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.

Claim: $\forall n \in \mathbb{N}\ (n \geq 0)$

proof strategy

Pf: Towards a universal generalization, let e be an arbitrary element in $\mathbb{N}$. By definition of $\mathbb{N}$, e is an integer and $e \geq 0$, which is what was required ▨

QED

Definitions: Using logic to formalize definition

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

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

Notice: we use $\subseteq$ (not $\subset$) for subset inclusion and we use $\subset$ for proper subset inclusion

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

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

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

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.

not (p is T and q is F)

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 $\neg q$.

want to show

To prove that one set is a subset of another, e.g. to show $A \subseteq B$: WTS $\forall x (x \in A \rightarrow x \in B)$ (HYP: $x \in A$; CONC: $x \in B$)

Let x be arbitrary. Towards a direct proof, assume $x \in A$ and we WTS $x \in B$. ....

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

Let x be arbitrary. WTS $x \in A \leftrightarrow x \in B$.
Equivalently, we WTS $x \in A \rightarrow x \in B$ and $x \in B \rightarrow x \in A$.
Goal ① WTS $x \in A \rightarrow x \in B$ Goal ② WTS $x \in B \rightarrow x \in A$ ...

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

Consider arbitrary x.
Goal ① Assume $x \in \{43, 7, 9\}$. WTS $x \in \{7, 43, 9, 7\}$

By definition of roster method

$x = 43 \vee x = 7 \vee x = 9.$

Proceeding by cases, we have three subgoals.

(1a) WTS $x = 43 \longrightarrow x \in \{7, 43, 9, 7\}$.

Assume, towards a direct proof, that $x = 43$. WTS $x \in \{7, 43, 9, 7\}$, which is true by definition of roster notation for sets.

(1b) WTS $x = 7 \longrightarrow x \in \{7, 43, 9, 7\}$

Assume, towards a direct proof, that $x = 7$. WTS $x \in \{7, 43, 9, 7\}$ which is true by definition of roster notation for sets.

(1c) WTS $x = 9 \longrightarrow x \in \{7, 43, 9, 7\}$.

Assume, towards a direct proof that $x = 9$. WTS $x \in \{7, 43, 9, 7\}$ which is true by definition of roster notation for sets.

Goal ② Assume $x \in \{7, 43, 9, 7\}$ WTS $x \in \{43, 7, 9\}$

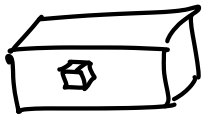
[[similar to Goal ①; complete for practice]].

Prove or **disprove**: $\{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\} \subseteq \{\mathtt{AA}, \mathtt{AC}, \mathtt{AU}, \mathtt{AG}\}$ $\forall x\,(x \in \{A,C,U,G\} \to x \in \{AA, AC, AU, AG\})$

Counterexample that disproves this universal claim is A because $A \in \{A,C,U,G\}$ and $A \notin \{AA, AC, AU, AG\}$ so conditional statement evaluates to $T \to F = F$.

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

Witness that proves this existential claim is $B = \{\emptyset\}$ because $\emptyset \in \{\emptyset\}$



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

Counterexample that disproves this universal claim is $B = \emptyset$ because $\emptyset \notin \emptyset$.

Another counterexample is $\{1,2,3\}$ because $\emptyset \notin \{1,2,3\}$

Prove or **disprove**: The empty set is a subset of every set. $\forall B\,(\emptyset \subseteq B)$

WTS $\forall B\, \forall x\,(x \in \emptyset \to x \in B)$

Consider arbitrary set B (towards universal generalizing)

Consider arbitrary x. (towards universal generalizing)

WTS $x \in \emptyset \to x \in B$.

By definition of $\emptyset$, $x \in \emptyset$ is F so by definition of conditional $x \in \emptyset \to x \in B = F \to ? = T$.

Prove or **disprove:** The empty set is a proper subset of every set. $\forall B(\emptyset \subseteq B \wedge \emptyset \neq B)$

Counterexample $B = \emptyset$

Notice $\emptyset \neq B$ is F because $B = \emptyset$ so predicat evaluates to $T \wedge F$ which is F by def of conjunction

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

the set of integer multiples of 4

Counterexample 6.

WTS $6 \in \{4,6\}$ is T and $6 \notin \{n \mid \exists c \in \mathbb{Z}\ (n = 4c\}$

Goal ① $6 \in \{4,6\}$ is true by definition of roster method.

