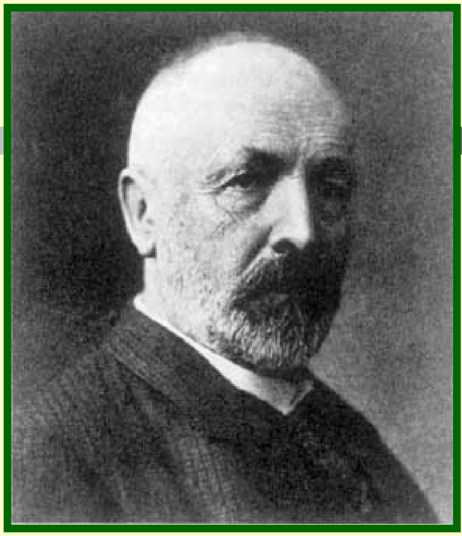
CS201: Discrete Mathematical Structures

Topic 2.1: SETS

(Discrete) STRUCTURES:

- SETS - one-place predicates

-(Binary) RELATIONS
  -two-place predicates



Georg Cantor
1845-1918

Topic 2.1:
The Theory of Sets

(Grimaldi (5th Edition): Sections 3.1-3.3 - pages 123- 150;
Rosen (8th Edition) : Sections 2.1-2.2 – pages 121-146)

Topic 2.1: Set Theory

a) Set Notations

b) Set Operations (defns using logic formulae)

c) Venn Diagrams

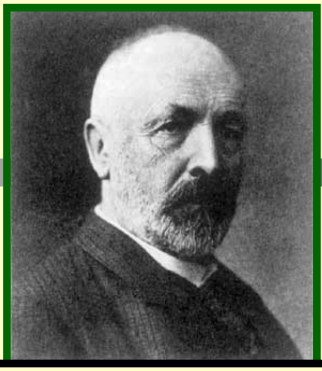
d) Set Cardinality: Finite and Infinite sets

e) Power Set

f) Additional set operations: Union, intersection, and set difference

g) Techniques for proving set identities

Introduction to Set Theory



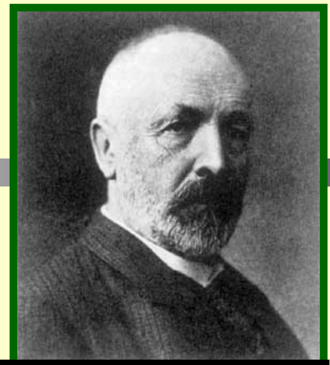
Georg Cantor
1845-1918

- 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.
- Sets are ubiquitous in computer software systems.
- *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*, …
- One way to denote a set *S* is 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.
- *Basic operation*: belongs to ($\in$)
  - The element a belongs to set S is denoted by $a \in S$.
  - The element d does not belong to set S is denoted by $d \notin S$.
- *Set builder notation* : For one-place predicate $P(x)$ over the universe of discourse, $\{x|P(x)\}$ is *the set of all x such that P(x).*
  - (the set $\{x|P(x)\}$ collects those x from the universe for which the predicate P(.) evaluates to "True".).

Basic properties of sets



Georg Cantor
1845-1918

- 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

Definitions!

- Two sets are 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* | *x* is an integer where *x* >0 and *x* <5 }

