## Week 6 at a glance

**We will be learning and practicing to:**

- Clearly and unambiguously communicate computational ideas using appropriate formalism. Translate across levels of abstraction.
  - Translating between symbolic and English versions of statements using precise mathematical language
  - Using appropriate signpost words to improve readability of proofs, including 'arbitrary' and 'assume'
- Know, select and apply appropriate computing knowledge and problem-solving techniques. Reason about computation and systems. Use mathematical techniques to solve problems. Determine appropriate conceptual tools to apply to new situations. Know when tools do not apply and try different approaches. Critically analyze and evaluate candidate solutions.
  - Judging logical equivalence of compound propositions using symbolic manipulation with known equivalences, including DeMorgan's Law
  - Writing the converse, contrapositive, and inverse of a given conditional statement
  - Determining what evidence is required to establish that a quantified statement is true or false
  - Evaluating quantified statements about finite and infinite domains
- Apply proof strategies, including direct proofs and proofs by contradiction, and determine whether a proposed argument is valid or not.
  - Identifying the proof strategies used in a given proof
  - Identifying which proof strategies are applicable to prove a given compound proposition based on its logical structure
  - Carrying out a given proof strategy to prove a given statement
  - Carrying out a universal generalization argument to prove that a universal statement is true
  - Using proofs as knowledge discovery tools to decide whether a statement is true or false

**TODO:**

Project due this week: May 8, 2024.

Review quiz based on class material each day (due Friday May 10, 2024).

# Week 6 Monday: Proofs for properties of sets and numbers

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

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

Note on notation
$\subseteq$ / $=$
possibly equal sets.

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

WTS $A \subseteq B \wedge B \subseteq A$

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

Example elements in $W$ are:

$\emptyset$ $\{1\}$ $\{1,3\}$ $\{1,2\}$

Note: $1 \notin W$
$1 \in \{1,2,3,4,5\}$

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

* For all $A, B \in W$, if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Towards a proof by universal generalization, let $A, B$ be arbitrary elements of $W$. WTS $A \subseteq B \rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$. (HYPOTHESIS)

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

By definition of $\subseteq$, WTS $\forall x ( x \in \mathcal{P}(A) \rightarrow x \in \mathcal{P}(B) )$ (HYP, CONC)

Towards a universal generalization, then direct proof, consider an arbitrary $x$ and assume $x \in \mathcal{P}(A)$. WTS $x \in \mathcal{P}(B)$.

[CONTINUED BELOW]

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

Towards universal generalization, consider arbitrary $A \in W$ and $B \in W$.
Assume (towards direct proof) that $\mathcal{P}(A) = \mathcal{P}(B)$. WTS $A = B$.
Goal ① WTS $A \subseteq B$. Consider arbitrary $x \in A$. WTS $x \in B$. Since $x \in A$, $\{x\} \subseteq A$. By definition of $\mathcal{P}$, $\{x\} \in \mathcal{P}(A)$. By assumption that $\mathcal{P}(A) = \mathcal{P}(B)$, $\{x\} \in \mathcal{P}(B)$. By definition of $\mathcal{P}$, $\{x\} \subseteq B$ so, by definition of subset, $x \in B$.
Goal ② WTS $B \subseteq A$. Identical argument to goal ① with roles of $A, B$ swapped.
Thus, $A \subseteq B$ and $B \subseteq A$ so $A = B$, as required ☒

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

Counterexample: $A = \{1,2\}$, $B = \{3\}$, $C = \{1,2,3\}$
- each is in $W$ because each is a subset of $\{1,2,3,4,5\}$
- $A \cup B = \{x \mid x \in A \vee x \in B\} = \{1,2,3\}$
  $A \cup C = \{x \mid x \in A \vee x \in C\} = \{1,2,1,2,3\} = \{1,2,3\}$ so $A \cup B = A \cup C$
- $B \neq C$ because $1 \notin B$ but $1 \in C$.

