Set Theory

CSE 215, Foundations of Computer Science
Stony Brook University

http://www.cs.stonybrook.edu/~cse215
Set theory

• Set theory is a branch of mathematical logic that studies sets, which informally are collections of objects.
  • Abstract set theory is one of the foundations of mathematical thought: most mathematical objects (e.g. numbers) can be defined in terms of sets

• Let S denote a set:
  • $a \in S$ (a is a member of S) means that a is an element of S
    • Example: $1 \in \{1,2,3\}$, $3 \in \{1,2,3\}$
  • $a \notin S$ (a is not a member of S) means that a is not an element of S
    • Example: $4 \notin \{1,2,3\}$

• If S is a set and P(x) is a property that elements of S may or may not satisfy: $A = \{x \in S \mid P(x)\}$ is the set of all elements x of S such that P(x)
Subsets: Proof and Disproof

• Def.: $A \subseteq B$ (A is a subset of B) $\iff \forall x, \text{if } x \in A \text{ then } x \in B$
  (it is a formal universal conditional statement)

• Negation: $A \not\subseteq B$ (A is not a subset of B) $\iff$
  $\exists x \text{ such that } x \in A \text{ and } x \not\in B$

• A is a proper subset of B ($A \subset B$) $\iff$
  (1) $A \subseteq B$ AND
  (2) there is at least one element in B that is not in A

• Examples:
  $\{1\} \subseteq \{1\}$
  $\{1\} \subset \{1, 2\}$
  $\{1, 2\} \not\subseteq \{1, 3\}$
  $\{1\} \subset \{1, \{1\}\}$
Set Theory

- **Element Argument**: the Basic Method for Proving That One Set Is a Subset of Another

Let sets $X$ and $Y$ be given. To prove that $X \subseteq Y$,

1. Suppose that $x$ is a particular [but arbitrarily chosen] element of $X$,
2. show that $x$ is also an element of $Y$. 

Set Theory

- Example of an Element Argument Proof:
  \[ A = \{ m \in \mathbb{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbb{Z} \} \]
  \[ B = \{ n \in \mathbb{Z} \mid n = 3s \text{ for some } s \in \mathbb{Z} \} \]

**A \subseteq B?**

Suppose \( x \) is a particular but arbitrarily chosen element of \( A \).
[We must show that \( x \in B \).]

By definition of \( A \), there is an integer \( r \) such that
\[ x = 6r + 12 \iff x = 3(2r + 4) \]

But, \( s = 2r + 4 \) is an integer because products and sums of integers are integers.
\[ x = 3s. \implies \text{By definition of } B, \ x \text{ is an element of } B. \]

Therefore, \( A \subseteq B \).
Set Theory

- Disprove $B \subseteq A$: $B \not\subseteq A$.

  $A = \{m \in \mathbb{Z} | m = 6r + 12 \text{ for some } r \in \mathbb{Z}\}$
  $B = \{n \in \mathbb{Z} | n = 3s \text{ for some } s \in \mathbb{Z}\}$

  Disprove $= \text{show that the statement } B \subseteq A \text{ is false.}$

  We must find an element of $B$ ($x=3s$) that is not an element of $A$ ($x=6r+12$).

  Let $x = 3 = 3 \times 1 \Rightarrow 3 \in B$

  $3 \in A$? We assume by contradiction $\exists r \in \mathbb{Z}$, such that:
  
  $6r+12=3$ (assumption) $\Rightarrow 2r + 4 = 1 \Rightarrow 2r = -3 \Rightarrow r = -3/2$

  But $r = -3/2$ is not an integer ($\not\in \mathbb{Z}$). Thus, contradiction $\Rightarrow 3 \not\in A$.

  $3 \in B$ and $3 \not\in A$, so $B \not\subseteq A$. 

(c) Paul Fodor (CS Stony Brook)
Set Equality

• A = B, if, and only if, every element of A is in B and every element of B is in A.

\[ A = B \iff A \subseteq B \text{ and } B \subseteq A \]

• Example:

\[ A = \{m \in \mathbb{Z} \mid m = 2a \text{ for some integer } a\} \]
\[ B = \{n \in \mathbb{Z} \mid n = 2b - 2 \text{ for some integer } b\} \]

\[ A = B ? \]

• Proof Part 1: A \subseteq B

Suppose x is a particular but arbitrarily chosen element of A. By definition of A, there is an integer a such that \( x = 2a \)
\[ x = 2a + 2 - 2 = 2(a + 1) - 2 \]
Let \( b = a + 1 \), then \( x = 2b - 2 \) for some integer b
Thus, \( x \in B \).
Set Equality

- Proof Part 2: $B \subseteq A$

Suppose $x$ is a particular but arbitrarily chosen element of $B$. By definition of $B$, there is an integer $b$ such that $x = 2b - 2$

$x = 2(b - 1)$

Let $a = b - 1$, then $x = 2a$ for some integer $a$

Thus, $x \in A$.