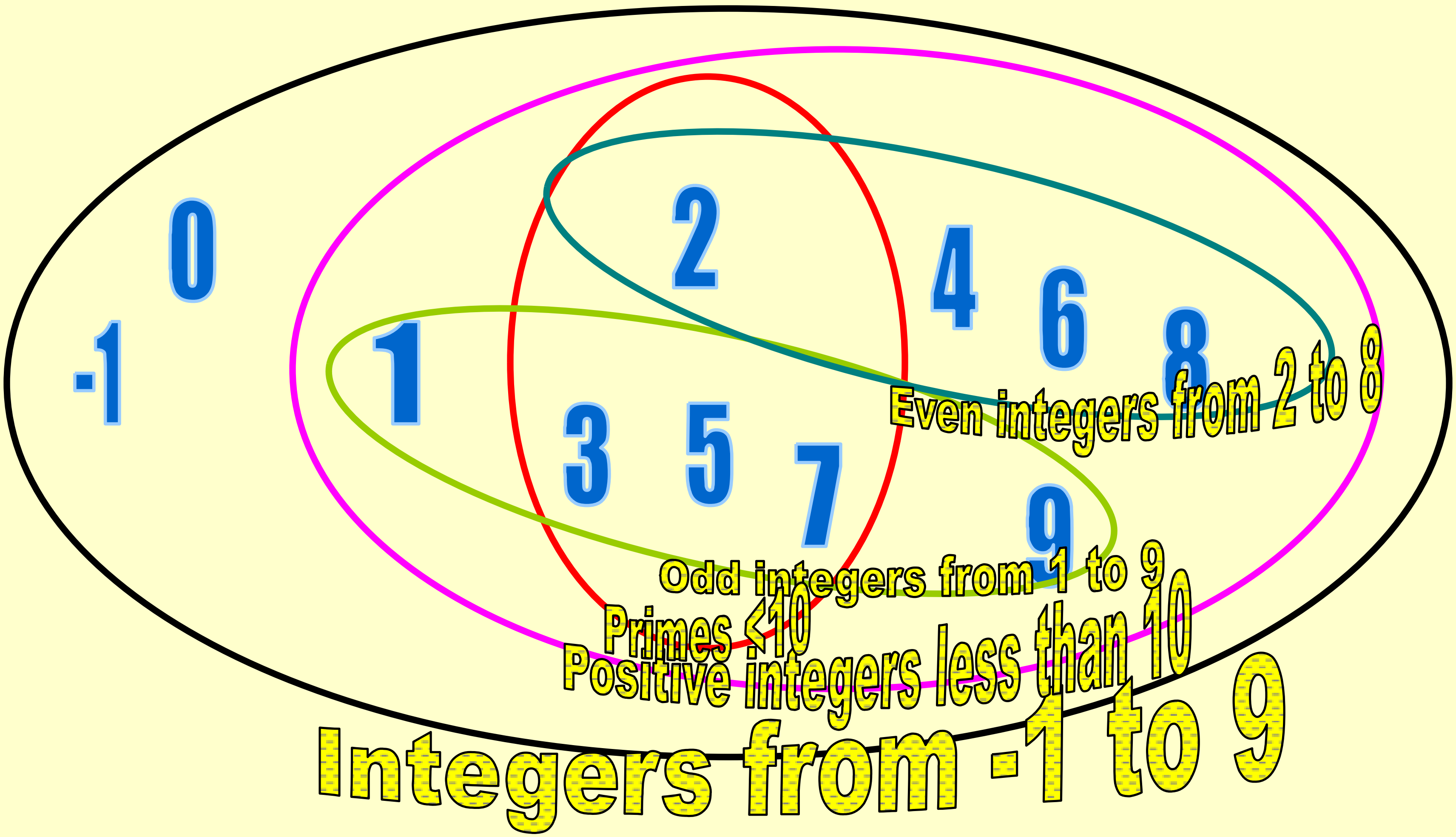
  =

  {*x* | *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 Zntegers.
  R = The "**R**eal" numbers, such as 374.1828471929498181917281943125 ...
- Infinite sets come in different sizes!

Venn Diagrams



Basic operation: Belonging to / Member of

- $x \in S$ ("x is in S") is the proposition that object x is an $\in$*(e)lement* or *member* of set S. Alternately, we also say that x belongs to S.
  - *e.g.* $3 \in \mathbf{N}$, "a"$\in \{x \mid x$ is a letter of the alphabet$\}$
  - Can define set equality in terms of $\in$ relation: $\forall S,T\colon S = T \leftrightarrow (\forall x : x \in S \leftrightarrow x \in T)$ "Two sets are equal iff they have all the same members."
- $x \notin S :\equiv \sim(x \in S)$ "x is not in S"

The Empty Set

- Φ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\Phi = \{\ \} = \{x \mid \textbf{False}\}$
- No matter the domain of discourse, we have the axiom $\sim\exists x : x \in \Phi$.
- Zermilo-Frankel Axioms of Set Theory (as part of our course) : watch 9.19 minute video of Albert R Mayer from https://www.youtube.com/watch?v=zcvsyL7GtH4

