MATH1064 Cheatsheet

Abyan Majid

View on GitHub

1 Logic, inference, and proof **2**
- 1.1 Truth tables . . . 2
- 1.2 Logical equivalences . . . 2
- 1.3 Equivalences for conditionals and biconditionals . 2
- 1.4 Equivalences for quantifiers . . . 2
- 1.5 Contrapositive, converse, and inverse of conditional statements . . . 2
- 1.6 Negation of quantifiers . . . 2
- 1.7 Rules of inference . . . 3
- 1.8 Rules of inference for quantified statements . . . 3
- 1.9 Proof methods . . . 3
- 1.10 Without loss of generality (WLOG) . . . 4

2 Sets, functions, sequences, sums **4**
- 2.1 Union, intersection, difference, complement, subset 4
- 2.2 Set identities and their logic counterparts . . . 4
- 2.3 Cardinality, power set, and cartesian product of sets 4
- 2.4 Proof methods for set equivalences . . . 4
- 2.5 Domain, codomain, preimage, image, range of functions . . . 4
- 2.6 Injective, surjective, bijective, and composite functions . . . 5
- 2.7 Proving injection, surjection, and non-existent functions . . . 5
- 2.8 Arithmetic and geometric sequences, and recurrence . . . 5
- 2.9 Fibonacci and factorials sequences . . . 5
- 2.10 Summation notation . . . 5
- 2.11 Summation definitions . . . 6

3 Number theory **6**
- 3.1 Addition, multiplication, and transitivity theorems of divisibility . . . 6
- 3.2 Quotient-Remainder theorem . . . 6
- 3.3 Expressions for quotient and remainder . . . 6
- 3.4 Lemma: bounds for divisors . . . 6
- 3.5 Congruence definition . . . 6
- 3.6 Congruence theorems . . . 6
- 3.7 Definitions and theorems for primes . . . 7
- 3.8 GCD and LCM definitions . . . 7
- 3.9 Finding GCD and LCM via prime factorization . 7
- 3.10 Finding GCD via Euclidean algorithm *(Credits: Anthony Cheung)* . . . 7
- 3.11 Verifying prime using trial division . . . 7

4 O-Notation, mathematical induction, recursion **8**
- 4.1 Big O, Big Ω, Big Θ . . . 8
- 4.2 Big O complexity order . . . 8
- 4.3 Some O-Notation properties . . . 8
- 4.4 Triangle inequality . . . 8
- 4.5 Induction - intuition and definition . . . 9
- 4.6 Template for induction . . . 9
- 4.7 Template for closed formula . . . 9
- 4.8 Template for linear homogeneous recurrence relation 9

5 Counting **10**
- 5.1 Product, sum, subtraction, divison rules . . . 10
- 5.2 Relevant applications of the product rule . . . 10
- 5.3 Tree diagrams . . . 10
- 5.4 Permutation: definition, theorem, corollaries . . . 10
- 5.5 Combination: definition, theorem, corollary . . . 11
- 5.6 Choosing k elements from n + order and repetition 11
- 5.7 Binomial theorem . . . 11
- 5.8 Pascal's identity and triangle . . . 11
- 5.9 Inlusion-exclusion . . . 12
- 5.10 Pigeonhole principle + generalized form . . . 12
- 5.11 Catalan numbers, balanced strings, dyck paths . 12

6 Discrete probability **13**
- 6.1 Discrete probability, compementary and union . . 13
- 6.2 Conditional probability, independent events . . . 13
- 6.3 Probability distribution, random variables . . . 14
- 6.4 Bayes' theorem . . . 14
- 6.5 Expected value, variance + useful identities . . . 14

7 Relations **15**
- 7.1 Relation definition, notation, complementary . . 15
- 7.2 Reflexivity, symmetry, transitivity, antisymmetry 15
- 7.3 Combining and composing relations . . . 15
- 7.4 Equivalence relation and class . . . 15
- 7.5 Partitions . . . 15
- 7.6 Partial and total orders . . . 16
- 7.7 Reflexive, symmetric, and transitive closures . . . 16

8 Graph theory **16**
- 8.1 Graph terminologies . . . 16
- 8.2 Handshake theorem . . . 18
- 8.3 Matrices, matrix multiplication, adjacency matrix 18
- 8.4 Graph isomorphism . . . 19

1 Logic, inference, and proof

1.1 Truth tables

p	q	**NOT** p $\neg p$	p **AND** q $p \wedge q$	p **OR** q $p \vee q$	p **XOR** q $p \oplus q$	**IF** p **THEN** q $p \to q$	q **IF AND ONLY IF** p $p \iff q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

1.2 Logical equivalences

Logical equivalence	**Name of law**
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	Commutative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Universal bound laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws
$\neg(\neg p) \equiv p$	Double negation law
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws

1.3 Equivalences for conditionals and biconditionals

Logical equivalence	**Description**
$p \to q \equiv \neg p \vee q$	Expressing $p \to$ as $\neg p \vee$
$p \iff q \equiv (p \to q) \wedge (q \to p)$	Expressing $\iff$ as a conjunction of conditionals

1.4 Equivalences for quantifiers

Logical equivalence	**Description**
$\forall x \in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n)$	Expressing $\forall$ as a conjunction of predicates
$\exists x \in D : P(x) \equiv P(x_1) \vee P(x_2) \vee ... \vee P(x_n)$	Expressing $\exists$ as a disjunction of predicates

