# Chapter 6 - Set Theory

## Part 2: Algebraic Proofs and Boolean Algebra

Sections 6.3 - 6.4

COMP 233 Discrete Mathematics | Birzeit University

# Where we are: Chapter 6 at a glance

| | | |
|---|---|---|
| 6.1 | **Set Basics** | Sets, subsets, operations, partitions, power sets, products |
| 6.2 | **Properties of Sets** | Set identities and the element method of proof |
| **6.3** | **Algebraic Proofs** | Disproof by counterexample; deriving identities algebraically |
| **6.4** | **Boolean Algebra** | The shared structure behind logic and sets |

*This deck covers 6.3 and 6.4 (6.1 and 6.2 were Part 1).*

# 6.3 Disproofs and Algebraic Proofs - outline

1. Disproving a false set property by counterexample
2. The number of subsets: $|P(X)| = 2^n$
3. Algebraic proofs of set identities
4. Symmetric difference (enrichment)

# Disproving a proposed set property

**Principle**

A property “for all sets A, B, C, …” is a universal statement.

To DISPROVE it, exhibit ONE counterexample: specific sets that make the two sides unequal.

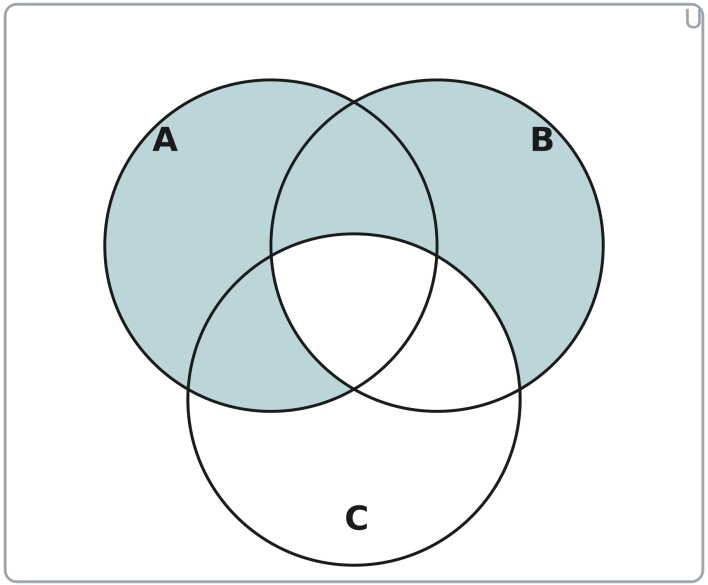
**The claim we will test (Epp 6.3.1)**

Is this true for all sets A, B, C ?

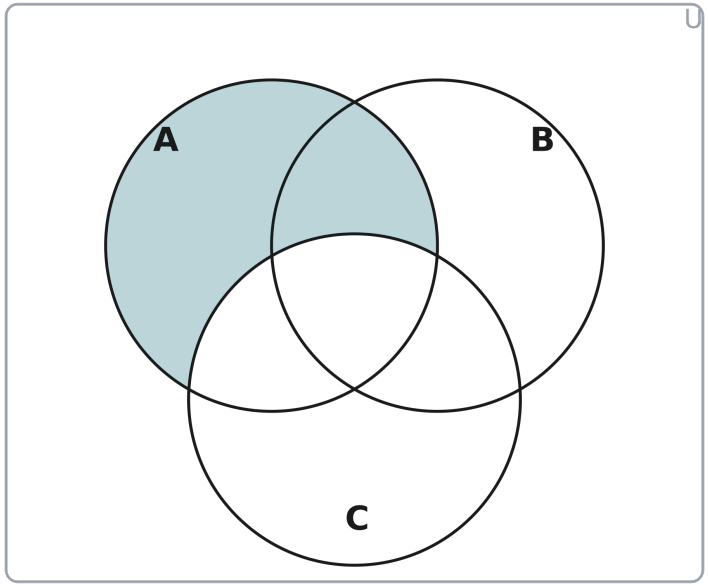
$$(A - B) \cup (B - C) = A - C$$

*Strategy: shade both sides on a Venn diagram; if the regions differ, hunt for a counterexample.*

# Step 1: the two sides shade different regions




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




$A - C$

**Different!**

The left shades part of B that lies outside A and C; the right never shades anything outside A.

# Step 2: a concrete counterexample settles it

**Counterexample**

Let $A = \varnothing$, $B = \{3\}$, $C = \varnothing$.

