Set Theory

Introduction to Set Theory

- A *set* is a 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.

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).*

  e.g., $\{x \mid x \text{ is an integer where } x>0 \text{ and } x<5\}$

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!
  - $\{a, b, c\} = \{a, a, b, a, b, c, c, c, c\}$.
  - This set contains at most 3 elements!

Definition of Set Equality

- Two sets are declared to be equal *if and only if* they contain <u>exactly the same</u> elements.
- In particular, it does not matter *how the set is defined or denoted.*
- For example: The set $\{1, 2, 3, 4\}$ =

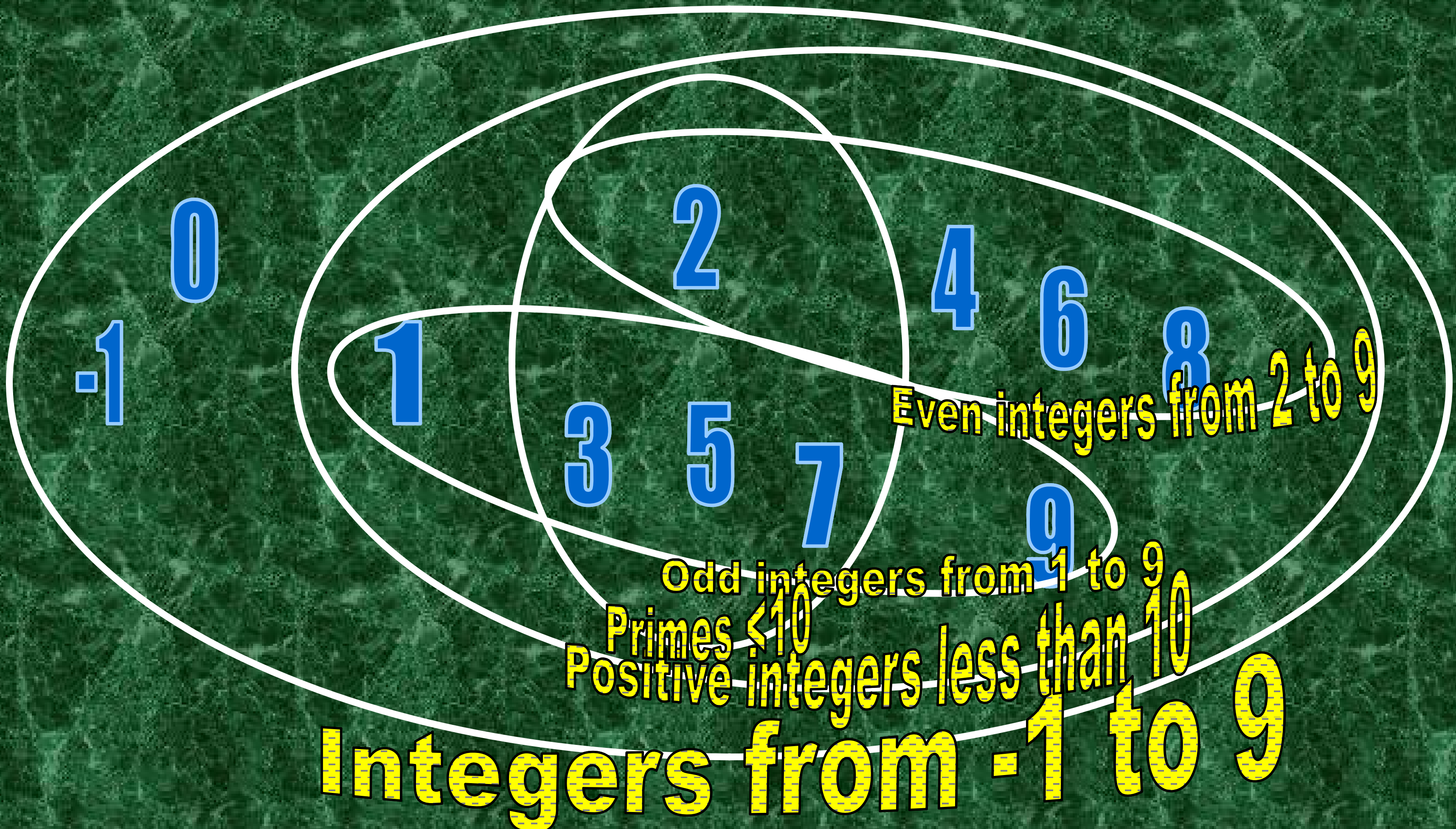
  $\{x \mid x$ is an integer where $x>0$ and $x<5\}$ =

  $\{x \mid x$ is a positive integer whose square is >0 and $<25\}$

Infinite Sets

- Conceptually, sets may be *infinite* (*i.e.*, not *finite*, without end, unending).
- Symbols for some special infinite sets:
  N = {0, 1, 2, …} The **n**atural numbers.
  Z = {…, -2, -1, 0, 1, 2, …} The *i*ntegers.
  R = The "**r**eal" numbers, such as 374.1828471929498181917281943125…
- Infinite sets come in different sizes!