1.5 Contrapositive, converse, and inverse of conditional statements

Given a conditional statement $p \to q$	
Contrapositive	$\neg q \to \neg p$
Converse	$q \to p$
Inverse	$\neg p \to \neg q$

1.6 Negation of quantifiers

Given	Negation
$\forall x \in D, P(x)$	$\exists x \in D : \neg P(x)$
$\exists x \in D : P(x)$	$\forall x \in D, \neg P(x)$

1.7 Rules of inference

Rule of inference	**Name**
$\dfrac{p \quad p \to q}{\therefore q}$	Modus ponens
$\dfrac{\neg q \quad p \to q}{\therefore \neg p}$	Modus tollens
$\dfrac{p \to q \quad q \to r}{\therefore p \to r}$	Hypothetical syllogism
$\dfrac{p \lor q \quad \neg p}{\therefore q}$	Disjunctive syllogism
$\dfrac{p}{\therefore p \lor q}$	Addition/generalization
$\dfrac{p \land q}{\therefore p}$	Simplification/specialisation
$\dfrac{p \quad q}{\therefore p \land q}$	Conjunction
$p \lor q$ $\neg p \lor r$	Resolution

1.8 Rules of inference for quantified statements

Rule of inference	**Name**
$\dfrac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for arbitrary } c}{\therefore \forall x P(x)}$	Universal generalisation
$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some } c}{\therefore \exists x P(x)}$	Existential generalisation

1.9 Proof methods

Name of proof	**Step-by-step procedure**	**Effective use case**
Direct proof	To prove $p \to q$: 1. assume p is true 2. show that q must also be true otherwise $p \to q$ is false since $\mathbf{T} \to \mathbf{F} \equiv \mathbf{F}$	When given a statement in the form $p \to q$
Proof by contraposition	Since $p \to q \equiv \neg q \to \neg p$, to prove $p \to q$: 1. assume $\neg q$ is true 2. show that $\neg p$ must also be true otherwise $\neg q \to \neg p$ is false since $\mathbf{T} \to \mathbf{F} \equiv \mathbf{F}$, and therefore $p \to q$ is false.	When given a statement in the form $p \to q$, and direct proof failed.
Proof by contradiction	To prove p, 1. assume $\neg p$ is true 2. show that $\neg p$ leads to a contradiction, i.e. $\neg p \to (r \land \neg r)$. Otherwise, p is true.	When given a statement in the form p
Disproof by counterexample	To disprove $\forall x \in D, P(x)$, find one example for which $P(x)$ is false.	When given state- -ments with universal quantifiers.
Proof by cases	To prove $\forall x \in D, P(x)$, 1. identify all cases for which the truthness/falsity of P(x) may vary. 2. make assumptions WLOG where necessary 3. show that all cases prove $P(x)$ true/false.	When it appears that you can prove one example and and every other example will follow.

1.10 Without loss of generality (WLOG)

Without loss of generality (WLOG) is the act of making a simplifying assumption along the lines of: "if this simple case is true, then trivially every other cases must be true".

2 Sets, functions, sequences, sums

2.1 Union, intersection, difference, complement, subset

Name	Set operation	Description
Union	$A \cup B$	All elements that are in A or B or both
Intersection	$A \cap B$	All elements that are both in A and B
Difference	$A \setminus B$	All elements that are in A but not in B
Complement	$\overline{A}$	All elements in the universal set that are not in A
Subset	$A \subseteq B$	A is a subset of B; every element in A is also in B
Proper subset	$A \subsetneq B$	A is a subset of B and $A \neq B$.

2.2 Set identities and their logic counterparts

Set	Logic
$\cap$ (intersection)	$\wedge$ (and)
$\cup$ (union)	$\vee$ (or)
$\overline{A}$ (complement)	$\neg$ (not)
U (universal set)	**T** (tautology)
$\emptyset$ (empty set)	**F** (contradiction)

2.3 Cardinality, power set, and cartesian product of sets

Name	Operation	Description	Given $A = \{p, q\}$, $B = \{r, s\}$
Cardinality	$\lvert A\rvert$	Number of elements in A	$\lvert A\rvert = 2$
Power set (Size of set = 2^n)	$\mathcal{P}(A)$	Set of all subsets of A including the empty set	$\mathcal{P}(A) = \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$
Cartesian product (Size of set = $\lvert A\rvert \cdot \lvert B\rvert$)	$A \times B$	Set of all ordered n-tuples from A and B	$A \times B = \{(p, r), (p, s), (q, r), (q, s)\}$

2.4 Proof methods for set equivalences

To prove $A = B$, show that A ⊆ B and B ⊆ A	
Method	**Step-by-step procedure**
Element method	To prove $A \subseteq B$, 1. let $x \in A$ 2. construct worded proof with set operations to arrive at $x \in B$
Logical equivalences	To prove $A \subseteq B$, 1. let $x \in A$ 2. rewrite set operators with their logical counterparts 3. derive $x \in B$ from $x \in A$ using logical equivalences

2.5 Domain, codomain, preimage, image, range of functions

Given $f : X \to Y$		Given $f(x) = y$	
Terminology	**Description**	**Terminology**	**Description**
Domain (X)	All possible inputs for f	Preimage (x)	$x \in X$ that is mapped to some $y \in Y$ by f
Codomain (Y)	All possible outputs for f	Image (y)	$y \in Y$ to which some $x \in X$ is mapped by f

2.6 Injective, surjective, bijective, and composite functions

Function type	Definition
Injective (one-to-one)	A function $f : X \to Y$ where $\forall x \in X$, x is assigned a different $y \in Y$, and $\|X\| \leq \|Y\|$.
Surjective (onto)	A function $f : X \to Y$ where all $\forall y \in Y$, y is an image of some $x \in X$, and $\|X\| \geq \|Y\|$.
Bijective (one-to-one correspondence)	A function that is both injective and surjective, where $\|X\| = \|Y\|$
Composite	A function $(f \circ g)(a) = f(g(a))$ where a function f takes another function g as input.

