CMSC 207- Lecture 17
CHAPTER 6: Set Theory (6.3 & 6.4)

Dr. Ahmed Tarek

Disproving a Stated Set Property

To show a universal statement is false, it suffices to find one example (called a counterexample) for which the statement is false.

Example 1 – *Finding a Counterexample for a Set Identity*

Is the following set property true?

For all sets *A*, *B*, and *C*, $(A - B) \cup (B - C) = A - C.$

Solution:

The property is true if, and only if, the given equality holds for *all* sets *A*, *B*, and *C*. So it is false if, and only if, there are sets *A*, *B*, and *C* for which the equality does *not* hold.

Example 1 – *Solution*

One way to solve this problem is to picture sets *A*, *B*, and *C* by drawing a Venn diagram such as that shown in Figure 6.3.1.

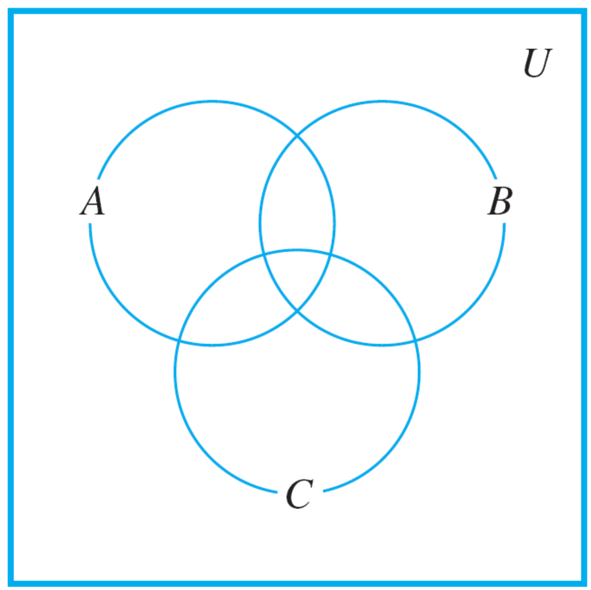

Figure 6.3.1

Example 1 – *Solution*

Find and shade the region corresponding to $(A - B) \cup (B - C)$. Then shade the region corresponding to $A - C$. These are shown in Figure 6.3.2.

