Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

• 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be **logically inconsistent**!
  
  – This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  
  – $\therefore$ The conjunction of the axioms is a contradiction!
  
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• **More sophisticated set theories fix this problem.**
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$
• 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 } x > 0 \text{ and } x < 5 \} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{The Natural numbers.} \]
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{The Integers.} \]
  \[ \mathbb{R} = \text{The “Real” numbers, such as } 374.1828471929498181917281943125\ldots \]

• “Blackboard Bold” or double-struck font (\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet$\}$
  - Can define set equality in terms of $\in$ relation:
    $\forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)$
    “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

- $\emptyset$ (“null”, “the empty set”) is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x|\text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x: x\in\emptyset$. 
Subset and Superset Relations

- $S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Note $S = T \iff S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg(S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
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 \( S \subsetneq T \).

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


Very Important!
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 \(|S| \in \mathbb{N}\), then we say \(S\) is finite. Otherwise, we say \(S\) is infinite.

• What are some infinite sets we’ve seen?

\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)
The **Power Set** Operation

- The *power set* \( P(S) \) of a set \( S \) is the set of all subsets of \( S \). \[ P(S) \equiv \{ x \mid x \subseteq S \}. \]
- *E.g.* \( P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \} \).
- Sometimes \( P(S) \) is written \( 2^S \).
- Note that for finite \( S \), \[ |P(S)| = 2^{|S|}. \]
- It turns out \( \forall S: |P(S)| > |S| \), *e.g.* \( |P(\mathbb{N})| > |\mathbb{N}| \). *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\mid P(x)\}.
• $\in$ relational operator, and the empty set $\emptyset$.
• Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
• Venn diagrams.
• Cardinality $|S|$ and infinite sets $N$, $Z$, $R$.
• Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  – (That do not have self-consistent properties.)
• These “sets” mathematically cannot exist.
• *E.g.* let $S = \{ x \mid x \not\in x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

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

Contrast with sets’ $\{\}$
Cartesian Products of Sets

• For sets $A$, $B$, their *Cartesian product* $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.

• *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$.

René Descartes (1596-1650)
Review of §1.6

• Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
• Set notations $\{a, b, ...\}$, $\{x \mid P(x)\}$...
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their $\text{Union } A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).

• Formally, $\forall A,B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.

• Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
Union Examples

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

Think “The **United** States of America includes every person who worked in **any** U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A,B: A \cap B = \{x \mid x \in A \land x \in B\}$.

• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):

  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The **intersection** of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[
|A \cup B| = |A| + |B| - |A \cap B|
\]

- Example: How many students are on our class email list? Consider set \( M \), \( I = \{ \text{students turned in an information sheet} \} \), \( M = \{ \text{sent the TAs their email address} \} \)

\[
|I \cup M| = |I| + |M| - |I \cap M|
\]
Set Difference

• For sets $A$, $B$, the *difference of $A$ and $B$*, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:

$$A \setminus B := \{x \mid x \in A \land x \notin B\}$$

$$= \{x \mid \neg(x \in A \rightarrow x \in B)\}$$

• Also called:

  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

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

- \Z - \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 $U$.
- 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 $U \setminus A$.
- *E.g.*, If $U = \mathbb{N}$, $\{3,5\} = \{0,1,2,4,6,7,\ldots\}$
More on Set Complements

- An equivalent definition, when $U$ is clear:

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

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U, A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A, A \cap B = B \cap A \)
- **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 provable from) DeMorgan’s Law for propositions.

\[
A \cup B = \overline{A} \cap \overline{B}
\]
\[
A \cap B = \overline{A} \cup \overline{B}
\]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

• Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

• Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(A)</td>
<td>(B)</td>
<td>(A \cup B)</td>
<td>((A \cup B) - B)</td>
<td>(A - B)</td>
<td></td>
</tr>
<tr>
<td>0 0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0 1</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1 0</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1 1</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Membership Table Exercise

Prove \((A \cup B)\overline{C} = (A\overline{C}) \cup (B\overline{C})\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B)\overline{C})</th>
<th>(A\overline{C})</th>
<th>(B\overline{C})</th>
<th>((A\overline{C}) \cup (B\overline{C}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
<td>(0)</td>
<td>(0)</td>
<td>(0)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>(A\overline{C})</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>(B\overline{C})</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>((A\overline{C}) \cup (B\overline{C}))</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>((A\overline{C}) \cup (B\overline{C}))</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>((A\overline{C}) \cup (B\overline{C}))</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>((A\overline{C}) \cup (B\overline{C}))</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>((A\overline{C}) \cup (B\overline{C}))</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-\), $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on 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:=∅, 1:=\{0\}, 2:=\{0,1\}, 3:=\{0,1,2\}, ...
  – Bit strings:
    0:=0, 1:=1, 2:=10, 3:=11, 4:=100, ...
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\neg$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects \((\text{elements})\) that we can describe (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be **logically inconsistent**!
  
  – This means, there exist naïve set theory propositions \(p\) such that you can prove that both \(p\) and \(\neg p\) follow logically from the axioms of the theory!
  
  – \(\therefore\) The conjunction of the axioms is a contradiction!

• More sophisticated set theories fix this problem.
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, $\{x \mid P(x)\}$ 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 \( \{1, 2, 3, 4\} = \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5\} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\} \)
Infinite Sets

- Conceptually, sets may be infinite \((i.e.,\) not finite, without end, unending). 
- Symbols for some special infinite sets: 
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \text{ The Natural numbers.} \]
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \text{ The Integers.} \]
  \[ \mathbb{R} = \text{The “Real” numbers, such as 374.1828471929498181917281943125…} \]
- “Blackboard Bold” or double-struck font \((\mathbb{N}, \mathbb{Z}, \mathbb{R})\) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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.* $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet\}
  - Can define set equality in terms of $\in$ relation:
    \[ \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T) \]
    "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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x|\text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x: x\in\emptyset$. 
Subset and Superset Relations

- \( S \subseteq T \) ("S is a subset of T") means that every element of \( S \) is also an element of \( T \).
- \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq S \).
- \( S \supseteq T \) ("S is a superset of T") means \( T \subseteq S \).
- Note \( S = T \iff S \subseteq T \land S \supseteq T \).
- \( S \nsubseteq T \) means \( \neg (S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \)
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 \( S \subsetneq T \).

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 $1 \neq \{1\} \neq \{\{1\}\}$ !!!!
Cardinality and Finiteness

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

\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)
The **Power Set Operation**

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
  Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S : |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \not\in$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set *descriptions* that lead to pathological structures that are not *well-defined*.
  - (That do not have self-consistent properties.)
- These “sets” mathematically *cannot* exist.
- *E.g.* let \( S = \{ x \mid x \notin x \} \). Is \( S \in S \)?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.

- **Note that** $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.

- Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., $n$-tuples.

Contrast with sets’ $\{\}$
Cartesian Products of Sets

• For sets $A$, $B$, their *Cartesian product* $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.  

• *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...

René Descartes  
(1596-1650)
Review of §1.6

• Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

- For sets $A$, $B$, their Union $A \cup B$ is the set containing all elements that are either in $A$, or ("\text{\texttt{v}}") in $B$ (or, of course, in both).
  - Formally, $\forall A, B: A \cup B = \{x \mid x \in A \lor x \in B\}$.
  - Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
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\}

Think “The **United** States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

• For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ and (“\(\land\)”) in $B$.

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):

  $$\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$$
Intersection Examples

• \{a,b,c\} \cap \{2,3\} = \emptyset
• \{2,4,6\} \cap \{3,4,5\} = \{4\}

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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.

Help, I’ve been disjointed!
Inclusion-Exclusion Principle

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

Example: How many students are on our class email list? Consider set 

\[ I = \{ \text{students turned in an information sheet} \} \]

\[ M = \{ \text{students sent the TAs their email address} \} \]

Some students did both!

\[ |I \cup M| = |I| + |M| - |I \cap M| \]

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 $B$. Formally:
  
  $A - B \equiv \{ x \mid x \in A \land x \notin B \}$
  
  $\quad = \{ x \mid \neg(x \in A \rightarrow x \in B) \}$

- Also called:
  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \( \{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} = \{1,4,6\} \)

- \( \mathbb{Z} - \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\} \)
  = \( \{x \mid x \) is an integer but not a nat. \#\} \)
  = \( \{x \mid x \) 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 \( U = \mathbb{N} \), \( \{3,5\} = \{0,1,2,4,6,7,\ldots\} \)
More on Set Complements

• An equivalent definition, when $U$ is clear:

$$\overline{A} = \{ x \mid x \not\in A \}$$
Set Identities

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U , A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A , A \cap B = B \cap A \)
- **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 provable 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 the \( E \)s 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 \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \).

- **Part 1:** 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, \( A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \).

- **Part 2:** Show \( (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \). …
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.
Prove \((A \cup B) - B = A - B\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) - B)</th>
<th>(A - B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
[Membership Table Exercise]

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

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$…
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets,
  \[ X = \{ A \mid P(A) \} \].
Generalized Union

- Binary union operator: $A \cup B$
- $n$-ary union:
  $$A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n)$$
  (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: \( \prod_{i=1}^{n} A_i \)
- Or for infinite sets of sets:
  \[ \prod_{A \in X} A \]
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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0,1\}$, $3 := \{0,1,2\}$, …
  – Bit strings:
    $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, …
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\overline{}$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

• 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).
Naïve set theory

- **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

- But, the resulting theory turns out to be **logically inconsistent**!
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

- More sophisticated set theories fix this problem.
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$
• 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 } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \] The natural numbers.
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \] The integers.
  \[ \mathbb{R} = \] The “Real” numbers, such as 374.1828471929498181917281943125…

• “Blackboard Bold” or double-struck font (\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn 1834-1923
Basic Set Relations: Member of

- \( x \in S \) ("x is in S") is the proposition that object \( x \) is an \( \text{Element} \) or \( \text{member} \) of set \( S \).
  
  - e.g. \( 3 \in \mathbb{N}, \) “a”\( \in \{x \mid x \text{ is a letter of the alphabet} \}\)
  
  - Can define set equality in terms of \( \in \) relation:
    \[ \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T) \]
    “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

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{ \} = \{ x | \text{False} \} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x: x \in \emptyset \).
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.
- \( S \subseteq T \iff \forall x (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, S \subseteq S \).
- \( S \supseteq T \) ("S is a superset of T") means \( T \subseteq S \).
- Note \( S = T \iff S \subseteq T \land S \supseteq T \).
- \( S \nsubseteq T \) means \( \neg (S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \)
Proper (Strict) Subsets & Supersets

- $S \subset T$ ("S is a proper subset of T") means that $S \subseteq T$ but $T \not\subset S$. 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 $1 \neq \{ 1 \} \neq \{ \{ 1 \} \}$ !!!!
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
- What are some infinite sets we’ve seen? $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
The *Power Set* Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$.  
  $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
  Note that for finite $S$,  
  $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.

