Lecture 3: logical equivalences and proofs

September 16, 2026

1 Recap

1.1 De Morgan's Laws and Negating Quantifiers

Recall De Morgan's laws, $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$ and $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$, and that quantifiers negate as $\neg(\exists x, P(x)) \equiv \forall x, \neg P(x)$ and $\neg(\forall x, P(x)) \equiv \exists x, \neg P(x)$.

Example 1.1. *Last time, we considered defining "odd" as "not even." Using negation, we can write this out:*

$$n \textit{ is odd iff } \forall k \in \mathbb{Z},\ 2k \neq n.$$

Similarly, we can define "irrational" as "not rational":

$$x \in \mathbb{R} \textit{ is irrational iff } \forall m, n \in \mathbb{Z},\ x \neq m/n.$$

1.2 Proving If and Only If

To prove $p \iff q$, you need to prove both directions: $p \implies q$ and $q \implies p$. (Alternatively, if you can write a single chain of steps that are all $\iff$, that suffices too.)

1.3 Proving Statements False

To prove a statement p is false, you prove that its negation $\neg p$ is true.

1.4 The Law of the Excluded Middle

Every proposition p satisfies $p \vee \neg p$: it is either true or false, with no third option.

2 Inverse, Converse, Contrapositive

Given a statement $p \implies q$, there are three related statements we might consider:

- $q \implies p$ (the **converse**)
- $\neg p \implies \neg q$ (the **inverse**)
- $\neg q \implies \neg p$ (the **contrapositive**)

Example 2.1. *Which of these are equivalent to the original statement $p \implies q$? Consider:*

$$x \textit{ is a square} \implies x \textit{ is a rectangle}, \qquad \textit{"I am in this room"} \implies \textit{"I am on campus."}$$

$p \implies q$ is *equivalent* to its contrapositive $\neg q \implies \neg p$ (but generally not to its inverse or converse). We can verify this with a truth table — a truth table is itself a kind of proof, since it's an argument that shows a statement is true.

Proposition 2.2. *For propositions p and q, $p \implies q$ is equivalent to $\neg q \implies \neg p$.*

Proof.

p	q	$\neg p$	$\neg q$	$p \implies q$	$\neg q \implies \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The columns for $p \implies q$ and $\neg q \implies \neg p$ match on every row, so the two are equivalent. □

3 Proving Logical Equivalences via Boolean Algebra

Alternatively, we can prove equivalences algebraically, the same way we use rules like associativity $(a + (b + c) = (a + b) + c)$, commutativity $(a + b = b + a)$, and distributivity $(a(b + c) = ab + ac)$ in ordinary algebra.

In boolean algebra, the rules are similar, and all fairly intuitive, but there are a lot of them:

	Law	Equivalences
1.	**Identity**	$p \wedge \mathrm{T} \equiv p \quad p \vee \mathrm{F} \equiv p$
2.	**Domination**	$p \vee \mathrm{T} \equiv \mathrm{T} \quad p \wedge \mathrm{F} \equiv \mathrm{F}$
3.	**Idempotent**	$p \vee p \equiv p \quad p \wedge p \equiv p$
4.	**Negation**	$p \wedge \neg p \equiv \mathrm{F} \quad p \vee \neg p \equiv \mathrm{T}$
5.	**Double Negation**	$\neg\neg p \equiv p$
6.	**Commutative**	$p \wedge q \equiv q \wedge p \quad p \vee q \equiv q \vee p$
7.	**Associative**	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \quad (p \vee q) \vee r \equiv p \vee (q \vee r)$
8.	**Distributive**	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
9.	**Absorption**	$p \vee (p \wedge q) \equiv p \quad p \wedge (p \vee q) \equiv p$
10.	**De Morgan's**	$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \neg(p \vee q) \equiv \neg p \wedge \neg q$
11.	**Implication**	$p \to q \equiv \neg p \vee q$
12.	**Biconditional**	$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

Figure 1: Logical equivalences, Table 2.13 in Prof. Ansaf's textbook.

