^2 \implies q^2 \text{ is even.}$$

Since q^2 is even, q must be even and $q = 2s$ for some s. Putting this all together we have:

$$\sqrt{2} = \frac{p}{q} = \frac{2r}{2s}$$

Consider this last equality. It implies that $gcd(p,q) \geq 2$. This contradicts our earlier assumption that $gcd(p,q) = 1$. Therefore, our original assumption must have been false, and we conclude that $\sqrt{2}$ is irrational. □

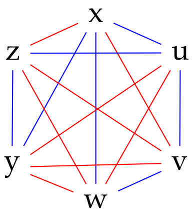
4.2 Proof by Cases

Sometimes it is useful to break a statement into cases and prove the statement for each case separately. These cases must capture all possible scenarios. Consider the following theorem:

Theorem 6. *In any group of* 6 *people, there are either* 3 *mutual friends (every pair knows each other) or* 3 *mutual strangers (no pair knows each other).*

Let's begin by considering the statement. With 6 people, there are 15 pairs. For each pair, they either know each other or they don't (each pair takes on one of two 'values'). Thus, there are $2^{15} = 32,768$ possible scenarios to consider. The large number of possibilities highlight that it would be unwieldy to try to list all possible scenarios individually. Instead, we will use a small number of cases that classify every scenario.

It may be helpful for understanding to draw a picture to help elucidate the cases. We have 6 people total. For any two people they either know each other or they are strangers. Consider a graph in which we label the six people. We add a blue edge between two people if they know each other, and add a red edge if they are strangers. A triangle of all red edges indicates that these three people are all strangers. A triangle of all blue edges indicates that these three people are mutual friends. For example:



Proof of Theorem 4.2. Fix a person x. There are two cases to consider:

Case A: There are ≥ 3 people who do not know x.

Case B: There are ≥ 3 people who know x.

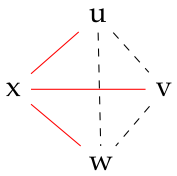


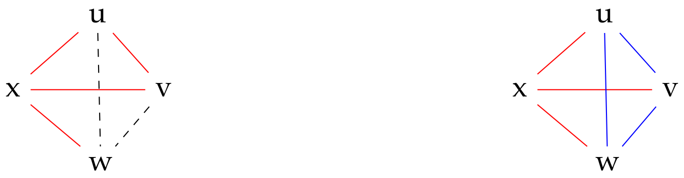
Figure 1: Case A

Splitting a group of 5 into two groups implies that the larger of the two groups must have at least 3 people in it. Hence, the two cases are exhaustive. Now, consider Case A. Case A occurs when at least three edges incident to x are red. Let three of these people be u, v, w. Our diagram:

We now consider the connections between u, v and w and define subcases.

Case A1: At least one pair among $(u,v)(v,w)$ or (u,w) do not know each other. Suppose this pair is (u,v). u and v do not know x, and they do not know each other. See Figure 2a.

Case A2: Every pair of people who do not know x know each other. In this case, u, v, w all know each other and, we have found 3 mutual friends. See 2b.



(a) Case A1

(b) Case A2

Figure 2: Case A

The theorem holds for both subcases; thus, the theorem holds for Case A. Now, consider Case B. There are at least 3 people who know x. At least three edges between x and the other people are blue. Let three of the people who know x be u, v, w. Our diagram:

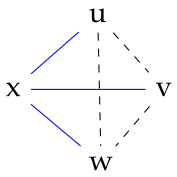
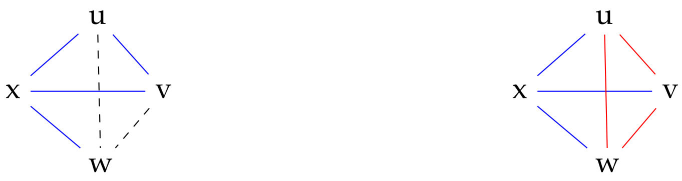


Figure 3: Case B

Case B1: At least one pair among $(u,v)(v,w)$ or (u,w) know each other. Suppose this pair is (u,v). Then, u, v, and x are 3 mutual friends. See 4a.

Case B2: All the people who know x do not know each other. In this case, u, v, w are 3 strangers. See 4b.

The theorem holds for both subcases, so the theorem holds for Case B. Thus, the theorem holds in all cases. □



(a) Case B1

(b) Case B2

Figure 4: Case B

5 Summary

In this lecture, we considered two forms of propositions: implications and equivalences. We saw examples of each type, and proved these statements. We also continued to build general strategies for proofs: including proving the contrapositive, proof by contradiction, and proof by cases.