Announcements

- Homework 2 due next lecture
- Little harder and longer than previous homework – don’t wait until night before

Introduction

- In previous lectures, we learned how to construct proofs using logical inference rules
- Such proofs are extremely formal and rigorous, but, for more complicated proofs, they can be very long and tedious
- In practice, mathematical proofs tend to be slightly less formal (e.g., can omit labeling names of inference rules)
- Today: Learn about proof-related mathematical concepts and proof strategies

Mathematical Theorems

- 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
- Once proven, conjectures become theorems
Story Behind Fermat’s Last Theorem
- Fermat’s last theorem was a conjecture for 360 years until it was finally proven by Andrew Wiles in 1995!
- Fermat scribbled this “theorem” in the margin of his copy of Arithmetica
- And also remarked: “I have discovered a truly marvelous proof of this, which this margin is too narrow to contain”
- Unknown if Fermat had a valid proof or what his proof was
- Finally proven by Wiles in 1995 using advanced results about elliptic curves

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, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k + 1)$, which is odd. Thus, if $n$ is odd, $n^2$ is also odd.
- **Observe**: This proof implicitly uses universal generalization and existential instantiation (where?)

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 if $m$ and $n$ are perfect squares, then $mn$ is also a perfect square.

Another Example
- **Example**: Prove that every odd number is the difference of two perfect squares.

Proof by Contraposition
- **Recall**: The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- **Recall**: A formula and its contrapositive are logically equivalent
- Hence, if you can prove $\neg q \rightarrow \neg p$, have shown $p \rightarrow q$
- This makes no difference from a logical point of view, but sometimes the contrapositive is easier to show by direct proof than the original
- Thus, in proof by contraposition, assume $\neg q$ and then use axioms, inference rules etc. to show that $\neg p$ must follow
Examples of Proof by Contraposition

- **Prove:** If $n^2$ is odd, then $n$ is odd.
- What is the contrapositive of this statement?
- **Proof:** Suppose $n$ is even. Then, there exists integer $k$ such that $n = 2k$.
- Then, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
- Thus, $n^2$ is also even.

Another Example

- **Prove:** If $n = ab$, then $a ≤ \sqrt{n}$ or $b ≤ \sqrt{n}$
- No obvious direct proof, therefore try proof by contraposition.
- **Note:** It may not always be immediately obvious whether to use direct proof or proof by contraposition. If you try one and it fails, try the other strategy!
- Over time, you will gain intuition about which proof strategies work well in which situations

Proof by Contradiction

- Suppose we want to show that $p → q$ is true
- The only way $p → q$ can be false if $p$ is true and $q$ is false
- **Proof by contradiction:** Show that $p ∧ ¬q$ is not possible
- i.e., assume both $p$ and $¬q$ and show that this yields a contradiction
- Proof by contradiction is a very widely used proof strategy

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 $p$.

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.

Another Example

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

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!
- Observe: The truth table method is essentially an (exhaustive) proof by cases...

Proof by Cases, cont.

- In general, there may be more than two cases to consider.
- Proof by cases says that to show
  \[(p_1 \lor p_2 \lor \cdots \lor p_k) \rightarrow q\]
  it suffices to show:
  \[p_1 \rightarrow q\]
  \[p_2 \rightarrow q\]
  \[\cdots\]
  \[p_k \rightarrow q\]
Combining Proofs, cont.

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

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 \( Q \)” (\( P \leftrightarrow Q \))
- 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?
- To show a statement is false, we provide counterexamples
- A counterexample is a concrete value for which the 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 \( n \geq 0 \), \( n^2 \geq 2n \)
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.

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 ≠ x, then y does not have the property.
- Alternatively, can show that if y has the desired property that x = y.

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 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 √2^√2. Either (i) it is rational or (ii) it is irrational.
- Case 1: We have x = y = √2. x^y is rational.
- Case 2: Let x = √2^√2 and y = √2, so both are irrational. Then, (√2^√2)^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.
- Such people are called intuitionists or constructivists.
- The branch of logic dealing with only constructive arguments is called intuitionistic 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 ≠ 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 ≠ 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 ≠ 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**: Exhausitively 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**: "sdjkfhiugyhlaks??fskl; QED."

Don’t use anything like these in CS243!!