This week's highlights

- Determine what evidence is required to establish that a quantified statement is true or false.
- Use logical equivalence to rewrite quantified statements (including negated quantified statements)
- Use universal generalization to prove that universal statements are true
- Define predicates associated with integer factoring and primes
- Define "arbitrary"
- Add to repertoire of proof strategies
- Identify the main connective of a proposition and associated proof strategies
- Determine whether a proposition is true or false using valid reasoning (proofs) in multiple contexts

Lecture videos

Week 5 Day 1 YouTube playlist
Week 5 Day 2 YouTube playlist
Week 5 Day 3 YouTube playlist

Monday February 1

When a predicate $P(x)$ is over a **finite** domain:

- To prove that $\forall x P(x)$ is true: _____
- To prove that $\forall x P(x)$ is false: _____
- To prove that $\exists x P(x)$ is true: _____
- To prove that $\exists x P(x)$ is false: _____

Proof of universal by exhaustion: To prove that $\forall x\, P(x)$ is true when P has a finite domain, evaluate the predicate at **each** domain element to confirm that it is always T.

Some sets of numbers

$\mathbb{N}$	The set of natural numbers	$\{0, 1, 2, 3, \ldots\}$	*Recursively defined by* Basis step: Recursive step:
$\mathbb{Z}$	The set of integers	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$	*Recursively defined by* Basis step: Recursive step:
$\mathbb{Z}^+$	The set of positive integers	$\{1, 2, 3, \ldots\}$	*Set builder notation definition is* $\{x \in \mathbb{N} \mid x > 0\} = \{x \in \mathbb{Z} \mid x > 0\}$
$\mathbb{Z}^{\neq 0}$	The set of nonzero integers		*Set builder notation definition is* $\{x \in \mathbb{Z} \mid (x < 0 \vee x > 0)\}$

Factoring

Definition (Rosen p. 238): When a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$.

Symbolically, $F(a, b)$ = _____ and is a predicate over the domain _____

Other (synonymous) ways to say that $F(a, b)$ is true:

a is a **factor** of b a is a **divisor** of b b is a **multiple** of a $a|b$ b **mod** $a = 0$

Translate these quantified statements by matching to English statement on right.

$\exists a \in \mathbb{Z}^{\neq 0}$ ($F(a, a)$)	No nonzero integer is a factor of itself.
$\exists a \in \mathbb{Z}^{\neq 0}$ ($\neg F(a, a)$)	
$\forall a \in \mathbb{Z}^{\neq 0}$ ($F(a, a)$)	At least one nonzero integer is a factor of itself.
$\forall a \in \mathbb{Z}^{\neq 0}$ ($\neg F(a, a)$)	
Every nonzero integer is a factor of itself.	Some nonzero integer is not a factor of itself.

Claim: Every nonzero integer is a factor of itself.
Proof:

Claim: The statement "There is a nonzero integer that does not divide its square." is True / False *Circle one*
Proof:

New! Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.
An **arbitrary** element of a set or domain is a fixed but unknown element from that set.

Definition (Rosen p. 257): An integer p greater than 1 is called **prime** means the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

A formal definition of the predicate Pr over the domain $\mathbb{Z}$ which evaluates to T exactly when the input is prime is:

Claim: 1 is not prime.
Proof:

Claim: 4 is not prime.
Proof:

$(p \rightarrow q) \equiv \neg(p \wedge \neg q)$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$ $q \vee \neg p \equiv p \rightarrow q$ $\neg\exists x\, P(x) \equiv \forall x\, \neg(P(x))$

To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.

To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.

To prove that $p \wedge q$ is false, it's enough to prove that p is false.
To prove that $p \wedge q$ is false, it's enough to prove that q is false.

Wednesday February 3

Recall the predicate $F(a, b) = \exists c \in \mathbb{Z}\ (b = ac)$ is a predicate over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$. In English, $F(a, b)$ evaluates to T means a is a nonzero integer, b is an integer, and a is a factor of b. An equivalent definition is that $F(a, b) = T$ exactly when b **mod** $a = 0$.

Definition (Rosen p. 257): An integer p greater than 1 is called **prime** means the only positive factors of p are 1 and p. We write $Pr(x)$ to indicate that an positive integer x is prime. A positive integer that is greater than 1 and is not prime is called composite.

Trial Division: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Claim: The statement "There are three consecutive positive integers that are prime." is True / False

Hint: These numbers would be of the form $p, p + 1, p + 2$ (where p is a positive integer).