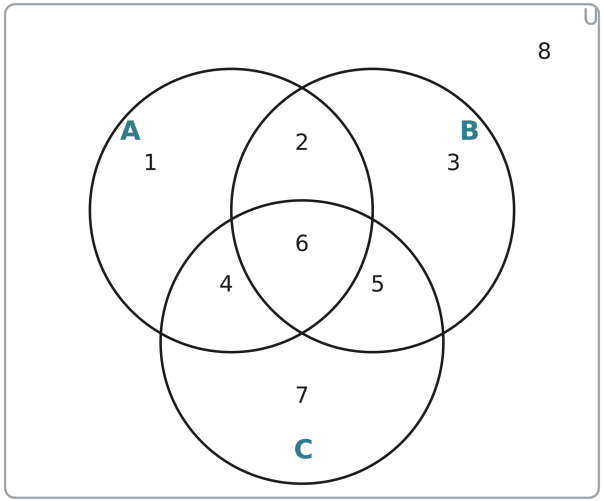
$A - B = \varnothing$ $\qquad$ $B - C = \{3\}$

$A - C = \varnothing$

Left: $(A - B) \cup (B - C) = \varnothing \cup \{3\} = \{3\}$

Right: $A - C = \varnothing$

$\{3\} \neq \varnothing$




*8 independent regions → Venn alone is informal*

# How many subsets does a set have?

**Theorem 6.3.1**

For every integer $n \geq 0$: if a set X has n elements, then P(X) has $2^n$ elements.

| n | example set | subsets | count = $2^n$ |
|---|---|---|---|
| 0 | ∅ | ∅ | 1 |
| 1 | {a} | ∅, {a} | 2 |
| 2 | {a, b} | ∅, {a}, {b}, {a,b} | 4 |
| 3 | {a, b, c} | … (all of them) | 8 |

*Each element is independently in or out of a subset: 2 choices, n times, gives $2^n$.*

# Proof of $|P(X)| = 2^n$ by induction (ch 5)

### Induction on n

Base n = 0:

∅ has exactly one subset (∅),

**and $2^0 = 1$. ✓**

**Inductive step:**

assume any k-element set has $2^k$ subsets.

Let X have k+1 elements; pick $z \in X$.

Subsets of X either omit z or contain z.

**#omit z** = #subsets of X−{z} = $2^k$.

$A \mapsto A \cup \{z\}$ pairs them, so #contain z = $2^k$.

Total = $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$. ✓

### Pairing for X = {x, y, z}

| omit z | contain z |
|---|---|
| ∅ | {z} |
| {x} | {x, z} |
| {y} | {y, z} |
| {x, y} | {x, y, z} |

*4 ↔ 4, so 8 = 2·4 total.*

# Algebraic proofs: chaining known identities

**The idea**

Instead of arguing element by element, transform one side into the other using the identities of Theorem 6.2.2, citing one law per step.

*It is like simplifying an algebraic expression in ordinary algebra - but the "numbers" are sets and the "operations" are ∪, ∩, and complement.*

**Most useful laws to keep ready**

Distributive  De Morgan  Double complement

Set difference: $A - B = A \cap B^c$ *(this turns every "–" into ∩ with a complement)*

# Worked algebraic proof 1

**Prove for all sets A, B, C: $(A \cup B) - C = (A - C) \cup (B - C)$ (Epp 6.3.2)**

$(A \cup B) - C$

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

$= C^c \cap (A \cup B)$ *commutative law for ∩*

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

$= (A \cap C^c) \cup (B \cap C^c)$ *commutative law for ∩*

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

# Worked algebraic proof 2

**Prove for all sets A, B: $A - (A \cap B) = A - B$ (Epp 6.3.3)**

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

# Symmetric difference (enrichment)

**Definition**

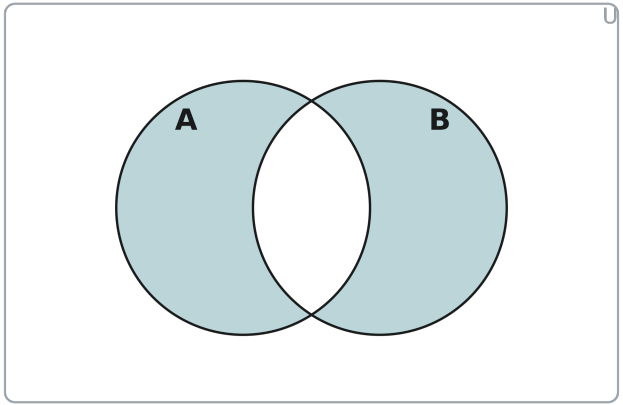
$$A \triangle B = (A - B) \cup (B - A)$$

