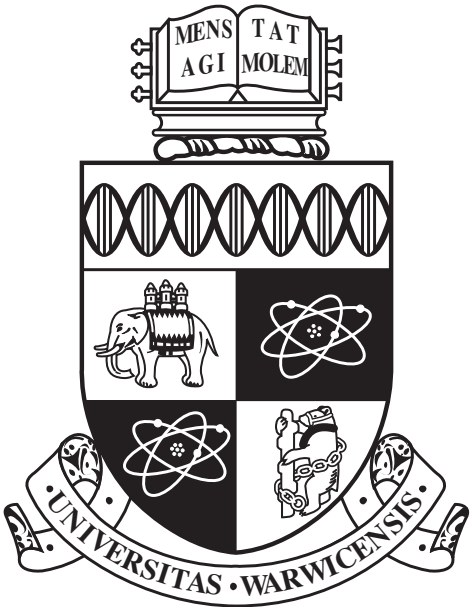
University of Warwick
Department of Computer Science

CS130

Mathematics for Computer Scientists I



Cem Yilmaz
December 22, 2021

Contents

1 Induction

1.1 Inductive definition

Inductive definitions are such that there is an initial case followed by an infinite case. For example: $a_0 = 0$ ad $a_{n+1} = 2a_n + 1$ where $n \in \mathbb{N}$.

1.2 Inductive proof

Inductive proof is used similarly to what an inductive definition would be, it would begin with a first case and then work until infinity.

2 Functions

Definition 2.1. Function Notation

The notation $f : X \to Y$ reads as mapping every element of X to an ambiguous element of the set Y. In other words, f such that X maps to Y. If we consider some number x such that $x \in X$, we can consider the mapping

$$x \mapsto x^2 - 3$$

The set of X and Y in $f : X \to Y$ is called domain and range. However, codomain is defined to be the numbers in range which do exist in set y, but are not necessarily mapped from the set X.
Note: we use the notation $\to$ to denote mapping from set to set and the notation $\mapsto$ when we talk about variables in X.

Definition 2.2. Definition of a function

A function is defined as something that maps *all* elements in X to *an* element in Y.

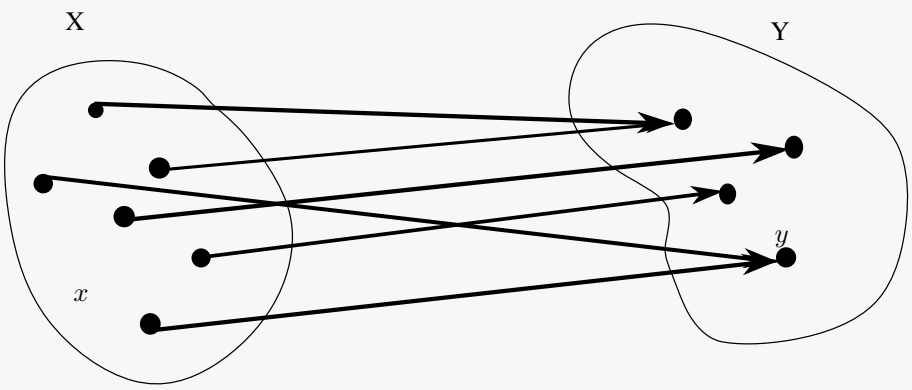


Figure 1: X set mapping to Y set. x maps to y.

Example 2.1. Question 1

Which are functions that are $f : \mathbb{R} \to \mathbb{R}$?

1. $f_1(x) = \frac{1}{x}$
2. $f_2(x) = \sqrt{x}$
3. $f_3(x) = \pm\sqrt{x^2 + 1}$

f_1 is not a function as $f\,(0)$ is undefined. (1)

f_2 is not a function as $x < 0$ is undefined. (2)

f_3 is not a function as when mapping a single x value, it maps into to two values ($\pm\sqrt{a}$) (3)

therefore it is actually $f : \mathbb{R} \to \mathbb{R}^2$. (4)

It is okay that multiple elements in X map into the same element in Y. However, it is not okay if a single X element maps to multiple Y elements.

2.1 Relationship Functions

Definition 2.3. Relation

A relation $R \subseteq X \times Y$ is a function if for every $x \in X$ there is a unique $y \in Y$ such that xRy. If we denote the function by f, then for every $x \in X$, the unique $y \in Y$ s.t. xRy is denoted $f(x)$. In other words, $f(x)$ is the unique y (image) for an x. x is also the pre-image of y.

2.2 Pre-image

Definition 2.4. Pre-image

Let $f : A \to B$ be a map between sets A and B. The the preimage of Y under f is denoted by $f^{-1}(Y)$, and is the set of all elements of A that map to elements in Y under f. Not to confuse with the inverse a function. Note that the complete pre-image of a function is always a set. A more general difference can be seen if we consider elements $a, \alpha \in A$, $a \neq \alpha : a \mapsto y \wedge \alpha \mapsto y$. In this case, the preimage would contain both a and α, but it is not a function. In a function, we would require to either have a or α.

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\} \tag{5}$$

2.3 Failure to be a function

Remember that

1. Every $x \in X$ must be mapped.
2. You cannot have x map into more than one.

2.4 Composition of functions

Recall that $R \subseteq A \times B$ and $Q \subseteq B \times C$, then $R \circ Q$, the composition of two relations.

Theorem 2.1. *Function Composition*

If $f : X \to Y$ and $g : Y \to Z$, the relation $f \circ g \subseteq X \times Z$ and is a function.

2.5 Properties of functions

Definition 2.5. Injectivity

A function $f : X \to Y$ is injective if it is one to one. That is, for every $x \in X$ maps to a unique $y \in Y$.

Definition 2.6. Surjectivity

A function $f : X \to Y$ is surjective if every value for every $y \in Y$, $\exists x \in X$ such that $f(x) = y$. That is, every y is matched.

Definition 2.7. Bijectivity

A function $f : X \to Y$ is bijective if it is both injective and surjective.

Theorem 2.2. *Inverse bijectivity*

A function $f : X \to Y$ is bijective if and only if the inverse relation $f^{-1} \subseteq Y \times X$ is a function.

3 Set Theory

In set builder notation, the set that is described as

$$E = \{2n : n \in \mathbb{Z}\}$$

Is read as, from the brackets "the set of all things of form", whilst the colon describes "such that". Hence, the expression reads as "E equals the set of all things of form 2n, such that n takes on all values in $\mathbb{Z}$., therefore the general rule is the following:

Definition 3.1. Set Builder Notation

General rule for set-builder notation is, for an example set of X,

$$X = \{\text{expression} : \text{rule}\} \tag{6}$$

Similarly, the cardinality of a set is expressed by

$$|X| \tag{7}$$

This counts the number of elements in a set.

3.1 Cardinality of two sets

Definition 3.2. Equinumerosity

Sets A and B are equinumerous if there is a bijection $f : A \to B$. This is denoted as $A \cong B$. In other words, they're isomorphic.

However, how would we define the cardinalities of $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Q}$ etc.? Notice the following:

$$\begin{aligned}
&A \cong A,\ \forall A;\\
&A \cong B \implies B \cong A,\ \forall A, B;\\
&A \cong B, B \cong C \implies A \cong C,\ \forall A, B, C
\end{aligned}$$

Notice that this is in fact an equivalence relation.

Definition 3.3. Countability

Consider the set

$$F_i = \{x \in \mathbb{N} : x < n\}$$

Then,

1. It is labelled "finite" if $S \cong F_i$ for some i;
2. It is labelled "countably infinite: if $S \cong \mathbb{N}$;
3. It is labelled as "countable" if it's finite or countably infinite;
4. It is labelled as "uncountable" if it's not countable.

