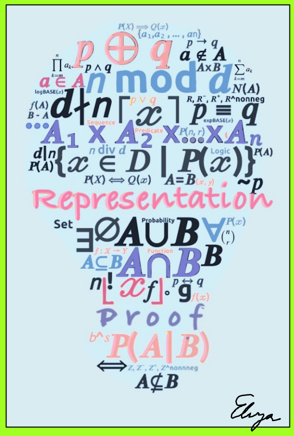
# Discrete Structures




## Lecture 14: Proofs with set theory

Susan L. Epstein

HUNTER

1

## Last time

- **Set theory proofs rely on definitions**
- How ∅ and $\boldsymbol{U}$ interact with arbitrary sets and with one another
- Intervals on the real number line are sets
- Element arguments facilitate set theory proofs

***We can prove some powerful results this way…***

**Proofs are key in all mathematics**



2

## Today's outline

- Properties of sets in proofs
- Set element proofs
- Algebraic set proofs
- Boolean algebras





## Review: basic ideas

- Set = collection of items called elements
  - Sets are typically named with uppercase letters $A \quad B \quad D$
  - Elements of a set are typically lowercase letters $a \quad b \quad x$
  - $\in$ denotes membership in a set $a \in A$
  - $\notin$ denotes non-membership in a set $a \notin A$
- Two ways to define a set
  - Enumerate its elements in curly brackets { } $\{2,3,5,7,11,\ldots\}$
  - Describe it by a precise rule $C = \{x \mid x \text{ is positive, even and} < 10\}$
- Universal set $\boldsymbol{U}$ = set of all elements
- Empty set $\emptyset$ = set containing no elements

**Reminder: Do not invent notation or language.**

# Review: sets, subsets and supersets

- Subset $A \subseteq B$ means $\forall x \in A, x \in B$ $\{1,2,3\} \subseteq \{x | 0 \leq x < 4\}$
- Proper subset $A \subset B$ means $\forall x \in A, x \in B$ and $\exists x \in B \ni x \notin A$ $\boldsymbol{N} \subset \boldsymbol{Z}$
- Superset $A \supseteq B$ means $\forall x \in B, x \in A$ $\{x | 0 \leq x < 4\} \supseteq \{1,2,\}$
- Proper superset $A \supset B$ means $\forall x \in b, x \in A$ and $\exists x \in A \ni x \notin B$ $\boldsymbol{Q} \supset \boldsymbol{Z}$
- Equality $A = B$ means $A \subseteq B$ and $B \subseteq A$ $\{1,2,3\} = \{x | 0 \leq x < 4\}$

**Reminder: Do not invent notation or language**



5

# Review: cardinality and tuples

- Cardinality $|A|$ = how many elements set contains $|\{1,9,2,3\}| = ?$
- Cartesian product $X \times Y = \{(x, y) | x \in X$ and $y \in Y\}$
  If $A = (4,5\}$ and $B = \{p, q\}$, then $A \times B = \{(4, p), (4, q), (5, p), (5, q)\}$
- $|X \times Y| = |X| \times |Y|$
- Ordered $n$-tuple = ordered set of $n$ elements formed from $n$ sets $A_1, A_2, \ldots, A_n$ in that order 3-tuple: $(4, 6, -2)$
- Cartesian product $A_1 \times A_2 \times \cdots \times A_n = \{(a, b, \ldots c) | a \in A_1,\ b \in A_2, \ldots, c \in A_n$
  If $A = (4,5\}$, $B = \{p, q\}$, and $C = \{cat, dog, 9\}$, then $(5, p, cat), \in A \times B \times C$
- $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \times |A_2| \times \cdots \times |A_n|$

