CMSC 250: Discrete Structures
Summer 2017

Lecture 5 - Outline

June 6, 2017

Proofs and an Introduction to Relations

Negating Quantifiers

In order to negate a quantified statement, the rule is to replace universal quantification ($\forall$) with existential quantification ($\exists$), replace existential quantification ($\exists$) with universal quantification ($\forall$), and finally negate the predicate that is being quantified.

To be explicit:

$$\neg(\forall x \in D, P(x)) \equiv \exists x \in D, \neg P(x)$$
$$\neg(\exists x \in D, P(x)) \equiv \forall x \in D, \neg P(x)$$
$$\neg(\forall x \in D, \forall y \in E, P(x,y)) \equiv \exists x \in D, \exists y \in E, \neg P(x,y)$$
$$\neg(\forall x \in D, \exists y \in E, P(x,y)) \equiv \exists x \in D, \forall y \in E, \neg P(x,y)$$
$$\neg(\exists x \in D, \forall y \in E, P(x,y)) \equiv \forall x \in D, \exists y \in E, \neg P(x,y)$$
$$\neg(\exists x \in D, \exists y \in E, P(x,y)) \equiv \forall x \in D, \forall y \in E, \neg P(x,y)$$

For example:

$$\neg(\forall x \in \mathbb{Z}, x+5=7) \equiv \exists x \in \mathbb{Z}, x+5 \neq 7$$
$$\neg(\exists x \in \text{Horses},\ x \text{ is red }) \equiv \forall x \in \text{Horses},\ x \text{ is not red}$$
$$\neg(\forall x \in Z, \exists y \in \mathbb{Z}, x+1=y) \equiv \exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x+1 \neq y$$
$$\neg(\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, xy=\sqrt{2}) \equiv \forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy=\sqrt{2}$$

This comes in handy when thinking about disproving claims. A claim must be true, or its negation is true. Therefore, in order to prove that a claim is false (*disprove* a claim), you must show that its negation is true.

For example, let's say that we are trying to disprove the claim that $\forall x \in \mathbb{Z}, x + 5 = 7$. We need to show that its negation is true. From the above example, we can see that the negation of the claim is $\exists x \in \mathbb{Z}, x + 5 \neq 7$. So, in order to prove the negation of the claim, we just need to show that there exists some integer x such that $x + 5 \neq 7$. One such integer that can be used is 1. We call 1 a counterexample to the claim.

Prove: Prove that there are infinitely many prime numbers.

Solution: Assume, for the sake of contradiction, that there are only finitely many primes. Since there are a finite number of primes, there must be a largest prime number. Let p be the largest prime number. Then all the prime numbers can be listed as

$$2, 3, 5, 7, 11, 13, \ldots, p$$

Consider an integer n that is formed by multiplying all the prime numbers together. That is,

$$n = (2 \times 3 \times 5 \times 7 \times \cdots p)$$

Let us consider $n+1$. Clearly, $n+1>p$. Since p is the largest prime number, $n+1$ cannot be a prime number. In other words, n is composite.

Let q be any arbitrary prime number. Because of the way we have constructed n, q cannot be a factor of $n+1$ since we can express $n+1 = q \times (2 \times 3 \times \cdots \times p) + 1$. That is, $n+1$ is not a multiple of q. This contradicts the Fundamental Theorem of Arithmetic, since it states that any integer can be uniquely represented as a product of primes.

Floors and Ceilings

Given any real number x, the **floor** of x, denoted by $\lfloor x \rfloor$, is defined as follows

$$\lfloor x \rfloor = n \leftrightarrow n \leq x < n+1 \wedge n \in \mathbb{Z}$$

Given any real number x, the **ceiling** of x, denoted by $\lceil x \rceil$, is defined as follows

$$\lceil x \rceil = n \leftrightarrow n-1 < x \leq n \wedge n \in \mathbb{Z}$$

Prove: Prove that, for all real numbers x and all integers m,

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

The challenge of this proof is that we do not yet have an expression for $\lfloor x \rfloor$ that is easy to manipulate. We propose the following expression:

For any $x \in \mathbb{R}$, we can express $x = \lfloor x \rfloor + \epsilon$, where $0 \leq \epsilon < 1$.

