Discrete Mathematics

Seminar I / II

Presented by: Rishabh Singh and Karen Zhang

Term 1, 2020

Table of contents

Sets, Functions and Sequences

Sets

Definition

A set is a collection of distinct objects (numbers, variables, other sets etc). We can define a set in two main ways. Firstly, we can list out all of the elements of a set, like

$$A = \{-2, -1, 0, 1, 2\}.$$

Alternatively, we can define a set using the following syntax

$$A = \{x \in \mathcal{U} \mid -2 \leq x \leq 2\}.$$

where $\mathcal{U}$ is itself a set. The above is read "The set of all elements, x, in $\mathcal{U}$ such that $-2 \leq x \leq 2$". This is a simple way of representing complex sets.

Sets, Continued

Elements

The objects in a set are called are called **elements** of the set. We write

$$a \in A,$$

to denote that an object a is an element of the set A.
Similarly,

$$a \notin A$$

denotes that the object a is not an element of set A.

Note

A set is not equal to the elements inside it, even if the set only has one element. That is to say $a \neq \{a\}$ and $a, b \neq \{a, b\}$

Some Important Sets

Sets

$$
\begin{aligned}
\mathbb{N} &= \{\text{The Natural Numbers}\} \\
&= \{0, 1, 2, 3, \ldots\} \\
\mathbb{Z} &= \{\text{The Integers}\} \\
&= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \\
\mathbb{Z}^+ &= \{\text{The Positive Numbers}\} \\
&= \{1, 2, 3, \ldots\} \\
\mathbb{Q} &= \{\text{The Rational Numbers}\} \\
&= \left\{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\right\} \\
\mathbb{R} &= \{\text{The Real Numbers}\} \\
\mathbb{C} &= \{\text{The Complex Numbers}\}
\end{aligned}
$$

Sets, continued

Equality

Two sets are equal if and only if they contain the same items. Following from the previous example:

$$\{-2, -1, 0, 1, 2\} = \{x \in \mathbb{Z} \mid -2 \leq x \leq 2\}$$

as both the sets define the same set of integers.

Note!

Sets ignore repetitions. For instance,

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

because both the sets only consists of elements 1, 2, 3, 4 and 5. All the repetitions of the numbers are ignored.

Containment

Subsets

Some sets may be "contained" inside other sets, i.e. all of the elements in A may also be elements of B. Then A is a **subset** of B, denoted

$$A \subseteq B.$$

However, if there is at least one element of A that is not in B, then

$$A \not\subseteq B.$$

Containment

$$\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Containment, continued

The Empty Set

The empty set, denoted $\varnothing = \{\}$, is a set containing nothing. Therefore, it a subset of all sets, including itself. The relation $\varnothing \subseteq A$ holds for all sets A.

Improper vs Proper Subsets

It is important to note that a 'subset' can be any chunk of a set: from none of set to the the entire set.
An important distinction is made: A is a proper subset of B (denoted $A \subset B$) if and only if $A \neq B$.

Equality

An important result is that if two sets A and B are equal, then v

$$A \subseteq B \text{ and } B \subseteq A$$

Additional Set Properties

Cardinality

The cardinality of a set A, denoted $|A|$, refers to the number of elements inside the set A.
Note: A set contained inside a set just counts as one element, regardless of its own cardinality.

$$|\{\mathbb{R}\}| = 1, \text{ despite } |\mathbb{R}| = \infty.$$

The Power Set

The power set, denoted $\mathcal{P}(A)$ is the set of all possible possible subsets of the elements in A. As an example...

$$\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Also, $|\mathcal{P}(A)| = 2^{|A|}$, which can be proven.

Additional Set Properties

Cartesian Product

The Cartesian Product two sets A and B is defined as follows

$$A \times B = \{(p, q) \mid p \in A, q \in B\}$$

This just means that it is a set of pairs consisting of every element in set A with every element of set B.

$A \times B$

Let $A = \{1, 2, 3\}$ and let $B = \{a, b, c\}$, then

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$$

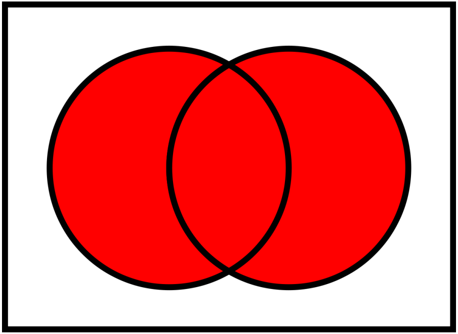
which is pretty cool.

Set Operations

Union

The **Union** of two sets is defined as

$$A \cup B = \{x \in \mathcal{U} \mid X \in A \text{ or } X \in B\}$$

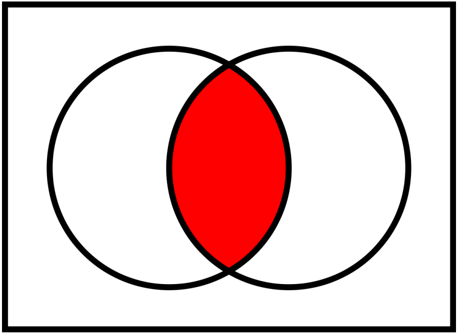


Set Operations

Intersection

The **Intersection** of two sets is defined as

$$A \cap B = \{x \in \mathcal{U} \mid x \in A \textbf{ and } x \in B\}$$

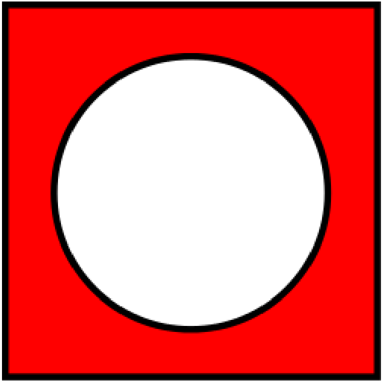


Set Operations

Complement

The **Complement** of a set A is defined as

$$A^c = \{x \in \mathcal{U} \mid x \notin A\}$$

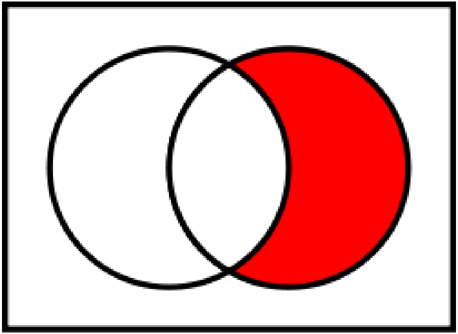


Set Operations

Difference

The **Difference** of two sets is defined as

$$A - B = A \backslash B = \{x \in \mathcal{U} \mid x \in A \textbf{ and } x \notin B\}$$