Thus $A \cup B = A \cup C \rightarrow B = C$ is false (its hypothesis is true while the conclusion is false) ☒

Our assumption is $x \in \mathcal{P}(A)$, namely $x \subseteq A$. Our goal is to prove $x \in \mathcal{P}(B)$, namely we want to show that $x \subseteq B$.

By definition, this means we want to show that $\forall y\,(y \in x \rightarrow y \in B)$.

Towards universal generalization, consider arbitrary $y$, and assume towards direct proof that $y \in x$. WTS $y \in B$.

Since have $x \subseteq A$ and $A \subseteq B$, since $y \in x$, by definition of subsets we have $y \in A$. But since $A \subseteq B$, by definition of subsets, we have $y \in B$. as required ∎

## Facts about numbers

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.

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

   $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ (x+y = y+x \wedge x \cdot y = y \cdot x)$

   $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ ((x+y)+z = x+(y+z) \wedge (x \cdot y) \cdot z = x \cdot (y \cdot z))$

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.

   (positive means strictly positive, i.e nonzero)

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

quotient

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

OVERLOADED SYMBOL | "divides" BUT in set builder notation, means "such that"

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 $a$ $\quad$ $a|b$

remainder is zero.

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.*

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

$\exists a \in \mathbb{Z}^{\neq 0}\ (\ \neg F(\ (a,a)\ )\ )$ there is a nonzero integer that is not its own factor.

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

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

Every nonzero integer is a factor of itself.

No nonzero integer is a factor of itself.

At least one nonzero integer is a factor of itself.

Some nonzero integer is not a factor of itself.

Recall: $\exists$ ... "there exists"
$\forall$ ... "Every..."

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

**Proof**: WTS $\forall a \in \mathbb{Z}^{\neq 0}(\ F(\ (a,a)\ )\ )$

Towards universal generalization, consider arbitrary nonzero integer $a$ and we want to show $F(\ (a,a)\ )$. By definition of $F$, this means showing $\exists c \in \mathbb{Z}\ (\underbrace{a}_{\text{LHS}} = \underbrace{c \cdot a}_{\text{RHS}})$. Need witness integer $c$, consider $c = 1$, and we confirm this is an integer and

RHS $= c \cdot a = 1 \cdot a = a =$ LHS, as required. ☒

(by choice of $c$; by properties of integer)

Notation: When proving LHS = RHS, start with one side, plug in values to transform to expression in the other side of desired equality

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

WTS $\neg \exists a \in \mathbb{Z}^{\neq 0}(\neg F(\ (a,a^2)\ ))$, namely (using DeMorgan's Law),
$\forall a \in \mathbb{Z}^{\neq 0}\ F(\ (a,a^2)\ )$.

Let $a$ be an arbitrary nonzero integer (towards a universal generalization), and we want to show $F(\ (a,a^2)\ )$, namely $\exists c \in \mathbb{Z}(a^2 = ca)$.

Consider $c = a$, an integer. It witnesses the existential statement because

LHS $= a^2 = a \cdot a = c \cdot a =$ RHS, as required ☒.

(def of square; def of $c$)

Notice: different witness for different choices of the value $a$

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

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

Towards universal generalization, let $a$ and $b$ be positive integers. Towards direct proof, assume $F(a,b)$. WTS $a \leq b$. By definition of factor, know $\exists c \in \mathbb{Z} (b = ac)$. Call such a witness $c$. Namely, we have $b = ac$. Because $a$ and $b$ are positive integers, Fact 2 gives that $c$ is positive, so Fact 5 gives that $ac \geq a$, and since $b = ac$, we have reached our goal, namely $b \geq a$.

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

Pf: We have already proved each 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.

Notice that $0 = 2 \cdot 0 + 0$ so $0 \bmod 2 = 0$ so 0 is even.