Venn Diagrams



Basic Set Relations: Member of

- $x \in S$ ("x is in S") is the proposition that object x is an $\in$*lement* or *member* of set S.
  - *e.g.* $3 \in \mathbf{N}$, "a"$\in \{x \mid x$ is a letter of the alphabet$\}$
- Can define <u>set equality</u> in terms of $\in$ relation:
  $\forall S,T: S=T \leftrightarrow (\forall x: x\in S \leftrightarrow x\in T)$
  "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”, “the empty set”) is the unique set that contains no elements whatsoever.
- $\varnothing = \{\} = \{x|\mathbf{False}\}$
- No matter the domain of discourse, we have the axiom

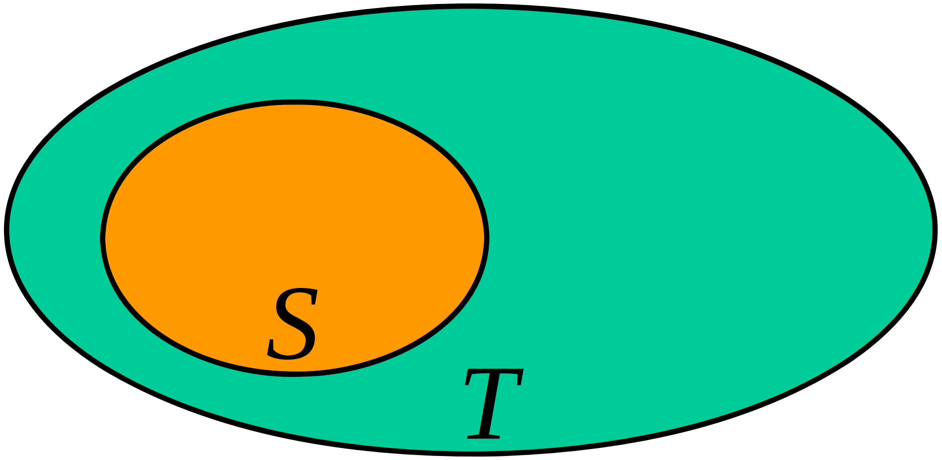
$$\neg\exists x\colon x\in\varnothing.$$

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.
- $S \subseteq T \Leftrightarrow \forall x\ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("S is a superset of T") means $T \subseteq S$.
- Note $S = T \Leftrightarrow S \subseteq T \wedge S \supseteq T$.
- $S \not\subseteq T$ 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 $T \nsubseteq S$. Similar for $S \supset T$.



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

Venn Diagram equivalent of $S \subset T$

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 $1 \neq \{1\} \neq \{\{1\}\}$!!!!

Very Important!

Cardinality and Finiteness

- $|S|$ (read "the *cardinality* of S") is a measure of how many different elements S has.
- *E.g.*, $|\varnothing|=0$, $|\{1,2,3\}| = 3$, $|\{a,b\}| = 2$,
  $|\{\{1,2,3\},\{4,5\}\}| =$ _2_
- We say S is *infinite* if it is not *finite*.
- 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}) = {∅, {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!

Ordered *n*-tuples

- 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, *etc.*
- These are like sets, except that duplicates matter, and the order makes a difference.
- Note $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, *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: $\neg\forall AB: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...