Therefore, we proved $A = B$. 

Venn Diagrams

- $A \subseteq B$

- $A \not\subseteq B$
Relations among Sets of Numbers

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ denote the sets of integers, rational numbers, and real numbers.
- $\mathbb{Z} \subseteq \mathbb{Q}$ because every integer is rational (any integer $n$ can be written in the form $n/1$).
- $\mathbb{Z}$ is a proper subset of $\mathbb{Q}$: there are rationals that are not integers (e.g., $1/2$).
- $\mathbb{Q} \subseteq \mathbb{R}$ because every rational is real.
- $\mathbb{Q}$ is a proper subset of $\mathbb{R}$ because there are real numbers that are not rational (e.g., $\sqrt{2}$).
Operations on Sets

Let $A$ and $B$ be subsets of a universal set $U$.

1. The union of $A$ and $B$: $A \cup B$ is the set of all elements that are in at least one of $A$ or $B$:

   $$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

2. The intersection of $A$ and $B$: $A \cap B$ is the set of all elements that are common to both $A$ and $B$.

   $$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

3. The difference of $B$ minus $A$ (relative complement of $A$ in $B$): $B - A$ (or $B \setminus A$) is the set of all elements that are in $B$ and not $A$.

   $$B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$$

4. The complement of $A$: $A^c$ is the set of all elements in $U$ that are not in $A$.

   $$A^c = \{x \in U \mid x \notin A\}$$
Operations on Sets

- Example: Let $U = \{a, b, c, d, e, f, g\}$ and let $A = \{a, c, e, g\}$ and $B = \{d, e, f, g\}$.
  - $A \cup B = \{a, c, d, e, f, g\}$
  - $A \cap B = \{e, g\}$
  - $B - A = \{d, f\}$
  - $A^c = \{b, d, f\}$
Subsets of real numbers

- Given real numbers $a$ and $b$ with $a \leq b$:
  - $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$
  - $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
  - $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
  - $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

- The symbols $\infty$ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:
  - $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$
  - $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$
  - $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$
  - $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$

- A single number is denoted in the usual set notation, e.g.: $\{3\}$
Subsets of real numbers

- Example: Let
  \[ A = (-1, 0] = \{x \in \mathbb{R} \mid -1 < x \leq 0\} \]
  \[ B = [0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\} \]
  \[ A \cup B = \{x \in \mathbb{R} \mid x \in (-1, 0] \text{ or } x \in [0, 1)\} = (-1, 1) \]
  \[ A \cap B = \{x \in \mathbb{R} \mid x \in (-1, 0] \text{ and } x \in [0, 1)\} = \{0\} \]
  \[ B - A = \{x \in \mathbb{R} \mid x \in [0, 1) \text{ and } x \notin (-1, 0]\} = (0, 1) \]
  \[ A^c = \{x \in \mathbb{R} \mid \text{ it is not the case that } x \in (-1, 0]\} = (-\infty, -1] \cup (0, \infty) \]
Set theory

• **Unions and Intersections of an Indexed Collection of Sets**

  • Given sets $A_0, A_1, A_2, \ldots$ that are subsets of a universal set $U$ and given a nonnegative integer $n$ (set sequence)
  
  $\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$

  $\bigcup_{i=1}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i \}$

  $\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \ldots, n\}$

  $\bigcap_{i=1}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i \}$
Indexed Sets

