Week 5 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:

Test 1 Attempt 1 in the CBTF this week at your scheduled time!

You must present a physical university-issued or government-issued ID. Copies, photos, or digital IDs are not accepted, and students without verifiable ID will not be permitted to test.

- Pockets must be empty upon entry. Students may bring only their ID and a pen or pencil into the testing center.

Review quiz based on Week 4 class material (due Friday 02/06/2026)

Midquarter feedback: please let us know what's working well for you and what isn't. `https://canvas.ucsd.edu/courses/71479/quizzes`

Week 5 Monday: Nested Quantifiers

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

Basis Step:	$\texttt{A} \in S, \texttt{C} \in S, \texttt{U} \in S, \texttt{G} \in S$
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 $s \in S, b_1 \in B, b_2 \in B$	$basecount(\ (sb_1, b_2)\ )$	$= \begin{cases} 1 + basecount(\ (s, b_2)\ ) & \text{when } b_1 = b_2 \\ basecount(\ (s, b_2)\ ) & \text{when } b_1 \neq b_2 \end{cases}$

Alternating nested quantifiers

there exists

For all

$$\forall s \in S\ \exists n \in \mathbb{N}\ (\ basecount(\ (s, \texttt{U})\ ) = n\ )$$

In English: For each strand, there is a nonnnegative integer that counts the number of occurrences of U in that strand.

True!

$$\exists n \in \mathbb{N}\ \forall s \in S\ (\ basecount(\ (s, \texttt{U})\ ) = n\ )$$

In English: There is a nonnnegative integer that counts the number of occurrences of U in every strand.

False!

Are these statements true or false?

Original
what would it take to prove....

Negation
what would it take to prove....

$$\forall s \in S\ \exists b \in B\ (\ basecount(\ (s,b)\ ) = 3\ )$$

In English: For each RNA strand there is a base that occurs 3 times in this strand.

Write the negation and use De Morgan's law to find a logically equivalent version where the negation is applied only to the BC predicate (not next to a quantifier).

$\neg \forall s \in S\ \exists b \in B\ (\ basecount\ (\ (s,b)) = 3)$

$\equiv\ \exists s \in S\ \neg(\exists b \in B\ (basecount\ (\ (s,b)\ ) = 3\ )\ )$

$\equiv\ \exists s \in S\ \forall b \in B\ \ (basecount\ (\ (s,b)\ ) \neq 3)\ )$

Is the original statement **True** or **False**?

The original statement is false as given by counterexample

$s =$ AAAAA

Need to check: $s \in S$? yes,

$\exists b \in B\ (basecount((AAAAA, b) = 3)$ is false?

Yes, by looking at table & value.

B	$basecount((AAAAA,b)) = 3$
A	$5 = 3$? F
C	$0 = 3$? F
G	$0 = 3$? F
U	$0 = 3$? F

Proof strategies

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. This is called "Proof of universal by **exhaustion**". exhaustive proof brute-force.
- To show that $\forall x P(x)$ is false: find a **counterexample**, a domain element where $P(x)$ evaluates to F.
- To show that $\exists x P(x)$ is true: find a **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. DeMorgan's Law gives that $\neg \exists x P(x) \equiv \forall x \neg P(x)$ so this amounts to a proof of universal by exhaustion.

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: For all __________

Proof: Let ___ be an arbitrary ______ element.

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

1. ~~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~~ shouldn't write

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

find witness x_1 that makes

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

find witness x_2 that makes

$P(x_1) \wedge P(x_2)$ true.

Can "cheat" by choosing $x_2 = x_1$

but instead we could write

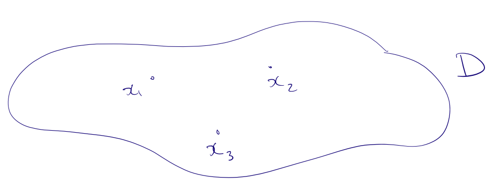
$\exists x_1 \in D \; \exists x_2 \in D \; (x_1 \neq x_2 \wedge P(x_1) \wedge P(x_2))$

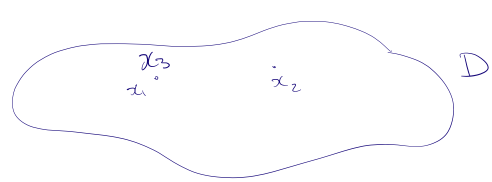
2. ~~True or False~~: To translate the statement "There are at most two elements in D where the predicate P evaluates to true", we could write

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

universal conditional

The number of (distinct) elements where predicate P evaluates to T is ≤ 2.





