Sets and Relations

Basics of Sets

A set is an unordered collection of "elements".

For example, $\mathbb{Z}$, $\mathbb{R}$, $\varnothing$, and $\{1,2\}$ are sets.

We are given (either implicitly or explicitly) a "universal set" from which elements come.
This is a very non-rigorous definition of a set (which is usually defined far more axiomatically), but it will suffice for our requirements.

We write $x \in S$ if the element x is present in the set S and $x \notin S$ otherwise. Eg. $0.5 \in \mathbb{R}$ and $0.5 \notin \mathbb{Z}$

We write $A \subseteq B$ for sets A and B if for all elements x in A, $x \in B$.

The complement of a set A, denoted A^c or $\bar{A}$, is the set of all elements that are not in A.
The union of sets A and B, denoted $A \cup B$, is the set of all elements present in either A or B.
The intersection of sets A and B, denoted $A \cap B$, is the set of all elements present in both A and B.
Given sets A and B, $A \setminus B$ is the set of all elements present in A and not present in B.

Given a predicate p, we can consider the set of all elements for which it holds, denoted as

$$A = \{x \mid p(x)\} \text{ or } \{x : p(x)\}$$

We can also define a "membership predicate" where $p(x)$ iff $x \in A$.

Sets and predicates are essentially the same thing expressed in two different forms.

So we can redefine the earlier operations by

$$x \in \bar{A} \equiv x \notin A \quad \longrightarrow \text{Unary operator}$$

$$\left.\begin{aligned} x \in A \cup B &\equiv x \in A \vee x \in B \\ x \in A \cap B &\equiv x \in A \wedge x \in B \\ x \in A \setminus B &\equiv x \in A \wedge \neg x \in B \\ &\equiv x \in A \not\to x \in B \\ x \in A \Delta B &\equiv x \in A \oplus x \in B \end{aligned}\right\} \text{Binary operators}$$

$\cup$, $\cap$, and Δ are associative.

Ex. Prove De Morgan's Laws:

$$\overline{S \cup T} = \bar{S} \cap \bar{T}$$

$$\overline{S \cap T} = \bar{S} \cup \bar{T} \quad \text{for sets } S, T.$$

$\cap$ distributes over $\cup$ and $\cup$ distributes over $\cap$.

For sets S, T, $S \subseteq T$ is equivalent to $\forall x \; x \in S \to x \in T$.
$S \supseteq T$ is equivalent to $\forall x \; x \in S \leftarrow x \in T$.
$S = T$ is equivalent to $\forall x \; x \in S \leftrightarrow x \in T$.

Note that $\emptyset \subseteq X$ is vacuously true for any set X.

If $S \subseteq T$ and $T \subseteq R$, then $S \subseteq R$.
(Just a consequence of $(a \to b) \to (b \to c) \equiv a \to c$)

If $S \subseteq T$, then $\bar{T} \subseteq \bar{S}$.
(Just the contrapositive)

To show equality of two sets A and B, we usually show $A \subseteq B$ and $B \subseteq A$.

Recall that we did this when showing

$$\{x : \exists u,v \in \mathbb{Z}\ x = au+bv\} = \{x : \gcd(a,b) \mid x\}$$

We denote the number of elements in a set S by $|S|$.

The Inclusion-Exclusion Principle states that

$$|S \cup T| = |S| + |T| - |S \cap T|.$$

This can be expanded to three sets as

$$|R \cup S \cup T| = |R| + |S| + |T| - |R \cap S| - |S \cap T| - |T \cap R| + |R \cap S \cap T|$$

This can be extended to any (countable) number of sets using induction on the number of sets.

Def. The Cartesian Product of sets S and T is the set

$$S \times T = \{(s,t) : s \in S \text{ and } t \in T)$$

$$(S = \emptyset \vee T = \emptyset) \leftrightarrow S \times T = \emptyset$$

$$|S \times T| = |S| \cdot |T|$$

This can be expanded to three sets as

$$R \times S \times T = \{(r,s,t) : r \in R,\ s \in S,\ t \in T\}$$

This is not exactly the same as $((r,s),t)$ but they are essentially the same; there is a bijection between the two.

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

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

(It also distributes on the other side.)

$$\overline{S \times T} = (\bar{S} \times \bar{T}) \cup (\bar{S} \times T) \cup (S \times \bar{T})$$

Relations

Def. Given sets A and B, a relation is a predicate over $A \times B$.