*the elements in exactly one of A, B (not both).*

**A few properties (exercises 47-50)**

$A \triangle B = B \triangle A$ $\quad$ $A \triangle \varnothing = A$

$A \triangle A = \varnothing$ $\quad$ $A \triangle A^c = U$




*$A \triangle B$ shaded*

# 6.4 Boolean Algebra - outline

1. One structure behind logic and sets
2. The definition of a Boolean algebra (5 axioms)
3. The smallest example: B = {0, 1}
4. Properties and the duality principle

*(Optional appendix at the end: Russell's paradox and the halting problem.)*

# One structure behind logic and sets

*Compare the laws from Chapter 2 (logic) and Theorem 6.2.2 (sets). They are identical in shape.*

| Logic | Sets | Boolean |
|---|---|---|
| $p \vee q \equiv q \vee p$ | $A \cup B = B \cup A$ | $a + b = b + a$ |
| $p \wedge q \equiv q \wedge p$ | $A \cap B = B \cap A$ | $a \cdot b = b \cdot a$ |
| $p \vee c \equiv p$ | $A \cup \varnothing = A$ | $a + 0 = a$ |
| $p \wedge t \equiv p$ | $A \cap U = A$ | $a \cdot 1 = a$ |
| $p \vee \sim p \equiv t$ | $A \cup A^c = U$ | $a + \bar{a} = 1$ |
| $p \wedge \sim p \equiv c$ | $A \cap A^c = \varnothing$ | $a \cdot \bar{a} = 0$ |

Correspondence: $\vee \leftrightarrow \cup \leftrightarrow +$ $\wedge \leftrightarrow \cap \leftrightarrow \cdot$ $t \leftrightarrow U \leftrightarrow 1$ $c \leftrightarrow \varnothing \leftrightarrow 0$ $\sim \leftrightarrow {}^c \leftrightarrow \bar{a}$

# Definition of a Boolean algebra (1 of 2)

**Setup**

A Boolean algebra is a set B with two operations $+$ and $\cdot$ such that for all a, b in B, both $a + b$ and $a \cdot b$ are in B, and these laws hold:

| | | |
|---|---|---|
| **1. Commutative** | $a + b = b + a$ | $a \cdot b = b \cdot a$ |
| **2. Associative** | $(a + b) + c = a + (b + c)$ | $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ |
| **3. Distributive** | $a + (b \cdot c) = (a + b) \cdot (a + c)$ | $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ |

# Definition of a Boolean algebra (2 of 2)

**4. Identity laws**

There exist two distinct elements $0$ and $1$ in B such that for all a:

$a + 0 = a$ $\qquad$ $a \cdot 1 = a$

**5. Complement laws**

For each a in B there is an element $\bar{a}$ (the complement of a) such that:

$a + \bar{a} = 1$ $\qquad$ $a \cdot \bar{a} = 0$

# The smallest Boolean algebra: B = {0, 1}

*With these tables, B = {0,1} satisfies all five axioms. This is the algebra of a single bit - the basis of digital logic.*

**+ (acts like OR)**

| + | 0 | 1 |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 1 |

**· (acts like AND)**

| · | 0 | 1 |
|---|---|---|
| **0** | 0 | 0 |
| **1** | 0 | 1 |

**Complement**

$\bar{0} = 1$

$\bar{1} = 0$

0 = false / off
1 = true / on

*Notice: 1 + 1 = 1, not 2. In a Boolean algebra "+" is OR, not ordinary addition.*

# Theorem 6.4.1: properties of any Boolean algebra

*Derivable from the five axioms alone - so they hold for sets, logic, and bits at once.*

| | | | |
|---|---|---|---|
| **Uniqueness** | the complement, 0, and 1 are unique | **De Morgan** | $\overline{a+b}=\overline{a}\cdot\overline{b}$ |
| **Double comp.** | $(\bar{a}\bar{)}$ = a | **De Morgan** | $\overline{a\cdot b}=\overline{a}+\overline{b}$ |
| **Idempotent** | a + a = a  a · a = a | **Absorption** | (a + b) · a = a  (a · b) + a = a |
| **Universal bound** | a + 1 = 1  a · 0 = 0 | **Comp. of 0, 1** | $\bar{0}$ = 1  $\bar{1}$ = 0 |

# Worked proof: the double complement law

**Prove: $(\bar{a}\bar{)} = a$ for every a in a Boolean algebra (Epp 6.4.1)**

**Idea**

Complements are unique. So if a satisfies the complement equations for $\bar{a}$, then a must BE the complement of $\bar{a}$, i.e. $(\bar{a}\bar{)} = a$.