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 \(\emptyset\).
- Set relations \(=, \subseteq, \supseteq, \subset, \supset, \emptyset\), etc.
- Venn diagrams.
- Cardinality \(|S|\) and infinite sets \(\mathbb{N}, \mathbb{Z}, \mathbb{R}\).
- Power sets \(P(S)\).
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined. (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- E.g. let $S = \{ x \mid x \not\in x \}$. Is $S \in S$?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, $n$-tuples.
Cartesian Products of Sets

• For sets $A$, $B$, their **Cartesian product** $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.

• *E.g.* $\{a,b\} \times \{1,2\} = \{(a,1),(a,2),(b,1),(b,2)\}$

• Note that for finite $A$, $B$, $|A \times B| = |A|\cdot|B|$.

• Note that the Cartesian product is *not* commutative: *i.e.*, $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$.

---

René Descartes (1596-1650)
Review of §1.6

• Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their union $A \cup B$ is the set containing all elements that are either in $A$, or ("\lor") in $B$ (or, of course, in both).

• Formally, $\forall A, B: A \cup B = \{ x | x \in A \lor x \in B \}$.

• Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset):
  $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$
Union Examples

- \(\{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\}\)
- \(\{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\} \Rightarrow \{2,3,5,7\}\)

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$.
**Intersection Examples**

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- Example: How many students are on our email list? Consider set \( I = M \), where \( I \) is the set of students who turned in an information sheet and \( M \) is the set of students who sent the TAs their email address. Some students did both! Thus, the number of students on our email list is:

\[ |I \cup M| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg(x \in A \rightarrow x \in B) \}$$

• Also called:

The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \{1,2,3,4,5,6\} – \{2,3,5,7,9,11\} = \{1,4,6\}
- \mathbb{Z} – \mathbb{N} = \{…, −1, 0, 1, 2, …\} − \{0, 1, …\} = \{x \mid x \text{ is an integer but not a nat.} \#\} = \{x \mid x \text{ is a negative integer}\} = \{…, −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 \( U \setminus A \).
- *E.g.,* If \( U = \mathbb{N} \), \( \{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots\} \)
More on Set Complements

- An equivalent definition, when $U$ is clear:

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

• Identity: \( A \cup \emptyset = A = A \cap U \)
• Domination: \( A \cup U = U, A \cap \emptyset = \emptyset \)
• Idempotent: \( A \cup A = A = A \cap A \)
• Double complement: \( \overline{\overline{A}} = A \)
• Commutative: \( A \cup B = B \cup A, A \cap B = B \cap A \)
• 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 provable from) DeMorgan’s Law for propositions.

\[
A \cup B = \overline{A} \cap \overline{B}
\]

\[
A \cap B = \overline{A} \cup \overline{B}
\]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A ∪ B) - B</th>
<th>A - B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

Prove \((A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>A \cup B</th>
<th>(A \cup B) \setminus C</th>
<th>A \setminus C</th>
<th>B \setminus C</th>
<th>(A \setminus C) \cup (B \setminus C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, \(X = \{A \mid P(A)\}\).
Generalized Union

• Binary union operator: $A \cup B$

• $n$-ary union:

$\bigcup_{i=1}^{n} A_i \\ A \cup A_2 \cup \ldots \cup A_n \equiv ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n))$

(grouping & order is irrelevant)

• “Big U” notation: $\bigcup_{A \in X} A$

• 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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, …
  – Bit strings: $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, …
Representing Sets with Bit Strings

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

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

In this representation, the set operators “∪”, “∩”, “¬” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• Basic premise: Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be logically inconsistent!
  – This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  – $\therefore$ The conjunction of the axioms is a contradiction!
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
Basic notations for sets

- For sets, we’ll use variables $S, T, U, \ldots$
- 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 \(\{a, b, c\} = \{a, c\} = \{b, c\} = \{a, a, b, a, b, c, c, c\}\).
  - 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 } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } x>0 \text{ and } x<25\}
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{The Natural numbers.} \]
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{The Integers.} \]
  \[ \mathbb{R} = \text{The “Real” numbers, such as } 374.1828471929498181917281943125\ldots \]
- “Blackboard Bold” or double-struck font (\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet\}
  - Can define set equality in terms of $\in$ relation:
    $\forall S,T: S=T \iff (\forall x: x \in S \iff x \in T)$
    "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

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{ \} = \{ x \mid False \} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x: x \in \emptyset \).
Subset and Superset Relations

- $S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S, S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Note $S = T \iff S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
Proper (Strict) Subsets & Supersets

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

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 $1 \not\in \{1\} \not\in \{\{1\}\}$ !!!!

Very Important!
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
- What are some infinite sets we’ve seen?

$\mathbb{N}, \mathbb{Z}, \mathbb{R}$
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 $2^S$.
  - Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, *e.g.* $|P(\mathbb{N})| > |\mathbb{N}|$.
  *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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$.
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- \( E.g. \) let \( S = \{ x \mid x \notin x \} \). Is \( S \in S \)?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

• These are like sets, except that duplicates matter, and the order makes a difference.
• For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
• Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
• Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., $n$-tuples.
Cartesian Products of Sets

- For sets $A$, $B$, their Cartesian product $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.
- *E.g.* $\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
- Note that for finite $A$, $B$, $|A \times B| = |A| \cdot |B|$.
- Note that the Cartesian product is not commutative: i.e., $\neg \forall A B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

• Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

- For sets $A$, $B$, their *Union* $A \cup B$ is the set containing all elements that are either in $A$, or ("\lor") in $B$ (or, of course, in both).
- Formally, $\forall A,B: A \cup B = \{ x | x \in A \lor x \in B \}$.
- Note that $A \cup B$ is a *superset* of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
Union Examples

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

Think “The **United** States of America includes every person who worked in **any** U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

• For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ and (“\&”) in $B$.

• Formally, $\forall A, B$: $A \cap B = \{x \mid x \in A \land x \in B\}$.

• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):

  $\forall A, B$: $(A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

• \(\{a, b, c\} \cap \{2, 3\} = \emptyset\)
• \(\{2, 4, 6\} \cap \{3, 4, 5\} = \{4\}\)

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- Example: How many students are on our class email list? Consider \( E = I \cup M \)
  \[ I = \{ \text{sent an information sheet} \} \]
  \[ M = \{ \text{sent the TAs their email address} \} \]
  Some students did both!

\[ |E| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:
  
  $$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$
  
  $$= \{ x \mid \neg(x \in A \rightarrow x \in B) \}$$

• Also called:
  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

• \{1,2,3,4,5,6\} – \{2,3,5,7,9,11\} = \{1,4,6\}

• \mathbb{Z} – \mathbb{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 $A$”

Chomp!
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 $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots \}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

• Identity: \( A \cup \emptyset = A = A \cap U \)
• Domination: \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
• Idempotent: \( A \cup A = A = A \cap A \)
• Double complement: \( \overline{\overline{A}} = A \)
• Commutative: \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
• 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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]
\[ A \cap B = \overline{A} \cup \overline{B} \]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

• Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

• Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

<table>
<thead>
<tr>
<th></th>
<th>B</th>
<th>A \cup B</th>
<th>( (A \cup B) - B )</th>
<th>A - B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

Prove \((A \cup B) - C = (A - C) \cup (B - C)\).
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,\ldots\}, \{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, \(X=\{A \mid P(A)\}\).
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:
  \[ A_1 \cap A_2 \cap \ldots \cap A_n \equiv (((A_1 \cap A_2) \cap \ldots) \cap A_n) \]
  (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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, ...
  - Bit strings: $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, ...
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\overline{\cdot}$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
• 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).
Naïve set theory

- **Basic premise**: Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

- **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

- **More sophisticated set theories fix this problem.**
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$

• 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,
  
  $\{x \mid P(x)\}$ 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 \textit{if and only if} they contain exactly the same elements.
- In particular, it does not matter \textit{how the set is defined or denoted}.
- \textbf{For example:} The set \{1, 2, 3, 4\} = 
  \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} = 
  \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25 \}
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as 374.1828471929498181917281943125…
- “Blackboard Bold” or double-struck font (\( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Basic Set Relations: Member of

• $x \in S$ (“$x$ is in $S$”) is the proposition that object $x$ is an \textit{element} or \textit{member} of set $S$.
  
  – e.g. $3 \in \mathbb{N}$, “a” $\in \{x \mid x$ is a letter of the alphabet$\}$
  
  – Can define set equality in terms of $\in$ relation: $\forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)$
    “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

• $\emptyset$ (“null”, “the empty set”) is the unique set that contains no elements whatsoever.

• $\emptyset = \{ \} = \{ x | \text{False} \}$

• No matter the domain of discourse, we have the axiom $\neg \exists x : x \in \emptyset$. 
Subset and Superset Relations

• $S \subseteq T$ (“$S$ is a subset of $T$”) means that every element of $S$ is also an element of $T$.

• $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$

• $\emptyset \subseteq S$, $S \subseteq S$.

• $S \supseteq T$ (“$S$ is a superset of $T$”) means $T \subseteq S$.

• Note $S = T \iff S \subseteq T \land S \supseteq T$.

• $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x \ (x \in S \land x \notin T)$
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 $S \subsetneq T$.

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 $1 \neq \{1\} \neq \{\{1\}\}$ !!!!
Cardinality and Finiteness

• \(|S|\) (read “the cardinality of \(S\)”\) is a measure of how many different elements \(S\) has.

• \(E.g., |\emptyset| = 0, \quad |\{1,2,3\}| = 3, \quad |\{a,b\}| = 2, \quad |\{\{1,2,3\},\{4,5\}\}| = \_\_\_2\_

• If \(|S|\in\mathbb{N}\), then we say \(S\) is finite. Otherwise, we say \(S\) is infinite.