**Reminder: Do not invent notation or language**



6

# Review: $\emptyset$ and $\boldsymbol{U}$

- Empty set $\emptyset$ = set containing no elements
  - $\emptyset = \{\,\}$
  - $\emptyset \subseteq A$
  - $A \cup \emptyset = A$
  - $A \cap \emptyset = \emptyset$
  - $\emptyset - A = \emptyset$
  - $A - \emptyset = A$
- Universal set $\boldsymbol{U}$ = set of all elements
  - $A \subseteq \boldsymbol{U}$
  - $A \cup \boldsymbol{U} = \boldsymbol{U}$
  - $A \cap \boldsymbol{U} = A$
  - $\boldsymbol{U} - A = A^C$
  - $A - \boldsymbol{U} = \emptyset$



7

# Useful set relationships

Inclusion of intersection

$\forall A, B \subseteq \boldsymbol{U}, A \cap B \subseteq A$ and $\forall A, B \in \boldsymbol{U}, A \cap B \subseteq B$

So $x \in A \cap B$ iff $x \in A$ and $x \in$ B

Inclusion in union

$\forall A, B \subseteq \boldsymbol{U}, A \subseteq A \cup B$ and $\forall A, B \in \boldsymbol{U}, B \subseteq A \cup B$

So $x \in A \cup B$ iff $x \in A$ or $x \in$ B

Transitivity of subsets

$\forall A, B, C \subseteq \boldsymbol{U}$ if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$



8

## Today's outline

- ✓ Properties of sets in proofs
- Set element proofs
- Algebraic set proofs
- Boolean algebras

Fall 2023 CSCI 150 9/29

9

## Procedural definitions support proofs

- Union $A \cup B = \{x | x \in A \text{ or } x \in B\}$

$$x \in X \cup Y \iff x \in X \textbf{ or } x \in Y$$

- Intersection $A \cap B = \{x | x \in A \text{ and } | x \in B\}$

$$x \in X \cap Y \iff x \in X \textbf{ and } x \in Y$$

- Difference $A - B = \{x | x \in A \text{ and } x \notin B\}$

$$x \in X - Y \iff x \in X \textbf{ and } x \notin Y$$

- Complement $A^C = \{\boldsymbol{x} | \boldsymbol{x} \notin A\}$

$$x \in X^C \iff x \notin X$$

- Cartesian product

$$(x, y) \in X \times Y \iff x \in X \textbf{ and } y \in Y$$

Fall 2023 CSCI 150 10/29

10

## A simple set element proof

Theorem: For any sets $A$ and $B$, $B \subseteq A \cup B$

Proof:

Let $x$ be any element of $B$.

We must show that $x \in A \cup B$.

By definition of union, $x \in A \cup B$ is true iff $x \in A$ or $x \in B$.

Since $x \in B, x \in A \cup B$.

**QED**

Fall 2023 CSCI 150 11/29

11

## Set equality proof ≡ 2 subset proofs

To prove that $A = B$ there are 2 parts: $A \subseteq B$ and $B \subseteq A$.

Theorem: $(A \cup B)^C = A^C \cap B^C$
Proof: Let $A$ and $B$ be arbitrary sets.
We must show that $(A \cup B)^C = A^C \cap B^C$.
Part 1: We must show that $(A \cup B)^C \subseteq A^C \cap B^C$.
Let $x$ be any element of $(A \cup B)^C$. By definition of complement, $x \notin (A \cup B)$.
By definition of union $x \notin A$ and $x \notin B$.
By definition of complement, $x \in A^C$ and $x \in B^C$ so by definition of intersection $x \in A^C \cap B^C$. Thus $(A \cup B)^C \subseteq A^C \cap B^C$.
Part 2: We must show that $A^C \cap B^C \subseteq (A \cup B)^C$.
Let $x$ be any element of $A^C \cap B^C$. By definition of intersection, $x \in A^C$ and $x \in B^C$.
By definition of complement, $x \notin A$ and $x \notin B$.
By definition of union, $x \notin (A \cup B)$ so by definition of complement $(A \cup B)^C$.
Thus $A^C \cap B^C \subseteq (A \cup B)^C$.
Since $(A \cup B)^C \subseteq A^C \cap B^C$ and $A^C \cap B^C \subseteq (A \cup B)^C$, by definition of set equality, $(A \cup B)^C = A^C \cap B^C$. **QED**