**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 $\forall p \in \mathbb{Z}^+ ($ p is not prime $\vee$ p+1 is not prime $\vee$ p+2 is not prime $)$

i.e. $\neg \exists p \in \mathbb{Z}^+ ($ p is prime $\wedge$ p+1 is prime $\wedge$ p+2 is prime $)$

Towards proof by universal generalization, consider an arbitrary positive integer $p$. WTS

( p is not prime ) $\vee$ ( p+1 is not prime ) $\vee$ ( p+2 is not prime ) $= T$

Notice that $p$ is even or odd.

[continued below].

**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 $\exists p \in \mathbb{Z}^+ (p \bmod 2 = 1 \wedge p \text{ is prime} \wedge p+2 \text{ is prime} \wedge p+4 \text{ is prime})$

Idea: Use $p=3$ as witness.
[Details left as exercise].

---

Continuation of previous argument.

Case 1: Assume $p \bmod 2 = 0$. Then 2 is a factor of $p$. Since $p>0$, adding 2 to both sides gives $p+2 > 2 > 1$. We can show that 2 is a factor of $p+2$: let $q$ be the quotient when dividing $p$ by 2 so $p = 2q$ (and $q$ is an integer) and adding 2 to both sides gives $p+2 = 2q+2 = 2(q+1)+0$ so $q+1$ is the quotient when dividing $p+2$ by 2 and $(p+2) \bmod 2 = 0$. Thus $p+2 > 1$ and 2 is a positive factor of $p+2$ that is neither 1 nor $p+2$ (because $p+2 > 2$) so $p+2$ is not prime.
Thus ($p$ is not prime) $\vee$ ($p+1$ is not prime) $\vee$ ($p+2$ is not prime) ☒

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

Case (2a) Assume $p=1$. Then $p$ is not prime (because prime numbers have to be greater than 1) so
($p$ is not prime) $\vee$ ($p+1$ is not prime) $\vee$ ($p+2$ is not prime)

Case (2b) Assume $p>1$. Then $p+1 > 2 > 1$. Moreover, if $q$ is the quotient upon dividing $p$ by 2, $p = 2q+1$, then $p+1 = (2q+1)+1 = 2q+2 = 2(q+1)+0$ so $(p+1) \bmod 2 = 0$ and we have that $p+1$ is an integer greater than 1 with 2 a positive factor of $p+1$ (that is neither 1 nor $p+1$, because we assumed $p+1 > 2$) so $p+1$ is not prime. Hence
($p$ is not prime) $\vee$ ($p+1$ is not prime) $\vee$ ($p+2$ is not prime) ☒

The proof by cases is complete and we have shown that there is no sequence of consecutive integers that are all prime ☒

# Week 6 Wednesday: Structural Induction

*Recall the definitions*: The set of RNA strands $S$ is defined (recursively) by:

| | |
|---|---|
| Basis Step: | $\mathtt{A} \in S, \mathtt{C} \in S, \mathtt{U} \in S, \mathtt{G} \in S$ |
| Recursive Step: | If $s \in S$ and $b \in B$, then $sb \in S$ |

where $sb$ is string concatenation.

The function *rnalen* that computes the length of RNA strands in $S$ is defined recursively by:

$$rnalen : S \to \mathbb{Z}^+$$

| | | |
|---|---|---|
| Basis Step: | If $b \in B$ then | $rnalen(b) = 1$ |
| Recursive Step: | If $s \in S$ and $b \in B$, then | $rnalen(sb) = 1 + rnalen(s)$ |

The function *basecount* that computes the number of a given base $b$ appearing in a RNA strand $s$ is defined recursively by:

$$basecount : S \times B \to \mathbb{N}$$

Basis Step: If $b_1 \in B, b_2 \in B$

$$basecount(\ (b_1, b_2)\ ) = \begin{cases} 1 & \text{when } b_1 = b_2 \\ 0 & \text{when } b_1 \neq b_2 \end{cases}$$

Recursive Step: If $s \in S, b_1 \in B, b_2 \in B$

$$basecount(\ (sb_1, b_2)\ ) = \begin{cases} 1 + basecount(\ (s, b_2)\ ) & \text{when } b_1 = b_2 \\ basecount(\ (s, b_2)\ ) & \text{when } b_1 \neq b_2 \end{cases}$$

