CS/Math 240: Introduction to Discrete Mathematics Fall 2015

Reading 4 : Proofs

Instructors: Beck Hasti and Gautam Prakriya

Up until now, we have been introducing mathematical notation to capture concepts such as propositions, implications, predicates, and sets. We need this machinery in order to be able to argue properties of discrete structures in a rigorous manner. As we were introducing new concepts, we stated various facts and gave proofs of some of them, but we were not explicit about what a correct proof should look like. In this reading we start discussing what constitutes a valid proof of a proposition and give some guidelines for writing proofs.

4.1 Proofs

We briefly mentioned what proofs were in the second reading. Let's repeat some of this discussion, and make our definition of a proof more precise.

Definition 4.1. *A* proof *of a proposition P is a chain of logical deductions ending in P and starting from some set of axioms.*

Our definition of a proof mentions axioms and logical deductions, both of which require further consideration. Let's discuss them one by one.

4.1.1 Axioms

Axioms are statements we take for granted and do not prove. The set of axioms we use depends on the area we work in. For geometry, we would use Euclid's five axioms of geometry. Another set of axioms are the ZFC axioms (the abbreviation stands for Zermelo, Fraenkel, and the axiom of Choice) which form the basis of all set theory. However, both of these sets of axioms are small and proving any substantial result starting just from those axioms requires a significant amount of work. Thus, such sets of axioms are more suitable for a course on logic than a course on discrete structures. In this course, we use a much larger set of axioms because our focus is on proof techniques and their applications to discrete structures. Thus, we will consider any familiar fact from math at the level of high school as an axiom. If you are unsure whether you can take something for granted on an assignment, just ask.

4.1.2 Logical Deductions

Logical deductions, which are sometimes called *inference rules*, tell us how to construct proofs of propositions out of axioms and other proofs. One example of an inference rule is *modus ponens*, which says that if we have a proof of P and a proof of $P \Rightarrow Q$, then we also have a proof of Q.

We now define some terminology and notation for describing inference rules. An inference rule consists of *antecedents* and a *conclusion*. Antecedents, also known as *premises*, are axioms or other proofs. If all the antecedents are true, the inference rule says that we have a proof of the conclusion. We sometimes also use the word *consequence* instead of the word conclusion. We illustrate this terminology on the example of modus ponens.

Example 4.1: Modus ponens deals with two statements, P and Q. The antecedents are P and $P \Rightarrow Q$, and the conclusion is Q. ⊠

To describe inference rules in a more compact way, we draw a horizontal line, place all antecedents above the horizontal line (either on the same line or on multiple lines), and write the conclusion below the horizontal line. In Figure 4.1a we show the notation for a general inference rule with antecedents $P_1, P_2, \ldots, P_k$ and conclusion Q, and we give two ways of writing modus ponens in Figures 4.1b and 4.1c.

$$\frac{P_1 \; P_2 \; \ldots P_k}{Q} \qquad \frac{P \; P \Rightarrow Q}{Q} \qquad \frac{\begin{array}{c} P \\ P \Rightarrow Q \end{array}}{Q}$$

(a) General case (b) Modus ponens using one line (c) Modus ponens using two lines

Figure 4.1: Notation for logical inference rules

4.2 Proof Techniques

In a proof, we apply logical deductions in order to reach the proposition we are proving from a set of axioms. We will not attempt to turn every logical step into the form of Figure 4.1 in this course, and will write proofs at a higher level.

We now present some proof techniques. We have seen examples of some of proofs already, but some of the proofs were too complicated to serve as examples illustrating the proof techniques. Below, we present proofs of simpler statements in order to highlight the proof techniques used.

4.2.1 Proofs "By Picture"

A common approach to constructing proofs is to capture a proposition using descriptive pictures and then reason about the pictures. This is a very powerful technique as it allows us to use our intuition. However, be warned that in some cases our intuition may lead us astray.

We now present a proof of the Pythagorean Theorem.

