Introduction

- Formalizing statements in logic allows formal, machine-checkable proofs
- But these kinds of proofs can be very long and tedious
- In practice, humans write slightly less formal proofs, where multiple steps are combined into one
- We’ll now move from formal proofs in logic to less formal mathematical proofs!

Some Terminology

- Important mathematical statements that can be shown to be true are theorems
- Many famous mathematical theorems, e.g., Pythagorean theorem, Fermat’s last theorem
- Pythagorean theorem: Let a, b the length of the two sides of a right triangle, and let c be the hypotenuse. Then, \( a^2 + b^2 = c^2 \)
- Fermat’s Last Theorem: For any integer \( n \) greater than 2, the equation \( a^n + b^n = c^n \) has no solutions for non-zero \( a, b, c \).

Theorems, Lemmas, and Propositions

- There are many correct mathematical statements, but not all of them called theorems
- Less important statements that can be proven to be correct are propositions
- Another variation is a lemma: minor auxiliary result which aids in the proof of a theorem/proposition
- Corollary is a result whose proof follows immediately from a theorem or proposition

Conjectures vs. Theorems

- Conjecture is a statement that is suspected to be true by experts but not yet proven
- Goldbach’s conjecture: Every even integer greater than 2 can be expressed as the sum of two prime numbers.
- This conjecture is one of the oldest unsolved problems in number theory

General Strategies for Proving Theorems

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!
Direct Proof

- To prove \( p \rightarrow q \) in a direct proof, first assume \( p \) is true.
- Then use rules of inference, axioms, previously shown theorems/lemmas to show that \( q \) is also true.
- Example: If \( n \) is an odd integer, than \( n^2 \) is also odd.
- Proof: Assume \( n \) is odd. By definition of oddness, there must exist some integer \( k \) such that \( n = 2k + 1 \). Then, \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \), which is odd. Thus, if \( n \) is odd, \( n^2 \) is also odd.

More Direct Proof Examples

- An integer \( a \) is called a perfect square if there exists an integer \( b \) such that \( a = b^2 \).
- Example: Prove that every odd number is the difference of two perfect squares.

Proof by Contraposition

- In proof by contraposition, you prove \( p \rightarrow q \) by assuming \( \neg q \) and proving that \( \neg p \) follows.
- Makes no difference logically, but sometimes the contrapositive is easier to show than the original.
- Prove: If \( n^2 \) is odd, then \( n \) is odd.
  -

Proof by Contradiction

- Proof by contradiction proves that \( p \rightarrow q \) is true by proving unsatisfiability of its negation.
- What is negation of \( p \rightarrow q \)?
- Assume both \( p \) and \( \neg q \) are true and show this yields contradiction.

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.
  -

Instructor: Isıl Dillig, CS311H: Discrete Mathematics Mathematical Proof Techniques 7/31

More Direct Proof Examples

- An integer \( a \) is called a perfect square if there exists an integer \( b \) such that \( a = b^2 \).
- Example: Prove that every odd number is the difference of two perfect squares.

Proof by Contraposition

- In proof by contraposition, you prove \( p \rightarrow q \) by assuming \( \neg q \) and proving that \( \neg p \) follows.
- Makes no difference logically, but sometimes the contrapositive is easier to show than the original.
- Prove: If \( n^2 \) is odd, then \( n \) is odd.
  -

Proof by Contradiction

- Proof by contradiction proves that \( p \rightarrow q \) is true by proving unsatisfiability of its negation.
- What is negation of \( p \rightarrow q \)?
- Assume both \( p \) and \( \neg q \) are true and show this yields contradiction.

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.
  -
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 \( p \).

In general, there may be more than two cases to consider. Proof by cases says that to show \((p_1 \vee p_2 \ldots \vee p_k) \rightarrow q\) it suffices to show:
- \( p_1 \rightarrow q \)
- \( p_2 \rightarrow q \)
- \( \ldots \)
- \( p_k \rightarrow q \)

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

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 \( \sqrt{2} \frac{x}{y} \).

We already proved \( \sqrt{2} \) is irrational.

If we can show that \( \frac{x}{y} \) is also irrational, we have a direct proof.
Combining Proofs, cont.

Lesson from Example

- In this proof, we combined direct and proof-by-contradiction strategies
- In more complex proofs, it might be necessary to combine two or even more strategies and prove helper lemmas
- It is often a good idea to think about how to decompose your proof, what strategies to use in different subgoals, and what helper lemmas could be useful

If and Only if Proofs

- Some theorems are of the form “P if and only if Q” (P ↔ Q)
- The easiest way to prove such statements is to show P → Q and Q → P
- Therefore, such proofs correspond to two subproofs
- One shows P → Q (typically labeled ⇒)
- Another subproof shows Q → P (typically labeled ⇐)

Example

- Prove “A positive integer n is odd if and only if n^2 is odd.”
  - ⇒ We have already shown this using a direct proof earlier.
  - ⇐ 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 to prove a statement is false?
- What is a counterexample for the claim “The product of two irrational numbers is irrational”?

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^1 is positive, n is also positive.
- For all integers n such that n ≥ 0, n^2 ≥ 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
- This sort of proof is called constructive proof
- Example: Prove there exists an integer that is the sum of two perfect squares
- But not all existence proofs are constructive – can prove existence through other methods (e.g., 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, $\sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$. Thus, $x^y$ is rational

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...”
- **Proof by illegibility:** “sdjkfiugyhlaks?fskl; QED.”

*Don’t use anything like these in CS311!!*