Set Theory

CSX2008 Mathematics Foundation for Computer Science

Department of Computer Science
Vincent Mary School of Science and Technology
Assumption University

Session Outline

- Set Theory
  - Review of basic definitions and notations
  - Properties of Subsets, the Empty set and Power sets
  - Proving and Disproving Properties of Sets and Set Identities
- Boolean Algebra

Set Definitions

Axiom of extension: a set is completely determined by what its elements are, regardless of the frequency nor the order of listing.

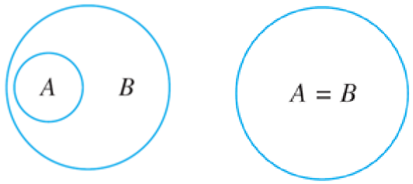
- In formal set theory, the words “set” and “element” are undefined terms.
- Just like “sentence”, “true”, “false” are undefined terms in Formal Logic
  - e.g. A statement is a sentence that can be determined true or false.
- Informally, think of a set as an unordered collection of elements (disregarding duplicates)
  - If *C* is the set of all the students in this class, then ‘Shiv’ is an element of *C*.

Set Notations

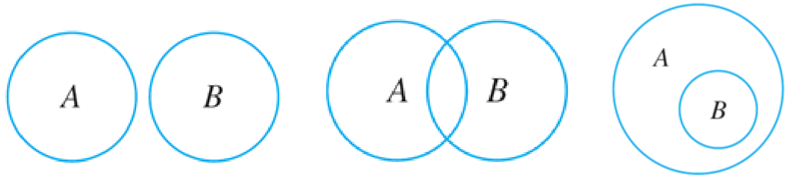
- Notations:
  - $x \in S$ means x is an element of the set S
  - $x \notin S$ means x is not an element of the set S
- Set-Roster notation
  - $A = \{ 3, 7, 9 \}$
  - $B = \{ 1, 2, 3, \ldots, 100 \}$
  - $C = \{ 1, 2, 3, \ldots \}$
- Set-Builder notation
  - $A = \{x \in S \mid P(x) \}$
  - e.g.) $A = \{x \in \mathbf{Z} \mid x = 2k$ for some integer $k. \}$

Subsets and Proper Subsets

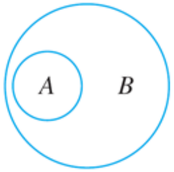
- $A \subseteq B$
  - set A is a **subset** of set B
  - $A \subseteq B \Leftrightarrow \forall x \in A, x \in B$



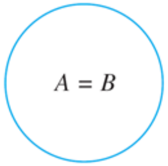
- $A \nsubseteq B$
  - set A is **not a subset** of set B
  - **Negation of subset** notation; therefore
  - $A \nsubseteq B \Leftrightarrow \exists x \in A$ such that $x \notin B$



- $A \subset B$
  - set A is a **proper subset** of B
  - $A \subset B \Leftrightarrow A \subseteq B$ and $A \neq B$
  - $A \subset B \Leftrightarrow (\forall x \in A, x \in B) \land (\exists x \in B$ such that $x \notin A)$

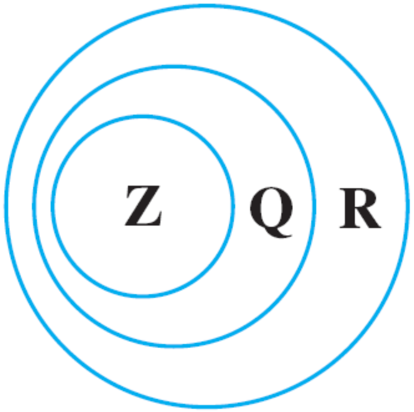


- $A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$
  - a set A **equals** to set B
  - To Prove $A = B$, we must show both that $A \subseteq B$ and that $B \subseteq A$



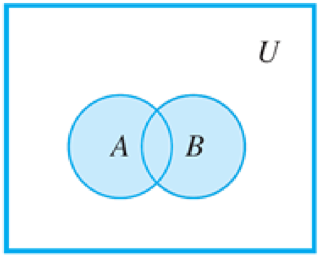
Common Sets of Numbers

- **R** set of all real numbers
- **Z** set of all integers
- **Q** set of all rational numbers (quotients)
- **R^-** set of negative real numbers
- **Z^+** set of positive integers
- **Z^{nonneg}** set of nonnegative integers i.e., {0, 1, 2, …}
- **N** set of natural numbers
  - could mean **Z^+ or Z^{nonneg}** depending on writers
  - **We avoid this terminology in this class**



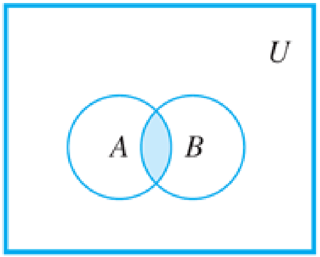
Common Set Operations (1)

- A Universal Set *aka* A Universe of Disclosure
  - A universal set is the collection of all objects in a particular context.
    - Precise definition depends on the context under consideration
  - Usually denoted as an uppercase italicized letter ***U***.
  - Note that all other sets in the context constitute subsets of the universal set.
- $\boldsymbol{A \cup B}$
  - The **union** of *A* and *B*
  - $A \cup B = \{ x \in U \mid x \in A$ **or** $x \in B \}$

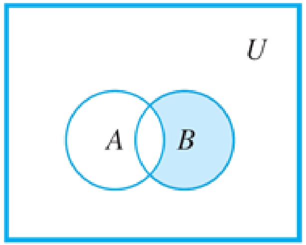


Common Set Operations (2)

