Set Theory

CSE 215, Foundations of Computer Science

Stony Brook University

http://www.cs.stonybrook.edu/~liu/cse215

Set theory

- Set theory is regarded as the foundation of mathematical thought.
  - All mathematical objects can be defined in terms of sets

everyday objects too

- Let S denote a set:

$a \in S$ means that a is an element of S

core of set theory

Example: $1 \in \{1,2,3\}$, $3 \in \{1,2,3\}$

$a \notin S$ 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:

$\{x \in S \mid P(x)\}$ is the set of all elements x of S such that P(x)

set comprehension/former/builder

Subsets: proof and disproof

- A is a **subset** of B

$$A \subseteq B \Leftrightarrow \forall x, \text{ if } x \in A \text{ then } x \in B$$

(it is a formal universal conditional statement)

- Negation:

$$A \nsubseteq B \Leftrightarrow \exists x \text{ such that } x \in A \text{ and } x \notin B$$

- A is a **proper subset of** B

$A \subset B \Leftrightarrow$ (1) $A \subseteq B$ and

(2) there is at least one element in B that is not in A

- Examples:

$\{1\} \subseteq \{1\}$ $\{1\} \subseteq \{1, \{1\}\}$

$\{1\} \subset \{1, 2\}$ $\{1\} \subset \{1, \{1\}\}$

Element argument

- **Element argument:**

The basic method for proving that one set is a subset of another

Let sets A and B be given.

To prove A ⊆ B

1. suppose x is a particular but arbitrarily chosen element of A,
2. show x is also an element of B.

Simpler:

take any x in A, and show x in B

Element argument: example 1

- **Example: $A \subseteq B$?**

  $A = \{m \in Z \,|\, m = 6r + 12 \text{ for some } r \in Z\}$

  $B = \{n \in Z \mid n = 3s \text{ for some } s \in Z\}$

  To prove $A \subseteq B$:

  - 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 $x = 6r + 12$, that is, $x = 3(2r + 4)$
  - $s = 2r + 4$ is an integer because products and sums of integers are integers.
  - So $x = 3s$ for integer s. By definition of B, x is an element of B.
  - Thus, $A \subseteq B$.

Element argument: example 2

- **Example:**

  $A = \{m \in \mathbf{Z} | m = 6r + 12 \text{ for some } r \in \mathbf{Z}\}$

  $B = \{n \in \mathbf{Z} \mid n = 3s \text{ for some } s \in \mathbf{Z}\}$

To disprove B ⊆ A: that is B ⊆ A is false, that is B ⊈ A

- We must find an element of B (x=3s) that is not an element of A (x=6r+12).
- Let x = 3 = 3 * 1 ➔ 3 ∈ B
- 3 ∈ A? Assume by contradiction ∃r ∈ Z, such that: 6r+12=3 (assumption) ➔2r + 4 = 1➔2r = -3➔r=-3/2

  r=-3/2 is not an integer, r ∉ Z. Thus, contradiction➔ 3∉A.
- 3 ∈ B and 3∉A, so B ⊈ A.

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:**

$A = \{m \in Z \mid m = 2a \text{ for some integer } a\}$

$B = \{n \in Z \mid n = 2b - 2 \text{ for some integer } b\}$

Proof Part 1: A ⊆ B

Suppose x is a particular but arbitrarily chosen element of A.

By definition of A, there is an integer a such that $x = 2a$

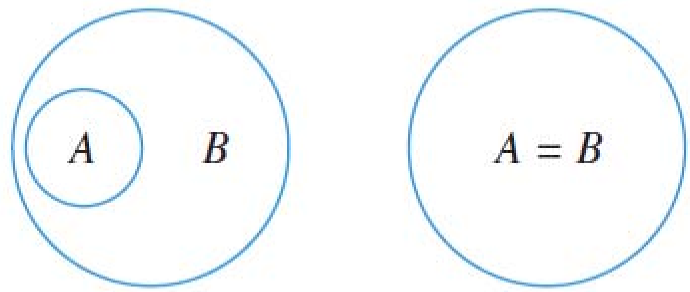
Let $b = a + 1$, $2b - 2 = 2(a + 1) - 2 = 2a + 2 - 2 = 2a = x$

Thus, $x \in B$.