• What are some infinite sets we’ve seen?

\[\mathbb{N}, \mathbb{Z}, \mathbb{R}\]
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 $2^S$.
- Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set *descriptions* that lead to pathological structures that are not *well-defined*.
  - (That do not have self-consistent properties.)
- These “sets” mathematically *cannot* exist.
- *E.g.* let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- *For purposes of this class, don’t worry about it!*

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$. Contrast with sets’ $\{\}$
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, $n$-tuples.
Cartesian Products of Sets

- For sets $A$, $B$, their *Cartesian product* $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.

- *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.

- Extends to $A_1 \times A_2 \times \ldots \times A_n$.

---

René Descartes (1596-1650)
Review of §1.6

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,\ldots\}$, $\{x \mid P(x)\}$...
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

- For sets $A$, $B$, their Union $A \cup B$ is the set containing all elements that are either in $A$, or ("\lor") in $B$ (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.  
- Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
Union Examples

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

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

• For sets $A$, $B$, their *intersection* $A \cap B$ is the set containing all elements that are simultaneously in $A$ and (“$\land$”) in $B$.
• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.
• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset):
  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

- \( \{a,b,c\} \cap \{2,3\} = \varnothing \)
- \( \{2,4,6\} \cap \{3,4,5\} = \{4\} \)

Think “The **intersection** of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- Example: How many students are on our class email list? Consider set \( E \) as students who turned in an information sheet and set \( M \) as students who sent the TAs their email address.

\[ |E \cup M| = |E| + |M| - |E \cap M| \]

Some students did both! Subtract 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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg (x \in A \rightarrow x \in B) \}$$

• Also called:

  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \(\{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} = \{1,4,6\}\)

- \(\mathbb{Z} - \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\}\)
  
  \(= \{x \mid x \text{ is an integer but not a nat. #}\}\)
  
  \(= \{x \mid x \text{ is a negative integer}\}\)
  
  \(= \{\ldots, -3, -2, -1\}\)
Set Difference - Venn Diagram

• $A \setminus B$ 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 $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots\}$
More on Set Complements

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

- **Identity:** $A \cup \emptyset = A = A \cap U$
- **Domination:** $A \cup U = U$, $A \cap \emptyset = \emptyset$
- **Idempotent:** $A \cup A = A = A \cap A$
- **Double complement:** $\overline{(\overline{A})} = A$
- **Commutative:** $A \cup B = B \cup A$, $A \cap B = B \cap A$
- **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 provable from) DeMorgan’s Law for propositions.

\[
\begin{align*}
A \cup B &= \overline{A} \cap \overline{B} \\
A \cap B &= \overline{A} \cup \overline{B}
\end{align*}
\]
Proving Set Identities

To prove statements about sets, of the form

\[ E_1 = E_2 \]  
(where the \( E \)s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \( (A \cup B) \overline{B} = A \overline{B} \).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>( A \cup B )</th>
<th>( (A \cup B) \overline{B} )</th>
<th>( A \overline{B} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

Prove \((A \cup B) \neg C = (A \neg C) \cup (B \neg C)\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) \neg C)</th>
<th>(A \neg C)</th>
<th>(B \neg C)</th>
<th>((A \neg C) \cup (B \neg C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x | P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\bar{S}$.
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets,

\[
X = \{ A \mid P(A) \}.
\]
Generalized Union

• Binary union operator: $A \cup B$

• $n$-ary union:
  \[
  A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n)
  \]
  (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: \( 0 := \emptyset, 1 := \{0\}, 2 := \{0,1\}, 3 := \{0,1,2\}, \ldots \)
  – Bit strings:
    \( 0 := 0, 1 := 1, 2 := 10, 3 := 11, 4 := 100, \ldots \)
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\neg$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• **Sets**
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• **Reading: Sections 1.6-1.7**

• **Upcoming**
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects 
  (*elements*) that we can *describe* (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be *logically inconsistent*!
  
  – This means, there exist naïve set theory propositions *p* such that you can prove that both *p* and *¬p* follow logically from the axioms of the theory!
  
  – ∴: The conjunction of the axioms is a contradiction!
  
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
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, $\{x \mid P(x)\}$ 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 \( \{1, 2, 3, 4\} \) = \( \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} \) = \( \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\} \)
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as 374.1828471929498181917281943125…

• “Blackboard Bold” or double-struck font \( (\mathbb{N}, \mathbb{Z}, \mathbb{R}) \) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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.* \( 3 \in \mathbb{N}, \text{ "a" } \in \{ x \mid x \text{ is a letter of the alphabet} \} \)
  - Can define set equality in terms of \( \in \) relation:
    \[
    \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)
    \]
    "Two sets are equal iff they have all the same members."

- \( x \notin S \iff \neg (x \in S) \) "x is not in S"
The Empty Set

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{ \} = \{ x \mid \text{False} \} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x : x \in \emptyset \).
Subset and Superset Relations

- $S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Note $S = T \iff S \subseteq T \land S \supseteq T$.
- $S \not\subseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$.
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 $1 \neq \{1\} \neq \{\{1\}\}$ !!!!
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 $|S|\in\mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
- What are some infinite sets we’ve seen?

$\mathbb{N} \mathbb{Z} \mathbb{R}$
The *Power Set* Operation

- **The power set** $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written $2^S$.
  
  Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$.
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
• These “sets” mathematically cannot exist.
• *E.g.* let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, $n$-tuples.
Cartesian Products of Sets

- For sets $A$, $B$, their **Cartesian product** $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.
- *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$....

René Descartes  
(1596-1650)
Review of §1.6

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\setminus$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their $\text{Union } A \cup B$ is the set containing all elements that are either in $A$, or ("\lor") in $B$ (or, of course, in both).

• Formally, $\forall A,B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.

• Note that $A \cup B$ is a $\text{superset}$ of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$
Union Examples

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

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset):

  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

Example: How many students are on our class email list? Consider \( M \), \( I \), and \( M \cap I \).

\( M = \{ \text{students who sent TAs their email address} \} \)
\( I = \{ \text{students who turned in an information sheet} \} \)
\( M \cap I = \{ \text{students who did both} \} \)

\[ |M \cup I| = |I| + |M| - |I \cap M| \]
Set Difference

• For sets $A$, $B$, the *difference of $A$ and $B*$, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:

\[
A \setminus B \equiv \{ x \mid x \in A \land x \notin B \} \\
= \{ x \mid \neg (x \in A \rightarrow x \in B) \}
\]

• Also called:
The *complement of $B$ with respect to $A$*. 
Set Difference Examples

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

- \(\mathbb{Z} - \mathbb{N}\) = \{\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 $U$.
- 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 $U \setminus A$.
- *E.g.*, If $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, ... \}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

![Diagram showing the complement of set A within a universal set U]
Set Identities

- Identity: \( A \cup \emptyset = A = A \cap U \)
- Domination: \( A \cup U = U \) , \( A \cap \emptyset = \emptyset \)
- Idempotent: \( A \cup A = A = A \cap A \)
- Double complement: \( \overline{\overline{A}} = A \)
- Commutative: \( A \cup B = B \cup A \) , \( A \cap B = B \cap A \)
- 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 provable from) DeMorgan’s Law for propositions.

\[
A \cup B = \overline{A} \cap \overline{B} \\
A \cap B = \overline{A} \cup \overline{B}
\]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 |
## Membership Table Exercise

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) - C)</th>
<th>(A - C)</th>
<th>(B - C)</th>
<th>((A - C) \cup (B - C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, 
\[ X = \{ A \mid P(A) \}. \]
Generalized Union

- Binary union operator: $A \cup B$
- $n$-ary union:
  $$A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n)$$
  (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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0,1\}$, $3 := \{0,1,2\}$, …
  – Bit strings: $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, …
Representing Sets with Bit Strings

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

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

In this representation, the set operators “∪”, “∩”, “¯” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

• **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).
Naïve set theory

- **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.
- But, the resulting theory turns out to be **logically inconsistent**!
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!
- More sophisticated set theories fix this problem.
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 \textit{if and only if} they contain \textit{exactly the same} elements.
- In particular, it does not matter \textit{how the set is defined or denoted}.
- \textbf{For example:} The set \{1, 2, 3, 4\} = \\
  \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} = \\
  \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  - \( \mathbb{N} = \{0, 1, 2, \ldots \} \) The Natural numbers.
  - \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots \} \) The Integer numbers.
  - \( \mathbb{R} = \) The “Real” numbers, such as 374.1828471929498181917281943125…
- “Blackboard Bold” or double-struck font (\( \mathbb{N, Z, R} \)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "$a" \in \{x \mid x \text{ is a letter of the alphabet}\}
  - Can define set equality in terms of $\in$ relation:
    \[ \forall S,T: S=T \iff (\forall x: x \in S \iff x \in T) \]
    "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

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{\} = \{x | \text{False}\} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x : x \in \emptyset \).
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.
- \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq S \).
- \( S \supseteq T \) ("S is a superset of T") means \( T \subseteq S \).
- Note \( S= T \iff S \subseteq T \land S \supseteq T \).
- \( S \nsubseteq T \) means \( \neg(S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \).
Proper (Strict) Subsets & Supersets

• \( S \subset T \) ("S is a proper subset of T") means that \( S \subseteq T \) but \( T \not\subset S \). Similar for \( S \subsetneq T \).

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 \textit{themselves} be sets.

• \textit{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 \( 1 \not\in \{1\} \not\in \{\{1\}\} \) !!!!
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 \(|S| \in \mathbb{N}\), then we say \(S\) is finite. Otherwise, we say \(S\) is infinite.
- What are some infinite sets we’ve seen?

\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)
The **Power Set** Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$.  
  \[ P(S) \equiv \{ x \mid x \subseteq S \} \].
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$. 
- Sometimes $P(S)$ is written $2^S$. 
  Note that for finite $S$, $|P(S)| = 2^{|S|}$. 
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$. 

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \varnothing$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- *E.g.* let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

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

Contrast with sets’ $\{\}$
Cartesian Products of Sets

• For sets $A$, $B$, their Cartesian product $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.

• 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: i.e., $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

• Sets $S, T, U$… Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their Union $A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).

• Formally, $\forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.

• Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$
Union Examples

• \( \{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\} \)
• \( \{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\} = \{2,3,5,7\} \)

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$.
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

Example: How many students are on our class email list? Consider set \( I \) and set \( M \),
\( I = \{ \text{students who turned in an information sheet} \} \)
\( M = \{ \text{students who sent the TAs their email address} \} \)
Subtract out the overlap:
\[ |I \cup M| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:
  \[
  A - B \equiv \{ x \mid x \in A \land x \notin B \}
  = \{ x \mid \neg(x \in A \rightarrow x \in B) \}
  \]

• Also called:
  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \{1,2,3,4,5,6\} – \{2,3,5,7,9,11\} = \{1,4,6\}
- \mathbb{Z} – \mathbb{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 $A$, Set $B$, $A - B$
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 $U \setminus A$.