2.7 Proving injection, surjection, and non-existent functions

What to prove	How to prove
$f : X \to Y$ is injective	1) If a graph of f is given or derivable, commit horizontal line test 2) Alternatively, show that if $f(x_1) = f(x_2)$ for arbitrary $x_1, x_2 \in X$ with $x_1 \neq x_2$, then $x_1 = x_2$.
$f : X \to Y$ is NOT injective	Show that $\exists x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$
$f : X \to Y$ is surjective	Show that $\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}$ such that $f(x) = y$
$f : X \to Y$ is NOT surjective	Show that $\exists y \in Y$ such that $\forall x \in X$, $f(x) \neq y$
$f : X \to Y$ is not a function	1) If a graph of f is given or derivable, commit vertical line test if there exists a vertical line that intersects the graph more than once, then f is not a function. 2) If the expression for f is given, make y the subject and prove algebraically that there are more than one value for y.

2.8 Arithmetic and geometric sequences, and recurrence

Name of sequence	Definition	n-th Term	Series
Arithmetic sequence	$\{a, a + d, a + 2d, ..., a + nd\}$, where a is the initial term and d is difference	$a_n = a_1 + (n - 1)d$	$S_n = n(\frac{a_1 + a_n}{2}))$
Geometric sequence	$\{a, ar, ar^2, ..., ar^n\}$, where a is the initial term and r is common ratio	$a_n = ar^{n-1}$	$S_n = a_1(\frac{1 - r^n}{1 - r})$

2.9 Fibonacci and factorials sequences

Name of sequence	Definition
Fibonacci sequence	a sequence $\{f_0, f_1, f_2\}$ defined by initial conditions $f_0 = 0$, $f_1 = 1$ and the recurrence relation $f_n = f_{n-1} + f_{n-2}$ for $n = 2, 3, 4, ...$
Factorials sequence	$(n!)_{n\geq 0} = \{1, 1, 2, 6, 24, 120, ...\}$, or defined recursively as $0! = 1$, $n! = (n - 1)! \times n$ for $n \geq 1$

2.10 Summation notation

To represent the sum of some sequence $a_m + a_{m+1} + ... + a_n$, we write: $\sum_{i=m}^{n} a_i$

2.11 Summation definitions

Property	Definition
Addition/subtraction over the same range	$\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_i = \sum_{i=m}^{n} (a_i \pm b_i)$
Taking out a common factor	$\sum_{i=m}^{n} ca_i = c \sum_{i=m}^{n} a_i$
Combining consecutive indices	$\sum_{i=p}^{q} a_i + \sum_{i=q+1}^{r} a_i = \sum_{i=p}^{r} a$ if $p \leq q \leq r$
Index shift	$\sum_{i=m}^{n} a_i = \sum_{i=m+p}^{n+p} a_{i-p} = \sum_{i=m-q}^{n-q} a_{i+q}$
Telescoping sums	$\sum_{i\,=\,m}^{n} (a_i - a_{i+1}) = a_m - a_{n+1}$ if $m \leq n$

3 Number theory

3.1 Addition, multiplication, and transitivity theorems of divisibility

Theorem	Definition
Addition	If $a\|b$ and $a\|c$, then $a\|(b+c)$
Multiplication	If $a\|b$, then $a\|bc$ for all $c \in \mathbb{Z}$
Transitivity	If $a\|b$ and $b\|c$, then $a\|c$

3.2 Quotient-Remainder theorem

Quotient-Remainder Theorem
Given integer $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exists Two unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

3.3 Expressions for quotient and remainder

Expressions for quotient (q) and remainder (r)
$q = a \textbf{ div } d = \lfloor \frac{a}{d} \rfloor$ $r = a \textbf{ mod } d = a - (d \times \lfloor \frac{a}{d} \rfloor)$

3.4 Lemma: bounds for divisors

Bounds for divisors
Let $n, d \in \mathbb{Z}$. If $\|n\| \geq 1$ and $d\|n$, then $0 < \|d\| \leq \|n\|$

3.5 Congruence definition

Congruence
$a \equiv b \pmod{m}$ denotes that a is congruent to $b \pmod{m}$ if and only if $m\|(a-b)$

3.6 Congruence theorems

Theorem 1
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a and b are congruent modulo m if and only if $\exists k \in \mathbb{Z}$ such that $a = b + km$

Theorem 2
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

3.7 Definitions and theorems for primes

Name	Definition
Prime number	Given $p \in \mathbb{Z}$ with $p > 1$, p is prime if the only positive factors of p are 1 and p.
Fundamental theorem of arithmetic	$\forall x \in \mathbb{Z}$ where $x > 1$, x can be written uniquely as a prime, or as a product of 2 or more primes where the prime factors are written in order of nondecreasing size.
Composite integer	$k \in \mathbb{Z}^+$ is a composite integer if $\exists a, b \in \mathbb{Z}^+$ where $a < k$ and $b < k$, such that $k = ab$.
Relatively prime	Let $a, b \in \mathbb{Z}$, a and b are realtively prime if $\gcd(a, b) = 1$
Pairwise relatively prime	$a_1, a_2, ..., a_n \in \mathbb{Z}$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i \leq j \leq n$