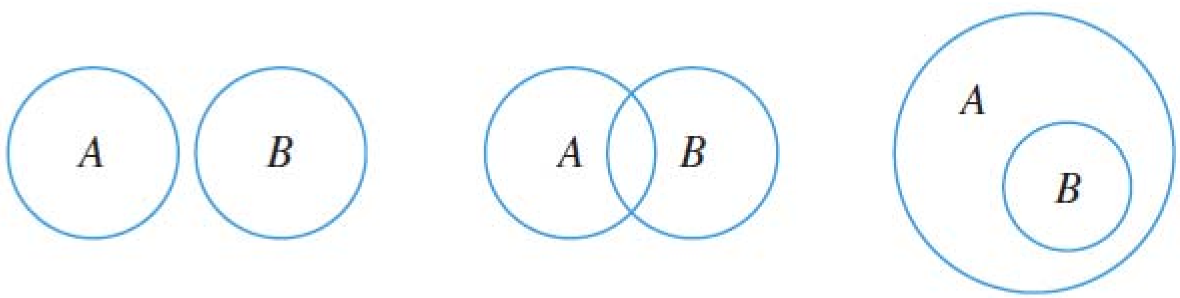
Proof Part 2: $B \subseteq A$ (proved in similar manner)

Venn diagrams

- A ⊆ B: 2 cases

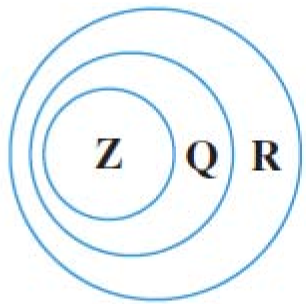


- A ⊈ B: 3 cases



Relations among sets of numbers

- **Z**, **Q**, and **R** denote the sets of integers, rational numbers, and real numbers



Z $\subseteq$ **Q** because every integer is rational (any integer n = n/1)

Z is a proper subset of **Q**

because there are rationals that are not integers (e.g., 1/2)

Q $\subseteq$ **R** because every rational is real

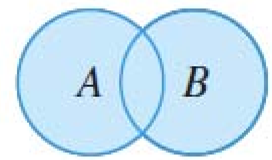
Q is a proper subset of **R**

because there are real numbers that are not rational (e.g., $\sqrt{2}$)

Operations on sets

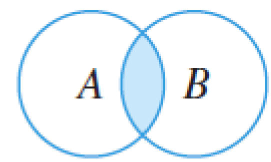
- Let A and B be subsets of a universal set U.
  - **union of A and B**:
    the set of all elements that are in at least one of A or B:

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



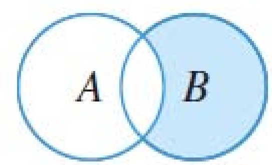
  - **intersection of A and B**:
    set of all elements that are common to both A and B.

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



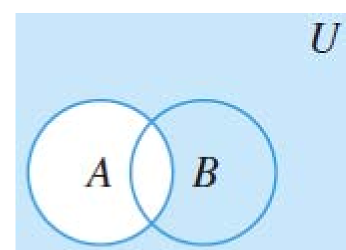
  - **difference of B minus A** (relative complement of A in B):
    B−A (or B\A) is the set of all elements that are in B and not A.

