Proof techniques: Direct Proofs

1 What is a Proof?

A **proof** is simply an argument that demonstrates that a statement is *definitely and unequivocally true*. Proofs should be understandable, clear, and well founded in logic. The ultimate goal of any proof is simply to *convince* the world of a statement, and as such most of us have some notion or instinct on how to "explain" that our idea is true. This section explores different ways of creating a *proper proof*: one that is logically sound, understandable, and clear. The methods of proof that are discussed in this course are essential to many applications of computer science: one many need to *argue* or *prove* that the output of a program is correct, or prove that a system is secure, or show that a system is operating consistently, or that a encryption method is safe.

Proving theorems can be difficult, and there is no magical formula that will tell you how it's done, nor is there a guaranteed path to success. Learning how to argue something is somewhat of an art, and is often a combination of techniques that you have learned, combined with a bit of inspiration. In our two lectures on proofs, we will practice common **types of proofs**: the direct proofs and the indirect proofs. This will enable you to identify and re-use these techniques in similar problems.

We will begin by drawing from some of the concepts and tools from *logic*...

1.1 Rules of Inference

One reason that logic is so important is that it provides a means of combining facts and information to produce *new* facts. This is something that we often do every day, and we may refer to it as a *pattern of thought*. For example, if someone told you that for lunch you could either have a sandwich or pizza, but then you found out they were sold out of pizza, you would *conclude* that you were having a sandwich. Sounds simple! This is an example of a **logical inference**. The logical inference rules that we will look at here are intuitively obvious, and you most likely use them in daily life. These rules have special names, which are not at all important for this course, but they are listed here just for reference.

Rule 1: Modus Ponens

If you know P is true, and you have a statement $P \to Q$, then you can conclude Q.

Rule 2: Modus Tollens

If you know $P \to Q$, and you know that Q is *false*, then you can conclude that P must be false.

Rule 3: Elimination

If you know that P or Q is true, and you know that P is *false*, then you can conclude that Q must be true.

There are many other logical deductions such as these that can be used in your proofs, and most of them are intuitively obvious.

The general **structure** of a proof usually consists of a *sequence of logical deductions* such as those above, which then results in the statement that you are trying to prove. This may seem daunting at first, since there is so much freedom in deciding what could follow next. However the good news is that many

proofs follow one of a handful of standard templates. We'll go through several of these patterns and give examples.

2 Direct Proof

The first technique is a *direct proof*. This method simply refers to the direct application of the *definitions and facts* given in the problem. We have already performed many direct proofs in this course, by simply applying the definition of the particular object. There is no technical information to add to this section, instead we proceed by working through some examples of direct proofs. The idea of these examples is to get more comfortable with proofs, and as such, most of them are very simple proofs based on numbers, division, etc.

We start with a very simple example of a direct proof on an *implication*, $P \to Q$. In this example, we simply **assume** P is true, and then **deduce** that Q is true.

Example 1. *Prove that if n is an even number, then n^2 is an even number.*

Solution: In a direct proof, we simply find a way to mathematically write down the information that we are given. Since n is an even number, then we know that it is a *multiple of 2*, which means that we can write it as $n = 2k$, for some number k. This is a very simple trick that can be used to express any even number (later we will express odd numbers as $2k + 1$). Since $n = 2k$, then $n^2 = 4k^2$. After that one step, we can see that n^2 is actually a multiple of 4, so certainly it is even.

Example 2. *Prove that using 8 cent stamps and 6 cent stamps, it is impossible to make a postage of 33 cents.*

Solution: Suppose we buy x of the 8-cent stamps, and y of the 6 cent stamps. Then the amount of postage we can make is $8x + 6y$. Notice that both $8x$ and $6y$ are even numbers, and thus their sum is also an even number. Thus the final postage amount will always be even, so it is impossible to make a postage of 33 cents.

Example 3. *Prove that for all integers a, b, and c, if a divides b, and b divides c, then a divides c.*

Solution: The direct proof starts with the information given and works *forward* towards the goal of proving that a divides c. For example, if a divides b, then we know that $b = ka$ (b is a multiple of a) for some integer k. We also know that $c = mb$ since b divides c which means that c is a multiple of b. At this point we have stated everything we "*know*" in terms of math and it remains to connect the dots. If we combine the two equations above we get:

$$c = mb = m(ka) = (mk)a$$

which means that c is a multiple of a. Thus a divides c and we have completed the proof.

Example 4. *Prove that if $x \neq 0$ is a rational number, then $1/x$ is also rational*

Solution: Since x is rational, that means that it can be written as a quotient of two integers. In other words there exists a $p, q \in \mathbb{Z}$ such that $\frac{p}{q} = x$. Now we work towards our goal: this means that $\frac{1}{x} = \frac{q}{p}$, which is *also* a quotient of integers. Therefore $1/x$ is also rational.