Example 3.1. Examples

Consider $\mathbb{N}\backslash\{0\} \cong \mathbb{N}$

$$f : \mathbb{N} \to \mathbb{N}\backslash\{0\} \tag{8}$$

For $f(x) = x + 1$, where $x \in \mathbb{N}$. Hence, it is countably infinite.

Consider $E = \{x \in \mathbb{N} :$ x is even $\cong \mathbb{N}$, then

$$f : \mathbb{N} \to E \tag{9}$$

Lastly, $\mathbb{Z} \cong \mathbb{N}$, where $f : \mathbb{N} \to \mathbb{Z}$. Consider

Theorem 3.1. $\mathbb{N}^2 \cong \mathbb{N}$

This is countably infinite.

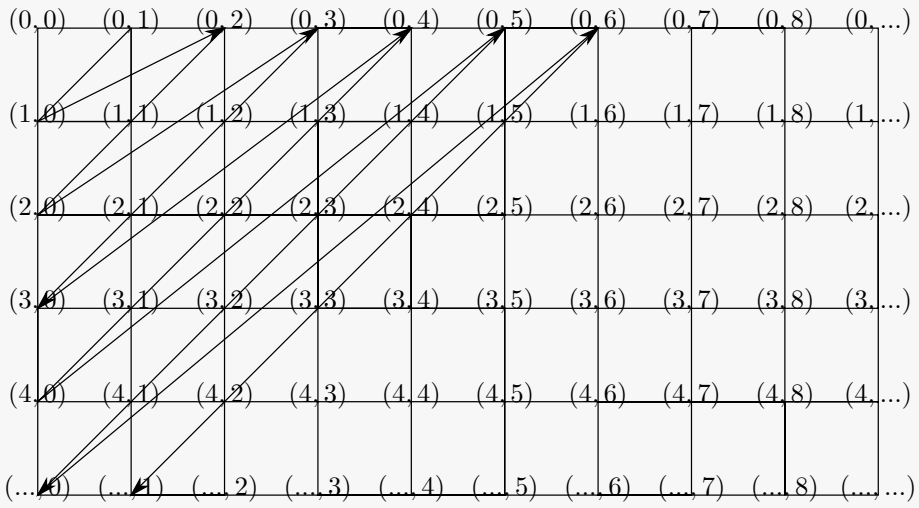


Figure 2: $\mathbb{N}^2$ graph and mapping

Notice that, if we were to pair every $(0, \ldots)$ to $\mathbb{N}$, we would have issue with the fact that the column is infinite. Same logic applies to rows. Therefore, we work diagonally instead as the diagram above

Theorem 3.2. *Powerset Isomorphism*

If S is a set, then $S \ncong 2^S$.

Proof. Assume $\exists f : S \to 2^S$ is a bijection. Let $A = \{x \in S : x \notin f(x)\}$. It follows that $A \subseteq S$ and $A \in 2^S$. And we know, for $A \in 2^S$, $\exists y \in S : f(y) = A$. Consider two cases

1. $y \in A \implies y \notin f(y) = A$. That is, if we know that y is in A, we must have the condition we set for A but get $y \notin f(y) = A$ instead.
2. $y \notin A \implies y \in f(y) = A$. But this is also a contradiction, considering that it is not in y, but still its equal to A.

□

3.2 Cartesian Product

Definition 3.4. Cartesian Product

The cartesian product of two sets A and B is another set, denoted as $A \times B$.

$$A \times B = \{(a, b) : a \in A, b \in B\} \tag{10}$$

Example 3.2. Cartesian Product Example

Consider sets A and B where $A = \{a, b, c\}$ and $B = \{x, y, z\}$, then $A \times B$

$$A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\} \tag{11}$$

In other words, you ensure that the pair of a single element in one of the sets has all possible combinations with other sets. These pair of numbers are called ordered pairs. The cardinality also follows that

$$| A \times B | = | A | \times | B | \tag{12}$$

However, for this to be true, A, B must be finite.

It also an interesting fact that $\mathbb{R}^2$ is $\mathbb{R} \times \mathbb{R}$, which denotes two coordinates (x, y) ! Another thing to note that $\mathbb{R} \times \mathbb{Z} \times \mathbb{N} \neq \mathbb{R} \times (\mathbb{Z} \times \mathbb{N})$ since the former is $\{(x, y, z) : x \in \mathbb{R}, y \in \mathbb{Z}, z \in \mathbb{N}\}$ whereas the latter $\{(x, (y, z)) : x \in \mathbb{R}, (y, z) \in \mathbb{Z} \times \mathbb{N}\}$

3.3 Subsets

Definition 3.5. Subset

For sets A, B, A is a subset of B iff every element in A is also an element of B.

$$A \subseteq B \tag{13}$$

Similarly, it is not a subset iff there is at least 1 element that is not shared.

Definition 3.6. $\varnothing \subseteq A$

For any element A, the empty set is always a subset. By definition 3.5, we know that something is not a subset when there is at least one element of the other subset that is not shared. However, empty set has no elements, and thus it is automatically a subset.

Theorem 3.3. 2^n *Subsets*

If a finite set has n elements, then it has 2^n subsets.

Proof. For every element present, we have 2 selections to go through, add the element or not. Then, for this decision, we can add another choice of selections for the next element. We continue this until we have covered all n elements. □

1. $1 \in \{1,\{1\}\}$ ..... 1 is the first element listed in $\{1,\{1\}\}$
2. $1 \not\subseteq \{1,\{1\}\}$ ..... because 1 is not a set
3. $\{1\} \in \{1,\{1\}\}$ ..... $\{1\}$ is the second element listed in $\{1,\{1\}\}$
4. $\{1\} \subseteq \{1,\{1\}\}$ ..... make subset $\{1\}$ by selecting 1 from $\{1,\{1\}\}$
5. $\{\{1\}\} \notin \{1,\{1\}\}$ ..... because $\{1,\{1\}\}$ contains only 1 and $\{1\}$, and not $\{\{1\}\}$
6. $\{\{1\}\} \subseteq \{1,\{1\}\}$ ..... make subset $\{\{1\}\}$ by selecting $\{1\}$ from $\{1,\{1\}\}$
7. $\mathbb{N} \notin \mathbb{N}$ ..... $\mathbb{N}$ is a set (not a number) and $\mathbb{N}$ contains only numbers
8. $\mathbb{N} \subseteq \mathbb{N}$ ..... because $X \subseteq X$ for every set X
9. $\varnothing \notin \mathbb{N}$ ..... because the set $\mathbb{N}$ contains only numbers and no sets
10. $\varnothing \subseteq \mathbb{N}$ ..... because $\varnothing$ is a subset of every set
11. $\mathbb{N} \in \{\mathbb{N}\}$ ..... because $\{\mathbb{N}\}$ has just one element, the set $\mathbb{N}$
12. $\mathbb{N} \not\subseteq \{\mathbb{N}\}$ ..... because, for instance, $1 \in \mathbb{N}$ but $1 \notin \{\mathbb{N}\}$
13. $\varnothing \notin \{\mathbb{N}\}$ ..... note that the only element of $\{\mathbb{N}\}$ is $\mathbb{N}$, and $\mathbb{N} \neq \varnothing$
14. $\varnothing \subseteq \{\mathbb{N}\}$ ..... because $\varnothing$ is a subset of every set
15. $\varnothing \in \{\varnothing,\mathbb{N}\}$ ..... $\varnothing$ is the first element listed in $\{\varnothing,\mathbb{N}\}$
16. $\varnothing \subseteq \{\varnothing,\mathbb{N}\}$ ..... because $\varnothing$ is a subset of every set
17. $\{\mathbb{N}\} \subseteq \{\varnothing,\mathbb{N}\}$ ..... make subset $\{\mathbb{N}\}$ by selecting $\mathbb{N}$ from $\{\varnothing,\mathbb{N}\}$
18. $\{\mathbb{N}\} \not\subseteq \{\varnothing,\{\mathbb{N}\}\}$ ..... because $\mathbb{N} \notin \{\varnothing,\{\mathbb{N}\}\}$
19. $\{\mathbb{N}\} \in \{\varnothing,\{\mathbb{N}\}\}$ ..... $\{\mathbb{N}\}$ is the second element listed in $\{\varnothing,\{\mathbb{N}\}\}$
20. $\{(1,2),(2,2),(7,1)\} \subseteq \mathbb{N}\times\mathbb{N}$ ..... each of (1,2), (2,2), (7,1) is in $\mathbb{N}\times\mathbb{N}$