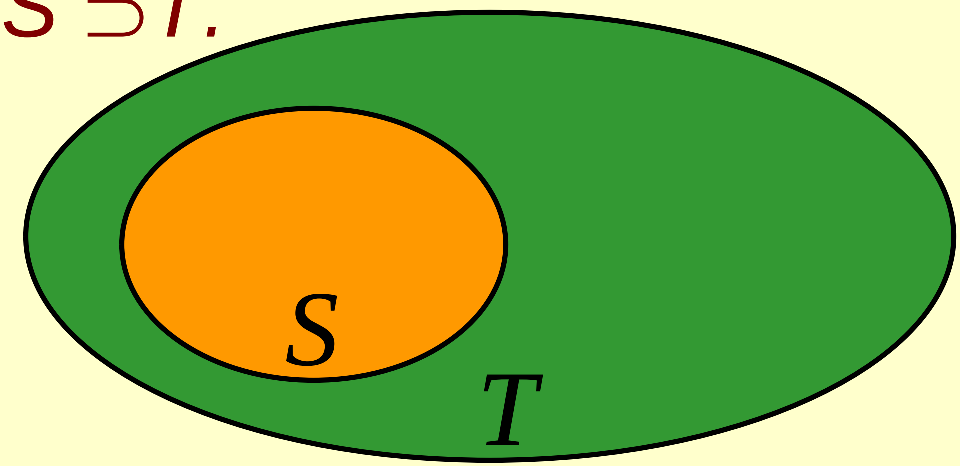
Subset and Superset Relations

- $S \subseteq T$ ("S is a subset of T") means that every element of S is also an element of T.
- $S \subseteq T \equiv \forall x\ (x \in S \rightarrow x \in T)$
- $\Phi \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("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 $\sim(S \subseteq T)$, *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 $S \supset T$.

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!

- Zermilo-Fraenkel Axioms of Set of our course) : watch 9.19 minute video of Albert R Mayer (MIT CS course) from https://www.youtube.com/watch?v=zcvsyL7GtH4

Zermelo-Fraenkel Axioms

Ernst Zermelo (1871-1953) gave axioms of set theory, which were improved by Adolf Fraenkel (1891-1965). This system of axioms called ZF or ZFC (if the axiom of choice is included) is the most widely used definition of sets.

(ZF1) Axiom of Extension(ality) Two sets are equal iff they have the same members:

$$\forall a \forall b (\forall x (x \in a \leftrightarrow x \in b) \leftrightarrow a = b)$$

(ZF2) Empty Set Axiom There is a set $\varnothing$ with no elements:

$$\exists a \forall x (\neg (x \in a))$$

(ZF3) Pairing Axiom If a and b are sets, there exists a set, $\{a, b\}$, whose members are exactly a and b:

$$\forall a \forall b \exists c (\forall x (x \in c \leftrightarrow ((x = a) \vee (x = b))))$$

Special case: $\{a, a\}$ denoted $\{a\}$—**singleton set.**

(ZF4) Union Axiom If a is a set there exists a set $\bigcup a$ whose members are the members of members of a:

$$\forall a \exists b \forall x (x \in b \leftrightarrow \exists y ((x \in y) \wedge (y \in a)))$$

Notation: $\bigcup \{a, b\}$ is denoted $a \cup b$.

(ZF5) Powerset Axiom If a is a set, there is a set, $\wp(a)$, whose members are the subsets of a:

$$\forall a \exists b \forall x (x \in b \leftrightarrow x \subseteq a)$$

[shorthand: $a \subseteq b$ stands for $\forall x (x \in a \to x \in b)$].

(ZF6) Separation Axiom (Scheme) (*alias* **Subset**, *alias* **Selection**). For any admissible formula $\varphi(x)$ and for any set a there is a set

$$\{ x \in a : \varphi(x) \}$$

whose members are those members of a which satisfy $\varphi(x)$.

(ZF7) Axiom of Infinity There exists an inductive set, that is,

$$\exists a (\varnothing \in a \wedge \forall x (x \in a \to x \cup \{x\} \in a))$$

(ZF8) Replacement Axiom (Scheme) 'The range of a partial function whose domain is a set is itself a set'. Let $\varphi(x, y)$ be an admissible formula such that $\forall s \exists t ((\varphi(s, t) \wedge \forall u (\varphi(s, u) \to u = t)))$ (that is, φ is a **class function**). Then

$$\forall a \exists b \forall y (y \in b \leftrightarrow \exists x (x \in a \wedge \varphi(x, y)))$$

(that is, when restricted to a set a, the range of φ is a set b).