Example 5. *Prove that if n is an integer that is a multiple of 3, then n can be written as the sum of 3 consecutive integers*

Solution: If n is a multiple of 3 then we know that it can be written as $n = 3k$ for some integer k. Now we need three *consecutive* integers that sum up to n, which is $3k$. It may be helpful to start with

an example to decide where to go next. Suppose $n = 27$, then $27/3 = 9$ and notice that $8 + 9 + 10 = 27$. Using this as a guideline, if $n = 3k$ the integers that would work in general would be:

$$(k-1) + k + (k+1) = 3k = n$$

Example 6. *Prove that if a is an integer and a^2 divides a, then $a \in \{-1, 0, 1\}$.*

Solution: Since we are told that a^2 divides a, then a is a multiple of a^2. Thus $a = ka^2$ for some integer k. Solving this equation gives:

$$a - ka^2 = 0$$
$$a(1 - ka) = 0$$

Thus $a = 0$ or $(1 - ka) = 0$. In the second case, $ka = 1$, which means $a = 1/k$. However, k is an integer, and a is an integer, and $1/k$ is only an integer if $k = 1$ or $k = -1$. Thus the only possibilities for a are $\{-1, 0, 1\}$.

Example 7. *Prove that every odd integer is the difference of two squares (Ex. $7 = 4^2 - 3^2$)*

Solution: For this proof, it helps to do a few cases and notice the pattern. Notice $7 = 4^2 - 3^2$, and $19 = 10^2 - 9^2$, and $5 = 3^2 - 2^2$. Notice that the two squares are always *consecutive*. You might also notice that the second square is the (odd number -1)/2. Once you notice this pattern, it can be extended into a formal proof. We start with what we know from the question: that the given integer, n, is *odd*. This means it is one more than a multiple of 2: so we can write $n = 2k + 1$ for some k. Now we need to show that this is the *difference* of two squares. Using the pattern seen in the examples we tested, the smaller square would be $(2k)/2 = k$, which means the first square would be $k + 1$. It remains to verify if their difference is indeed n:

$$(k+1)^2 - (k^2) = (k^2 + 2k + 1) - k^2 = 2k + 1 = n$$

and thus the difference of $(k + 1)^2$ and k^2 is our original odd number.

2.1 Proof by cases:

In proving a statement is true, we sometimes have to examine multiple cases before showing the statement is true in all possible scenarios.

Example 8. *For any integer n, the number $(n^3 - n)$ is even.*

Solution: Since this proof is for *any* n, we could consider proving it for two cases: one where n is assumed to be odd and one where we assume that n is even. In both cases, the result should be true.

Case 1: n is even. Then $n = 2k$ for some integer k. Then we have:

$$n^3 - n = (2k)^3 - (2k) = 8k^3 - 2k = 2(4k^2 - k)$$

Since the right hand side is a *multiple of 2*, then regardless of k, the result is an *even* number. Thus $n^3 - n$ is even.

Case 2: n is odd. Then $n = 2k + 1$ for some integer k. This gives:

$$n^3 - n = (2k+1)^3 - (2k+1) = 8k^3 + 12k^2 + 6k + 1 - 2k - 1 = 2(4k^3 + 6k^2 + 2k)$$

where again we have a multiple of 2 on the right, and thus $n^3 - n$ is even.

After exhausting both cases, we conclude that $n^3 - n$ is always even.

Example 9. *Every collection of 6 people includes a set of 3 people who have* ***never*** *met each other, OR a set of 3 people who* ***all*** *know each other.*

Solution: Suppose that we consider one of the 6 people, call him "*Bob*". There are two cases:

Case 1: Of the remaining 5 people, there are at least 3 who **have** met Bob.

Case 2: Of the remaining 5 people, at least 3 have **not** met Bob.

These two cases exhaust the possibilities for the remaining 5 people.

Let's look at Case 1. There are at least 3 people who know Bob. Suppose they are called a, b, c. Then it is possible that those 3 people don't know *each other*. In which case, we have just found a group of 3 people who don't know each other, and the theorem is proved. Otherwise, of a, b, c there may be some pair that has met each other: suppose it was pair a, b. Then the set made up of a, b, Bob is a set of three people who all know each other. So in Case 1, we have found 3 people who either all know each other, or are all strangers.

Next let's look at Case 2. There are 3 people who have NOT met Bob. Call them d, e, f. Suppose those people d, e, f all know each other. Then we have found a set of 3 people who all know each other, and the theorem is proved. Otherwise suppose that some pair, say d, e don't know each other. Then the set d, e, Bob forms a group of 3 people who do not know each other, and again, the theorem is true.

