CS311H: Discrete Mathematics
Mathematical Proof Techniques
Instructor: Işıl Dillig

Review of Proof Strategies

Many different strategies for proving theorems:

- **Direct proof**: \( p \rightarrow q \) proved by directly showing that if \( p \) is true, then \( q \) must follow
- **Proof by contraposition**: Prove \( p \rightarrow q \) by proving \( \neg q \rightarrow \neg p \)
- **Proof by contradiction**: Prove that the negation of the theorem yields a contradiction
- **Proof by cases**: Exhaustively enumerate different possibilities, and prove the theorem for each case

In many proofs, one needs to combine several different strategies!

Quick Example

- Prove: If \( n = ab \), then \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \)

Proof by Contradiction

- Suppose we want to show that \( p \rightarrow q \) is true
- **Recall**: Formula is valid iff negation is undated
- What is the negation of \( p \rightarrow q \)?
- **Proof by contradiction**: Show that \( p \land \neg q \) is not possible

Example

- Prove by contradiction that "If \( 3n + 2 \) is odd, then \( n \) is odd."
Another Example

- **Recall:** Any rational number can be written in the form \( \frac{p}{q} \) where \( p \) and \( q \) are integers and have no common factors.

- **Example:** Prove by contradiction that \( \sqrt{2} \) is irrational.

- **Proof:** Suppose \( \sqrt{2} \) was rational. Then, \( \sqrt{2} = \frac{p}{q} \) where \( p, q \) are integers with no common factors.

  - By squaring both sides, we have: \( 2 = \frac{p^2}{q^2} \), i.e., \( 2q^2 = p^2 \)
  - Since \( p^2 \) is even, \( p \) must also be even (proved earlier)
  - Hence, \( p = 2k \) for some \( k \), and \( p^2 = 4k^2 = 2q^2 \).

Example, cont

- This implies \( q^2 = 2k^2 \); thus, \( q^2 \) is also even

  - Again, if \( q^2 \) is even, this means \( q \) is even.

  - But since both \( p \) and \( q \) are even, this means they have a common factor, i.e., 2

  - But this contradicts our assumption!

Proof by Cases

- In some cases, it is very difficult to prove a theorem by applying the same argument in all cases

  - For example, we might need to consider different arguments for negative and non-negative integers

  - **Proof by cases** allows us to apply different arguments in different cases and combine the results

    - Specifically, suppose we want to prove statement \( p \), and we know that we have either \( q \) or \( r \)

    - If we can show \( q \rightarrow p \) and \( r \rightarrow p \), then we can conclude \( p \)

Proof by Cases, cont.

- In general, there may be more than two cases to consider

  - **Proof by cases** says that to show

    \[ (p_1 \lor p_2 \ldots \lor p_k) \rightarrow q \]

    it suffices to show:

    - \( p_1 \rightarrow q \)
    - \( p_2 \rightarrow q \)
    - \( \ldots \)
    - \( p_k \rightarrow q \)

Example

- Prove that \( |xy| = |x||y| \)

  - Here, proof by cases is useful because definition of absolute value depends on whether number is negative or not.

  - There are four possibilities:
    1. \( x, y \) are both non-negative
    2. \( x \) non-negative, but \( y \) negative
    3. \( x \) negative, \( y \) non-negative
    4. \( x, y \) are both negative

  - We’ll prove the property by proving these four cases separately

Proof

- **Case 1:** \( x, y \geq 0 \). In this case, \( |xy| = xy = |x||y| \)

- **Case 2:** \( x \geq 0, y < 0 \). Here, \( |xy| = -xy = x \cdot (-y) = |x||y| \)

- **Case 3:** \( x < 0, y \geq 0 \). Here, \( |xy| = -xy = (-x) \cdot y = |x||y| \)

- **Case 4:** \( x, y < 0 \). Here, \( |xy| = xy = (-x) \cdot (-y) = |x||y| \)

  - Since we proved it for all cases, the theorem is valid.

  - **Caveat:** Your cases must cover all possibilities; otherwise, the proof is not valid!
Another Example

- Prove that \( \max(x, y) + \min(x, y) = x + y \)

Combining Proof Techniques

- So far, our proofs used a single strategy, but often it’s necessary to combine multiple strategies in one proof.
- **Example**: Prove that every rational number can be expressed as a product of two irrational numbers.
  
  **Proof**: Let’s first employ direct proof.
  
  Observe that any rational number \( r \) can be written as \( \sqrt{2} \cdot r \).
  
  We already proved \( \sqrt{2} \) is irrational.
  
  If we can show that \( r \sqrt{2} \) is also irrational, we have a direct proof.

Combining Proofs, cont.

- Now, employ proof by contradiction to show \( r \sqrt{2} \) is irrational.
  
  Suppose \( \sqrt{2} \) was rational.
  
  Then, for some integers \( p, q \): \( \sqrt{2} = \frac{p}{q} \).
  
  This can be rewritten as \( \sqrt{2} = \frac{ap}{bq} \).
  