- Example: for each positive integer $i$, 
  \[ A_i = \{ x \in \mathbb{R} \mid -1/i < x < 1/i \} = (-1/i, 1/i) \]
- \[ A_1 \cup A_2 \cup A_3 = \{ x \in \mathbb{R} \mid x \text{ is in at least one of the intervals } (-1, 1), (-1/2, 1/2), (-1/3, 1/3) \} = (-1, 1) \]
- \[ A_1 \cap A_2 \cap A_3 = \{ x \in \mathbb{R} \mid x \text{ is in all of the intervals } (-1, 1), (-1/2, 1/2), (-1/3, 1/3) \} = (-1/3, 1/3) \]
- \[ \bigcup_{i=1}^{\infty} A_i = \{ x \in \mathbb{R} \mid x \text{ is in at least one of the intervals } (-1/i, 1/i) \text{ where } i \text{ is a positive integer} \} = (-1, 1) \]
- \[ \bigcap_{i=1}^{\infty} A_i = \{ x \in \mathbb{R} \mid x \text{ is in all of the intervals } (-1/i, 1/i), \text{ where } i \text{ is a positive integer} \} = \{ 0 \} \]
The Empty Set \( \emptyset \ (\{\}\) )

- \( \emptyset = \{\} \) a set that has no elements
- Examples:
  - \( \{1,2\} \cap \{3,4\} = \emptyset \)
  - \( \{x \in \mathbb{R} \mid 3 < x < 2\} = \emptyset \)
Partitions of Sets

- A and B are **disjoint** ⇔ $A \cap B = \emptyset$
  - the sets A and B have no elements in common
- Sets $A_1, A_2, A_3, \ldots$ are **mutually disjoint** (pairwise disjoint or non-overlapping) ⇔ no two sets $A_i$ and $A_j$ ($i \neq j$) have any elements in common
  - $\forall i,j = 1,2,3,\ldots, i \neq j \Rightarrow A_i \cap A_j = \emptyset$
- A finite or infinite collection of nonempty sets $\{A_1,A_2, A_3,\ldots\}$ is a **partition** of a set A ⇔
  1. $A = \bigcup_{i=1}^{\infty} A_i$
  2. $A_1, A_2, A_3, \ldots$ are mutually disjoint
Partitions of Sets

• Examples:

  • \( A = \{1, 2, 3, 4, 5, 6\} \)

  \( A_1 = \{1, 2\} \quad A_2 = \{3, 4\} \quad A_3 = \{5, 6\} \)

  \( \{A_1, A_2, A_3\} \) is a partition of \( A \) because:

  \[ A = A_1 \cup A_2 \cup A_3 \]

  \( A_1, A_2 \) and \( A_3 \) are mutually disjoint:

  \[ A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset \]

  • \( T_1 = \{n \in \mathbb{Z} \mid n = 3k, \text{ for some integer } k\} \)

  \( T_2 = \{n \in \mathbb{Z} \mid n = 3k + 1, \text{ for some integer } k\} \)

  \( T_3 = \{n \in \mathbb{Z} \mid n = 3k + 2, \text{ for some integer } k\} \)

  \( \{T_1, T_2, T_3\} \) is a partition of \( \mathbb{Z} \)
Power Set

• Given a set A, the *power set* of A, P(A), is the set of all subsets of A

• Examples:

  P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}
  P(\emptyset) = \{\emptyset\}
  P(P(\emptyset)) = P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}
  P(P(P(\emptyset))) = P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}
Cartesian Product

- An **ordered n-tuple** \((x_1, x_2, ..., x_n)\) consists of the elements \(x_1, x_2, ..., x_n\) together with the ordering: first \(x_1\), then \(x_2\), and so forth up to \(x_n\).

- Two ordered n-tuples \((x_1, x_2, ..., x_n)\) and \((y_1, y_2, ..., y_n)\) are **equal**: \((x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n) \iff x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } ... x_n = y_n\)

- The **Cartesian product** of \(A_1, A_2, ..., A_n\):
  \[A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \mid a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}\]

- Example: \(A = \{1, 2\}, B = \{3, 4\}\)
  \[A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}\]
Cartesian Product

- Example: let $A = \{x, y\}$, $B = \{1, 2, 3\}$, and $C = \{a, b\}$

$A \times B \times C = \{(u,v,w) \mid u \in A, v \in B, \text{ and } w \in C\}$

$= \{(x, 1, a), (x, 2, a), (x, 3, a), (y, 1, a), (y, 2, a),$
  $(y, 3, a), (x, 1, b), (x, 2, b), (x, 3, b), (y, 1, b),$
  $(y, 2, b), (y, 3, b)\}$

$(A \times B) \times C = \{(u,v) \mid u \in A \times B \text{ and } v \in C\}$

$= \{((x, 1), a), ((x, 2), a), ((x, 3), a), ((y, 1), a),$
  $((y, 2), a), ((y, 3), a), ((x, 1), b), ((x, 2), b), ((x, 3), b),$
  $((y, 1), b), ((y, 2), b), ((y, 3), b)\}$
Properties of Sets