Fall 2023 CSCI 150 12/29

12

## Another set equality proof (1)

Theorem: For all sets $A, B, C, A \cap (B - C) = (A \cap B) - (A \cap C)$.
Let $A$ and $B$ be arbitrary sets.
We must show that $A \cap (B - C) = (A \cap B) - \ (A \cap C)$

Part 1: We must show that $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$.
Let $x$ be any element in $A \cap (B - C)$.
By definition of intersection, $x \in A$ and $x \in (B - C)$.
By definition of set difference $x \in B$ and $x \notin C$.
By definition of complement, $x \in C^C$.
Since $x \in A$ and $x \in B$, by definition of intersection $x \in (A \cap B)$.
Since $x \notin C$, by definition of intersection $x \notin (A \cap C)$.
Thus by definition of set difference $x \in (A \cap B) - (A \cap C)$ and

$$A \cap (B - C) \subseteq (A \cap B) - (A \cap C).$$

Fall 2023 CSCI 150 13/29

13

## Another set equality proof (2)

Part 2: We must show that $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$.
Let $x \in$ be any element in $(A \cap B) - (A \cap C)$.
By definition of set difference, $x \in (A \cap B)$ and $x \notin (A \cap C)$..
By definition of intersection, $x \in A$ and $x \in B$.
Since $x \notin (A \cap C)$ and $x \in A$ it must be that $x \notin C$.
By definition of complement, $x \in C^C$.
Since $x \in B$ and $x \in C^C$, by definition of intersection, $x \in B \cap C^C$ and by definition of set difference $x \in B - C$.
Since $x \in A$ and $x \in B - C$, by definition of intersection $x \in A \cap (B - C)$.
Thus $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$.

Since $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$ and $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$, by definition of set equality, $(A \cup B)^C \ = A^C \cap B^C$.
**QED**

Fall 2023 CSCI 150 14/29

14

## How to prove with ∅

Typically by contradiction, where you show that something is in ∅.

Theorem: For any empty set $E$ and any set $A$, $E \subseteq A$.

Proof:

Assume $E \nsubseteq A$. We will show that this assumption logically leads to a contradiction.

By definition of subset, there is some element $x \in E$ such that $x \notin A$. But by definition, $E$ has no elements.

Contradiction.

Because the assumption led to a contradiction, it must be true that $E \subseteq A$.

**QED**





## Another proof about ∅

Theorem: The empty set is unique.

Proof:

Assume that there are 2 distinct empty sets $E$ and $F$.

We will show that this assumption logically leads to a contradiction.

By the proof on the previous slide, an empty set is a subset of any set.

Thus $E \subseteq F$ and $F \subseteq E$. By definition of set equality, $E = F$. This contradicts are assumption that the sets are distinct.

Contradiction.

Because the assumption led to a contradiction, it must be true that the empty set is unique.

**QED**

## How to disprove a statement

- Find a counterexample

All primes are odd

- By contradiction

The empty set is unique

Any questions?

Fall 2023 CSCI 150 17/29

17

## Today's outline

✓ Properties of sets in proofs
✓ Set element proofs
- Algebraic set proofs
- Boolean algebras

Fall 2023 CSCI 150 18/29

18

# Set identities (1)

**All sets here are assumed to be subsets of $U$**

- Union is commutative
  For all sets $A$ and $B$, $A \cup B = B \cup A$
- Intersection is commutative
  For all sets $A$ and $B$, $A \cap B = B \cap A$
- Union is associative
  For all sets $A, B$ and $C$, $(A \cup B) \cup C = A \cup (B \cup C)$
- Intersection is associative:
  For all sets $A, B$ and $C$, $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributive laws: For all sets $A, B$ and $C$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Identity laws: For all sets $A$, $A \cup \emptyset = A$ and $A \cap U = A$
- Complement laws: For all sets $A$, $A \cup A^C = U$ and $A \cap A^C = \emptyset$
- Double complement law: For all sets $A$, $(A^C)^C = A$

