Sets

Def: *set* - an *unordered collection of elements*

Ex: \{1, 2, 3\} or \{hi, there\}

Venn Diagram:

Def: two sets are *equal* iff they contain the *same* elements

Ex: \{1, 2, 3\} = \{2, 3, 1\}

\{0\} \neq \{1\}

\{3, 5\} = \{3, 5, 3, 3, 5\}
• **Set construction:**
  | or \( \exists \) means “such that”

Ex: \( \{k \mid 0 < k < 4\} \)

\( \{k \mid k \text{ is a perfect square}\} \)

• **Set membership:** \( \in \quad \notin \)

Ex: \( 7 \in \{p \mid p \text{ prime}\} \)

\( q \notin \{0, 2, 4, 6, \ldots\} \)

• **Sets can contain other sets**

Ex: \( \{2, \{5\}\} \)

\( \{\{\{0\}\}\} \neq \{0\} \neq 0 \)

\( S = \{1, 2, 3, \{1\}, \{\{2\}\}\} \)
# Common Sets

<table>
<thead>
<tr>
<th>Set</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naturals:</td>
<td>$\mathbb{N} = {1, 2, 3, 4, \ldots}$</td>
</tr>
<tr>
<td>Integers:</td>
<td>$\mathbb{Z} = {\ldots, -2, -1, 0, 1, 2, \ldots}$</td>
</tr>
<tr>
<td>Rationals:</td>
<td>$\mathbb{Q} = \left{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right}$</td>
</tr>
<tr>
<td>Reals:</td>
<td>$\mathbb{R} = {x \mid x \text{ a real #}}$</td>
</tr>
<tr>
<td>Empty set:</td>
<td>$\emptyset = {}$</td>
</tr>
</tbody>
</table>

$\mathbb{Z}^+ = \text{non-negative integers}$

$\mathbb{R}^- = \text{non-positive reals, etc.}$
Multisets

Def: a *set* w/repeated elements allowed (i.e., each element has “multiplier”)

Ex: \{0, 1, 2, 2, 2, 5, 5\}

For multisets: \{3, 5\} \neq \{3, 5, 3, 3, 5\}

Sequences

Def: ordered list of elements

Ex: (0, 1, 2, 5) “4-tuple”
    (1,2) \neq (2,1) “2-tuple”
Subsets

- **Subset notation:**
  
  $S \subseteq T \iff (x \in S \Rightarrow x \in T)$

- **Proper subset:**
  
  $S \subset T \iff ((S \subseteq T) \land (S \neq T))$
  
  $S = T \iff ((T \subseteq S) \land (S \subseteq T))$
  
  $\forall S \quad \emptyset \subseteq S$
  
  $\forall S \quad S \subseteq S$
• **Union:**

\[ S \cup T = \{ x \mid x \in S \lor x \in T \} \]

• **Intersection:**

\[ S \cap T = \{ x \mid x \in S \land x \in T \} \]
• **Set difference:** $S - T$

$$S - T = \{x \mid x \in S \land x \notin T\}$$

![Venn diagram for set difference](image)

• **Symmetric difference:** $S \oplus T$

$$S \oplus T = \{x \mid x \in S \oplus x \in T\}$$

$$= S \cup T - S \cap T$$

![Venn diagram for symmetric difference](image)
• Universal set:  $U$ (everything)

• Set complement: $S'$ or $\bar{S}$

$$S' = \{x \mid x \notin S\} = U - S$$

• Disjoint sets: $S \cap T = \emptyset$

$$S - T = S \cap T'$$

$S - S = \emptyset$
Examples

\[ \mathbb{N} \cup \mathbb{Z} \cup \mathbb{Q} \cup \mathbb{R} = \mathbb{R} \]

\[ \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \]

\[ \forall x \in \mathbb{R} \quad x \leq x^2+1 \]

\[ \forall x, y \in \mathbb{Q} \quad \min(x, y) = \max(x, y) \iff x = y \]

\[ \mathbb{R}^+ \cup \mathbb{R}^- = \mathbb{R} \]

\[ \mathbb{R}^+ \cap \mathbb{R}^- = \{0\} \]
Set Identities

- **Identity:**
  \[ S \cup \emptyset = S \]
  \[ S \cap U = S \]

- **Domination:**
  \[ S \cup U = U \]
  \[ S \cap \emptyset = \emptyset \]

- **Idempotent:**
  \[ S \cup S = S \]
  \[ S \cap S = S \]

- **Complementation:**
  \[ (S')' = S \]
Set Identities (Cont.)