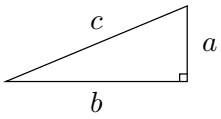


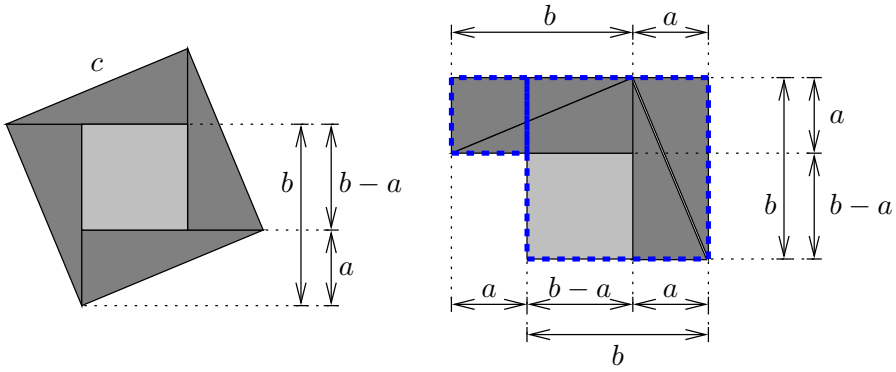
Figure 4.2: A right triangle with sides of length a, b, and c

Proposition 4.2 (Pythagorean Theorem)**.** *In a right triangle where the hypotenuse has length c and the other two sides have lengths a and b, we have $a^2 + b^2 = c^2$.*

Proof. Consider a right triangle like the one in Figure 4.2. We take four copies of the triangle and arrange them in two different ways.

First, form a square with the hypotenuse as the side. Its area is c^2. We show this arrangement in Figure 4.3a. The four copies of the right triangle are shaded in dark gray. The space shaded light gray inside the square in Figure 4.3a is a square of side length $b - a$.

Now rearrange the five pieces differently, as shown in Figure 4.3b. The thick blue lines indicate that we can view this arrangement as two squares of sides a and b placed next to each other. The square on the right has length is b, so the area of that square is b^2. The square on the left has side length a, so its area is a^2, and the total area is, therefore, $a^2 + b^2$.



(a) An arrangement of four copies of the right triangle from Figure 4.2. There is a square in the middle.

(b) A rearrangement of Figure 4.3a.

Figure 4.3: Two arrangements of four triangles and a square.

Since we obtained the second picture from the first one by rearranging, they have the same area, which completes the proof that $a^2 + b^2 = c^2$. □

The use of Venn diagrams to prove properties of sets is another example of a proof "by picture".

While such proofs are often very appealing, they don't constitute a valid proof in mathematics. Pictures are typically used only to aid our intuition.

4.2.2 Proving Implications

We now consider statements of the form $P \Rightarrow Q$, and look at two approaches to constructing proofs of such statements

4.2.2.1 Direct Proof

In order to prove the implication $P \Rightarrow Q$ using a direct proof, we take the following three steps.

Step 1: Assume that P holds. We usually write this as the first sentence in the proof.

Step 2: Logically derive Q from P.

Step 3: Say that Q holds. This is usually the last sentence in the proof.

As an example, we prove the statement that if an integer is odd, then so is its square. We state it as Theorem 4.3.

Theorem 4.3. $(\forall x \in \mathbb{Z})$ *x is odd* $\Rightarrow$ *x^2 is odd.*

The statements P and Q for the implication in Theorem 4.3 are P: "x is odd" and "Q: x^2 is odd".

Note that the implication is universally quantified. Whenever we prove a universally quantified statement, we have to prove it for every x in the domain. In our case, we have to prove the implication $P \Rightarrow Q$ for every integer x. It does not suffice to prove, say, that if 3 is odd, then 9 is odd. We cannot make any assumption about x besides the fact that it's odd.

For the purposes of presentation, we label where the three steps outlined earlier in the margin.

Proof of Theorem 4.3.

Step 1 Let x be an integer, and assume that x is odd.

Step 2 Since x is odd, we can write x as $x = 2y + 1$ for some $y \in \mathbb{Z}$. In particular, $y = \frac{x-1}{2}$. Then $x^2 = (2y+1)^2 = 4y^2 + 4y + 1 = 2(2y^2 + 2y) + 1$. Since y is an integer, so is $2y^2 + 2y$, which means that $x^2 = 2z + 1$ for some $z \in \mathbb{Z}$.

Step 3 Therefore, x^2 is odd. □

We usually highlight the end of the proof in some way. In the proof above, we used a square in the lower right corner at the end of the last paragraph. Another common way to end a proof is to write Q.E.D. This comes from Latin "quod erat demonstrandum", which means "which is what had to be shown".