The most important ones are 10 (De Morgan's) and 11 (an equivalent way of writing $p \implies q$). Let's use these to prove $p \implies q \equiv \neg q \implies \neg p$ again:

$$\begin{aligned}
p \implies q &\equiv \neg p \vee q && \text{Implication} \\
&\equiv q \vee \neg p && \text{Commutativity} \\
&\equiv \neg(\neg q) \vee \neg p && \text{Double Negation} \\
&\equiv \neg q \implies \neg p && \text{Implication.}
\end{aligned}$$

4 Proof by Contrapositive

Since a statement and its contrapositive are equivalent, we can prove $p \implies q$ by instead proving $\neg q \implies \neg p$.

Proposition 4.1. *Let $x, y \in \mathbb{N}$. If $xy > 50$, then $x > 7$ or $y > 7$.*

Proof. We prove the contrapositive: if $\neg(x > 7$ or $y > 7)$, then $\neg(xy > 50)$. By De Morgan's laws, the hypothesis becomes $x \leq 7$ and $y \leq 7$. Then

$$xy \leq 7 \cdot 7 = 49 \leq 50,$$

so $\neg(xy > 50)$, as needed. □

Example 4.2. *How would you prove this statement: if r is irrational, then $\sqrt{r}$ is irrational. This seems hard to prove directly! What is the contrapositive?*

5 Proof by Example and Counterexample

We can prove statements of the form "there exists $x \ldots$" by simply presenting an example, and disprove statements of the form "for all $x \ldots$" by simply presenting a counterexample.

Example 5.1. *Is $\forall x, \exists y, xy = 1$ true? It's false: taking $x = 0$, we have $xy = 0 \neq 1$ for every y. To prove this rigorously, negate the statement to get $\exists x, \forall y, xy \neq 1$, and prove* that *directly: let $x = 0$; then for all y, $xy = 0 \neq 1$, as needed.*

Proposition 5.2. *There exists a perfect square that is also a perfect cube.*

Proof. $64 = 8^2 = 4^3$. □

Proposition 5.3. *The statement "for all $x \in \mathbb{N}$, $x^2 + x + 17$ is prime" is false.*

Proof. Consider $x = 17$: then $x^2 + x + 17 = 17(17 + 1 + 1)$ is divisible by 17, so not prime. □

6 Infinitely many primes

Theorem 6.1. *There are infinitely many primes.*

Before proving this, note that we haven't formally defined "infinity" yet — so let's rewrite the statement using ideas we already know: *for every prime, there exists a larger number that is also prime.*

Proof. Suppose, for the sake of contradiction, that there are finitely many primes $p_1, \ldots, p_n$. Consider $x = p_1 p_2 \cdots p_n + 1$. Since x is an integer greater than 1, it must be divisible by some prime, so $p_k \mid x$ for some $k \in [n]$. Then

$$\frac{x}{p_k} = \Big(\prod_{i \neq k} p_i\Big) + \frac{1}{p_k}.$$

The first term is an integer, but $\frac{1}{p_k}$ is not, so x/p_k is not an integer, contradicting $p_k \mid x$. ↯

So, there are infinitely many primes. □

Intuitively, the idea is this: suppose that there are only (for example) four primes: 2, 3, 5, and 7. Then, every number must be divisible by at least one of these primes. But $2 \cdot 3 \cdot 5 \cdot 7 + 1$ is not:

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 + 1}{2} = 3 \cdot 5 \cdot 7 + \frac{1}{2}$$

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 + 1}{3} = 2 \cdot 5 \cdot 7 + \frac{1}{3}$$

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 + 1}{5} = 2 \cdot 3 \cdot 7 + \frac{1}{5}$$

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 + 1}{7} = 2 \cdot 3 \cdot 5 + \frac{1}{7}$$

The remainder of 1 always results in a fractional part left over. So, $2 \cdot 3 \cdot 5 \cdot 7 + 1$ must be divisible by some other prime, so there must be primes other than 2,3,5, and 7.