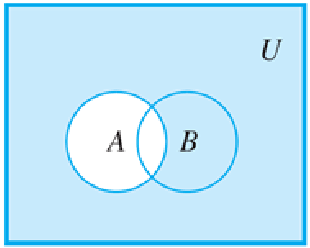
- $\boldsymbol{A \cap B}$
  - The intersection of A and B
  - $A \cap B = \{ x \in U \mid x \in A \textbf{ and } x \in B \}$



- $\boldsymbol{B - A}$
  - The difference of B minus A (or relative complement of A in B)
  - $B - A = \{ x \in U \mid x \in B \textbf{ and } x \notin A \}$



- $\boldsymbol{A^c}$
  - The complement of A
  - $A^c = \{ x \in U \mid x \notin A \}$



Unions and Intersections of Multiple sets

- **Definition**

Unions and Intersections of an $\boxed{\text{Indexed Collection of Sets}}$

Given sets $A_0,\ A_1,\ A_2, \ldots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

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

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i\}.$$

$$\bigcup_{i=0}^{n} A_i = A_0 \cup A_1 \cup \cdots \cup A_n$$

$$\bigcap_{i=0}^{n} A_i = A_0 \cap A_1 \cap \cdots \cap A_n$$

Intervals

- Real number line is continuous
- How many real numbers are there between 0.4 and 0.5?
- A convenient notation for subset of real numbers that are intervals: (*a*,*b*), [*a*,*b*], (*a*, *b*], [*a*, *b*)
  - (,) represents Excluding
  - [,] represents Including

• Notation

Given real numbers a and b with $a \le b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a,\ b] = \{x \in \mathbf{R} \mid a \le x \le b\}$$

$$(a, b] = \{x \in \mathbf{R} \mid a < x \le b\} \qquad [a,\ b) = \{x \in \mathbf{R} \mid a \le x < b\}.$$

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \qquad [a, \infty) = \{x \in \mathbf{R} \mid x \ge a\}$$

$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \qquad [-\infty, b) = \{x \in \mathbf{R} \mid x \le b\}.$$

Note that the **End point of unbounded side** is always "**Excluding**"

- Since no real number can actually equal infinity.

Intervals

- **Notation**

Given real numbers a and b with $a \le b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a, b] = \{x \in \mathbf{R} \mid a \le x \le b\}$$

$$(a, b] = \{x \in \mathbf{R} \mid a < x \le b\} \qquad [a, b) = \{x \in \mathbf{R} \mid a \le x < b\}.$$

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \qquad [a, \infty) = \{x \in \mathbf{R} \mid x \ge a\}$$

$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \qquad [-\infty, b) = \{x \in \mathbf{R} \mid x \le b\}.$$

Note that the end point of unbounded side is always "Excluding"

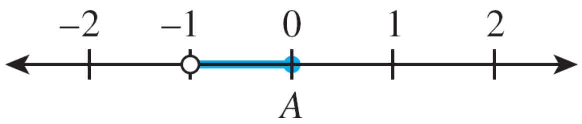
- Since no real number can actually equal infinity.

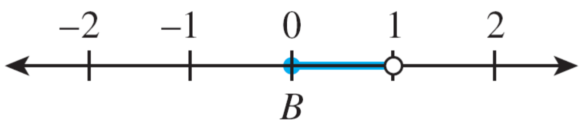
Exercises

Let A = (-1, 0] and B = [0, 1)

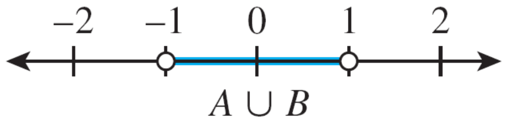
Find $A \cup B$, $A \cap B$, $B - A$, and A^c

Note that implied universe of disclosure is R

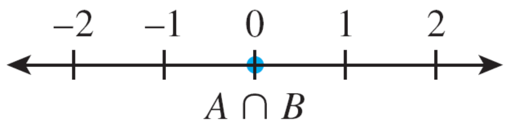




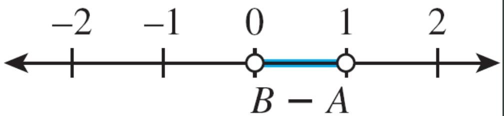
- $A = (-1, 0] = \{x \in \mathbf{R} \mid -1 < x \leq 0\}$
- $B = [0, 1) = \{x \in \mathbf{R} \mid 0 \leq x < 1\}$
- $A \cup B$ $= \{x \in \mathbf{R} \mid x \in (-1, 0] \text{ or } x \in [0, 1)\}$
  $= \{x \in \mathbf{R} \mid -1 < x \leq 0 \text{ or } 0 \leq x < 1\}$
  $= \{x \in \mathbf{R} \mid -1 <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



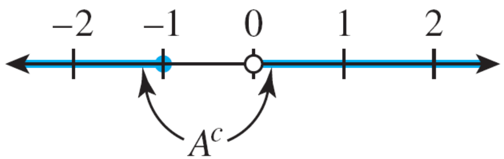
- $A \cap B = \{0\}$
  - Why?



