COMPSCI 230: Discrete Mathematics for Computer Science January 9, 2019

Lecture 1

Lecturer: Debmalya Panigrahi *Scribe: Kevin Sun*

1 Overview

The primary goal of the first few lectures is to give an overview of mathematical proofs, namely, what they entail and how we generally write them. In this lecture, we will examine the fundamental notions associated with mathematical proofs and explore various techniques for writing proofs.

2 Propositions and Predicates

Before we can begin writing proofs, we must first understand what proofs are. In different areas (e.g., mathematics, philosophy, physics), proofs mean different things; in this class, we will solely consider proofs in a mathematical context.

2.1 Propositions

The goal of every mathematical proof is to demonstrate the truth value of a statement known as a proposition, so understanding the notion of propositions is essential to understanding proofs.

Definition 1. *A* proposition *is a statement that is either true or false.*

For example, the statement "$1 + 2 = 3$" is a true proposition, while the statement "$2 + 2 = 5$" is a false proposition. The statement "It will rain tomorrow" is *not* a proposition, because its truth value depends on unknown circumstances. We are often interested in propositions whose truth value is fixed but difficult to determine; we now give some examples.

Example 1: Consider the following proposition: for every positive integer n, the number $n^2 + n + 1$ is prime. How can we determine its truth value? One way is to simply test the statement for different values of n. For $n = 1, 2, 3$, this statement is easily verified, but for $n = 4$, we have $n^2 + n + 1 = 4^2 + 4 + 1 = 21$, which is not prime. Since 4 is a positive integer yet 21 is not prime, we can conclude that the proposition is false.

In the above example, $n = 4$ is a *counterexample* to the proposition. In general, providing a counterexample is one way to prove that any proposition is false. However, this method does not allow us to show that a true statement is indeed true. Furthermore, finding counterexamples can often be difficult, as we will see.

Example 2: Consider the following proposition: for every positive integer n, the number $n^2 + n + 41$ is prime. Again, we can try to determine its truth value by testing the statement for different values of n. In this case, the statement is true for $n = 1, 2, 3, \ldots, 39$. However, if we examine the case $n = 40$, we notice the following:

$$n^2 + n + 41 = 40^2 + 40 + 41 = 40 \cdot (40 + 1) + 41 = 40 \cdot 41 + 41 = (40 + 1) \cdot 41,$$

which is clearly divisible by 41, and hence, not prime.

Example 3: The following proposition is known as *Euler's conjecture*, proposed by the great mathematician Leonhard Euler in 1769: For all integers k and n greater than 1, if there exist $n+1$ positive integers $a_1, a_2, \ldots, a_n, b$ such that $a_1^k + a_2^k + \cdots + a_n^k = b^k$, then $k \leq n$.

This statement is a little difficult to parse, so let us first consider the case where $k = n = 2$. We can indeed find positive integers a_1, a_2, b such that $a_1^2 + a_2^2 = b^2$; any Pythagorean triple will do. Now if $k = 1$ and $n = 2$, then it is very trivial to find positive integers a_1, a_2, b such that $a_1^1 + a_2^1 = b^1$. The statement is saying that if $k > n$, then we will no longer be able to find $n+1$ positive integers such that the inequality holds (because if we did, that would mean $k \leq n$).

Euler's conjecture was disproved in 1986 by Noam Elkies, who gave the following counterexample: $n = 3, k = 4, a_1 = 95800, a_2, = 217519, a_3 = 414560, b = 422481$. It is by no means obvious, but it is indeed the case that

$$95800^4 + 217519^4 + 414560^4 = 411481^4,$$

yet here we have $k > n$, so the conjecture is false. This is another example that shows how difficult it can be to find even one counterexample to a proposition; this one took mathematicians over 200 years to find!