Fall 2023 CSCI 150 19/29

19

# Set identities (2)

**All sets here are assumed to be subsets of $U$**

- Idempotent Laws: For all sets $A$, (same set has no effect on itself)
  $A \cup A = A$ and $A \cap A = A$
- Universal Bound Laws: For all sets $A$, (constant overrides another value) $A \cup U = U$ and $A \cap \emptyset = \emptyset$
- De Morgan's Laws: For all sets $A$ and $B$ $(A \cup B)^C = A^C \cap B^C$
  $(A \cap B)^C = A^C \cup B^C$
- Absorption Laws: For all sets $A$ and $B$ (simpler expression generalizes over a more restrictive one) $A \cup (A \cap B) = A$
  $A \cap (A \cup B) = A$
- Complements of U and $\emptyset$: $\boldsymbol{U}^C = \emptyset$
  $\emptyset^C = \boldsymbol{U}$
- Set Difference Law: For all sets $A$ and $B$, $A - B = A \cap B^C$

Fall 2023 CSCI 150 20/29

20

## Sequence of statements with reasons

Theorem: For all sets $A, B, C, (A \cup B) - C = (A - C) \cup (B - C)$

| | |
|---|---|
| $(A \cup B) - C = (A \cup B) \cap C^C$ | Set difference law |
| $= C^C \cap (A \cup B)$ | Commutative law for ∩ |
| $= (C^C \cap A) \cup (C^C \cap B)$ | Distributive law for ∩ over ∪ |
| $= (A \cap C^C) \cup (B \cap C^C)$ | Commutative law for ∩ |
| $= (A - C) \cup (B - C)$ | Set difference law |

Your text calls this an algebraic proof.



21

## Another algebraic proof

- Theorem: For all sets $A, B, C, A \cap (B - C) = (A \cap B) - (A \cap C)$

| | |
|---|---|
| $(A \cap B) - (A \cap C) = (A \cap B) \cap (A \cap C)^C$ | Set difference law |
| $= (A \cap B) \cap (A^C \cup C^C)$ | De Morgan's law |
| $= ((A \cap B) \cap A^C) \cup ((A \cap B) \cap C^C))$ | Distributive law for ∩ over ∪ |
| $= (A^C \cap (A \cap B)) \cup ((A \cap B) \cap C^C)$ | Commutative law for ∩ |
| $= ((A^C \cap A) \cap B) \cup ((A \cap B) \cap C^C)$ | Associative law for ∩ |
| $= (\emptyset \cap B) \cup ((A \cap B) \cap C^C)$ | Complement law |
| $= \emptyset \cup ((A \cap B) \cap C^C)$ | Universal bound law |
| $= (A \cap B) \cap C^C)$ | Universal bound law |
| $= A \cap (B \cap C^C)$ | Associative law |
| $= A \cap (B - C)$ | Set difference law |



22

## Today's outline

- ✓ Properties of sets
- ✓ Set element proofs
- ✓ Algebraic set proofs
- Boolean algebras

Fall 2023 CSCI 150 23/29

23

## Boolean algebra

A set $B$ and 2 operations ($+$ and $\cdot$) under which it closed; it has 5 properties:

- Commutative laws: $\forall a, b \in B$,

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

- Associative laws : $\forall a, b, c \in B$,

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

- Distributive laws : $\forall a, b, c \in B$,

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

- Identity laws: $\exists\ 0,1 \in B$ such that $\forall a \in B$,

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

Don't panic
This is not arithmetic!