• **Commutative Law:**
  
  \[ S \cup T = T \cup S \]
  
  \[ S \cap T = T \cap S \]

• **Associative Law:**
  
  \[ S \cup (T \cup V) = (S \cup T) \cup V \]
  
  \[ S \cap (T \cap V) = (S \cap T) \cap V \]
Set Identities (Cont.)

• **Distributive Law:**

\[ S \cup (T \cap V) = (S \cup T) \cap (S \cup V) \]

\[ S \cap (T \cup V) = (S \cap T) \cup (S \cap V) \]

• **Absorption:**

\[ S \cup (S \cap T) = S \]

\[ S \cap (S \cup T) = S \]
DeMorgan's Laws

\[(S \cup T)' = S' \cap T'\]

\[(S \cap T)' = S' \cup T'\]

Boolean logic version:

\[(X \land Y)' = X' \lor Y'\]

\[(X \lor Y)' = X' \land Y'\]
Generalized $\cup$ and $\cap$

\[ \bigcup_{1 \leq i \leq n} S_i = S_1 \cup S_2 \cup S_3 \cup ... \cup S_n \]
\[ = \{ x \mid \exists i \ 1 \leq i \leq n \ \exists x \in S_i \} \]

\[ \bigcap_{1 \leq i \leq n} S_i = S_1 \cap S_2 \cap S_3 \cap ... \cap S_n \]
\[ = \{ x \mid \forall i \ 1 \leq i \leq n \ \Rightarrow x \in S_i \} \]
Set Representation

- \( U = \{x_1, x_2, x_3, x_4, \ldots, x_{n-1}, x_n\} \)

Ex: \( S = \{x_1, x_3, x_n\} \)

bits: \(1 0 1 0 \ldots 0 0 1\)

1010000...01 encodes \( \{x_1, x_3, x_n\} \)
0111000...00 encodes \( \{x_2, x_3, x_4\} \)

- “or” yields union:
  
  \[
  \begin{align*}
  &1010000...01 &\{x_1, x_3, x_n\} \\
  \lor &0111000...00 &\{x_2, x_3, x_4\} \\
  \end{align*}
  \]
  
  \(1111000...01\) \(\{x_1, x_2, x_3, x_4, x_n\}\)

- “and” yields intersection:
  
  \[
  \begin{align*}
  &1010000...01 &\{x_1, x_3, x_n\} \\
  \land &0111000...00 &\{x_2, x_3, x_4\} \\
  \end{align*}
  \]
  
  \(0010000...00\) \(\{x_3\}\)
• **Set closure:** WRT operation $\Delta$
  \[ \forall x, y \in S \implies x \Delta y \in S \]

Ex: $\mathbb{R}$ is closed under addition since $x, y \in \mathbb{R} \implies x + y \in \mathbb{R}$

**Abbreviations**

• **WRT**  "with respect to"

• **WLOG**  "without loss of generality"

"*When ideas fail, words come in very handy.*"  
- Goethe (1749-1832)
Cartesian Product

- **Ordered n-tuple**: element sequence
  
  Ex: \((2,3,5,7)\) is a 4-tuple

- **Tuple equality**:
  
  \[(a,b) = (x,y) \iff (a=x) \land (b=y)\]
  
  Generally: \((a_i) = (x_i) \iff \forall i \ a_i = x_i\)

- **Cross-product**: ordered tuples
  
  \[S \times T = \{(s,t) \mid s \in S, t \in T\}\]

  Ex: \[\{1, 2, 3\} \times \{a,b\} = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}\]