Example 4: Euler's conjecture, given in Example 2.1, is a generalization of the following proposition proposed by Pierre de Fermat in 1637: for any integer $k \geq 1$, if there exist positive integers a_1, a_2, b such that $a_1^k + a_2^k = b^k$, then $k \leq 2$. This proposition is one of the most notable statements in all of mathematics, and is known as *Fermat's Last Theorem*. Unlike Euler's conjecture, Fermat's Last Theorem is true. The first complete proof was given by Andrew Wiles in 1995, over 300 years after the proposition was proposed, and involved many advanced techniques in mathematics. This example shows that proofs, like counterexamples, can also be very elusive.

2.2 Predicates

Predicates are special kinds of propositions that we often consider when writing mathematical proofs. In this section, we will look at examples of predicates that are always true, sometimes true, and never true.

Definition 2. *A* predicate *is a proposition whose truth value depends on the value of certain parameters (also known as arguments or variables).*

Example 1: Suppose $P(n) = n^2 + n + 1$. The following is a predicate: "$P(n)$ is prime." As we can see, the truth value of this predicate depends on the value of n: some values of n (e.g., 1, 2, 3) make the predicate true, while others (e.g., 4) make the predicate false.

Example 2: Suppose $P(n) = n^2 + 2n + 1$ and consider the following predicate: "$P(n)$ is a square number." This predicate is always true, regardless of the value of n, because $n^2 + 2n + 1 = (n+1)^2$, so $P(n)$ can be written as $(n+1)^2$, which is clearly a square number.

We now take the opportunity to introduce some notation. Again, suppose $P(n) = n^2 + 2n + 1$ and consider the predicate "$P(n)$ is a square number." Since this statement is true for all values of n, we can write the following proposition:

$$\forall n : P(n) \text{ is a square number.} \tag{1}$$

Here, the "$\forall$" symbol represents "for all", and the ":" represents "such that". Statement (1) is a proposition, not a predicate, because its truth value is fixed: it is either the case that $n^2 + 2n + 1$ is a square number for every value of n, or it is not the case.

Example 3: Suppose $P(n) = n^2 + n + 1$ and consider the predicate "$P(n)$ is a square number." Unlike the previous two example predicates, this predicate is always false. We can see this by noticing that in order for $P(n)$ to be a perfect square, it must be equal to m^2 for some integer m. Clearly, setting $m = n$ cannot work because $n^2 < n^2 + n + 1$, but setting $m = n + 1$ does not work either because $n^2 + n + 1 < (n + 1)^2$. Since there are no integers bigger than n *and* smaller than $n + 1$, we can conclude that the predicate is always false.

We conclude with some more notation. Suppose $P(n) = n^2 + 7n + 1$ and consider the predicate "$P(n)$ is a square number." We see that for $n = 1$ the predicate is true, but for $n = 2$, the predicate is false. Since the predicate is not true for all values of n, the proposition shown in (1) is false. However, since the predicate is true for at least one value of n, the following proposition is true:

$$\exists n : P(n) \text{ is a square number.}$$

Here, the "$\exists$" symbol represents "there exists".

3 What is a Proof?

Now that we understand the notion of propositions and predicates, we can begin discussing proofs. The idea behind proofs was invented by the mathematician Euclid in Alexandria, Egypt around 300 BC. This system is known as the *axiomatic method*, and can be summarized as follows:

1. We start with a set of statements known as *axioms*. An axiom is a basic statement that is simply accepted as true.
2. We apply *logical deduction rules* to the axioms, and the resulting statements, until we arrive at the proposition we wish to prove.

Propositions that have been proven are often called lemmas, theorems, or corollaries. A *lemma* is a preliminary proposition useful for proving other propositions, a *theorem* is an important proposition, and a *corollary* is a proposition that follows in just a few logical steps from a theorem. These definitions are not precise, but mathematicians often use these terms to organize the structure of proofs and mathematical information.

3.1 Axioms

Given the axiomatic method, perhaps the first question one might ask is the following: which statements are we allowed to use as axioms? For the purposes of essentially all of mathematics, a set of axioms known as the *Zermelo-Fraenkel with Choice* (ZFC) axioms is used in present day mathematics.