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



  - **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: examples

- Let $U = \{a, b, c, d, e, f, g\}$

  $A = \{a, c, e, g\}$

  $B = \{d, e, f, g\}$

  - $A \cup B = \{a, c, d, e, f, g\}$
  - $A \cap B = \{e, g\}$
  - $B - A = \{d, f\}$
  - $A^c = \{b, d, f\}$

Subsets of real numbers

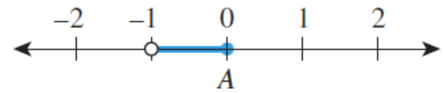
- Given real numbers a and b with $a \leq b$:
  - $(a, b) = \{x \in R \mid a < x < b\}$
  - $(a, b] = \{x \in R \mid a < x \leq b\}$
  - $[a, b) = \{x \in R \mid a \leq x < b\}$
  - $[a, b] = \{x \in R \mid a \leq x \leq b\}$

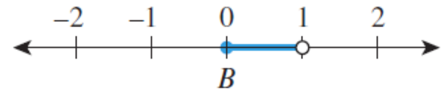
- The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:
  - $(a,\infty)=\{x \in R \mid a < x\}$
  - $[a,\infty) =\{x \in R \mid a \leq x\}$
  - $(-\infty, b)=\{x \in R \mid x < b\}$
  - $(-\infty, b]=\{x \in R \mid x \leq b\}$

Subsets of real numbers: examples

- Let $A = (-1, 0] = \{x \in R \mid -1 < x \leq 0\}$

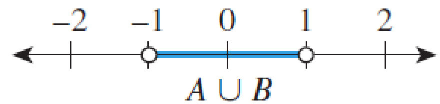
  $B = [0, 1) = \{x \in R \mid 0 \leq x < 1\}$





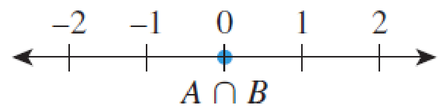
  - $A \cup B = \{x \in R \mid x \in (-1, 0] \text{ or } x \in [0, 1)\}$

    $= \{x \in R \mid x \in (-1, 1)\} = (-1, 1)$



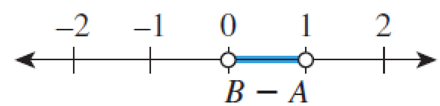
  - $A \cap B = \{x \in R \mid x \in (-1, 0] \text{ and } x \in [0, 1)\}$

    $= \{0\}$



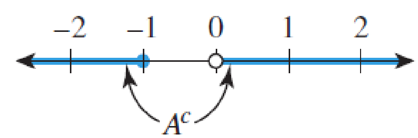
  - $B - A = \{x \in R \mid x \in [0, 1) \text{ and } x \notin (-1, 0]\}$

    $= (0, 1)$



  - $A^c = \{x \in R \mid x \notin (-1, 0]\}$

    $= (-\infty, -1] \cup (0, \infty)$



Indexed collection of sets

- **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: examples

- For each positive integer i,

  $A_i = \{x \in \mathbf{R} \mid -1/i < x < 1/i\} = (-1/i, 1/i)$

  - $A_1 \cup A_2 \cup A_3 = \{x \in \mathbf{R} \mid$ x is in at least one of the intervals $(-1,1), (-1/2, 1/2), (-1/3, 1/3)\} = (-1, 1)$
  - $A_1 \cap A_2 \cap A_3 = \{x \in \mathbf{R} \mid$ x is in all of the intervals $(-1,1), (-1/2,1/2), (-1/3, 1/3)\} = (-1/3, 1/3)$

  - $\bigcup_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid$ x is in at least one of the intervals $(-1/i, 1/i)$ where i is a positive integer$\} = (-1, 1)$
  - $\bigcap_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid$ x is in all of the intervals $(-1/i, 1/i)$, where i is a positive integer$\} = \{0\}$

