Monday October 25

Proof strategies

We now have propositional and predicate logic that can help us express statements about any domain. We will develop proof strategies to craft valid argument for proving that such statements are true or disproving them (by showing they are false). We will practice these strategies with statements about sets and numbers, both because they are familiar and because they can be used to build cryptographic systems. Then we will apply proof strategies more broadly to prove statements about data structures and machine learning applications.

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

- To show that $\forall x P(x)$ is true: check that $P(x)$ evaluates to T at each domain element by evaluating over and over.
- To show that $\forall x P(x)$ is false: find one counterexample, a domain element where $P(x)$ evaluates to F.
- To show that $\exists x P(x)$ is true: find one witness, a domain element where $P(x)$ evaluates to T.
- To show that $\exists x P(x)$ is false: check that $P(x)$ evaluates to F at each domain element by evaluating over and over.

New! **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.

New! Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain of quantification 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.

Definitions:

A **set** is an unordered collection of elements. When A and B are sets, $A = B$ (set equality) means

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

When A and B are sets, $A \subseteq B$ ("A is a **subset** of B") means

$$\forall x(x \in A \rightarrow x \in B)$$

When A and B are sets, $A \subsetneq B$ ("A is a **proper subset** of B") means

$$(A \subseteq B) \wedge (A \neq B)$$

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.

New! Proof of disjuction using equivalent conditional: To prove that the disjunction $p \vee q$ is true, we can rewrite it equivalently as $\neg p \rightarrow q$ and then use direct proof or contrapositive proof.

New! Proof by Cases: To prove q, we can work by cases by first describing all possible cases we might be in and then showing that each one guarantees q. Formally, 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.

New! Proof of conjunctions with subgoals: To show that $p \wedge q$ is true, we have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.

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

To prove that one set is a subset of another, e.g. to show $A \subseteq B$:

To prove that two sets are equal, e.g. to show $A = B$:

Example: $\{43, 7, 9\} = \{7, 43, 9, 7\}$

Prove or **disprove**: $\{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\} \subseteq \{\mathtt{AA}, \mathtt{AC}, \mathtt{AU}, \mathtt{AG}\}$

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

Prove or **disprove**: For every set B, $\emptyset \in B$.

Prove or **disprove**: The empty set is a subset of every set.

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

Prove or **disprove**: $\{4, 6\} \subseteq \{n \mid \exists c \in \mathbb{Z}(n = 4c)\}$

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

Consider ..., an **arbitrary** .... **Assume** ..., we **want to show** that .... Which is what was needed, so the proof is complete $\square$.

or, in other words:

Let ... be an **arbitrary** .... **Assume** ..., **WTS** that ... **QED**.

Review

1.

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

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

2.

For each of the following English statements, select the correct translation, or select None.

Challenge: determine which of the statements are true and which are false.

(a) Every set is a subset of itself.

(b) Every set is an element of itself.

(c) Some set is an element of all sets.

(d) Some set is a subset of all sets.

i. $\forall X\ \exists Y\ (X \in Y)$

ii. $\exists X\ \forall Y\ (X \in Y)$

iii. $\forall X\ \exists Y\ (X \subseteq Y)$

iv. $\exists X\ \forall Y\ (X \subseteq Y)$

v. $\forall X\ (X \in X)$

vi. $\forall X\ (X \subseteq X)$

3. We want to hear how the term and this class are going for you. Please complete the midquarter feedback form: https://forms.gle/w3D7ifAWnD5sWwHf9

Wednesday October 27

Cartesian product: When A and B are sets,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Example: $\{43, 9\} \times \{9, \mathbb{Z}\} =$

Example: $\mathbb{Z} \times \emptyset =$

Union: When A and B are sets,

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Example: $\{43, 9\} \cup \{9, \mathbb{Z}\} =$

Example: $\mathbb{Z} \cup \emptyset =$

Intersection: When A and B are sets,

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Example: $\{43, 9\} \cap \{9, \mathbb{Z}\} =$

Example: $\mathbb{Z} \cap \emptyset =$

Set difference: When A and B are sets,

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Example: $\{43, 9\} - \{9, \mathbb{Z}\} =$

Example: $\mathbb{Z} - \emptyset =$

Disjoint sets: sets A and B are disjoint means $A \cap B = \emptyset$

Example: $\{43, 9\}, \{9, \mathbb{Z}\}$ are not disjoint

Example: The sets $\mathbb{Z}$ and $\emptyset$ are disjoint

Power set: When U is a set, $\mathcal{P}(U) = \{X \mid X \subseteq U\}$

Example: $\mathcal{P}(\{43, 9\}) =$

Example: $\mathcal{P}(\emptyset) =$

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

Example elements in W are:

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**: $\forall A \in W \, \forall B \in W \, \forall C \in W \; (A \cup B = A \cup C \;\rightarrow\; B = C)$

Review

1.

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

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

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

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

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

2.

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, c onsidering 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.

(a) First approach, assumption.

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

(c) Second approach, assumption.

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

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

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

Friday October 29

Facts about numbers

1. Addition and multiplication of real numbers are each commutative and associative.

2. The product of two positive numbers is positive, of two negative numbers is positive, and of a positive and a negative number is negative.

3. The sum of two integers, the product of two integers, and the difference between two integers are each integers.

4. For every integer x there is no integer strictly between x and $x+1$,

5. When x, y are positive integers, $xy \geq x$ and $xy \geq y$.

Factoring

Definition: 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 $\quad$ a is a **divisor** of b $\quad$ b is a **multiple** of a $\quad$ $a|b$

When a is a positive integer and b is any integer, $a|b$ exactly when b **mod** $a = 0$

When a is a positive integer and b is any integer, $a|b$ exactly $b = a \cdot (b$ **div** $a)$

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

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

Claim: Every nonzero integer is a factor of itself.

Proof:

Prove or **Disprove**: There is a nonzero integer that does not divide its square.

Prove or **Disprove**: Every positive factor of a positive integer is less than or equal to it.

Claim: Every nonzero integer is a factor of itself and every nonzero integer divides its square.

Definition: an integer n is **even** means that there is an integer a such that $n = 2a$; an integer n is **odd** means that there is an integer a such that $n = 2a + 1$. Equivalently, an integer n is **even** means $n \ \textbf{mod} \ 2 = 0$; an integer n is **odd** means $n \ \textbf{mod} \ 2 = 1$. Also, an integer is even if and only if it is not odd.

Definition: 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.

Extra examples: Use the definition to prove that 1 is not prime, 2 is prime, 3 is prime, 4 is not prime, 5 is prime, 6 is not prime, and 7 is prime.

True or False: The statement "There are three consecutive positive integers that are prime."

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

Proof: We need to show _____

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

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 _____

Review

1.

Recall the predicate $F(\ (a,b)\ )$ = "a is a factor of b" over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$ we worked with in class. 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.

Which of the following formalizes the definition of the predicate $Pr(x)$ over the set of integers, and evaluates to T exactly when x is prime. (Select all and only correct options.)

(a) $\forall a \in \mathbb{Z}^{\neq 0}\ (\ (x > 1 \wedge a > 0) \rightarrow F(\ (a,x)\ ))$

(b) $\neg\exists a \in \mathbb{Z}^{\neq 0}\ (x > 1 \wedge (a = 1 \vee a = x) \wedge F(\ (a,x)\ ))$

(c) $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 0 \wedge F(\ (a,x)\ )\ ) \rightarrow (a = 1 \vee a = x)\ )$

(d) $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 1 \wedge \neg(a = x)\ ) \rightarrow \neg F(\ (a,x)\ )\ )$