Mat2033 - Discrete Mathematics

Set Theory

Introduction to Set Theory

- A **set** is a new type of structure, representing an unordered collection (group, plurality) of zero or more distinct (different) objects.
- Set theory deals with operations between, relations among, and statements about sets.
- All of mathematics can be defined in terms of some form of set theory (using predicate logic).

Basic notations for sets

- For sets, we'll use variables S, T, U, …
- We can denote a set S in writing by listing all of its elements in curly braces:
  - {a, b, c} is the set of whatever 3 objects are denoted by a, b, c.
- Set builder notation: For any proposition P(x) over any universe of discourse, $\{x|P(x)\}$ is the set of all x such that P(x).

Basic properties of sets

- Sets are inherently unordered:
  - No matter what objects a, b, and c denote, {a, b, c} = {a, c, b} = {b, a, c} = {b, c, a} = {c, a, b} = {c, b, a}.
- All elements are distinct (unequal); multiple listings make no difference!
  - If a=b, then {a,b,c}={a,c}={b,c}={a,a,b,a,b,c,c,c,c}.
  - This set contains at most 2 elements!

Definition of Set Equality

- Two sets are declared to be equal if and only if they contain *exactly the same elements*.
- In particular, it does not matter how the set is defined or denoted.
- For example: The set

$\{1, 2, 3, 4\}$

$= \{x \mid x \text{ is an integer where } 0 < x < 5\}$

$= \{x \mid x \text{ is a positive integer where } 0 < x^2 < 25\}$

Infinite Sets

- Conceptually, sets may be infinite
- Symbols for some special infinite sets:

$\mathbf{N} = \{0, 1, 2, \ldots\}$ The Natural numbers.

$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ The Integers.

$\mathbf{R} =$ The Real numbers.

Basic Set Relations: Member of

- $x \in S$ ("x is in S") is the proposition that object x is an element or member of set S.
  - e.g. $3 \in \mathbf{N}$,
  - "a"$\in \{x \mid x \text{ is a letter of the alphabet}\}$
  - Can define set equality in terms of $\in$ relation:

    $$\forall S,T\text{: } S=T \leftrightarrow (\forall x\text{: } x \in S \leftrightarrow x \in T)$$

    "Two sets are equal iff they have all the same members."
- $x \notin S :\equiv \neg(x \in S)$ "x is not in S"

The Empty Set

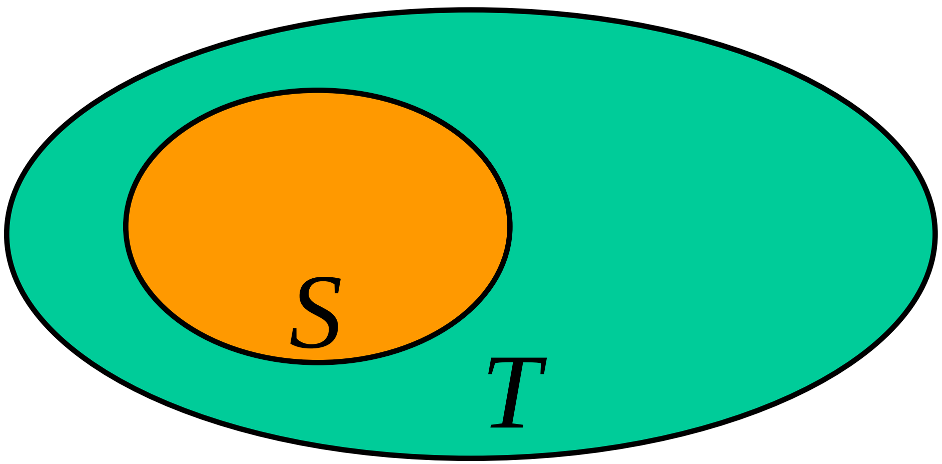
- $\varnothing$ ("null set", "empty set") is the unique set that contains no elements whatsoever.
- $\varnothing = \{\}$
- No matter what is the domain of discourse (or u.d.), we have the axiom $\neg\exists x\colon x\in\varnothing$.