After analyzing both cases, where in each case we have proved the theorem, we can say that the statement is true in all cases.

Example 10. *Prove that* $|x + y| \leq |x| + |y|$ *for all real numbers* x, y.

Solution: This problem involves the absolute value of x and y. Since the operation of taking the absolute value depends on whether or not the numbers are positive or negative, we need to consider all possible pairs of cases for the two numbers, x, and y. Thus there are 4 cases to analyze:

Case 1: Suppose that x, y are both positive. Then $|x+y| = x+y = |x|+|y|$. And thus the statement is actually an *equality* in this case. Nevertheless, we have shown that $|x + y| \leq |x| + |y|$.

Case 2: Suppose that $x = 0$. Then $|x + y| = |y|$ and $|x| + |y| = |y|$. So $|x + y| = |x| + |y|$, and the statement is also true (as an equality) in this case. The same argument works for when $y = 0$.

Case 3: Suppose that $x, y < 0$. Then $|x+y| = -x-y$ and $|x| = -x$ and $|y| = -y$. So $|x+y| = |x|+|y|$ and the statement is an equality in this case, and therefore true.

Case 4: Suppose that one is positive and one is negative: $x > 0$ and $y < 0$. Then the sum, $x+y$, might then be *zero*, it might be *positive*, or it might be *negative*. If the sum is zero, then $|x + y| = 0 \leq |x| + |y|$ and the result is true. If it is *positive*, then $|x+y| = x+y \leq |x|+|y|$ (by definition of the absolute values). And again, the result is true. Finally, if it is *negative* then $|x + y| = -(x + y) = -x - y$. Remember that $x > 0$ and $y < 0$, so $-x - y < x - y = |x| + |y|$ and we have shown that $|x + y| \leq |x| + |y|$. So in this case the statement is true. If the situation in case 4 were reversed, $(y > 0, x < 0)$, the argument would be identical.

2.2 If and only if statements

Many theorems assert that two statements are logically equivalent, and are read "*if and only if*". For example, "*A number is even* ***if and only if*** *its square is even*". Recall from the section on logic, that the operator $\iff$ is used to represent that two statements are equivalent, and it represents **both**: $P \to Q$ and $Q \to P$. For every proof of and if and only if, there are therefore **two steps** to the proof: first we prove $P \to Q$ and then we prove $Q \to P$.

Example 11. *Prove that if n is an integer, then 6 divides n if and only if 2 divides n and 3 divides n.*

Solution:

$\Rightarrow$: Here we assume that 6 divides n and we try to show that this implies 2 divides and 3 divides n. Note that if 6 divides n then we can write $n = 6k$ for some integer k. Thus $n = 2 \cdot 3 \cdot k$. So n is a multiple of 2 and a multiple of 3, and therefore both 2 and 3 divide n.

$\Leftarrow$: Here we assume that both 2 and 3 divide n, and we try to show that 6 divides n. Since 2 divides n, then $n = 2k$ for some k. And since 3 divides n, then $n = 3m$ for some other integer m. Now we have to find how to put this together. The trick is to find a way to combine the fact that $n = 3m$ and $n = 2k$. In order to do this, we need an expression that involves n *twice*. We notice that one can write n as:

$$n = 3n - 2n = 3(2k) - 2(3m) = 6k - 6m = 6(k - m)$$

The right hand side is a multiple of 6, and thus 6 divides n.

3 Proof by Contrapositive

In proving an implication, $P \to Q$, the direct proof starts with the premise P and continues with a sequence of deductions until it arrive at the conclusion (Q). In Example 1, we **assumed** n was even (P), and then **deduced** that n^2 was even (Q). However, sometimes assuming P is true gives us very little concrete information that we can work with, and it is difficult to move forward with a set of deductions, thus we end up in a dead end.

In this section, we introduce a new technique that is sometimes quite useful for proving implications, which is called a **proof by contraposition**. Recall from our lessons on propositional logic, we learned that $P \to Q$ is logically equivalent to $\neg Q \to \neg P$. Since they are equivalent, we could prove $\neg Q \to \neg P$, and in doing so, the statement $P \to Q$ would also be true. For example, here is a statement written in the original and the contrapositive:

Original: "*Every time it rains, I bring my umbrella*"

Contrapositive: "*If I don't bring my umbrella, it's not raining*"

If we prove the second statement above, then we have **also** proved the original statement. This is the idea behind a **contrapositive** proof: one assumes $\neg Q$ is true and works through deductions until we arrive at $\neg P$ as the conclusion. We will start with an example where a contrapositive proof is much simpler than the direct approach.