Figure 3: Rules of "in" and "subsets"

3.4 Set Operators

$$
\begin{aligned}
A \cup B &= \{x : x \in A \text{ and } x \in B\} \\
A \cap B &= \{x : x \in A \text{ and } x \in B\} \\
A \backslash B &= \{x : x \in A \text{ and } x \notin B\} \\
A \triangle B &= (B \backslash A) \cup (A \backslash B) && = A \cup B \backslash A \cap B \\
\overline{A} &= S \backslash A && \text{Where } A \subseteq S
\end{aligned}
$$

3.5 Power Set

Definition 3.7. Power Set

The power set is defined to be collection of all subsets of some set.

$$\mathbb{P}(\{a\}) = \{\varnothing, \{a\}\} \tag{14}$$

4 Boolean Logic

4.1 Logic of Propositions

Definition 4.1. Atomic Propositions

This propositions consist of simple statements p.

$$p_1, p_2, q \tag{15}$$

Definition 4.2. Compound Propositions

Compound propositions consists of composite of propositions e.g.

$$p \wedge q \tag{16}$$

4.2 Logical Statements

In this section, we will show the logical propositions that are used in computer science. Note that every logical function is of the kind

$$F : B^n \to B$$

where $n \in \mathbb{Z}^+$ and $B \in \{T, F\}$

4.2.1 NOT

A "not" statement (negation) would imply that it is the opposite of something. For example, if we state that statement A is true, then not statement A would be false. It is denoted by the symbol $\neg$. The truth table is as follows:

Table 1: NOT Statement

Value 1	Output
T	F
F	T

4.2.2 AND

An "and" (conjunction) statement states that A and B can only be true when both are true. This is denoted by the symbol $\wedge$. The truth table is as follows:

Table 2: AND Statement

Value 1	Value 2	Output
T	T	T
T	F	F
F	T	F
F	F	F

4.2.3 OR

An "or" statement (disjunction) states that A and B can only provide a true output as long as one of them is true. This symbol is donated by $\vee$. The truth table is as follows:

Table 3: OR Statement

Value 1	Value 2	Output
T	T	T
T	F	T
F	T	T
F	F	F

4.2.4 XOR

A "XOR" (Exclusive OR) states that A and B can only provide a true statement as long as one of them true, excluding the case where both are true. This symbol is donated by $\oplus$. The truth able is as follows:

Table 4: XOR Statement

Value 1	Value 2	Output
T	T	F
T	F	T
F	T	T
F	F	F

4.2.5 Equivalence

An "Equivalence" (Otherwise known as biconditional, iff) states that as long as both A and B have the same binary outputs, then the output is true. It can also be used for more complex logical statements to state that they're the same. This symbol is denoted by $\equiv$ or $\leftrightarrow$. The truth table is as follows:

Table 5: Equivalence Statement

Value 1	Value 2	Output
T	T	T
T	F	F
F	T	F
F	F	T

Notice that this is actually $\neg\left(A \oplus B\right)$.

4.2.6 Material Conditional

A "Material Conditional" states that if A, then B. There are many ways looking at this statement, such as B only if A. What this implies is that if B is true, we know that A must be true. However, if B is false, then we are given no information on A, it could be true or false. This symbol is denoted by $\rightarrow$. The truth table is as follows:

Table 6: Material Conditional Statement

Value 1	Value 2	Output
T	T	T
T	F	F
F	T	T
F	F	T

Notice that $A \rightarrow B = \neg A \vee B$

4.2.7 Necessity

Necessity for two statements P and Q, for the material equivalence relation $P \implies Q$, would read as "Q is necessary for P ". That is, it is necessary that Q is true for P to be true.

4.2.8 Sufficiency

Sufficiency for two statements P and Q, for the material equivalence relation $P \impliedby Q$ would be read as "Q is sufficient for P". That is, because Q being true always implies P being true, but P not being true does not imply Q is not true. Finally, indeed, one could say P is necessary and sufficient for Q, which would give $P \iff Q$.

4.2.9 Associativity

Associativity is defined to be that order does not matter in an equation. In boolean logic, it follows that OR statements and AND statements are associative, that is

$$A \wedge B \wedge C \iff (A \wedge B) \wedge C \iff A \wedge (B \wedge C)$$
$$A \vee B \vee C \iff (A \vee B) \vee C \iff A \vee (B \vee C)$$

4.2.10 Commutativity

Commutativity is defined to show that order does not matter if you switch your variables around.

$$A \wedge B \iff B \wedge A$$
$$A \vee B \iff B \vee A$$

4.2.11 Logical Identities

The following are logical identities:

$x \vee F \equiv x$	Identity	$x \wedge T \equiv x$
$x \vee x \equiv x$	Idempotence	$x \wedge x \equiv x$
$\neg (x \vee y) \equiv \neg x \wedge \neg y$	De Morgan's Laws	$\neg (x \wedge y) \equiv \neg x \vee \neg y$
$x \vee (x \wedge y) \equiv x$	Absorption	$x \wedge (x \vee y) \equiv x$
$x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$	Distributivity	$x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$
$x \vee T \equiv T$	Annihilation	$x \wedge F \equiv F$

There are also identities in which

$$x \wedge (\neg x \vee y) \equiv x \wedge y$$
$$x \vee (\neg x \wedge y) \equiv x \vee y$$

Proof. Proof of absorption and equivalence of the absorptions. We begin with the left equation.

$$\begin{aligned} & x \vee (x \wedge y) \\ =& (x \wedge T) \vee (x \wedge y) \\ =& x \wedge (T \vee y) \\ =& x \wedge T \\ =& x \end{aligned}$$

Now the right equation

$$\begin{aligned} & x \wedge (x \vee y) \\ =& (x \vee F) \wedge (x \vee y) \\ =& x \vee (y \wedge F) \\ =& x \vee F \\ =& x \end{aligned}$$

We show equivalence

$$\begin{aligned} & x \vee (x \wedge y) \\ =& (x \vee x) \wedge (x \vee y) \\ =& x \wedge (x \vee y) \end{aligned}$$

The other way around

$$\begin{aligned} & x \wedge (x \vee y) \\ =& (x \wedge x) \vee (x \wedge y) \\ =& x \vee (x \wedge y) \end{aligned}$$

□

4.2.12 Order of operations

Listed from most important by ascending order.

1. NOT
2. AND
3. OR

4.2.13 Isomorphism

$\langle T, F, \wedge, \vee, \neg \rangle$ is isomorphic to $\langle 1, 0, min, max, \bar{} \rangle$ (See Equinumerosity)

4.3 Different Negations

4.3.1 Converse

This is a special case of the material conditional. $B \to A$ is called the converse of $A \to B$.

4.3.2 Contrapositive

This is also a special case of the material conditional. $\neg B \to \neg A$ is called the contrapositive of $A \to B$. A special property of the contrapositive is that $\neg B \to \neg A$ shares the same truth values as $A \to B$. This is because the statement is false only when $\neg A$ is false and $\neg B$ is true. That is, originally, A must be true and B must be false.

4.3.3 Inverse

Similarly, a special of the material conditional. $\neg A \to \neg B$ is called the inverse of $A \to B$.