Goal ② WTS $\neg\exists c \in \mathbb{Z}(6 = 4c)$, equivalently using quantifier De Morgan's rule, WTS $\forall c \in \mathbb{Z}\ (6 \neq 4c)$.

continued below

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

the set of last digits of integer multiples of 4.

Consider arbitrary x and assume $x \in \{4,6\}$.
By definition of roster method, $x = 4 \vee x = 6$.

Case 1: $x = 4$. WTS $\exists n\,(4 = n \bmod 10 \wedge \exists c \in \mathbb{Z}\,(n = 4c))$
witness for existential is $n = 24$ because $24 = 2 \cdot 10 + 4$ so $24 \bmod 10 = 4$
and for second conjunct have witness $c = 6$: $n = 24 = 4 \cdot 6 = 4c$, as required.

Case 2: $x = 6$ WTS $\exists n\,(6 = n \bmod 10 \wedge \exists c \in \mathbb{Z}\,(n = 4c))$
witness for existential is $n = 36$ because $36 = 3 \cdot 10 + 6$ so
$16 \bmod 10 = 6$ and for second conjunct have witness $c = 9$: $n = 36 = 4 \cdot 9 = 4c$
as required.

Signposting vocabulary:

Consider ..., an **arbitrary** .... **Assume** ..., we **want to show** that .... Which is what was needed, so the proof is complete □.
or, in other words:
Let ... be an **arbitrary** .... **Assume** ..., **WTS** that ... **QED**.

continuation:

WTS $\forall c \in \mathbb{Z}\ (6 \neq 4c)$

Towards universal generalization
let $c \in \mathbb{Z}$ be arbitrary.

By properties of integers,
$c \leq 1 \vee c > 2$
is true.

We proceed by case.

Case ① Assume $c \leq 1$. We WTS $6 \neq 4c$.
Multiplying both sides of $c \leq 1$ by 4: $4c \leq 4$ and since $4 < 6$ we have $4c < 6$ so $4c \neq 6$.

Case ② Assume $c > 2$. We WTS $6 \neq 4c$
Multiplying both sides of $c > 2$ by 4: $4c > 8$ and since $8 > 6$, we have $4c > 6$ so $4c \neq 6$.

Since each case guarantees what we want to show, the proof is complete.

■

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, note: type

conjunction

ordered pairs

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

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

Example: $\mathbb{Z} \times \emptyset =$ $\{(a,b) \mid a \in \mathbb{Z} \wedge b \in \emptyset\} = \emptyset$ (F)

Union: When A and B are sets,

disjunction

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

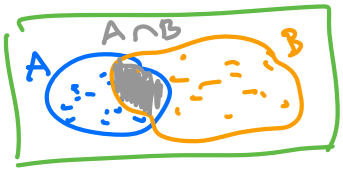
Example: $\{43, 9\} \cup \{9, \mathbb{Z}\} =$ $\{43, 9, \mathbb{Z}\}$

Example: $\mathbb{Z} \cup \emptyset =$ $\{x \mid x \in \mathbb{Z} \vee x \in \emptyset\} = \{x \mid x \in \mathbb{Z}\} = \mathbb{Z}$. ($x \in \emptyset$: F)

Intersection: When A and B are sets,

conjunction

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



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

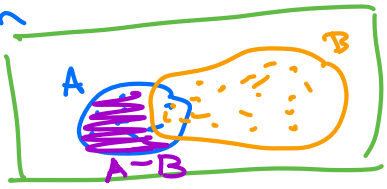
Example: $\mathbb{Z} \cap \emptyset =$ $\{x \mid x \in \mathbb{Z} \wedge x \in \emptyset\} = \{x \mid \text{False}\} = \emptyset$ ($x \in \emptyset$: F)

$P \wedge F \equiv F$

Set difference: When A and B are sets,

conjunction, negation

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



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

Example: $\mathbb{Z} - \emptyset =$ $\{x \mid x \in \mathbb{Z} \wedge x \notin \emptyset\} = \{x \mid x \in \mathbb{Z}\} = \mathbb{Z}$. ($x \notin \emptyset$: T)

$P \wedge T \equiv P$

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

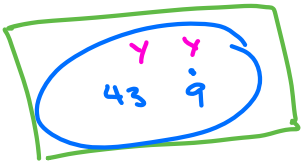
Example: $\{43, 9\}, \{9, \mathbb{Z}\}$ are not disjoint