Set Algebra Laws

Associative Laws

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

Commutative Laws

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Distributive Laws

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

De Morgans Laws

$$(A \cup B)^c = (A^c \cap B^c)$$
$$(A \cap B)^c = (A^c \cup B^c)$$

Set Algebra Laws

Identity Laws

$$A \cup \varnothing = A$$
$$A \cap \mathcal{U} = A$$

Idempotent Laws

$$A \cup A = A$$
$$A \cap A = A$$

Negation Laws

$$A \cup A^c = \mathcal{U}$$
$$A \cap A^c = \varnothing$$

Difference Law

$$A - B = A \backslash B = A \cap B^c$$

Set Algebra Laws

Domination Laws

$$A \cup \mathcal{U} = \mathcal{U}$$
$$A \cap \varnothing = \varnothing$$

Absorption Laws

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

Double Complement Law

$$(A^c)^c = A$$

Duality

Swapping $\cap$ and $\cup$, and $\mathcal{U}$ and $\varnothing$ in a law leads the **dual** of that law (for all laws except the Difference Law).

Functions

Functions

A **function** is a relation where all the elements of one set to another set.
Formally, a function f from all the elements of X to the elements of set Y is denoted $f : X \to Y = \{(x, y) \in X \times Y \mid y = f(x)\}$.

Definition

A **function** f from a set X to Y is a subset of the set $X \times Y$ with the property

for each $x \in X$ there is exactly one ordered pair $(x, y) \in f$.

The notation $f : X \to Y$ implies that the set X is the **domain** and that the set Y is the **codomain** of the function f.

Floor and Ceil functions

Important Functions

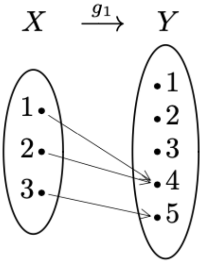
The floor and ceil functions have domain $\mathbb{R}$ and codomain $\mathbb{Z}$

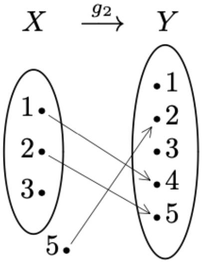
For any $x \in \mathbb{R}$ the **floor** of x, denoted $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

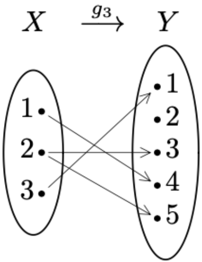
For any $x \in \mathbb{R}$ the **ceil** of x, denoted $\lceil x \rceil$ is the smallest integer greater than of equal to x.

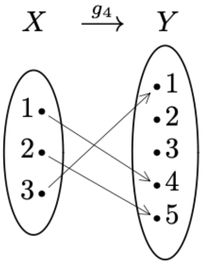
$$\lfloor \pi \rfloor = 3 \ , \qquad \lceil \pi \rceil = 4 \ ,$$
$$\lfloor 1081 \rfloor = 1081 \ , \quad \lceil 1081 \rceil = 1081 \ ,$$
$$\lfloor -\tfrac{1}{2} \rfloor = -1 \ , \qquad \lceil -\tfrac{1}{2} \rceil = 0 \ .$$

Arrow Diagrams









Types of Functions

Injection

A function f is **one-to-one** or **injective** if $f(x_1) = f(x_2)$ implies $x_1 = x_2$. In other words, there is a one-to-one $x - y$ correspondence.

Surjection

A function $f : X \to Y$ is **onto** or **surjective** if for every $y \in Y$, there is an $x \in X$ such that $f(x) = y$. That is, its range is equal to its codomain.

Bijection

A function $f : X \to Y$ is **bijective** iff it is both injective and surjective.
This is a necessary property for a function to have to be invertible - or have an inverse.

Composition of Functions and Inverse Functions

Composition of Functions

Let $g : X \to Y$ and $f : Y \to Z$, then the composition of f and g, denoted $f \circ g : X \to Z$, is defined by

$$(f \circ g)(x) = f(g(x))$$

Inverse Function

If a function $f : X \to Y$ is bijective, then there exists a function $g : Y \to X$ such that given any $y \in Y$, $g(y) = x$ which is the x such that $f(x) = y$.

$$g : Y \to X = \{(y, x) \in Y \times X \mid f(x) = y\}$$

Notation

The inverse of a function $f : X \to Y$ is more commonly denoted $f^{-1} : Y \to X$.

Composition with Inverse + Additional Notation

Composition with Inverse

If $f : X \to Y$ is a bijection, then

$$f^{-1} \circ f = \iota_X \text{ and } f \circ f^{-1} = \iota_Y$$

where ι_X and ι_Y are the identity functions on X and Y respectively.

Function Set Argument

Let $f : X \to Y$. If A is a set such that $A \subseteq X$, then

$$f(A) = \{f(x) \mid x \in A\}$$

Similarly, if $f^{-1} : Y \to X$ and $B \subseteq Y$, then $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$

Sequences

Definition

A sequence is a function with domain a subset of $\mathbb{Z}$. When discussion a sequence, convention dictates we write a_n instead of $a(n)$ - whereas the entire list sequence will either be denotes $\{a_n\}$, or by the list

$$a_1, a_2, a_3, \ldots$$

Note:

- The domain of the sequence is usually $\mathbb{N}$ or $\mathbb{Z}^+$, and sometimes a finite set i.e. $\{1, 2, \ldots, n\}$
- Order and Repetition are important when it comes to sequences

Summation

Summation Notation

$$\sum_{j=m}^{n} a_j,$$

where $\{a_j\}$ is a sequence and $m \leq n$ just means

$$a_m + a_{m+1} + \cdots + a_n$$

Note

The sum

$$\sum_{j=0}^{n} 1 = n + 1$$

since it has $n+1$ terms.