• E.g., If $U = \mathbb{N}$, $\{3,5\} = \{0,1,2,4,6,7,...\}$
More on Set Complements

- An equivalent definition, when $U$ is clear:

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

![Diagram showing set $A$ and its complement $\overline{A}$ in the universal set $U$.]
Set Identities

• Identity: \( A \cup \emptyset = A = A \cap U \)
• Domination: \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
• Idempotent: \( A \cup A = A = A \cap A \)
• Double complement: \( \overline{\overline{A}} = A \)
• Commutative: \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
• 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 provable 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 the \( E \)s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# Membership Table Exercise

Prove \((A \cup B)^c = (A^c \cup B^c)\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B)^c)</th>
<th>(A^c)</th>
<th>(B^c)</th>
<th>((A^c \cup B^c))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,\ldots\}$, $\{x \mid P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets \(X = \{A \mid P(A)\}\).
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_1 \cap A_2 \cap \ldots \cap A_n \equiv (((\ldots ((A_1 \cap A_2) \cap \ldots) \cap A_n)) \quad \text{(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**: \(0\equiv \emptyset, \ 1\equiv \{0\}, \ 2\equiv \{0,1\}, \ 3\equiv \{0,1,2\}, \ldots\)
  - **Bit strings**: \(0\equiv 0, \ 1\equiv 1, \ 2\equiv 10, \ 3\equiv 11, \ 4\equiv 100, \ldots\)
Representing Sets with Bit Strings

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

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

In this representation, the set operators “\(\cup\)”, “\(\cap\)”, “\(\overline{\cdot}\)” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

• **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• **More sophisticated set theories fix this problem.**
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 } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as 374.1828471929498181917281943125…
- “Blackboard Bold” or double-struck font (\( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn 1834-1923
Basic Set Relations: Member of

• \( x \in S \) ("x is in S") is the proposition that object \( x \) is an \textit{element} or \textit{member} of set \( S \).
  
  \begin{itemize}
  \item \( e.g. \ 3 \in \mathbb{N}, \ "a" \in \{x \mid x \text{ is a letter of the alphabet}\} \)
  \item Can define set equality in terms of \( \in \) relation: 
  \[ \forall S,T: S= T \iff (\forall x: x \in S \iff x \in T) \]
  "Two sets are equal iff they have all the same members."
  \end{itemize}

• \( x \notin S \equiv \neg(x \in S) \) "x is not in S"
The Empty Set

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{ \} = \{ x | \text{False} \} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x : x \in \emptyset \).
Subset and Superset Relations

• $S \subseteq T$ (“$S$ is a subset of $T$”) means that every element of $S$ is also an element of $T$.

• $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$

• $\emptyset \subseteq S$, $S \subseteq S$.

• $S \supseteq T$ (“$S$ is a superset of $T$”) means $T \subseteq S$.

• Note $S = T \iff S \subseteq T \land S \supseteq T$.

• $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
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:

\[
\{1,2\} \subset \{1,2,3\}
\]
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.

• What are some infinite sets we’ve seen?

$\mathbb{N} \mathbb{Z} \mathbb{R}$
The \textit{Power Set} Operation

- The \textit{power set} $P(S)$ of a set $S$ is the set of all subsets of $S$. \[ P(S) := \{ x \mid x \subseteq S \}. \]
- \textit{E.g.} $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$. 
- Sometimes $P(S)$ is written $2^S$.
  Note that for finite $S$, \[ |P(S)| = 2^{|S|}. \]
- \textit{It turns out} $\forall S: |P(S)| > |S|$, \textit{e.g.} $|P(\mathbb{N})| > |\mathbb{N}|$. \textit{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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \notin$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- E.g. let \( S = \{ x \mid x \notin x \} \). Is \( S \in S \)?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, $n$-tuples.
Cartesian Products of Sets

• For sets \( A, B \), their Cartesian product
\[
A \times B \equiv \{(a, b) \mid a \in A \land b \in B \}.
\]
• 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: i.e., \( \forall A, B: A \times B \neq B \times A \).
• Extends to \( A_1 \times A_2 \times \ldots \times A_n \ldots \)

René Descartes
(1596-1650)
Review of §1.6

• Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

- For sets \( A, B \), their \textit{Union} \( A \cup B \) is the set containing all elements that are either in \( A \), \textit{or} ("\( \lor \)"") in \( B \) (or, of course, in both).
- Formally, \( \forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \} \).
- Note that \( A \cup B \) is a \textit{superset} of both \( A \) and \( B \) (in fact, it is the smallest such superset): \( \forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B) \)
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\}

Think “The **United** States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)

CompSci 102 © Michael Frank
The Intersection Operator

• For sets $A$, $B$, their *intersection* $A \cap B$ is the set containing all elements that are simultaneously in $A$ and (“and”) in $B$.

• Formally, $\forall A,B: A \cap B = \{x \mid x \in A \land x \in B\}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset):
  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The \textbf{intersection} of University Ave. and W 13th St. is just that part of the road surface that lies on \textit{both} streets.”
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 set $A$?
- How many elements are in set $B$?

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

Example: How many students are on our class email list?

- $E = I_1 \cup I_2$, where $I_1$ are students who turned in an information sheet,
  and $I_2$ are students who sent the TAs their email address.

- Some students did both!

$$|E| = |I_1| + |I_2| - |I_1 \cap I_2|$$

In intersection, to count them once, double count them, and subtract items counted twice.
Set Difference

- For sets $A$, $B$, the *difference of $A$ and $B$*, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:
  
  $$
  A \setminus B \equiv \{ x \mid x \in A \land x \notin B \}
  $$
  
  $$
  = \{ x \mid \neg(x \in A \Rightarrow x \in B) \}
  $$

- Also called:
  
  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

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

- \(\mathbb{Z} \setminus \mathbb{N}\) = \{\ldots, -1, 0, 1, 2, \ldots\} \setminus \{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 $U$.

• 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 $U \setminus A$.

• *E.g.*, If $U=\mathbb{N}$, $\{3,5\} = \{0,1,2,4,6,7,\ldots\}$
More on Set Complements

- An equivalent definition, when $U$ is clear:

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

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U, \ A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A, \ A \cap B = B \cap A \)
- **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 provable 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 the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- **Part 1:** 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- **Part 2:** Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B)^\sim - B = A^\sim - B.\)

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>(A \cup B)</th>
<th>((A \cup B)^\sim - B)</th>
<th>(A^\sim - B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

\[
\begin{array}{cccccc}
A & B & C & A \cup B & (A \cup B) - C & A - C & B - C & (A - C) \cup (B - C) \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$ ...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\setminus$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, \(X=\{A \mid P(A)\}\).
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:
  \[ A_1 \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n) \]
  (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.
- \textit{E.g.}, one can represent natural numbers as
  - Sets: $0\equiv\emptyset$, $1\equiv\{0\}$, $2\equiv\{0,1\}$, $3\equiv\{0,1,2\}$, ...
  - Bit strings: $0\equiv0$, $1\equiv1$, $2\equiv10$, $3\equiv11$, $4\equiv100$, ...
Representing Sets with Bit Strings

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

E.g. \( U = \mathbb{N} \), \( S = \{2,3,5,7,11\} \), \( B = 001101010001 \).

In this representation, the set operators “\( \cup \)”, “\( \cap \)”, “\( \overline{\cdot} \)” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• **Sets**
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• **Reading: Sections 1.6-1.7**

• **Upcoming**
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

- **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.
- **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!
- **More sophisticated set theories fix this problem.**
Basic notations for sets

- For sets, we’ll use variables $S, T, U, \ldots$
- 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 \( \{1, 2, 3, 4\} = \{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5\} = \{x \mid x \text{ is a positive integer whose square is } > 0 \text{ and } < 25\} \)
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  - \( \mathbb{N} = \{0, 1, 2, \ldots\} \)  The Natural numbers.
  - \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \)  The Integers.
  - \( \mathbb{R} = \) The “Real” numbers, such as \( 374.1828471929498181917281943125\ldots \)
- “Blackboard Bold” or double-struck font (\( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, “$a$” $\in \{x \mid x$ is a letter of the alphabet$\}$
  – Can define set equality in terms of $\in$ relation: $\forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)$
    “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

• $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
• $\emptyset = \{\} = \{x | \text{False}\}$
• No matter the domain of discourse, we have the axiom $\neg \exists x: x \in \emptyset$. 
Subset and Superset Relations

- \( S \subseteq T \) (“\( S \) is a subset of \( T \)”) means that every element of \( S \) is also an element of \( T \).
- \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq S \).
- \( S \supseteq T \) (“\( S \) is a superset of \( T \)”) means \( T \subseteq S \).
- Note \( S = T \iff S \subseteq T \land S \supseteq T \).
- \( S \nsubseteq T \) means \( \neg(S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \)
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 \( 1 \neq \{1\} \neq \{\{1\}\} \) !!!!
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
- What are some infinite sets we’ve seen? $\mathbb{N} \mathbb{Z} \mathbb{R}$
The *Power Set* Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$.  
  $P(S) :\equiv \{ x \mid x \subseteq S \}$.  
- *E.g.* $P(\{a, b\}) = \{ \emptyset, \{a\}, \{b\}, \{a, b\} \}$.  
- Sometimes $P(S)$ is written $2^S$.  
  Note that for finite $S$,  
  $|P(S)| = 2^{|S|}$.  
- It turns out $\forall S: |P(S)| > |S|$, *e.g.*  
  $|P(\mathbb{N})| > |\mathbb{N}|$.  
  *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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \varnothing$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set *descriptions* that lead to pathological structures that are not *well-defined*.
  - (That do not have self-consistent properties.)
- These “sets” mathematically *cannot* exist.
- *E.g.* let \( S = \{ x \mid x \notin x \} \). Is \( S \in S \)?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

• These are like sets, except that duplicates matter, and the order makes a difference.

• For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.

• Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.

• Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, $n$-tuples.

Contrast with sets’ {}
Cartesian Products of Sets

• For sets $A$, $B$, their *Cartesian product* $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.

• *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: *i.e.*, $\neg \forall A,B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a, b, \ldots\}$, $\{x \mid P(x)\}$...
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\setminus$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their Union $A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).