3.8 GCD and LCM definitions

Name	Definition
Greatest Common Divisor	Let $a, b \in \mathbb{Z}$ where $a \neq 0$ and $b \neq 0$. The GCD of a and b, denoted $\gcd(a, b)$ is d such that $d \mid a$ and $d \mid b$
Least Common Multiple	The LCM of a and b, denoted $\mathrm{lcm}(a, b)$, is the smallest $k \in \mathbb{Z}^+$ such that $a \mid k$ abd $b \mid k$
Relationship between GCD and LCM of $a, b \in \mathbb{Z}$	$ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$

3.9 Finding GCD and LCM via prime factorization

Suppose the prime factorization of $a, b \in \mathbb{Z}$ are:

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_n^{a_n}$$
$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_n^{b_n}$$

What to find	How
GCD	$\gcd(a, b) = (P_1^{\min(a_1, b_1)})(P_2^{\min(a_2, b_2)})...(P_n^{\min(a_n, b_n)})$
LCM	$\mathrm{lcm}(a, b) = (P_1^{\max(a_1, b_1)})(P_2^{\max(a_2, b_2)})...(P_n^{\max(a_n, b_n)})$

3.10 Finding GCD via Euclidean algorithm *(Credits: Anthony Cheung)*

Euclidean algorithm	
Step	**What to do**
1	Calculate $a \div b$ to find quotient q and remainder r that satisfy $a = bq + r$
2	Case I. If $r = 0$, then conclude that $\gcd(a, b)$= b
3	Case II. Else if $r \neq 0$, then repeat steps 1 and 2 but calculate $\gcd(b, r)$ instead

Example: $\gcd(345, 92)$= 23

$$\begin{array}{ccccccc}
\textit{dividend} & & \textit{divisor} & & \textit{quotient} & & \textit{remainder} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
345 & = & 92 & \times & 3 & + & 69 \\
92 & = & 69 & \times & 1 & + & 23 \\
69 & = & 23 & \times & 3 & + & 0 \\
 & & \uparrow & & & & \uparrow \\
 & & \text{gcd} & & & & \textit{STOP}
\end{array}$$

3.11 Verifying prime using trial division

Trial divison
Given $a \in \mathbb{Z}$, a is prime, if for all primes $k \leq \sqrt{a}$, $k \mid a$.

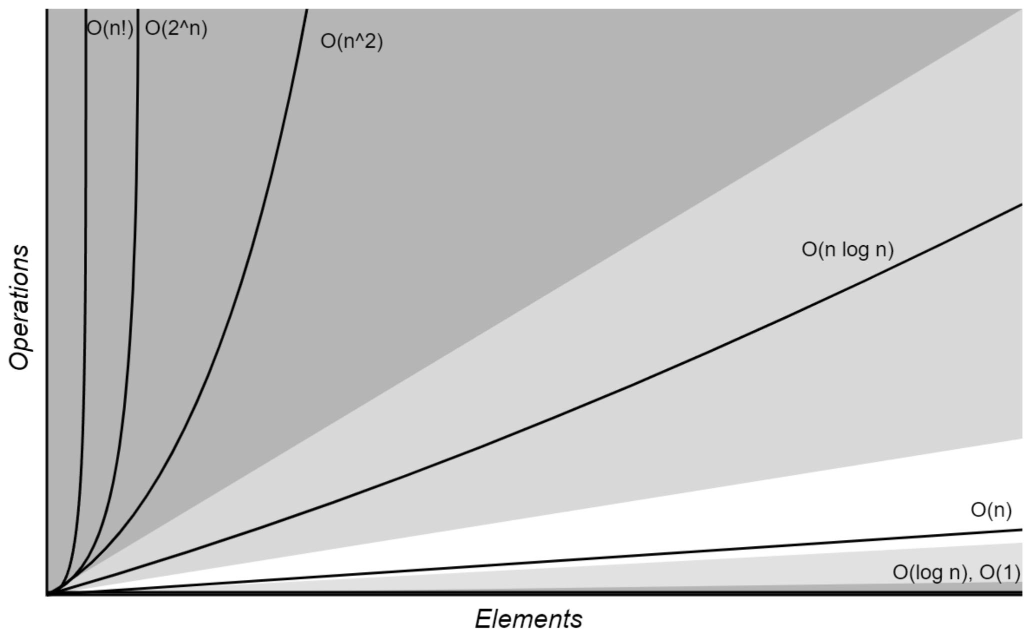
4 O-Notation, mathematical induction, recursion

4.1 Big O, Big Ω, Big Θ

O-Notation	**Definition**
Worst-case complexity (O) *"$f(x)$ grows SLOWER than $g(x)$"*	$f(x)$ is $O(g(x))$ if and only if $\forall x > k, \lvert f(x)\rvert \leq C\lvert g(x)\rvert$, for some constants C and k.
Best-case complexity (Ω) *"$f(x)$ grows FASTER than $g(x)$"*	$f(x)$ is $\Omega(g(x))$ if and only if $\forall x > k, \lvert f(x)\rvert \geq C\lvert g(x)\rvert$, for some positive constants C and k.
Average-case complexity (Θ) *"$f(x)$ grows at the SAME RATE as $g(x)$"*	$f(X)$ is $\Theta(g(x))$ if and only if $f(x) \in O(g(x))$ and $f(x) \in \Omega(g(x))$. That is, $C_1\lvert g(x)\rvert \leq \lvert f(x)\rvert \leq C_2\lvert g(x)\rvert$ for positive constants C_1, C_2, k