Some common sums

Examples

$$\sum_{j=0}^{n} ar^j = a\frac{r^{n-1}-1}{r-1}$$

$$\sum_{j=1}^{n} 1 = n$$

$$\sum_{j=1}^{n} j = \frac{1}{2}n(n+1)$$

$$\sum_{j=1}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1)$$

Transformations of Sums

Addition and Multiplication by a scalar

$$\sum_{k=1}^{n}(a_k \pm b_k) = \left(\sum_{k=1}^{n} a_k\right) \pm \left(\sum_{k=1}^{n} b_k\right)$$

$$\sum_{k=1}^{n} ca_k = c\sum_{k=1}^{n} a_k$$

Shifting the Index of Summation

Substituting $k = j + p$ yields

$$\sum_{j=m}^{n} a_j = \sum_{k=m+p}^{n+p} a_{k-p}$$

Examples

Reversing the summation

$$\begin{aligned}\sum_{j=m}^{n} &= a_m + a_{m+1} + a_{m+2} + \cdots + a_n \\ &= a_n + \cdots + a_{m+2} + a_{m+1} + a_m \\ &= \sum_{k=m}^{n} a_{n+m-k}\end{aligned}$$

This is equivalent to a substitution of $k = m + n - j$.

Examples, continued

Telescoping series

Work out

$$\sum_{k=1}^{n} \frac{1}{k(k+1)}$$

$$\begin{aligned}
\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} \\
&= \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) \\
&- \left(\frac{1}{2} + \cdots + \frac{1}{n} + \frac{1}{n+1}\right) \\
&= 1 - \frac{1}{n-1}
\end{aligned}$$

Integers, Modular Arithmetic and Relations

Number Theory

Divisibility

Number Theory is the study of important properties of positive integers, and divisibility is an important part of this.

Definition

Let a and b be integers. If there exists an integer m such that $b = am$, it can be said that "a divides b", or "a is a factor of b" or $a \mid b$.

Properties of Divisibility

Let $a, b, c \in \mathbb{Z}$

- If $a \mid b$ and $a \mid c$ then $a \mid b \pm c$.
- Let $s, t \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$ then $a \mid sb + tc$.
- If $a \mid b$ and $b \mid c$ then $a \mid bc$.

Prime and Composite Numbers

Primes

An integer $n > 1$, is said to be **prime** if it has no (positive) factors other than itself and 1. Any number which isn't prime is said to be **composite**.

The Fundamental Theorem of Arithmetic

Any positive integer n can be factorised into a product of primes. Moreover, a given n only has one such factorization.

Prime Factorization

$$345 = 3 \times 5 \times 23$$

$$1134 = 2 \times 3^4 \times 7$$

Checking for primes

Theorem

A composite number, n must have a factor c such that $1 < c \leq \sqrt{n}$.

Proof

If n is composite, we can write that $n = ab$, where $1 < a < n$. If $1 < a \leq \sqrt{n}$ then we can take $a = c$. If not, then

$$n > a > \sqrt{n}$$
$$1 < n/a < \sqrt{n}$$

we can take $b = c$, since $b = n/a$.

This further means that any composite number n must have a prime factor p such that $1 < p \leq \sqrt{n}$. So, if n has no prime factor $< \sqrt{n}$, then it is a prime number.

The Greatest Common Factor

Common Divisors

Let a, b be two nonzero integers. Any positive integer d such that $d \mid a$ and $d \mid b$ is called a **common divisor** of a and b. The *largest* such d is called the greatest common divisor, or the gcd.

Common Multiples

If $a \mid m$ and $b \mid m$, then m is a **common multiple** of a and b. The *smallest* such m is called the lowest common multiple, or the lcm.

We write both of these as $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in math.

Euclidean Algorithm

Division Algorithm

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Then there exist a unique pair of integers q, r such that

$$a = bq + r \qquad 0 \leq r < b$$

Theorem

Let a, b, q, r be integers such that $a = bq + r$, then

$$\gcd(a, b) = \gcd(b, r)$$

This theorem forms the basis for Euclid's algorithm.

Euclidean Algorithm

Finding $\gcd(14307, 11343)$

We can repeatedly use the theorem to deduce the following:

$$\begin{aligned}
14307 &= 1 \times 11343 + 2964 \\
11343 &= 3 \times 2964 + 2451 \\
2964 &= 1 \times 2451 + 513 \\
2451 &= 4 \times 513 + 399 \\
513 &= 1 \times 399 + 114 \\
399 &= 3 \times 114 + 57 \\
114 &= 2 \times 57
\end{aligned}$$

Therefore, we find that $\gcd(114, 57) = 57$. By the theorem on the last slide, $\gcd(14307, 11343) = 57$. This is Euclidean Algo.

Euclidean Algorithm, formal statement

Let a and b be positive integers; suppose that

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

where $q_i, r_i \in \mathbb{Z}^+$. Since

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n,$$

we can conclude that

$$\gcd(a, b) = r_n.$$

Extended Euclidean Algorithm

This can be used to solve equations of the form $ax + by = d$ where $d = \gcd(a, b)$ for $x, y \in \mathbb{Z}$.

Using a simpler example

One would compute $\gcd(854, 651)$ in the following way:

$$\begin{aligned} 854 &= 1 \times 651 + 203 \\ 651 &= 3 \times 203 + 42 \\ 203 &= 4 \times 42 + 35 \\ 42 &= 1 \times 35 + 7 \\ 35 &= 5 \times 7 \end{aligned}$$

However, we can use the above working out to solve the equation $854x + 651y = 7$. This will be more important later...

Extended Euclidean Algorithm, continued

Working Backward

Working from the second-last equation on the prev slide...

$$\begin{aligned} 7 &= 42 - 35 \\ &= (651 - 3 \times 203) - (203 - 4 \times 42) \\ &= 651 - 4 \times 203 + 4 \times 42 \\ &= 651 - 4 \times (854 - 651) + 4 \times (651 - 3 \times (854 - 651)) \\ &= 5 \times 651 - 4 \times 854 + 4 \times (4 \times 651 - 3 \times 854) \\ &= -16 \times 854 + 21 \times 651 \\ &= 854x + 651y \end{aligned}$$

so, one solution to the linear equation is $x = -16$ and $y = 21$. We can extend this solution to include all possible solutions.

The Bézout Property

Theorem

If we have integers $a, b, c, d \in \mathbb{Z}$ such that $\gcd(a, b) = d$, then if we consider the equation

$$ax + by = c \qquad (\star)$$

- If $c = d$, then $(\star)$ has a solution $x, y \in \mathbb{Z}$
- If $d \mid c$, then $(\star)$ has a solution in integers
- If $\gcd(c, d) = 1$, then $(\star)$ has no solutions in $\mathbb{Z}$

Also, $x = x_0 - \lambda b$ and $y = y_0 + \lambda a$ represent all solns.