Example 12. *Prove that if $3n + 2$ is odd, then n is odd.*

Solution: If one were to attempt a direct proof, we would assume $3n + 2$ is odd, which is not so easy to work with directly. In the contrapositive approach, we assume $\neg Q$: n is *even*, and attempt to conclude $\neg P : 3n + 2$ is even. If n is even, then $n = 2k$. This is something that we can work with! We can plug this into: $3n + 2 = 6k + 2$, which is the sum of two even numbers, and thus is even. We have shown that $3n + 2$ is even and our proof by contraposition has succeeded: we have proved "*if $3n + 2$ is odd, then n is odd*".

Example 13. *Suppose $x \in \mathbb{Z}$. If $x + y$ is even, then x and y have the same parity.*

Solution: The contrapositive of the above statement is: "*If x and y have opposite parity, then $x + y$ is odd*". Having opposite parity means that one is even and one is odd. So if we assume x is even and y is odd, (the reverse situation would have the same proof), then $x = 2n$ and $y = 2m + 1$ for some integers

n and m. (Note than when you have 2 different numbers you need 2 different variables n, m). Thus $x + y = 2n + 2m + 1 = 2(n + m) + 1$, which is a multiple of two, plus one. The result is an odd number. Thus the contrapositive is true, and therefore the original statement is true.

Example 14. *If r is irrational, then $\sqrt{r}$ is also irrational.*

Solution: This is a perfect situation which demonstrates that assuming P (r is irrational) gives us little direct information to work with. The contrapositive statement is "*If $\sqrt{r}$ is rational, then r is rational*". Assuming $\sqrt{r}$ gives us something that we can work with directly: it allows us to conclude that there exist integers p, q, $q \neq 0$ such that

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

and thus

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

and now we have expressed r as a fraction of two integers, p^2 and q^2, thus r is rational. Thus we have proven $\neg P$: r is rational. The statement "*if r is irrational then $\sqrt{r}$ is irrational* is true by contraposition.

Example 15. *If a^2 is not divisible by 4, then a is odd.*

Solution: In a direct proof, knowing that a^2 is *not* divisible by 4 is cumbersome to work with. We would have to take all 3 cases that involve a number not being divisible by 4. In the contrapositive proof, we assume a is even (which is much easier to work with), and prove a^2 is divisible by 4. If a is even, then $a = 2k$ for some integer k. Then $a^2 = 4k^2$ which is a multiple of 4 and thus divisible by 4.

Example 16. *If $n = ab$ where a, b are both positive integers, prove that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.*

Solution: The statement in contrapositive form is: "*if $\neg(a \leq \sqrt{n}$ or $b \leq \sqrt{n})$ then $ab \neq n$*". Note that we need to use de Morgan's laws to negate the statement Q. In doing so, we have the following contrapositive statement: "*if $(a > \sqrt{n}$ and $b > \sqrt{n})$ then $ab \neq n$*". In this statement, we assume that both a and b are larger than $\sqrt{n}$. We can apply this information when we multiply them together:

$$ab > \sqrt{n} \cdot \sqrt{n} = n$$

and thus $ab > n$, which means that $ab \neq n$, and we have proven the contrapositive statement.

Example 17. *Suppose you have a collection of 5-cent stamps and 8-cent stamps.*

(a) Prove that if you made an even amount of postage, that you must have used an even number of at least one of the types of stamps.

(b) Next, suppose that you made exactly 72 cents of postage. Prove that you used at least 6 of one type of stamp.

Solution (a): The contrapositive statement is: "If you used an odd number of *both* types of stamps, then you made an odd amount of postage". Suppose you used n of the 8-cent stamps and m of the 5-cent stamps. Then the contrapositive statement tells us that n is odd, so $n = 2k + 1$ for some k. Similarly, m is odd: $m = 2l + 1$ for some integer l. Our total postage is then:

$$8n + 5m = 8(2k + 1) + 5(2l + 1) = 16k + 8 + 10l + 5 = 16k + 10l + 13 = 2(8k + 5l) + 13$$

which is an even number plus and odd number (the result is an odd number). Thus the amount of postage is odd, and we have proved the contrapositive.

Solution (b): The contrapositive statement is that if *both* $m < 6$ and $n < 6$, then you did *not* make 72 cents of postage. Note that if $m < 6$, then $m \leq 5$ since m is an integer. Similarly, $n \leq 5$. Thus our postage is:

$$5n + 8m \leq 25 + 40 = 65$$

and thus the postage is at most 65. Therefore it is *not* 72, and we have successfully proven the contrapositive.