• Formally, $\forall A, B: A \cup B = \{x \mid x \in A \lor x \in B\}$.

• Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
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\}

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A,B: A \cap B = \{x \mid x \in A \land x \in B\}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$.
Intersection Examples

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

Think “The **intersection** of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
Disjointedness

- Two sets $A$, $B$ are called \textit{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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- How many elements are in \( A \) or \( B \)?

**Example:** How many students are on our class email list? Consider set \( I \) as students who have submitted an information sheet and set \( M \) as students who have sent the TAs their email address.

\[ |I \cup M| = |I| + |M| - |I \cap M| \]

Some students did both! Still!

**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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg(x \in A \rightarrow x \in B) \}$$

• Also called:
The *complement of $B$ with respect to $A$.*
Set Difference Examples

- \( \{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} = \{1,4,6\} \)
- \( \mathbb{Z} - \mathbb{N} = \{…, -1, 0, 1, 2, …\} - \{0, 1, …\} \)
  - \( = \{x \mid x \text{ is an integer but not a nat. \#}\} \)
  - \( = \{x \mid x \text{ is a negative integer}\} \)
  - \( = \{…, -3, -2, -1\} \)
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 \( U \setminus A \).

• E.g., If \( U = \mathbb{N} \), \( \{3,5\} = \{0,1,2,4,6,7,...\} \)
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

• Identity: \( A \cup \emptyset = A = A \cap U \)
• Domination: \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
• Idempotent: \( A \cup A = A = A \cap A \)
• Double complement: \( \overline{\overline{A}} = A \)
• Commutative: \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
• 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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]
\[ A \cap B = \overline{A} \cup \overline{B} \]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
  …
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 \((A \cup B) \overline{\neg B} = A \overline{\neg B}\).

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(A)</td>
<td>(B)</td>
<td>(A \cup B)</td>
<td>((A \cup B) \overline{\neg B})</td>
<td>(A \overline{\neg B})</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>(A \cup B)</td>
<td>((A \cup B) - C)</td>
<td>(A - C)</td>
<td>(B - C)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$…
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, 
  \[X=\{A \mid P(A)\}.
\]
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:
  $A_1 \cap A_2 \cap \ldots \cap A_n \equiv (\ldots ((A_1 \cap A_2) \cap \ldots) \cap A_n)$
  (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: $0 := \emptyset, 1 := \{0\}, 2 := \{0, 1\}, 3 := \{0, 1, 2\}, \ldots$
  – Bit strings:
    $0:=0, 1:=1, 2:=10, 3:=11, 4:=100, \ldots$
Representing Sets with Bit Strings

For an enumerable u.d. $U$ with ordering $x_1, x_2, \ldots$, represent a finite set $S \subseteq U$ as the finite bit string $B=b_1b_2\ldots b_n$ where $\forall i: x_i \in S \iff (i<n \land b_i=1)$.

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\overline{}$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

- **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.
- **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!
- **More sophisticated set theories fix this problem.**
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$
• 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 } x > 0 \text{ and } x < 5\} = \\
\{x \mid x \text{ is a positive integer whose square is } > 0 \text{ and } < 25\}
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{The Natural numbers.} \]
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{The Integers.} \]
  \[ \mathbb{R} = \text{The “Real” numbers, such as 374.1828471929498181917281943125…} \]

• “Blackboard Bold” or double-struck font (\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, “$a$”$ \in \{x \mid x$ is a letter of the alphabet$\}$
  - Can define set equality in terms of $\in$ relation:
    $\forall S,T: S = T \iff (\forall x: x \in S \iff x \in T)$
    “Two sets are equal iff they have all the same members.”
- $x \notin S \iff \neg(x \in S)$ “$x$ is not in $S$”
The Empty Set

- \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{ \} = \{ x | \text{False} \} \)
- No matter the domain of discourse, we have the axiom \( \neg \exists x: x \in \emptyset \).
Subset and Superset Relations

- $S \subseteq T$ (“$S$ is a subset of $T$”) means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- \(\emptyset \subseteq S, S \subseteq S\).
- $S \supseteq T$ (“$S$ is a superset of $T$”) means $T \subseteq S$.
- Note $S=T \iff S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
Proper (Strict) Subsets & Supersets

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

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 \( 1 \neq \{ 1 \} \neq \{ \{ 1 \} \} \) !!!!
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 $|S|\in\mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
- What are some infinite sets we’ve seen? $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
The *Power Set* Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$. Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- *E.g.* let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!

---

Bertrand Russell
1872-1970
Ordered \( n \)-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For \( n \in \mathbb{N} \), an ordered \( n \)-tuple or a sequence or list of length \( n \) is written \((a_1, a_2, \ldots, a_n)\). Its first element is \( a_1 \), etc.
- Note that \((1, 2) \neq (2, 1) \neq (2, 1, 1)\).
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, \ldots, \( n \)-tuples.

Contrast with sets’ \{\}
Cartesian Products of Sets

• For sets $A$, $B$, their Cartesian product $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.

• 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: i.e., $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

• Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

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

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):
  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

• \{a,b,c\} \cap \{2,3\} = \emptyset
• \{2,4,6\} \cap \{3,4,5\} = \{4\}

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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.

Help, I’ve been disjointed!
Inclusion-Exclusion Principle

\[ |S \cup B| = |A| + |B| - |A \cap B| \]

- How many students are on our class email list? Consider set \( I \), \( I = \{ \text{sent the TA information} \} \)
- And set \( M \), \( M = \{ \text{sent the TA their email address} \} \)
- Some students did both!
- \[ |S \cup M| = |I| + |M| - |I \cap M| \]
Set Difference

• For sets $A$, $B$, the *difference of $A$ and $B$*, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:

$$A \setminus B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg (x \in A \rightarrow x \in B) \}$$

• Also called:

The *complement of $B$ with respect to $A$.*
Set Difference Examples

• \{1, 2, 3, 4, 5, 6\} – \{2, 3, 5, 7, 9, 11\} = \{1, 4, 6\}

• \(\mathbb{Z} – \mathbb{N}\) = \{\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

- $A \setminus B$ 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 \( U = \mathbb{N} \), \( \{3,5\} = \{0,1,2,4,6,7,...\} \)
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
- **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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]
\[ A \cap B = \overline{A} \cup \overline{B} \]
To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) \neg B = A \neg B\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) \neg B)</th>
<th>(A \neg B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) - C)</th>
<th>(A - C)</th>
<th>(B - C)</th>
<th>((A - C) \cup (B - C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

• Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• Set notations \{a,b,...\}, \{x|P(x)\}…
• Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
• Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
• Set equality proof techniques:
  – Mutual subsets.
  – Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, \(X=\{A \mid P(A)\}\).
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: $A_1 \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n)$ (grouping & order is irrelevant)
- “Big Arch” notation: $\prod_{i=1}^{n} A_i$
- Or for infinite sets of sets: $\prod_{A \in X} A$
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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, ...
  - Bit strings: $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, ...
Representing Sets with Bit Strings

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

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

In this representation, the set operators “∪”, “∩”, “¬” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

- Sets
  - Indirect, by cases, and direct
  - Rules of logical inference
  - Correct & fallacious proofs

- Reading: Sections 1.6-1.7

- Upcoming
  - Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

- **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

- **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

- **More sophisticated set theories fix this problem.**
Basic notations for sets

- For sets, we’ll use variables \( S, T, U, \ldots \)
- 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 } x>0 \text{ and } x<5 \} =
  \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{The Natural numbers.} \]
  \[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{The Integers.} \]
  \[ \mathbb{R} = \text{The “Real” numbers, such as } 374.1828471929498181917281943125\ldots \]
- “Blackboard Bold” or double-struck font (\(\mathbb{N}, \mathbb{Z}, \mathbb{R}\)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. \( 3 \in \mathbb{N} \), "a" \( \in \{x \mid x \text{ is a letter of the alphabet}\}\)
  - Can define set equality in terms of \( \in \) relation:
    \[ \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T) \]
    "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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x|\text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg \exists x: x \in \emptyset$. 
Subset and Superset Relations

• \( S \subseteq T \) ("S is a subset of T") means that every element of \( S \) is also an element of \( T \).
• \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
• \( \emptyset \subseteq S, \ S \subseteq S \).
• \( S \supseteq T \) ("S is a superset of T") means \( T \subseteq S \).
• Note \( S = T \iff S \subseteq T \land S \supseteq T \).
• \( S \nsubseteq T \) means \( \neg (S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \)
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 $S \subset T$.

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., $|\emptyset|=0$, $|\{1,2,3\}| = 3$, $|\{a,b\}| = 2$, $|\{\{1,2,3\},\{4,5\}\}| = 2$
• If $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
• What are some infinite sets we’ve seen? $\mathbb{N}, \mathbb{Z}, \mathbb{R}$
The **Power Set** Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \coloneqq \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
  Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, *e.g.* $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \notin$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.  
  – (That do not have self-consistent properties.)
• These “sets” mathematically cannot exist.
• E.g. let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!
Ordered \( n \)-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For \( n \in \mathbb{N} \), an ordered \( n \)-tuple or a sequence or list of length \( n \) is written \((a_1, a_2, \ldots, a_n)\). Its first element is \( a_1 \), etc.
- Note that \((1, 2) \neq (2, 1) \neq (2, 1, 1)\).
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, \ldots, \( n \)-tuples.
Cartesian Products of Sets

- For sets $A, B$, their Cartesian product $A \times B := \{(a, b) \mid a \in A \land b \in B\}$.
- 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: i.e., $\neg \forall A B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
Start §1.7: The Union Operator

• For sets $A$, $B$, their $\text{Union} \ A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).

• Formally, $\forall A, B: A \cup B = \{x \mid x \in A \lor x \in B\}$.

• Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$
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\}

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)

CompSci 102 © Michael Frank
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.

• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):
  \[ \forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B) \]
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

Example: How many students are on our class email list? Consider set \( M, I = \{ \text{students who turned in an information sheet} \}, \]
\( M = \{ \text{students who sent the TAs their email address} \}, \]
\( |I \cup M| = |I| + |M| - |I \cap M| \)

Some students did both!
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 $B$. Formally:

$$A – B : \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg (x \in A \rightarrow x \in B) \}$$

• Also called:
The *complement of $B$ with respect to $A$*. 
Set Difference Examples

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

- \mathbb{Z} – \mathbb{N} = \{…, –1, 0, 1, 2, …\} – \{0, 1, …\}
  = \{x \mid x \text{ is an integer but not a nat. #}\}
  = \{x \mid x \text{ is a negative integer}\}
  = \{…, –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 $U = \mathbb{N}$, \[ \{3,5\} = \{0,1,2,4,6,7,\ldots\} \]
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

- **Identity**: \( A \cup \emptyset = A = A \cap U \)
- **Domination**: \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
- **Idempotent**: \( A \cup A = A = A \cap A \)
- **Double complement**: \( \overline{\overline{A}} = A \)
- **Commutative**: \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
- **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 provable 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 the \( E \)s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) - B = A - B\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) - B)</th>
<th>(A - B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

• Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
• Set notations $\{a, b, \ldots\}$, $\{x \mid P(x)\}$…
• Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
• Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
• Set equality proof techniques:
  – Mutual subsets.
  – Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered *sets* of sets, \(X = \{ A \mid P(A) \}\).
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:
  \[ A_1 \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2)\cap\ldots)\cap A_n) \]
  (grouping & order is irrelevant)
- “Big Arch” notation:
  \[
  \prod_{i=1}^{n} A_i
  \]
- Or for infinite sets of sets:
  \[
  \prod_{A \in X} A
  \]
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*: \(0 := \emptyset, 1 := \{0\}, 2 := \{0, 1\}, 3 := \{0, 1, 2\}, \ldots\)
  - *Bit strings*: \(0 := 0, 1 := 1, 2 := 10, 3 := 11, 4 := 100, \ldots\)
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\overline{\cdot}$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

• 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects (*elements*) that we can *describe* (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be *logically inconsistent*!
  – This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  – $\therefore$ The conjunction of the axioms is a contradiction!
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
Basic notations for sets

- For sets, we’ll use variables $S, T, U, \ldots$
- 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 \textit{if and only if} they contain \textit{exactly the same} elements.
- In particular, it does not matter \textit{how the set is defined or denoted}.
- \textbf{For example:} The set \( \{ 1, 2, 3, 4 \} = \{ x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5 \} = \{ x \mid x \text{ is a positive integer whose square is } > 0 \text{ and } < 25 \} \)
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as \(374.1828471929498181917281943125\ldots\)

• “Blackboard Bold” or double-struck font \(\mathbb{N}, \mathbb{Z}, \mathbb{R}\) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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.* \( 3 \in \mathbb{N}, \) "a" \( \in \{x \mid x \text{ is a letter of the alphabet}\} \)
  - Can define set equality in terms of \( \in \) relation:
    \[ \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T) \]
    "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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x | \text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg \exists x : x \in \emptyset$. 
Subset and Superset Relations

- \( S \subseteq T \) ("\( S \) is a subset of \( T \)") means that every element of \( S \) is also an element of \( T \).
- \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq S \).
- \( S \supseteq T \) ("\( S \) is a superset of \( T \)") means \( T \subseteq S \).
- Note \( S = T \iff S \subseteq T \land S \supseteq T \).
- \( S \nsubseteq T \) means \( \neg(S \subseteq T) \), i.e. \( \exists x (x \in S \land x \notin T) \)
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 \( S \subset T \).

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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.
• What are some infinite sets we’ve seen? $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
The Power Set Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
  Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, *e.g.* $|P(\mathbb{N})| > |\mathbb{N}|$.
  *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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \notin$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  – (That do not have self-consistent properties.)
• These “sets” mathematically cannot exist.
• E.g. let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

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

Contrast with sets’ \{\}
Cartesian Products of Sets

• For sets $A$, $B$, their Cartesian product
  $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.

• *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$.

René Descartes (1596-1650)
Review of §1.6

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a, b, \ldots\}$, $\{x \mid P(x)\}$...
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\setminus$. 
Start §1.7: The Union Operator

- For sets $A$, $B$, their **Union** $A \cup B$ is the set containing all elements that are either in $A$, or ("\lor") in $B$ (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.
- Note that $A \cup B$ is a **superset** of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$.
Union Examples

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

Think “The **United** States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)

CompSci 102 © Michael Frank
The Intersection Operator

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

• Formally, \( \forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \} \).

• Note that \( A \cap B \) is a *subset* of both \( A \) and \( B \) (in fact it is the largest such subset):

\[ \forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B) \]
Intersection Examples

• \( \{a, b, c\} \cap \{2, 3\} = \emptyset \)
• \( \{2, 4, 6\} \cap \{3, 4, 5\} = \{4\} \)

Think “The **intersection** of University Ave. and W 13th St. is just that part of the road surface that lies on *both* streets.”
Disjointedness

• Two sets $A$, $B$ are called \textit{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.

Help, I’ve been disjointed!
Inclusion-Exclusion Principle

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- Example: How many students are on our class email list? Consider the sets:
  - \( I = \{ \text{students turned in an information sheet} \} \)
  - \( M = \{ \text{students sent the TAs their email address} \} \)

Some students did both! Now, the total number of students is:

\[ |I \cup M| = |I| + |M| - |I \cap M| \]
Set Difference

• For sets $A$, $B$, the *difference of $A$ and $B$*, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:
  \[ A \setminus B \equiv \{ x \mid x \in A \land x \notin B \} \]
  \[ = \{ x \mid \neg(x \in A \rightarrow x \in B) \} \]

• Also called:
  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

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

- \(\mathbb{Z} – \mathbb{N}\) = \{\ldots, -1, 0, 1, 2, \ldots\} – \{0, 1, \ldots\} = \{x \mid x\ is\ an\ integer\ but\ not\ a\ nat.\ #\} = \{x \mid x\ 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 $A$”

$A$ $B$

Chomp!
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 $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots \}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

- **Identity:** $A \cup \emptyset = A = A \cap U$
- **Domination:** $A \cup U = U$, $A \cap \emptyset = \emptyset$
- **Idempotent:** $A \cup A = A = A \cap A$
- **Double complement:** $(\overline{A}) = A$
- **Commutative:** $A \cup B = B \cup A$, $A \cap B = B \cap A$
- **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 provable 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 the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. ...
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 \((A \cup B) - B = A - B\).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(A \cup B)</th>
<th>((A \cup B) - B)</th>
<th>(A - B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>A \cup B</th>
<th>(A \cup B) - C</th>
<th>A - C</th>
<th>B - C</th>
<th>(A - C) \cup (B - C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S, T, U$… Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$. 
- Set notations $\{a,b,...\}, \{x|P(x)\}$…
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\bar{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, \(X = \{A \mid P(A)\}\).
Generalized Union

- Binary union operator: \( A \cup B \)
- \( n \)-ary union:
  \[ A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n) \]
  (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: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, ...
  - Bit strings: $0 := 0$, $1 := 1$, $2 := 10$, $3 := 11$, $4 := 100$, ...
Representing Sets with Bit Strings

For an enumerable u.d. $U$ with ordering $x_1, x_2, \ldots$, 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 \iff (i < n \land b_i = 1)$. 

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

In this representation, the set operators “∪”, “∩”, “¬” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects \((\text{elements})\) that we can *describe* (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be *logically inconsistent*!
  
  – This means, there exist naïve set theory propositions \(p\) such that you can prove that both \(p\) and \(\neg p\) follow logically from the axioms of the theory!
  
  – \(\therefore\) The conjunction of the axioms is a contradiction!

  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
Basic notations for sets

- For sets, we’ll use variables $S, T, U, \ldots$
- 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 \( \{1, 2, 3, 4\} = \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\} \)
Infinite Sets

- Conceptually, sets may be infinite (i.e., not finite, without end, unending).
- Symbols for some special infinite sets:
  \[ \mathbb{N} = \{0, 1, 2, \ldots \} \] The Natural numbers.
  \[ \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \] The Integers.
  \[ \mathbb{R} = \text{The “Real” numbers, such as } 374.1828471929498181917281943125 \ldots \]
- “Blackboard Bold” or double-struck font (\(\mathbb{N, Z, R}\)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet\}
  – Can define set equality in terms of $\in$ relation:
    $\forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)$
    "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

• $\emptyset$ (“null”, “the empty set”) is the unique set that contains no elements whatsoever.
• $\emptyset = \{ \} = \{ x \mid \text{False} \}$
• No matter the domain of discourse, we have the axiom $\neg \exists x : x \in \emptyset$. 
Subset and Superset Relations

- $S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S, \ S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Note $S = T \iff S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$.
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 \( 1 \neq \{1\} \neq \\{\{1\}\} \)!!!!
Cardinality and Finiteness

• $|S|$ (read “the cardinality of $S$”) is a measure of how many different elements $S$ has.

$E.g., |\emptyset| = 0, \quad |\{1,2,3\}| = 3, \quad |\{a,b\}| = 2, \quad |\{\{1,2,3\},\{4,5\}\}| = 2$

• If $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.

• What are some infinite sets we’ve seen?

$\mathbb{N} \mathbb{Z} \mathbb{R}$
The *Power Set* Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
- Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, *e.g.* $|P(\mathbb{N})| > |\mathbb{N}|$.