The empty set

- The **empty set** $\emptyset = \{\}$ is a set that has no elements

- **Examples:**

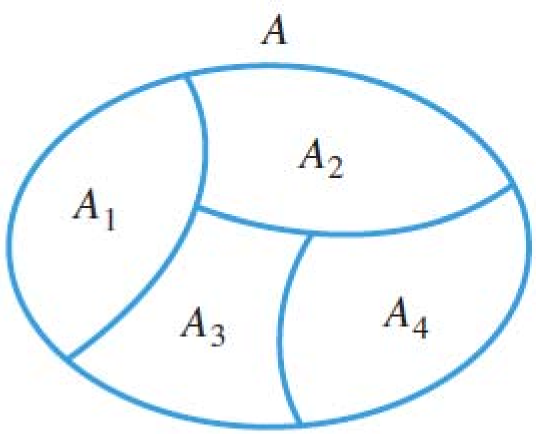
  - $\{1,2\} \cap \{3,4\} = \emptyset$

  - $\{x \in R \mid 3 < x < 2\} = \emptyset$

Partitions of sets

- A and B are **disjoint** $\Leftrightarrow A \cap B = \emptyset$
  - 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) $\Leftrightarrow \forall\, i,j = 1,2,3,\ldots,\ i \neq j \rightarrow A_i \cap A_j = \emptyset$
  - no two sets A_i and A_j $(i \neq j)$ have any elements in common
- A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3, \ldots\}$ is a **partition** of a set A $\Leftrightarrow$

1. $A = \bigcup_{i=1}^{\infty} A_i$
2. $A_1, A_2, A_3, \ldots$ are mutually disjoint



Partitions of sets: example

- $A = \{1, 2, 3, 4, 5, 6\}$

  $A_1 = \{1, 2\}$ $A_2 = \{3, 4\}$ $A_3 = \{5, 6\}$

  $\{A_1, A_2, A_3\}$ is a partition of A, because

  1. $A = A_1 \cup A_2 \cup A_3$
  2. A_1, A_2 and A_3 are mutually disjoint:

  $$A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$$

- $T_1 = \{n \in \mathbf{Z} \mid n = 3k, \text{ for some integer } k\}$

  $T_2 = \{n \in \mathbf{Z} \mid n = 3k + 1, \text{ for some integer } k\}$

  $T_3 = \{n \in \mathbf{Z} \mid n = 3k + 2, \text{ for some integer } k\}$

  $\{T_1, T_2, T_3\}$ is a partition of $\mathbf{Z}$

Power set

- Given a set A,

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

- **Examples:**

  - $P(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$
  - $P(\emptyset) = \{\emptyset\}$
  - $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Cartesian product

- An **ordered n-tuple** $(x_1,x_2,\ldots,x_n)$ consists of the elements $x_1,x_2,\ldots,x_n$ together with the ordering: first x_1, then x_2, and so forth up to x_n
- Two ordered n-tuples $(x_1,x_2,\ldots,x_n)$ and $(y_1,y_2,\ldots,y_n)$ are **equal:**

  $(x_1,x_2,\ldots,x_n)=(y_1,y_2,\ldots,y_n) \Leftrightarrow x_1=y_1$ and $x_2=y_2$ and … $x_n=y_n$

- The **Cartesian product** of $A_1,A_2,\ldots,A_n$:

  $$A_1\times A_2\times\ldots\times A_n=\{(a_1, a_2,\ldots, a_n) \mid a_1\in A_1, a_2\in A_2,\ldots, a_n\in A_n\}$$

- **Example:** $A=\{1,2\}$, $B=\{3,4\}$

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

Cartesian product: more examples

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

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

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

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

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

Supplemental: Algorithm to check subset

- **Input:** m, n [positive integers], A,B [one-dimensional arrays]

Algorithm body:

```
i := 1,    answer := "A ⊆ B"
while (i ≤ m   and   answer = "A ⊆ B")
        j := 1,   found := "no"
        while (j ≤ n   and   found = "no")
                if a[i] = b[j] then found := "yes"
                j := j + 1
        end while
        if found = "no" then answer := "A ⊈ B"
        i := i + 1
end while
Output: answer [a string]: "A ⊆ B" or "A ⊈ B"
```

complicated
and inefficient too

```
answer = "A ⊆ B" if … else "A ⊈ B"
```

```
each(x in A, has=x in B)   da
all( x in B  for x in A)   da/py
each x in A  has x in B    abc
forall x in A |  x in B    setl
```

