Lec 07: Contradiction and Contraposition

Prof. Adam J. Aviv

GW

CSCI 1311 Discrete Structures I
Spring 2023

Recall the structure of direct proofs

If we want to show some statement is true, say $P(x) \implies Q(x)$:

Goal:	To prove $P(x) \implies Q(x)$
Approach:	Assume $P(x)$
	$\vdots$
	Therefore $Q(x)$

Direct Proof Techniques

- By example
  - Use to prove and existential quantifier
- By counterexample
  - Use to disprove a universal quantifier
- By generic particular
  - Use to prove a universal quantifier or disprove an extensional quantifier when you can show something is true for an arbitrarily chosen element.
- By cases
  - Use to prove universal quantifiers when it can be shown that there exists a set of finite cases for the quantification, for example, either even or odd. Each case can then be proven separately.

Other Proof techniques

We will explore two other proof techniques

- Proof by contradiction:
  - To prove P, show that $\neg P \implies$ c
- Proof by contraposition (contrapositive)
  - To prove $P \implies Q$, show that $\neg Q \implies \neg P$

Proof by Contraction

Goal:	To prove P
Approach:	Assume $\neg P$
	$\vdots$
	R
	$\vdots$
	$\neg R$
Conclusion:	$\neg P \implies R \wedge \neg R$ a contradiction
	Therefore: P holds.

Well Ordered Principle

Definition

The well-ordered principle of integers states that for every non-empty set of positive integers, there must exists a smallest element.

Example

The set $\{5, 8, 22, 13\}$ has a smallest value, 5.

The set $\{x^2 \mid x \in \mathbb{Z}+ \text{ and } 5 \leq x \leq 10\}$ has a smallest value, 25.

Theorem

Any integer greater than 1 is divisible by a prime number.

Proof.

Let n be an integer greater than 1, and let's define $D = \{d \in \mathbb{Z}^+ \mid d|n\} \backslash \{1, n\}$, or more generally, the set of factors that divides n, excluding 1 and n. We can explore two cases

- If $|D| = 0$, then n is prime. Since $n|n$, we have shown our result.
- If $|D| > 0$, then n is composite. By the well-ordered principle, there must exists a smallest element d_0, *and we can prove d_0 must be prime by contradiction. Assume that d_0 is composite . . .*

□

Where is the contradiction? (Discuss!)

Two hints:

- A positive integer $n > 1$ is composite if, and only if, there exists integers r and s, where $n = rs$, $1 < r < n$ and $1 < s < n$.
- Divisibility is transitive: For integers a and b, if $a|b$ and $b|c$, then $a|c$

Proof.

. . .

Assume that d_0 is composite.

There must exist an integer c such that $c|d_0$ where $1 < c < d_0$. By transitivity of divisibility $c|n$ because $c|d_0$ and $d_0|n$.

In that case, c must also be an element in D, but $c < d_0$. We have a contradiction because d_0 was the smallest element of D and $c < d_0$ and $c \in D$. Therefore d_0 cannot be composite, and must be prime. □

Unique Factorization

The proof that all integers are divisible by a prime (and a few other theorems) will eventually lead you to this amazing fact, that all positive integers have a unique prime factorization. This called the **Fundamental Theorem of Arithmetic** (FTA).

Theorem (Fundamental Theorem of Arithmetic (FTA))

Given any integer $n > 1$, there exists a positive integer k, distinct primes $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

and $p_1 < p_2 < \ldots < p_k$

To prove FTA, you must show that there exists a set of prime factors for every number *and* those prime factors are unique.

We will prove existence with (strong) induction next week, and you will prove the uniqueness in lab.

Exercise

Prove the following theorems by contradictions.

There is no greatest integer.

There is no integer that is both even and odd.

Both proofs rely on the fact that ***integers are closed under addition/subtraction****, but* ***not closed under division*** *such as 1/2 or 2/3. That is if a and b are integers, then $a + b$ and $a - b$ are also integers but a/b may not be.*

Euclid's proof for infinite primes (1)

This fact was proven more than 2000(!) years ago by Euclid (ca. 300 BCE).

Theorem

There is an infinite number of primes.

Take a moment to reflect on how amazing that is. **Arabic numbers were not even invented yet (ca. 500 CE)!**

But, first we need to show the following lemma:

Lemma

For integers a, b, c If integer $a|b$ and $a|c$ then $a|(b-c)$

Proof.

If $a|b$ and $a|c$, then exists k and k' such that $b = ak$ and $c = ak'$. Then $b - c = ak - ak' = a(k - k')$, thus $a|(b - c)$. □

Euclid's proof for infinite primes (2)

Theorem

There is an infinite number of primes.

Proof.

Assume there is exactly k primes, from $p_1 < p_2 < \ldots < p_k$, and define the number $n = p_1 p_2 \ldots p_k$ as the multiplication of *all* k primes. Let $m = n + 1$, the multiplication of *all* the primes, plus 1. By the assumptions, m cannot be prime (it is composite) because $m > p_k$, the largest prime!