Examples

- $73x + 30y = 1$ has a solution since $\gcd(73, 30) = 1$.
- $42x + 99y = 6$ has a solution since $\gcd(42, 99) = 3$ and $3 \mid 6$.
- $91x + 49y = 2$ has no solution since $\gcd(91, 49) = 7$ and $2 \nmid 7$.

Modular Arithmetic

Definition

Let m be an integer. Two integers a and b are said to be **congruent module** m, denoted

$$a \equiv b \pmod{m}$$

if $m \mid a - b$

Ways of Expressing Congruence

Note:

- $a \equiv b \pmod{n}$
- $m \mid a - b$
- $a = b + km$
- a and b have the same remainder upon division by m

all mean the same thing.

Properties of Congruence

Properties

- Let $a, b, c, d, m \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$
  - $a + c \equiv b + d \pmod{m}$
  - $a - c \equiv b - d \pmod{m}$
  - $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \in \mathbb{Z}$ then $ca \equiv cb \pmod{m}$
- If $\equiv b \pmod{m}$ and $n \geq 0$ then $a^n \equiv b^n \pmod{m}$
- If $a \equiv b \pmod{m}$ and $n \mid m$ then $a \equiv b \pmod{n}$

Power Congruence

Finding a^b mod c

The properties of modular arithmetic and congruence make it easy to simplify expressions of the form a^b mod c, for really large b, where computation may not necessarily be ideal.
Simplification becomes easy, given we are able to find one power n such that a^n mod $c = \pm 1$ or are able to notice a pattern of repetitions.

Find the last two digits of $7^{1234567}$

The last two digits of $7^{1234567}$ can be expressed as $7^{1234567}$ mod 100. Observing successive value for 7^a mod 100,

$$7^1 \equiv 7 \pmod{100} \qquad 7^3 \equiv 7 \cdot 49 \equiv 343 \equiv 43 \pmod{100}$$

$$7^2 \equiv 7 \cdot 7 \equiv 49 \pmod{100} \qquad 7^4 \equiv 7 \cdot 43 \equiv 301 \equiv 1 \pmod{100}$$

Solutions to Congruences

Number of Solutions to Congruences

Considering the congruence $ax \equiv b \pmod{m}$

- If $\gcd(a, m) = 1$, then the congruence has one unique solution
- If $\gcd(a, m)$ is not a factor of b, then the congruence has no solutions
- If $\gcd(a, m) = g$ is a factor of b then,
  - the congruence has a unique solution mod m/g,
  - the congruence has g solutions mod m

Examples

- $17x = 1 \pmod{5}$ has a unique solution mod 13.
- $68x = 11 \pmod{51}$ doesn't have a solution.
- $52x = 8 \pmod{60}$
  - has a unique solution mod 15
  - has 4 solutions mod 60

Canceling/Simplifying Congruences

Simplification 1

The congruences

$$ax \equiv b \pmod{m} \text{ and } cax \equiv cb \pmod{cm}$$

have the same solutions.

Simplfication 2

Given $\gcd(c, m) = 1$, the congruences

$$ax \equiv b \pmod{m} \text{ and } cax \equiv cb \pmod{m}$$

have the same solutions.

Testing for Primes 2: Electric Boogaloo

Fermat's Little Theorem

Let $p > 1$. If p is prime, then for every $a \in \mathbb{Z}$ we have

$$a^p \equiv a \pmod{p}$$

This means that if we have

$$a^p \not\equiv a \pmod{p}$$

for any $a \in \mathbb{Z}$, then p is composite

Negative Test Only

Note: Fermat's Little Theorem only provides us with a negative test for primes. It can definitively state whether a number is composite, but even if the theorem holds for all a, then its 'probably' but not definitively prime.

Relations

Definitions

A relation R from a set A to a set B is a set of **ordered** pairs (a, b), where $a \in A$ and $b \in B$ (i.e. R is a subset of $A \times B$).

To specify if two elements are related:

- $(a, b) \in R$
- aRb

Functions

A function is a type of relation R where for every $a \in A$, there is one and only one $b \in B$ such that aRb

Representing Relations

Two useful ways of representing a relation on a **finite** set:

Matrix

Choose an specific order for the n elements of a set A, e.g. $A = \{a_1, a_2, \ldots, a_n\}$
The matrix M_R of a relation on set A is the $n \times n$ matrix where

$$m_{i,j} = \begin{cases} 1 & \text{if } a_i R a_j \\ 0 & \text{if } a_i \not R\, a_j \end{cases}$$

- More than one possible matrix (elements of a set can be listed in different orders)

Arrow Diagram

A point is drawn for each element of A, with an arrow drawn from a_i to a_j iff a_i is related to a_j.

Reflexive

Definition

A relation R on a set A is reflexive if every element of A is related to itself.

- For every $a \in A$, aRa

Representation

- The diagonal entries of matrix M_R must always be 1
- Every point in the arrow diagram will have an arrow pointing to itself

Symmetric

Definition

A relation R on a set A is symmetric if when one element is related to another, the second is also related to the first.

- For all $a, b \in A$, if aRb then bRa

Representation

- Given matrix M_R, $m_{i,j} = m_{j,i}$
- If there is an arrow from a_i to a_j, there must be an arrow from a_j to a_i (double arrow)

Transitive

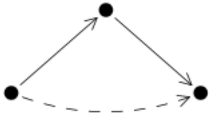
Definition

A relation R on a set A is transitive if when one element is related to a second, and the second is related to a third, then the first element must be related to the third.

- For all $a, b, c \in A$, if aRb and bRc, then aRc

Representation

- Calculate ${M_R}^2$ and look at the non-zero entries. If M_R has the entry 1 in all of these places, then the relation is transitive



Antisymmetric

Definition

A relation R on a set A is antisymmetric if two distinct elements of A are related in one way or the other, or neither, but NEVER both.

- For all $a, b \in A$, if aRb and bRa, then $a = b$

Representation

- Given matrix M_R and $(i \neq j)$, $m_{i,j}$ and $m_{j,i}$ cannot both equal 1
- No double arrows in arrow diagram

Note

Antisymmetric is NOT the opposite of symmetric!