Subset and Superset Relations

- $S \subseteq T$ ("S is a subset of T") means that every element of S is also an element of T.
- $S \subseteq T \Leftrightarrow \forall x\ (x \in S \rightarrow x \in T)$
- $\varnothing \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("S is a superset of T") means $T \subseteq S$.
- Note $S=T \Leftrightarrow S \subseteq T \wedge S \supseteq T$.
- $\boldsymbol{S} \nsubseteq \boldsymbol{T}$ means $\neg(S \subseteq T)$, i.e. $\exists x(x \in S \wedge x \notin T)$

Proper (Strict) Subsets & Supersets

- $S \subset T$ ("S is a proper subset of T") means that $S \subseteq T$ but $T \not\subseteq S$. Similar for $S \supset T$.



Venn Diagram equivalent of S⊂T

Example:
$\{1,2\} \subset \{1,2,3\}$

Sets Are Objects, Too!

- The objects that are elements of a set may themselves be sets.
- E.g. let $S=\{x \mid x \subseteq \{1,2,3\}\}$, then

  $S=\{\emptyset, \{1\}, \{2\}, \{3\},$
  $\{1,2\}, \{1,3\}, \{2,3\},$
  $\{1,2,3\}\}$
- Note that $1 \neq \{1\} \neq \{\{1\}\}$!!!!

Cardinality and Finiteness

- $|S|$ (read "the cardinality of S") is a measure of how many different elements S has.
- E.g., $|\emptyset|=0$, $|\{1,2,3\}| = 3$, $|\{a,b\}| = 2$,
  $|\{\{1,2,3\},\{4,5\}\}| =$ 2
- If $|S|\in\mathbf{N}$, then we say S is finite. Otherwise, we say S is infinite.
- What are some infinite sets we've seen?

  N, **Z**, **R** ,…

The Power Set Operation

- The power set $P(S)$ of a set S is the set of all subsets of S. $P(S) = \{x \mid x \subseteq S\}$.
- E.g. $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written $\mathbf{2}^S$. Note that for finite S, $|P(S)| = 2^{|S|}$.
- It turns out that $|P(\mathbf{N})| > |\mathbf{N}|$. There are different sizes of infinite sets!

Review: Set Notations So Far

- Variable objects x, y, z; sets S, T, U.
- Literal set $\{a, b, c\}$ and set-builder $\{x|P(x)\}$.
- $\in$ relational operator, and the empty set $\varnothing$.
- Set relations $=$, $\subseteq$, $\supseteq$, $\subset$, $\supset$, $\not\subset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets **N**, **Z**, **R**.
- Power sets $P(S)$.

Ordered n-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbf{N}$, an ordered n-tuple or a sequence of length n is written $(a_1, a_2, \ldots, a_n)$. The first element is a_1, the second element is a_2 , etc.
- Note $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quin<u>tuples</u>, …, n-tuples.

Cartesian Products of Sets

- For sets A, B, their Cartesian product

  $$A \times B :\equiv \{(a, b) \mid a \in A \wedge b \in B\}.$$

- E.g. $\{a,b\} \times \{1,2\} = \{(a,1),(a,2),(b,1),(b,2)\}$
- Note that for finite A, B,

  $$|A \times B| = |A| . |B|$$

- Note that the Cartesian product is not commutative: $\neg \forall A,B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n \ldots$

The Union Operator

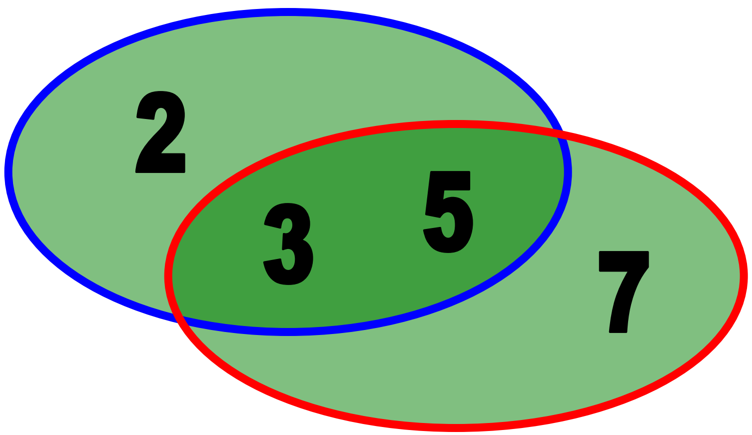
- For sets A, B, their union $A \cup B$ is the set containing all elements that are either in A, **or** ("$\vee$") in B (or, of course, in both).
- Formally, $\forall A,B$: $A \cup B = \{x \mid x \in A \vee x \in B\}$.
- Note that $A \cup B$ contains all the elements of A **and** it contains all the elements of B:

$$\forall A, B: \big((A \cup B) \supseteq A \big) \wedge \big((A \cup B) \supseteq B \big)$$