It is equivalently a subset of $A \times B$.
We restrict ourselves to the case $A = B$, namely homogeneous relations.
We typically write $p(a,b)$ as $a \sqsubset b$, $a \sim b$, $a \leq b$ etc.

A relation can be represented as
→ A subset of $S \times S$

$$= \{(a,b) : a \sqsubset b\}$$

→ A boolean matrix where $M_{a,b} = T$ iff $a \sqsubset b$.
→ A directed graph where $a \to b$ iff $a \sqsubset b$.
(we will study these later)

Since relations are just sets, we can translate all the set operations into relation operations. (The universal set is just $S \times S$ then)
Given a relation R,
→ The transpose of R, denoted R^T is $\{(x,y) : (y,x) \in R\}$.
(or converse)

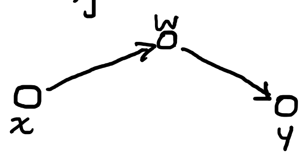
$$(M^T_{x,y} = M_{y,x})$$

→ The composition of R and R' is given by

$$R \circ R' = \{(x,y) : \exists w \in S \ (x,w) \in R \text{ and } (w,y) \in R'\}$$

$$(M \circ M')_{x,y} = \exists w \ (M_{x,y} \wedge M_{w,y})$$

↳ Boolean matrix multiplication
$\vee$ instead of $+$ and
$\wedge$ instead of $\times$.



A relation R is said to be
→ reflexive if $\forall x \ R(x,x)$ holds.
all the diagonal entries in the matrix are true.
all the nodes have self-loops.

→ Irreflexive if $\forall x \; \neg R(x,x)$

all the diagonal entries in the matrix are false.

no nodes have self-loops.

→ Symmetric if $\forall x \forall y \; (R(x,y) \leftrightarrow R(y,x))$

the matrix is symmetric.

there are only self loops and bidirectional edges.

→ Anti-Symmetric if $\forall x \forall y ((x=y) \vee (R(x,y) \rightarrow \neg R(y,x)))$

(equivalent to $\forall x \forall y \; ((R(x,y) \wedge R(y,x)) \rightarrow (x=y))$)

the matrix is anti-symmetric.

there are no bidirectional edges.

Note that the equality relation is both symmetric and anti-symmetric.

→ Transitive if $\forall a \forall b \forall c \; ((R(a,b) \wedge R(b,c)) \rightarrow (R(a,c)))$.

$R \circ R \subseteq R \;\equiv\; \forall k > 1 \, (R^k \subseteq R)$ $\quad (R^k = \overbrace{R \circ R \circ \cdots \circ R}^{k \text{ times}})$

if there is a "path" from a to b in the graph, there is an edge (a,b).

→ Intransitive if it is not transitive.

The complete relation $R = S \times S$ is reflexive, symmetric, and transitive.

Def. Given a relation R, we define its reflexive/symmetric/transitive closure as the minimal relation $R' \supseteq R$ s.t. R' is reflexive/symmetric/transitive.

↳ in the sense that we cannot remove any edges.

Def. A relation R is said to be an equivalence relation if it is reflexive, symmetric, and transitive.

e.g. is a relative, is congruent mod 12

Given a relation, we define the equivalence class of x by

$$Eq(x) = \{y : x \sim y\}$$

Note that

- by reflexivity, every element is in its own equivalence class.
- if $Eq(x) \cap Eq(y) \neq \emptyset$, then $Eq(x) = Eq(y)$.

Proof. Let $z \in Eq(x) \cap Eq(y)$. and arbitrary $a \in Eq(x)$.

We have $y \sim z$, $x \sim z$, and $x \sim a$

$\Rightarrow y \sim z$, $z \sim x$, and $x \sim a$. (by symmetry)

$\Rightarrow$ We have $y \sim a$ (by transitivity)

$\Rightarrow a \in Eq(y) \Rightarrow Eq(x) \subseteq Eq(y)$.

Similarly, $Eq(y) \subseteq Eq(x)$ and the two are equal.

The above two imply that the set of equivalence classes partition the domain.

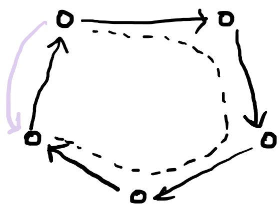
(For $P_1, \dots, P_t \subseteq S$, $\{P_1, \dots, P_t\}$ is said to partition S if $P_1 \cup \dots \cup P_t = S$ and $P_i \cap P_j = \emptyset$ for $i \neq j$.)