Equivalence Relations

Definition

Equivalence relations are **reflexive**, **symmetric** and **transitive**.

- Denoted by $\sim$.

Intuitively...

- Tells us when two things are "the same"
- E.g. Two sets are equal if they have the same elements, two triangles are similar if they have the same angles etc.

Equivalence classes

Definition

For any $a \in A$, the equivalence class of a with respect to $\sim$ is the set

$$[a] = \{x \in A \mid x \sim a\}$$

Intuitively...

- Collects together the objects which are "the same" and regard them as a single "object"
- E.g. Given $\sim$ is $\equiv \pmod 5$, then the five equivalence classes are the sets $[0]$, $[1]$, $[2]$, $[3]$, $[4]$

Equivalence Relations and Classes Theorem

Theorem

Let $\sim$ be an equivalence relation on set A. Then

- For all $a \in A$, $a \in [a]$
  - Every element of A is in some equivalence class
  - Every equivalence class contains at least one element
- For all $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$
- For all $a, b \in A$, $a \not\sim b$ if and only if $[a] \cap [b] = \emptyset$
  - Equivalence classes are either equal or pairwise disjoint

Example

2016 Semester 2 Final Q2 (ii)

Let $\sim$ be the relation on the set of integers $\mathbb{Z}$ be defined by

$$a \sim b \text{ if and only if } a^2 \equiv b^2 \pmod{4}.$$

1. Show that $\sim$ is an equivalence relation.
2. Find the equivalence classes of $\sim$.

Partial Order

Definition

A partial order is **reflexive, antisymmetric** and **transitive**.

- Denoted by $\preceq$, where $a \preceq b$ reads 'a precedes or equals b'

Intuitively...

- Tells us which of two elements 'comes first'.
  - E.g. $a \leq b$ is equivalent to saying a comes before b if elements are listed in increasing order.

Partial Order

Additional Property

$$\text{For all } a, b \in A, \text{either } a \preceq b \text{ or } b \preceq a$$

- If the above property is true, this is called a total order (any two elements can be ordered) or a linear order (elements can be ordered in a line).
- E.g. $\geq$, $\leq$

Poset

The term "poset" can be used for a set A with a partial order defined $(A, \preceq)$.

Hasse Diagrams

Definition

To represent a partial order $\preceq$ on a finite set A:

- For $a \prec b$, draw a point for a positioned below b
- Draw a line from a to b if and only if $a \prec b$ and there is no c such that $a \prec c \prec b$ (Transitivity is assumed).
- Do not draw any loops to indicate $a \preceq a$. Reflexivity is assumed.

Posets

Definitions

Let $\preceq$ be a partial order on a set A, where $x \in A$. x is called:

- **Greatest** if every element is related to it ($a \preceq x$ for all $a \in A$)
- **Least** if it is related to every element ($x \preceq a$ for all $a \in A$)
- **Maximal** if it is related to no element except itself ($x \preceq a$ only if $x = a$)
- **Minimal** if no element except itself is related to it ($a \preceq x$ only if $x = a$)

Posets

Lower and upper bounds

Let $\preceq$ be a partial order on a set A, where $a, b \in A$. Then for any $x \in A$,

- x is a **lower bound** of a and b if $x \preceq a$ and $x \preceq b$
- x is an **upper bound** of a and b if $a \preceq x$ and $b \preceq x$
- the **greatest lower bound** (if it exists), denoted by $glb(a, b)$ is the greatest element in the set of lower bounds
- the **least upper bound** (if it exists), denoted by $lub(a, b)$ is the least element in the set of upper bounds

Example

2018 Semester 1 Q2 (iii)

Let $S = \{2, 3, 4, 5, 10, 15, 20, 30, 40, 120\}$.

1. Draw the Hasse diagram for $\{S, |\}$.
2. Find all
   1. maximal elements,
   2. minimal elements.
3. Find two elements of S that do not have a greatest lower bound and explain why they do not.

Graph Theory

Introduction to Graph Theory

Definitions

A graph G consists of a finite set of **vertices** V, a finite set of **edges** E and an **endpoint function** $f : E \to$ {unordered pairs of vertices}

- f assigns each edge to either one or two vertices

More definitions

Terminology

- Two vertices are **adjacent** if joined by an edge
- An edge is **incident** on each of its endpoints
- **Isolated:** a vertex without incident edges (degree 0)
- **Loop:** an edge with only one endpoint/vertex
- **Parallel/multiple:** two or more edges with the same endpoint
- **Simple graph:** a graph with no loops or parallel edges
- The **degree** of a vertex v, denoted by $\mathbf{deg(v)}$ is the number of edges incident on v
  - Loops are counted twice

The Handshaking Lemma

Theorem

The sum of the degrees of all the vertices equals twice the number of edges,

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

Corollary

In any graph,

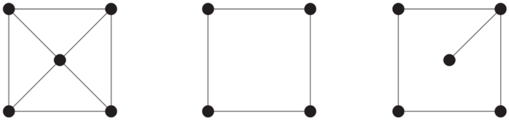
- The sum of the degrees is even.
- The number of vertices having odd degree is even.
  - Proof by contradiction

Special Graphs

Subgraphs

A graph G' with vertices V' and edges E' is a subgraph of the graph G with vertices V and edges E if:

- $V' \subseteq V$
- $E' \subseteq E$
- each edge in G' has the same endpoints as in G



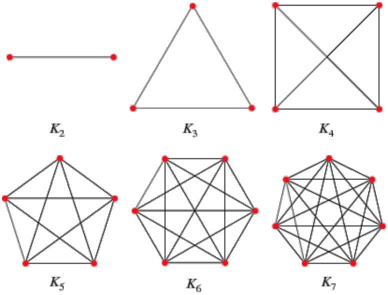
G $\quad$ G' $\quad$ G''

Special Graphs

Complete graph

The complete graph, denoted by K_n for $n \geq 1$, consists of n vertices with exactly one edge between each pair of distinct vertices.