Union Examples

- $\{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\}$
- $\{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\}$

  $= \{2,3,5,7\}$



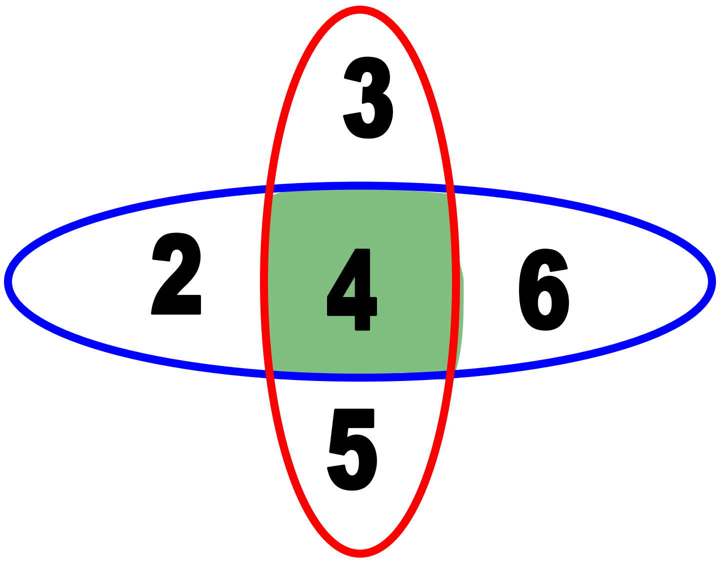
The Intersection Operator

- For sets A, B, their intersection $A \cap B$ is the set containing all elements that are simultaneously in A **and** (“$\wedge$”) in B.
- Formally, $\forall A,B: A\cap B \equiv \{x \mid x\in A \wedge x\in B\}$.
- Note that $A\cap B$ is a subset of A **and** it is a subset of B:

  $\forall A, B: ((A\cap B) \subseteq A) \wedge ((A\cap B) \subseteq B)$

Intersection Examples

- $\{a,b,c\} \cap \{2,3\} = \underline{\ \emptyset\ }$
- $\{2,4,6\} \cap \{3,4,5\} = \underline{\ \{4\}\ }$



Disjointedness

- Two sets A, B are called disjoint (i.e., unjoined) iff their intersection is empty. ($A \cap B = \varnothing$)
- Example: the set of even integers is disjoint with the set of odd integers.

Inclusion–Exclusion Principle

- How many elements are in $A \cup B$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Example:

How many positive integers between 50 and 100

a) are divisible by 7? Which integers are these?

b) are divisible by 11? Which integers are these?

c) are divisible by both 7 and 11? Which integers are these?

d) are divisible by 7 or 11? Which integers are these?

a) Seven: 56, 63, 70, 77, 84, 91, 98

b) Five: 55, 66, 77, 88, 99

c) One: 77

d) Eleven: 55, 56, 63, 66, 70, 77, 84, 88, 91, 98, 99

Set Difference

- For sets A, B, the difference of A and B, written $A-B$, is the set of all elements that are in A but not B.
- $A - B = \{x \mid x \in A \land x \notin B\}$
  $= \{x \mid \neg(x \in A \rightarrow x \in B) \}$
- Also called:
  The complement of B with respect to A.

