COMP 233 Discrete Mathematics

Set Theory

6.3: Disproof, Algebraic Proofs, and Boolean Algebras

(Dis)proving

Prove that: For all sets A, B, and C, (A -B) U (B -C) = A -C ?

Example: All people except who are Palestinians with the set of Palestinians except who are female, are the same set as all people except who are female

Counterexample 1: 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

$$(A - B) \cup (B - C) = \{1, 4\} \cup \{2, 3\} = \{1, 2, 3, 4\}, \quad \text{whereas} \quad A - C = \{1, 2\}.$$

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

Counterexample 2: Let $A = \emptyset$, $B = \{3\}$, and $C = \emptyset$.

Problem-Solving Strategy

How can you discover whether a given universal statement about sets is true or false?

There are two basic approaches:

- **Optimistic approach**: simply plunge in and start trying to prove the statement,
- **Pessimistic approach**, searching for conditions that must be fulfilled to construct a counterexample.

- The trick is to be ready to switch to the other approach if the one you are trying does not look promising.
- For more difficult questions, you may alternate several times between the two approaches before arriving at the correct answer.

"Algebraic" Method for Proving a Set Property

New prosperities can be devised directly from existing prosperities.

Algebraic Proof of a Set Identity

To prove that an equation holds for all sets *A*, *B*, and *C*,

suppose that *A*, *B*, and *C* are any sets. Then, starting with **one** side of the identity,

show that you can **transform** it, by successive application of the **general properties in Theorem 6.2.2**, into the **other** side of the identity.

5

Guidelines for constructing an Algebraic proof

- See Theorem 6.2.2
- Cite a property from Theorem 6.2.2 for every step of the proof.
- Be precise (e.g., by Theorem 6.2.2, **3. b.**) or (by **distributive law of union**)
- Simplify terms as much as you can

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

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

$$\underbrace{A_1}_{A} \cap (\underbrace{A_2}_{B} \cup \underbrace{A_3}_{C}) = (\underbrace{A_1}_{A} \cap \underbrace{A_2}_{B}) \cup (\underbrace{A_1}_{A} \cap \underbrace{A_3}_{C}),$$

$$\underbrace{(W \cap X)}_{A} \cap (\underbrace{Y}_{B} \cup \underbrace{Z}_{C}) = (\underbrace{(W \cap X)}_{A} \cap \underbrace{Y}_{B}) \cup (\underbrace{(W \cap X)}_{A} \cap \underbrace{Z}_{C}),$$

Example1: Set properties

Prove: For all sets A, B, and C, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Proof: Let A, B, and C be any sets. Then

$(A \cap B) \cup C = C \cup (A \cap B)$ by ___?___

$= (C \cup A) \cap (C \cup B)$ by ___?___

$= (A \cup C) \cap (B \cup C)$ by ___?___.

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

Exqmple2: Algebraic Proof

Construct an algebraic proof that for all sets A and B,

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

Proof:
Let A and B any sets. Then

$A \cup (B - A) = A \cup (B \cap A^C)$ - Set diff Law (12)

$= (A \cup B) \cap (A \cup A^C)$ - Assoc. Law (2.a)

$= (A \cup B) \cap U$ - Complement Law (5.a)

$=(A \cup B)$ - Identity Law (4.b)

Exqmple3: Algebraic Proof

Construct an algebraic proof that for all sets A, B, and C,
(A ∪ B) – C = (A – C) ∪ (B – C).

Let A, B, and C be any sets. Then

$$
\begin{aligned}
(A \cup B) - C &= (A \cup B) \cap C^c && \text{by the set difference law} \\
&= C^c \cap (A \cup B) && \text{by the commutative law for } \cap \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{by the distributive law} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{by the commutative law for } \cap \\
&= (A - C) \cup (B - C) && \text{by the set difference law.}
\end{aligned}
$$

■

Exqmple4: Algebraic Proof

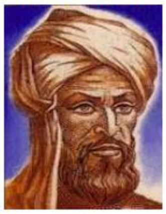
Construct an algebraic proof to show that for all sets *A* and *B*,
***A* – (*A* ∩ *B*) = *A* – *B*.**

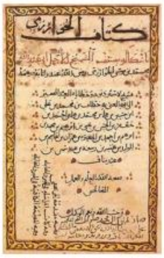
$$
\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{by the set difference law} \\
&= A \cap (A^c \cup B^c) && \text{by De Morgan's laws} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{by the distributive law} \\
&= \emptyset \cup (A \cap B^c) && \text{by the complement law} \\
&= (A \cap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

6.4: Boolean Algebras

What is Algebra?