4.2.2.2 Indirect Proof

In an indirect proof of the implication $P \Rightarrow Q$, we prove the contrapositive implication $\neg Q \Rightarrow \neg P$. Since the contrapositive of an implication is logically equivalent to the original implication, proving the contrapositive also proves the original implication. We outline the steps in an indirect proof below.

Step 1: Say that we use an indirect proof, and state the contrapositive of the implication we are proving.

Step 2: Use a proof technique of our choice to prove the contrapositive.

Step 3: Conclude that the original implication is proved.

The inference rule for an indirect proof is

$$\frac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q}.$$

We often use an indirect proof if the implication we want to prove contains negations. For such implications, an indirect proof is a natural way to go because taking the contrapositive removes negations from the statement of the implication. We demonstrate this technique on the proof of the statement which says that if a positive real number is not rational, its square root is not rational either. Notice that we use a direct proof to prove the contrapositive in this example.

Theorem 4.4. $(\forall x \in \mathbb{R}^+) x \notin \mathbb{Q} \Rightarrow \sqrt{x} \notin \mathbb{Q}$.

Again, we highlight the steps we mentioned earlier in the margin.

Proof.

Step 1 We prove the contrapositive of our statement, that is, we show that if $\sqrt{x}$ is rational, then so is x.

Step 2 We use a direct proof to prove the contrapositive.

Let x be a positive real number, and assume that $\sqrt{x} \in \mathbb{Q}$. Then

$$\sqrt{x} = \frac{a}{b} \qquad \text{for some} \quad a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0. \tag{4.1}$$

Taking the square of both sides of (4.1) yields $x = (a/b)^2$. Now $(\sqrt{x})^2 = x$ and $(a/b)^2 = a^2/b^2$, so $x = a^2/b^2$. Since a is an integer, so is a^2, and since b is a positive integer, so is b^2, which means that x is a rational number.

Step 3 It follows that if $x \notin \mathbb{Q}$, then $\sqrt{x} \notin \mathbb{Q}$. □

4.2.3 Proving Equivalences

Recall that an equivalence is a statement of the form $P \iff Q$.

4.2.3.1 Proving Two Implications

One way to rewrite an equivalence $P \iff Q$ is $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Thus, if both implications hold, then so does the equivalence. Thus, to prove an equivalence is true, we can take the following steps

Step 1: State that we prove two equivalences

Step 2: Prove the implication $P \Rightarrow Q$ using a proof technique of your choice. Make sure you state your choice of proof technique.

Step 3: Prove the implication $Q \Rightarrow P$ using a proof technique of your choice.

Step 4: In the conclusion, state what you proved.

The inference rule for this kind of proof is

$$\frac{P \Rightarrow Q \quad Q \Rightarrow P}{P \iff Q}.$$

As an example, we prove another relationship between an integer and its square. As will be apparent from the proof, Theorem 4.5 is a strengthening of Theorem 4.3.

Theorem 4.5. $(\forall x \in \mathbb{Z})$ *x is even $\iff$ x^2 is even.*

Proof.

Step 1 Let $x \in \mathbb{Z}$. We prove the equivalence "x is even $\iff$ x^2 is even" by proving the implications "x is even $\Rightarrow$ x^2 is even" and "x^2 is even $\Rightarrow$ x is even".

Step 2 We first prove that if x is even, then so is x^2. We do so by a direct proof.

If x is even, we can write $x = 2y$ for some $y \in \mathbb{Z}$. By squaring both sides, we get $x^2 = (2y)^2 = 4y^2 = 2(2y^2)$. Now $2y^2$ is an integer, which means that x^2 is even.

Step 3 Next, we prove that if x^2 is even, then so is x. We prove this using an indirect proof.

Observe that the statement "if x^2 is even, then so is x" is the contrapositive of Theorem 4.3. Recall that Theorem 4.3 says that if x is odd, then so is x^2. Its contrapositive says that if x^2 is not odd, then x is not odd. But this is equivalent to saying that if x^2 is even, then so is x, which is what we wanted to show.

Step 4 It follows that x is even if and only if x^2 is even. □

The proof of Theorem 4.5 uses a theorem we proved earlier. Using theorems to prove other theorems is common practice. The programming analog of this is calling a function instead of writing all the code for that function again from scratch. It makes no sense to reprove a fact that has already been proved, just like it makes no sense to rewrite a function that is provided to us. Of course, there are exceptions to this rule, such as if we want to prove a slightly different fact or if we want to override some function in a subclass, but in general, we should attempt to use existing work before we "reinvent the wheel".