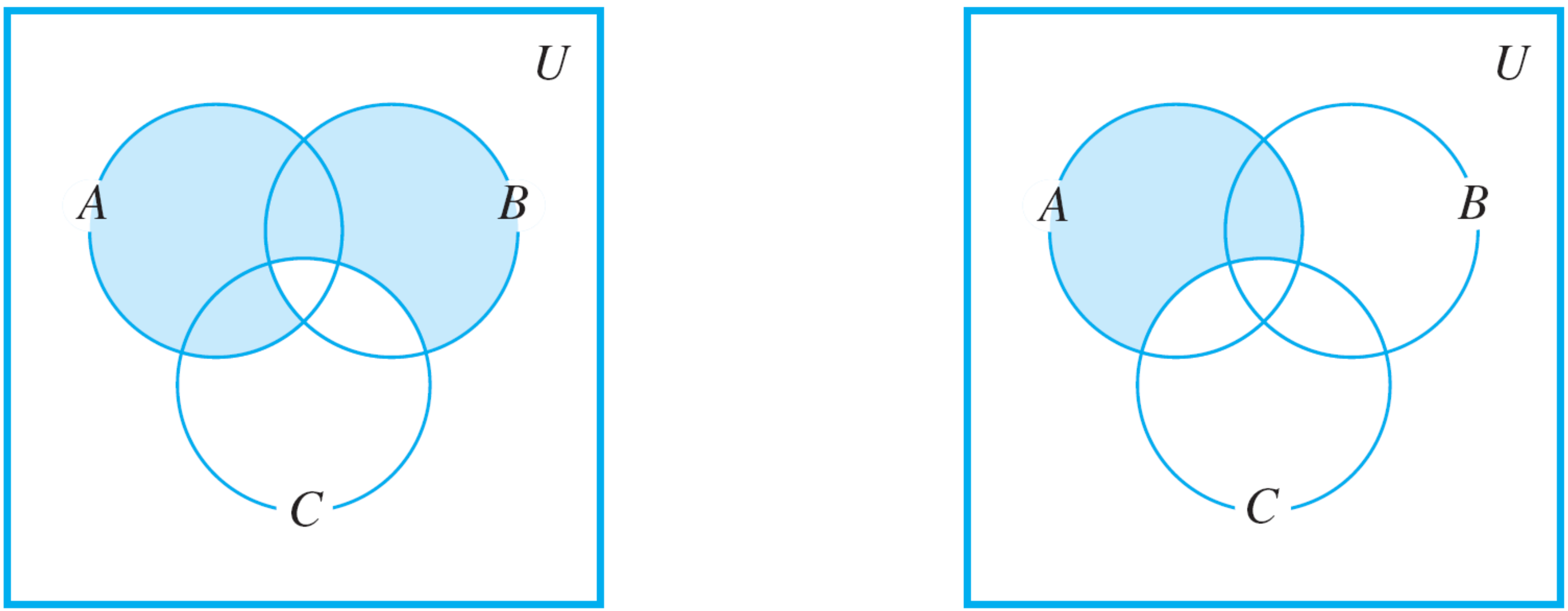

Figure 6.3.2

Example 1 – *Solution*

Comparing the shaded regions seems to indicate visually that the property is false. For instance, if there is an element in B that is not in either A or C, then this element would be in $(A - B) \cup (B - C)$ (because of being in B and not C) but it would not be in $A - C$ since $A - C$ contains nothing outside A. **Similarly**, an element that is in both A and C but not B would be in $(A - B) \cup (B - C)$ (because of being in A and not B), but it would not be in $A - C$ (because of being in both A and C).

Example 1 – *Solution*

Construct a concrete counterexample in order to confirm your answer and to ensure that you did not make a mistake either in drawing or analyzing diagrams. One way is to put one of the integers from 1–7 into each of the seven subregions enclosed by the circles representing A, B, and C. If the proposed set property had involved set complements, it would be helpful to label the region outside the circles, and so we place the number 8 there.

Example 1 – *Solution*

(See Figure 6.3.3.) Next define discrete sets *A*, *B*, and *C* to consist of all the numbers in their respective sub-regions.

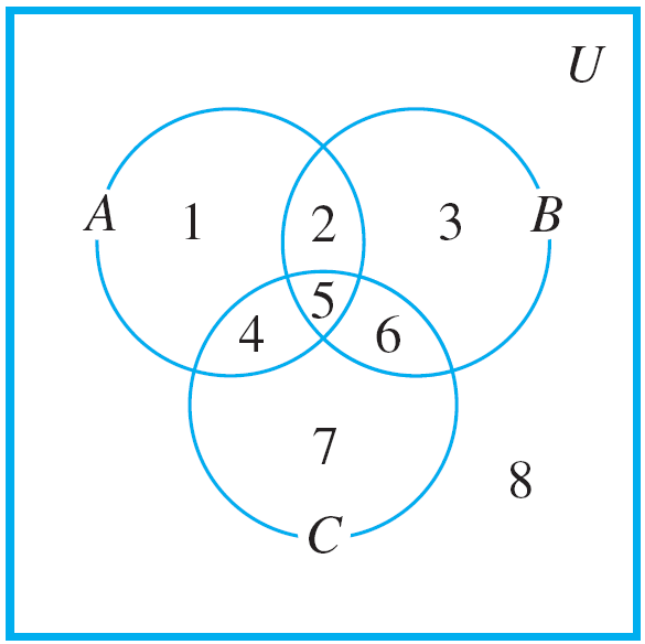

Figure 6.3.3

Example 1 – *Solution*

Counterexample 1: Per the numbering in Fig 6.3.3

Let $A = \{1,\ 2,\ 4,\ 5\}$, $B = \{2,\ 3,\ 5,\ 6\}$, and $C = \{4,\ 5, 6,\ 7\}$.

Then

$$A - B = \{1, 4\}, \quad B - C = \{2,\ 3\}, \quad \text{and} \quad A - C = \{1,\ 2\}.$$

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

whereas $A - C = \{1,\ 2\}$.

Since $\{1,\ 2,\ 3,\ 4\} \neq \{1,\ 2\}$, we have that $(A - B) \cup (B - C) \neq A - C$.