If m is composite, by our earlier theorem, then there must exists a prime $p|m$. By our assumption, p must be one of the $p_1 \ldots p_k$ primes. Also $p|n$ because $n = p_1 p_2 \ldots p_k$. By the lemma, it must be the case that $p|(m - n)$. But $m - n = 1$, so $p|1$ implying $p \leq 1$. p cannot be prime: a contradiction.

There cannot be a finite number of primes; there is an infinite number. □

Rationals ($\mathbb{Q}$) and Irrationals

Definition

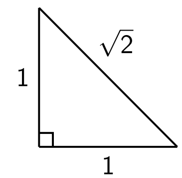
A real number r is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is irrational.

$$r \in \mathbb{Q} \iff (\exists a, b \in \mathbb{Z})(r = \frac{a}{b} \text{ and } b \neq 0)$$

We say $\frac{a}{b}$ is in reduced form if there are no common factors. Another way to say this is that a and b are relatively prime. **All rationals can be expressed in reduced form.**

Geometric representation of the $\sqrt{2}$

In Euclidean geometry, you could construct $\sqrt{2}$ using a ruler and compass.



But it was a great unsolved problem (of the classical era) if this number can be expressed in terms of a ratio, that is, is it rational?

Evenness of Squares (1)

Before proving irrationality of $\sqrt{2}$, we will need the following lemma.

Lemma

n is even if, and only if, n^2 is even.

Note this is a bi-conditional statement:

$$(\forall n \in \mathbb{Z})(\text{Even}(n) \leftrightarrow \text{Even}(n^2)) \equiv$$
$$(\forall n \in \mathbb{Z})(\text{Even}(n) \rightarrow \text{Even}(n^2)) \wedge (\text{Even}(n) \leftarrow \text{Even}(n^2))$$

It is equivalent to the *and* of two implications, and we must prove both!

Lemma $\implies$: n is even if, and only if, n^2 is even.

if n is even, then n^2 is even

Proof.

If n is even, then exists a k such that $n = 2k$. Then $n^2 = 4k^2 = 2(2k^2)$, and n^2 is even. □

What about proving the other directions?
If we assume n^2 is even, we are left with $n^2 = 2k$ for some integer k
. . . how do we show that n is even?

Proof by Contraposition

Recall that $p \to q \equiv \neg q \to \neg p$, so another way to prove an implication is by showing the contrapositive is true. This technique is called proof by contraposition (or more simply, proof by contrapositive)

Goal:	To prove $P \implies Q$
Approach:	Assume $\neg Q$
	$\vdots$
	Therefore $\neg P$
Conclusion:	$\neg Q \implies \neg P$, which is equivalent to $P \implies Q$

Evenness of Square (2)

What is the contrapositive of the implication?

Lemma $\Leftarrow$: n is even if, and only if, n^2 is even.

if n^2 is even, then n is even

"If n is not even, then n^2 is not even." Or, put another way, "if n is odd, then n^2 is odd." Prove it now!

Proof.

Assume that n is odd, then $n = 2k + 1$ and $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so n^2 is odd.

By contraposition, if n is odd, then n^2 is odd shows that if n^2 is even, then n is even.

□

Irrationality of $\sqrt{2}$ (2)

Proof of Irrationality of $\sqrt{2}$

Assume that $\sqrt{2}$ is rational, then there exists integers a and b such that $\sqrt{2} = a/b$ and a and b are relatively prime, that is a and b do not share common divisors and so a/b is in reduced form. Then

$$\begin{aligned}\sqrt{2} &= \frac{a}{b}\\ 2 &= \frac{a^2}{b^2}\\ 2b^2 &= a^2\end{aligned}$$

Thus a^2 is even, and by the lemma, so is a. So we can write $a = 2k$ for some integer k.

Irrationality of $\sqrt{2}$ (3)

Poof of the Irrationality of $\sqrt{2}$ (cont.)

Substituting in $a = 2k$, we have

$$\begin{aligned}2b^2 &= a^2\\ 2b^2 &= (2k)^2\\ 2b^2 &= 4k^2\\ b^2 &= 2k^2\end{aligned}$$

Thus b is also even. If a is even, and b is even, then they share a common divisor, namely 2, and are not relatively prime and the fraction is not in reduced form: a contradiction.

Thus $\sqrt{2}$ cannot be rational and is irrational. □

Exercise

Proof the following, by proving the contrapositive.

If $3k + 2$ is odd, then k is odd.

For all integers $n > 2$, if n is prime, then n is odd.

Pigeons and Holes

Theorem (Pigeonhole Principle)

Let n and k be positive integers. When placing n objects into k boxes, if $n > k$ then at least one box must contain more than one object.

Proof.

Proof by contraposition. We can show that: If all k boxes contain *at most* one object, then $k \leq n$. Observe that the max number of objects n is the

same as the number of boxes k since there is at most one per box. It is the case $k \leq n$. By the contrapositive, we conclude the theorem is true. □

Examples of applying the pigeonhole principle

For every 27 word sequence in the US constitution, at least two words will start will the same letter.

If you pick five numbers from integers 1 to 8, then two of them must add up to 9.

In New York City, there are two non-bald people who have the same number of hairs on their head.

https://mindyourdecisions.com/blog/2008/11/25/16-fun-applications-of-the-pigeonhole-principle/