4.3.4 English Examples

Example 4.1. English Example

Let us consider the following statement:

If it is my birthday, I get cake

The converse of this statement would be "If I get cake, then it is my birthday".
The contrapositive of this statement would be "If I do not get cake, then it is not my birthday".
The inverse would be "If it is not my birthday, then I do not get cake".
Notice that, only the contrapositive of this statement shares the original truth value. That is, we know that for all birthdays, we get cake, and it is impossible to have an instance that when we do get a cake, it cannot be our birthday (thus false). We are not given any information on when it is not birthday, thus we take all cases when it is not birthday as true.
The contrapositive statement, on the other hand, works similarly. We know that for all days we do not get cake, then it is not our birthday. However, we cannot have an instance where we do not get cake and it is our birthday (false). We are not given information as to when we do get cake, thus we take all such instances as true.

$$\forall Birthday \subseteq Cake \iff Cake' \cap Birthday = \varnothing$$

4.4 Relations

Definition 4.3. Relation

Given sets A, B, a relation between A and B is a subset of $A \times B$

$$R \subseteq A \times B \tag{17}$$

4.4.1 The inverse

Definition 4.4. Inverse of a relation

The inverse of a relation $R \subseteq A \times B$ is the relation $R^{-1} = \{(b, a) \in B \times A$ between B and A $(a, b) \in R\}$

4.4.2 Composition

Definition 4.5. Composition of sets

$$R \circ Q = \{(a, c) \in A \times C \text{ if and only if there is } b \in B \text{ where } (a, b) \in R, (b, c) \in R\} \tag{18}$$

4.4.3 Reflexivity

Definition 4.6. Reflexivity

A relation R on set S is reflexive aRa for every $a \in S$, that is, no matter which a you pick, the pair $(a, a) \in R$.

4.4.4 Connex

Definition 4.7. Connex

A relation R on set S is reflexive $aRb \vee bRa$ for every $a, b \in S$. Note that this by definition also implies reflexivity.

4.4.5 Symmetry

Definition 4.8. Symmetry

A relation R on set S is symmetric $aRb \rightarrow bRa \; \forall a, b \in S$, that is, for all pairs $(a, b) \in R \rightarrow (b, a) \in R$

4.4.6 Antisymmetric

Definition 4.9. Antisymmetric

if aRb and bRa together imply $a = b$ for all a, b.

4.4.7 Transitivity

Definition 4.10. Transitivity

If aRb, bRc together imply aRc.

4.4.8 Equivalence

Definition 4.11. Equivalence

A relation is equivalent if it is reflexive, symmetry and transitive.

4.4.9 Partial Order

Definition 4.12. Partial Order

A relation is partial order if it is reflexive, antisymmetric and transitive.

4.4.10 Total Order

Definition 4.13. Total Order

A total order is a relation that is connex, antisymmetric and transitive.

4.5 Equivalence relations

S, an equivalence relation R on S, for every $a \in S$, denoted by $[a]$ (the equivalence class) with respect to R. That is,

$$[a] = \{x \in S \ : \ aRx\}$$

Example 4.2. Example 1

Consider the relation for $\mathbb{Z}$ such that $\mathbb{Z} \equiv 2\mathrm{mod}$. Then, it follows that

$$[5] = \{5, -5, 3, -3, 1, -1, 7, -7, 9, -9, \ldots\} \tag{19}$$

Creates a set of all numbers that meet this condition. Note that $[5] = [7] = [odd]$

Lemma 4.1. *Equivalence Class representatives*

$\forall b \in [a], [b] = [a]$

Proof.

$$aRb \implies (sym) \implies bRa, a \in [b] \tag{20}$$

(Note that the symmetry comes from the fact that it is equivalent). We show that $[a] \subseteq [b]$: Take $c \in [a]$. aRc and $bRa \implies (trans) \implies bRc$ We do the same argument for $[b] \subseteq [a]$, and therefore $[a] = [b]$ □

Lemma 4.2. *Overlap or Coincision*

$\forall a, b \in S$, either $[a] \cap [b] = \varnothing$ or $[a] = [b]$

Proof. Suppose $\exists c \in [a] \cap [b]$

$$c \in [a] \implies [a] = [c] \text{ by previous lemma} c \in [b] \implies [b] = [c] \tag{21}$$

Therefore, this c does exist, or it does not. □

Definition 4.14. Partitioning

Sets $(A_i)_{i \in I}$ forms a partition if $\forall i, j \in I$ and $i \neq j$

$$\bigcup_{i \in I} A_i \text{ and } A_i \cap A_j = \varnothing \tag{22}$$

Theorem 4.3. *Partitions of a set and disjoints*

Every equivalence relation R on S partitions S into disjoint equivalence classes.

Proof.

$$\frac{S}{r} = \{[a]_R \ : \ a \in S\} \tag{23}$$

Is the quotient of S with respect to R

$$\bigcup_{A \in \frac{S}{r}} \subseteq S \tag{24}$$

From the second lemma we know that they're all disjoint, but we need to show that their union is indeed equal to the set:

$$\forall x \in S, x \in [x] \in \frac{S}{r} \tag{25}$$

$$\implies \bigcup_{A \in \frac{S}{r}} = S \tag{26}$$

□

5 Predicates and Quantifiers

5.1 Predicates

A predicate is defined to be a statement with a variable that refers to an object. For example,
$p_1(u)$, $u > 2$ and $u < 17$, $u \in \mathbb{Z}$.
Predicates can be true or false but not both.

5.2 Quantifiers

You can place quantifiers before predicates. E.g.

$$\text{Quantifiers} \begin{cases} \exists u, \text{there exists} \\ \forall u, \text{for all} \end{cases}$$

Example 5.1. Example 1

Is the statement $\forall u \exists v : |u - v| = 1$ true?
It is asking whether for all u, there exists a v that will make the relation $|u - v| = 1$ true.
Certainly, we can just pick $v = u + 1$

Example 5.2. Exampel 2

Is the statement $\exists u \forall u \ \ |u - v| = 1$ true?
This is asking whether there exists an integer u such that it is a distance of 1 from all integers in u.
This is certainly false.

5.3 Game Interpretation

We assume the $\exists$ is a player called Izzy which wants to make statements true. $\forall$ is a player called Al who wants to make the statements false.
Izzy, to win, looks to find just a singular example in a statement by picking a value for a variable. Al, on the other hand, tries to pick a value of variable to make the statement false.

Example 5.3. Example 1

Let the predicate $S(x, y)$, be the statement $x < y$. Then, for the statement

$$\forall x \exists y S(x, y) \tag{27}$$

We read from left to write. First, Al must be a number. For the sake of the example, he picks 19. Then, Izzy picks a number to make the statement true. She picks 20. Al cannot win because Izzy picks that number.

Example 5.4. Example 2

Continuing with predicate from example 1, the statement

$$\exists y \forall x S(x, y) \tag{28}$$

Izzy picks a number. Let us call it 17. Al then picks 19. Izzy cannot find a number that will make this true because Al can just pick a number that is 1 bigger.

