Lecture 3: Logic and Proofs

September 1, 2026

Lecturer and scribe: Karthik Gajulapalli

1 From Observations to Proofs

In physics, observations help us formulate hypotheses. We test these hypotheses by comparing their predictions with further observations. A new experiment can give us a reason to revise a theory.

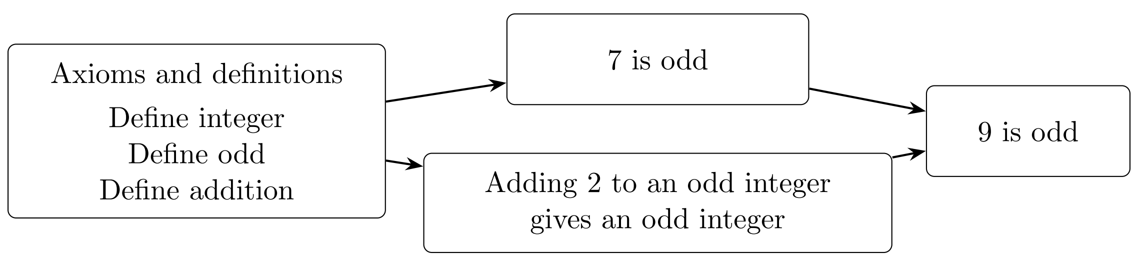
In mathematics, we begin with assumptions and definitions, and use logic to derive conclusions. A **proof** explains why a conclusion must follow from those starting points. For example, using the Peano axioms and the usual definitions of arithmetic, we can prove:

> If seven is odd, then nine is odd.

No future observation can invalidate a correct proof of this statement under the same assumptions and definitions.

1.1 How Statements Depend on One Another

We can picture a proof as a network of statements: axioms and definitions support intermediate results, which support further conclusions. Here is one possible argument that nine is odd:



An arrow records a dependency in the proof. Here the two intermediate statements are used *together* to prove that nine is odd.

This is a **directed acyclic graph**:[1] its arrows have a direction and form no cycles. A proof cannot use its own conclusion to justify itself. The diagram shows only the dependencies used in this particular proof.

[1]We will study more about graphs later in this class.

2 Implication: "If P, Then Q"

A **proposition** is a statement that is either true or false. We use letters such as P and Q to stand for propositions. Our main tool for expressing a mathematical claim is the **implication**

$$P \Rightarrow Q,$$

read as "if P, then Q." We call P the **hypothesis** and Q the **conclusion**. The implication says that whenever P is true, Q must also be true.

2.1 When Is an Implication True?

There is exactly one way for $P \Rightarrow Q$ to be false: P is true but Q is false. That is a **counterexample** to the implication. The truth table is therefore:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Here T and F mean true and false, respectively; they play the same roles as 1 and 0 in our Boolean truth tables from Lecture 2.

When P is false, the implication is **vacuously true**, regardless of the value of Q. The statement only makes a requirement when P holds. If P does not hold, there is no violation of that requirement.

For example, consider these statements about ordinary pigs and the Moon:

- *If* 9 *is even, then the Moon is made of cheese.* The hypothesis and conclusion are both false, so this is a true implication of the form F $\Rightarrow$ F.
- *If pigs can fly, then pigs can oink.* The hypothesis is false and the conclusion is true, so this is a true implication of the form F $\Rightarrow$ T.

These examples sound strange because an implication in logic does not assert a causal connection between its two parts. In particular, a vacuously true implication does not tell us that its conclusion is true. To infer Q from $P \Rightarrow Q$, we also need to know that P is true.

2.2 Writing Implication Using NOT and OR

Recall our method from Lecture 2: to write a Boolean function in **disjunctive normal form (DNF)**, write one AND term for each row where the output is true, and then OR those terms together.

The three true rows of the implication table give

$$(P \Rightarrow Q) \;\equiv\; (P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q).$$

The symbol $\equiv$ means **logical equivalence**: both expressions have the same truth value for every choice of truth values for P and Q. Now apply the Boolean algebra laws from Lecture 2:

$$\begin{aligned}
(P \Rightarrow Q) &\equiv (P \wedge Q) \vee \big(\neg P \wedge (Q \vee \neg Q)\big) && \text{(distributivity)}\\
&\equiv (P \wedge Q) \vee \neg P && \text{(complement, identity)}\\
&\equiv \neg P \vee (P \wedge Q) && \text{(commutativity)}\\
&\equiv (\neg P \vee P) \wedge (\neg P \vee Q) && \text{(distributivity)}\\
&\equiv \neg P \vee Q && \text{(complement, identity).}
\end{aligned}$$

Thus

$$\boxed{(P \Rightarrow Q) \;\equiv\; \neg P \vee Q.}$$

This identity will explain several different ways to prove an implication.