**Verify the two complement equations for $\bar{a}$:**

$\bar{a} + a = a + \bar{a} = 1$ *commutative, then complement law*

$\bar{a} \cdot a = a \cdot \bar{a} = 0$ *commutative, then complement law*

$\therefore$ by uniqueness of complements, $(\bar{a}\bar{)} = a$

# Worked proof: an idempotent law

**Prove: $a + a = a$ for every $a$ in a Boolean algebra (Epp 6.4.2)**

**Read each step's justification on the right**

| | |
|---|---|
| $a$ | |
| $= a + 0$ | *0 is the identity for +* |
| $= a + (a \cdot \bar{a})$ | *complement law for ·* |
| $= (a + a) \cdot (a + \bar{a})$ | *distributive law (+ over ·)* |
| $= (a + a) \cdot 1$ | *complement law for +* |
| $= a + a$ | *1 is the identity for ·* |

*Reading top to bottom: $a = a + a$, hence $a + a = a$.*

# The duality principle

**Principle**

Swap $+ \leftrightarrow \cdot$ and $0 \leftrightarrow 1$ throughout any Boolean identity. The result (its DUAL) is also a valid identity - automatically, with no new proof.

| An identity | Its dual |
|---|---|
| $a + 0 = a$ | $a \cdot 1 = a$ |
| $a + \bar{a} = 1$ | $a \cdot \bar{a} = 0$ |
| $a + 1 = 1$ | $a \cdot 0 = 0$ |
| $a + (b \cdot c) = (a+b) \cdot (a+c)$ | $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ |

# A little history: from al-Khwarizmi to Boole

### The word “algebra”

It comes from  al-jabr,  in the title of al-Khwarizmi's 9th-century book on solving equations. “Algebra” originally meant manipulating symbols by fixed rules.

### Boole's leap (1847)

George Boole applied that same symbolic method to LOGIC, in The Mathematical Analysis of Logic. Truth and reasoning became calculation - the foundation of every digital computer.

# Recommended exercises (Epp, 4th ed.)

| | |
|---|---|
| 6.3 Find a counterexample | 1, 2, 3, 4 |
| 6.3 Prove or disprove | 5, 6, 7, 9, 10, 13 |
| 6.3 Algebraic proofs (cite each step) | 30, 31, 32, 34, 35, 38 |
| 6.3 Simplify an expression | 41, 42, 43 |
| 6.3 Symmetric difference (enrichment) | 46, 47, 48, 49, 50 |
| 6.4 Boolean algebra proofs from axioms | 1, 2, 3, 4, 5 |
| 6.4 Work in B = {0, 1} | 10, 11 |

# Summary

- To DISPROVE a universal set property, one counterexample is enough.
- A set with n elements has $2^n$ subsets (proved by induction).
- Algebraic proofs chain the identities of Theorem 6.2.2, citing one law per step.
- Logic, sets, and bits all obey the same laws - they are Boolean algebras.
- A Boolean algebra is a set with +, ·, complement, 0, 1, defined by five axioms.
- Duality: swapping + ↔ · and 0 ↔ 1 turns any identity into another valid one.

Optional appendix

# Beyond the syllabus: two famous paradoxes

*Russell's paradox and the halting problem - both use the same self-reference trick. Enrichment only; not examinable.*

# Appendix: Russell's paradox

**The set that breaks naive set theory**

Some sets are not members of themselves (the set of all integers is not an integer). Let:

$S = \{ A \mid A \text{ is a set and } A \notin A \}$.  Is $S \in S$ ?

**Both answers contradict**

If $S \in S$, then S meets its own defining rule, so $S \notin S$.

If $S \notin S$, then S meets the rule, so $S \in S$.

**Either way - contradiction. So "S" cannot be a set.**

# Appendix: the halting problem

**Turing's question (1936)**

Could one program CheckHalt(X, D) decide, for EVERY program X and input D, whether X halts or loops forever?

**Theorem 6.4.2: No such program can exist.**

**The self-reference trap**

Build Test(X): if CheckHalt(X, X) says “halts”, loop forever; else halt.

Now run Test(Test): if it halts, CheckHalt said “halts”, so it loops; if it loops, it halts.

**Contradiction - so CheckHalt cannot exist.**