Set Difference Examples

- $\{1,\cancel{2},\cancel{3},4,\cancel{5},6\} - \{2,3,5,7,9,11\} = \{1,4,6\}$

- $\mathbf{Z} - \mathbf{N} =$

  $= \{\cdots , -1, 0, 1, 2, \cdots \} - \{0, 1, \cdots \}$

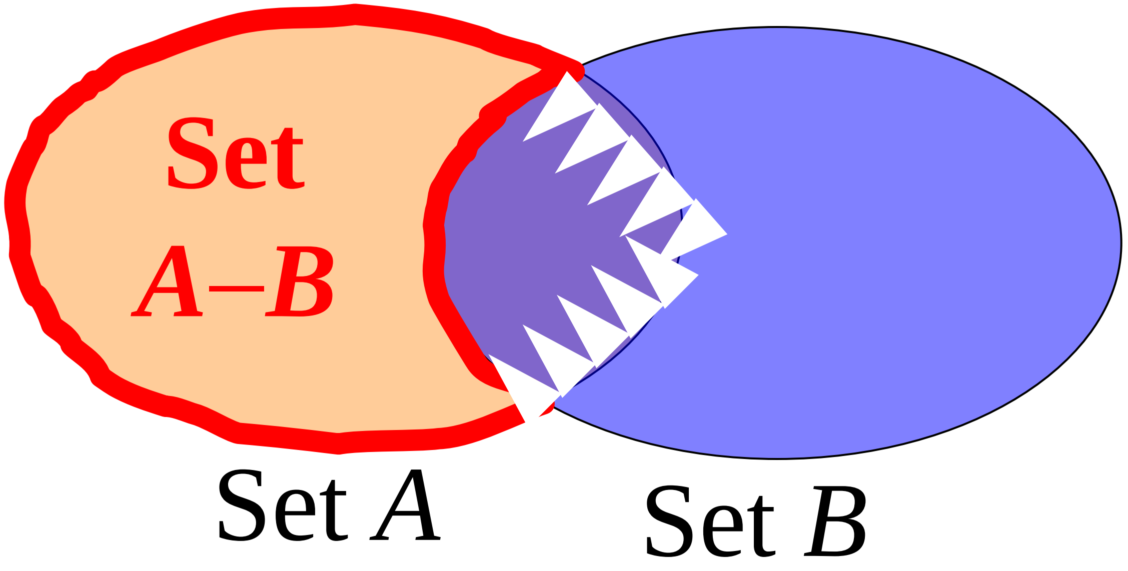
  $= \{x \mid x \text{ is an integer but not a Natural.}\}$

  $= \{x \mid x \text{ is a negative integer}\}$

  $= \{\ldots , -3, -2, -1\}$

Set Difference - Venn Diagram

- $A-B$ is what's left after B "takes a bite out of A"



Set Complements

- The universe of discourse can itself be considered a set, call it U.

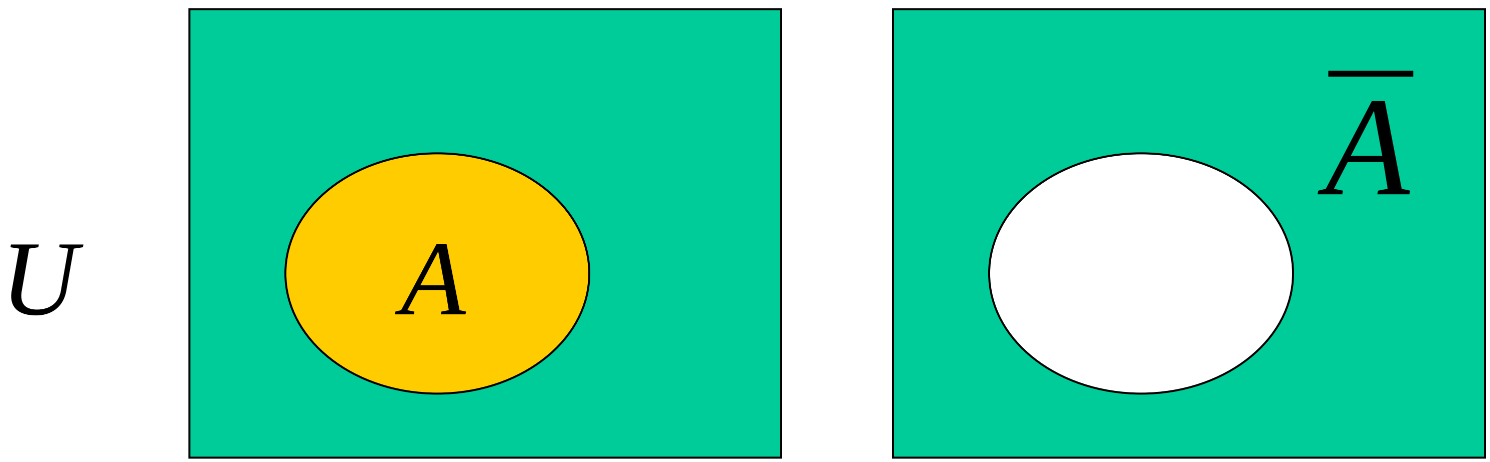
- When the context clearly defines U, we say that for any set $A \subseteq U$, the complement of A, written $\bar{A}$, is the complement of A w.r.t. U, i.e., it is U−A.