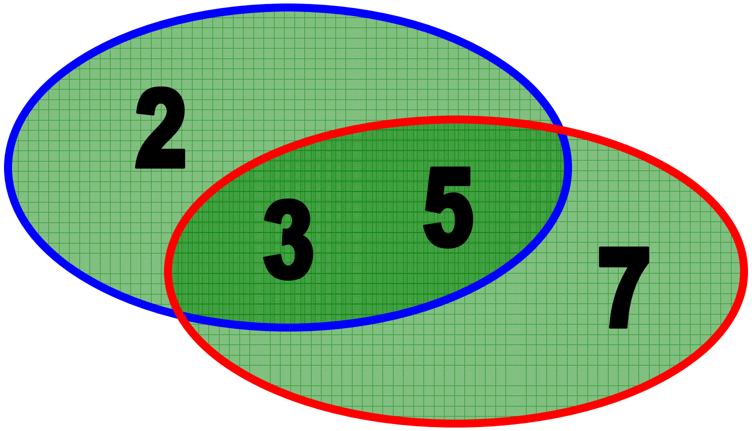
The Union Operator

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

Union Examples

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

Required Form

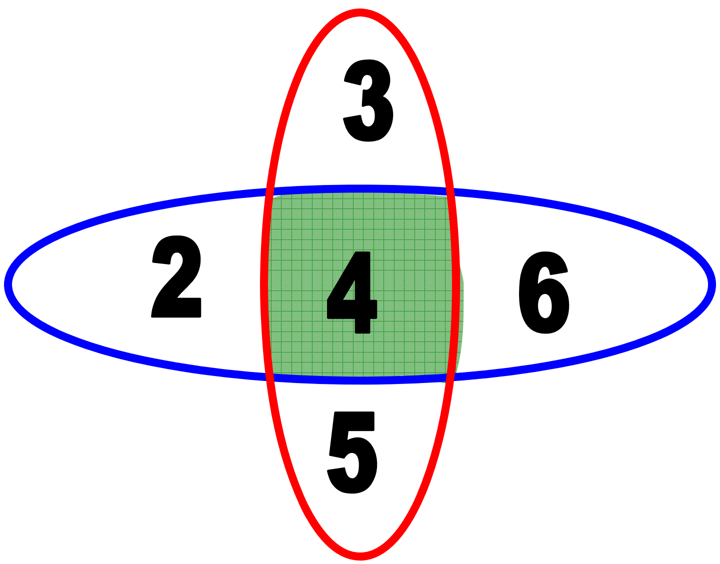


The Intersection Operator

- 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. ($A \cap B = \emptyset$)
- Example: the set of even integers is disjoint with the set of odd integers.

Inclusion-Exclusion Principle

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

- Ex

$\{2,3,5\} \cup \{3,5,7\}$ … $\{2,3,5,7\}$

Subtract out items in intersection, to compensate for double-counting them!

Set Difference

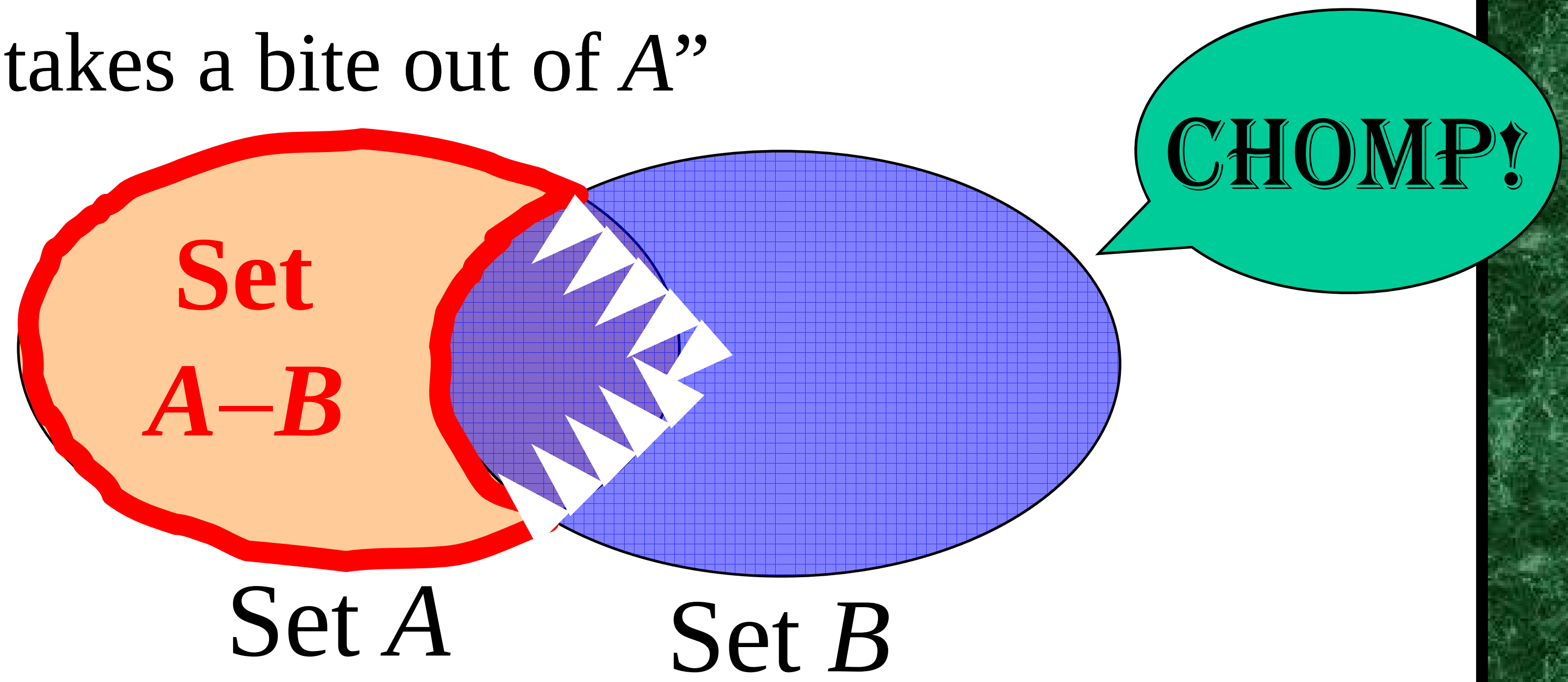
- For sets A, B, the *difference of A and B*, written $A–B$, is the set of all elements that are in A but not B.
- $A - B :\equiv \{x \mid x \in A \wedge \mathrm{x} \notin B\}$
  $= \{x \mid \neg(\, x \in A \rightarrow x \in B\,)\,\}$
- Also called:
  The *complement of B with respect to A*.