Al-Khwarizmi 850 – 780 (Baghdad)





الكتاب المختصر في حساب الجبر والمقابلة

The Compendious Book on Calculation by Completion and Balancing

Developed an advanced arithmetical system with which they were able to do calculations in an algorithmic fashion.

Statements to describe relationships between things

Symbols and the rules for manipulating these symbols

Do you know any algebra (جبر)?

Boolean Algebra

Introduced by George Boole in his first book The Mathematical Analysis of Logic (1847),

George Boole
1815-1864,
England

A structure abstracting the computation with the truth values false and true.

Instead of elementary algebra where the values of the variables are numbers, and the main operations are addition and multiplication, the main operations of Boolean algebra are the conjunction ($\wedge$) the disjunction ($\vee$) and the negation not ($\neg$).

Used extensively in the simplification of logic Circuits

Compare logical equivalences and set properties

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

Compare logical equivalences and set properties

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. $\emptyset^c = U$

Both are special cases of the same general structure, known as a Boolean algebra

The structure of the statement forms is essentially identical to the structure of the set of subsets of a universal set

Correspondence between Logic & Sets

∨ (or) correspond to ∪ (union)

∧ (and) correspond to ∩ (intersection)

t (a tautology) correspond to U (a universal set)

c (a contradiction) correspond to ∅ (the empty set)

~ (negation) correspond to c (complementation)

Logic	Sets
statement	set
F	empty set Ø
T	universal set U
disjunction V	union ∪
conjunction Λ	intersection ∩
Negation ~	Set complement

De

We'll show how to derive the various properties associated with a Boolean algebra from a set of just five axioms

A **Boolean al**... ...oted $+$ and $\cdot$, such tha... ...lowing 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

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

Properties of a 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:

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

Example

Using the axioms we can prove that

x = x . x

x = x .1	By axiom 4
= x (x + ~x)	By axiom 5 (1 = a + ~a)
= x . x + x . ~x	By axiom 3 (distributive law)
= x . x + 0	By axiom 5 (0 = a . ~a)
= x . x	By axiom 4 (a + 0 = a)

Example

Using the axioms we can prove that

x = x + x

x = x + 0	By axiom 4
= x + (x . ~x)	By axiom 5 (0 = a . ~a)
= (x + x) . (x + ~x)	By axiom 3 (distributive law)
= (x + x) . 1	By axiom 5 (1 = a + ~a)
= x + x	By axiom 4 (a . 1 = a)

Proof: Uniqueness of the Complement Law

For all a and x in B,

if a+x=1 and a·x=0 then x=~a

x=x·1	because 1 is an identity for ·
=x·(a+~a)	by the complement law for +
=x·a +x·~a	by the distributive law for · over +
=a·x+x·~a	by the commutative law for ·
=0+x· ~a	by hypothesis
=a·~a+x·~a	by the complement law for ·
=(~a·a)+(~a·x)	by the commutative law for ·
=~a·(a+x)	by the distributive law for · over +
=~a·1	by hypothesis
=~a	because 1 is an identity for ·

Theorem 6.4.1 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

$$\overline{a} + a = a + \overline{a} \quad \text{by the commutative law}$$
$$= 1 \quad \text{by the complement law for 1}$$

and

$$\overline{a} \cdot a = a \cdot \overline{a} \quad \text{by the commutative law}$$
$$= 0 \quad \text{by the complement law for 0.}$$

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, we conclude that $\overline{(\overline{a})} = a$.