  Generally, \(S \times T \neq T \times S\)
• **Generalized cross-product:**

\[ S_1 \times S_2 \times \ldots \times S_n \]
\[ = \{ (x_1, \ldots, x_n) \mid x_i \in S_i, \ 1 \leq i \leq n \} \]

\[ T^i = T \times T^{i-1} \]
\[ T^1 = T \]

• **Euclidean plane** = \( \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 \)

• **Euclidean space** = \( \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3 \)

• **Russel’s paradox:** set of all sets that do not contain themselves:

\[ \{ S \mid S \notin S \} \]

Q: Does S contain itself??
Functions

- **Function**: mapping $f:S \rightarrow T$

Domain $S$

Range $T$

- **k-ary**: has k “arguments”
- **Predicate**: with range $= \{\text{true, false}\}$
Function Types

- **One-to-one function:** “1-1”
  \[ a, b \in S \land a \neq b \Rightarrow f(a) \neq f(b) \]
  Ex: \( f: \mathbb{R} \rightarrow \mathbb{R}, f(x)=2x \) is 1-1
  \( g(x)=x^2 \) is not 1-1

- **Onto function:**
  \[ \forall t \in T \ \exists s \in S \in f(s)=t \]
  Ex: \( f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x)=13-x \) is onto
  \( g(x)=x^2 \) is not onto
1-to-1 Correspondence

- **1-to-1 correspondence:** \( f: S \leftrightarrow T \)

  \( f \) is both 1-1 and onto

Ex: \( f: \mathbb{R} \leftrightarrow \mathbb{R} \ \ \exists \ f(x)=x \) (identity)

\[ h: \mathbb{N} \leftrightarrow \mathbb{Z} \ \ \exists \ h(x)=\frac{x-1}{2}, \ x \text{ odd}, \]

\[ -\frac{x}{2}, \ x \text{ even}. \]
• **Inverse function:**

\[ f: S \rightarrow T \quad f^{-1}: T \rightarrow S \]

\[ f^{-1}(t) = s \quad \text{if} \quad f(s) = t \]

Ex: \( f(x) = 2x \quad f^{-1}(x) = x/2 \)

• **Function composition:**

\( \beta: S \rightarrow T, \alpha: T \rightarrow V \)

\[ (\alpha \cdot \beta)(x) = \alpha(\beta(x)) \]

\( (\alpha \cdot \beta): S \rightarrow V \)

Ex: \( \beta(x) = x + 1 \quad \alpha(x) = x^2 \)

\( (\alpha \cdot \beta)(x) = x^2 + 2x + 1 \)
Thm: \((f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x\)
Set Cardinality

- **Cardinality**: $|S| = \#\text{elements in } S$

  Ex:  $|\{a,b,c\}| = 3$

  $|\{p \mid p \text{ prime } < 9\}| = 4$

  $|\emptyset| = 0$

  $|\{\{1,2,3,4,5\}\}| = ?$

- **Powerset**: $2^S = \text{set of all subsets}$

  $2^S = \{T \mid T \subseteq S\}$

  Ex: $2^{\{a,b\}} = \{\{\}, \{a\}, \{b\}, \{a,b\}\}$

  Q: What is $2^\emptyset$?
Theorem: \(|2^S|=2^{|S|}\)

Proof:

“Sometimes when reading Goethe, I have the paralyzing suspicion that he is trying to be funny.”
- Guy Davenport
Generalized Cardinality

• S is at least as large as T:
  \[ |S| \geq |T| \implies \exists \ f:S \rightarrow T, \ f \ \text{onto} \]
i.e., “S covers T”

Ex: \( r: \mathbb{R} \rightarrow \mathbb{Z} \), \( r(x) = \text{round}(x) \)

  \[ \implies |\mathbb{R}| \geq |\mathbb{Z}| \]

• S and T have same cardinality:
  \[ |S| = |T| \implies |S| \geq |T| \land |T| \geq |S| \]
or
\[ \exists \ 1-1 \ \text{correspondence} \ S \leftrightarrow T \]

