CSE 20
DISCRETE MATH

Fall 2020

http://cseweb.ucsd.edu/classes/fa20/cse20-a/

Learning goals

Today's goals

- Evaluate which proof technique(s) is appropriate for a given proposition
- Trace and/or construct a proof by contradiction

Greatest and least

A. There is a greatest integer

B. There is a least integer

C. There is a greatest prime number

D. There is a least prime number

E. More than one of the above

Two approaches

Goal: Disprove an existential claim

Approach 1: Prove the equivalent universal claim

Approach 2: Proof by contradiction

New! Proof by Contradiction (Rosen 1.7 p86)
To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Assume $\neg p$, that there is a greatest integer

Scratch work

Identify r = “there are two numbers that are each bigger than the other”

To show: $(r \wedge \neg r)$

Two approaches

Goal: Disprove an existential claim

Approach 1: Prove the equivalent universal claim

Approach 2: Proof by contradiction

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

Idea: Use assumption to build a number that is not a product of primes

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

We can name all primes (since there are finitely many integers between 2 and n_{BIG})

$$n_1, n_2, \ldots, n_{BIG}$$

Consider the number **$C = (n_1\, n_2 \cdots n_{BIG}) + 1$**. This is a positive integer greater than 1.
Lemma: C does not have any prime factors and thus is not a product of primes.

Theorem: There is no greatest prime number.

Assume $\neg p$, that there is a greatest prime number, call it n_{BIG}.

Choose r = ”Every positive integer greater than 1 is a product of primes.”

To show $(r \wedge \neg r)$

We have proved that r is True.
To show: r is False (under assumption).

Lemma: There is an integer, C, that is not a product of primes.

Since assuming that there is a greatest prime guarantees $(r \wedge \neg r)$ the assumption must be **false**. Thus, its negation is true.

- A counterexample can be used to prove that $\forall x P(x)$ is **false**.
- A witness can be used to prove that $\exists x P(x)$ is **true**.
- **Proof by universal generalization**: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.
- To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.
- **Proof of Conditional by Direct Proof**: To prove that the implication $p \to q$ is true, we can assume p is true and use that assumption to show q is true.
- **Proof of Conditional by Contrapositive Proof**: To prove that the implication $p \to q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.
- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \to q$ and $p_2 \to q$.
- **Proof by Contradiction** To prove that a statement p is true, pick another statement r and if we can show that $\neg p \to (r \wedge \neg r)$ then we can conclude that p is true.
- **Proof by Structural Induction** To prove a universal quantification over a recursively defined set:

  Basis Step: Show the statement holds for elements specified in the basis step of the definition.
  Recursive Step: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- **Proof by Mathematical Induction** To prove a universal quantification over the set of all integers greater than or equals some base integer b:

  Basis Step: Show the statement holds for b.
  Recursive Step: Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Strong Induction** To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

  Basis Step: Show the statement holds for b, $b + 1$, $\ldots$, $b + j$.
  Recursive Step: Consider an arbitrary integer n greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b + 1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n + 1$.

Choosing a proof strategy

When might it be appropriate to use induction?

A. To prove that an existential claim is true
B. To prove that a universal claim is false
C. To prove that a conditional claim is true
D. More than one of the above
E. None of the above

Choosing a proof strategy

When might it be appropriate to use proof by contradiction?

A. To prove that an existential claim is true
B. To prove that a universal claim is false
C. To prove that a conditional claim is true
D. More than one of the above
E. None of the above

The square root of 2 $\sqrt{2}$

Which of the following statements is **not** true about this number?

A. It is a real number.
B. It is strictly less than 2.
C. It is strictly greater than 1.
D. It is a solution to $x^2 - 2 = 0$.
E. It is even.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: The definition of the set of rational numbers is the collection of fractions p/q where p is an integer and q is a nonzero integer.

Looking for a **witness** p and q, we can write the square root of 2 as the fraction $\sqrt{2}$ /1, where 1 is a nonzero integer. Since the numerator is not in the domain, this witness is not allowed, and we have shown that the square root of 2 is not a fraction of integers (with nonzero denominator). Thus, the square root of 2 is not rational.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, we will define a statement r such that $(\sqrt{2} \in \mathbb{Q}) \rightarrow (r \wedge \neg r)$

….<<fill in once we know what r should be>>….