These can be visualized as the graph comprising several cliques.

An equivalence relation R is its own symmetric, reflexive, and transitive closure.

We can also think of an acyclic relation wherein it is not possible to follow a sequence of self-loop edges and get back to where you started from.

A transitive anti-symmetric relation is acyclic.
(If it is cyclic, we can go around to the previous edge of the cycle, use transitivity, and get a contradiction to the anti-symmetry.



It is also true that transitive and acyclic relations are anti-symmetric.

Posets

We define an equivalence relation as one that is transitive, reflexive, and symmetric.
If we replace "symmetric" with "anti-symmetric", we get a different type of relation. $\subseteq$ is an example of such a relation.
(on some set of sets)

Def. A relation that is transitive, reflexive, and anti-symmetric is known as a partial order.

If we further replace "reflexive" with "irreflexive", we get a strict partial order. For example, $<$.

Note that we can replace anti-symmetry with acyclicity in both of the above
"Order" refers to the property of being transitive and acyclic.
"Partial" because not every pair of elements is comparable.
(consider $\subseteq$)

Def. A poset (partially ordered set) is a non-empty set with a partial order on it.

A poset is typically denoted as $(S, \leqslant)$

$\subseteq$ is indeed a partial order on any set of sets as for any sets P, Q, R, $P \subseteq P$, $P \subseteq Q \wedge Q \subseteq R \rightarrow P \subseteq R$, and $P \subseteq Q \wedge Q \subseteq P \rightarrow P = Q$.

Another example of a poset is $(\mathbb{Z}^+, |)$

$a | a$

$a|b \wedge b|c \rightarrow a|c$

$a|b \wedge b|a \rightarrow a=b$

Def. Let $(S, \leq)$ be a poset.

(i) $x \in S$ is maximal if $\nexists\, y \in S \setminus \{x\}$ $x \leq y$

(ii) $x \in S$ is minimal if $\nexists\, y \in S \setminus \{x\}$ $y \leq x$

Maximal/minimal elements need not exist or be unique.

consider $(\mathbb{Z}, \leq)$

any prime is a minimal element of $(\mathbb{Z}^+, |)$

Ex. Prove that any finite poset has at least one maximal and minimal element.

Try induction on the cardinality of the set.

Def. Let $(S, \leq)$ be a poset.

(i) $x \in S$ is a greatest element if $\forall y \in S$ $y \leq x$.

(ii) $x \in S$ is a least element if $\forall y \in S$ $x \leq y$.

Greatest/least elements need not exist but if they do, they are unique.

Use anti-symmetry.

Given a partial order $\leq$, we can define its reflexive reduction $<$ by

$a < b$ iff $a \neq b$ and $a \leq b$.

Note that $\leq$ is the reflexive closure of $<$.

A relation $\sqsubseteq$ is a transitive reduction of $\leq$ if

- $\rightarrow$ $\leq$ is the transitive closure of $\sqsubseteq$.
- $\rightarrow \forall a,b \; (a \sqsubseteq b \longrightarrow \nexists m \in S \setminus \{a,b\} \;\; a \leq m \leq b)$

(there is no alternative path from a to b)

It is essentially the graph with the least edges among all graphs with transitive closure $\leq$.

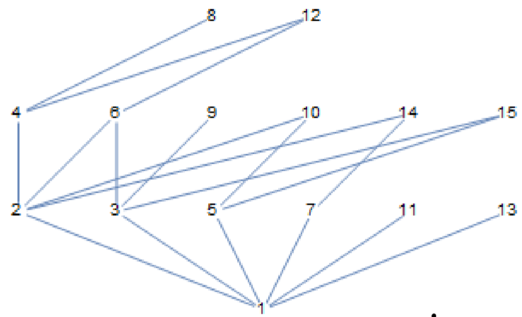
It is not even immediately clear if a transitive reduction of $\leq$ exists in general.

- It is well-defined for finite posets. Define $a \sqsubseteq b$ iff $a \leq b$ and $\nexists m \in S \setminus \{a,b\} \;\; a \leq m \leq b$. Try induction.
- It need not exist for infinite sets — consider $(\mathbb{R}, \leq)$

If the transitive reduction does exist, it is unique.

$(\mathbb{Z}^+, \sqsubset)$ where $a \sqsubset b$ iff b/a is prime or 1 is the transitive reduction of $(\mathbb{Z}^+, |)$.