• Generalizes finite cardinality:
  \( \{1, 2, 3, 4, 5\} \geq \{a, b, c\} \)
Infinite Sets

- **Infinite set**: $|S| > k \ \forall k \in \mathbb{Z}$
  or
  $\exists$ 1-1 corres. $f : S \leftrightarrow T, S \subset T$

  Ex: $\{p \mid p \text{ prime}\}$, $\mathbb{R}$

- **Countable set**: $|S| \leq |\mathbb{N}|$

  Ex: $\emptyset, \{p \mid p \text{ prime}\}, \mathbb{N}, \mathbb{Z}$

- **S is strictly smaller than T**: $|S| < |T| \ \Rightarrow \ |S| \leq |T| \ ^\wedge \ |S| \neq |T|$

- **Uncountable set**: $|\mathbb{N}| < |S|$

  Ex: $|\mathbb{N}| < \mathbb{R}$

  $|\mathbb{N}| < [0,1] = \{x \mid x \in \mathbb{R}, 0 \leq x \leq 1\}$
**Thm:** \( \exists 1\text{-}1 \text{ correspondence } \mathbb{Q} \leftrightarrow \mathbb{N} \)

**Pf (dove-tailing):**

<table>
<thead>
<tr>
<th>6</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<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>

| 1 | 2 | 3 | 4 | 5 | 6 |
Thm: $|\mathbb{R}| > |\mathbb{N}|$

Pf (diagonalization):

Assume $\exists$ 1-1 corres. $f: \mathbb{R} \leftrightarrow \mathbb{N}$

Construct $x \in \mathbb{R}$:

\[
f(1) = 2.718281828\ldots \quad \rightarrow \quad 8
\]
\[
f(2) = 1.414213562\ldots \quad \rightarrow \quad 2
\]
\[
f(3) = 1.618033989\ldots \quad \rightarrow \quad 9
\]

$x = 0.829\ldots \neq f(K) \; \forall K \in \mathbb{N}$

$\Rightarrow f$ not a 1-1 correspondence

$\Rightarrow$ contradiction

$\Rightarrow \mathbb{R}$ is uncountable
Q: Is $|2^Z| = |\mathbb{R}|$?
Q: Is $|\mathbb{R}| > |[0,1]|$?
Thm: any set is "smaller" than its powerset.

\[ |S| < |2^S| \]
Infinities

• $|\mathbb{N}| = \aleph_0$

• $|\mathbb{R}| = \aleph_1$

• $\aleph_0 < \aleph_1 = 2^{\aleph_0}$

• “Continuum Hypothesis”

\[ \exists \omega \in \aleph_0 < \omega < \aleph_1 \]

Independent of the axioms! [Cohen, 1966]

• Axiom of choice [Godel 1938]

• Parallel postulate
Infinity Hierarchy

• $\aleph_i < \aleph_{i+1} = 2^{\aleph_i}$

$0, 1, 2, \ldots, k, k+1, \ldots, \aleph_0,$

$\aleph_1, \aleph_2, \ldots, \aleph_k, \aleph_{k+1}, \ldots,$

$\aleph_0, \aleph_1, \ldots, \aleph_k, \aleph_{k+1}, \ldots$

• First inaccessible infinity: $\omega$...

For an informal account on infinities, see e.g.: Rucker, *Infinity and the Mind*, Harvester Press, 1982.
**Thm:** # algorithms is countable.

**Pf:** sort programs by size:

- "main(){}
- "main(){int k; k=7;}
- "<all of UNIX>"
- "<Windows XP>"
- "<intelligent program>"

⇒ # algorithms is countable!
Thm: # of functions is uncountable.
Pf: consider 0/1-valued functions (i.e., functions from $\mathbb{N}$ to $\{0,1\}$):
\[
\{(1,0), (2,1), (3,1), (4,0), (5,1), \ldots\}
\]
\[\Rightarrow \quad \{2, 3, 5, \ldots\} \in 2^\mathbb{N}\]

So, every subset of $\mathbb{N}$ corresponds to a different 0/1-valued function

$|2^\mathbb{N}|$ is uncountable (why?)
\[\Rightarrow \text{# functions is uncountable!}\]
Thm: most functions are uncomputable!