- n vertices
- $\binom{n}{2}$ edges

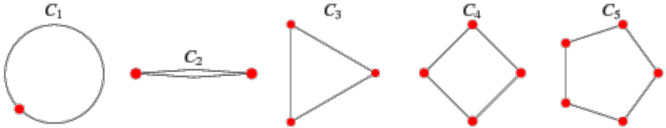


Special Graphs

Cycle

The cycle, denoted by C_n for $n \geq 3$, consists of:

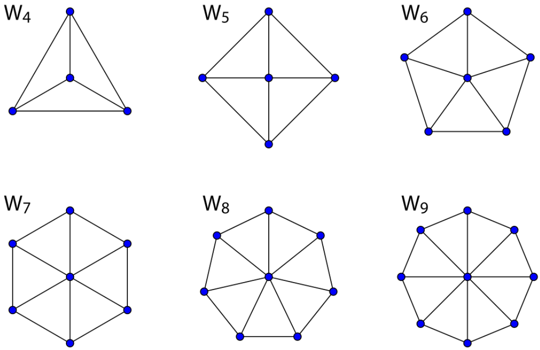
- n vertices $v_1, v_2, \ldots, v_n$
- edges $v_1 v_2, v_2 v_3, \ldots, v_{n-1} v_n$



Special Graphs

Wheel

The wheel, denoted by W_n for $n \geq 3$, consists of C_n and another vertex v_0 adjacent to each of the vertices in C_n.

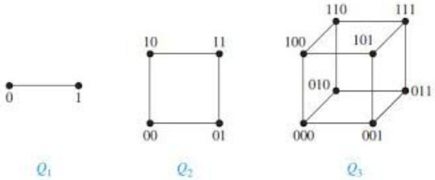


Special Graphs

n-cube

The n-cube, denoted by Q_n, has 2^n vertices labelled with 2^n bit strings of length n.

- Two vertices are adjacent if and only if their labels differ in exactly one place (e.g. the vertex 011 is adjacent to vertex 010 and vertex 111 in a Q_3 graph).
- Note that 2^n bit strings are a string of length n made up of 0's and 1's.
- Q_n has n x 2^{n-1} edges (by the Handshaking Lemma).



Bipartite Graph

Definition

A simple graph where the vertices can be partitioned into **two disjoint, non-empty sets** and no two vertices in the same set are adjacent.

- A graph is bipartite if and only if there are no odd cycles.

Useful conclusions

- C_n is bipartite if and only if n is even
- W_n is NEVER bipartite
- Q_n is ALWAYS bipartite

Tips

Try redrawing the graph isomorphically to test if a graph is bipartite.

Complete Bipartite Graph

Definition

A simple bipartite graph with vertices partitioned sets V_1 and V_2, where:

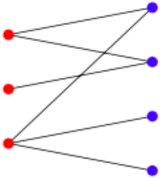
- V_1 has m vertices and V_2 has n vertices
- Every vertex in V_1 is connected to every vertex in V_2

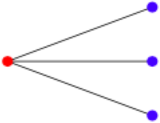
A complete bipartite graph is denoted by $\mathbf{K_{m,n}}$ with $\mathbf{m+n}$ **vertices** and **mn edges**.

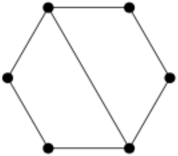
Extra content

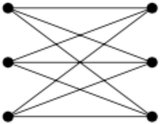
Tripartite/Complete tripartite graphs have vertices partitioned into three disjoint, non-empty sets.

Bipartite Graphs

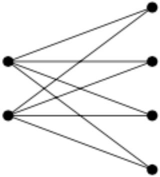








$K_{3,3}$



$K_{2,4}$

Complementary Graph

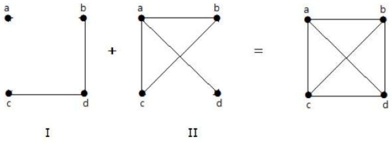
Definition

Given a simple graph G, the complement denoted by $\overline{G}$ consists of:

- the same vertices as G
- an edge between vertices if and only if the vertices are NOT adjacent in G

Tips

Edges that you don't have in G, you will have in $\overline{G}$.



Paths and Circuits

Walks

A **walk** is a finite sequence of alternating vertices and edges

$$v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n$$

where each edge e_i is incident on two vertices v_{i-1} and v_i.

- **Length** of a walk is equal to the number of edges (n edges), and has $n+1$ vertices.
- A **closed walk** begins and ends at the same vertex.

Paths and Circuits

Paths

A **path** is a walk in which ALL edges are different.

- A **simple path** exists if there are no repeated vertices.

Circuits

A **circuit** is a path which begins and ends at the same vertex.

- A **simple circuit** exists if there are no repeated vertices except for the first and last vertex.

Paths and Circuits

Theorem

Let a, b be vertices in G. There is a walk from a to b if and only if there is a simple path from a to b.

Corollary

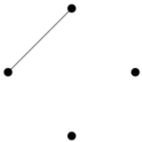
Let G be a graph with n vertices. If there is a walk from a to b then there is a walk of length **at most** $n-1$ from a to b.

Connected Graph

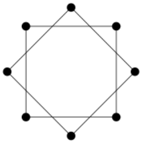
Definition

G is connected if there is a walk between any two distinct vertices of G. The **connected components** is G are its maximal connected subgraphs.

- A connected graph has only one connected component.



G



H

Euler circuit/path

Let G be a graph.

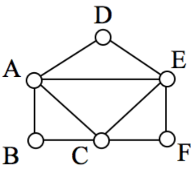
Euler circuit

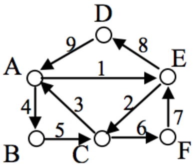
An Euler circuit in G is a circuit containing **every edge** of G **exactly once**.

- Begins and ends at the same vertex

Euler path

An Euler path in G is a path containing **every edge** of G **exactly once**.





Theorems for Euler circuit/path

Let G be a connnected graph.

Existence of an Euler circuit

If every vertex in G has an **even degree**, then G has an Euler circuit.

Existence of an Euler path

Let a and b be distinct vertices of G. A Euler path from a to b exists if and only if **a, b are of odd degree** and **every other vertex of G is of even degree**.

Hamilton circuit/path

Let G be a graph.

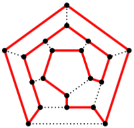
Hamilton circuit

A Hamilton circuit in G is a circuit containing **every vertex** of G **exactly once**.

- Begins and ends at the same vertex

Hamilton path

An Hamilton path in G is a path containing **every vertex** of G **exactly once**.



Theorems for Hamilton circuit/path

Note

There's no simple method of determining if a Hamilton circuit/path exists.

Let G be a connnected graph with n vertices, $n \geq 3$.