4.2.3.2 Chains of Equivalences

Another way to prove that the equivalence $P \iff Q$ is true is to demonstrate a sequence of statements $P_1, P_2, \ldots, P_k$ such that P is P_1, $P_1 \iff P_2$, $\ldots$, $P_{k-1} \iff P_k$, and P_k is Q. Formally, the inference rule is

$$\frac{P_1 \iff P_2 \quad P_2 \iff P_3 \quad \cdots \quad P_{k-1} \iff P_k}{P_1 \iff P_k}.$$

When we prove an equivalence by proving two implications, we argue $P \Rightarrow Q$ and $Q \Rightarrow P$ separately. But if all steps in the proof are equivalences and not just implications, we prove $P \Rightarrow Q$ and $Q \Rightarrow P$ at the same time.

As an example of this proof technique, we prove a relationship between even and odd numbers.

Theorem 4.6. $(\forall x \in \mathbb{Z})$ x^2 *is even* $\iff$ $(x+1)^2$ *is odd.*

Proof. Pick $x \in \mathbb{Z}$. We prove the equivalence "x^2 is even $\iff$ $(x+1)^2$ is odd" by constructing a chain of equivalences.

We know by Theorem 4.5 than x^2 is even if and only if x is even. The latter is true if and only if $x+1$ is odd. Note that Theorem 4.5 also tells us that x^2 is odd if and only if x is odd. Therefore, using $x+1$ instead of x in our alternative formulation of Theorem 4.5, we see that $x+1$ is odd if and only if $(x+1)^2$ is odd.

Thus, we have shown that x^2 is even if and only if $(x+1)^2$ is odd. □

4.2.4 Proof by Contradiction

The last two sections discussed proof techniques that apply to proving specific kinds of statements. With this section, we move towards more general proof techniques.

In order to prove a statement P by contradiction, we assume that P is false, and show that this assumption leads to a false statement. The inference rule for a proof by contradiction is

$$\frac{\neg P \Rightarrow \text{false}}{P}.$$

At a first sight, an argument by contradiction looks strange because the reasoning happens in an "absurd world" where we assume a false statement. Therefore, such proofs are less intuitive, and you should avoid them as much as possible. It is often possible to rewrite a proof by contradiction as a direct proof or an indirect proof. In some cases, however, proof by contradiction is the only possibility.

We saw an example of a proof by contradiction in the reading on sets where we showed that the power set of the natural numbers is not countable. In this reading we prove a simpler statement. We also use the next proof to show how to label equations. Labeling some of our equations with numbers or other symbols makes it easy to refer to them later without writing long English sentences.

Theorem 4.7. $\sqrt{2} \notin \mathbb{Q}$.

Proof. We give a proof by contradiction.

Assume that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ for some $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b \neq 0$.

We first rewrite a/b so that the numerator and the denominator share no common factors. Let $\gcd(a, b)$ be the greatest common divisor of a and b, and define $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$.

Note that $a/b = a'/b'$ because dividing the numerator and the denominator of a fraction by the same number doesn't change the value of the fraction. We now have

$$\sqrt{2} = \frac{a'}{b'} \quad \text{where} \quad \gcd(a', b') = 1. \tag{4.2}$$

By squaring (4.2), we get $2 = (a'/b')^2 = (a')^2/(b')^2$, so

$$2(b')^2 = (a')^2. \tag{4.3}$$

Therefore, $(a')^2$ is even, which implies that a' is even by Theorem 4.5. Hence, we can write

$$a' = 2c, c \in \mathbb{Z}. \tag{4.4}$$

Substituting (4.4) into (4.3) tells us that $2(b')^2 = (2c)^2 = 4c^2$, so $(b')^2 = 2c^2$. It follows that $(b')^2$ is even. By Theorem 4.5, this means that b' is even.

We have shown that a' and b' are both even, which means that 2 is a common divisor of a' and b'. This is a contradiction with the fact that $\gcd(a', b') = 1$, so the statement that 2 is a common divisor of a' and b' is false. What led to this contradiction was the assumption that $\sqrt{2} \in \mathbb{Q}$, so this assumption is false. Therefore, the opposite of our assumption is true, and we have $\sqrt{2} \notin \mathbb{Q}$, which is what we wanted to show. □

4.2.5 Proof by Cases

Another technique that is generally applicable is proving a statement by cases. We have actually used this technique already, but did not state it explicitly. Proving logical equivalence of propositional formulas by truth tables is a proof by cases in which every row of the truth table corresponds to one case.