- E.g., If U=**N**, $\overline{\{3,5\}} = \{0,1,2,4,6,7,\ldots\}$

More on Set Complements

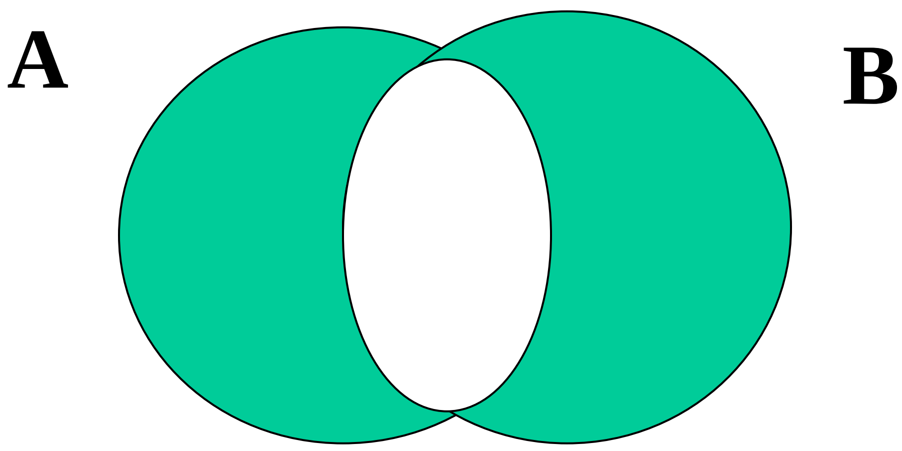
- An equivalent definition, when U is clear:

$$\overline{A} = \{x \mid x \notin A\}$$



Symmetric difference

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



Cardinality

- $|P \cup Q| = |P|+|Q|-|P \cap Q|$
- $|P \oplus Q| = |P|+|Q|-2|P \cap Q|$
- $|P-Q| = |P|-|P \cap Q|$
- $|\overline{A}|=|U|-|A|$, U is universe of discourse

Set Identities

- Identity:

$$A \cup \emptyset = A, \quad A \cap U = A$$

- Domination:

$$A \cup U = U, \quad A \cap \emptyset = \emptyset$$

- Idempotent:

$$A \cup A = A = A \cap A$$

Set Identities

- Double complement:

$$\overline{(\overline{A})} = A$$

- Commutative:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

- Associative:

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

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

DeMorgan's Law for Sets

- Exactly analogous to (and derivable from) DeMorgan's Law for propositions.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Proving Set Identities

To prove statements about sets, of the form E1 = E2 (where Es are set expressions), here are three useful techniques:

1. Prove E1 $\subseteq$ E2 and E2 $\subseteq$ E1 separately.
2. Use set builder notation & logical equivalences.
3. Use a membership table.

Method 1: Mutual subsets

Example: Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
  - Assume $x \in A \cap (B \cup C)$, & show $x \in (A \cap B) \cup (A \cap C)$.
  - We know that $x \in A$, and either $x \in B$ or $x \in C$.
    - Case 1: $x \in B$. Then $x \in A \cap B$, so $x \in (A \cap B) \cup (A \cap C)$.
    - Case 2: $x \in C$. Then $x \in A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
- **Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. … Homework.**

Method 3: Membership Tables

- Just like truth tables for propositional logic.
- Columns for different set expressions.
- Rows for all combinations of memberships in constituent sets.
- Use "1" to indicate membership in the derived set, "0" for non-membership.
- Prove equivalence with identical columns.

Membership Table Example

Example: Prove $(A \cup B) - B = A - B$.

A	B	$A \cup B$	$(A \cup B) - B$	$A - B$
0	0	0	0	0
0	1	1	0	0
1	0	1	1	1
1	1	1	0	0

Membership Table Exercise

Exercise: Prove $(A\cup B)-C = (A-C)\cup(B-C)$.