- Inclusion of Intersection:
  \[ A \cap B \subseteq A \quad \text{and} \quad A \cap B \subseteq B \]

- Inclusion in Union:
  \[ A \subseteq A \cup B \quad \text{and} \quad B \subseteq A \cup B \]

- Transitive Property of Subsets:
  \[ A \subseteq B \text{ and } B \subseteq C \implies A \subseteq C \]

- Elements:
  \[ x \in A \cup B \iff x \in A \text{ or } x \in B \]
  \[ x \in A \cap B \iff x \in A \text{ and } x \in B \]
  \[ x \in B - A \iff x \in B \text{ and } x \notin A \]
  \[ x \in A^c \iff x \notin A \]
  \[ (x, y) \in A \times B \iff x \in A \text{ and } y \in B \]
Proof of a Subset Relation

• For all sets A and B, \( A \cap B \subseteq A \).

The statement to be proved is universal:

\[ \forall \text{ sets } A \text{ and } B, \ A \cap B \subseteq A \]

Suppose A and B are any (particular, but arbitrarily chosen) sets.

\( A \cap B \subseteq A \), we must show \( \forall x, \ x \in A \cap B \rightarrow x \in A \)

Suppose x is any (particular but arbitrarily chosen) element in \( A \cap B \).

By definition of \( A \cap B \), \( x \in A \) and \( x \in B \).

Therefore, \( \therefore x \in A \)  

So, \( A \cap B \subseteq A \)
Set Identities

- For all sets A, B, and C:
  - Commutative Laws: $A \cup B = B \cup A$ and $A \cap B = B \cap A$
  - Associative Laws: $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
  - Distributive Laws: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - Identity Laws: $A \cup \emptyset = A$ and $A \cap U = A$
  - Complement Laws: $A \cup A^c = U$ and $A \cap A^c = \emptyset$
  - Double Complement Law: $(A^c)^c = A$
  - Idempotent Laws: $A \cup A = A$ and $A \cap A = A$
  - Universal Bound Laws: $A \cup U = U$ and $A \cap \emptyset = \emptyset$
  - De Morgan’s Laws: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$
  - Absorption Laws: $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
  - Complements of U and $\emptyset$: $U^c = \emptyset$ and $\emptyset^c = U$
  - Set Difference Law: $A - B = A \cap B^c$
Proof of a Set Identity

- For all sets A, B, and C, \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \)

Suppose A, B, and C are arbitrarily chosen sets.

1. \( A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \)

Show: \( \forall x, \text{ if } x \in A \cup (B \cap C) \text{ then } x \in (A \cup B) \cap (A \cup C) \)

Suppose \( x \in A \cup (B \cap C) \), arbitrarily chosen. (1)

We must show \( x \in (A \cup B) \cap (A \cup C) \).

From (1), by definition of union, \( x \in A \) or \( x \in B \cap C \)

Case 1.1: \( x \in A \). By definition of union: \( x \in A \cup B \) and \( x \in A \cup C \)

By definition of intersection: \( x \in (A \cup B) \cap (A \cup C) \). (2)

Case 1.2: \( x \in B \cap C \). By definition of intersection: \( x \in B \) and \( x \in C \)

By definition of union: \( x \in A \cup B \) and \( x \in A \cup C \). And (2) again.

2. \( (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C) \) (proved in similar manner)
Proof of a De Morgan’s Law for Sets

- For all sets A and B: \((A \cup B)^c = A^c \cap B^c\)

Suppose A and B are arbitrarily chosen sets.

\((\Rightarrow)\) Suppose \(x \in (A \cup B)^c\).

By definition of complement: \(x \notin A \cup B\)

it is false that \((x \text{ is in } A \text{ or } x \text{ is in } B)\)

By De Morgan’s laws of logic: \(x \text{ is not in } A \text{ and } x \text{ is not in } B.\)

\[x \notin A \text{ and } x \notin B\]

Hence \(x \in A^c \text{ and } x \in B^c\)

\[x \in A^c \cap B^c\]

\((\Leftarrow)\) Proved in similar manner.
Intersecting and Union with a Subset

- For any sets $A$ and $B$, if $A \subseteq B$, then $A \cap B = A$ and $A \cup B = B$

  $A \cap B = A \iff (1) A \cap B \subseteq A$ and $(2) A \subseteq A \cap B$

  $(1)$ $A \cap B \subseteq A$ is true by the inclusion of intersection property

  $(2)$ Suppose $x \in A$ (arbitrary chosen).