5.4 Quantification over finite sets

for some set $A \in \{1, 2, 3, 4, \ldots, n\}$, the statement

$$\forall x \in A \; . \; P(x) \equiv \bigwedge_{k=1}^{n} P(x)$$

As all of them must be true. Furthermore,

$$\exists x \in A \; . \; P(x) \equiv \bigvee_{k=1}^{n} P(x)$$

Example 5.5. Example 1

For some $S = \{1, 2, 3, 4, \ldots, n\}$, express $\forall x \in S$ and $\exists y \in S \; . \; f(x, y)$ in ands and ors.

$$= (\exists y f(1, y)) \wedge (\exists y f(2, y)) \wedge (\exists y f(3, y)) \wedge \cdots \tag{29}$$

$$= (f(1,1) \vee f(1,2) \vee f(1,3) \vee \cdots) \wedge (f(1,2) \vee (f(2,2) \vee f(3,2) \vee \cdots) \wedge \cdots \tag{30}$$

$$= \bigwedge_{x=1}^{n} \bigvee_{y=1}^{n} f(x, y) \tag{31}$$

5.5 Working with Quantifiers

5.5.1 De Morgan's Laws of Quantifiers

It follows that

$$\neg(\forall x \; . \; P(x)) \equiv \exists x \; . \; \neg P(x)$$

That is, we know we can make the statement $\forall x \; . \; P(x)$ false by picking just 1 value of x that shows that this statement is false. The negation of this, would be that if we pick the same x to $P(x)$ we would obtain true. In other words, just need to one find one x that will make the statement false negated to true. Similarly,

$$\neg(\exists x \; . \; P(x)) \equiv \forall x \; . \; \neg P(x)$$

Using similar logic, we can argue that the statement $\exists x \; . \; P(x)$ will be false only when we cannot pick an x. If this is negated and becomes true, we can say that for all x, the statement $P(x)$ is false.
Note that when using negation, it swaps between $\exists$ and $\forall$, and the negation is transferred to the predicate.

5.5.2 Distribution of $\forall$ and $\exists$

$$\begin{aligned}
\forall x(P(x) \land Q(x)) &\equiv (\forall x.P(x)) \land (\forall x.Q(x) \\
\exists(P(x) \land Q(x)) &\implies (\exists x.P(x)) \land (\exists x.Q(x)) \\
\forall x(P(x) \lor Q(x)) &\impliedby (\forall x.P(x)) \lor (\forall x.Q(x)) \\
\exists x(P(x) \lor Q(x)) &\equiv (\exists x.P(x)) \lor (\exists x.Q(x))
\end{aligned}$$

Note that the converse for the second statement does not work, as you can pick separate x values for Q and P. Similarly, for the third statement, the converse does not work. One example is that all integers are even or odd, but not all integers are even nor all integers are odd.

5.6 Uniqueness

Uniqueness is denoted by $\exists!$

6 Proofs

6.1 Direct Proofs

Direct proofs are proofs that are shown by algebra. Direct proofs want to show implications of the form $P \implies Q$.

6.2 Cases in Proofs

You can also use cases in proves. However, these cases should take all possible domains of the input, and furthermore, must cover all possible cases in the domain.

6.3 Proof by Contrapositive

This proof assumes you taking the negation of the right side of the if statement. For example, $A \implies B$, assume $\neg B \implies \neg A$.

6.4 Proof by Contradiction

Contradiction works by taking the statement $A \implies B$ and then showing that $A \implies$ is false. We know that $\neg B \implies F$ is true only when $\neg B$ is false. Therefore B is true.

6.5 Nonconstructive Proof

Example 6.1. Example 1

Statement: $\exists x, y \in \mathbb{R}\backslash\mathbb{Q} : x^y \in \mathbb{Q}$

Proof. Consider $a = \sqrt{2}^{\sqrt{2}}$ and consider $b = \sqrt{2}$. It follows that $a^b = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = 2$
If $a, b \in \mathbb{R}\backslash\mathbb{Q}$, then $x = a, y = b$.
If $a \in \mathbb{Q}$, then $x = \sqrt{2}, y = \sqrt{2}$ □

The trick to this proof is by considering both cases when something is rational or irrational, both lead to a rational answer.

7 Graph Theory

A graph is an ordered pair $G = (V, E)$ where V is the set of vertices and E is the set of edges. An edge, on the other hand, can also be seen as an ordered pair of vertices.

7.1 Directed and Undirected

It is possible that edges in a graph have directions, that is, in a directed edge, it follows that $(u, v) \neq (v, u)$. However, in an undirected graph, it follows the equality $(u, v) = (v, u)$. Unordered pairs are sometimes denoted as $\{u, v\}$.

7.2 Terminology

7.2.1 Graph Properties

Definition 7.1. Symmetry

A graph is undirected if it is symmetric. That is, $(u, v) \implies (v, u)$. On the other hand, a directed graph does not have the symmetric property.

Definition 7.2. Reflexive

Recall that reflexive is $(u, u) \in E$ where $\forall u \in V$. Irreflexive holds the fact that $(u, u) \in E \forall u \in V$. This tells us whether there are loops.

Definition 7.3. Parallel

Edges are parallel if and only if the ordered pairs are the same. In a directed graph, they begin and end with the same vertices and point to the same direction. In an undirected graph, they're parallel if they begin and end in the same vertices.

Definition 7.4. Simple Graph

A graph is simple if it is symmetric, unparallel and contains no loops.

Definition 7.5. Incident

An edge is incident to a vertex if it is connected to it. In other words, if an edge e connects 2 vertices u and v, then e is incident to v and e is incident to u. It is also possible to call u, v endpoints of edge e.

Definition 7.6. Degree

Degree of a vertex is the number of edges that is incident to v. Notice that loops count as twice in an undirected graph. Usually denoted as $deg(v)$. In directed graphs, we also denote $deg_{out}(v)$ and $deg_{in}(v)$.

Definition 7.7. Bipartite Graph

A graph $G = (V, E)$ is bipartite if $V = V_1 \cup V_2$ such that every $e \in E$ connects some vertex from V_1 with a vertex from V_2, and these vertices are of partitioned vertex sets do not have an edge to connect themselves. Another way to check if a graph is bipartite by considering colouring of graphs. That is, let set C of colours be mapping s.t. $F : V \to C$ that is where $\exists (u, v) \in E$ then $f(u) \neq f(v)$.

7.2.2 Special cases of Walks

Definition 7.8. Loop

An edge is a loop if it begins from a vertex and connects to the same vertex

$$(u, u), u \in V \tag{32}$$

Definition 7.9. Walk

A sequence of edges on a graph $G = (V, E)$ is a sequence of alternating vertex and then edges. E.g. A sequence of edges is also sufficient if edges don't need to be specified.

Definition 7.10. Path

A walk is a path if it does not repeat any vertex.

Definition 7.11. Trail

A walk is a trail if it does not repeat any edges.

Definition 7.12. Tour

A walk is a tour if $v_0 = v_n$, that is, it ends in the same vertex it began.

Definition 7.13. Cycle

A cycle is when a graph is a tour and a path.

Definition 7.14. Simple Cycle

A walk is a simpel cycle when a graph is a tour and a simple path, that is, it ends where it began and it does not repeat a vertex except the last.

Definition 7.15. Simple Path

A walk is simple path if it does not repeat any vertices.

Definition 7.16. Reachability

Two vertices of a graph $G = (V, E)$ where $u, v \in V$ is called "reachable" or accessible if there exists a walk from u to v.

7.3 Connectivity

Definition 7.17. Connectedness

An undirected graph $G = (V, E)$ is "connected" if and only if $\forall u, v \in V$, there exists a walk from u to v. Two vertices $u, v \in V$ are said to be connected if $\exists e \in E : e = (u, v) \vee (v, u)$. Otherwise, it is called disconnected.

Definition 7.18. Strongly connected

A directed graph $G = (V, E)$ is "strongly connected" if and only if $\forall u, v$ which is reachable, there exists a walk from u to v and from v to u.

Definition 7.19. Weakly connected

A directed graph $G = (V, E)$ is weakly connected if replacing all undirecting all edges leads to a connected graph.

Definition 7.20. Semi connectedness

A directed graph $G = (V, E)$ is semi connected if $\forall u, v \in V$ there is a walk from u to v.

7.4 Isomorphism

Graphs are isomorphic for graphs $G_1 = (V_1, E_1), G_2(V_2, E_2)$ if and only if $f : V_1 \to V_2$ is a bijective function s.t. for all $u, v \in V_1$, $(u, v) \in E_1$ iff $(f(u), f(v)) \in E_2$.