Sufficient condition for a Hamilton circuit (Dirac's Theorem)

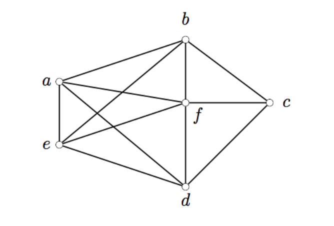
G has a Hamilton circuit if $deg(v) \geq \frac{1}{2}n$ for each $v \in V$.

- THE CONVERSE IS FALSE!
- E.g. C_5.

Example

2018 Semester 2 Q2 (iii)

Consider the following graph G.



1. Does G have a Euler path? Explain your answer.
2. Does G have a Hamilton circuit? Explain your answer.
3. Is G bipartite? Explain your answer.

Adjacency Matrix

Definition

Given a graph G with vertices $v_1, v_2, \ldots, v_n$, the adjacency matrix is the n x n matrix $A = [a_{i,j}]$ with:

$$a_{i,j} = \text{number of edges with endpoints } v_i \text{ and } v_j.$$

- A is symmetric
- A for a simple graph has elements 1 and 0 only, and diagonal entries are 0.

Note

A changes depending on the order of vertices. Make sure to specify the order of vertices.

Incidence Matrix

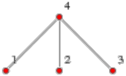
Definition

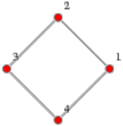
Given a graph G with vertices $v_1, v_2, \ldots, v_n$ and edges $e_1, e_2, \ldots, e_m$, the incidence matrix is the n x m matrix $M = [m_{i,j}]$ with:

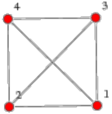
$$m_{i,j} = \begin{cases} 1 & \text{if } e_j \text{ is incident on } v_i \\ 0 & \text{if otherwise} \end{cases}$$

- Two edges are parallel if the two columns have the same entries
- An edge is a loop if there is only one entry of element 1 in the column
- A vertex is isolated if it is a 0 row

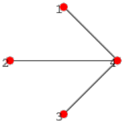
Matrices

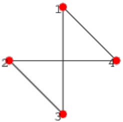


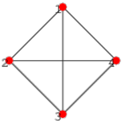




$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$







$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Interpreting Adjacency Matrices

Let G be a graph with the ordered vertices $v_1, v_2, \ldots, v_n$, and adjacency matrix A.

Counting walks theorem

The **number of walks** of length k from v_i to v_j is the (i, j) element of A^k.

- Proof by induction.

Adjacency matrix of a connected graph

Let $C = I + A + A^2 + \cdots + A^{n-1}$. G is connected if and only if C has no 0 entries.

Isomorphism

Definition

Let G_1 and G_2 be two graphs with vertex sets V_1 and V_2, and edge sets E_1 and E_2 respectively. G_1 and G_2 are isomorphic if there exist bijections

$$f : V_1 \to V_2 \text{ and } g : E_1 \to E_2$$

where $e \in E_1$ is incident on $v \in V_1$ iff $g(e)$ is incident on $f(v)$.

Isomorphism for simple graphs

Let G_1 and G_2 be two simple graphs with vertex sets V_1 and V_2, and edge sets E_1 and E_2 respectively. G_1 and G_2 are isomorphic if there exists a bijection $f : V_1 \to V_2$ which preserves adjacency.

- a is adjacent to b in G_1 iff $f(a)$ is adjacent to $f(b)$ in G_2.

Isomorphic invariants

If a graph G is isomorphic to a graph H with property P, then G also has property P. P is called an isomorphic invariant.

Some invariants

- number of vertices
- number of edges
- sum of degrees
- number of vertices of a given degree
- number of circuits of given length
- connectivity
- being bipartite
- existence of Euler circuit/Hamilton circuit

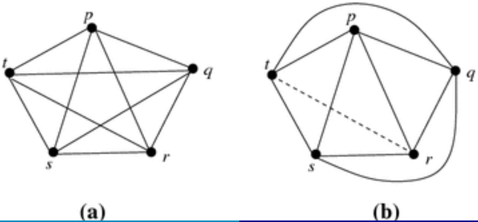
Planar Graphs

Definition

A graph G is planar iff it can be drawn with no intersecting edges. This is called a **planar map/planar representation**.

Regions

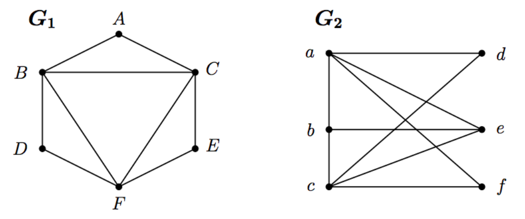
- The edges of a planar map separate a plane into finite regions, with exactly one unbounded region.
- The **degree of a region** is the number of edges bounding the region.



Example

2018 Semester 1 Final Q2 (iv)

Consider the graphs G_1 and G_2.



1. Does G_1 contain a Euler circuit? Explain your answer.
2. Is G_2 planar? Explain your answer.
3. Are G_1 and G_2 isomorphic?. Explain your answer.
4. Does G_2 contain a Hamilton cycle? Explain your answer.

Dual

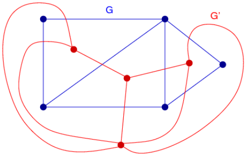
Dual of a Planar Graph

The dual of a planar graph G is a planar map G^* with:

- a vertex v_R in G^* that corresponds to each region R of G.
- an edge e^* of G^* joining a pair of vertices, such that an edge e of G lies between regions R, R' iff e^* is incident with v_R, v'_R.

Fun Facts

- Dual of a planar graph is also planar, and has the same number of edges as the original graph.
- $\sum deg(V) = \sum deg(R) = 2e$



Theorems for Planar Graphs

Euler's formula

Let G be a connected planar graph with r regions, e edges and v vertices.

$$r + v = e + 2$$

Proof by induction on e.

Inequalities

Let G be a **simple** connected planar graph with v vertices and e edges. Then,

$$e \leq 3v - 6.$$

If G has no circuits of length 3, then

$$e \leq 2v - 4.$$

Example

2014 Semester 1 Final Q2 (iv)

1. State Euler's formula for a connected planar graph having v vertices, r regions and e edges.
2. Show that if G is a connected planar simple graph with $v \geq 3$, then
$$e \leq 3v - 6.$$
3. Hence show that a connected planar simple graph with $v \geq 3$ has at least one vertex of degree less than or equal to 6.