(just a consequence of the fundamental theorem of arithmetic)



We see that this gives a less cluttered view of the divisibility relation.

The transitive reduction of the reflexive reduction carries all the information of the poset. This gives rise to the idea of a Hasse diagram, which is the graph of this reduction with the arrowheads implicitly taken to point upwards.

If $(S, \leq)$ is a poset and $T \subseteq S$, we can also define a maximal/minimal/greatest/least element of T.

Def. Let $(S, \leq)$ be a poset and $T \subseteq S$. We call $x \in S$ an

1. upper bound of T if $\forall y \in T$, $y \leq x$.
2. lower bound of T if $\forall y \in T$ $x \leq y$.

We further define x to be the least upper bound of T to be the least element of $\{x \in S : x \text{ is an upper bound of } T\}$.

We define x to be the greatest lower bound of T to be the greatest element of $\{x \in S : x \text{ is a lower bound of } T\}$.

Let us go back to the example of $(\mathbb{Z}^+, |)$
For $T = \{a, b\}$, the greatest lower bound of T is their gcd and the least upper bound is their lcm.
How does this generalize to (finite) sets T in $(\mathbb{Z}^+, |)$?

The idea of a "partial" order suggests that there also exists a "total" order.

Def. Let $(S, \leq)$ be a poset. $\leq$ is said to be a total order if for all $a, b \in S$, either $a \leq b$ or $b \leq a$.

(Every pair of elements is comparable)

In this case, the Hasse diagram is just a straight line.
This is a basic property that distinguishes, say, $(\mathbb{N}, \leq)$ from $(\mathbb{N}, |)$.
If S is finite, then there is also a unique maximal/minimal element.

Def. Let $P = (S, \sqsubseteq)$ be a poset. $(S, \leq)$ is said to be an extension of P if $\forall a, b \in S$ $a \sqsubseteq b \rightarrow a \leq b$.

This suggests that we might be able to "build" a total order from any partial order.

(this is called topological sorting)

We can prove by induction on $|S|$ that this is possible for any finite poset.

What about infinite posets? The "Order Extension Principle" is typically taken as an axiom.

(It can be shown that the axiom of choice implies this)

$(\mathbb{N}, \leq)$ is a topological sorting of $(\mathbb{N}, |)$.

Consider $(\mathbb{N}, \sqsubseteq)$ where $a \sqsubseteq b$ iff

→ $a=1$ or

→ a, b both prime or both composite and $a \leq b$.

→ a prime and b composite.

This is a topological sorting of $(\mathbb{N}, |)$.

Chains

Let $(S, \leq)$ be a poset.

Def. $C \subseteq S$ is said to be a chain if $\forall a, b \in C$, either $a \leq b$ or $b \leq a$.

$(C, \leq)$ is then a total order.

Def. $A \subseteq S$ is said to be an anti-chain if $\forall a, b \in A$, neither $a \leq b$ nor $b \leq a$ unless $a = b$.

$(A, \leq)$ is then just $(A, =)$

Note that a subset of any chain/anti-chain is a chain/anti-chain.

a singleton set is both a chain and an anti-chain.

Ex: Show that if C is a chain and A is an anti-chain, $|A \cap C| \leq 1$.

In the Hasse diagram earlier, we saw the elements arranged in "levels".

Def: For any $a \in S$, we define its height by the maximum size of a chain with maximum a.

For finite sets, this is well-defined as the set of chains is finite and non-empty ($\{a\}$ is a chain).

In $(\mathbb{N}, |)$, the height of $m = \underbrace{p_1^{d_1} \cdots p_t^{d_t}}_{\text{prime factorisation}}$ is $1 + \sum_{i=1}^{t} d_i$.

The height of a poset is defined as $\max\{\text{height}(a) : a \in S\}$.
$\max\{|C| : \text{chain } C\}$

Let $A_h = \{a \in S : \text{height}(a) = h\}$
We claim that for all h, A_h is an anti-chain.
(Otherwise, if $a \leq b$ with $\text{height}(a) = h$ and $a \neq b$
show that $\text{height}(b) \geq h+1$)
We can then also define the height of the poset by $\max\{h : A_h \neq \emptyset\}$

Note that the A_h's partition S (for finite S).
It turns out that this is the "minimal" partition of S into anti-chains.

