Middlebury

CSCI 200: Math Foundations of Computing

Spring 2026

Lecture 6M: Indirect Proofs

Goals for today:

- Prove an implication using the contrapositive.
- Prove by assuming a contradiction.
- Prove an if-and-only-if.

If there are n pigeonholes and $n + 1$ pigeons, then at least two pigeons will go to the same pigeonhole.

pigeonhole principle

But first: proving with examples.

Which could be proved using an example?

(single)

✗ A. $\forall x \in S, p(x)$

✗ B. $\forall x \in S, \neg p(x)$

✗ C. $\neg \exists x \in S : p(x)$ $\quad \forall x \in S,\ \neg p(x)$

✓ D. $\neg \forall x \in S, p(x)$ $\quad \exists x \in S,\ \neg p(x)$

Proof Method #3: contrapositive.

Rule 3: $\dfrac{p \to q}{\therefore \neg q \to \neg p}$

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

(p: a^2 is not divisible by 4; q: a is odd.)

proof: We prove the contrapositive: if a is even, then a^2 is divisible by 4.

Let a be an even integer, which means $a = 2k$, $k \in \mathbb{Z}$.

We want to show that a^2 is divisible by 4.

Starting with $a^2 = (2k)^2 = 4k^2 = 4m$, $m \in \mathbb{Z}$.

This means a^2 is divisible by 4.

Therefore, by the contrapositive, if a^2 is not divisible by 4, then a is odd.

□

Prove: *If* a^2 *is even, then* a *is even.*

p q

$\neg p$: a^2 is odd

$\neg q$: a is odd.

proof: We prove the contrapositive: if a is odd, then a^2 is odd.

Let a be an odd integer, so $a = 2k+1$, $k \in \mathbb{Z}$.

We want to show a^2 is odd.

Starting with $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2+2k)+1$

$= 2m+1$ $m \in \mathbb{Z}$.

Therefore, by the contrapositive, if a^2 is even then a is even.

□

LEMMA for our next proof.

Proof Method #4: contradiction.

Example: *Prove that $\sqrt{2}$ is irrational.*

P

rational: $\frac{m}{n}$ $m,n \in \mathbb{Z}$, $n \neq 0$

Steps:

1. Assume $\neg p$ is true.
2. Try to show a contradiction happens.
3. Because of the contradiction, then p must be true.

proof: We use a proof by contradiction.

Suppose $\sqrt{2}$ is rational, that is $\sqrt{2} = \frac{m}{n}$ for $m,n \in \mathbb{Z}$.

Assume $\frac{m}{n}$ is simplified to lowest terms.

$\frac{4}{6} \rightarrow \frac{2}{3}$

Then $m^2 = 2n^2$, so m^2 is even, meaning m is also even (by thm on last slide).

So, if m is even, then $m = 2k$ for some $k \in \mathbb{Z}$.

Then going back to $m^2 = (2k)^2 = 4k^2 = 2n^2$, so $n^2 = 2k^2$ and n is even.

Then $n = 2l$, $l \in \mathbb{Z}$. Then $\frac{m}{n} = \frac{2k}{2l}$ which is not simplified to lowest terms. This is a contradiction, so $\sqrt{2}$ is irrational. □

[Exercise 1]

Suppose $a \in \mathbb{Z}$***. Prove that*** $14 \mid a$ ***if and only if*** $7 \mid a$ ***and*** $2 \mid a$.

P

Q

$P \leftrightarrow Q$

$(P \rightarrow Q) \wedge (Q \rightarrow P)$

show both of these.

[Exercise 1]

Suppose $a \in \mathbb{Z}$***. Prove that*** $14 \mid a$ ***if and only if*** $7 \mid a$ ***and*** $2 \mid a$.

proof: We prove ① if $14|a$ then $7|a$ and $2|a$ and ② if $7|a$ and $2|a$, then $14|a$.

First, we show that if $14|a$, then $7|a$ and $2|a$. Suppose $14|a$, so $a = 14k$, $k \in \mathbb{Z}$.

This means $a = 2(\underbrace{7k}_{m}) = 2m$, so $2|a$.

Also, $a = 7(\underbrace{2k}_{\ell}) = 7\ell$, so $7|a$. Therefore, both 2 and 7 divide a.

Second, we show that if $7|a$ and $2|a$, then $14|a$. Suppose $2|a$ and $7|a$.

Then $a = 2k$, $k \in \mathbb{Z}$ and $a = 7m$, $m \in \mathbb{Z}$. Since $a = 2k$, a is even.

So $a = 7m$ is also even, which can only be even if m is even. (similar to Lemma 11.1. if $a \cdot b$ is even, a is even, or b is even, or both are even)

Therefore $a = 7(\underbrace{2\ell}_{m}) = 14m$, so $14|a$. □

contrapositive (sketch)

a: odd
b: odd
$a \cdot b$: odd

$(2x+1)(2y+1) = \underbrace{2z+1}_{\text{odd}}$

(a, b)

The Pigeonhole Principle.

$p \wedge q \rightarrow r$ $\quad \neg(p \wedge q) = \neg p \vee \neg q$

If there are n pigeonholes and $n+1$ pigeons, then at least two pigeons will go to the same pigeonhole.

proof: We use the contrapositive:

if there are less than 2 (0,1) pigeons going to a pigeonhole, then there are not n pigeonholes or not (n+1) pigeons.

If at most 1 pigeon goes to a pigeonhole, and there are n pigeonholes, then there are at most n pigeons, which is not (n+1) pigeons. So there are not (n+1) pigeons, then by contrapositive, __ is true. □