At this point, we've seen the proof strategies

- A **counterexample** to prove that $\forall x P(x)$ is **false**.
- A **witness** to prove that $\exists x P(x)$ is **true**.
- **Proof of universal by exhaustion** to prove that $\forall x\, P(x)$ is true when $P$ has a finite domain
- **Proof by universal generalization** to prove that $\forall x\, P(x)$ is true using an arbitrary element of 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.
- Proof of conditional by **direct proof**
- Proof of conditional by **contrapositive proof**
- Proof of disjuction using equivalent conditional: To prove that the disjunction $p \vee q$ is true, we can rewrite it equivalently as $\neg p \to q$ and then use direct proof or contrapositive proof.
- **Proof by cases**.

Which proof strategies could be used to prove each of the following statements?

*Hint: first translate the statements to English and identify the main logical structure.*

$\forall s \in S$ ( $rnalen(s) > 0$ ) Every RNA strand has (strictly) positive length

Domain, S, is infinite

Pf: Consider arbitrary strand s. WTS rnalen(s) > 0 (use definition!)

To be continued.

$\forall b \in B\ \exists s \in S$ ( $basecount(\ (s, b)\ )\ > 0$ ) For each base, there's an RNA strand with at least one occurrence of that base.

Domain, B

Pf: By exhaustion

- Evaluate $\exists s \in S$ ( basecount( (s,A) ) > 0 ): True, using witness s=A (in domain S; basecount(A,A) = 1 > 0 ☺ — basis step, def of function)
- C U G

$\forall s \in S\ \exists b \in B$ ( $basecount(\ (s, b)\ ) > 0$ ) For each strand, there's a base that occurs at least once in that strand

Pf: By universal generalization, consider an arbitrary strand s

WTS $\exists b \in B$ ( basecount( (s,b) ) > 0 )

Case 1: $s \in B$

Case 2: $s \notin B$

To be continued...

$\exists s \in S\ (rnalen(s) = basecount(\ (s, \mathtt{A})\ )$ There is a strand whose length matches the number of occurrences of A in that strand.

Pf: Find witness $s \in S$

eg. s = A

Fill in calculations..

$\forall s \in S\ (rnalen(s) \geq basecount(\ (s, \mathtt{A})\ ))$ For each strand, the length of the strand is no less than the number of occurrences of A in that strand.

To be continued...

**Claim** $\forall s \in S$ ( $rnalen(s) > 0$ )

**Proof**: Let $s$ be an arbitrary RNA strand. By the recursive definition of $S$, either $s \in B$ or there is some strand $s_0$ and some base $b$ such that $s = s_0 b$. We will show that the inequality holds for both cases.

**Basis Case**: Assume $s \in B$. We need to show $rnalen(s) > 0$. By the basis step in the definition of $rnalen$,

$$rnalen(s) = 1$$

which is greater than 0, as required.

**Recursive Step Case**: Assume there is some strand $s_0$ and some base $b$ such that $s = s_0 b$. We will show *(the stronger claim)* that

$$\forall u \in S \; \forall b \in B \; ( \; rnalen(u) > 0 \rightarrow rnalen(ub) > 0 \; )$$

Consider an arbitrary RNA strand $u$ and an arbitrary base $b$, and assume towards a direct proof, that

$$rnalen(u) > 0$$

We need to show that $rnalen(ub) > 0$.

$$rnalen(ub) = 1 + rnalen(u) > 1 + 0 = 1 > 0$$

as required.