Set Difference Examples

- $\{1,\cancel{2},\cancel{3},4,\cancel{5},6\} - \{2,3,5,7,9,11\} =$ <u>{1,4,6}</u>
- $\mathbf{Z} - \mathbf{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\}$
  $= \{x \mid x \text{ is an integer but not a nat. \#}\}$
  $= \{x \mid x \text{ is a negative integer}\}$
  $= \{\ldots, -3, -2, -1\}$

Set Difference - Venn Diagram

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



Set Complements

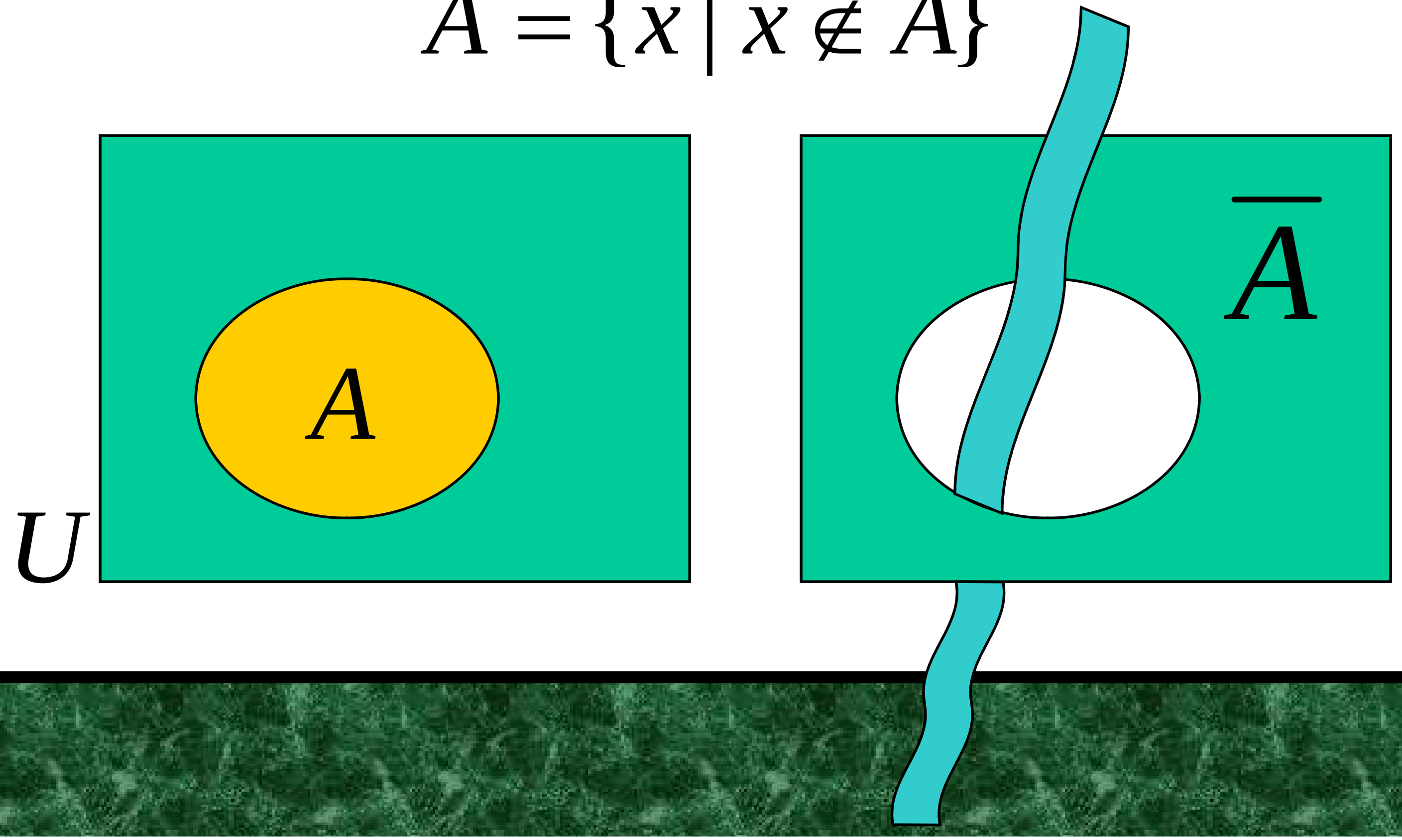
- The *universe of discourse* can itself be considered a set, call it U.
- The *complement* of A, written $\overline{A}$, is the complement of A w.r.t. U, *i.e.*, it is $U-A$.
- *E.g.*, If $U=\mathbf{N}$,