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

Suggestion: $A - B = A - (A \cap B)$

subsets

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



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

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

Notice

① $1 \notin \{43, 9, \mathbb{Z}\}$

② $\emptyset \notin \{43, 9, \mathbb{Z}\}$

③ $\{43, 9\} - \{9, \mathbb{Z}\} \neq \{9, \mathbb{Z}\} - \{43, 9\}$

④ $\forall X\ (\emptyset \in \mathcal{P}(X))$

⑤ $\emptyset$ is disjoint from itself because $\emptyset \cap \emptyset = \emptyset$

Number of distinct elements in W is 32 because it is $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$

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

Example elements in W are:

NNNNN $\emptyset$ YNNNN $\{1\}$ NNYNN $\{3\}$ NNNYY $\{4, 5\}$ NYNNY $\{2, 5\}$ NYYYN $\{2, 3, 4\}$ YYYYY $\{1, 2, 3, 4, 5\}$

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

Pf: Goal is to prove that for any sets, if one is a subset of another then its power set is a subset of the power set of that other set.

Towards a proof by universal generalization consider arbitrary elements $A \in W$, $B \in W$.

WTS $A \subseteq B \rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Towards a direct proof, assume (1) $A \subseteq B$ and WTS $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

By definition of subset, this means we WTS $\forall X (X \in \mathcal{P}(A) \rightarrow X \in \mathcal{P}(B))$

Towards universal generalization, let X be arbitrary and assume (towards direct proof) that $X \in \mathcal{P}(A)$. WTS $X \in \mathcal{P}(B)$

By definition of power set we have assumed (2) $X \subseteq A$ and WTS $X \subseteq B$.

By definition of subset, WTS $\forall x (x \in X \rightarrow x \in B)$

Towards univ. gen. let x be arbitrary assume, (3) $x \in X$. WTS $x \in B$. By def of subset, since $x \in X$ (3) and $X \subseteq A$ (2), have $x \in A$. And since $x \in A$ and $A \subseteq B$ (1) we get $x \in B$ ∎

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

Practice: translate each of these using quantifiers, logical operators

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 $b = ac$ = $ac + 0$ ← remainder b mod a, ↳ quotient b div a

Symbolically, $F(\ (a,b)\ ) = \exists\, c \in \mathbb{Z}\ (b = ac)$ and is a predicate over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$

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	$a \mid b$

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** $a)$

Notice: in set builder notation, "|" mean such that

and in the function |x| → absolute value.

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: WTS $\forall a \in \mathbb{Z}^{\neq 0}\ \exists c \in \mathbb{Z}\ (a = ca)$

Towards universal generalization, consider arbitrary a, a nonzero integer.

WTS $\exists c \in \mathbb{Z}\ (a = ca)$.

Need witness: $c = 1$, an integer and we check predicate holds by evaluating

LHS = a RHS = $ca = 1 \cdot a = a$

so they agree, as required ∎

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

$\neg \exists a \in \mathbb{Z}^{\neq 0}\ \neg F((a, a^2))$

$a \mid a^2$ or $a^2 \bmod a = 0$

WTS $\forall a \in \mathbb{Z}^{\neq 0}\ \neg\neg F((a,a^2))$, i.e. $\forall a \in \mathbb{Z}^{\neq 0}\ F((a,a^2))$

Let a be an arbitrary nonzero int (towards universal generalization), and we want to show $\exists c \in \mathbb{Z}\ (a^2 = ac)$. Consider $c = a$ (value of witness depends on value of a). an integer (by choice of a as a nonzero integer), and LHS = a^2, RHS = $ac = a \cdot a = a^2$, as required ∎

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

$\forall b \in \mathbb{Z}^+\ \forall a \in \mathbb{Z}^+\ (F((a,b)) \rightarrow a \leq b)$

Let b, a be arbitrary positive integers.

Towards a direct proof, assume $F((a,b))$

WTS $a \leq b$. By def of predicate F, knw $\exists c \in \mathbb{Z}\ (b = ac)$. Call such a witness c.

In other words, have $b = ac$.

because b and a are positive integers, Fact 2 gives that c is positive.

So by Fact 5 $ac \geq a$, and since $b = ac$, we have reached our goal, that $b \geq a$ ∎

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

$(\forall a \in \mathbb{Z}^{\neq 0}\ F(a,a)) \wedge (\forall a \in \mathbb{Z}^{\neq 0}\ F(a,a^2))$

Goal 1: Prove left conjunct ✓ (see prev. page)

Goal 2: Prove right conjunct ✓ (" ")

So the conjunction has been proved ∎

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 **mod** $2 = 0$; an integer n is **odd** means n **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).

