
csci54 – discrete math & functional programming
more logic, introduction to proofs

last time

- ▶ propositional logic:
 - ▶ practice with logical equivalence
- ▶ introduction to predicate logic:
 - ▶ definition of a predicate
 - ▶ quantifiers: forall, exists
 - ▶ theorems in predicate logic



from last time

- ▶ Exactly one of the following two propositions is a theorem.
Which one?

$$(1) \quad [\forall x \in S : P(x) \vee Q(x)] \Leftrightarrow [\forall x \in S : P(x)] \vee [\forall x \in S : Q(x)]$$

$$(2) \quad [\exists x \in S : P(x) \vee Q(x)] \Leftrightarrow [\exists x \in S : P(x)] \vee [\exists x \in S : Q(x)]$$

- ▶ (2) is the theorem.
- ▶ Prove that your answer is correct.
 - ▶ What is a proof?
 - ▶ A convincing argument that something is true.



Solution. Claim (B) is a theorem. To prove it, we'll show that the left-hand side implies the right-hand side, and vice versa. (That is, we're proving $p \Leftrightarrow q$ by proving both $p \Rightarrow q$ and $q \Rightarrow p$, which is a legitimate proof because $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$.) Both proofs will use the technique of assuming the antecedent.

First, let's prove that $[\exists x \in S : P(x) \vee Q(x)]$ implies $[\exists x \in S : P(x)] \vee [\exists x \in S : Q(x)]$:

Suppose that $[\exists x \in S : P(x) \vee Q(x)]$ is true. Then there is some particular $x^* \in S$ for which either $P(x^*)$ or $Q(x^*)$. But in either case, we're done: if $P(x^*)$ then $\exists x \in S : P(x)$ because x^* satisfies the condition; if $Q(x^*)$ then $\exists x \in S : Q(x)$, again because x^* satisfies the condition.

Second, let's prove that $[\exists x \in S : P(x)] \vee [\exists x \in S : Q(x)]$ implies $[\exists x \in S : P(x) \vee Q(x)]$:

Suppose that $[\exists x \in S : P(x)] \vee [\exists x \in S : Q(x)]$ is true. Thus either there's an $x^* \in S$ such that $P(x^*)$ or an $x^* \in S$ such that $Q(x^*)$. That x^* suffices to make the left-hand side of (B) true.

-
- ▶ What makes something "a convincing argument"?



some definitions

- ▶ an integer k is even if and only if there exists an integer r such that $k=2r$
- ▶ an integer k is odd if and only if there exists an integer r such that $k=2r+1$
- ▶ $k|m$ if and only if there exists an integer r such that $m=kr$. This is equivalent to saying that " $m \bmod k = 0$ " or that " k evenly divides m ".
- ▶ an integer $k>1$ is prime if the only positive integers that evenly divide k are 1 and k itself.
- ▶ an integer $k>1$ is composite if it is not prime.
- ▶ an integer k is a perfect square if and only if there exists an integer r such that $k=r^2$



example 1

- ▶ Consider the statement "for all positive integers n , $2n=n^2$ "
 - ▶ Why isn't this true?
 - ▶ Consider $n = 3$
 - ▶ Why is this a valid justification?

- ▶ How would you write this as a statement in predicate logic?
$$\forall n \in \mathbb{Z}^+ : 2n = n^2$$
 - ▶ Showing that this statement is not true is the same as showing that its negation is true.



negating quantifiers

- ▶ The following are both theorems

$$\neg[\forall x \in S : P(x)] \Leftrightarrow [\exists x \in S : \neg P(x)]$$

$$\neg[\exists x \in S : P(x)] \Leftrightarrow [\forall x \in S : \neg P(x)]$$

- ▶ practice: what is the negation of the following? simplify as much as possible.

$$\exists x \in S : P(x) \vee Q(x)$$

example 1 - revisited

- ▶ Consider the statement "for all positive integers n , $2n=n^2$ "
- ▶ How would you prove that this statement is false?
 - ▶ Consider the following counterexample. If $n=3$, then $2n=6$ and $n^2=9$.
 - ▶ Since there exists a positive integer such that $2n \neq n^2$, the original statement is false.



example 2

- ▶ Claim: let x be any integer. if x is a perfect square, then $4x$ is a perfect square
- ▶ How could you write the claim as a statement in predicate logic?
- ▶ How would you prove the claim is true?
- ▶ Why is this justification valid?



assuming the antecedent, modus ponens

- ▶ assuming the antecedent.
 - ▶ to show "if a then b", only need to show that if a is true, then b is true.
- ▶ two tautologies that are used repeatedly in proofs through a chain of reasoning.

$$(p \Rightarrow q) \wedge p \Rightarrow q \quad \text{Modus Ponens}$$

$$(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p \quad \text{Modus Tollens}$$



example 2 - revisited

- ▶ Claim: let x be any integer. if x is a perfect square, then $4x$ is a perfect square

- ▶ How would you prove the claim is true?
 - ▶ assume x is a perfect square (assuming the antecedent)
 - ▶ then there exists an integer r such that $x = r^2$ (definition of perfect square, modus ponens)
 - ▶ then $4x = 4r^2 = (2r)^2$ (algebra)
 - ▶ therefore $4x$ is a perfect square (definition of perfect square)
 - ▶ in conclusion, for any integer x , if x is a perfect square then $4x$ is a perfect square.





Nested quantifiers

- ▶ Let A be an array of n integers with 1-based indexing. What is the following asserting?

$$\forall i \in \{1, 2, \dots, n\} : [\exists j \in \{1, 2, \dots, n\} : (i \neq j) \wedge (A[i] = A[j])]$$

- ▶ How could you write the following using nested quantifiers?

Every program that was turned in failed at least one test case.



Nested quantifiers - questions

- ▶ What are the rules with nested quantifiers?
- ▶ Can you flip the order of nested quantifiers?
- ▶ What happens if you negate a nested quantifier?



Nested quantifiers – order sometimes matters

- ▶ Exactly one of the following is true. Which? Why?

$$\exists y \in \mathbb{R} : \forall x \in \mathbb{R} : x < y$$

$$\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x < y$$

- ▶ However, if two or two, can flip order. Following are both theorems

$$\forall x \in S : \forall y \in T : P(x, y) \Leftrightarrow \forall y \in T : \forall x \in S : P(x, y)$$

$$\exists x \in S : \exists y \in T : P(x, y) \Leftrightarrow \exists y \in T : \exists x \in S : P(x, y)$$



Negating nested quantifiers

- ▶ Consider the following statement:

$$\forall i \in \{1, 2, \dots, n\} : [\exists j \in \{1, 2, \dots, n\} : (i \neq j) \wedge (A[i] = A[j])]$$

- ▶ Simplify the negation:

- ▶ $\neg \forall i \in \{1, 2, \dots, n\} : [\exists j \in \{1, 2, \dots, n\} : (i \neq j) \wedge (A[i] = A[j])]$