(ZF9) Axiom of Foundation (*alias* **Regularity**) Every non-empty set is well-founded (that is, contains an element minimal w.r.t. $\in$):

$$\forall a (a \neq \varnothing \to (\exists x (x \in a \wedge x \cap a = \varnothing)).$$

Consistency and completeness in Set Theory —Revisited from Topic 1.05 – slides 14-15

- A system of axioms is called complete, if all the true statements can be proven from the axiom.
- A system of axioms is called consistent if it is not possible to derive a contradiction from them.
- A set of axioms is relatively consistent with respect to a second set of axioms, if the first set is consistent if the second one is.
- A statement is called independent of a system of axioms, if it cannot be proved or disproved using the axioms.

- K. Gödel showed that
  - *In any consistent axiomatic system (formal system of mathematics) sufficiently strong to allow one to do basic arithmetic, one can construct a statement about natural numbers that can be neither proved nor disproved within that system.*
    Rephrased: *a sufficiently strong system is not complete.*
  - *Any sufficiently strong consistent system cannot prove its own consistency.*
  - *Therefore set theory is neither complete, nor can it be proven to be consistent within the realm of set theory.*
  - (1935) ZFC is relatively consistent with ZF

- F. Cohen (1963) showed the axiom of choice is independent of ZF.

The Continuum hypothesis

- Cantor expected that all infinite subsets of **R** have either the cardinality $\aleph_0$ or the cardinality c of the continuum.
- Assuming the axiom of choice; rephrased there are no cardinals between c=$2^{\aleph_0}$ and $\aleph_1$.
- The continuum hypothesis can be phrased as $2^{\aleph_0} = \aleph_1$
- The generalized continuum hypothesis reads $2^{\aleph_\alpha} = \aleph_{\alpha+1}$
- Gödel (1939) proved that the (generalized) continuum hypothesis is consistent with ZFC**.**
- P. Cohen proved
  - The continuum hypothesis is independent of ZFC.
  - The negation of the continuum hypothesis is consistent with ZFC

Kurt Gödel and Paul J. Cohen

- Born in1906 in Brno
- 1929 PhD at the Unversity of Vienna
- 1930 faculty at the University of Vienna
- 1931 Incompleteness Theorems.
- 1932 Habilitation
- 1940 emigration to the US bcoming citizen in 1948.
- Member of the IAS in Princeton (permanent from 1953 on)
- 1940 relative consistency of the continuum-hypothesis.
- Died in 1978

- Born in 1934
- 1958 PhD University of Chicago
- Was at MIT and the IAS and became faculty at Stanford in 1961
- 1966 Fields Medal
- Invented “forcing”. This can be used to show the independence of the axiom of choice and the generalized continuum hypothesis.

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

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, *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}×{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: $\sim\forall A,B$: A×B=B×A.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...

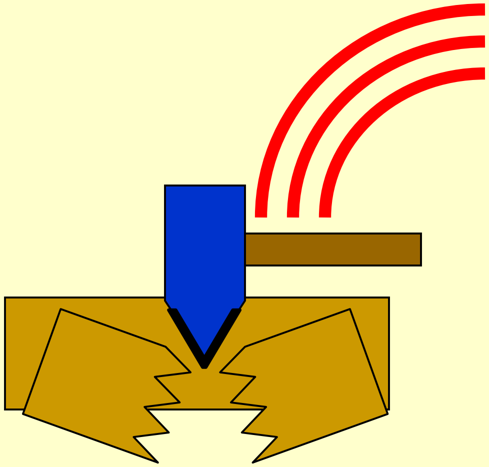
René Descartes (1596-1650)

Review

- Sets S, T, U... Special sets **N**, **Z**, **R**.
- Set notations {a,b,...}, $\{x|P(x)\}$...
- Set relation operators $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$. (These form propositions.)
- Finite vs. infinite sets.
- Set operations $|S|$, P(S), $S \times T$.
- Next : More set ops: $\cup$, $\cap$, $-$.

The Union Operator

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



After the downward-pointing "axe" of "$\vee$" splits the wood, you can take 1 piece OR the other, or both.