- **Class Practice Exercise**

The Number of Subsets of a Set

The following theorem states the important fact that if a set has n elements, then its power set has 2^n elements.

The proof uses mathematical induction and is based on the following observations. Suppose X is a set and z is an element of X.

1. The subsets of X can be split into two groups: those that do not contain z and those that do contain z.

2. The subsets of X that do not contain z are the same as the subsets of $X - \{z\}$.

The Number of Subsets of a Set

3. The subsets of X that do not contain z can be matched up one for one with the subsets of X that do contain z by matching each subset A that does not contain z to the subset $A \cup \{z\}$ that contains z.

   Thus there are as many subsets of X that contain z as there are subsets of X that do not contain z.

The Number of Subsets of a Set

For instance, if $X = \{x, y, z\}$, the following table shows the correspondence between subsets of X that do not contain z and subsets of X that contain z.

Subsets of X That Do Not Contain z		Subsets of X That Contain z
$\emptyset$	$\longleftrightarrow$	$\emptyset \cup \{z\} = \{z\}$
$\{x\}$	$\longleftrightarrow$	$\{x\} \cup \{z\} = \{x, z\}$
$\{y\}$	$\longleftrightarrow$	$\{y\} \cup \{z\} = \{y, z\}$
$\{x, y\}$	$\longleftrightarrow$	$\{x, y\} \cup \{z\} = \{x, y, z\}$

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.

The Number of Subsets of a Set

Proof (by mathematical induction):

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

Any set with *n* elements has 2^n subsets. $\leftarrow P(n)$

Show that *P*(0) is true:

To establish $P(0)$, we must show that Any set with 0 elements has 2^0 subsets. $\leftarrow P(0)$

But 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 elements has one subset. Since $1 = 2^0$, we have that $P(0)$ is true.

The Number of Subsets of a Set

Show that for all integers $k \geq 0$, if $P(k)$ is true then $P(k + 1)$ is also true: *[Suppose that P(k) is true for a particular but arbitrarily chosen integer* $\boldsymbol{k} \geq \mathbf{0}$. *That is:]* Suppose that $\boldsymbol{k}$ is any integer with $\boldsymbol{k} \geq \mathbf{0}$ such that **Any set with k elements has 2^k subsets**. $\leftarrow P(k)$
inductive hypothesis

[We must show that $P(k + 1)$ *is true. That is:]*

We must show that Any set with $k + 1$ elements has 2^{k+1} subsets. $\leftarrow P(k+1)$

The Number of Subsets of a Set

Let X be a set with $k + 1$ elements. Since $k + 1 \geq 1$, we may pick an arbitrary element z in X. Observe that any subset of X either contains z or not. Furthermore, any subset of X that does not contain z is a subset of $X - \{z\}$. And any subset A of $X - \{z\}$ can be matched up with a subset B, equal to $A \cup \{z\}$, of X that contains z. Consequently, there are as many subsets of X that contain z as do not, and thus there are twice as many subsets of X as there are subsets of $X - \{z\}$.

The Number of Subsets of a Set

But $X - \{z\}$ has k elements, and so

$$\text{the number of subsets of } X - \{z\} = 2^k \qquad \text{by inductive hypothesis.}$$

Therefore,

$$\begin{aligned}\text{the number of subsets of } X &= 2 \cdot (\text{the number of subsets of } X - \{z\}) \\ &= 2 \cdot (2^k) \qquad \text{by substitution} \\ &= 2^{k+1} \qquad \text{by basic algebra.}\end{aligned}$$

[This is what was to be shown.]

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

"Algebraic" Proofs of Set Identities

Let *U* be a universal set and consider the power set of *U*, $\mathscr{P}(U)$. The set identities given in Theorem 6.2.2 hold for all elements of $\mathscr{P}(U)$.

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,

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

"Algebraic" Proofs of Set Identities

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,

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

“Algebraic” Proofs of Set Identities

Once a certain number of identities and other properties have been established, new properties can be derived from them algebraically without having to use element method arguments.

It turns out that only identities (1–5) of Theorem 6.2.2 are needed to prove any other identity involving only unions, intersections, and complements.

Example 3 – *Deriving a Set Identity Using Properties of Ø*

Construct an algebraic proof that for all sets *A* and *B*, $A - (A \cap B) = A - B$.

Cite a property from Theorem 6.2.2 for every step of the proof.