Kuratowski's Theorem

Theorem

A graph is planar iff it has no subgraph

- K_5
- $K_{3,3}$
- any graph homeomorphic to K_5 or $K_{3,3}$

Note: Homeomorphic graphs are obtained by adding vertices of degree 2 onto existing edges.

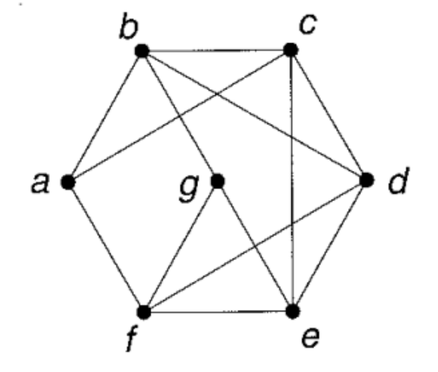
Trial and error

Using this theorem to show a graph is not planar takes a lot of trial and error in deleting edges and redrawing the graph...

Example

2019 Term 2 Final Q1 (iv)

Show that the following graph is NOT planar.



Trees

Definition

A connected graph with no circuits of length 1 or more.

Theorems regarding trees:

Trees and paths

A graph is a tree if and only if there exists a unique simple path between any two vertices.

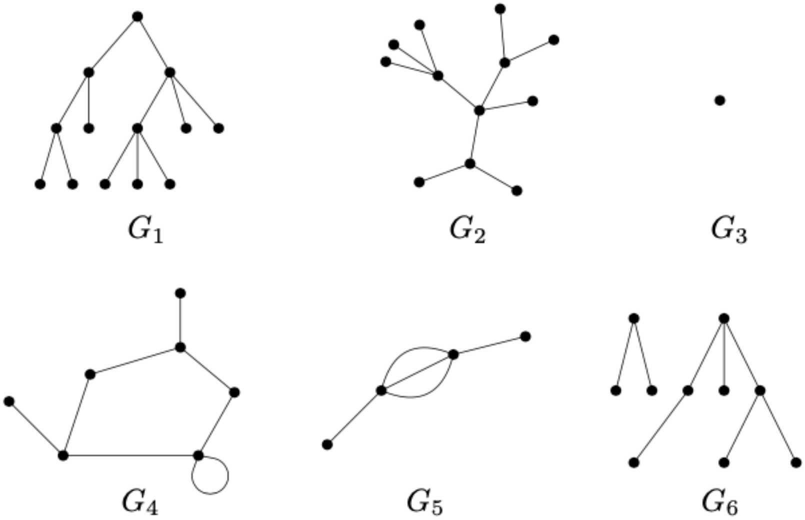
Vertices of Trees

Any tree with n vertices has at least two vertices of degree 1. $(n \geq 2)$

Edges of Trees

Any tree with n vertices has $n-1$ edges. The converse is also true but only for connected graphs.

Which of these are trees?



Example

2015 Semester 1 Final Q2 (v)

Prove that the average vertex degree

$$\frac{1}{n} \sum_{v \in V(T)} d(v)$$

of a tree T on $|V(T)| = n$ vertices is strictly less than 2.

Minimisation

Definitions

- Each edge of a **weighted graph** has a real number $w(e)$ called the **weight** of the edge associated with it.
- A **spanning tree** is a subgraph of a graph G which contains every vertex of G.
- A **minimal spanning tree** is a spanning tree for a weighted graph which has the *least possible sum of weights of its edges*.

Kruskal's algorithm

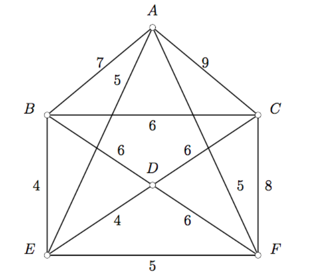
This algorithm is used to produce a minimal spanning tree for a given weighted graph G.

Method

1. Start with a graph T with the same vertices as G but no edges.
2. Sort the edges into increasing order of weight.
3. Select the smallest weighted edge. Add this edge to T if it doesn't create a circuit.
4. Continue to the next smallest weighted edge and repeat step 3.
5. When all the vertices of T are connected, you should have a minimal spanning tree.

Example

2018 Semester 2 Final Q2 (iv)



Use Kruskal's algorithm to construct a minimal spanning tree T for the following weighted graph. Make a table showing the details of each step.

Shortest Path Problem

Definitions

- The **weight of a path** is the sum of the weights of the edges in the path.
- The **distance** $d(u, v)$ is the minimum weight of any path from u to v.
- The **shortest $\mathbf{v_0}$- path spanning tree** has the property:
  - The path in the tree from v_0 to every vertex v has no greater weight than any other path from v_0 to v.

BEWARE

Make sure you know the difference between minimal spanning tree and shortest path problems.

Dijkstra's Algorithm

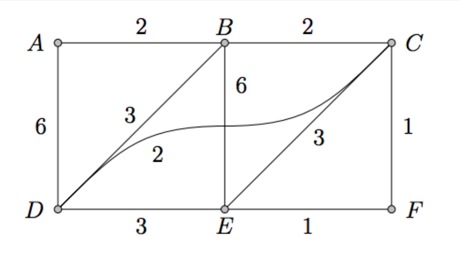
This algorithm is used to produce a shortest v_0-path spanning tree for a given weighted graph G.

Method

1. Start with a graph T with vertex v_0 only and no edges.
2. Consider all edges with one vertex in T and one vertex v NOT in T.
3. Choose the edge that gives a shortest path from v_0 to v.
4. Add this edge and v to T, provided it doesn't create a circuit.
5. Repeat steps $2-4$ until T contains all vertices of G.

Example

2019 Term 1 Final Q3 (iv)



1. Use Djikstra's algorithm to find a spanning tree that gives the shortest paths from A to every other vertex of the graph. Make a table showing the details of each step.
2. Is this spanning tree found in part 1 a minimal spanning tree? Explain your answer.

Tips and Tricks

Relations

- Set out your proofs carefully and clearly to avoid losing easy marks.
- Be careful when drawing your Hasse diagram.

Graph Theory

- This section of discrete is VERY content heavy, so make sure you know your definitions!
- Since there are a lot of theorems and algorithms, don't confuse them.
- Proofs for the theorems aren't usually tested in the exam, but it's best to know an overview of the derivation.
- May ask you to give the definition or state a theorem.