Proof: We need to show _____

Claim: The statement "There are three consecutive odd positive integers that are prime." is True / False

Hint: These numbers would be of the form $p, p + 2, p + 4$ (where p is an odd positive integer).

Proof: We need to show _____

Proof of universal by exhaustion: To prove that $\forall x\, P(x)$ is true when P has a finite domain, evaluate the predicate at **each** domain element to confirm that it is always T.

Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.

To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.

To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.

To prove that $p \wedge q$ is false, it's enough to prove that p is false.
To prove that $p \wedge q$ is false, it's enough to prove that q is false.

Each Netflix user's viewing history can be represented as a n-tuple indicating their preferences about movies in the database, where n is the number of movies in the database. Each element in the n-tuple indicates the user's rating of the corresponding movie: 1 indicates the person liked the movie, -1 that they didn't, and 0 that they didn't rate it one way or another. Consider a four movie database. Recall the Netflix example from class: Consider a four movie database. We denote the set of possible ratings $\{-1, 0, 1\} \times \{-1, 0, 1\} \times \{-1, 0, 1\} \times \{-1, 0, 1\}$ as R_4. We have the functions

$$d_{1,4}(\ (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)\ ) = \sum_{i=1}^{4} ((|\ x_i - y_i\ | + 1)\ \mathbf{div}\ 2)$$

$$d_{2,4}(\ (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)\ ) = \sqrt{\sum_{i=1}^{4} (x_i - y_i)^2}$$

Claim: The statement "$\forall r_1 \in R_4\ \forall r_2 \in R_4\ (\ r_1 = r_2 \rightarrow \neg\ (d_{1,4}(r_1, r_2) < d_{2,4}(r_1, r_2))\ )$" is True / False

The statement in English: _____

Claim: The statement "$\forall r_1 \in R_4\ \forall r_2 \in R_4\ (\ d_{1,4}(r_1, r_2) < d_{2,4}(r_1, r_2)\ )$" is True / False

The statement in English: _____

Friday February 5

Term	Definition	Examples
set	an unordered collection of elements	
set equality	When A and B are sets, $A = B$ means $\forall x(x \in A \leftrightarrow x \in B)$	$\{43, 7, 9\} = \{7, 43, 9, 7\}$ $\left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\right\} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q$
subset	When A and B are sets, $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$	
proper subset	When A and B are sets, $A \subsetneq B$ means $(A \subseteq B) \wedge (A \neq B)$	

Claim: $\{\texttt{A}, \texttt{C}, \texttt{U}, \texttt{G}\} \subseteq \{\texttt{AA}, \texttt{AC}, \texttt{AU}, \texttt{AG}\}$ **Prove** or **disprove** *Circle one*

Claim: $\{4, 6\} \subseteq \{n \textbf{ mod } 10 \mid \exists c \in \mathbb{Z}(n = 4c)\}$ **Prove** or **disprove** *Circle one*

Claim: The empty set is a proper subset of every set. **Prove** or **disprove** *Circle one*

Claim: For some set B, $\emptyset \in B$. **Prove** or **disprove** *Circle one*

Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.

Evidence for conjunction being true or false:
To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.
To prove that $p \wedge q$ is false, it's enough to prove that p is false.
To prove that $p \wedge q$ is false, it's enough to prove that q is false.

New! Proof by Cases: To prove q, if we know that $p_1 \vee p_2$ is true, and we can show that $(p_1 \rightarrow q)$ is true and we can show that $(p_2 \rightarrow q)$, then we can conclude q is true. Sec 1.8 p92

Term	Definition	Examples
Cartesian product	When A and B are sets, $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$	$\{43, 9\} \times \{9, A\} =$ $\mathbb{Z} \times \emptyset =$
union	When A and B are sets, $A \cup B = \{x \mid x \in A \vee x \in B\}$	$\{43, 9\} \cup \{9, A\} =$ $\mathbb{Z} \cup \emptyset =$
intersection	When A and B are sets, $A \cap B = \{x \mid x \in A \wedge x \in B\}$	$\{43, 9\} \cap \{9, A\} =$ $\mathbb{Z} \cap \emptyset =$
set difference	When A and B are sets, $A - B = \{x \mid x \in A \wedge x \notin B\}$	$\{43, 9\} - \{9, A\} =$ $\mathbb{Z} - \emptyset =$
disjoint sets	sets A and B are disjoint means $A \cap B = \emptyset$	$\{43, 9\}, \{9, A\}$ are not disjoint $\mathbb{Z}, \emptyset$ are disjoint
power set	When S is a set, $\mathcal{P}(S) = \{X \mid X \subseteq S\}$	$\mathcal{P}(\{43, 9\}) =$ $\mathcal{P}(\emptyset) =$

Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\}) =$ _____

Prove or **disprove**: $\forall A \in W \, \forall B \in W \; (A \subseteq B \; \rightarrow \; \mathcal{P}(A) \subseteq \mathcal{P}(B))$

Extra example: **Prove** or **disprove**: $\forall A \in W \, \forall B \in W \; (\mathcal{P}(A) = \mathcal{P}(B) \; \rightarrow \; A = B)$

Extra example: **Prove** or **disprove**: $\forall A \in W \, \forall B \in W \, \forall C \in W \; (A \cup B = A \cup C \; \rightarrow \; B = C)$

New! Proof of conditional by direct proof: To prove that the conditional statement $p \rightarrow q$ is true, we can assume p is true and use that assumption to show q is true.
New! Proof of Conditional by Contrapositive Proof: To prove that the implication $p \rightarrow q$ is true, we can assume q is false and use that assumption to show p is also false. Sec 1.7 p83

Review quiz questions

1. **Monday** Consider the predicate $F(a, b) =$ "a is a factor of b" over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$. Consider the following quantified statements

   (i) $\forall x \in \mathbb{Z}\ (F(1, x))$
   (ii) $\forall x \in \mathbb{Z}^{\neq 0}\ (F(x, 1))$
   (iii) $\exists x \in \mathbb{Z}\ (F(1, x))$
   (iv) $\exists x \in \mathbb{Z}^{\neq 0}\ (F(x, 1))$
   (v) $\forall x \in \mathbb{Z}^{\neq 0}\ \exists y \in \mathbb{Z}\ (F(x, y))$
   (vi) $\exists x \in \mathbb{Z}^{\neq 0}\ \forall y \in \mathbb{Z}\ (F(x, y))$
   (vii) $\forall y \in \mathbb{Z}\ \exists x \in \mathbb{Z}^{\neq 0}\ (F(x, y))$
   (viii) $\exists y \in \mathbb{Z}\ \forall x \in \mathbb{Z}^{\neq 0}\ (F(x, y))$

   (a) Select the statement whose translation is

   > "The number 1 is a factor of every integer."

   or write NONE if none of (i)-(viii) work.

   (b) Select the statement whose translation is

   > "Every integer has at least one nonzero factor."

   or write NONE if none of (i)-(viii) work.

   (c) Select the statement whose translation is

   > "There is an integer of which all nonzero integers are a factor."

   or write NONE if none of (i)-(viii) work.

   (d) For each statement (i)-(viii), determine if it is true or false.

2. **Wednesday** Suppose $P(x)$ is a predicate over a domain D.

   (a) True or False: To translate the statement "There are at least two elements in D where the predicate P evaluates to true", we could write

   $$\exists x_1 \in D\, \exists x_2 \in D\, (P(x_1) \wedge P(x_2))$$

   (b) True or False: To translate the statement "There are at most two elements in D where the predicate P evaluates to true", we could write

   $$\forall x_1 \in D\, \forall x_2 \in D\, \forall x_3 \in D\ (\ (\ P(x_1) \wedge P(x_2) \wedge P(x_3)\ ) \rightarrow (\ x_1 = x_2 \vee x_2 = x_3 \vee x_1 = x_3$$

3. **Friday** Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. Which of the following are true about W? (Select all and only that apply.)

(a) $\emptyset \in W$

(b) $\emptyset \subseteq W$

(c) $\emptyset \subsetneq W$

(d) $\{1,2,3,4,5\} \in W$

(e) $\{1,2,3,4,5\} \subseteq W$

(f) $\{1,2,3,4,5\} \subsetneq W$

4. **Friday** Recall the Netflix example from class: Consider a four movie database. We denote the set of possible ratings $\{-1,0,1\}\times\{-1,0,1\}\times\{-1,0,1\}\times\{-1,0,1\}$ as R_4. We have the functions

$$d_{1,4}(\ (x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4)\ ) = \sum_{i=1}^{4}((|\ x_i - y_i\ | + 1)\ \textbf{div}\ 2)$$

$$d_{2,4}(\ (x_1,x_2,x_3,x_4),(y_1,y_2,y_3,y_4)\ ) = \sqrt{\sum_{i=1}^{4}(x_i-y_i)^2}$$

Claim: $\forall r_1 \in R_4\ \forall r_2 \in R_4\ (\ r_1 = r_2 \rightarrow \neg\,(d_{1,4}(r_1,r_2) < d_{2,4}(r_1,r_2))\ )$

Select the correct choice to fill in the blanks in the following proof of the claim.