*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 $\emptyset$.
• Set relations $=, \subseteq, \supseteq, \subset, \supset, \emptyset$, etc.
• Venn diagrams.
• Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
• Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

• There are some naïve set *descriptions* that lead to pathological structures that are not *well-defined*.
  – (That do not have self-consistent properties.)
• These “sets” mathematically *cannot* exist.
• *E.g.* let $S = \{ x \mid x \notin x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

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

Contrast with sets’ $\{\}$
Cartesian Products of Sets

- For sets $A$, $B$, their *Cartesian product* $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.
- *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: *i.e.*, $\neg \forall A B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...
Review of §1.6

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x\mid P(x)\}$…
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\setminus$. 
Start §1.7: The Union Operator

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

Think “The **United** States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...).
The Intersection Operator

- For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ and ("and") in $B$.
- Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.
- Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset):
  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The \textbf{intersection} of University Ave. and W 13th St. is just that part of the road surface that lies on \textit{both} streets.”
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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

• Example: How many students are on our class email list? Consider set $M$, \[ M = \{ s\text{'s sent the TAs their email address}\} \]

Some students did both!

\[ |I \cup M| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg (x \in A \rightarrow x \in B) \}$$

• Also called:

The *complement of $B$ with respect to $A*$.
Set Difference Examples

• \{1,2,3,4,5,6\} – \{2,3,5,7,9,11\} = \{1,4,6\}

• \(\mathbb{Z} – \mathbb{N}\) = \{… , –1, 0, 1, 2, … \} – \{0, 1, … \} = \{x \mid x \text{ is an integer but not a nat. #}\} = \{x \mid x \text{ is a negative integer}\} = \{… , –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 $U\setminus A$.
- E.g., If $U = \mathbb{N}$, $\{3,5\} = \{0,1,2,4,6,7,\ldots\}$
More on Set Complements

- An equivalent definition, when $U$ is clear:

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

- Identity: \( A \cup \emptyset = A = A \cap U \)
- Domination: \( A \cup U = U \), \( A \cap \emptyset = \emptyset \)
- Idempotent: \( A \cup A = A = A \cap A \)
- Double complement: \( \overline{\overline{A}} = A \)
- Commutative: \( A \cup B = B \cup A \), \( A \cap B = B \cap A \)
- 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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]

\[ A \cap B = \overline{A} \cup \overline{B} \]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- **Part 1:** 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- **Part 2:** Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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.
Prove \((A \cup B)^\complement B = A^\complement B\).
Membership Table Exercise

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

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>(A \cup B)</th>
<th>((A \cup B) - C)</th>
<th>(A - C)</th>
<th>(B - C)</th>
<th>((A - C) \cup (B - C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a, b, \ldots\}$, $\{x \mid P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, \(X=\{A \mid P(A)\}\).
Generalized Union

- Binary union operator: $A \cup B$
- $n$-ary union:
  $\bigcup \bigcup \ldots \bigcup \bigcup \bigcup A_n := \big((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)\big)$
  (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: \(0 := \emptyset, 1 := \{0\}, 2 := \{0,1\}, 3 := \{0,1,2\}, \ldots\)
  - Bit strings: \(0 := 0, 1 := 1, 2 := 10, 3 := 11, 4 := 100, \ldots\)
Representing Sets with Bit Strings

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

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\neg$” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

- **Basic premise:** Any collection or class of objects *(elements)* that we can *describe* (by any means whatsoever) constitutes a set.
- **But, the resulting theory turns out to be logically inconsistent!**
  - This means, there exist naïve set theory propositions \( p \) such that you can prove that both \( p \) and \( \neg p \) follow logically from the axioms of the theory!
  - \( \therefore \) The conjunction of the axioms is a contradiction!
  - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!
- **More sophisticated set theories fix this problem.**
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$

• 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 \( \{1, 2, 3, 4\} = \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\} \).
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as 374.182847192948181917281943125…

• “Blackboard Bold” or double-struck font (\( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet$\}$
  – Can define set equality in terms of $\in$ relation:
    $\forall S,T: S=T \iff (\forall x: x \in S \iff x \in T)$
    “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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x \mid \text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg \exists x : x \in \emptyset$. 
Subset and Superset Relations

- $S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.
- $S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S, S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Note $S = T \iff S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg (S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
Proper (Strict) Subsets & Supersets

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

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 $1 \neq \{1\} \neq \{\{1\}\}$ !!!!
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.

• What are some infinite sets we’ve seen? $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
The *Power Set* Operation

- The *power set* \( P(S) \) of a set \( S \) is the set of all subsets of \( S \).
  \[ P(S) \equiv \{ x \mid x \subseteq S \}. \]
- *E.g.* \( P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \} \).
- Sometimes \( P(S) \) is written \( 2^S \).
  
  Note that for finite \( S \), \( |P(S)| = 2^{|S|} \).
- It turns out \( \forall S: |P(S)| > |S| \), *e.g.* \( |P(\mathbb{N})| > |\mathbb{N}| \).

*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 \( \{x \mid P(x)\} \).
• \( \in \) relational operator, and the empty set \( \emptyset \).
• Set relations =, \( \subseteq, \supseteq, \subset, \supset, \notin \), etc.
• Venn diagrams.
• Cardinality \( |S| \) and infinite sets \( \mathbb{N}, \mathbb{Z}, \mathbb{R} \).
• Power sets \( P(S) \).
Naïve Set Theory is Inconsistent

- There are some naïve set descriptions that lead to pathological structures that are not well-defined. (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- \( E.g. \) let \( S = \{ x \mid x \not\in x \} \). Is \( S \in S \)?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don’t worry about it!
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., $n$-tuples.
Cartesian Products of Sets

• For sets $A$, $B$, their *Cartesian product* $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.

• *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: i.e., $\neg \forall A B: A \times B = B \times A$.

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...

René Descartes (1596-1650)
Review of §1.6

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\setminus$. 
Start §1.7: The Union Operator

• For sets \( A, B \), their **union** \( A \cup B \) is the set containing all elements that are either in \( A \), or (“\( \lor \)”) in \( B \) (or, of course, in both).

• Formally, \( \forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \} \).

• Note that \( A \cup B \) is a **superset** of both \( A \) and \( B \) (in fact, it is the smallest such superset):

\[
\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)
\]
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\}

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)

CompSci 102 © Michael Frank
The Intersection Operator

• For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ and ("\(\land\)") in $B$.
• Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$.
• Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$.
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

- Example: How many students are on our class email list? Consider \( E \), \( M \), \( I \), \( M \)

\[ I = \{ \text{students turned in an information sheet} \} \]
\[ M = \{ \text{students sent the TAs their email address} \} \]

\[ |M| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg (x \in A \rightarrow x \in B) \}$$

• Also called:

  The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \( \{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} = \{1,4,6\} \)

- \( \mathbb{Z} - \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\} = \{x \mid x \text{ is an integer but not a nat. }\} = \{x \mid x \text{ is a negative integer}\} = \{\ldots, -3, -2, -1\} \)
Set Difference - Venn Diagram

- $A - B$ is what’s left after $B$ “takes a bite out of $A$”

Set $A - B$

Set $A$

Set $B$

Chomp!
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 $U=\mathbb{N}$, $\{3,5\} = \{0,1,2,4,6,7,...\}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

$$\overline{A} = \{ x \mid x \not\in A \}$$
Set Identities

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U, \ A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A, \ A \cap B = B \cap A \)
- **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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]

\[ A \cap B = \overline{A} \cup \overline{B} \]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

• Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

• Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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 \((A \cup B) \neg B = A \neg B\).

<table>
<thead>
<tr>
<th>(A)</th>
<th>(B)</th>
<th>(A \cup B)</th>
<th>((A \cup B) \neg B)</th>
<th>(A \neg B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
## Membership Table Exercise

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

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>(A \cup B)</th>
<th>((A \cup B) - C)</th>
<th>(A - C)</th>
<th>(B - C)</th>
<th>((A - C) \cup (B - C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, \(X=\{A \mid P(A)\}\).
Generalized Union

- Binary union operator: \( A \cup B \)
- \( n \)-ary union:
  \[ A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n) \]
  (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: \(0 := \emptyset, 1 := \{0\}, 2 := \{0,1\}, 3 := \{0,1,2\}, \ldots\)
  
  – Bit strings:
    \[0 := 0, 1 := 1, 2 := 10, 3 := 11, 4 := 100, \ldots\]
Representing Sets with Bit Strings

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

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

In this representation, the set operators “∪”, “∩”, “¯” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects (elements) that we can describe (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be *logically inconsistent*!
  – This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  – $\therefore$ The conjunction of the axioms is a contradiction!
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
Basic notations for sets

• For sets, we’ll use variables $S, T, U, \ldots$
• 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 \( \{1, 2, 3, 4\} = \{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} = \{x \mid x \text{ is a positive integer whose square is } x>0 \text{ and } x<25 \} \)
Infinite Sets

- Conceptually, sets may be *infinite* (*i.e.*, not *finite*, without end, unending).
- Symbols for some special infinite sets:
  \[ N = \{0, 1, 2, \ldots\} \quad \text{The Natural numbers.} \]
  \[ Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{The Integers.} \]
  \[ R = \text{The “Real” numbers, such as 374.1828471929498181917281943125…} \]
- “Blackboard Bold” or double-struck font (*N*, *Z*, *R*) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams

John Venn
1834-1923
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. $3 \in \mathbb{N}$, "a" $\in \{x \mid x$ is a letter of the alphabet\}
  - Can define set equality in terms of $\in$ relation: $
    \forall S,T: S = T \iff (\forall x: x \in S \iff 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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{ \} = \{ x | False \}$
- No matter the domain of discourse, we have the axiom $\neg \exists x : x \in \emptyset$. 
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 $S = T \Leftrightarrow S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg(S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
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 $S \subsetneq T$.

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 \( 1 \neq \{1\} \neq \{\{1\}\} \) !!!!
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 $|S|\in\mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.

• What are some infinite sets we’ve seen?

$\mathbb{N} \not\in \mathbb{R}$
The **Power Set** Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written $2^S$.
  - Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, e.g. $|P(\mathbb{N})| > |\mathbb{N}|$.
  - *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 $\emptyset$.
- Set relations $=$, $\subseteq$, $\supseteq$, $\subset$, $\supset$, $\emptyset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$. 
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  – (That do not have self-consistent properties.)

• These “sets” mathematically cannot exist.

• E.g. let $S = \{ x \mid x \notin x \}$. Is $S \in S$?

• Therefore, consistent set theories must restrict the language that can be used to describe sets.

• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an ordered $n$-tuple or a sequence or list of length $n$ is written $(a_1, a_2, \ldots, a_n)$. Its first element is $a_1$, etc.
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., $n$-tuples.
Cartesian Products of Sets

• For sets $A$, $B$, their **Cartesian product**
  \[ A \times B \equiv \{ (a, b) \mid a \in A \land b \in B \} \].

• *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: *i.e.*, \( \neg \forall A B: A \times B = B \times A \).

• Extends to $A_1 \times A_2 \times \ldots \times A_n$...

René Descartes (1596-1650)
Review of §1.6

- Sets $S$, $T$, $U$... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 

CompSci 102 © Michael Frank
Start §1.7: The Union Operator

- For sets $A$, $B$, their **Union** $A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.
- Note that $A \cup B$ is a **superset** of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$. 
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\}

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

- For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ and ("\$\cap\$") in $B$.
- Formally, $\forall A, B: A \cap B = \{ x \mid x \in A \land x \in B \}$. 
- Note that $A \cap B$ is a subset of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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

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

\[ |A \cup B| = |A| + |B| - |A \cap B| \]

Example: How many students are on our class email list? Consider \( E \) = \( I \cup M \), where \( I = \{ s \text{ sent the TAs their email address} \} \) and \( M = \{ s \text{ turned in an information sheet} \} \).