  From $A \subseteq B$, then $x \in B$ (by definition of subset relation).

  From $x \in A$ and $x \in B$, thus $x \in A \cap B$ (by definition of $\cap$)

  $A \subseteq A \cap B$

  $A \cup B = B \iff (3) A \cup B \subseteq B$ and $(4) B \subseteq A \cup B$

  $(3)$ and $(4)$ proved in similar manner to $(1)$ and $(2)$
The Empty Set Properties

• A Set with No Elements Is a Subset of Every Set:
  If E is a set with no elements and A is any set, then E ⊆ A

Proof (by contradiction): Suppose there exists an empty set E with no elements and a set A such that E ∉ A.

By definition of ∉: there is an element of E (x∈E) that is not an element of A (x∉A).

Contradiction with E was empty, so x∉E.

• Uniqueness of the Empty Set: There is only one set with no elements.

Proof: Suppose E₁ and E₂ are both sets with no elements.

By the above property: E₁⊆E₂ and E₂⊆E₁ ➔ E₁=E₂
The Element Method

- To prove that a set \( X = \emptyset \), prove that \( X \) has no elements by contradiction:
  - suppose \( X \) has an element and derive a contradiction.

- Example 1: For any set \( A \), \( A \cap \emptyset = \emptyset \).
  Proof: Let \( A \) be a particular (arbitrarily chosen) set. \( A \cap \emptyset = \emptyset \) \iff \( A \cap \emptyset \) has no elements
  Proof by contradiction: suppose there is \( x \) such that \( x \in A \cap \emptyset \).
  By definition of intersection, \( x \in A \) and \( x \in \emptyset \)
  Contradiction since \( \emptyset \) has no elements.
The Element Method

• Example 2: For all sets $A$, $B$, and $C$, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.

Proof: Suppose $A$, $B$, and $C$ are any sets such that $A \subseteq B$ and $B \subseteq C^c$

Suppose there is an element $x \in A \cap C$.

By definition of intersection, $x \in A$ and $x \in C$.

From $x \in A$ and $A \subseteq B$, by definition of subset, $x \in B$.

From $x \in B$ and $B \subseteq C^c$, by definition of subset, $x \in C^c$.

By definition of complement $x \notin C$ (contradiction with $x \in C$).
Disproofs

- Disproving an alleged set property amounts to finding a counterexample for which the property is false.

- Example: Disprove that for all sets $A, B$, and $C$,

$$ (A\setminus B) \cup (B\setminus C) = A\setminus C \ ? $$

The property is false $\iff$ there are sets $A$, $B$, and $C$ for which the equality does not hold.

Counterexample 1: $A = \{1,2,4,5\}$, $B = \{2,3,5,6\}$, $C = \{4,5,6,7\}$

$$(A\setminus B) \cup (B\setminus C) = \{1,4\} \cup \{2,3\} = \{1,2,3,4\} \neq \{1,2\} = A\setminus C$$

Counterexample 2: $A = \emptyset$, $B = \{1\}$, $C = \emptyset$

$$(A\setminus B) \cup (B\setminus C) = \{\} \cup \{1\} = \{1\} \neq \{\} = A\setminus C$$

(c) Paul Fodor (CS Stony Brook)
Cardinality of a set

- The cardinality of a set $A$: $N(A)$ or $|A|$ is a measure of the "number of elements of the set"
- Example: $|\{2, 4, 6\}| = 3$
- For any sets $A$ and $B$, 
  
  $$|A \cup B| + |A \cap B| = |A| + |B|$$
- If $A$ and $B$ are disjoint sets, then
  
  $$|A \cup B| = |A| + |B|$$
  
  $$|A \cap B| = 0$$
The Size of the Power Set

- For all int. \( n \geq 0 \), \( X \) has \( n \) elements \( \rightarrow P(X) \) has \( 2^n \) elements.

Proof (by mathematical induction): \( Q(n) \): Any set with \( n \) elements has \( 2^n \) subsets.

\( Q(0) \): Any set with 0 elements has \( 2^0 \) subsets:

The power set of the empty set \( \emptyset \) is the set \( P(\emptyset) = \{ \emptyset \} \).