4.2 Big O complexity order

Big O complexity order
$O(1) < O(\log(n)) < O(n) < O(n\log(n)) < O(n^2) < O(2^n) < O(n!)$



4.3 Some O-Notation properties

#	**Property**
1	$f(n) \in O(f(n))$
2	$O(c \cdot f(n)) = O(f(n))$
3	$O(f(n) + f(n)) = O(f(n))$
4	$O(f(n)g(n)) = f(n) \cdot O(g(n))$

4.4 Triangle inequality

Triangle inequality
$\lvert a + b\rvert \leq \lvert a\rvert + \lvert b\rvert$ Useful for problems in the form $a + b \in O(g(n))$, $a + b \in \Omega(g(n))$, or $a + b \in \Theta(g(n))$

4.5 Induction - intuition and definition

Point	Explanation
Intuition	Suppose we have a ladder, and (1) We can reach the first rung of the ladder *#BASIS* (2) If we can reach a particular rung of the ladder, then we can reach the next rung *#INDUCTIVE HYPOTHESIS* *#INDUCTION:* By (1), we can reach the first rung. By (2), since we can reach the first rung, then we can reach the second rung. Then by (2) again, since we can reach the second rung, then we can reach the third rung. Repeating (2), we can show that we can reach the fourth rung, the fifth, and so on.
Definition	To prove $\forall n \in \mathbb{Z}^+, P(n)$, we complete two steps: (1) Basis step: Verify that $P(1)$ is true (2) Inductive step: Show that $\forall k \in \mathbb{Z}^+, P(k) \rightarrow P(k+1)$. To do this you assume $P(k)$ is true (inductive hypothesis). Then, show that if $P(k)$ is true, then $P(k+1)$ must also be true.

4.6 Template for induction

Step	What to do
1	Express statement to be proved in the form "$\forall n \geq b, P(n)$ for a fixed b"
2	BASIS STEP: Show that $P(b)$ is true
3	INDUCTIVE STEP: (3.1) State inductive hypothesis in the form "assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$" (3.2) State what $P(k+1)$ says, ie. what needs to be proved under inductive hypothesis (3.3) Prove $P(k+1)$ using assumption $P(k)$
4	State the conclusion, e.g. "$\therefore$ By induction, $\forall n \in \mathbb{Z}^+$ with $n \geq b$, $P(n)$."

4.7 Template for closed formula

Step	What to do
1	BASIS STEP: Verify initial conditions for which T_n is true
2	INDUCTIVE STEP: (2.1) Rewrite T_{k+1} in terms of previous terms, eg. T_k (2.2) Use the inductive hypothesis T_k to prove T_{k+1}

4.8 Template for linear homogeneous recurrence relation

Given a linear homogeneous recurrence relation $a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + ... + \alpha_k a_{n-k}$	
Step	**What to do**
1	Get characteristic polynomial: $x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - ... - \alpha_k x^0 = 0$
2	Factor: $x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - ... - \alpha_\ell x^0 = (x - \lambda_1)(x - \lambda_2)...(x - \lambda_k)$
3	Write roots as sum with coefficients determined by the initial conditions (3a) For any roots λ_a and λ_b, if $\lambda_a \neq \lambda_b$, write their sum as $A\lambda_a^n + B\lambda_b^n$ for constants A, B (3b) For any roots λ_a and λ_b, if $\lambda_a = \lambda_b$, write their sum as $(A + Bn)\lambda^n$, where $\lambda = \lambda_a = \lambda_b$, for constants A, B Initial conditions of the recurrence relation determine constants $A, B, ...$
4	Repeating step (3) until the last term and write the general solution **Example:** Given recurrence relation of order 4 with factors in step (2) $\lambda_1 = \lambda_2 \neq \lambda_3 \neq \lambda_4$, the general solution is given by $a_n = (A + Bn)\lambda^n + C\lambda_3^n + D\lambda_4^n$, where $\lambda = \lambda_1 = \lambda_2$, for consants A, B, C, D

5 Counting

5.1 Product, sum, subtraction, divison rules

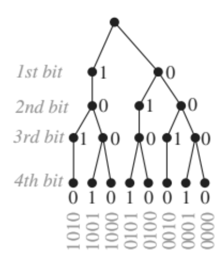
Rule	Definition
Product rule	Given a procedure with two tasks, where 1. The first task can be done in n_1 ways 2. The second task can be done in n_2 ways The total number of ways to do the procedure is $n_1 \times n_2$
Sum rule	Given a task that can be done in one of n_1 ways or in one of n_2, where n_1 and n_2 are mutually exclusive, then the total number of ways to do the task is $n_1 + n_2$
Subtraction rule	If a task can be done in ONLY either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2 - M$, where M is the number of ways common to both ways. In set notation: $\lvert A_1 \cup A_2\rvert = \lvert A_1\rvert + \lvert A_2\rvert - \lvert A_1 \cap A_2\rvert$
Division rule	Given a task that can be done in n ways which can be, categorized into d groups, the total number of ways to do the task is $\frac{n}{d}$ In set notation: If a set A is the union of n pairwise disjoint subsets each with d elements, then $n = \frac{\lvert A\rvert}{d}$

5.2 Relevant applications of the product rule

Example	By product rule
No. of functions from a set with n elements to a set with m elements	m^n
No. of injective functions from a set with n elements to a set with m elements	$m \times (m-1) \times (m-2) \times ... \times (n-m+1)$
No. of subsets of a finite set S	$\lvert\mathcal{P}(S)\rvert = 2^{\lvert S\rvert}$

5.3 Tree diagrams

Tree diagrams
Counting problems can sometimes be solved using tree diagrams where each branch represent a possible choice



Example: There are 8 bit strings of length 4 without consecutive 1s

5.4 Permutation: definition, theorem, corollaries

Definition of permutation
A permutation of a set of distinct objects is an ordered arrangement of these objects. An r-permutation is said to be an ordered arrangement of r elements of a set.