7.5 Theorems

Theorem 7.1. *Handshaking Theorem*

For some undirected graph $G = (V, E)$

$$\sum_{v \in V} deg(v) = 2|E| \tag{33}$$

Proof. LHS is the number of endpoints of edges.
RHS is the number of edges.
Thus, this holds because every edge has 2 endpoints. □

7.6 Eulerian and Hamiltonian Cycles

7.6.1 Eulerian Cycles

Definition 7.21. Eulerian Cycle

A cycle in $G = (V, E)$ is Eulerian if $\forall e \in E$ appears only exactly once.

Theorem 7.2. *Existence of an Eulerian Cycle*

An undirected graph $G = (V, E)$ has an Eulerian Cycle if and only if it is connected and every vertex $v \in V$, $deg(v) = 2n$ for some $n \in \mathbb{Z}^+$.

Proof. We first proof the necessity. That is, $\implies$. Consider connected graph $G = (V, E)$. Let $C : v_0 \to v_1 \to v_2 \to v_m$ be an Eulerian cycle, $v_0 = v_m$. Now, if we consider $\forall u, v \in V$. They occur in the cycle C because they are not isolated. Then indeed, $T : u \to v$, as such it is connected. Then, if a vertex v appears k times in the cycle C, then $deg(v) = 2k$, as it must enter and then leave from connectivity. The only exception is that there are loops, however, loops also add 2 edges to a degree v, therefore, it makes no change. □

Proof. We now proof sufficiency, that is, $\impliedby$. Induction on $|E|$.
Consider the base case, $|E| = 0$. Since V is not empty, that means $v \in V$ is isolated. Indeed, $deg(v) = 0$ and it is even, and is the only vertex, thus it is true for base case.
Assumption: Assume true for $G = (V, E)$ where $|E| = 2k$ and $k \in \mathbb{N}$.
Inductive step: consider $G(V_1, E_1)$, where $|E_1| = |E| + 2n$ and $|V_1| = V + z$. Since it is true for assumption, consider thethe graph □

In an directed graph $G_D = (V_D, E_D)$, there exists an Eulerian cycle if and only if a directed graph is strongly connected and for each $v \in V_D$ is such that $deg_{out}(v) = deg_{in}(v)$.

7.6.2 Hamiltonian Cycle

Definition 7.22. Hamiltonian Cycles

A cycle in $G = (V, E)$ is Hamiltonian if and only if $\forall v \in V$ appears only exactly once. We yet do not know a certain theorem that would completely define the existence of such a cycle.

7.7 Partial Order Diagrams

7.7.1 Definitions

Recall that a partial order is reflexive, transitive and antisymmetric. There are ways to combine partial ordered relations. Consider the set $P = \{0, 1\}$, where $a \sim b$ denotes $a \leq b$. Then, $R = \{00, 01, 10, 11\}$. Then, how would we define the same relation on $P \times P$? There are two formal ways:

1. Lexicographic ordering: $(p_1, q_1) \leq_{lex} (p_2, q_2)$ iff $p_1 \leq p_2$ or $p_1 = p_2$ and $q_1 \leq q_2$.
2. Product ordering: $p_1, q_1) \leq_{pr}$ iff $p_1 \leq p_2$ and $q_1 \leq q_2$.

Definition 7.23. Covering

x is covered by y iff $\nexists z \in P$, $x < z < y$ and $x < y$.

$$x \lessdot y \tag{34}$$

Definition 7.24. The least element

The least element is an element $x \in P$ if $\forall y \in P$, $x \lessdot y$ for some poset P. Furthermore, the minimal element if it is the least element and it also implies $y = x$.

Definition 7.25. The greatest element

The greatest element is an element $x \in P$ if $\forall y \in P$, $y \lessdot x$ for some poset P. Furthermore, it is also a maximal element if it is the greatest element and it also implies $x = y$.

It is important to notice the difference between the maximal element and the greatest element, as it is to notice the difference between the least and the minimal element. As such, consider the following example:

Example 7.1. Partial Order Element Distinction

Consider the set $P = \{a, b, c, d\}$ and the poset $(P, \preceq)$ defined to be such that the following holds $\preceq = \{(a, a), (b, b), (c, c), (d, d), (a, c), (a, d), (b, c), (b, d)\}$. Then, its Hasse diagram is as follows:

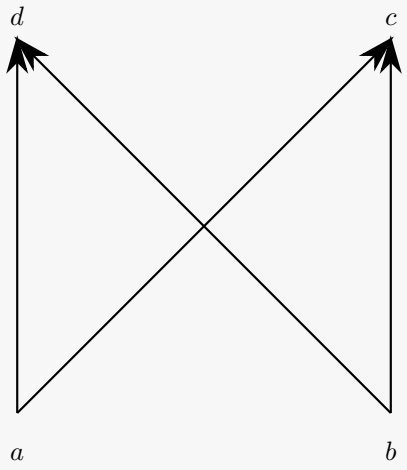


Figure 4: Hasse of poset $(P, \preceq)$

Indeed, we have 2 least elements and 2 greatest elements, however, we do not have minimal nor maximal defined.

7.7.2 Hasse Diagrams

Definition 7.26. Hasse Diagram

of a poset P, is the diected graph $G_P = (V, E)$ such that $V = P$ and $E = \{(x, y) : x \lessdot y\}$. In partial orders, because of antisymmetry, they're directed acyclic graphs. That is, all elements in a cycle are a single element.

Example 7.2. Hasse Diagram Example

The following example shows the Hasse Diagram of the set P where $P = \{x, y, z\}$. Let the poset X be defined by $X = (2^P, \subseteq)$.

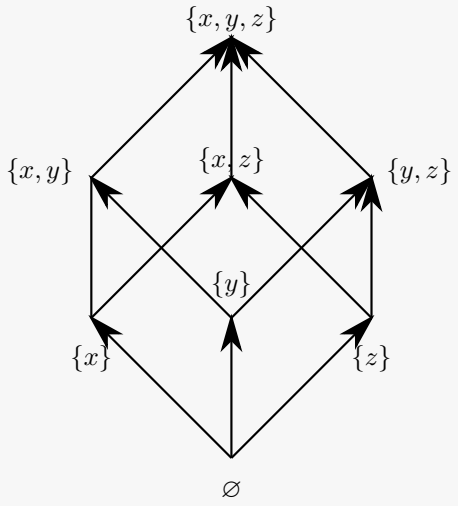


Figure 5: Hasse Diagram of the powerset 2^P

Notice that reflexivity is not shown, as every element is reflexive by definition of poset. Furthermore, transitivity is implied by the ordering of the set from bottom to the top. Lastly, antisymmetry ensures that all unique elements do not coincide with each other.

7.8 Planar Graphs

Definition 7.27. Planar

A graph is "planar" if there exists a set of rules for edges. For example, when drawing a demonstration of a graph, it must be that some edges do not touch/cross each other.

Example 7.3. Example 1

For example, a graph consisted of 3 houses and 3 wells. Each house must have a path to each well, and these paths must not cross.
In particular, this problem os non-planar because such a graph does not exist.

Note that if a planar graph is subdivided (a vertex added to an edge which does not change paths), it still planar. Furthermore, if a subgraph G is not planar of a graph G, then G is not planar as well. This leads to the theorem

Theorem 7.3. *Kuratowski's Theorem*

An undirected graph $G = (V, E)$ not planar if and only if G has a subgraph H that is isomorphic to a graph obtained from $K_{3,3}$ or from K_5 by a sequence of edge subdivisions.

Lemma 7.4. *Degree of planars*

Every planar graph contains a vertex with degree $deg(v) \leq 5$.

Theorem 7.5. *Euler's Formula*

Euler's formula states that In planar graphs $G = (V, E)$, where F is the faces of a graph, it must be true that $|V| - |E| + |F| \equiv 2$. The proof is beyond this module.

Theorem 7.6. *4-colouring*

Every planar graph has a 4 colouring. The proof is beyond this module. However, note that the real proof was done through assisting of computers.