**Proof by Structural Induction** To prove a universal quantification over a recursively defined set:

**Basis Step**: Show the statement holds for elements specified in the basis step of the definition.

**Recursive Step**: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

**Claim** $\forall s \in S\,(rnalen(s) \geq basecount(\ (s, \mathtt{A})\ ))$:

**Proof**: We proceed by structural induction on the recursively defined set $S$.

**Basis Case**: We need to prove that the inequality holds for each element in the basis step of the recursive definition of $S$. Need to show

$$(\ rnalen(\mathtt{A}) \geq basecount(\ (\mathtt{A}, \mathtt{A})\ )\ ) \wedge (\ rnalen(\mathtt{C}) \geq basecount(\ (\mathtt{C}, \mathtt{A})\ )\ )$$
$$\wedge(\ rnalen(\mathtt{U}) \geq basecount(\ (\mathtt{U}, \mathtt{A})\ )\ ) \wedge (\ rnalen(\mathtt{G}) \geq basecount(\ (\mathtt{G}, \mathtt{A})\ )\ )$$

We calculate, using the definitions of *rnalen* and *basecount*:

Goal 1: LHS = rnalen(A) = 1 by basis step in def of rnalen
RHS = basecount( (A,A) ) = 1 by basis step in def of basecount, with $b_1 = b_2$
since LHS = RHS, LHS ≥ RHS as required.

Goal 2: LHS = rnalen(C) = 1 by basis step in def of rnalen
RHS = basecount( (C,A) ) = 0 by basis step in def of basecount, with $b_1 \neq b_2$
since LHS > RHS, LHS ≥ RHS as required.

Goal 3, Goal 4: similar.

**Recursive Case**: We will prove that

$$\forall u \in S\ \forall b \in B\ (\ rnalen(u) \geq basecount(\ (u, \mathtt{A})\ ) \rightarrow rnalen(ub) \geq basecount(\ (ub, \mathtt{A})\ )\ )$$

Consider arbitrary RNA strand $u$ and arbitrary base $b$. Assume, as the **induction hypothesis**, that $rnalen(u) \geq basecount(\ (u, \mathtt{A})\ )$. We need to show that $rnalen(ub) \geq basecount(\ (ub, \mathtt{A})\ )$.

LHS RHS

Using the recursive step in the definition of the function *rnalen*:

LHS = $rnalen(ub) = 1 + rnalen(u)$

The recursive step in the definition of the function *basecount* has two cases. We notice that $b = \mathtt{A} \vee b \neq \mathtt{A}$ and we proceed by cases.

RHS

*Case i.* Assume $b = \mathtt{A}$.

Using the first case in the recursive step in the definition of the function *basecount*:

$$basecount(\ (ub, \mathtt{A})\ ) = 1 + basecount(\ (u, \mathtt{A})\ )$$

By the **induction hypothesis**, we know that $basecount(\ (u, \mathtt{A})\ ) \leq rnalen(u)$ so:

$$basecount(\ (ub, \mathtt{A})\ ) = 1 + basecount(\ (u, \mathtt{A})\ ) \leq 1 + rnalen(u) = rnalen(ub)$$

and, thus, $basecount(\ (ub, \mathtt{A})\ ) \leq rnalen(ub)$, as required.

*Case ii.* Assume $b \neq \mathtt{A}$.

Using the second case in the recursive step in the definition of the function *basecount*:

$$basecount(\ (ub, \mathtt{A})\ ) = basecount(\ (u, \mathtt{A})\ )$$

By the **induction hypothesis**, we know that $basecount(\ (u, \mathtt{A})\ ) \leq rnalen(u)$ so:

$$basecount(\ (ub, \mathtt{A})\ ) = basecount(\ (u, \mathtt{A})\ ) \leq rnalen(u) < 1 + rnalen(u) = rnalen(ub)$$

and, thus, $basecount(\ (ub, \mathtt{A})\ ) \leq rnalen(ub)$, as required.

# Week 6 Friday: Structural and Mathematical Induction

To organize our proofs, it's useful to highlight which claims are most important for our overall goals. We use some terminology to describe different roles statements can have.