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



- A^c $= \{x \in \mathbf{R} \mid \text{it is not the case that } x \in (-1, 0]\}$
  $= \{x \in \mathbf{R} \mid \text{it is not the case that } (-1 < x \text{ and } x \leq 0)\}$
  $= \{x \in \mathbf{R} \mid -1 \geq x \text{ or } x > 0)\} = \{x \in \mathbf{R} \mid x \leq -1 \text{ or } x > 0)\}$
  $= (-\infty, -1] \cup (0, \infty)$



Exercises

$$A_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} < x < \frac{1}{i}\right\} = A_i = \left(-\frac{1}{i}, \frac{1}{i}\right).$$

Find $A_1 \cup A_2 \cup A_3$ and $A_1 \cap A_2 \cap A_3$.

For each positive integer *i*, let

$$A_1 \cup A_2 \cup A_3 = \left\{x \in \mathbf{R} \mid x \text{ is in at least one of the intervals } (-1, 1), \text{ or } \left(-\frac{1}{2}, \frac{1}{2}\right), \text{ or } \left(-\frac{1}{3}, \frac{1}{3}\right)\right\}$$

$= \{x \in \mathbf{R} \mid -1 < x < 1\}$ because all the elements in $\left(-\frac{1}{2}, \frac{1}{2}\right)$ and $\left(-\frac{1}{3}, \frac{1}{3}\right)$ are in $(-1, 1)$

$= (-1, 1)$

$$A_1 \cap A_2 \cap A_3 = \left\{x \in \mathbf{R} \mid x \text{ is in all of the intervals } (-1, 1), \text{ and } \left(-\frac{1}{2}, \frac{1}{2}\right), \text{ and } \left(-\frac{1}{3}, \frac{1}{3}\right)\right\}$$

$= \left\{x \in \mathbf{R} \mid -\frac{1}{3} < x < \frac{1}{3}\right\}$ because $\left(-\frac{1}{3}, \frac{1}{3}\right) \subseteq \left(-\frac{1}{2}, \frac{1}{2}\right) \subseteq (-1, 1)$

$= \left(-\frac{1}{3}, \frac{1}{3}\right)$

The Empty Set (1)

Can there be a set that has no elements?

- For the elegance and convenience of the set theory, we allow such a set called empty set denoted $\emptyset$.
  - Similar reasons for defining $0! = 1$.
  - e.g.) $\{1, 3\} \cap \{2, 4\} = \emptyset$
- There is a reason why we call it the empty set.
  - because there is only one such set
  - Uniqueness of the empty set

The Empty Set (2)

Theorem: An empty set is a subset of every set.

Proof (by Contradiction)

Suppose Not. Suppose there exists a p.b.a.c. set *E* with no elements and a p.b.a.c. set *A* such that $\boldsymbol{E \not\subseteq A}$.

Then by the definition of subset, there would be an element of *E* that is not an element of *A*.

But there can be no such element since *E* has no element.

This is a contradiction.

Thus the supposition is false, and therefore, the theorem an empty set is a subset of every set is true

The Empty Set (3)

Theorem: An empty set is a subset of every set.

It follows from the above theorem that there is only one set with no elements.

- Thus the empty set is unique.

The Empty Set (4)

Corollary: Uniqueness of the empty set

Proof:

Suppose E_1 and E_2 are both sets with no elements.
By the above theorem, $E_1 \subseteq E_2$ since E_1 has no elements.

It is also case that $E_2 \subseteq E_1$ since E_2 has no elements.
Thus, $E_1 = E_2$ by definition of set equality.
Therefore, there is only one set with no elements.

- So in order to show that a certain set is *the* empty set, you just need to show that it has no elements.
  - Usually by Proof by Contradiction
  - Suppose Not: Suppose Not Empty and show it leads to a contradiction

Power Sets

- **Definition**

Given a set A, the **power set** of A, denoted $\mathscr{P}(A)$, is the set of all subsets of A.

The importance of The power set axiom is that it **is a set**.

- The set of **all subsets** of a set.

Find the power set of {x,y}.

- What are the subsets of {x,y}?

- Don’t forget that the empty set is a subset of every set

Theorem 6.3.1

For all integers $n \geq 0$, if a set X has n elements, then $\mathscr{P}(X)$ has 2^n elements.

How can we prove it by method of Mathematical Induction?

Theorem 6.3.1

For all integers $n \geq 0$, if a set X has n elements, then $\mathscr{P}(X)$ has 2^n elements.

Suppose *X* is a set and *a* is an element of *X*.
(*X* has at least one element)

- The subsets of *X* can be split into two groups:
  - Those that contain *a*.
  - Those that do not contain *a*;
- The subsets of *X* that do not contain *a* are the same as the subsets of $(X - \{a\})$
- There are as many subsets of *X* that contain *a* as there are subsets of *X* that do not contain *a*.
  - Assume *A* is a subset of *X* that does not contain *a*.
  - Then, $A \cup \{a\}$ is a subset of *X* that contains *a*.
- Demonstrative Example: Let $X = \{ a, b, c\}$
  - Subsets of *X* that do Not contain *a*.
    - $\emptyset$, $\{b\}$, $\{c\}$, $\{b, c\}$
  - Subsets of *X* that contains *a*.
    - $\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}$

Got the idea how to prove?

- Number of subsets of a set having *k* elements
- is equal to twice the number of subsets of a set having $k - 1$ elements.

Proof of Theorem 6.3.1

Proof (by mathematical induction):

Let the property $P(n)$ be the following sentence:

Any set with n elements has 2^n subsets.

Basis Step:
The only set with zero elements is the empty set, and the only subset of the empty set is itself.

Thus a set with zero element has one subset.

Since $1 = 2^0$, $P(0)$ is true.