Subtract out \( |I \cap M| \) to compensate for double-counting the students who both sent their email address and turned in their information sheet.

\[ |E| = |I| + |M| - |I \cap M| \]
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 $B$. Formally:

$$A - B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg(x \in A \rightarrow x \in B) \}$$

• Also called:

The *complement of $B$ with respect to $A$*. 
Set Difference Examples

- \{1,2,3,4,5,6\} \setminus \{2,3,5,7,9,11\} = \{1,4,6\}
- \mathbb{Z} \setminus \mathbb{N} = \{-\ldots, -1, 0, 1, 2, \ldots\} \setminus \{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

- \( A \setminus B \) is what’s left after \( B \) “takes a bite out of \( A \)”

\[
\begin{align*}
\text{Set } A & \quad \text{Set } B \\
A \setminus B & \quad \text{Chomp!}
\end{align*}
\]
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 $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots \}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

- Identity: $A \cup \emptyset = A = A \cap U$
- Domination: $A \cup U = U$, $A \cap \emptyset = \emptyset$
- Idempotent: $A \cup A = A = A \cap A$
- Double complement: $(\overline{A}) = A$
- Commutative: $A \cup B = B \cup A$, $A \cap B = B \cap A$
- 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 provable 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 the $E$s 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. …
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.
Prove \((A \cup B) \overline{B} = A \overline{B}\).

<table>
<thead>
<tr>
<th>(A)</th>
<th>(B)</th>
<th>(A \cup B)</th>
<th>((A \cup B) \overline{B})</th>
<th>(A \overline{B})</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# Membership Table Exercise

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

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>A \cup B</td>
<td>(A \cup B) - C</td>
<td>A - C</td>
<td>B - C</td>
<td>(A - C) \cup (B - C)</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0 0 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0 1 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0 1 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1 0 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1 1 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1 1 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Review of §1.6-1.7

- Sets $S, T, U$... Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$...
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S=T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $\neg$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1,\ldots,A_n)\), or even on unordered sets of sets, 

\[ X = \{ A \mid P(A) \} \.]
Generalized Union

- **Binary union operator**: $A \cup B$
- **$n$-ary union**: $A \cup A_2 \cup \ldots \cup A_n \equiv (((A_1 \cup A_2) \cup \ldots) \cup A_n)$ (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: $0:=\emptyset$, $1:=\{0\}$, $2:=\{0,1\}$, $3:=\{0,1,2\}$, ...
  – Bit strings:
    $0:=0$, $1:=1$, $2:=10$, $3:=11$, $4:=100$, ...


CompSci 102 © Michael Frank
Representing Sets with Bit Strings

For an enumerable u.d. $U$ with ordering $x_1, x_2, \ldots$, represent a finite set $S \subseteq U$ as the finite bit string $B=b_1 b_2 \ldots b_n$ where

$$\forall i: x_i \in S \iff (i < n \land b_i = 1).$$

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

In this representation, the set operators “∪”, “∩”, “¬” are implemented directly by bitwise OR, AND, NOT!
Today’s topics

• Sets
  – Indirect, by cases, and direct
  – Rules of logical inference
  – Correct & fallacious proofs

• Reading: Sections 1.6-1.7

• Upcoming
  – Functions
Introduction to Set Theory (§1.6)

- 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).
Naïve set theory

• **Basic premise:** Any collection or class of objects (*elements*) that we can *describe* (by any means whatsoever) constitutes a set.

• But, the resulting theory turns out to be *logically inconsistent*!
  
  – This means, there exist naïve set theory propositions $p$ such that you can prove that both $p$ and $\neg p$ follow logically from the axioms of the theory!
  
  – $\therefore$ The conjunction of the axioms is a contradiction!
  
  – This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!

• More sophisticated set theories fix this problem.
Basic notations for sets

- For sets, we’ll use variables $S, T, U, \ldots$
- 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, $\{x\mid P(x)\}$ 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 \textit{if and only if} they contain \textit{exactly the same} elements.

• In particular, it does not matter \textit{how the set is defined or denoted}.

• \textbf{For example:} The set \{1, 2, 3, 4\} =
\{x \mid x \text{ is an integer where } x>0 \text{ and } x<5 \} =
\{x \mid x \text{ is a positive integer whose square is } >0 \text{ and } <25\}
Infinite Sets

• Conceptually, sets may be infinite (i.e., not finite, without end, unending).

• Symbols for some special infinite sets:
  \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  \( \mathbb{R} = \) The “Real” numbers, such as 374.1828471929498181917281943125…

• “Blackboard Bold” or double-struck font \( (\mathbb{N}, \mathbb{Z}, \mathbb{R}) \) is also often used for these special number sets.

• Infinite sets come in different sizes!

More on this after module #4 (functions).
Venn Diagrams
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. \( 3 \in \mathbb{N} \), "\( a \)" \( \in \{x \mid x \text{ is a letter of the alphabet}\} \)
  - Can define set equality in terms of \( \in \) relation:
    \[
    \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T)
    \]
    "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

- $\emptyset$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\emptyset = \{\} = \{x | \text{False}\}$
- No matter the domain of discourse, we have the axiom $\neg \exists x: x \in \emptyset$. 
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 $S = T \leftrightarrow S \subseteq T \land S \supseteq T$.
- $S \nsubseteq T$ means $\neg(S \subseteq T)$, i.e. $\exists x (x \in S \land x \notin T)$
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 $1 \not= \{1\} \not= \{\{1\}\}$ !!!!
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 $|S| \in \mathbb{N}$, then we say $S$ is finite. Otherwise, we say $S$ is infinite.

• What are some infinite sets we’ve seen? $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
The *Power Set* Operation

- The *power set* $P(S)$ of a set $S$ is the set of all subsets of $S$. $P(S) \equiv \{ x \mid x \subseteq S \}$.
- *E.g.* $P(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$.
- Sometimes $P(S)$ is written $2^S$.
- Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S: |P(S)| > |S|$, *e.g.* $|P(\mathbb{N})| > |\mathbb{N}|$. *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 $\emptyset$.
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \not\in$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $N, Z, R$.
- Power sets $P(S)$.
Naïve Set Theory is Inconsistent

• There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  – (That do not have self-consistent properties.)
• These “sets” mathematically cannot exist.
• E.g. let $S = \{ x \mid x \not\in x \}$. Is $S \in S$?
• Therefore, consistent set theories must restrict the language that can be used to describe sets.
• For purposes of this class, don’t worry about it!

Bertrand Russell
1872-1970
Ordered $n$-tuples

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

Contrast with sets’ {}
Cartesian Products of Sets

- For sets $A, B$, their *Cartesian product* $A \times B \equiv \{(a, b) \mid a \in A \land b \in B\}$.
- *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*: *i.e.*, $\forall A B: A \times B \neq B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n...$
Review of §1.6

• Sets $S, T, U$… Special sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
• 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 up: §1.5: More set ops: $\cup$, $\cap$, $\neg$. 
For sets $A$, $B$, their $\text{Union } A \cup B$ is the set containing all elements that are either in $A$, or (“$\lor$”) in $B$ (or, of course, in both).

Formally, $\forall A, B: A \cup B = \{ x | x \in A \lor x \in B \}$.

Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$
Union Examples

- \( \{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\} \)

- \( \{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\} = \{2,3,5,7\} \)

Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)
The Intersection Operator

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

• Formally, $\forall A, B: A \cap B = \{x \mid x \in A \land x \in B\}$.

• Note that $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset):

  $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$
Intersection Examples

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

Think “The intersection of University Ave. and W 13th St. is just that part of the road surface that lies on both streets.”
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.

Help, I’ve been disjointed!
Inclusion-Exclusion Principle

- Subtract out items in intersection, to compensate for double-counting them!
- Example: How many students are on our class email list? Consider $M$, $I = \{s \in S | s$ turned in an information sheet\}$, $M = \{s \in S | s$ sent the TAs their email address\}$
- Some students did both!
- \[ |I \cup M| = |I| + |M| - |I \cap M| \]
Set Difference

• For sets $A$, $B$, the **difference of $A$ and $B$**, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$. Formally:

$$A \setminus B \equiv \{ x \mid x \in A \land x \notin B \}$$

$$= \{ x \mid \neg(x \in A \rightarrow x \in B) \}$$

• Also called:

  The **complement of $B$ with respect to $A$**.
Set Difference Examples

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

- \mathbb{Z} \setminus \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} \setminus \{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 $U$.
- 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 $U = \mathbb{N}$, $\{3, 5\} = \{0, 1, 2, 4, 6, 7, \ldots \}$
More on Set Complements

• An equivalent definition, when $U$ is clear:

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

- **Identity:** \( A \cup \emptyset = A = A \cap U \)
- **Domination:** \( A \cup U = U \) , \( A \cap \emptyset = \emptyset \)
- **Idempotent:** \( A \cup A = A = A \cap A \)
- **Double complement:** \( \overline{\overline{A}} = A \)
- **Commutative:** \( A \cup B = B \cup A \) , \( A \cap B = B \cap A \)
- ** 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 provable from) DeMorgan’s Law for propositions.

\[ A \cup B = \overline{A} \cap \overline{B} \]

\[ A \cap B = \overline{A} \cup \overline{B} \]
Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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 \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \).

- Part 1: 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, \( A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \).

- Part 2: Show \( (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \). …
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 \((A \cup B)^{-}B = A^{-}B\).

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Membership Table Exercise

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

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(A \cup B\) | \((A \cup B) - C\) | \(A - C\) | \(B - C\) | \((A - C) \cup (B - C)\)
Review of §1.6-1.7

- Sets $S$, $T$, $U$… Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a,b,...\}$, $\{x|P(x)\}$…
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\overline{S}$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.
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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, \(X = \{A \mid P(A)\}\).
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:
  \[ A_1 \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n) \]
  (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: $0:=\emptyset$, $1:=\{0\}$, $2:=\{0,1\}$, $3:=\{0,1,2\}$, …
  – Bit strings: $0:=0$, $1:=1$, $2:=10$, $3:=11$, $4:=100$, …
Representing Sets with Bit Strings

For an enumerable u.d. $U$ with ordering $x_1, x_2, \ldots$, represent a finite set $S \subseteq U$ as the finite bit string $B=b_1b_2\ldots b_n$ where
\[
\forall i: x_i \in S \iff (i < n \land b_i = 1).
\]

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

In this representation, the set operators “$\cup$”, “$\cap$”, “$\neg$” are implemented directly by bitwise OR, AND, NOT!