A	B	C	$A\cup B$	$(A\cup B)-C$	$A-C$	$B-C$	$(A-C)\cup(B-C)$
0	0	0					
0	0	1					
0	1	0					
0	1	1					
1	0	0					
1	0	1					
1	1	0					
1	1	1					

Generalized Unions & Intersections

- Since union & intersection are commutative and associative, we can extend them from operating on ordered pairs of sets (A,B) to operating on sequences of sets $(A_1,\cdots,A_n)$, or even unordered sets of sets, $X=\{A \mid P(A)\}$.

Generalized Union

- Binary union operator: $A \cup B$

- n-ary union:

$$A_1 \cup A_2 \cup \ldots \cup A_n :\equiv ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)$$

(grouping & order is irrelevant)

- "Big U" notation: $\bigcup_{i=1}^{n} A_i$

- Or for infinite sets of sets: $\bigcup_{A \in X} A$

Generalized Intersection

- Binary intersection operator: $A \cap B$

- n-ary intersection:

$$A_1 \cap A_2 \cap \ldots \cap A_n :\equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n)$$

(grouping & order is irrelevant)

- "Big Arch" notation: $\bigcap_{i=1}^{n} A_i$

- Or for infinite sets of sets: $\bigcap_{A \in X} A$

Representations

- A frequent theme of this course will be methods of representing one discrete structure using another discrete structure of a different type.
- E.g., one can represent natural numbers as
  - Sets:

    $0 :\equiv \varnothing$, $1 :\equiv \{0\}$, $2 :\equiv \{0,1\}$, $3 :\equiv \{0,1,2\}$, …
  - Bit strings:

    $0 :\equiv$ `0`, $1 :\equiv$ `1`, $2 :\equiv$ `10`, $3 :\equiv$ `11`, $4 :\equiv$ `100`, …

Representing Sets with Bit Strings

For an enumerable u.d. U with ordering $\{x_1, x_2, \ldots, x_n\}$, represent a finite set $S \subseteq U$ as the finite bit string $B = b_1 b_2 \ldots b_n$ where $\forall i$: $x_i \in S \leftrightarrow (i < n \wedge b_i = 1)$.

E.g. $U = \mathbf{N}$, $S = \{2,3,5,7,11\}$, $B = 001101010001$.

In this representation, the set operators "$\cup$", "$\cap$", "$\bar{\ }$" are implemented directly by bitwise OR, AND, NOT!

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws

TABLE 1 Set Identities.

Identity	*Name*
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

The **symmetric difference** of A and B, denoted by $A \oplus B$, is the set containing those elements in either A or B, but not in both A and B.

Find the symmetric difference of $\{1, 3, 5\}$ and $\{1, 2, 3\}$.

Show that $A \oplus B = (A \cup B) - (A \cap B)$.

Show that $A \oplus B = (A - B) \cup (B - A)$.

Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$.

b) $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$.

d) $A \oplus \overline{A} = U$.

Example: Show that $A \oplus B = (A \cup B) - (A \cap B)$.

Example: Show that $A \oplus B = (A \cup B) - (A \cap B)$.

element is in $(A \cup B) - (A \cap B)$ if it is in the union of A and B but not in the intersection of A and B, which means that it is in either A or B but not in both A and B. This is exactly what it means for an element to belong to $A \oplus B$.

Example: Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$.

b) $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$.

d) $A \oplus \overline{A} = U$.

Example: Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$. **d)** $A \oplus \overline{A} = U$.

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

Example: Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$. **d)** $A \oplus \overline{A} = U$.

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

Example: Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$. **d)** $A \oplus \overline{A} = U$.

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

c) $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \overline{A} = \overline{A}$

Example: Show that if A is a subset of a universal set U, then

a) $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.

c) $A \oplus U = \overline{A}$. **d)** $A \oplus \overline{A} = U$.

a) $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

b) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

c) $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \overline{A} = \overline{A}$

d) $A \oplus \overline{A} = (A - \overline{A}) \cup (\overline{A} - A) = A \cup \overline{A} = U$

Examples: U = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

A= {1, 2, 3, 4, 5}, B = {4, 5, 6, 7, 8}. Then

- $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\}$
- $A \cap B = \{4, 5\}$
- $\overline{A} = \{0, 6, 7, 8, 9, 10\}$
- $\overline{B} = \{0, 1, 2, 3, 9, 10\}$
- $A - B = \{1, 2, 3\}$
- $B - A = \{6, 7, 8\}$
- $A \oplus B = \{1, 2, 3, 6, 7, 8\}$