We need to show that

$\neg \exists p \in \mathbb{Z}^+ (Pr(p) \wedge Pr(p+1) \wedge Pr(p+2))$

i.e. we need to show that

$\forall p \in \mathbb{Z}^+ (\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2))$

Let p be an arbitrary positive int.

Notice that $p \bmod 2 = 0 \vee p \bmod 2 = 1$

Case ① Assume $p \bmod 2 = 0$. Then 2 is a factor of p. Moreover, $p+2 > 2$ because p is positive (so $p > 0$). Since 2 is a factor of p, it is also a factor of $p+2$ (exercise: prove this) so $p+2 > 1$, and 2 is a positive factor of $p+2$ that is neither 1 nor $p+2$ so $p+2$ is not prime. Thus $\neg Pr(p+2)$ holds and so $\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2)$ is true.

Case ② Assume $p \bmod 2 = 1$. Then $(p=1) \vee (p>1)$ because p is a positive int.

Case 2a Assume $p=1$. Then p is not prime by definition of primes requiring them to be greater than 1. So $\neg Pr(p)$ is true, thus $\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2)$ is true.

Case 2b Assume $p>1$. Then $p+1>2>1$. Moreover, since $p \bmod 2 = 1$, $p+1$ is even (Exercise: prove this.). Thus $p+1$ is greater than 1 and 2 is a positive factor of $p+1$ that is neither 1 nor $p+1$. In particular, this means $p+1$ is not prime, i.e. $\neg Pr(p+1)$. Thus $\neg Pr(p) \vee \neg Pr(p+1) \vee \neg Pr(p+2)$ is true.

The proof by cases is complete and we have shown that there is no sequence of three consecutive positive integers that are prime.

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 $\exists p \in \mathbb{Z}^+ (p \bmod 2 = 1 \wedge Pr(p) \wedge Pr(p+2) \wedge Pr(p+4))$

Idea: witness 3, 5, 7.

Consider $p = 3$, a positive integer.
We evaluate each of the four conjuncts:

(1) $p \bmod 2 = 3 \bmod 2 = 1$ because $3 = 1 \cdot 2 + 1$

(2) To check if $Pr(p)$ we check
- $p > 1$? Yes, $3 > 1$.
- the only positive factors of p are $1, p$?
  We only need to check positive ints $2, \ldots, p-1$ because we proved that positive factors of p are $\leq p$.
  With $p = 3$, only consider 2 and since $3 \bmod 2 = 1$ (see above), 2 is not a factor of 3 so 3 is prime.

(2) To check if $Pr(p+2)$ we check
- $p+2 > 1$? Yes, $3+2 = 5 > 1$.
- the only positive factors of $p+2$ are $1, p+2$?
  We check 2, 3, 4:
  $5 \bmod 2 = 1$ b/c $5 = 2 \cdot 2 + 1$ so 2 is not a factor of 5
  $5 \bmod 3 = 2$ b/c $5 = 1 \cdot 3 + 2$ so 3 is not a factor of 5
  $5 \bmod 4 = 1$ b/c $5 = 1 \cdot 4 + 1$ so 4 is not a factor of 5

Thus 5 is prime.

(3) To check if $Pr(p+4)$ we check

- $p+4 > 1$? Yes, $3+4 = 7 > 1$.
- the only positive factors of $p+4$ are $1, p+4$? We check $2, 3, 4, 5, 6$:

$7 \bmod 2 = 1$ b/c $7 = 3 \cdot 2 + 1$ so 2 is not a factor of 7

$7 \bmod 3 = 1$ b/c $7 = 2 \cdot 3 + 1$ so 3 is not a factor of 7

$7 \bmod 4 = 3$ b/c $7 = 1 \cdot 4 + 3$ so 4 is not a factor of 7

$7 \bmod 5 = 2$ b/c $7 = 1 \cdot 5 + 2$ so 5 is not a factor of 7

$7 \bmod 6 = 1$ b/c $7 = 1 \cdot 6 + 1$ so 6 is not a factor of 7.

Thus 7 is prime.

We have proved that

$$(p \bmod 2 = 1 \wedge Pr(p) \wedge Pr(p+2) \wedge Pr(p+4))$$

is true for the positive integer $p = 3$ so we found a witness that proves the existential claim ∎

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