Useful theorem for permutation
Given $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$ with $1 \le r \le n$, the r-permutations of a set with n distinct elements is given by $P(n,r) = n \times (n-1) \times (n-2) \times \ldots \times (n-r+1)$
Corollary 1
If n and r are integers with $0 \le r \le n$, then $P(n,r) = \dfrac{n!}{(n-r)!}$
Corollary 2
$P(n,n) = n!$

5.5 Combination: definition, theorem, corollary

Definition of combination
An r-combination of elements of a set with n elements is an unoredered selection of r elements from the set. Common notations include $\binom{n}{r}$, $C(n,r)$, and ${}^nC_r$

Useful theorem for combinations
Given $n, r \in \mathbb{Z}$, where $n \ge 0$ and $0 \le r \le n$, the number of r-permutations of a set with n elements is $C(n,r) = \dfrac{n!}{r!(n-r)!}$
Corollary
Let $n, r \in \mathbb{Z}$, with $n, r \ge 0$ and $r \le n$, then $C(n,r) = C(n, n-r)$

5.6 Choosing k elements from n + order and repetition

	Order matters	Order doesn't matter
Repetition is allowed	n^k	$\binom{k+n-1}{n-1}$
Repetition is not allowed	$\dfrac{n!}{(n-k)!}$	$\binom{n}{k}$

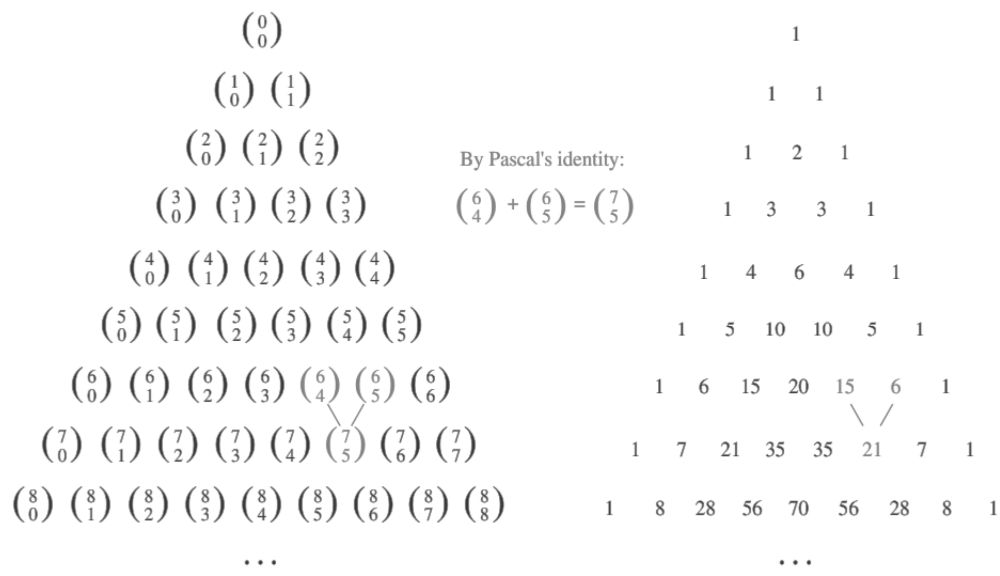
5.7 Binomial theorem

Binomial theorem
Let x and y be variables, and let n be a nonnegative integer. Then, we have: $(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$
Corollary 1
Let n be a nonnegative integer. Then, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
Corollary 2
Let $n \in \mathbb{Z}^+$. Then, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$
Corollary 3
Let n be a nonnegative number. Then, $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$

5.8 Pascal's identity and triangle

Pascal's identity
Let $n, k \in \mathbb{Z}^+$ with $n \ge k$. Then, $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Pascal's triangle



5.9 Inlusion-exclusion

Lemmas for the size of set union
No of elements in 2 sets: $\lvert A \cup B \rvert = \lvert A \rvert + \lvert B \rvert - \lvert A \cap B \rvert$ No of elements in 3 sets: $\lvert A \cup B \cup C \rvert = \lvert A \rvert + \lvert B \rvert + \lvert C \rvert - \lvert A \cap B \rvert - \lvert A \cap C \rvert - \lvert B \cap C \rvert + \lvert A \cap B \cap C \rvert$

Principle of Inclusion-Exclusion

Let $A_1, A_2, \ldots, A_n$ b finite sets. Then the size of set union of n sets is given by:

$$|A_1 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \sum_{i<j<k<\ell} |A_i \cap A_j \cap A_k \cap A_\ell| + \ldots \pm |A_1 \cap A_2 \cap \ldots \cap A_n|$$

In short, you simply follow:

1. Add the size of each set individually
2. Subtract all two-way intersections
3. Add all three-way intersections
4. Subtract all four-way intersections
5. Add all five-way intersections

And so on...