3 Direct Proof

To prove $P \Rightarrow Q$ **directly**, assume that P is true and use definitions and previously established facts to show that Q follows. We do not need to prove P as part of this argument: our task is to show what follows *if* P holds.

The background axioms remain available throughout the proof. We add P as a temporary hypothesis and derive Q from these assumptions together:

$$\boxed{\text{Axioms}} \qquad + \qquad P \qquad \Longrightarrow \qquad Q$$

Here + means “together with.” We may also use definitions and results already proved from the axioms.

3.1 Arithmetic Conventions

The **integers** are zero, the positive whole numbers, and their negatives.

For the examples below, we use the usual arithmetic laws for integers, such as distributivity. We will not derive all of these laws from the Peano axioms in this lecture. An integer n is:

- **even** if $n = 2k$ for some integer k;
- **odd** if $n = 2k + 1$ for some integer k.

We also use the basic arithmetic fact that every integer is exactly one of even or odd. Thus, for an integer, "not odd" means even, and "not even" means odd. Throughout our proofs, we also use the fact that the integers are closed under addition and multiplication: adding or multiplying two integers yields another integer.

Two integers have **the same parity** if they are both even or both odd. They have **different parities** if one is even and the other is odd.

Claim 1. *If seven is odd, then nine is odd.*

Direct proof. Assume that seven is odd. By the definition of odd, there is an integer k such that $7 = 2k + 1$. Then

$$9 = 7 + 2 = (2k + 1) + 2 = 2(k + 1) + 1.$$

Since $k + 1$ is an integer, this expresses 9 as twice an integer plus one. Therefore, nine is odd. □

The same argument proves a more general statement: adding 2 to any odd integer gives an odd integer. We use the familiar numbers 7 and 9 here to compare the structures of several proof methods.

4 Proof by Contrapositive

Starting with our identity for implication and using commutativity of OR, we obtain

$$(P \Rightarrow Q) \;\equiv\; \neg P \vee Q \;\equiv\; Q \vee \neg P \;\equiv\; (\neg Q \Rightarrow \neg P).$$

For the last step, write $\neg Q \Rightarrow \neg P$ in its NOT–OR form and use double negation: $\neg(\neg Q) \vee \neg P \equiv Q \vee \neg P$.

We call $\neg Q \Rightarrow \neg P$ the **contrapositive** of $P \Rightarrow Q$. Since they are logically equivalent, we can prove $P \Rightarrow Q$ by assuming that Q is false and showing that P must be false as well.

4.1 Claim 1 by Contrapositive

The contrapositive of Claim 1 is:

> If nine is not odd, then seven is not odd.

Here the hypothesis happens to be false. A conditional proof examines what would follow if the hypothesis held; temporarily assuming it does not assert that nine is actually even.

Proof. Assume that nine is not odd. Then nine is even, so $9 = 2k$ for some integer k. It follows that

$$7 = 9 - 2 = 2k - 2 = 2(k - 1).$$

Since $k - 1$ is an integer, seven is even and hence is not odd. This proves the contrapositive, and therefore proves the original claim. □

4.2 An Example Where the Contrapositive Helps

Claim 2. *For every integer n, if n^2 is even, then n is even.*

A direct proof would start with $n^2 = 2k$ and try to deduce that n is twice an integer. That conclusion does not follow merely by taking a square root. The contrapositive gives us a useful expression for n itself, so the algebra is more straightforward.

Proof by contrapositive. Let n be an arbitrary integer and assume that n is not even. Then n is odd, so $n = 2k + 1$ for some integer k. Squaring gives

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

The number $2k^2 + 2k$ is an integer, so n^2 is odd and therefore is not even. We have proved that if n is not even, then n^2 is not even, which is the contrapositive of the claim. □

5 Proof by Contradiction

De Morgan's law gives another useful way to read an implication:

$$(P \Rightarrow Q) \;\equiv\; \neg P \vee Q \;\equiv\; \neg(P \wedge \neg Q).$$

In words, $P \Rightarrow Q$ says that P and $\neg Q$ cannot both be true. To prove it **by contradiction**, temporarily assume both P and $\neg Q$, and show that these assumptions lead to something impossible. For example, we might derive both a statement and its negation, or obtain a false equation such as $0 = 1$.

This differs from a contrapositive proof: a contrapositive proof assumes $\neg Q$ and derives $\neg P$; a contradiction proof assumes $P \wedge \neg Q$ and derives an impossibility.

5.1 Claim 1 by Contradiction

Proof by contradiction. Assume that seven is odd and that nine is not odd. The first assumption gives $7 = 2k + 1$ for some integer k. Consequently,

$$9 = 7 + 2 = 2(k + 1) + 1,$$

so nine is odd. This contradicts the assumption that nine is not odd. Therefore, seven cannot be odd while nine is not odd, which proves Claim 1. □

5.2 An Example Where Contradiction Helps

More generally, to prove any statement by contradiction, assume its negation and derive an impossibility. Here is an example.