Inductive Step:
Suppose that any set with k elements has 2^k subsets for a p.b.a.c. integer $k \geq 0$.
We need to show that any set with $k + 1$ elements has 2^{k+1} subsets.

Let X be a set with $k + 1$ elements.
Since $k + 1 \geq 1$, we may select an element a in X.
Observe that any subset of X either contains a or not.

Proof of Theorem 6.3.1 (cont'd)

Let X be a set with $k + 1$ elements.

Since $k + 1 \geq 1$, we may select an element a in X.

Observe that any subset of X either contains a or not. Let $T = X - \{a\}$.

Note that any subset of X that do not contain a is a subset of T.

And any subset A of T can be matched up with a subset B of X that contains a such that $B = A \cup \{a\}$.

Consequently, there are as many subsets of X that contain a as those that do not.

Thus, there are twice as many subsets of X as there are subsets of $X - \{a\}$.

But $X - \{a\}$ has k elements [since X has $k + 1$ elements]

So the number of subsets of $X - \{a\} = 2^k$ [by the inductive hypothesis].

Therefore, the number of subsets of $X = 2 \cdot (2^k)$

$= 2^{k+1}$ [as was to be shown] Q.E.D.

Disjoint Sets

• Definition

Two sets are called **disjoint** if, and only if, they have no elements in common.
Symbolically:

$$A \text{ and } B \text{ are disjoint} \quad \Leftrightarrow \quad A \cap B = \emptyset.$$

• Definition

Sets $A_1, A_2, A_3 \ldots$ are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) if, and only if, no two sets A_i and A_j with distinct subscripts have any elements in common. More precisely, for all $i, j = 1, 2, 3, \ldots$

$$A_i \cap A_j = \emptyset \quad \text{whenever } i \neq j.$$

Exercises

- Let $A_1 = \{3, 5\}$, $A_2 = \{1, 4, 6\}$, and $A_3 = \{2\}$. Are A_1, A_2, and A_3 mutually disjoint?

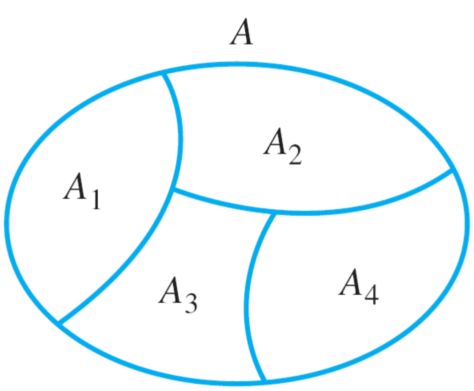
- Let $B_1 = \{2, 4, 6\}$, $B_2 = \{3, 7\}$, and $B_3 = \{4, 5\}$. Are B_1, B_2, and B_3 mutually disjoint?

Partition of Sets

- **Definition**

A finite or infinite collection of $\boxed{\text{nonempty sets } \{A_1, A_2, A_3 \ldots\}}$ is a **partition** of a set A if, and only if,

1. A is the union of all the A_i
2. The sets $A_1, A_2, A_3, \ldots$ are mutually disjoint.



$A = A_1 \cup A_2 \cup A_3 \cup A_4$

A_1 , A_2 , A_3 and A_4 are mutually disjoint

So $\{ A_1 , A_2 , A_3 , A_4 \}$ is a partition of the set A.

A is a union of mutually disjoint subsets.

Exercise

Let $T_0 = \{ n \in \mathbf{Z} \mid n = 3k, \text{ for some integer } k \}$

$T_1 = \{ n \in \mathbf{Z} \mid n = 3k + 1, \text{ for some integer } k \}$

$T_2 = \{ n \in \mathbf{Z} \mid n = 3k + 2, \text{ for some integer } k \}$

Is $\{T_0, T_1, T_2\}$ a partition of **Z**?

- $\mathbf{Z} = T_0 \cup T_1 \cup T_2$

Exercises

- Let $A = \{a, b\}$. Find all the partitions of A.
  - $\{ \{a\}, \{b\} \}$
  - $\{ \{a, b\} \}$
- Find the partitions of $\{a, b, c\}$

Ordered n-tuples

• Definition

Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. The **ordered n-tuple, $(x_1, x_2, \ldots, x_n)$,** consists of $x_1, x_2, \ldots, x_n$ together with the ordering: first x_1, then x_2, and so forth up to x_n. An ordered 2-tuple is called an **ordered pair,** and an ordered 3-tuple is called an **ordered triple.**

Two ordered n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are **equal** if, and only if, $x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$.

Symbolically:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \quad \Leftrightarrow \quad x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n.$$

In particular,

$$(a, b) = (c, d) \quad \Leftrightarrow \quad a = c \text{ and } b = d.$$

Is $(1, 2, 3, 4) = (1, 2, 4, 3)$?

Is $\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right)$?

Side Notes

Be warned that the notation for the ordered pair (a, b) is identical to the notation for the interval (a, b).

- However, the context of usage will make it clear what the notation refers

+

Cartesian Products

- **Definition**

Given sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$ denoted $\boldsymbol{A_1 \times A_2 \times \ldots \times A_n}$, is the $\boxed{\text{set of all ordered } n\text{-tuples } (a_1, a_2, \ldots, a_n)}$ where $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$.

Symbolically:

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

In particular,

$$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1 \text{ and } a_2 \in A_2\}$$

is the Cartesian product of A_1 and A_2.

Exercises

Let $A_1 = \{x, y\}$, $A_2 = \{1, 2, 3\}$, and $A_3 = \{a, b\}$.