Solution: Let $x = y + \epsilon$, where $y = \lfloor x \rfloor$ and $0 \leq \epsilon < 1$. Then,

$$\begin{aligned}
x + m &= y + \epsilon + m \\
\lfloor x + m \rfloor &= \lfloor y + m + \epsilon \rfloor \\
&= y + m \\
&= \lfloor x \rfloor + m
\end{aligned}$$

Proving a bi-conditional

In order to prove a bi-conditional (iff) statement $p \leftrightarrow q$, we should prove $p \rightarrow q$ and prove $q \rightarrow p$. By proving this, we have proved $p \leftrightarrow q$.

We can do this since $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$. We can prove this logical equivalence with the following truth table.

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	F	F	F
F	T	F	T	T	F
F	F	T	T	T	T

Prove: Prove that for all integers x and y, xy is odd iff x is odd and y is odd.

Solution: To prove that claim, we need to prove both directions:

1. If x is odd and y is odd, then xy is odd.
2. If xy is odd, then x is odd and y is odd.

Let us prove the first claim. Let x and y be arbitrary odd numbers. Then, $x = 2k + 1$ and $y = 2l + 1$, for some integers k and l. We have

$$\begin{aligned} x \cdot y =& (2k + 1) \cdot (2l + 1) \\ =& 4kl + 2(k + l) + 1 \\ =& 2(2kl + k + l) + 1 \end{aligned}$$

Let $p = 2kl + k + l$. Since k and l are integers, p is an integer and $x \cdot y = 2p + 1$ is odd.

Let us prove the second claim. We choose a proof by contrapositive, i.e. we choose to prove that "If x is even or y is even, then xy is even.".

We have two cases to consider here:

Case 1: x and y are both even

Let x and y be arbitrary even integers. By definition, $x = 2k$ and $y = 2\ell$ for some $k, \ell \in \mathbb{Z}$.

$$\begin{aligned} xy =& (2k)(2\ell) \\ =& 4k\ell \\ =& 2(2k\ell) \end{aligned}$$

Let $m = 2k\ell$. Since $xy = 2m$ for some $m \in \mathbb{Z}$, it is even by definition.

Case 2: exactly one of x and y is even

With loss of generality, let x be the one that is even and y be the one that is odd. By definition, $x = 2k$ and $y = 2\ell + 1$, for some $k, \ell \in \mathbb{Z}$.

$$\begin{aligned} xy =& (2k)(2\ell + 1) \\ =& 4k\ell + 2k \\ =& 2(2k\ell + k) \end{aligned}$$

Let $m = 2k\ell + k$. Since $xy = 2m$ for some $m \in \mathbb{Z}$, it is even by definition.

Since we have proven both claims (both directions), we have proven the original claim.

Relations

A *binary relation* is a set of ordered pairs. For example, let $R = \{(1,2), (2,3), (5,4)\}$. Then since $(1,2) \in R$, we say that 1 is related to 2 by relation R. We denote this by $1\,R\,2$. Similarly, since $(4,7) \notin R$, 4 is not related to 7 by relation R, denoted by $4 \not R\, 7$.

A binary relation R from set A to set B is a subset of the cartesian product $A \times B$. When $A = B$ (i.e. $R \subseteq A \times A$), we say that R is a relation on set A.

Below are some more examples of relations.

- "is a student in" is a relation from the set of students to the set of courses.
- "has a crush on" is a relation on the set of people in this world
- "$=$" is a relation on $\mathbb{Z}$
- "$\lfloor x \rfloor$" is a relation from the set of real numbers to the set of integers

Properties of Relations

Let R be a relation defined on set A. We say that R is

- *reflexive*, if for all $x \in A$, $(x, x) \in R$.
- *irreflexive*, if for all $x \in A$, $(x, x) \notin R$.
- *symmetric*, if for all $x, y \in A$, $(x, y) \in R \implies (y, x) \in R$.
- *antisymmetric*, if for all $x, y \in A$, $x\,R\,y$ and $y\,R\,x \implies x = y$.
- *transitive*, if for all $x, y, z \in A$, $x\,R\,y$ and $y\,R\,z \implies x\,R\,z$.

Note that the terms *reflexive* and *irreflexive* are not opposites. Similarly, note that the terms *symmetric* and *antisymmetric* are not opposites. A relation may be both symmetric and antisymmetric or can neither be symmetric nor be antisymmetric.

Catalog of LaTeX Commands

$\lfloor x \rfloor$ - `\lfloor x \rfloor`