Solution:

Suppose *A* and *B* are any sets. Then

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

Example 3 – *Solution*

$= (A \cap A^c) \cup (A \cap B^c)$	by the distributive law
$= \emptyset \cup (A \cap B^c)$	by the complement law
$= (A \cap B^c) \cup \emptyset$	by the commutative law for $\cup$
$= A \cap B^c$	by the identity law for $\cup$
$= A - B$	by the set difference law.

- **Class Practice Exercise**

Laws of Logical Equivalence and Set Properties

Table 6.4.1 summarizes the main features of the logical equivalences from Theorem 2.1.1 and the set properties from Theorem 6.2.2. The entries in the two columns are pretty similar.

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. $A \cap U = A$

Table 6.4.1

Laws of Logical Equivalence and Set Properties

Logical Equivalences	Set Properties
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. $\emptyset^c = U$

Table 6.4.1 (continued)

Laws of Logical Equivalence

Theorem 2.1.1 Logical Equivalences

Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1.	*Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2.	*Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3.	*Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4.	*Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5.	*Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6.	*Double negative law:*	$\sim(\sim p) \equiv p$	
7.	*Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8.	*Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9.	*De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10.	*Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11.	*Negations of* $\mathbf{t}$ *and* $\mathbf{c}$*:*	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

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:*

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

Set Identities

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,

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

Boolean Algebra

If you let ∨ (*or*) correspond to ∪ (union), ∧ (*and*) correspond to ∩ (intersection), **t** (a tautology) correspond to *U* (a universal set), **c** (a contradiction) correspond to Ø (the empty set), and ~ (negation) correspond to ^{c} (complementation), then you can see that the structure of the set of statement forms with operations ∨ and ∧ is essentially identical to the structure of the set of subsets of a universal set with operations ∪ and ∩.

In fact, both are special cases of the same general structure, known as a *Boolean algebra*.

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

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

Boolean Algebra

In any Boolean algebra, the complement of each element is unique, the quantities 0 and 1 are unique.

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 $a \in B$, $\overline{(\overline{a})} = a$.

Boolean Algebra

cont'd

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:

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

Boolean Algebra

All parts of the definition of a Boolean algebra and most parts of Theorem 6.4.1 contain paired statements. For instance, the distributive laws state that for all a, b, and c in B,

(a) $a + (b \cdot c) = (a + b) \cdot (a + c)$ and

(b) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

and the identity laws state that for all a in B,

(a) $a + 0 = a$ and (b) $a \cdot 1 = a$.

Boolean Algebras

Each of the paired statements can be obtained from the other by interchanging all the **+** and · signs and interchanging 1 and 0. *Such interchanges transform any Boolean identity into its* ***dual*** *identity.*

It can be proved that the dual of any Boolean identity is also an identity. This is called the **duality principle** for a Boolean algebra.

Example 1 – *Solution*

Theorem 6.4.1(3) Double Complement Law

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

Proof:

Suppose *B* is a Boolean algebra and *a* is any element of *B*. Then

$$\overline{a} + a = a + \overline{a} \qquad \text{by the commutative law}$$

$$= 1 \qquad \text{by the complement law for 1}$$

and

$$\overline{a} \cdot a = a \cdot \overline{a} \qquad \text{by the commutative law}$$

Example 1 – *Solution*

$$= 0 \qquad \text{by the complement law for } 0.$$

Thus a satisfies the two equations with respect to $\overline{a}$ that are satisfied by the complement of $\overline{a}$. From the fact that the complement of a is unique, it can be conclude that $\overline{(\overline{a})} = a$.

- **Class Practice Exercise**

Example 3 – *The Barber Puzzle*

In a certain 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?

Solution:

Neither yes nor no. If the barber shaves himself, he is a member of the class of men who shave themselves.

But no member of this class is shaved by the barber, and so the barber does *not* shave himself.

Example 3 – *Russell's Paradox*

On the other hand, if the barber does not shave himself, he belongs to the class of men who do not shave themselves.

But the barber shaves every man in this class, so the barber *does* shave himself.

This is called ***Russell's Paradox.***

Since the barber neither shaves himself nor doesn't shave himself, the sentence "The barber shaves himself" is neither true nor false.

But the sentence arose in a natural way from a description of a situation, which never existed.