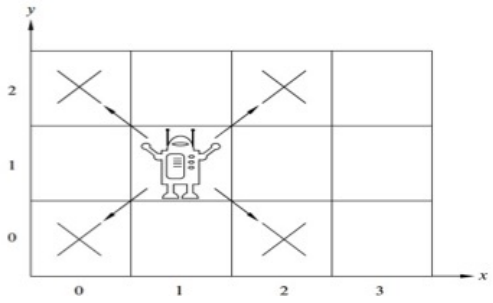
**Theorem**: Statement that can be shown to be true, usually an important one.

Less important theorems can be called **proposition**, **fact**, **result**, **claim**.

**Lemma**: A less important theorem that is useful in proving a theorem.

**Corollary**: A theorem that can be proved directly after another one has been proved, without needing a lot of extra work.

**Invariant**: A theorem that describes a property that is true about an algorithm or system no matter what inputs are used.




**Theorem**: A robot on an infinite 2-dimensional integer grid starts at $(0, 0)$ and at each step moves to diagonally adjacent grid point. This robot can / cannot (*circle one*) reach $(1, 0)$.

**Definition** The set of positions the robot can visit $Pos$ is defined by:

Basis Step: $(0, 0) \in Pos$
Recursive Step: If $(x, y) \in Pos$, then

are also in $Pos$

*Example elements of Pos are*:

**Lemma**: $\forall (x, y) \in Pos$ ($x + y$ is an even integer )

*Why are we calling this a lemma?*

Proof of theorem using lemma: To show is $(1, 0) \notin Pos$. Rewriting the lemma to explicitly restrict the domain of the universal, we have $\forall (x, y)$ ( $(x, y) \in Pos \rightarrow (x+y$ is an even integer) ). Since the universal is true, ( $(1, 0) \in Pos \rightarrow (1 + 0$ is an even integer) ) is a true statement. Evaluating the conclusion of this conditional statement: By definition of long division, since $1 = 0 \cdot 2 + 1$ (where $0 \in \mathbb{Z}$ and $1 \in \mathbb{Z}$ and $0 \leq 1 < 2$ mean that 0 is the quotient and 1 is the remainder), $1$ **mod** $2 = 1$ which is not 0 so the conclusion is false. A true conditional with a false conclusion must have a false hypothesis: $(1, 0) \notin Pos$, QED. □

Proof of lemma by structural induction:

**Basis Step**:

**Recursive Step**: Consider arbitrary $(x, y) \in Pos$. To show is:

$$(x + y \text{ is an even integer}) \rightarrow (\text{sum of coordinates of next position is even integer})$$

Assume **as the induction hypothesis, IH** that:

The set $\mathbb{N}$ is recursively defined. Therefore, the function $sumPow : \mathbb{N} \to \mathbb{N}$ which computes, for input $i$, the sum of the nonnegative powers of 2 up to and including exponent $i$ is defined recursively by

Basis step: $sumPow(0) = 1$

Recursive step: If $x \in \mathbb{N}$, then $sumPow(x+1) = sumPow(x) + 2^{x+1}$

$sumPow(0) =$

$sumPow(1) =$

$sumPow(2) =$

Fill in the blanks in the following proof of

$$\forall n \in \mathbb{N}\ (sumPow(n) = 2^{n+1} - 1)$$

**Proof**: Since $\mathbb{N}$ is recursively defined, we proceed by _____.

**Basis case**: We need to show that _____. Evaluating each side: $LHS = sumPow(0) = 1$ by the basis case in the recursive definition of $sumPow$; $RHS = 2^{0+1} - 1 = 2^1 - 1 = 2 - 1 = 1$. Since $1 = 1$, the equality holds.