When $P(x_1) = T$ and $P(x_2) = T$ and $P(x_3) = T$,

Never will have that $x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3$.

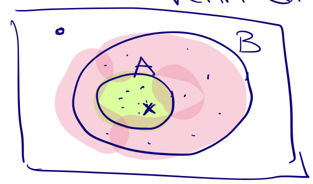
Week 5 Wednesday: Proof Strategies and Sets

Definitions:

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

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

Venn diagram



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

\subseteq

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

$x \in A$?	$x \in B$?	$x \in A \rightarrow x \in B$
T	T	T
~~T~~	~~F~~	~~F~~
F	T	T
F	F	T

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

\subsetneq

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

$\subset$ \subset : ambiguous

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. $\equiv \neg q \rightarrow \neg p$

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

HYP: $\neg p$ CONC: q

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 $p_1 \lor p_2$ 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 $p \land q$ is true, we have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.

$p \leftrightarrow q \equiv p \rightarrow q \land q \rightarrow p$

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

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

We WTS want to show $\forall x (x \in A \rightarrow x \in B)$.
Let x be an arbitrary element. Assume, towards a direct proof, that $x \in A$. WTS that $x \in B$ .....

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

We WTS $\forall x (x \in A \leftrightarrow x \in B)$. Let x be an arbitrary element
We can proceed to prove two subgoals
Goal (1) WTS $x \in A \rightarrow x \in B$.
Goal (2) WTS $x \in B \rightarrow x \in A$.

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

Let x be an arbitrary element. We WTS $x \in \{43,7,9\} \longleftrightarrow x \in \{7,43,7,9\}$.
We have two subgoals. etc...

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

ORIGINAL

$\forall x \, (x \in \{A,C,U,G\} \to x \in \{AA, AC, AU, AG\})$

ITS NEGATION

$\neg \forall (\qquad)$

$\equiv \exists x \, \neg (x \in \{A,C,U,G\} \to x \in \{AA, AC, AU, AG\})$

$\equiv \exists x \, (x \in \{A,C,U,G\} \land x \notin \{AA, AC, AU, AG\})$

Consider $x = A$ as a witness.

Evaluate

$\underbrace{A \in \{A, C, U, G\}}_{T} \land \underbrace{A \notin \{AA, AC, AU, AG\}}_{T}$.

a true statement, so $x = A$ is a witness to the statement that is logically equivalent to the negation of the original statement, so we disproved the original statement.

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

We can't use $\emptyset$ because $\emptyset \notin \emptyset$.

But we can use $B = \{\emptyset\}$ as a witness to $\exists B \, (\emptyset \in B)$.

$\{\emptyset, 1, a\}$

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

We can use $B = \emptyset$ as a counterexample to $\forall B \, (\emptyset \in B)$ because $\emptyset \notin \emptyset$.

$\{1, 2, 3\}$

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

aka $\forall X \, \forall x \, (\underbrace{x \in \emptyset}_{F} \to x \in X)$

Notice: $\emptyset \subseteq \mathbb{Z}$ but $\emptyset \notin \mathbb{Z}$

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

$\forall X (\emptyset \subsetneq X)$

Counterexample

$X = \emptyset$

even though $\emptyset \subseteq \emptyset$, it's not going to be the case that $\emptyset \neq \emptyset$ so not a proper subset.

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

Consider finding a counterexample x which makes

$x \in \{4,6\} \longrightarrow x \in \{n \mid \exists c \in \mathbb{Z} (n=4c)\}$

"the set of integer multiples of 4"

false.

extra practice

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

By exhaustion prove that

$4 \in \{n \text{ mod } 10 \mid \exists c \in \mathbb{Z} (n=4c)\}$

and $6 \in \{n \text{ mod } 10 \mid \exists c \in \mathbb{Z} (n=4c)\}$

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

or, in other words:

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

Week 5 Friday: Proof Strategies and Sets

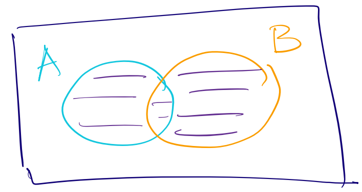
Cartesian product: When A and B are sets,

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

Example: $\{43,9\} \times \{9,\mathbb{Z}\} =$ $\{\boxed{(43,9)}, (43,\mathbb{Z}), (9,9), (9,\mathbb{Z})\}$ not equal!