$$\overline{\{3,5\}} = \{0,1,2,4,6,7,\ldots\}$$

More on Set Complements

- An equivalent definition, when U is clear:

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



Set Identities

- Identity: $A \cup \varnothing = A \quad A \cap U = A$
- Domination: $A \cup U = U \quad A \cap \varnothing = \varnothing$
- Idempotent: $A \cup A = A = A \cap A$
- 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 $E_1 = E_2$ (where Es are set expressions), here are three useful techniques:

- Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.
- Use logical equivalences.
- 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 $(A\cap B)\cup(A\cap C) \subseteq A\cap(B\cup C)$. …

Method 2: LHS=RHS through Identities

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

$$
\begin{aligned}
\text{L.H.S} &= (A - B) - C \\
&= (A \cap B') \cap C' \\
&= A \cap B' \cap C'
\end{aligned}
$$

$$
\begin{aligned}
\text{R.H.S} &= (A - C) - (B - C) \\
&= (A \cap C') - (B \cap C') \\
&= (A \cap C') \cap (B \cap C')' \\
&= (A \cap C') \cap (B' \cup C) \\
&= A \cap [C' \cap (B' \cup C)] \\
&= A \cap [(C' \cap B') \cup (C' \cap C)] \\
&= A \cap [(C' \cap B') \cup \phi] \\
&= A \cap (C' \cap B') \\
&= A \cap B' \cap C'
\end{aligned}
$$

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

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

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 Union

- Binary union operator: $A \cup B$
- n-ary union:
  $A \cup A_2 \cup \ldots \cup A_n :\equiv ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)$
  (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:
  $A \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n)$
  (grouping & order is irrelevant)
- "Big Arch" notation: $\bigcap_{i=1}^{n} A_i$
- Or for infinite sets of sets: $\bigcap_{A \in X} A$

Bit Vector Representation of Sets

- Let $U = \{x_1, x_2, \ldots, x_n\}$, and let $A \subseteq U$.
- Then the *characteristic vector* of A is the n-vector whose elements, x_i, are 1 if $x_i \in A$, and 0 otherwise.
- Ex. If $U = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, and $A = \{x_1, x_3, x_5, x_6\}$, then the characteristic vector of A is

$$(101011)$$

Operation in Vector Representation

- Ex. If U = $\{x_1, x_2, x_3, x_4, x_5, x_6\}$,
- A = $\{x_1, x_3, x_5, x_6\}$, and B = $\{x_2, x_3, x_6\}$,
- Then we have a quick way of finding the characteristic vectors of $A \cup B$ and $A \cap B$.

A	1	0	1	0	1	1
B	0	1	1	0	0	1
$A \cup B$	1	1	1	0	1	1
$A \cap B$	0	0	1	0	0	1

Bit-wise OR

Bit-wise AND