Prior to the introduction of ZFC, Georg Cantor proposed a set-theory-based axiomatic system to lay the foundation of mathematics in the late 19th century. Cantor's basic axiom was that a set is a collection of objects. But in 1901, Bertrand Russell discovered a paradox, now known as Russell's

paradox, that arises due to this definition: let R be the set of all sets that do not contain themselves. (After all, a set is simply of collection of objects, so it is possible for one of these objects to be the set itself.) The paradox arises when we ask the following: is R a member of itself?

To avoid this paradox, Ernst Zermelo proposed a set of axioms that eventually evolved to ZFC. Understanding the contents of these axioms is beyond the scope of this course; for our purposes, we can essentially consider anything we've ever learned in a math class as an axiom.

3.2 Logical Deduction Rules

Now that we've explained the set of axioms that most mathematicians use, let's see examples of logical deduction rules. Recall that a proof is essentially repeated applications of these rules until the desired proposition is reached. Here, we let P, Q, and R denote three propositions. We also let the " $\implies$ " symbol represent the word "implies", and the "$\neg$" symbol denote "not". (The truth value of the proposition $\neg P$ is the opposite of that of the P.)

Example 1:

$$\frac{P, \quad P \implies Q}{Q}$$

This rule simply states that a proof of P together with a proof of the proposition "$P \implies Q$" is a proof of Q. This rule is formally known as *modus ponens*. Intuitively, this rule seems obvious, but as we shall see in this course, these rules constitute the essence of mathematical proofs.

The statements above the line are known as *antecedents*, and the statement below the line is known as the *conclusion* or *consequent*. In general, a logical deduction rule tells us that when the antecedents have been proven, then so has the consequent.

Example 2:

$$\frac{P \implies Q, \quad Q \implies R}{P \implies R}$$

This rule is known as the *chain rule*.

Example 3:

$$\frac{\neg P \implies \neg Q}{Q \implies P}$$

This rule illustrates the notion of a *contrapositive*: the contrapositive of a proposition of the form "$A \implies B$" is "$\neg B \implies \neg A$" and is logically equivalent to the original proposition (that is, their truth values are the same regardless of the truth values of A and B). Note that the above explanation of Euler's conjecture involved the contrapositive of the proposed statement.

Each example given above is a logical deduction rule that is *sound*, that is, any assignment of truth values to P, Q, R that makes all the antecedents true must also make the consequent true. The following rule is not sound:

$$\frac{\neg P \implies \neg Q}{P \implies Q}$$

because if P is true and Q is false, then the antecedent is true but the consequent is false. We will further explore this concept in later lectures, when we discuss propositional logic in more detail.

3.3 Proof Patterns

Now that we've seen the essential ingredients of proofs (axioms and logical deduction rules), we can finally examine some general patterns for proofs. Although every proof has its own details to consider, many proofs follow one of just a handful of general patterns.

As mentioned earlier, 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. For example, the first example of Section 2.1 can be written as "If n is a positive integer, then $n^2 + n + 1$ is prime." 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:

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.

A direct proof: 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. This means n is either 1 or 2, but 1 is not divisible by 2, so n must be equal to 2, as desired.

Proving the contrapositive: 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, it would be enough for us to prove the contrapositive.

After stating the contrapositive, we then prove it by giving a direct proof (as we did in the previous pattern). In this case, to begin writing the direct proof, we start by assuming $n \neq 2$. 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. However, $n \neq 2$ so n must be greater than 2. But any number greater than 2 that is divisible by 2 cannot be 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. For now, the objective is to become familiar with the structure and appearance of proofs.

4 Summary

In this lecture, we saw the fundamental notions of proofs, namely propositions, predicates, axioms, and logical deduction rules. We gave examples of each of these concepts, as well as proof patterns that illustrate the general structure of proofs.