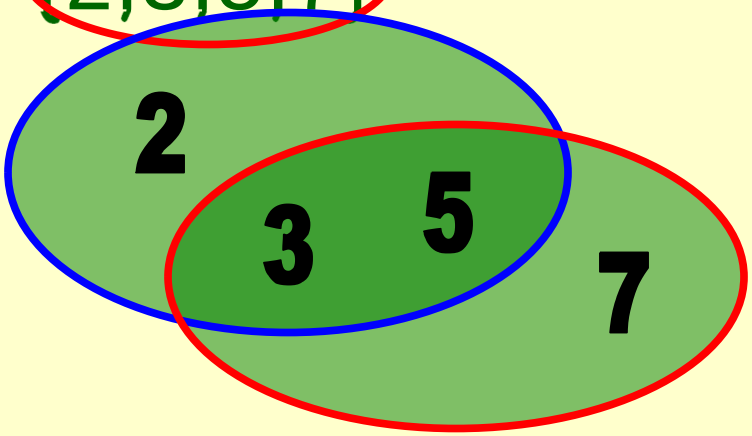
The Union Operator : using $\supseteq$ operation

- 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



Think “The **Uni**on of IIT Indore students includes every person who studies in <u>any</u> department in IIT Indore.”

The Intersection Operator

Definitions!

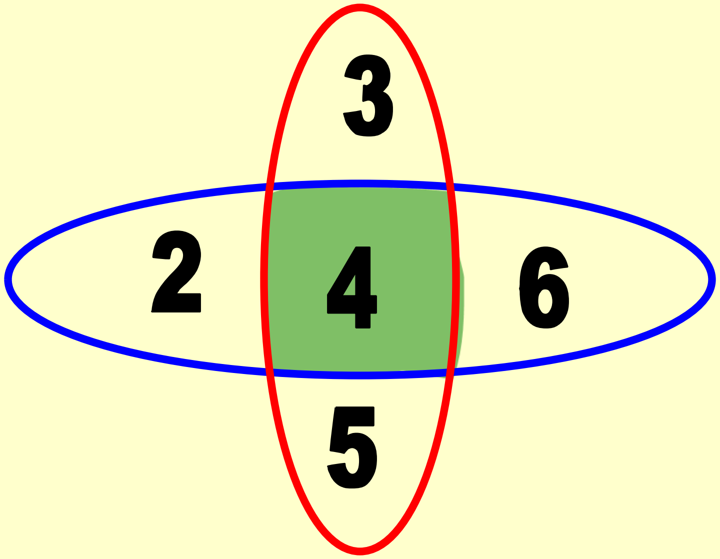
- For sets A, B, their *intersection* $A \cap B$ is the set containing all elements that are simultaneously in A **and** ("$\wedge$") in B.
- Formally,

$$\forall A, B\colon A \cap B \equiv \{x \mid x \in A \wedge x \in B\}.$$

- Note that $A \cap B$ is a subset of A **and** it is a subset of B:
  $\forall A, B\colon (A \cap B \subseteq A) \wedge (A \cap B \subseteq B)$

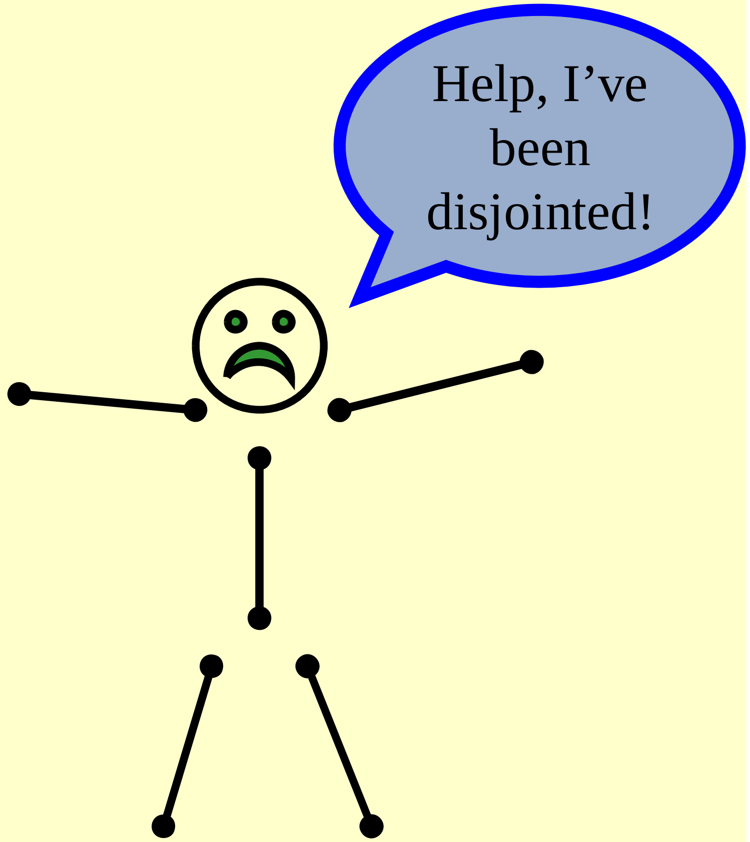
Intersection Examples

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



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.