\( P(\emptyset) \) has \( 1 = 2^0 \) element: the empty set \( \emptyset \).

For all integers \( k \geq 0 \), if \( Q(k) \) is true then \( Q(k+1) \) is also true.

\( Q(k) \): Any set with \( k \) elements has \( 2^k \) subsets.

We show \( Q(k+1) \): Any set with \( k + 1 \) elements has \( 2^{k+1} \) subsets.

Let \( X \) be a set with \( k + 1 \) elements and \( z \in X \) (since \( X \) has at least one element).

\( X - \{z\} \) has \( k \) elements, so \( P(X - \{z\}) \) has \( 2^k \) elements.

Any subset \( A \) of \( X - \{z\} \) is a subset of \( X \): \( A \in P(X) \).

Any subset \( A \) of \( X - \{z\} \), can also be matched with \( \{z\} \): \( A \cup \{z\} \in P(X) \)

All subsets \( A \) and \( A \cup \{z\} \) are all the subsets of \( X \) \( \Rightarrow P(X) \) has \( 2^k + 2^k = 2 \times 2^k = 2^{k+1} \) elements.
Algebraic Proofs of Set Identities

• Algebraic Proofs = Use of laws to prove new identities
  1. Commutative Laws: \( A \cup B = B \cup A \) and \( A \cap B = B \cap A \)
  2. Associative Laws: \((A \cup B) \cup C = A \cup (B \cup C)\) and \((A \cap B) \cap C = A \cap (B \cap C)\)
  3. Distributive Laws: \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \) and 
     \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \)
  4. Identity Laws: \( A \cup \emptyset = A \) and \( A \cap U = A \)
  5. Complement Laws: \( A \cup A^c = U \) and \( A \cap A^c = \emptyset \)
  6. Double Complement Law: \( (A^c)^c = A \)
  7. Idempotent Laws: \( A \cup A = A \) and \( A \cap A = A \)
  8. Universal Bound Laws: \( A \cup U = U \) and \( A \cap \emptyset = \emptyset \)
  9. De Morgan’s Laws: \( (A \cup B)^c = A^c \cap B^c \) and \( (A \cap B)^c = A^c \cup B^c \)
 10. Absorption Laws: \( A \cup (A \cap B) = A \) and \( A \cap (A \cup B) = A \)
 11. Complements of \( U \) and \( \emptyset \): \( U^c = \emptyset \) and \( \emptyset^c = U \)
 12. Set Difference Law: \( A - B = A \cap B^c \)
Algebraic Proofs of Set Identities

- Example: for all sets $A, B,$ and $C$, $(A \cup B) - C = (A - C) \cup (B - C)$.

Algebraic proof:

$$(A \cup B) - C = (A \cup B) \cap C^c \quad \text{by the set difference law}$$

$$= C^c \cap (A \cup B) \quad \text{by the commutative law for } \cap$$

$$= (C^c \cap A) \cup (C^c \cap B) \quad \text{by the distributive law}$$

$$= (A \cap C^c) \cup (B \cap C^c) \quad \text{by the commutative law for } \cap$$

$$= (A - C) \cup (B - C) \quad \text{by the set difference law.}$$
Example: for all sets $A$ and $B$, $A - (A \cap B) = A - B$.

1. $A - (A \cap B) = A \cap (A \cap B)^c$ by the set difference law
2. $= A \cap (A^c \cup B^c)$ by De Morgan’s laws
3. $= (A \cap A^c) \cup (A \cap B^c)$ by the distributive law
4. $= \emptyset \cup (A \cap B^c)$ by the complement law
5. $= (A \cap B^c) \cup \emptyset$ by the commutative law for $\cup$
6. $= A \cap B^c$ by the identity law for $\cup$
7. $= A - B$ by the set difference law.
Correspondence between logical equivalences and set identities