- Find $A_1 \times A_2$
- Find $(A_1 \times A_2) \times A_3$
- Find $A_1 \times A_2 \times A_3$
- Is $(A_1 \times A_2) \times A_3$ same as $A_1 \times A_2 \times A_3$?

Method of Proving Subset Relations

Recall that $A \subseteq B \Leftrightarrow \forall x \in U$, if $x \in A$ then $x \in B$

- It's a universal conditional statement.

Therefore, to prove that $A \subseteq B$

- Suppose that *x* is a p.b.a.c. element of *A*.
- Show that *x* is an element of *B*.

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

Demonstrative Example

Exercise

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

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

- Prove that $A \subseteq B$
- Disprove that $B \subseteq A$

Exercise

Let $A = \{ m \in \mathbf{Z} \mid m = 6r + 12, \text{ for some } r \in \mathbf{Z} \}$
$B = \{ n \in \mathbf{Z} \mid n = 3s, \text{ for some } s \in \mathbf{Z} \}$

Prove that $A \subseteq B$

Proof:

Suppose x is a p.b.a.c. element of A.
By definition of A, there is an integer r such that $\boldsymbol{x = 6r + 12}$.
Let $s = 2r + 4$.
Then s is an integer because products and sums of integers are integers
Also note that $\mathbf{3}\boldsymbol{s} = 3(2r + 4) = \mathbf{6}\boldsymbol{r} \mathbf{+ 12} = x$,
Thus, by definition of *B*, *x* is an element of *B*.
[Note that we are showing that a p.b.a.c element that satisfies the definition of A also satisfies the definition of B]

- $x = 6r + 12 = 3(2r + 4) = 3s$, where $s = 2r + 4$

Exercise

Let $A = \{ m \in \mathbf{Z} \mid m = 6r + 12, \text{ for some } r \in \mathbf{Z} \}$
$B = \{ n \in \mathbf{Z} \mid n = 3s, \text{ for some } s \in \mathbf{Z} \}$

How can we disprove that $B \subseteq A$?

- To disprove a universal statement, you find a counterexample
- Show that there is an element of B that is not an element of A.

Let $x = 3$.

Then $x \in B$ because $3 = 3 \cdot 1$ and 1 is an integer.

But then $x \notin A$ because there is no integer r such that $3 = 6r + 12$.

We prove $x \notin A$ by method of **Proof by Contradiction**.

Suppose that $6r + 12 = 3$ for some integer r.
Then $2r + 4 = 1$ by dividing both sides by 3
By subtracting 4 from both sides, we have $2r = -3$.
Thus $\boldsymbol{r = -3/2}$ by dividing both sides by 2.
But -3/2 is **not an integer contradicting the supposition**.

Exercise

Let

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

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

Prove that $A = B$.

- Note that to prove $A = B$, you must prove both $A \subseteq B$ and $B \subseteq A$

Proof of $\boldsymbol{A \subseteq B}$

Suppose x is a p.b.a.c. element of A.

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

Let $b = a + 1$.

Then b is an integer because it is a sum of integers.

Observe that $2b - 2 = 2(a + 1) - 2 = 2a + 2 - 2 = 2a = x$

Thus, by definition of B, x is an element of B.

Proof of $\boldsymbol{B \subseteq A}$

Suppose x is a p.b.a.c. element of B. By definition of B, there is an integer b such that $x = 2b - 2$.

Let $a = b - 1$. Then a is an integer because it is a difference of integers.

Observe that $2a = 2(b - 1) = 2b - 2 = x$

Thus, by definition of A, x is an element of A.

Demonstrative Exercise

Prove that for all sets A and B, $A \cap B \subseteq A$.

- BTW, $A \cap B \subseteq A$ means $(A \cap B) \subseteq A$ because union, intersection and difference has high precedence over subset operation.

Proof:

Suppose A and B are p.b.a.c sets and suppose x is a p.b.a.c. element of $A \cap B$.

Then $x \in A$ and $x \in B$ by definition of intersection

In particular, $x \in A$.

Therefore, $A \cap B \subseteq A$. Q.E.D.

Note that in our proof above, we make use of the following:

- $X \subseteq Y \Leftrightarrow \forall x \in X, x \in Y$
- $A \cap B = \{ x \in U \mid x \in A \textbf{ and } x \in B \}$
- $p \wedge q$, therefore, p.

Some Subset Relations

Theorem 6.2.1 Some Subset Relations

1. *Inclusion of Intersection:* For all sets A and B,

$$\text{(a) } A \cap B \subseteq A \quad \text{and} \quad \text{(b) } A \cap B \subseteq B.$$

2. *Inclusion in Union:* For all sets A and B,

$$\text{(a) } A \subseteq A \cup B \quad \text{and} \quad \text{(b) } B \subseteq A \cup B.$$

3. *Transitive Property of Subsets:* For all sets A, B, and C,

$$\text{if } A \subseteq B \text{ and } B \subseteq C, \text{ then } A \subseteq C.$$

Set Identities

An identity is an equation that is universally true for all elements in some set.

- For example, the equation $a + b = b + a$ is an identity for real numbers because it is true for all real numbers a and b.

Following properties of set are some well known set identities

- Equations that are true for all sets in some universal set.