Properties of sets

- Inclusion of intersection: $A \cap B \subseteq A$ and $A \cap B \subseteq B$
- Inclusion in union: $A \subseteq A \cup B$ and $B \subseteq A \cup B$
- Transitivity of subset: $A \subseteq B$ and $B \subseteq C \rightarrow A \subseteq C$

- Set operations: logical definitions (textbook calls them procedural)
  - $x \in A \cup B \Leftrightarrow x \in A$ or $x \in B$
  - $x \in A \cap B \Leftrightarrow x \in A$ and $x \in B$
  - $x \in B - A \Leftrightarrow x \in B$ and $x \notin A$
  - $x \in A^c \Leftrightarrow x \notin A$
  - $(x, y) \in A \times B \Leftrightarrow x \in A$ and $y \in B$

in given file sets.da

```
setof(x, x in A, x in B)  da
{x for x in A if x in B}  da/py
{x: x in A, x in B}       da ideal
```

Example proof: inclusion of intersection

- For all sets A and B, **$A \cap B \subseteq A$**
  - The statement to be proved is universal:

    $\forall$ sets A and B, $A \cap B \subseteq A$

  - Suppose A and B are any two particular but arbitrarily chosen sets.
  - To show $A \cap B \subseteq A$, 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, $x \in A$

Q.E.D.

Set identities

- For all sets A, B, and C:
  - Commutativity: $A \cup B = B \cup A$ and $A \cap B = B \cap A$
  - Associativity: $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
  - Distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - 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: $(A^c)^c = A$
  - 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: $A - B = A \cap B^c$

Example proof: distributivity

- 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.
  - **Part 1.** $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

    To show: $\forall x$, if $x \in A \cup (B \cap C)$ then $x \in (A \cup B) \cap (A \cup C)$

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

    Then by definition of union, $x \in A$ or $x \in B \cap C$

    Case 1: $x \in A$. By definition of union, $x \in A \cup B$ and $x \in A \cup C$

    By definition of intersection: $x \in (A \cup B) \cap (A \cup C)$ (*)

    Case 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 $x \in A \cup C$. So (*) again

  - **Part 2.** $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ (proved in similar manner)

Example proof: De Morgan's law

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

  - Suppose A and B are arbitrarily chosen sets.
  - (➔) Suppose $x \in (A \cup B)^c$.

    By definition of complement: $x \notin A \cup B$

    That is, it is false that (x is in A or x is in B)

    By De Morgan's laws of logic: x is **not** in A and x is **not** in B

    That is, $x \notin A$ and $x \notin B$

    By definition of complement: $x \in A^c$ and $x \in B^c$

    By definition of intersection: $x \in A^c \cap B^c$

  - (🡐) Proved in similar manner.

Intersection and union with a subset

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

$A \cap B = A \Leftrightarrow$ (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 $\cap$)

So, $A \subseteq A \cap B$

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

(3) and (4) are proved in similar manner to (1) and (2)

The empty set: two 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 is a 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 has no element.

  So E ⊆ A. **Q.E.D.**

- **Uniqueness of the empty set**

  There is only one set with no elements.

  Proof: Suppose E_1 and E_2 are both sets with no elements.

  By the above property: $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ ➔ $E_1 = E_2$ **Q.E.D.**

Element method for proving $\emptyset$

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

- **Example**: For any set A, $A \cap \emptyset = \emptyset$.

Proof: Let A be a particular but arbitrarily chosen set.

$$A \cap \emptyset = \emptyset \Leftrightarrow A \cap \emptyset \text{ has no elements}$$

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 with $\emptyset$ having no elements. **Q.E.D.**

Element method: example 2

- **Example**: 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 $B \subseteq C^c$

Proof by contradiction: 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, $x \in C^c$.