Set Difference

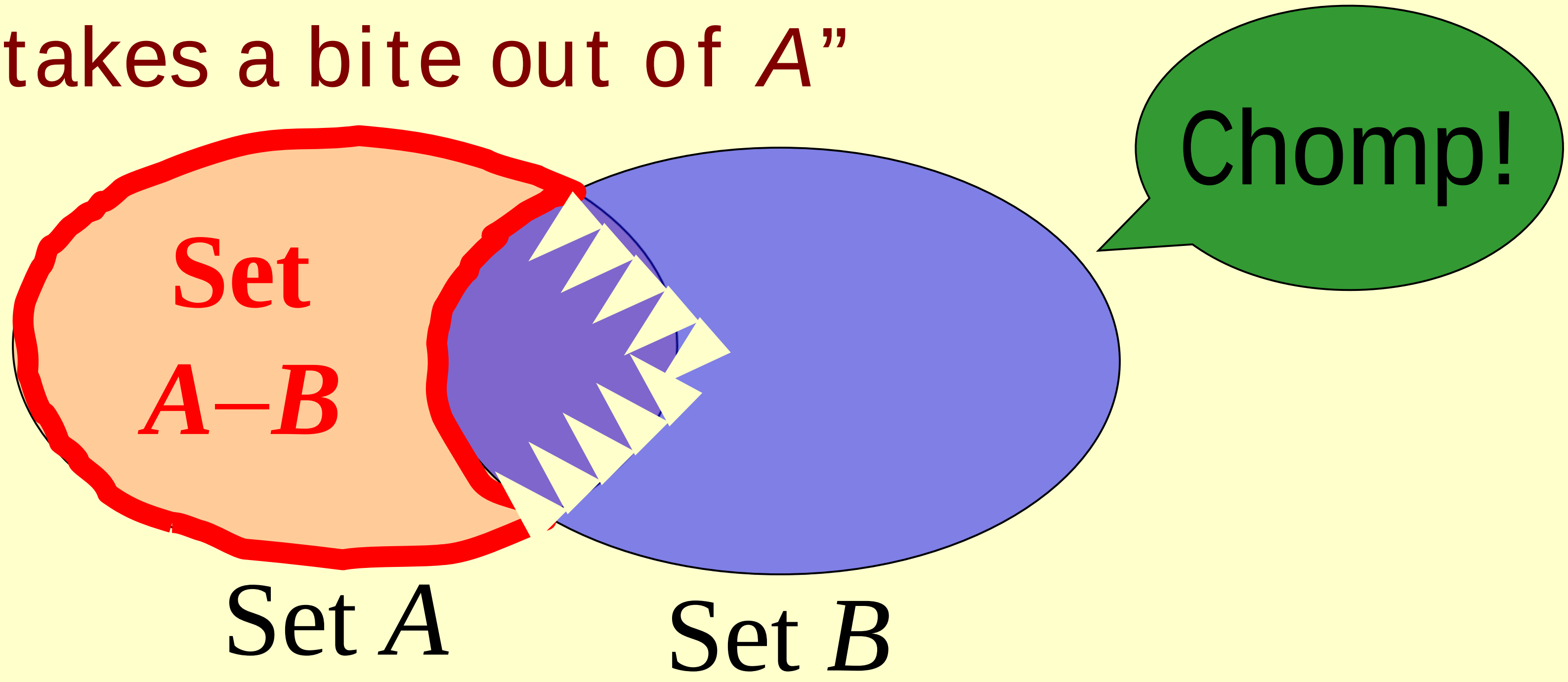
- For sets *A*, *B*, the *difference of A and B*, written $A-B$, is the set of all elements that are in *A* but not *B*.
- $A - B :\equiv \{x \mid x \in A \wedge x \notin B\}$
  $= \{x \mid \sim(x \in A \rightarrow x \in B) \}$
- Also called:
  The *complement of B with respect to A*.