  Since \( r \) is rational, it can be written as quotient of integers:
  
  \[ \sqrt{2} = \frac{a}{b} \cdot \frac{p}{q} \]
  
  But this would mean \( \sqrt{2} \) is rational, a contradiction.

Lesson from Example

- In this proof, we combined direct and proof-by-contradiction strategies – “proof within proof”
  
  In more complex proofs, it might be necessary to combine two or even more strategies and prove helper lemmas.

If and Only If Proofs

- Some theorems are of the form “\( P \) if and only if \( Q \)” (\( P \leftrightarrow Q \))
  
  The easiest way to prove such statements is to show \( P \rightarrow Q \) and \( Q \rightarrow P \).
  
  Therefore, such proofs correspond to two subproofs.
  
  One shows \( P \rightarrow Q \) (typically labeled \( \Rightarrow \))
  
  Another subproof shows \( Q \rightarrow P \) (typically labeled \( \Leftarrow \)).

Example

- Prove “A positive integer \( n \) is odd if and only if \( n^2 \) is odd.”
  
  \( \Rightarrow \) We have already shown this using a direct proof earlier.
  
  \( \Leftarrow \) We have already shown this by a proof by contraposition.
  
  Since we have proved both directions, the proof is complete.
Counterexamples

- So far, we have learned about how to prove statements are true using various strategies
- But how do we prove that a statement is false?
- Prove that the claim “The product of two irrational numbers is irrational” is false.

Prove or Disprove

Which of the statements below are true, which are false? Prove your answer.

- For all integers $n$, if $n^2$ is positive, $n$ is also positive.
- For all integers $n$, if $n^3$ is positive, $n$ is also positive.
- For all integers $n$ such that $n \geq 0$, $n^2 \geq 2n$

Existence and Uniqueness

- Common math proofs involve showing existence and uniqueness of certain objects
- Existence proofs require showing that an object with the desired property exists
- Uniqueness proofs require showing that there is a unique object with the desired property

Existence Proofs

- One simple way to prove existence is to provide an object that has the desired property – called constructive proof
- Example: Prove there exists an integer that is the sum of two perfect squares
- But not all existence proofs have to be constructive – possible to prove existence through other methods such as proof by contradiction or proof by cases
- Such indirect existence proofs called nonconstructive proofs

Non-Constructive Proof Example

- Prove: “There exist irrational numbers $x, y$ s.t. $x^y$ is rational”
- We’ll prove this using a non-constructive proof (by cases), without providing irrational $x, y$
- Consider $\sqrt{2}^{\sqrt{2}}$. Either (i) it is rational or (ii) it is irrational
- Case 1: We have $x = y = \sqrt{2}$ s.t. $x^y$ is rational
- Case 2: Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, so both are irrational. Then, $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}} = 2$. Thus, $x^y$ is rational

Non-Constructive Proofs

- This proof is non-constructive because it does not give concrete irrational numbers $x, y$ for which $x^y$ is rational
- In classical mathematics/logic, such non-constructive proofs are completely acceptable
- However, there is a school of mathematicians/logicians who only accept constructive proofs
- The branch of logic dealing with only constructive arguments is called intuitionistic (constructive) logic
Proving Uniqueness

- Some statements in mathematics assert uniqueness of an object satisfying a certain property.
- To prove uniqueness, must first prove existence of an object $x$ that has the property.
- Second, we must show that for any other $y$ s.t. $y \neq x$, then $y$ does not have the property.
- Alternatively, can show that if $y$ has the desired property that $x = y$.

Example of Uniqueness Proof

- Prove: "If $a$ and $b$ are real numbers with $a \neq 0$, then there exists a unique real number $r$ such that $ar + b = 0$".
- **Existence**: Using a constructive proof, we can see $r = -b/a$ satisfies $ar + b = 0$.
- **Uniqueness**: Suppose there is another number $s$ such that $s \neq r$ and $as + b = 0$. But since $ar + b = as + b$, we have $ar = as$, which implies $r = s$.

Summary of Proof Strategies

- **Direct proof**: $p \rightarrow q$ proved by directly showing that if $p$ is true, then $q$ must follow.
- **Proof by contraposition**: Prove $p \rightarrow q$ by proving $\neg q \rightarrow \neg p$.
- **Proof by contradiction**: Prove that the negation of the theorem yields a contradiction.
- **Proof by cases**: Exhaustively enumerate different possibilities, and prove the theorem for each case.

Invalid Proof Strategies

- **Proof by obviousness**: "The proof is so clear it need not be mentioned!"
- **Proof by intimidation**: "Don’t be stupid – of course it’s true!"
- **Proof by mumbo-jumbo**: $\forall \alpha \in \theta \exists \beta \in \alpha \circ \beta \approx \gamma$
- **Proof by intuition**: "I have this gut feeling."
- **Proof by resource limits**: "Due to lack of space, we omit this part of the proof..."

Don’t use anything like these in CS311!!