Proof: Towards universal generalization, let e_1 be **Blank (a)** element of R_4 and let e_2 be **Blank (a)** element of R_4. We need to show that $e_1 = e_2 \rightarrow \neg((d_{1,4}(e_1,e_2) < d_{2,4}(e_1,e_2))\ )$. Towards a **Blank (b)**, we assume $e_1 = e_2$ and we need to prove that $\neg((d_{1,4}(e_1,e_2) < d_{2,4}(e_1,e_2))\ )$. Calculating, $d_{1,4}(e_1,e_2) = d_{1,4}(e_1,e_1)$ by assumption that e_1 and e_2 are equal, and therefore (since each element in the summation in the definition of $d_{1,4}$ will be 0 because it is the quotient of 1 upon division by 2, since the absolute value of the difference of a number with itself is 0), $d_{1,4}(e_1,e_2) = 0$. Similarly, $d_{2,4}(e_1,e_2) = d_{2,4}(e_1,e_1)$ by assumption, and therefore (since each term in the sum in the definition of $d_{2,4}$ will be 0 because it is the square of the difference of a number with itself), $d_{2,4}(e_1,e_2) = 0$. Thus, $d_{1,4}(e_1,e_2) = d_{2,4}(e_1,e_2)$ so $d_{1,4}(e_1,e_2) < d_{2,4}(e_1,e_2)$ is False. By definition of negation, $\neg(d_{1,4}(e_1,e_2) < d_{2,4}(e_1,e_2))$ is true, as required. Thus the direct proof is complete and we have proved that the predicate being claimed to be universally true is true for an arbitrary element. This means the universal generalization is also complete, and the proof is done. $\square$

For Blank (a):

i. a counterexample

ii. a witness

iii. an arbitrary

For Blank (b)

i. universal generalization

ii. exhaustion

iii. direct proof

iv. proof by cases

5. **Friday** Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. The statement

$$\forall A \in W \ \forall B \in W \ \forall C \in W \ (A \cup B = A \cup C \ \rightarrow \ B = C)$$

is false. Which of the following choices for A, B, C could be used to give a counterexample to this claim? (Select all and only that apply.)

(a) $A = \{1, 2, 3\}, B = \{1, 2\}, C = \{1, 3\}$

(b) $A = \{\emptyset, 1, 2, 3\}, B = \{1, 2\}, C = \{1, 3\}$

(c) $A = \{1, 2, 3\}, B = \{1, 2\}, C = \{1, 4\}$

(d) $A = \{1, 2\}, B = \{2, 3\}, C = \{1, 3\}$

(e) $A = \{1, 2\}, B = \{1, 3\}, C = \{1, 3\}$

6. **Friday** Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$. Consider the statement

$$\forall A \in W \ \forall B \in W \ \big((\mathcal{P}(A) = \mathcal{P}(B)) \ \rightarrow \ (A = B)\big)$$

This statement is true. A proof of this statement starts with universal generalization, considering arbitrary A and B in W. At this point, it remains to prove that $(\mathcal{P}(A) = \mathcal{P}(B)) \ \rightarrow \ (A = B)$ is true about these arbitrary elements. There are two ways to proceed:

> First approach: By direct proof, in which we assume the hypothesis of the conditional and work to show that the conclusion follows.
>
> Second approach: By proving the contrapositive version of the conditional instead, in which we assume the negation of the conclusion and work to show that the negation of hypothesis follows.

Pick an option from below for the assumption and "need to show" in each approach.

(a) First approach, assumption.

(b) First approach, "need to show".

(c) Second approach, assumption.

(d) Second approach, "need to show".

(i) $\forall X(X \subseteq A \leftrightarrow X \subseteq B)$

(ii) $\exists X(X \subseteq A \leftrightarrow X \subseteq B)$

(iii) $\forall X(X \subseteq A \oplus X \subseteq B)$

(iv) $\exists X(X \subseteq A \oplus X \subseteq B)$

(v) $\forall x(x \in A \leftrightarrow x \in B)$

(vi) $\exists x(x \in A \leftrightarrow x \in B)$

(vii) $\forall x(x \in A \oplus x \in B)$

(viii) $\exists x(x \in A \oplus x \in B)$