7.9 Trees

Definition 7.28. Tree

An undirected graph $G = (V, E)$ is a tree if is connected and acyclic. That is, it is connected for all vertices $v \in V$, there exists no cycle.

Definition 7.29. Spanning Tree

A subgraph $G' = (V, F)$ of a graph $G = (V, E)$ is a spanning tree if G' is a tree.

Theorem 7.7. *Connectivity of cycles*

Suppose an edge is removed from a cycle in a connected graph. Then the graph is still connected.

Proof. $\forall u, v \in V$, $\exists$path $u \to *v$ in the original graph. For u, v if this path avoided the edge, then it is still a path in the new graph. Otherwise, replace the removed edge by the path between its endpoints (note this exists because the edge was in a cycle). □

Theorem 7.8. *Every graph has a spanning tree*

Proof. Induction on $|E|$.
Base case: $|E| = 0$. In this case, $|V| = 1$. This is a tree.
Inductive step: Assume true for $|E| = m$, where $m \in \mathbb{N}$.
If G has no cycles, then we are done as it is a tree.
Suppose there is a cycle in G. We remove an edge from the *cycle*, obtaining $G_1 = (V, E_1)$. $|E_1| = m$. By the inductive hypothesis, G_1 has a spanning tree, $T = (V, F)$. $F \subseteq E_1 \subseteq E$, so T is also a spanning tree of G □

Theorem 7.9. *Adding a new edge to same vertices creates a cycle*

Proof. Suppose $e = (u, v)$ is the new edge in the graph $G' = (V, E')$. Since G was connected previously, it had a path $u \to *v : u, e_1, u_1, e_2, u_2, e_3, \ldots, v$. We can now create a cycle by considering path $u, \ldots, v, e, u$. □

Theorem 7.10. *Theorem 3*

Let $G = (V, E)$ be an undirected graph with $|V| = p$ and $|E| = q$. Then,

1. G has $\geq p - q$ connected components
2. If G is acyclic, then it has exactly $p - q$ connected components.

Proof. G can be obtained from $(V, \varnothing)$ by adding all the edges in E. Suppose these edges are $e_1, e_2, e_3, \ldots, e_q$. We begin with p connected components. If we add an edge $\{u, v\}$, u, v belong to different connected component. The number of connected components decreases by 1. However, if u, v are connected components already, then it is still a component by its own as it creates a cycle, so the number stays the same. Therefore, at most there are $p - q$ connected components. □

Theorem 7.11. *Five definitions of Trees*

Suppose $G = (V, E)$ is a undirected simple graph where $|E| = p$ and $|V| = q$. Then, the following are equivalent:

1. G is acyclic and connected
2. G is acyclic and $q = p - 1$
3. G is connected and $q = p - 1$
4. G is connected and removing any edge makes it disconnected
5. G is acyclic but adding any edge on the same vertices creates a cycle

Proof. $1 \implies 2 \implies 3 \implies 4 \implies 5 \implies 1$
$1 \implies 2$: By Theorem 7.10, there are $p - q$ connected components. However, it is a connected graph, therefore there is only 1 connected component. As such, $1 = p - q$.
$2 \implies 3$: There are exactly $p - q$ connected components. However, $1 = p - q$ therefore it is connected as it is a singular component.
$3 \implies 4$: By Theorem 7.10, after edge removal, $q' = p - 2$. The new graph has $\geq p - (p - 2)$ connected components. As such, it is disconnected.
$4 \implies 5$: By Theorem 7.7 (contrapositive), the graph is acyclic. By Theorem 7.9, edge addition creates a cycle
$5 \implies 1$: If disconnected, then add edge between 2 components without creating new cycles (Theorem 7.7). This cannot be true. □

There are several consequences of this theorem. For example, 4 says that it is a minimal in a partial order. Condition 5 similarly tells us that the graph is maximally acyclic. Exercise:
Show condition 6, that is, for every node u, v, there is a unique path from u to v.

Definition 7.30. Rooted Trees

A rooted tree is a tree in which one vertex is distinguished and called a tree root.

Definition 7.31. Leaf

A leaf in a tree is a vertex v in a tree $G = (V, E) : deg(v) = 1$.

Definition 7.32. Forest

A disjoint collection of trees is called a forest.

8 Probability

Definition 8.1. Sample Space

Sample space is the set that consists all possible outcomes or results of an experiment. This set is generally denoted by Ω.

For example, if we consider the toss of a coin twice, then we can either get H or T. Then, 2 coin tosses can be described by the set $P = \{H, T\}$, then $P \times P = \{HH, TH, HT, TT\}$. In very big examples, such as picking 5 cards from a deck, where $C = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\} \times \{2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A\}$ we could just limit our samplespace Ω to be $\Omega = \{A \subseteq C : |A| = 5\}$ where A represents the possible cards that we pick.

8.1 Combinatorics

8.1.1 Permutations

Definition 8.2. Permutation

Permutation is a bijection on a finite set. That is, $f : S \to S$ where $|S| = n$, $n \in \mathbb{Z}^+$.

$$Perm(S) = \{c \in S^{|S|} : \text{every element in ordered pair is unique}\} \tag{35}$$
$$|Perm(S)| = n! \text{ where } |S| = n \tag{36}$$

For example, for $S = \{a, b, c\}$, we get $Perm(S) = \{abc, acb, bca, bac, cab, cba\}$ and $|Perm(S)| = 6$

Definition 8.3. Arrangements

An arrangement is an injective function $f : \{1, \ldots, \kappa\} \to S$. It is a sequence of length κ where elemenets are from S without repetitions.

$$Arr(s, \kappa) = \{c \subseteq S : |c| = \frac{n!}{(n-k)!}\} \tag{37}$$

For example, $S = \{a, b, c\}$, then $|Arr(s, 2)| = n \cdot (n-1)$. In particular, the example is then 6 (ab, ac, ba, bc, ca, cb) $3 \cdot 2 = 6$ from the fact that we can pick 3 objects in the beginning and then 2. The generalisation is as follows: $|Arr(s, \kappa)| = n \cdot (n-1) \cdot \ldots (n - \kappa + 1)$. One could also think of arrangements as permutations but limited on κ factors instead of the whole set cardinality.

Definition 8.4. Combinations

Sometimes, we do not require to distinguish orders. This leads to subsets of S of size κ. That is

$$Comb(s, \kappa) = \{c \subseteq S : |c| = k\} \tag{38}$$

$a_1 \sim a_2$ if they contain exactly the same objects, then

$$|Comb(s, \kappa)| = \frac{|Arr(s, \kappa)|}{\kappa!} \tag{39}$$

This can otherwise be written as

$$\frac{n!}{\kappa!(n-\kappa)!} \tag{40}$$

For example, if we had $S = \{1, 2, 3, 4, 5\}$, then if we were to have 3 elements we know there are $5 \cdot 4 \cdot 3$ ways to arrange them. However, we can permute 3 objects $3 \cdot 2 \cdot 1$ times and we want to ensure they are unique, therefore

$$\frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} = 10$$

8.2 Assigning Probabilities

Definition 8.5. Probability Spaces

The ordered triple (Ω, F, P) where $F = 2^{\Omega}$ and P is the probability measure. $P : F \to [0, 1]$. In this case, F represents all possible events. The probability measure for $\Omega = \{w_1, w_2, \ldots, w_3\}$ and $p_1, p_2, \ldots, p_m \in \mathbb{R} : p_i \geq 0$ and $\sum_{i=1}^{m} p_i = 1$. For $E = \{w_1, \ldots, w_k\}$, $P(E) = \sum_{w_i \in E} p_n$

Example 8.1. Example 1

In a loaded die, $\Omega = \{1, 2, 3, 4, 5, 6\}$ and $p_1 = p_2 = \ldots = p_5 = \frac{1}{10}$, $p_6 = \frac{1}{2}$. Then, $Even = \{2, 4, 6\}$ and $p(Even) = p_2 + p_4 + p_6 = 0.7$.