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

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

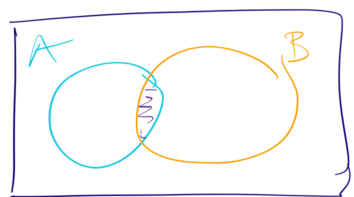


Union: When A and B are sets,

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

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

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

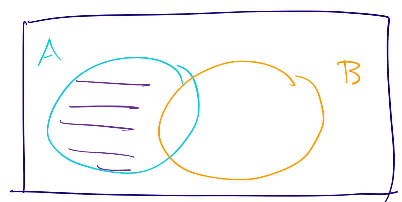


Intersection: When A and B are sets,

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

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

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



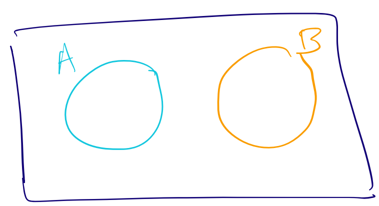
Set difference: When A and B are sets,

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

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

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

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

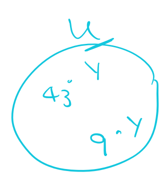


Disjoint sets: sets A and B are disjoint means $A \cap B = \emptyset$

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

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

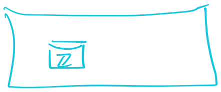
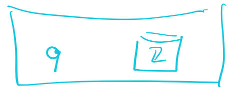
$\mathcal{P}(\{43,9,1\}) = \{\emptyset, \{1\}, \{9\}, \{43\}, \{9,43\}, \{1,43\}, \{1,9\}, \{43,9,1\}\}$

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

Need to show $\forall x\, (x \in A \to x \in B)$

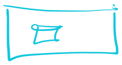
To prove that two sets are equal, e.g. to show $A = B$: $\forall x\, (x \in A \leftrightarrow x \in B)$

To prove that two sets are not equal, need $\exists x\, (x \in A \oplus x \in B)$

Example:  $\{\mathbb{Z}\} \neq \{9, \mathbb{Z}\}$ 

1 element — 2 elements

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

$W = \{X \mid X \subseteq \{1,2,3,4,5\}\}$  $\{\emptyset\} \neq \emptyset$ 

1 element — 0 elements

Example elements in W are:

$\{1\}$ $\{3,4\}$ $\emptyset$ $\{1,2,3,4,5\}$

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

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

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

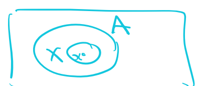
By def of subset, we WTS $\forall X \, (X \in \mathcal{P}(A) \to X \in \mathcal{P}(B))$

Consider an arbitrary X. We WTS $\underbrace{X \in \mathcal{P}(A)}_{\text{HYP}} \to \underbrace{X \in \mathcal{P}(B)}_{\text{CONC}}$.

Towards a direct proof, assume $X \in \mathcal{P}(A)$, we WTS $X \in \mathcal{P}(B)$

By definition of power sets, we WTS $X \subseteq B$.

In other words, we WTS $\forall x \, (x \in X \to x \in B)$. Consider arbitrary x. Towards direct proof, assume $x \in X$. WTS $x \in B$.

By assumption that $X \in \mathcal{P}(A)$, we know $X \subseteq A$. 

By definition of subset, since $x \in X$, also have $x \in A$. By assumption that $A \subseteq B$, and by definition of subset, since $x \in A$, $x \in B$ too.

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 sets A and B.

Assume towards direct proof that $\mathcal{P}(A) = \mathcal{P}(B)$. WTS $A = B$.

Goal ① WTS $A \subseteq B$ Consider arbitrary x and assume $x \in A$. WTS $x \in B$.

Since $x \in A$, $\{x\} \in \mathcal{P}(A)$ and since $\mathcal{P}(A) = \mathcal{P}(B)$ we have $\{x\} \in \mathcal{P}(B)$

In other words $\{x\} \subseteq B$ so by definition of subset $x \in B$, as required.

Goal ② WTS $B \subseteq A$ Consider arbitrary x and assume $x \in B$. WTS $x \in A$.

Since $x \in B$, $\{x\} \in \mathcal{P}(B)$ and since $\mathcal{P}(A) = \mathcal{P}(B)$ we have $\{x\} \in \mathcal{P}(A)$

In other words $\{x\} \subseteq A$ so by definition of subset $x \in A$, as required.

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 is choice of A, B, C where

① $A \subseteq \{1,2,3,4,5\}$

② $B \subseteq \{1,2,3,4,5\}$

③ $C \subseteq \{1,2,3,4,5\}$

④ $A \cup B = A \cup C$

⑤ $B \neq C$