In a proof of a proposition P by cases, we come up with a set of conditions $C_1, C_2, \ldots, C_k$ such that every one of them implies P, and where we are guaranteed in any situation that at least one of these conditions is true. Formally, we have the following inference rule:

$$\frac{(C_1 \vee C_2 \vee \cdots \vee C_k) \;\; C_1 \Rightarrow P \;\; C_2 \Rightarrow P \;\; \cdots \;\; C_k \Rightarrow P}{P}.$$

We give an example of this proof technique by proving an elementary fact about graphs.

Theorem 4.8. *Every group of* 6 *people contains a subgroup of* 3 *people who are mutual acquaintances or a subgroup of* 3 *people who are mutual strangers.*

Proof. Let Alice be one of the people. Consider two cases.

Case 1. Suppose that Alice knows at least three people from the group. We have two subcases in this situation.

Case 1.1. Suppose that among Alice's acquaintances, there are at least two people who know each other. Then Alice and those two people are all mutual acquaintances.

Case 1.2. Now suppose that no acquaintance of Alice knows anybody else who knows Alice. In that case, any group of 3 of Alice's acquaintances is a group of mutual strangers.

Since either there is a pair of Alice's acquaintances who know each other (case 1.1), or there isn't one (case 1.2), we have shown that if Alice has at least three acquaintances, then the group contains a subgroup of three mutual acquaintances or a subgroup of three mutual strangers. This completes the proof for case 1.

Case 2. Now suppose that Alice knows at most two people from the group. We have two cases in this situation.

Case 2.1. Suppose that among people Alice doesn't know, there are at least two people who don't know each other. Then Alice and those two people are all mutual strangers.

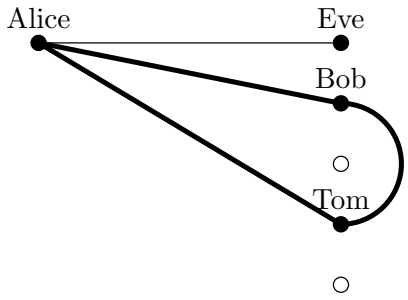
Case 2.2. Now suppose that all people not known by Alice know each other. In that case, any group of 3 such people is a group of mutual acquaintances.

Since either there is a pair of people not known by Alice who also don't know each other (case 2.1), or all people not known by Alice know each other (case 2.2), we have shown that if Alice has at most two acquaintances, then the group contains a subgroup of three mutual acquaintances or a subgroup of three mutual strangers. This completes the proof for case 2.

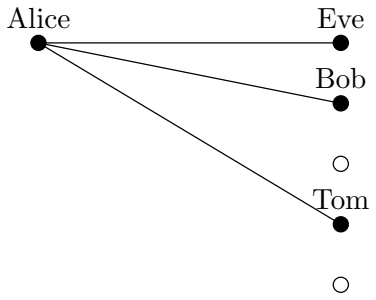
Finally, since Alice either has at least three (Case 1) or at most two (Case 2) acquaintances, we have shown that the group contains a subgroup of three mutual acquaintances or a subgroup of three mutual strangers. □

Observe that the proof for Case 2 is the same as the proof for Case 1, except the roles of the words "acquaintance" and "stranger" are switched.

We mentioned that Theorem 4.8 was a statement about graphs, yet we did not use any graph terminology in the theorem or its proof. Here is the connection. Represent the six people as vertices in a graph. There is an edge connecting two vertices if the people those vertices correspond to know each other. Now Alice is one vertex in the graph, and is connected to some number of vertices by edges. In Case 1, there area at least 3 edges connecting Alice to other vertices. Furthermore, in Case 1.1, there is at least one edge between vertices representing people who know Alice, and in Case 1.2 there are no such edges. We show these two cases in Figures 4.4a and 4.4b.



(a) Case 1.1: Some pair of Alice's acquaintances know each other. The three thick lines show that Alice, Bob and Paul are mutual acquaintances.



(b) Case 1.2: No pair of Alice's acquaintances know each other. There are no edges between the vertices labeled Eve, Bob and Tom, which means that those three people are mutual strangers.

Figure 4.4: Graphs representing Case 1 in the proof of Theorem 4.8.