Theo: [Mirsky's Theorem]
The least number of anti-chains needed to partition S is exactly the size of a largest chain.
(For chain $C \subseteq S$, we need at least $|C|$ anti-chains to cover C
as $|C \cap A| \leq 1$ for any anti-chain A.)

The following similar result also holds.

Theo. [Dilworth's Theorem]
The least number of chains needed to partition S is exactly the size of a largest anti-chain.

We shall prove this using Mirsky's theorem later in graph theory.

Functions

Recall that we spoke of predicates as something which assigns a value of $\underbrace{\text{True or False}}$ to each member of the domain.
↳ {True, False} is the co-domain.

More generally, a function with domain A and co-domain B is represented $f: A \to B$.

Every element in A has exactly one value in B that it maps to.

The image of f is the set of values in B that are mapped to.

$$\text{Im}(f) = \{ y \in B : \exists x \in A \ f(x) = y \}$$

We can think of a function as a relation on $A \times B$ such that for all $a \in A$, $|\{(a,x) \in R_f : x \in B\}| = 1$. Every a has a unique b such that $(a,b) \in R_f$.

We can then also represent a function as a matrix.
(usually domain on horizontal axis and co-domain on vertical axis)

When the domain and co-domain are ordered, we can "plot" the function. We only show part of the domain/co-domain when they are infinite.

If $f: A \to B$ and $g: B \to C$, their composition, denoted $g \circ f : A \to C$ is given by $(g \circ f)(a) = (g(f(a))$ for each $a \in A$.
More generally, it is defined only if $f: A \to B$ and $g: C \to D$ such that $\text{Im}(f) \subseteq C$.
Note that $\text{Im}(g \circ f) \subseteq \text{Im}(g)$

Def. Let $f: A \to B$ be a function. f is said to be

$Im(f) = B$ ← • onto/a surjection if for all $b \in B$, $\exists a \in A$ such that $f(a) = b$.
• one-one/an injection if for all $a_1, a_2 \in A$, $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
• a bijection if it is both an injection and a surjection.

Note that given any $f: A \to B$, we can define the onto function $f': A \to Im(f)$ such that for all $x \in A$, $f(x) = f'(x)$

Any strictly increasing/decreasing function is one-one.

A function $f: A \to B$ is said to be invertible if there is a function $g: B \to A$ such that $g \circ f = id_A$

↳ the identity function: $id(a) = a$ for all $a \in A$.

We claim that one-one functions are invertible.

Indeed, given one-one $f: A \to B$, we can define $g: B \to A$ by

for $y \in Im(f)$, $g(y) = x$ such that $f(x) = y$ (this x is unique as f is one-one)

for $y \notin Im(f)$, let $g(y)$ be some arbitrary element in A.

such that $g \circ f = id_A$.

Note that this g need not be invertible.

Similarly, it can further be shown that any invertible function is one-one.

As a bijection is both onto and one-one, every element in the co-domain has a unique preimage.

↳ $a \in A$ such that $f(a) = b$

Therefore, if $f: A \to B$ is a bijection, we can (uniquely) define an $f^{-1}: B \to A$ such that $f^{-1} \circ f = id_A$ and $f \circ f^{-1} = id_B$.

Try proving this!

This implies $(f^{-1})^{-1} = f$.

Suppose $f: A \to B$ where A and B are finite. Then

- $|Im(f)| \leq |A|$ with equality when f is one-one.
- $|Im(f)| \leq |B|$ with equality when f is onto.
- If f is onto, then $|A| \geq |B|$
- If f is one-one, then $|A| \leq |B|$

  The contrapositive of this: "If $|A| > |B|$ then f is not one-one" is the basis of the pigeonhole principle.
- If f is a bijection, then $|A| = |B|$.
- If $|A| = |B|$, then f is onto $\Leftrightarrow$ f is one-one $\Leftrightarrow$ f is a bijection.

Suppose $f: A \to B$ and $g: B \to C$. Then

- $Im(g \circ f) \subseteq Im(g)$
- If f and g are onto, then $g \circ f$ is onto.

  If $g \circ f$ is onto, then g is onto.
- If f and g are one-one, then $g \circ f$ is one-one.

  If $g \circ f$ is one-one, then f is one-one.
- If f and g are bijections, then $g \circ f$ is a bijection.

  If $g \circ f$ is a bijection, then f is one-one and g is onto.

What if we instead have $g: C \to D$ where $C \subseteq B$?

Try proving all of these!