# CS311H: Discrete Mathematics

## Rules of Inference
## Mathematical Proofs

Instructor: Işıl Dillig



## Summary of Inference Rules for Quantifiers

| Name | Rule of Inference |
|---|---|
| Universal Instantiation | $\frac{\forall x.P(x)}{P(c)}$ (any $c$) |
| Universal Generalization | $\frac{P(c) \quad (\text{for arbitrary } c)}{\forall x.P(x)}$ |
| Existential Instantiation | $\frac{\exists x.P(x)}{P(c) \text{ for fresh } c}$ |
| Existential Generalization | $\frac{P(c)}{\exists x.P(x)}$ |



## Example 1

- Prove that these hypotheses imply $\exists x.(P(x) \land \neg B(x))$:
  1. $\exists x.\ (C(x) \land \neg B(x))$ (Hypothesis)
  2. $\forall x.\ (C(x) \rightarrow P(x))$ (Hypothesis)



## Example 2

- Prove the below hypotheses are contradictory by deriving false
  1. $\forall x.(P(x) \rightarrow (Q(x) \land S(x)))$ (Hypothesis)
  2. $\forall x.(P(x) \land R(x))$ (Hypothesis)
  3. $\exists x.(\neg R(x) \lor \neg S(x))$ (Hypothesis)



## Example 3

Prove $\exists x.\ father(x, Evan)$ from the following premises:

1. $\forall x.\forall y.\ ((\text{parent}(x, y) \land male(x)) \rightarrow father(x, y))$
2. $\text{parent}(Tom, Evan)$
3. $\text{male}(Tom)$



## Example 4

Prove the validity of the following formula:

$$((\forall x.P(x)) \land (\forall x.Q(x))) \rightarrow (\forall x.(P(x) \land Q(x)))$$

## Example 5

Is the following formula valid, unsatisfiable, or contingent?

$$(\forall x.(P(x) \lor Q(x))) \to (\forall x.P(x) \lor \forall x.Q(x))$$



## Example 5, cont.

What's wrong with the following "proof" of validity?

1. $(\forall x.(P(x) \lor Q(x))) \land \neg(\forall x.P(x) \lor \forall x.Q(x))$ premise
2. $(\forall x.(P(x) \lor Q(x)))$ $\land$-elim, 1
3. $\neg(\forall x.P(x) \lor \forall x.Q(x))$ $\land$-elim, 1
4. $\exists x.\neg P(x) \land \exists x.\neg Q(x)$ De Morgan, 3
5. $\exists x.\neg P(x)$ $\land$-elim, 4
6. $\exists x.\neg Q(x)$ $\land$-elim, 4
7. $\neg P(c)$ $\exists$-inst, 5
8. $\neg Q(c)$ $\exists$-inst, 6
9. $P(c) \lor Q(c)$ $\forall$-inst, 2
10. $Q(c)$ $\lor$-elim, 9, 7
11. $Q(c) \land \neg Q(c)$ $\land$-intro, 10, 8



## Introduction to Mathematical Proofs

- Formalizing statements in logic allows formal, machine-checkable proofs
- But these kinds of proofs can be very long and tedious
- In practice, humans write slight 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: $p \to q$ proved by directly showing that if $p$ is true, then $q$ must follow
- Proof by contraposition: Prove $p \to q$ by proving $\neg q \to \neg p$
- 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 $p \to q$ 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. $\square$



## 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 $p \to q$ 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 $p \to q$ is true by proving unsatisfiability of its negation
- What is negation of $p \to q$?
- 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.
- 
- 
- 
- 



## Example, cont

- 
- 
- 
- 



## 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 $q \to p$ and $r \to p$, 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

$$(p_1 \vee p_2 \ldots \vee p_k) \to q$$

it suffices to show:

$$p_1 \to q$$
$$p_2 \to q$$
$$\ldots$$
$$p_k \to q$$



## 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

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

## 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 $\sqrt{2}\frac{r}{\sqrt{2}}$
- We already proved $\sqrt{2}$ is irrational.
- If we can show that $\frac{r}{\sqrt{2}}$ 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 $Q$" $(P \leftrightarrow Q)$
- 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 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 $n^3$ 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
- 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 contructive – 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, $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$. 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: $p \to q$ proved by directly showing that if $p$ is true, then $q$ must follow
- Proof by contraposition: Prove $p \to q$ by proving $\neg q \to \neg p$
- 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: $\forall \alpha \in \theta \exists \beta \in \alpha \diamond \beta \approx \gamma$
- 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: "sdjikfhiugyhjlaks??fskl; QED."

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