<table>
<thead>
<tr>
<th>Logical Equivalences</th>
<th>Set Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all statement variables $p$, $q$, and $r$:</td>
<td>For all sets $A$, $B$, and $C$:</td>
</tr>
<tr>
<td>a. $p \lor q \equiv q \lor p$</td>
<td>a. $A \cup B = B \cup A$</td>
</tr>
<tr>
<td>b. $p \land q \equiv q \land p$</td>
<td>b. $A \cap B = B \cap A$</td>
</tr>
<tr>
<td>a. $p \land (q \land r) \equiv p \land (q \land r)$</td>
<td>a. $A \land (B \cup C) = A \cup (B \cup C)$</td>
</tr>
<tr>
<td>b. $p \lor (q \lor r) \equiv p \lor (q \lor r)$</td>
<td>b. $A \land (B \cap C) = A \cap (B \cap C)$</td>
</tr>
<tr>
<td>a. $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$</td>
<td>a. $A \land (B \cup C) = (A \land B) \cup (A \land C)$</td>
</tr>
<tr>
<td>b. $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$</td>
<td>b. $A \land (B \cap C) = (A \land B) \cap (A \land C)$</td>
</tr>
<tr>
<td>a. $p \lor c \equiv p$</td>
<td>a. $A \cup \emptyset = A$</td>
</tr>
<tr>
<td>b. $p \land t \equiv p$</td>
<td>b. $A \cap U = A$</td>
</tr>
<tr>
<td>a. $p \lor \neg p \equiv t$</td>
<td>a. $A \cup A^c = U$</td>
</tr>
<tr>
<td>b. $p \land \neg p \equiv c$</td>
<td>b. $A \cap A^c = \emptyset$</td>
</tr>
<tr>
<td>$\neg (\neg p) \equiv p$</td>
<td>$(A^c)^c = A$</td>
</tr>
<tr>
<td>a. $p \lor p \equiv p$</td>
<td>a. $A \cup A = A$</td>
</tr>
<tr>
<td>b. $p \land p \equiv p$</td>
<td>b. $A \cap A = A$</td>
</tr>
<tr>
<td>a. $p \lor t \equiv t$</td>
<td>a. $A \cup U = U$</td>
</tr>
<tr>
<td>b. $p \land c \equiv c$</td>
<td>b. $A \cap \emptyset = \emptyset$</td>
</tr>
<tr>
<td>a. $\neg (p \lor q) \equiv \neg p \land \neg q$</td>
<td>a. $(A \cup B)^c = A^c \cap B^c$</td>
</tr>
<tr>
<td>b. $\neg (p \land q) \equiv \neg p \lor \neg q$</td>
<td>b. $(A \cap B)^c = A^c \cup B^c$</td>
</tr>
<tr>
<td>a. $p \lor (p \land q) \equiv p$</td>
<td>a. $A \cup (A \cap B) = A$</td>
</tr>
<tr>
<td>b. $p \land (p \lor q) \equiv p$</td>
<td>b. $A \cap (A \cup B) = A$</td>
</tr>
<tr>
<td>a. $\neg t \equiv c$</td>
<td>a. $U^c = \emptyset$</td>
</tr>
<tr>
<td>b. $\neg c \equiv t$</td>
<td>b. $\emptyset^c = U$</td>
</tr>
</tbody>
</table>
Boolean Algebra

- \( \lor \) (or) corresponds to \( \cup \) (union)
- \( \land \) (and) corresponds to \( \cap \) (intersection)
- \( \sim \) (negation) corresponds to \( ^c \) (complementation)
- \( t \) (a tautology) corresponds to \( \cup \) (a universal set)
- \( c \) (a contradiction) corresponds to \( \emptyset \) (the empty set)

- Logic and sets are special cases of the same general structure Boolean algebra.
Boolean Algebra

- A Boolean algebra is a set $B$ together with two operations $+$ and $\cdot$, such that for all $a$ and $b$ in $B$ both $a + b$ and $a \cdot b$ are in $B$ and the following properties hold:

1. Commutative Laws: For all $a$ and $b$ in $B$, $a + b = b + a$ and $a \cdot b = b \cdot a$
2. Associative Laws: For all $a$, $b$, and $c$ in $B$,
   
   $$(a + b) + c = a + (b + c) \text{ and } (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
3. Distributive Laws: For all $a$, $b$, and $c$ in $B$, $a + (b \cdot c) = (a + b) \cdot (a + c)$
   and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
4. Identity Laws: There exist distinct elements 0 and 1 in $B$ such that for all $a$ in $B$, $a + 0 = a$ and $a \cdot 1 = a$
5. Complement Laws: For each $a$ in $B$, there exists an element in $B$, $\overline{a}$, complement or negation of $a$, such that $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$
Properties of a Boolean Algebra

• Uniqueness of the Complement Law: For all $a$ and $x$ in $B$, if $a + x = 1$ and $a \cdot x = 0$ then $x = \bar{a}$

• Uniqueness of 0 and 1: If there exists $x$ in $B$ such that $a + x = a$ for all $a$ in $B$, then $x = 0$, and if there exists $y$ in $B$ such that $a \cdot y = a$ for all $a$ in $B$, then $y = 1$.