**Recursive case**: Consider arbitrary natural number $n$ and assume, as the _____ that $sumPow(n) = 2^{n+1} - 1$. We need to show that _____. Evaluating each side:

$$LHS = sumPow(n+1) \overset{\text{rec def}}{=} sumPow(n) + 2^{n+1} \overset{\text{IH}}{=} (2^{n+1} - 1) + 2^{n+1}.$$

$$RHS = 2^{(n+1)+1} - 1 \overset{\text{exponent rules}}{=} 2 \cdot 2^{n+1} - 1 = \left(2^{n+1} + 2^{n+1}\right) - 1 \overset{\text{regrouping}}{=} (2^{n+1} - 1) + 2^{n+1}$$

Thus, $LHS = RHS$. The structural induction is complete and we have proved the universal generalization. □

**Proof by Mathematical Induction**

To prove a universal quantification over the set of all integers greater than or equal to some base integer $b$,

**Basis Step**: Show the property holds for $b$.

**Recursive Step**: Consider an arbitrary integer $n$ greater than or equal to $b$, assume (as the **induction hypothesis**) that the property holds for $n$, and use this and other facts to prove that the property holds for $n + 1$.

## Review Quiz

1. Set properties

(a)

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.)

i. $A = \{1,2,3\}, B = \{1,2\}, C = \{1,3\}$
ii. $A = \{1,2,3\}, B = \{2\}, C = \{2\}$
iii. $A = \{\emptyset, 1,2,3\}, B = \{1,2\}, C = \{1,3\}$
iv. $A = \{1,2,3\}, B = \{1,2\}, C = \{1,4\}$
v. $A = \{1,2\}, B = \{2,3\}, C = \{1,3\}$
vi. $A = \{1,2\}, B = \{1,3\}, C = \{1,3\}$

(b)

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.

i. First approach, assumption.
ii. First approach, "need to show".
iii. Second approach, assumption.
iv. 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) $\exists x(x \in A \oplus x \in B)$

(c)

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.*

i. Every set is a subset of itself.
ii. Every set is an element of itself.
iii. Some set is an element of all sets.
iv. 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. $\forall X\ (X \subseteq X)$

2. Number properties

(a)

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) $\exists y \in \mathbb{Z}\ \forall x \in \mathbb{Z}^{\neq 0}\ (F(\ (x,y)\ ))$

i. Select the statement whose translation is
"The number 1 is a factor of every integer."
or write NONE if none of (i)-(viii) work.
ii. Select the statement whose translation is
"Every integer has at least one nonzero factor."
or write NONE if none of (i)-(viii) work.
iii. 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.
iv. For each statement (i)-(viii), determine if it is true or false.

(b)

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.)

i. $\forall a \in \mathbb{Z}^{\neq 0}\ (\ (x > 1 \wedge a > 0) \rightarrow F(\ (a,x)\ ))$
ii. $\neg\exists a \in \mathbb{Z}^{\neq 0}\ (x > 1 \wedge (a = 1 \vee a = x) \wedge F(\ (a,x)\ ))$
iii. $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 0 \wedge F(\ (a,x)\ )\ ) \rightarrow (a = 1 \vee a = x)\ )$
iv. $(x > 1) \wedge \forall a \in \mathbb{Z}^{\neq 0}\ (\ (\ a > 1 \wedge \neg(a = x)\ ) \rightarrow \neg F(\ (a,x)\ )\ )$

3. Structural induction

(a) Recall the definitions of the functions *rnalen* and *basecount* from class.

i. Select all and only options that give a witness for the existential quantification

$$\exists s \in S \ (\ rnalen(s) = basecount(\ (s, \texttt{U})\ )\ )$$

A. `A`
B. `UU`
C. `CU`
D. $(\texttt{U}, 1)$
E. None of the above.

ii. Select all and only options that give a counterexample for the universal quantification

$$\forall s \in S \ (\ rnalen(s) > basecount(\ (s, \texttt{G})\ )\ )$$

A. `U`
B. `GG`
C. `AG`
D. `CUG`
E. None of the above.

iii. Select all and only the true statements

A. $\forall s \in S\ \exists b \in B\ \ (\ rnalen(s) = basecount(\ (s, b)\ )\ )$
B. $\exists s \in S\ \forall b \in B\ \ (\ rnalen(s) = basecount(\ (s, b)\ )\ )$
C.