Set Identities

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,

$$\text{(a) } A \cup B = B \cup A \quad \text{and} \quad \text{(b) } A \cap B = B \cap A.$$

2. *Associative Laws:* For all sets A, B, and C,

$$\text{(a) } (A \cup B) \cup C = A \cup (B \cup C) \quad \text{and}$$
$$\text{(b) } (A \cap B) \cap C = A \cap (B \cap C).$$

3. *Distributive Laws:* For all sets, A, B, and C,

$$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
$$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

4. *Identity Laws:* For all sets A,

$$\text{(a) } A \cup \emptyset = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$

5. *Complement Laws:*

$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$

6. *Double Complement Law:* For all sets A,

$$(A^c)^c = A.$$

7. *Idempotent Laws:* For all sets A,

$$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$

8. *Universal Bound Laws:* For all sets A,

$$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \emptyset = \emptyset.$$

9. *De Morgan's Laws:* For all sets A and B,

$$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$

10. *Absorption Laws:* For all sets A and B,

$$\text{(a) } A \cup (A \cap B) = A \quad \text{and} \quad \text{(b) } A \cap (A \cup B) = A.$$

11. *Complements of U and $\emptyset$:*

$$\text{(a) } U^c = \emptyset \quad \text{and} \quad \text{(b) } \emptyset^c = U.$$

12. *Set Difference Law:* For all sets A and B,

$$A - B = A \cap B^c.$$

Proving the Properties of Set Identities

Reminded that to prove set equality, we need to prove that the two sets are subsets of each other

Prove that for all sets A, B, and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Structure of the Proof:

Suppose A, B, and C are p.b.a.c. sets

Proof of $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Suppose $x \in A \cup (B \cap C)$
[Show the steps to go from the above supposition to the conclusion below]
Thus $x \in (A \cup B) \cap (A \cup C)$

Proof of $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Suppose $x \in A \cup (B \cap C)$
[Show the steps to go from the above supposition to the conclusion below]
Thus $x \in (A \cup B) \cap (A \cup C)$

Thus $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof of Distributive Law for Sets

Proof:

Suppose A, B, and C are p.b.a.c. sets

Proof of $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Suppose $x \in A \cup (B \cap C)$. By definition of union, $x \in A$ **or** $x \in B \cap C$

Case 1 ($x \in A$):

Since $x \in A$, by definition of union $x \in A \cup B$ **and** $x \in A \cup C$.
Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

Case 2 ($x \in B \cap C$):

Since $x \in B \cap C$, by the definition of intersection $x \in B$ **and** $x \in C$.
Since $x \in B$, $x \in (A \cup B)$ by definition of union
Since $x \in C$, $x \in (A \cup C)$ by definition of union
Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

In both cases, $x \in (A \cup B) \cap (A \cup C)$, thus $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ by definition of subset.

Proof of Distributive Law for Sets (cont'd)

Proof of $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Suppose $x \in (A \cup B) \cap (A \cup C)$.
By definition of intersection, $x \in (A \cup B)$ **and** $x \in (A \cup C)$.
Consider the two cases: $x \in A$ and $x \notin A$

Case 1 ($x \in A$):

Since $x \in A$, we can conclude that $A \cup (B \cap C)$ by definition of union.

Case 2 ($x \notin A$):

From the supposition, we know $x \in (A \cup B)$ **and** $x \in (A \cup C)$
Since $x \in (A \cup B)$ and $x \notin A$, $x \in B$.
Since $x \in (A \cup C)$ and $x \notin A$, $x \in C$.
So $x \in B$ **and** $x \in C$ meaning $x \in B \cap C$ by definition of intersection.

Since $x \in B \cap C$, it follows that $x \in A \cup (B \cap C)$ by definition of union.

In both cases, $A \cup (B \cap C)$, thus $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ by definition of subset. Since both subset relations have been proved, it follows that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ by the definition of set equality.

Exercise

Prove that for all sets A and $B_1, B_2, B_3, \ldots, B_n$,

$$A \cup \left(\bigcap_{i=1}^{n} B_i \right) = \bigcap_{i=1}^{n} (A \cup B_i)$$

Note that above is simply the Distributive Law generalized for an indexed collection of sets.

Therefore, the general structure and strategy of the proof is same as the one demonstrated in the previous slide.

Do it on your exercise book.

A sample proof can also be found in your text book.

- Page 363

De Morgan's Law for Sets

Theorem 6.2.2(9)(a) A De Morgan's Law for Sets

For all sets A and B, $(A \cup B)^c = A^c \cap B^c$.

Exercise: Proof of De Morgan's Law for Sets

Proof:

Suppose A and B are p.b.a.c sets.

Proof of $(A \cup B)^c \subseteq A^c \cap B^c$:

Suppose $x \in (A \cup B)^c$. By definition of complement, $x \notin A \cup B$

$$\equiv \sim(x \in A \cup B) \equiv \sim(x \in A \text{ or } x \in B) \equiv x \notin A \text{ and } x \notin B$$

Hence $x \in A^c \cap B^c$ by definition of intersection. Therefore, $(A \cup B)^c \subseteq A^c \cap B^c$ by definition of subset.

Proof of $A^c \cap B^c \subseteq (A \cup B)^c$:

Suppose $x \in A^c \cap B^c$. By definition of intersection, $x \in A^c$ and $x \in B^c$, and by definition of complement, $x \notin A$ and $x \notin B$

Note that $x \notin A$ and $x \notin B \equiv \sim(x \in A \text{ or } x \in B) \equiv \sim(x \in A \cup B) \equiv x \notin A \cup B$
Hence $x \in (A \cup B)^c$ by definition of complement.
Therefore, $A^c \cap B^c \subseteq (A \cup B)^c$ by definition of subset.