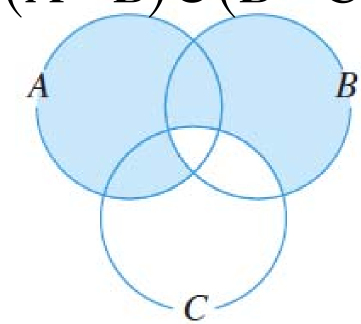
By definition of complement $x \notin C$. Contradiction with $x \in C$.

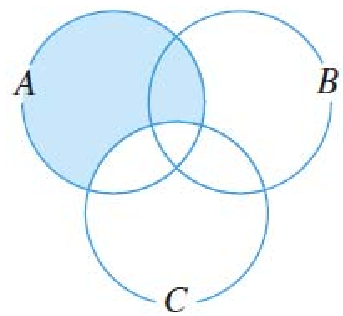
Q.E.D.

More proofs

- 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,

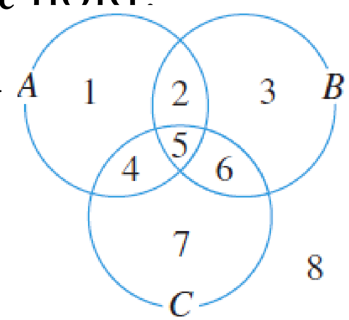
$$(A-B)\cup(B-C) \quad = \quad A-C$$





There are sets A, B, and C for which the equality does not hold.

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



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

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

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

  $$|A \cup B| = |A| + |B|$$

Number of subsets of a set

- For all integer $n \geq 0$, **X has n elements → P(X) has 2^n elements**

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

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

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

P(Ø) has $1=2^0$ element: the empty set Ø.

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

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

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

Let X be a set with k+1 elements and z ∈ 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 ∈ P(X).

Any subset A of X−{z}, can also be matched up with {z}: A∪{z} ∈ P(X)

All subsets A and A∪{z} are all the subsets of X → P(X) has $2*2^k=2^{k+1}$ elements

Algebraic proofs of set identities

- Algebraic proofs = Use of laws to prove new identities
  - Commutativity: $A \cup B = B \cup A$ and $A \cap B = B \cap A$
  - Associativity: $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
  - Distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - 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: $(A^c)^c = A$
  - 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: $A - B = A \cap B^c$

Algebraic proofs: example 1

- For all sets A, B, and C,

$$(A \cup B) - C = (A - C) \cup (B - C)$$

Proof:

$(A \cup B) - C$	$= (A \cup B) \cap C^c$	by set difference law
	$= C^c \cap (A \cup B)$	by commutative law for $\cap$
	$= (C^c \cap A) \cup (C^c \cap B)$	by distributive law
	$= (A \cap C^c) \cup (B \cap C^c)$	by commutative law for $\cap$
	$= (A - C) \cup (B - C)$	by set difference law

Algebraic proofs: example 2

- For all sets A and B,

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

Proof:

$A - (A \cap B)$	$= A \cap (A \cap B)^c$	by set difference law
	$= A \cap (A^c \cup B^c)$	by De Morgan's laws
	$= (A \cap A^c) \cup (A \cap B^c)$	by distributive law
	$= \emptyset \cup (A \cap B^c)$	by complement law
	$= (A \cap B^c) \cup \emptyset$	by commutative law for $\cup$
	$= A \cap B^c$	by identity law for $\cup$
	$= A - B$	by set difference law