Pf: \# algorithms is countable
    \# functions is \textbf{not} countable

⇒ \exists \textbf{more} functions than
    algorithms / programs!

⇒ some functions \textbf{do not} have
    algorithms!

Ex: The \textbf{halting problem}

Given a program P and input I, does P halt on I?

Def: H(P,I) = 1 if P halts on I
      0 otherwise
The Halting Problem

H: Given a program P and input I, does P halt on I? i.e., does $P(I)\downarrow$?

Thm: H is uncomputable

Pf: Assume subroutine S solves H.

Construct:
Analyze:

\[ S' \]
\[ P \]
\[ I \]
\[ S \]

\[ P(I) \downarrow? \]
\[ \infty \]
\[ yes \]
\[ no \]
\[ yes \]

\[ S'(S') \downarrow \Rightarrow S'(S') \uparrow \]
\[ S'(S') \uparrow \Rightarrow S'(S') \downarrow \]

so, \[ S'(S') \uparrow \iff S'(S') \downarrow \]
a contradiction!

\[ \Rightarrow S \text{ does not correctly compute } H \]

But \( S \) was an arbitrary subroutine, so
\[ \Rightarrow H \text{ is not computable!} \]
Pigeon-Hole Principle

If \( N+1 \) objects are placed into \( N \) boxes \( \implies \exists \) a box with 2 objects.

If \( M \) objects are placed into \( N \) boxes & \( M>N \implies \exists \) box with \( \left\lfloor \frac{M}{N} \right\rfloor \) objects.

- Useful in proofs & analyses
Relations

Relation: a set of “ordered tuples”

Ex: \{(a,1),(b,2), (b,3)\}

“<” \{(x,y) \mid x,y \in \mathbb{Z}, x<y\}

Reflexive: \ x \heartsuit x \ \forall x

Symmetric: \ x \heartsuit y \Rightarrow y \heartsuit x

Transitive: \ x \heartsuit y \wedge y \heartsuit z \Rightarrow x \heartsuit z

Antisymmetric: \ x \heartsuit y \Rightarrow \neg(y \heartsuit x)

Ex: \leq \text{ is reflexive, transitive, not symmetric}
Equivalence Relations

Def: reflexive, symmetric, & transitive

Ex: standard equality “=”

\[ x=x \]
\[ x=y \implies y=x \]
\[ x=y \land y=z \implies x=z \]

Partition - disjoint equivalence classes:
Closures

• **Transitive closure** of ♥: TC
  smallest superset of ♥ satisfying
  \[ x ♥ y \land y ♥ z \Rightarrow x ♥ z \]

  Ex: “predecessor”
  \[ \{(x-1,x) \mid x \in \mathbb{Z}\} \]
  TC(predecessor) is “<” relation

• **Symmetric closure** of ♥:
  smallest superset of ♥ satisfying
  \[ x ♥ y \Rightarrow y ♥ x \]
Graphs

• A special kind of relation

Graphs can model:
• Common relationships
• Communication networks
• Dependency constraints
• Reachability information

+ many more practical applications!

Graph $G=(V,E)$: set of vertices $V$, and a set of edges $E \subseteq V \times V$

Pictorially: nodes & lines
Undirected Graphs

Def: edges have no direction

- Example of undirected graph:

\[ V = \{a, b, c, d, e\} \]
\[ E = \{(c, a), (c, b), (c, d), (c, e), (a, b), (b, d), (d, e)\} \]
Directed Graphs

Def: edges have direction

- Example of directed graph:

```
V={a,b,c,d,e}
E={(a,b),(a,c),(b,c),(b,d),
   (d,c),(d,e),(c,e)}
```
Graph Terminology

Graph $G = (V, E)$, $E \subseteq V \times V$

- node $\equiv$ vertex
- edge $\equiv$ arc

Vertices $u, v \in V$ are **neighbors** in $G$ iff $(u, v)$ or $(v, u)$ is an edge of $G$