Since both subset relations have been proved, it follows that $(A \cup B)^c = A^c \cap B^c$ by the definition of set equality.

For your Exercise Book

- Slide #27, #28 list some well known set identities
- I have demonstrated proofs of Distributive Law and De Morgan's Law for Sets in previous slides.
- Make sure that you can do the proofs for other remaining set identities.
    - That is prove by the Universal Generalization Method

Exercise

Consider the following statement:

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

- Observe that it's a Universal Conditional statement
- How can we prove such a statement?
  - Suppose A and B are **p.b.a.c sets such that $A \subseteq B$**
  - And **show that $A \cap B = A$**.

Proof:

Suppose A and B are p.b.a.c sets such that $A \subseteq B$.

Proof $A \cap B \subseteq A$:

This is true by the inclusion property of intersection.

- See slide #26, and #26 (or you can prove again if you like)

Proof of $A \subseteq A \cap B$:

Suppose $x \in A$.

It is also case that $x \in B$ since $A \subseteq B$.

Hence $x \in A$ and $x \in B$.

Therefore, $x \in A \cap B$ by definition of intersection

Proposition 6.2.6

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

Prove the above proposition

Proof:

Suppose A, B, and C are p.b.a.c sets such that $A \subseteq B$ and $B \subseteq C^c$.

[To show $A \cap C = \emptyset$, we simply need to show that $A \cap C$ contains no element by uniqueness of the empty set; see slide #11]

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

Then, by definition of intersection, $\boldsymbol{x \in A}$ and $\boldsymbol{x \in C}$

Since $A \subseteq B$, $\boldsymbol{x \in B}$ by definition of subset.

It's also case that $\boldsymbol{x \in C^c}$ since $B \subseteq C^c$ by definition of subset.

It follows that $\boldsymbol{x \notin C}$ by definition of complement.

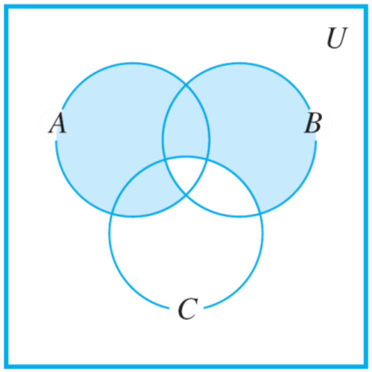
Thus $x \in C$ and $x \notin C$, which is **a contradiction**.

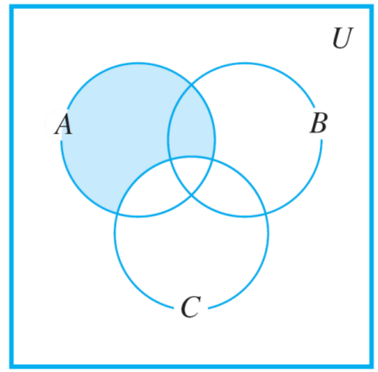
Therefore, the supposition that there is an element x in $A \cap C$ is false and thus $A \cap C = \emptyset$. Q.E.D.

Exercise

Either Prove or Disprove the following:

For all sets, A, B, and C, $\mathbf{(A - B) \cup (B - C) = A - C}$





How to formally disprove?

Demonstrate a counterexample:

Let $A = \{7\}$, $B = \emptyset$ and $C = \{7\}$. Then

$A - B = \{7\}$, $B - C = \emptyset$, and $A - C = \emptyset$.

Hence $(A - B) \cup (B - C) = \{7\}$, whereas $A - C = \emptyset$.

Since $\{7\} \neq \emptyset$, $(A - B) \cup (B - C) \neq A - C$

Deriving Set Identities Algebraically.

- A standard way to prove the identities is to make use of Universal Generalization.
- Another way to prove certain set identities is to show the equality by **deriving the equivalence algebraically *making use of other existing laws of set identities***.

For example, to show $A - (A \cap B) = A - B$.

$$
\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{by the set difference law} \\
&= A \cap (A^c \cup B^c) && \text{by De Morgan's laws} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{by the distributive law} \\
&= \emptyset \cup (A \cap B^c) && \text{by the complement law} \\
&= A \cap B^c && \text{by the identity law for } \cup \\
&= (A \cap B^c) \cup \emptyset && \text{by the commutative law for } \cup \\
&= A - B && \text{by the set difference law.}
\end{aligned}
$$

Exercise

Construct an algebraic proof that for all sets A, B, and C, $(A \cup B) - C = (A - C) \cup (B - C)$ citing the law applied in your transformation.

$(A \cup B) - C = (A \cup B) \cap C^c$ *by the set difference law*

$= C^c \cap (A \cup B)$ *by the commutative law*

$= (C^c \cap A) \cup (C^c \cap B)$ *by the distributive law*

$= (A \cap C^c) \cup (B \cap C^c)$ *by the commutative law*

$= (A - C) \cup (B - C)$ *by the set difference law*

What can you observe?

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. $A \cup (B \cup C) \equiv A \cup (B \cup C)$ b. $A \cap (B \cap C) \equiv A \cap (B \cap C)$
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. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$

What can you observe?

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. $A \cup (A \cap B) \equiv A$ b. $A \cap (A \cup B) \equiv A$
a. $\sim \mathbf{t} \equiv \mathbf{c}$ b. $\sim \mathbf{c} \equiv \mathbf{t}$	a. $U^c = \emptyset$ b. $\emptyset^c = U$

Boolean Algebra

- Logical Equivalences in Propositional Logic
- Laws of Set Identities

Both are just special cases of the **same general structure**, known as a **Boolean Algebra**.