• Double Complement Law: For all $a \in B$, $(\bar{\bar{a}}) = a$

• Idempotent Law: For all $a \in B$, $a + a = a$ and $a \cdot a = a$.

• Universal Bound Law: For all $a \in B$, $a + 1 = 1$ and $a \cdot 0 = 0$.

• De Morgan’s Laws: For all $a$ and $b \in B$, $\bar{a + b} = \bar{a} \cdot \bar{b}$ and $\bar{a \cdot b} = \bar{a} + \bar{b}$

• Absorption Laws: For all $a$ and $b \in B$, $(a + b) \cdot a = a$ and $(a \cdot b) + a = a$

• Complements of 0 and 1: $\bar{0} = 1$ and $\bar{1} = 0$. 
Properties of a Boolean Algebra

- Uniqueness of the Complement Law: For all $a$ and $x$ in $B$, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$

Proof: Suppose $a$ and $x$ are particular (arbitrarily chosen) in $B$ that satisfy the hypothesis: $a + x = 1$ and $a \cdot x = 0$.

\[
\begin{align*}
x & = x \cdot 1 \quad \text{because 1 is an identity for } \cdot \\
& = x \cdot (a + \overline{a}) \quad \text{by the complement law for } + \\
& = x \cdot a + x \cdot \overline{a} \quad \text{by the distributive law for } \cdot \text{ over } + \\
& = a \cdot x + x \cdot \overline{a} \quad \text{by the commutative law for } \cdot \\
& = 0 + x \cdot \overline{a} \quad \text{by hypothesis} \\
& = a \cdot \overline{a} + x \cdot \overline{a} \quad \text{by the complement law for } \cdot \\
& = (\overline{a} \cdot a) + (\overline{a} \cdot x) \quad \text{by the commutative law for } \cdot \\
& = \overline{a} \cdot (a + x) \quad \text{by the distributive law for } \cdot \text{ over } + \\
& = \overline{a} \cdot 1 \quad \text{by hypothesis} \\
& = \overline{a} \quad \text{because 1 is an identity for } \cdot 
\end{align*}
\]
Most sets are not elements of themselves.

Imagine a set $A$ being an element of itself $A \in A$.

Let $S$ be the set of all sets that are not elements of themselves:

$$S = \{ A \mid A \text{ is a set and } A \not\in A \}$$

Is $S$ an element of itself? Yes & No contradiction.

- If $S \in S$, then $S$ does not satisfy the defining property for $S$: $S \not\in S$.
- If $S \not\in S$, then satisfies the defining property for $S$, which implies that: $S \in S$. 

(c) Paul Fodor (CS Stony Brook)
The Barber Puzzle

• In a town there is a male barber who shaves all those men, and only those men, who do not shave themselves.

• Question: Does the barber shave himself?
  • If the barber shaves himself, he is a member of the class of men who shave themselves. The barber does not shave himself because he doesn’t shave men who shave themselves.
  • If the barber does not shave himself, he is a member of the class of men who do not shave themselves. The barber shaves every man in this class, so the barber must shave himself.

Both Yes & No derive contradiction!
Russell’s Paradox

- One possible solution: except powersets, whenever a set is defined using a predicate as a defining property, the set is a subset of a *known* set.
- Then $S$ (form Russell’s Paradox) is not a set in the universe of sets.
The Halting Problem

- There is no computer algorithm that will accept any algorithm X and data set D as input and then will output “halts” or “loops forever” to indicate whether or not X terminates in a finite number of steps when X is run with data set D.

Proof sketch (by contradiction): Suppose there is an algorithm CheckHalt such that for any input algorithm X and a data set D, it prints “halts” or “loops forever”.

A new algorithm Test(X)

loops forever if CheckHalt(X, X) prints “halts” or

stops if CheckHalt(X, X) prints “loops forever”.

Test(Test) = ?

- If Test(Test) terminates after a finite number of steps, then the value of CheckHalt(Test, Test) is “halts” and so Test(Test) loops forever. Contradiction!
- If Test(Test) does not terminate after a finite number of steps, then CheckHalt(Test, Test) prints “loops forever” and so Test(Test) terminates. Contradiction!

So, CheckHalt doesn’t exist.