Ex: $a$ & $b$ are neighbors
    $a$ & $e$ are **not** neighbors
Undirected Node Degree

Degree in **undirected** graphs:

\[
\text{Degree}(v) = \# \text{ of adjacent (incident) edges to vertex } v \text{ in } G
\]

Ex: \( \text{deg}(c)=4 \) \( \text{deg}(f)=0 \)
Directed Node Degree

Degree in directed graphs:

In-degree($v$) = # of incoming edges
Out-degree($v$) = # of outgoing edges

Ex: in-deg($c$)=3    out-deg($c$)=1
      in-deg($f$)=0    out-deg($f$)=0
Q: Show that at any party there is an even number of people who shook hands an odd number of times.
Complete graph $K_n$ contains all edges i.e., $E = \{\{u,v\} \in V \times V \mid u \neq v\}$

Q: How many edges are there in $K_n$?

Subgraph of $G$ is $G' = (V',E')$ where $V' \subseteq V$ and $E' \subseteq E$

Q: Give a (non-trivial) lower bound on the number of graphs over $n$ vertices.
Paths in Graphs

Undirected path in a graph:

A graph is connected iff there is a path between any pair of nodes:
Directed path in a graph:

Graph is **strongly connected** iff there is a directed path between *any* node pair:

Ex: connected but not **strongly**:
A cycle in a graph:

A tree is an acyclic graph.

Tree $T=(V',E')$ spans $G=(V,E)$ if $T$ is a connected subgraph with $V'=V$
Q: How many edges are there in a tree over n vertices?

Q: Is the # of distinct spanning trees in a graph G always polynomial in |G|?
Graph Traversals

Breadth-first search:

Depth-first search:

O(E+V) time for either BFS or DFS

Yields a spanning tree for the graph
Topological Sort

Given a digraph, list vertices so that all edges point/direct to the right:

Can be done in $O(E+V)$ time

Application: scheduling w/constraints
Weighted Graphs

Each edge has a weight: \( w: E \rightarrow \mathbb{Z} \)

Weights can model many things:

- Distances / lengths
- Speed / time
- Costs

Cost(\( G \)) = sum of edge costs

Find a shortest / least-expensive subgraph with a given property
Adjacency list:

1: (a) → b → c
2: (b) → a → d
3: (c) → a
4: (d) → b

Adjacency matrix:

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>c</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>d</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Discrete Probability

Sample space: set of possible outcomes

Event E: subset of sample space S

Probability p of an event: \(|E| / |S|\)

- \(0 \leq p \leq 1\)

- \(p(\text{not}(E)) = 1 - p(E)\)

- \(p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)\)

Ex: two dice yielding total of 9

\(E = \{(3,6),(4,5),(5,4),(6,3)\}\)

\(S = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}\)

\(p(E) = |E|/|S| = 4/36 = 1/9\)
General Probability

Outcome $x_i$ is assigned probability $p(x_i)$

- $0 \leq p(x_i) \leq 1$
- $\sum p(x_i) = 1$
- $E = \{a_1, a_2, \ldots, a_m\} \rightarrow p(E) = \sum p(a_i)$
- $p(\neg E) = 1 - p(E)$
- $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$

Conditional Probability

$p(E \mid F) = \text{probability of } E \text{ given } F$

$p(E \cap F) = p(F) \cdot p(E \mid F)$
Ex: what is the probability of two siblings being both male, given that one of them is male?

Let \((x,y)\) be the two siblings

Sample space: \(\{(m,m),(m,f),(f,m),(f,f)\}\)

Let \(E = \text{both are male}\)

\[= \{(m,m)\}\]

Let \(F = \text{at least one is male}\)

\[= \{(m,m),(m,f),(f,m)\}\]

\(E \cap F = \{(m,m)\}\)

\[= \text{both are male}\]

\[p(E \cap F) = p(F) \cdot p(E \mid F)\]

\[p(E \mid F) = \frac{p(E \cap F)}{p(F)} = \frac{1/4}{3/4} = 1/3\]