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, we will define a statement r such that $(\sqrt{2} \in \mathbb{Q}) \rightarrow (r \wedge \neg r)$

….<<fill in once we know what r should be>>….

Greatest common divisor (Rosen 4.3 p265) Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(a, b)$.

Lemma 1: For every two integers p and q, not both zero, $gcd\left(\frac{p}{gcd(p,q)}, \frac{q}{gcd(p,q)}\right) = 1$.

Lemma 2: For every two integers a and b, not both zero, with $gcd(a, b) = 1$, it is not the case that both a is even and b is even.

Lemma 3: For every integer x, x is even if and only if x^2 is even.

Lemma 1: For every two integers p and q, not both zero, $gcd\left(\frac{p}{gcd(p,q)}, \frac{q}{gcd(p,q)}\right) = 1$.

Lemma 2: For every two integers a and b, not both zero, with $gcd(a, b) = 1$, it is not the case that both a is even and b is even.

Lemma 3: For every integer x, x is even if and only if x^2 is even.

Challenge: prove these lemmas.

Hints:

- Write numbers as products of primes
- Use definitions (of even, gcd)
- Use direct proof & proof by contrapositive for biconditional (see bonus video)

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, we will define a statement r such that $(\sqrt{2} \in \mathbb{Q}) \to (r \wedge \neg r)$

In a direct proof of the conditional, we assume $(\sqrt{2} \in \mathbb{Q})$. Namely, there are (positive) integers p, q with $\sqrt{2} = \frac{p}{q}$

Rewrite this fraction in lowest terms: divide p and q by greatest common divisor $\sqrt{2} = \frac{a}{b}$ with gcd(a,b)=1.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even.

Squaring both sides and clearing denominator: $2b^2 = a^2$.

By definition of even (since b^2 is an integer), a^2 is even.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even.

Squaring both sides and clearing denominator: $2b^2 = a^2$.

By definition of even (since b^2 is an integer), a^2 is even.

By **Lemma 3**, this guarantees a is even too. By definition of even, there is some integer, call it c, such that a = 2c.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even…. From definitions, a is even, so there is some integer, call it c, such that a = 2c. Plugging into equation relating a and b:

$$2b^2 = a^2 = (2c)^2 = 4c^2.$$

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even…. From definitions, a is even, so there is some integer, call it c, such that a = 2c. Plugging into equation relating a and b:

$$2b^2 = a^2 = (2c)^2 = 4c^2.$$

Dividing both sides by two gives $b^2 = 2c^2$, and since c^2 is an integer, the definition of even means that b^2 is even. Applying **Lemma 3**: b is even.

The square root of 2

Goal: The square root of 2 is not a rational number.

Attempted proof: Towards a proof by contradiction, ….

…assuming square root of 2 is rational gives integers a, b with gcd(a,b)=1 and $\sqrt{2} = \frac{a}{b}$. By **Lemma 2** a and b are not both even…. From definitions, a is even, so there is some integer, call it c, such that a = 2c. Plugging into equation relating a and b:

$$2b^2 = a^2 = (2c)^2 = 4c^2.$$

Dividing both sides by two gives $b^2 = 2c^2$, and since c^2 is an integer, the definition of even means that b^2 is even. Applying **Lemma 3**: b is even. Thus, a is even and b is even.

The square root of 2

Goal: The square root of 2 is not a rational number.

~~**Attempted**~~ **Proof**: Towards a proof by contradiction, we will define a statement r such that $(\sqrt{2} \in \mathbb{Q}) \rightarrow (r \wedge \neg r)$

In a direct proof of the conditional, we assume $(\sqrt{2} \in \mathbb{Q})$. Namely, there are (positive) integers p,q with $\sqrt{2} = \frac{p}{q}$

Rewrite this fraction in lowest terms: divide p and q by greatest common divisor $\sqrt{2} = \frac{a}{b}$ with gcd(a,b)=1.

Define r = “it is not the case that both a is even and b is even”

By **Lemma 2,** r is true…. By definitions, Lemma 2 and Lemma 3, r is false.

Recap

Proof by contradiction can be useful in proving negations of existentials.

In a proof by contradiction, we are proving a conditional claim $\neg p \to (r \wedge \neg r)$ where the hypothesis is the **negation of the statement we are trying to prove** and the conclusion is up to us to figure out!

For next time

Reading for next time: Section 4.3 Example 2 Section (p. 258), Section 1.7 Example 9 (p. 86)