A number is **rational** if it can be written as a/b, where a and b are integers and $b \neq 0$. A real number that is not rational is called **irrational**.

Claim 3. *The number* $\sqrt{2}$ *is irrational.*

There is no proposed fraction for us to compute directly. A contradiction proof lets us assume that such a fraction exists and then examine what that assumption would force.

Proof by contradiction. Assume that $\sqrt{2}$ is rational. Write

$$\sqrt{2} = \frac{a}{b},$$

where a and b are positive integers and the fraction is in lowest terms. In particular, a and b have no common integer factor greater than 1; any common factors have been canceled.

Squaring and multiplying by b^2 gives

$$a^2 = 2b^2.$$

Thus a^2 is even. By Claim 2, a is even, so $a = 2k$ for some integer k. Substituting gives

$$(2k)^2 = 2b^2 \implies 4k^2 = 2b^2 \implies b^2 = 2k^2.$$

Now b^2 is even, so Claim 2 tells us that b is even as well. Both a and b are divisible by 2, contradicting our choice of a fraction in lowest terms. Therefore, $\sqrt{2}$ is irrational. □

5.3 Connection to Stable Matching

This is also the structure we used to prove stability in Lecture 1. We assumed, for a contradiction, that the final matching had a blocking pair: an innovator and an investor who each preferred one another to their assigned partners.

Because the innovator proposed in order of preference, they must have proposed to this investor before reaching their final partner. The investor rejected that proposal, either immediately or later, in favor of someone they preferred. Since an investor's held partner only improves during the algorithm, their final partner must also be preferred to this innovator. This contradicts the assumption that the pair was blocking. Therefore, no blocking pair exists.

6 The Converse and "If and Only If"

Unlike AND, OR, and XOR, implication is **not commutative**. In general,

$$(P \Rightarrow Q) \not\equiv (Q \Rightarrow P).$$

For example, when P is false and Q is true, $P \Rightarrow Q$ is true but $Q \Rightarrow P$ is false.

We call $Q \Rightarrow P$ the **converse** of $P \Rightarrow Q$. For an arithmetic example, consider an integer n:

> If n is divisible by 4, then n is even.

This is true: if $n = 4k$ for an integer k, then $n = 2(2k)$ is even. Its converse is false: 2 is even but is not divisible by 4. The converse reverses the direction of an implication; the contrapositive reverses the direction *and negates both statements*.

A common mistake. Consider the argument:

> Every multiple of four is even. This number is even. Therefore, this number is a multiple of four.

For the number 2, both premises are true but the conclusion is false. Knowing $P \Rightarrow Q$ and Q does not, in general, allow us to infer P.

6.1 Proving Both Directions

When both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true, we say P **if and only if** Q, abbreviated P **iff** Q, and write $P \Leftrightarrow Q$. In symbols,

$$(P \Leftrightarrow Q) \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

An "if and only if" proof must establish *both directions*. The symbol $\Leftrightarrow$ forms a proposition, while $\equiv$ records that two expressions have matching truth tables.

Claim 4. *For every integer x, x is even if and only if x^2 is even.*

Proof. We prove each direction separately.

Forward direction: if x is even, then x^2 is even. Write $x = 2k$ for an integer k. Then

$$x^2 = (2k)^2 = 4k^2 = 2(2k^2),$$

which is even because $2k^2$ is an integer.

Reverse direction: if x^2 is even, then x is even. This is exactly Claim 2, which we proved by contrapositive. Since both directions hold, the equivalence follows. □

7 Proof by Cases

Sometimes we can divide a problem into a few possibilities and prove the desired statement in each one. This is called **proof by cases**. The cases must be **exhaustive**: every possibility must be covered. Checking a few examples is not enough; each case must account for all inputs of that type.

Claim 5. *The sum of two integers is even if and only if the two integers have the same parity.*

Proof. Let a and b be integers. Each is either even or odd, so there are four cases. In the expressions below, r and s are integers.

Case 1. Both are even. Write $a = 2r$ and $b = 2s$. Then

$$a + b = 2r + 2s = 2(r + s),$$

so the sum is even.

Case 2. Both are odd. Write $a = 2r + 1$ and $b = 2s + 1$. Then

$$a + b = (2r + 1) + (2s + 1) = 2(r + s + 1),$$

so the sum is even.

Case 3. a is even and b is odd. Write $a = 2r$ and $b = 2s + 1$. Then

$$a + b = 2r + (2s + 1) = 2(r + s) + 1,$$

so the sum is odd.

Case 4. a is odd and b is even. Write $a = 2r + 1$ and $b = 2s$. Then

$$a + b = (2r + 1) + 2s = 2(r + s) + 1,$$

so the sum is odd.

The first two cases show that having the same parity implies an even sum. The last two show that having different parities gives an odd sum; consequently, an even sum forces the same parity. This establishes both directions of the claim. □