You can consider a Boolean Algebra as a way of expressing Propositional Logic you learned during week#2, but using the following symbolic notation:

- 1 for the value of true
- 0 for the value of false
- + for disjunction operator (or)
- · for conjunction operator (and)
- ¯ for negation operator (complement)

For example,

Commutative laws expressed in Boolean Algebra notation

- $a + b = b + a$ and $a \cdot b = b \cdot a$

Identity laws expressed in Boolean Algebra notation

- $a + 0 = a$ and $a \cdot 1 = a$

Negation laws expressed in Boolean Algebra notation

- $a + \bar{a} = 1$ and $a \cdot \bar{a} = 0$

Five Basic Axioms of Boolean Algebra

- **Definition: Boolean Algebra**

A **Boolean algebra** is a set B together with two operations, generally denoted $+$ 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,

$$\text{(a) } a + b = b + a \quad \text{and} \quad \text{(b) } a \cdot b = b \cdot a.$$

2. *Associative Laws:* For all a, b, and c in B,

$$\text{(a) } (a + b) + c = a + (b + c) \quad \text{and} \quad \text{(b) } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

3. *Distributive Laws:* For all a, b, and c in B,

$$\text{(a) } a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad \text{(b) } a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

4. *Identity Laws:* There exist distinct elements 0 and 1 in B such that for all a in B,

$$\text{(a) } a + 0 = a \quad \text{and} \quad \text{(b) } a \cdot 1 = a.$$

5. *Complement Laws:* For each a in B, there exists an element in B, denoted $\overline{a}$ and called the **complement** or **negation** of a, such that

$$\text{(a) } a + \overline{a} = 1 \quad \text{and} \quad \text{(b) } a \cdot \overline{a} = 0.$$

Exercise

Prove the following property of a Boolean Algebra by deriving the equivalence using the five basic axioms.

For all elements a in a Boolean algebra B, $\boldsymbol{a + a = a}$

- **Idempotent law**

Proof:

Suppose B is a Boolean algebra and a is a p.b.a.c. element of B

Then observe that

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

Exercise

Prove the following property of a Boolean Algebra by deriving the equivalence using the five basic axioms.

For all a and x in B, if $a + x = 1$ and $a \cdot x = 0$, then $x = \bar{a}$

- Uniqueness of the Complement Law

Proof:

Suppose a and x are p.b.a.c. elements of a Boolean algebra B that satisfy the hypothesis that $a + x = 1$ and $a \cdot x = 0$. Then observe that

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

Exercise

Proof:

Suppose a and x are p.b.a.c. elements of a Boolean algebra B that satisfy the hypothesis that $a + x = 1$ and $a \cdot x = 0$. Then observe that

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

Double Complement Law

Theorem 6.4.1(3) Double Complement Law

For all elements a in a Boolean algebra B, $\overline{(\overline{a})} = a$.

Exercise

Prove the following property of a Boolean Algebra by deriving the equivalence using the five basic axioms.

Proof:

Suppose *B* is a Boolean algebra and *a* is a p.b.a.c. element of *B.*
Then observe that

$$\begin{aligned} \overline{a} + a &= a + \overline{a} && \text{by the commutative law} \\ &= 1 && \text{by the complement law for 1} \end{aligned}$$

And also observe that

$$\begin{aligned} \overline{a} \cdot a &= a \cdot \overline{a} && \text{by the commutative law} \\ &= 0 && \text{by the complement law for 0.} \end{aligned}$$

Note that *a* satisfies the two equations with respect to $\bar{a}$ that are satisfied by the complement of $\bar{a}$.

Therefore, *a* must be the unique complement of $\bar{a}$, i.e. *a* = $\overline{(\overline{a})}$

Properties of Boolean Algebra

Theorem 6.4.1 Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Law:* For all a and x in B, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$.
2. *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 $y = 1$.
3. *Double Complement Law:* For all $a \in B$, $\overline{(\overline{a})} = a$.
4. *Idempotent Law:* For all $a \in B$,

$$\text{(a) } a + a = a \quad \text{and} \quad \text{(b) } a \cdot a = a.$$

5. *Universal Bound Law:* For all $a \in B$,

$$\text{(a) } a + 1 = 1 \quad \text{and} \quad \text{(b) } a \cdot 0 = 0.$$

6. *De Morgan's Laws:* For all a and $b \in B$,

$$\text{(a) } \overline{a + b} = \overline{a} \cdot \overline{b} \quad \text{and} \quad \text{(b) } \overline{a \cdot b} = \overline{a} + \overline{b}.$$

7. *Absorption Laws:* For all a and $b \in B$,

$$\text{(a) } (a + b) \cdot a = a \quad \text{and} \quad \text{(b) } (a \cdot b) + a = a.$$

8. *Complements of* 0 *and* 1:

$$\text{(a) } \overline{0} = 1 \quad \text{and} \quad \text{(b) } \overline{1} = 0.$$

Duality Principle

- 0 and 1 are dual to each other
- Conjunction (·) and Disjunction (+) are duals of each other
- Complement is a self-dual.

Duality Principle asserts that Boolean algebra is unchanged when all duals are interchanged.

- Given a Boolean identity, there exists a dual identity formed by interchanging all the duals in the given Boolean identity.

Examples

- Consider the commutative laws
  - $a + b = b + a$
  - There exists the dual identity: $a \cdot b = b \cdot a$

Exercise

- What is the dual identity of the following Boolean identity law?
  - $(a + b) \cdot a = a$