Example 8.2. Coins

For a coin that is tossed k times, what is the probability that there are z heads?
Whilst this question may seem hard at first, let us assign our sample space as $\Omega = \{H, T\}^k$. Then, from the sample space, we need 3 out of k objects that have an H. That is, ${}^kC_3$. It follows that

$$\frac{1}{2^k} \cdot |3H| \tag{41}$$

$$= \frac{1}{2^k} \cdot {}^kC_3 \tag{42}$$

Definition 8.6. Mutually Exclusive

Two events are mutually exclusive if for $P(E) \in [0, 1]$ and $P(A_1 \cup \ldots \cup A_k) = \sum_{i=1}^{k} P(A_i)$, $A_i \cap A_i = \varnothing, i \neq j$. Then, $P(A \cup B) = P(A + B)$ only if $P(A \cap B) = 0$.

Theorem 8.1. *Union Bound*

$$P(\bigcup_{i=1}^{n} A_i) \leq \sum_{i=1}^{n} P(A_i) \tag{43}$$

Theorem 8.2. *Inclusion - Exclusion Principle*

$$P(\bigcup_{i=1}^{n} A_i) = \tag{44}$$

$$= \sum_{i=1}^{n} P(A_i) - \sum_{1 \leq i_1 < i_2 \leq n} P(A_{i_1} \cap A_{i_2}) + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} P(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \ldots + (-1)^{n+1} P(A \cap \ldots \cap A_n) \tag{45}$$

Definition 8.7. Conditional Probability

Conditional probability is considering the probability of an event A given that B has happened, defined as the following:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{46}$$

One can interpret this as limiting your sample space to only the event B, when B is the new U.

Theorem 8.3. *Law of total probability*

For all events that are mutually exclusive each other, call them events $B_1, B_2, \ldots, B_k$, it follows that for all events $A \in 2^\Omega$,

$$P(A) = \sum_{i=1}^{k} P(A|B_i) \cdot P(B_i) \tag{47}$$

From the fact that $P(A|B_i) \cdot P(B_i) = P(A \cap B_i)$

Theorem 8.4. *Bayes' Theorem*

For all events that are mutually exclusive to teach other, call them evenets $B_1, B_2, \ldots, B_k$, it follows that for all events $A \in 2^\Omega$ the following holds:

$$P(B_i|A) = \frac{P(B_i \cap A)}{P(A)} \tag{48}$$

$$= \frac{P(A|B_i) \cdot P(B_i)}{\sum_{j=1}^{k} P(A|B_j) \cdot P(B_j)} \tag{49}$$

The denominator is from the fact of Law of total probability. The numerator is re-arrange using conditional probability the other way around.

Definition 8.8. Independence

Two events A, B are independent if the following holds:

$$P(A \cap B) = P(A) \cdot P(B) \tag{50}$$

That is, obtaining the result of one does not affect the probability of getting the other.

8.3 Expectation and Variance

Example 8.3. Bernoulli Trial

$= \{h, t\}$ Let $P(\{t\}) = p \in [0, 1]$ where $p = 0.4$. Then, $P(\{h\}) = 0.6 = 1 - p$ Define

$$X(w) = \begin{cases} 1 \text{ if } w = t \\ 0 \text{ if } w = h \end{cases} \tag{51}$$

X has Bernoulli distribution with parameter p.

8.3.1 Averages

Definition 8.9. Expectation

Consider the probability space $(\Omega, 2^{\Omega}, P)$. Then, let us define $X : \Omega \to \mathbb{R}$ is random v. Suppose X only takes values $\{0, 1, 2, 3\}$. Then, the expectation of $E(X) = \sum_{i=0}^{3} i \cdot P(X = i)$. This is

$$P(X = 1) + 2P(X = 2) + 3P(X = 3) \tag{52}$$

One could view expectation as a weighted average. For a finite set, the expectation is defined to be

$$E(X) = \sum_{i=1}^{n} a_i \cdot P(X = a_i) \tag{53}$$

More importantly, for some $a \in \mathbb{R}$,

$$E(X + Y) = E(X) + E(Y)$$
$$E(aX) = aE(X)$$

If random variables X and Y are independent, then

$$E(X \cdot Y) = E(X) \cdot E(Y)$$

However, the notion of 'average' is complicated. Whilst expectation does kind of determine the 'average' value, we can also denote the average through median and mode.

Definition 8.10. Median

Median is defined to be the number in the middle when ordered by ascending numbers.

$$1, 2, 2, 2, 2, 2, 3, 99, 99, 99, 99 \tag{54}$$

In this case, the median is 2.

Definition 8.11. Mode

The mode is defined to be the number that appears in a list of probability events the most. It is also a notion of 'average'

Theorem 8.5. *Markov's Inequality*

Markov's Inequality gives us information about an X as a random variable with $X \geq 0$. $\forall a \in \mathbb{R}^+$, the inequality

$$P(X \geq a) \leq \frac{E(X)}{a} \tag{55}$$

must hold.

Proof. Assume that $Range(X)$ is finite. That is, $\exists v_1, v_2, \ldots, v_n \in \mathbb{R}^+ : \sum_{i=1}^{n} P(X = v_i) = 1$.

Table 7: Probability Table

i	v_1	v_2	$\ldots$	v_n
$P(X = i)$	p_1	p_2	$\ldots$	p_n

Then indeed, $E(X) = \sum_{i=1}^{n} p_i \cdot v_i$. Consider $S = \{i : v_i < a\}$ and $T = \{i : v_i \geq a\}$ Then,

$$\begin{aligned}
&\sum_{i=1}^{n} p_i \cdot v_i = \underbrace{\sum_{i \in S} p_i \cdot v_i}_{\geq 0} + \sum_{i \in T} p_i \cdot v_i \\
\implies &\sum_{i \in S} p_i \cdot v_i + \sum_{i \in T} p_i \cdot v_i \geq \sum_{i \in T} p_i \cdot \underbrace{v_i}_{\geq a} \\
\implies &\sum_{i \in T} v_i \cdot p_i \geq \sum_{i \in T} p_i \cdot a \\
&\sum_{i \in T} p_i \cdot a = a \sum_{i \in T} p_i = aP(X \geq a) \\
\implies &E(X) \geq aP(X \geq a) \\
\implies &\frac{E(X)}{a} \geq P(X \geq a)
\end{aligned}$$

As required. □

8.3.2 Variance and Standard Deviation

Definition 8.12. Variance

The variance measures the spread of a random variable X. The standard deviation of X is given as $\sqrt{Var(X)}$.

$$\begin{aligned}
Var(X) &= E(X - E(X))^2 &(56)\\
&= E(X^2) - E(X)^2 &(57)
\end{aligned}$$

9 Exam tips

1. For truth tables of n variables, there are 2^n possible total different inputs.
2. Use lexicographic ordering. That is, for a truth table, make one variable alternate every one statement. The next variable will alternate every 2 variables. The next one every 4. The next one every 8 etc.

A Interchanging $\exists$ and $\forall$ and variables

For set $S = \{0, 1, 2, 3, n\}$

Example A.1. Example 1

$\forall x \exists y . f(x, y)$

$$\bigwedge_x \bigvee_y f(x, y) \tag{58}$$

Example A.2. Example 2

$\forall y \exists x . f(x, y)$

$$\bigwedge_y \bigvee_x f(x, y) \tag{59}$$

Example A.3. Example 3

$\exists x \forall y . f(x, y)$

$$\bigvee_x \bigwedge_y f(x, y) \tag{60}$$

Example A.4. Example 4

$\exists y \forall x f(x, y)$

$$\bigvee_y \bigwedge_x f(x, y) \tag{61}$$