Set Difference Examples

- $\{1,\cancel{2},\cancel{3},4,\cancel{5},6\} - \{2,3,5,7,9,11\} =$
  $\underline{\quad\{1,4,6\}\quad}$
- $\mathbf{Z} - \mathbf{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\}$
  $= \{x \mid x \text{ is an integer but not a natural \#}\}$
  $= \{x \mid x \text{ is a negative integer}\}$
  $= \{\ldots, -3, -2, -1\}$

Set Difference - Venn Diagram

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

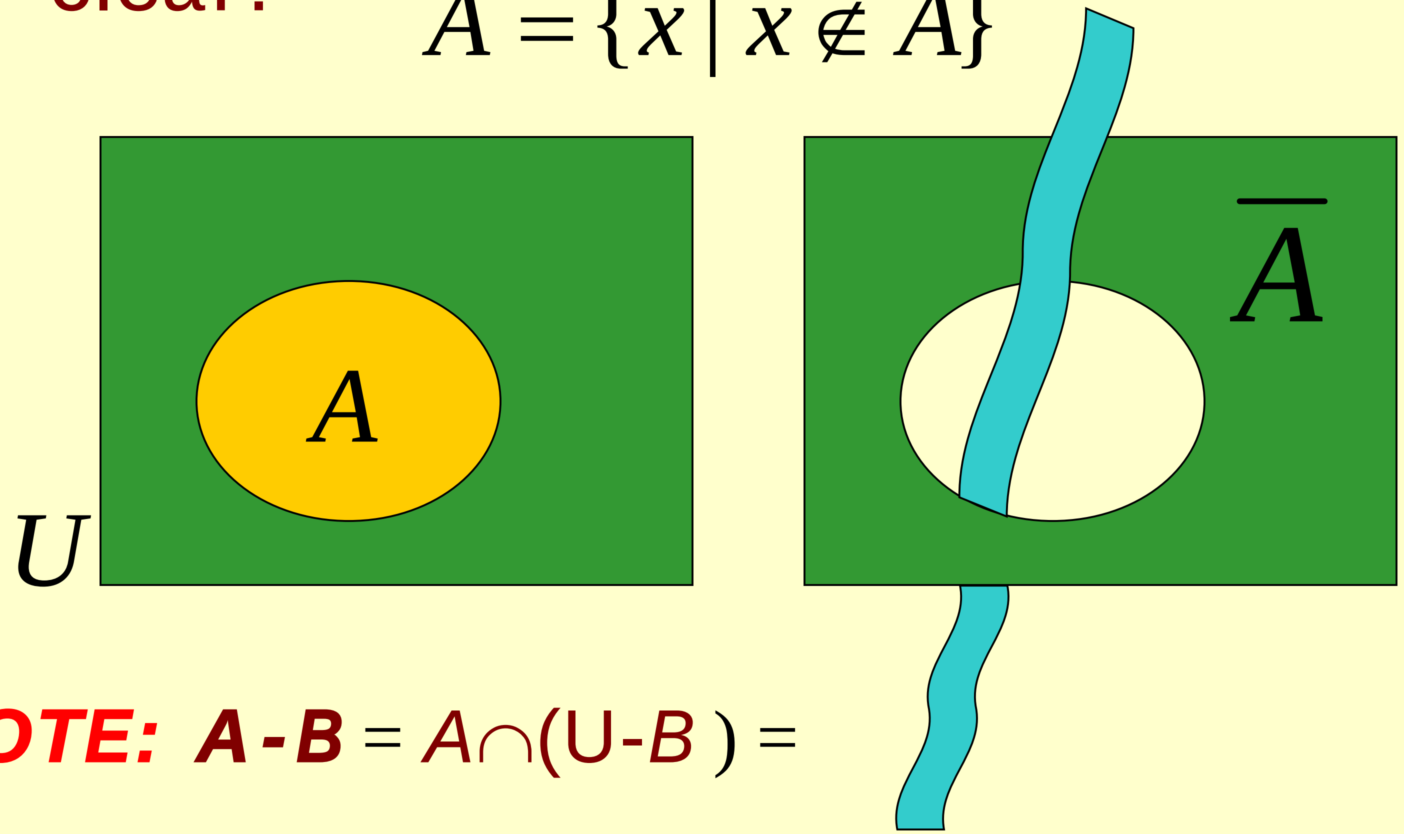


Set Complements

- 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 $\overline{A}$, is the complement of *A* w.r.t. *U*, *i.e.*, it is $U - A$.
- *E.g.,* If *U*=**N**, $\overline{\{3,5\}} = \{0,1,2,4,6,7,...\}$