$$\forall s_1 \in S\ \forall s_2 \in S\ \forall b \in B\ \Big(\ \big(rnalen(s_1) = basecount(\ (s_1, b)\ ) \\ \wedge\ rnalen(s_2) = basecount(\ (s_2, b)\ ) \wedge rnalen(s_1) = rnalen(s_2)\big) \rightarrow s_1 = s_2\Big)$$

D. None of the above.

(b)

Recall the set $Pos$ defined by the recursive definition

| | |
|---|---|
| Basis Step: | $(0, 0) \in Pos$ |
| Recursive Step: | If $(x, y) \in Pos$ then $(x + 1, y + 1) \in Pos$ and $(x + 1, y - 1) \in Pos$ and $(x - 1, y - 1) \in Pos$ and $(x - 1, y + 1) \in Pos$ |

i. Select all and only the ordered pairs below that are elements of $Pos$

A. $(0, 0)$
B. $(4, 0)$
C. $(1, 1)$
D. $(1.5, 2.5)$
E. $(0, -2)$

ii. What is another description of the set $Pos$ ? (Select all and only the true descriptions.)

A. $\mathbb{Z} \times \mathbb{Z}$
B. $\{(n, n) \mid n \in \mathbb{Z}\}$
C. $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid (a + b)\ \textbf{mod}\ 2 = 0\}$

4. Mathematical induction

(a)

Select all and only the true statements below about the relationship between structural induction and mathematical induction.

i. Both structural induction and mathematical induction are proof strategies that may be useful when proving universal claims about recursively defined sets.

ii. Mathematical induction is a special case of structural induction, for the case when the domain of quantification is $\{n \in \mathbb{Z} \mid n \geq b\}$ for some integer $b$.

iii. Universal claims about the set of all integers may be proved using structural induction but not using mathematical induction.

(b)

Consider the following function definitions

$$2^n : \mathbb{N} \to \mathbb{N} \text{ given by } 2^0 = 1 \quad \text{and} \quad 2^{n+1} = 2 \cdot 2^n$$

$$n! : \mathbb{N} \to \mathbb{N} \text{ given by } 0! = 1 \quad \text{and} \quad (n+1)! = (n+1)n!$$

i. Select all and only true statements below:

A. $2^0 < 0!$

B. $2^1 < 1!$

C. $2^2 < 2!$

D. $2^3 < 3!$

E. $2^4 < 4!$

F. $2^5 < 5!$

G. $2^6 < 6!$

H. $2^7 < 7!$

ii. Fill in the blanks in the following proof.

**Claim**: For all integers $n$ greater than or equal to 4, $2^n < n!$

**Proof**: We proceed by mathematical induction on the set of integers greater than or equal to 4.

**Basis step**: Using the __BLANK 1__,

$$2^4 = 2 \cdot 2^3 = 2 \cdot 2 \cdot 2^2 = 2 \cdot 2 \cdot 2 \cdot 2^1 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2^0 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 = 16$$

and

$$4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2! = 4 \cdot 3 \cdot 2 \cdot 1! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 24$$

Since $16 < 24$, we have proved that $2^4 < 4!$ , as required.

**Recursive step**: Consider an arbitrary integer $k$ that is greater than or equal to 4 and assume as the __BLANK 2__, that $2^k < k!$ . We want to show that $2^{k+1} < (k+1)!$ .

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k && \text{by } \_\_BLANK3\_\_ \\ &< 2 \cdot k! && \text{by } \_\_BLANK4\_\_ \\ &< k \cdot k! && \text{by } \_\_BLANK5\_\_ \\ &< (k+1) \cdot k! && \text{by } \_\_BLANK6\_\_ \\ &= (k+1)! && \text{by } \_\_BLANK7\_\_ \end{aligned}$$

as required.

A. properties of addition, multiplication, and $<$ for real numbers
B. definitions of the functions $2^n$ and $n!$
C. definition of $k$
D. induction hypothesis

5. Midquarter feedback