5.10 Pigeonhole principle + generalized form

Pigeonhole principle
If you have n pigeons sitting in k pigeonholes, and if $n > k$, then at least one of the pigeonholes contains at least two pigeons.

Generalised pigeonhole principle
If you have n pigeons sitting in k pigeonholes, and if $n > k \cdot m$, then at least one of the pigeonholes contains at least $m + 1$ pigeons.

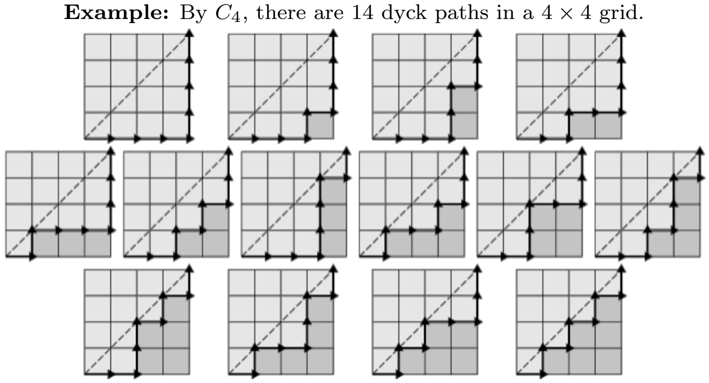
5.11 Catalan numbers, balanced strings, dyck paths

Balanced strings
A **string** is a sequence of brackets where order matters   A **balanced string** is a string where all opening bracket "(" is closed with a ")"   Examples:))((and (() not balanced, meanwhile ()() and (()) are balanced.

Catalan numbers
A sequence of natural numbers such that the n-th term is given by $C_n = \frac{1}{n+1}\binom{2n}{n}$ for $n \geq 0$ Click here for 6 proofs of the catalan numbers **First few terms:** $C_0 = 1, C_1 = 1, C_2 = 2, C_3 = 5, C_4 = 14, C_5 = 42, C_6 = 132, C_7 = 429, C_8 = 1430, ...$

Catalan numbers for balanced strings
A catalan number C_n represent all possible combinations of balanced strings with n opening brackets **Example:** By C_3, there are 5 balanced strings when there are 3 opening and 3 closing brackets, ie. ((())), ()()(), (())(), ()(()), (()())

Catalan numbers for dyck paths
A catalan number C_n represent all dyck paths in a $n \times n$ grid, ie. monotonic lattice paths that stays below the diagonal line **Example:** By C_4, there are 14 dyck paths in a 4×4 grid.



6 Discrete probability

6.1 Discrete probability, compementary and union

Basic definition for discrete probability
Let a sample space S be the set of possible outcomes, and let an event E be a subset of S. Then, the probability of event E occuring is given by $p(E) = \frac{\lvert E \rvert}{\lvert S \rvert} = \sum_{s \in E} p(s)$

Name	Definition
Complementary event	$p(\overline{E}) = 1 - p(E)$
Union of events	$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$

6.2 Conditional probability, independent events

Name	Definition
Conditional probability	Let E and F be events with $p(F) > 0$. The conditional probability E given F, is given by: $p(E\|F) = \frac{p(E \cap F)}{p(F)}$
Independent events	Events E and F are independent if and only if $p(E \cap F) = p(E)p(F)$. That is to say, E and F are NOT independent if $p(E \cap F) \neq p(E)p(F)$

6.3 Probability distribution, random variables

Name	Definition
Probability distribution	The probabilty distribution of a variable X is a function $p : S \to [0,1]$ such that $\sum_{s \in S} p(x) = 1$
Random variable	A function $X : S \to \mathbb{R}$ defined on outcomes of sample space S **Example:** Let $X(t)$ be no. of heads in 3 coin flips. Therefore $X(t)$ takes on the values: $X(HHH) = 3$ $X(HHT) = X(HTH) = X(THH) = 2$ $X(TTH) = X(THT) = X(HTT) = 1$ $X(TTT) = 0$
Distribution of a random variable	A set of pairs $(r, p(X = r))$ for all $r \in X(s)$ where $p(X = r)$ is the probability that X takes the value of r. **Example:** The distribution of random variable $X(t)$ is the set of pairs $\{(3, \frac{1}{8}), (2, \frac{3}{8}), (1, \frac{3}{8}), (0, \frac{1}{8})\}$

6.4 Bayes' theorem

Bayes' theorem
Let E, F be events from sample space S such that $p(E) \neq 0$ and $p(F) \neq 0$. Then, $p(F\|E) = \frac{p(E\|F)p(F)}{p(E\|F)p(F) + p(E\|\overline{F})p(\overline{F})}$

6.5 Expected value, variance + useful identities

Name	Definition
Expected value	The expected value of a random variable X on a sample space S is given by $E(X) = \sum_{s \in S} p(s)X(s) = \sum_{r \in X(S)} p(X = r)r$
Variance	The variance of a random variable X on a sample space S is given by $V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s)$

Useful identities for expected value and variance	
Name	**Definition**
Linearity of expectation	Let X, Y be random variables and $a, b \in \mathbb{R}$. Then, $E(X_1 + X_2 + ... + X_n) = E(X_1) + E(X_2) + ... + E(X_n)$, $E(aX + b) = aE(X) + b$
Variance	$V(X) = E(X^2) - E(X)^2 = E((X - E(X))^2)$
Expected value and variance of independent events	If X and Y are independent, then $E(XY) = E(X) \times E(Y)$ and $V(X + Y) = V(X) + V(Y)$