More on Set Complements

- An equivalent definition, when *U* is clear: $\overline{A} = \{x \mid x \notin A\}$



***NOTE:* A - B** = $A \cap (U - B) =$

Set Identities

- Identity: $A \cup \emptyset = A \quad A \cap U = A$
- Domination: $A \cup U = U \quad A \cap \emptyset = \emptyset$
- Idempotent: $A \cup A = A = A \cap A$
- 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.

Augustus De Morgan (1806-1871)

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

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

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:

1. Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ 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 $(A\cap B)\cup(A\cap C) \subseteq A\cap(B\cup C)$. …

Method 2: logical Equivalences

- Exactly follow propositional logic
  - (We shall omit details for this method – as they quickly follow from the discussion in Method 3).
  - Organized form of this method gives rise to Method 3: Membership Tables, which we shall see in more detail.

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	$A \cup B$	$(A \cup B) - B$	$A - B$
$\notin$	$\notin$	$\notin$	$\notin$	$\notin$
$\notin$	$\in$	$\in$	$\notin$	$\notin$
$\in$	0	$\in$	$\in$	$\in$
$\in$	$\in$	$\in$	$\notin$	$\notin$

Membership Table Exercise

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

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

First set of "Equiv. Laws of Sets"

- Double complement: $\overline{(\overline{A})} \equiv A$
- De Morgan's laws: $\overline{(A \cap B)} \equiv \overline{A} \cup \overline{B}$

$$\overline{(A \cup B)} \equiv \overline{A} \cap \overline{B}$$

Augustus De Morgan (1806-1871)

Key to remember: "Double D – laws"

Second set of "Equiv. Laws of Sets"

- Commutative laws: $A \cap B \equiv B \cap A$

  $A \cup B \equiv B \cup A$
- Associative laws: $(A \cap B) \cap C \equiv A \cap (B \cap C)$

  $(A \cup B) \cup C \equiv A \cup (B \cup C)$
- Distributive laws: $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$

  $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
- Absorption laws: $A \cap (A \cup B) \equiv A$

  $A \cup (A \cap B) \equiv A$

Key to remember: "CADA – laws"

Third set of "Equiv. Laws of Sets"

- Idempotent laws: $A \cap A \equiv A$

  $A \cup A \equiv A$

- Identity laws: $A \cap U \equiv A$

  $A \cup \Phi \equiv A; \; A - B = A \cap \overline{B}$

- Inverse laws: $A \cap \overline{A} \equiv \Phi$

  $A \cup \overline{A} \equiv U$

- Domination laws: $A \cap \Phi \equiv \Phi$

  $A \cup U \equiv U$

Key to remember: "I^{3}D – laws"

Key for Complete set to remember: "Double D –CADA – I^{3}D"

A set of "Equiv. Laws of Sets"

Key for three sets of Laws of Logic : "Double D –CADA – I ^{3}D"

- Ten laws:

- Double Complement, De Morgans laws : Double D
- Commutative, Associative, Distributive, Absorption laws : CADA
- Idempotent, Identity, Inverse, Domination laws : I ^{3}D

➢ How to prove these laws: "construct ***membership*** tables for left hand side (LHS), RHS, and show that they are identical"

➢ (Work out details : left as exercise.)

Review

- Sets S, T, U… Special sets **N**, **Z**, **R**.
- Set notations {a,b,...}, $\{x|P(x)\}$… $\overline{S}$
- Relations: $x \in S$, $S \subseteq T$, $S \not\subset T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$,
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.

Additional Reading, Tutorials and Exercises

- Grimaldi (5th Edition): Sections 3.1-3.3 - pages 123- 150;

  Exercises 3.1 – (30 in number) pages 134-136;

  Exercises 3.2 – (20 in number) pages 146-147;

  Exercises 3.3 (10 in number) page 150.

- Rosen (8th Edition) : Sections 2.1-2.2 – pages 121-146

  Exercises 2.1 – (51 in number) pages 131-133;

  Exercises 2.2 – (75 in number) pages 146-146;