- Complement laws: For each $a \in B$, $\exists\ \bar{a} \in B$ called the complement or negation of $a$

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

Fall 2023 24/29

24

# Readily derivable properties

- Complements of 0 and 1: $\overline{0} = 1$ and $\overline{1} = 0$
- Uniqueness of the complement law: $\forall a, x \in B$, if $a + x = 1$ and $a \cdot x = 0$ then $x = \bar{a}$
- Uniqueness of the identities:
  If $\exists x \in B$ such that $\forall a \in B, a + x = a$ then $x = 0$
  If $\exists y \in B$ such that $\forall a \in B, a \cdot x = a$ then $y = 1$
- Double complement law: $\forall a \in B$, $\overline{(\bar{a})} = a$
- Idempotent law : $\forall a \in B$, $a + a = a$ and $a \cdot 0 = 0$
- Universal bound law: $\forall a \in B$, $a + 1 = 1$ and $a \cdot 0 = 0$
- De Morgan's laws : $\forall a, b \in B$, $\overline{a + b} = \bar{a} \cdot \bar{b}$ and $\overline{a \cdot b} = \bar{a} + \bar{b}$
- Absorption laws : $\forall a, b \in B$, $(a + b) \cdot a = a$ and $(a \cdot b) + a = a$

***Does all this seem familiar?***

Fall 2023 CSCI 150 25/29

25

# Table 6.4.1 (part 1)

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

Notice anything?!

Fall 2023 CSCI 150 26/29

26

# Table 6.4.1 (part 2)

| Logical Equivalences | Set Properties |
|---|---|
| a. $p \vee p \equiv p$<br>b. $p \wedge p \equiv p$ | a. $A \cup A = A$<br>b. $A \cap A = A$ |
| a. $p \vee \mathbf{t} \equiv \mathbf{t}$<br>b. $p \wedge \mathbf{c} \equiv \mathbf{c}$ | a. $A \cup U = U$<br>b. $A \cap \emptyset = \emptyset$ |
| a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$<br>b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$ | a. $(A \cup B)^c = A^c \cap B^c$<br>b. $(A \cap B)^c = A^c \cup B^c$ |
| a. $p \vee (p \wedge q) \equiv p$<br>b. $p \wedge (p \vee q) \equiv p$ | a. $A \cup (A \cap B) \equiv A$<br>b. $A \cap (A \cup B) \equiv A$ |
| a. $\sim\mathbf{t} \equiv \mathbf{c}$<br>b. $\sim\mathbf{c} \equiv \mathbf{t}$ | a. $U^c = \emptyset$<br>b. $\emptyset^c = U$ |

Notice anything?!



27

# Explanation

The versions of logic and set theory introduced here are both Boolean algebras. (There are many others.)

Here's are the correspondences

| Boolean algebra | Logic | Set theory |
|---|---|---|
| + | ∨ | ∪ |
| . | ∧ | ∩ |
| 0 | $\boldsymbol{t}$ | $\boldsymbol{U}$ |
| 1 | $\boldsymbol{c}$ | ∅ |

Any questions?



28

## Proof methods (so far)

Truth table

Sequence of statements with reasons

Logic (modus ponens, modus tollens,…)

Predicate logic (quantification, vacuous truth)

Generalization from the generic particular

Proof by contradiction

Proof by contraposition

Proof by cases

Mathematical induction

Strong mathematical induction

Proof by set element

Algebraic set proof



29

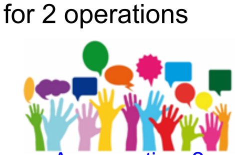
## What you should know

**Set theory proofs rely on definitions**

- Set theory properties are analogous to those of CSCI 150 formal logic
- Set theory proofs are either element proofs that rely on definitions, or algebraic proofs that rely on set theory laws
- A Boolean algebra has identities and complements for 2 operations that are associative, commutative, and distributive

propositional logic set theory

**Next up: *Relations***




**Time to finish up that Opening sheet!**

**Problem set 13,14 is due on Monday, October 30 at 11PM**



30