Logical equivalences vs set identities

Logical Equivalences	Set Properties
For all statement variables p, q, and r:	For all sets A, B, and C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv p \wedge (q \wedge r)$ b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	a. $A \cup (B \cup C) = A \cup (B \cup C)$ b. $A \cap (B \cap C) = A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$
a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \emptyset$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \emptyset = \emptyset$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$
a. $p \vee (p \wedge q) \equiv p$ b. $p \wedge (p \vee q) \equiv p$	a. $A \cup (A \cap B) = A$ b. $A \cap (A \cup B) = A$
a. $\sim \mathbf{t} \equiv \mathbf{c}$ b. $\sim \mathbf{c} \equiv \mathbf{t}$	a. $U^c = \emptyset$ b. $\emptyset^c = U$

Boolean algebra

- Logic vs sets

  - ∨ (or) corresponds to ∪ (union)
  - ∧ (and) corresponds to ∩ (intersection)
  - ~ (negation) corresponds to ^{c} (complementation)
  - t (a tautology) corresponds to U (a universal set)
  - c (a contradiction) corresponds to ∅ (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 · , such that, for all a and b in B, both a + b and a · b are in B and the following properties hold:
  - Commutativity: for all a and b in B, $a+b=b+a$ and $a \cdot b=b \cdot a$
  - Associativity: for all a,b, c in B,

    $(a+b)+c=a+(b+c)$ and $(a \cdot b) \cdot c=a \cdot (b \cdot c)$
  - Distributivity: for all a, b, and c in B,

    $a+(b \cdot c)=(a+b) \cdot (a+c)$ and $a \cdot (b+c)=(a \cdot b)+(a \cdot c)$
  - Identity laws: there exist distinct elements 0 and 1 in B

    such that for all a in B, $a+0=a$ and $a \cdot 1=a$
  - 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 $x=\overline{a}$
- 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 $a \in B$, $\overline{(\overline{a})} = a$
- 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 $b \in B$, $\overline{a+b}=\overline{a} \cdot \overline{b}$ and $\overline{a \cdot b}=\overline{a}+\overline{b}$
- 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: $\overline{0} = 1$ and $\overline{1} = 0$.

Example proof

- **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 $a \cdot x=0$.

$x = x \cdot 1$	because 1 is an identity for ·
$= x \cdot (a + \overline{a})$	by the complement law for +
$= x \cdot a + x \cdot \overline{a}$	by the distributive law for · over +
$= a \cdot x + x \cdot \overline{a}$	by the commutative law for ·
$= 0 + x \cdot \overline{a}$	by hypothesis
$= a \cdot \overline{a} + x \cdot \overline{a}$	by the complement law for ·
$= (\overline{a} \cdot a) + (\overline{a} \cdot x)$	by the commutative law for ·
$= \overline{a} \cdot (a + x)$	by the distributive law for · over +
$= \overline{a} \cdot 1$	by hypothesis
$= \overline{a}$	because 1 is an identity for ·

Russell's paradox

- Most sets are not elements of themselves. A possible exception: The set of all abstract ideas might be considered an abstract idea.
- 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:

$$S = \{A \mid A \text{ is a set and } A \notin A\}$$

- Is S an element of itself?
  - If $S \in S$, then S does not satisfy the defining property for S, so $S \notin S$.
  - If $S \notin S$, then satisfies the defining property for S, so $S \in S$.
- It cannot be either!

Russell’s paradox: 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.

- 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 solution

- Except for power set, whose existence is guaranteed by an axiom, whenever a set is defined using a predicate as a defining property, the set is a subset of a known set. (elements are from a known set)

- Then, S from Russell's Paradox is not a subset of a known set

  S = {A | A is a set and A ∉ A} (A's are not from a known set)

  A ∈ S ⇔ A is a set and A ∉ A

  A in S ⇔ A is a set and A not in A

  B shave A ⇔ A is a man and A not shave A

- Solution is good for practical examples:

  S = {x in blocks | x is blue}

The halting problem

- There is no computer algorithm that will accept any algorithm X and data set D as input and then 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 CheckHalt(Test, Test) prints "halts", 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", so Test(Test) terminates. Contradiction!

So, CheckHalt doesn't exist.