7 Relations

7.1 Relation definition, notation, complementary

Realtion definition, notation, complementary
A relation R from set X to set Y is a subset of $X \times Y$. The complementary relation $\overline{R}$ is given as $\overline{R} = (X \times Y) \backslash R$ Notations to express "x is related to y": • $(x, y) \in R$ • xRy • $x \sim y$

7.2 Reflexivity, symmetry, transitivity, antisymmetry

Let R be a relation on X	
Property	**Definition**
Reflexivity	R is reflexive provided that $\forall x \in X$, $(x, x) \in R$
Symmetric	R is symmetric provided that $\forall x, y \in X$, if $(x, y) \in R$, then $(y, x) \in R$
Transitive	R is transitive provided that $\forall x, y, z \in X$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$
Antisymmetry	R is antisymmetric provided that $\forall x, y \in X$, if $(x, y) \in R$ and $(y, x) \in R$, then $x = y$

7.3 Combining and composing relations

Combining and composing relations
Since relations R_1, R_2 from X to Y are just subsets of $X \times Y$, we can use set operations to create new relations e.g. $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 \backslash R_2$ **Composition of relations:** We can compose relations R from X to Y and S from Y to Z to get a new relation $S \circ R = \{(a, c) \| \exists b \in Y : aRb \wedge bSc\} \subseteq X \times Z$

7.4 Equivalence relation and class

Let R be a relation on X	
Name	**Definition**
Equivalence relation	R is an equivalence realtion on X if and only if the relation R on the non-empty set X is reflexive, symmetric, and transitive.
Equivalence class	If R is an equivalence relation on X and $x \in X$, then the set $[x] = \{y \in X \| (x, y) \in R\}$ is the equivalence class of x In simpler terms: An equivalence class is a set of numbers all of which are equal to one another under the given relation.

7.5 Partitions

Partitions
A set $\{S_1, S_2, ...\}$ is a partition of S if: (1) $S_i \neq \emptyset$ for all i (2) $S = S_1 \cup S_2 \cup S_3 \cup ...$ (3) $S_i \cap S_j = \emptyset$ where $i \neq j$ **Example:** $S = \{1, 2, 3, 4, 5\}$, $S_1 = \{1\}$, $S_2 = \{2, 5\}$, $S_3 = \{3, 4\}$ (1) $S_1 \neq \emptyset$, $S_2 \neq \emptyset$, $S_3 \neq \emptyset$ (2) $S_1 \cup S_2 \cup S_3 = \{1, 2, 3, 4, 5\} = S$ (3) $S_1 \cap S_2 = \emptyset$, $S_2 \cap S_3 = \emptyset$, $S_1 \cap S_3 = \emptyset$ $\therefore$ $\{S_1, S_2, S_3\}$ is a partition of S

7.6 Partial and total orders

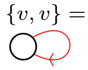
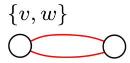
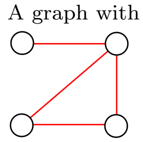
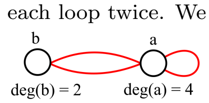
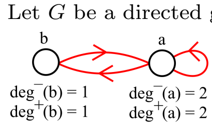
Property	**Definition**
Partial order	A relation R on a set X which is reflexive, transitive, and anti-symmetric is called a "partial order" on X.
Total order	$\forall a, b \in X$, if aRb or bRa, then R is called a "total order" on X.

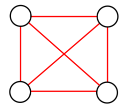
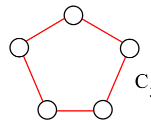
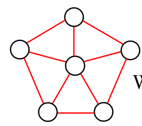
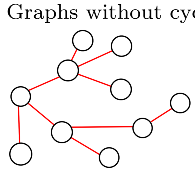
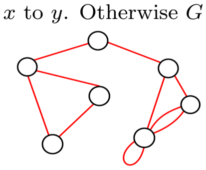
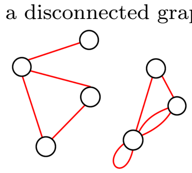
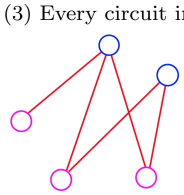
7.7 Reflexive, symmetric, and transitive closures

Closure	**How to derive**
Reflexive (ref(R))	The smallest reflexive relation containing R (i.e. ref(R)) is given by ref(R)$= R \cup \{(x,x)\|x \in X\}$, where $\triangle = \{(x,x)\|x \in X\}$ is the diagonal relation
Symmetric (sym(R))	The smallest symmetric relation containg R (i.e. sym(R)) is given by $R \cup R^{-1} = R \cup \{(y,x)\|(x,y) \in R\}$, where $R^{-1} = \{(y,x)\|(x,y) \in R\}$ is the inverse relation to R
Transitive (tra(R))	Use Warshall's algorithm: Loop over vertices (e.g. $1, 2, 3, \ldots, n$) A) Identify all incoming edges B) Identify all outgoing edges C) Connect incoming vertices to outgoing vertices Repeat loop until nothing cahnges (at most n times)

8 Graph theory

8.1 Graph terminologies

Terminology	**Definition**
Graph	A graph G is a structure comprised of 2 finite sets: - a non-empty set $V(G)$ of vertices - a set $E(G)$ of edges, where each edge is associated with a set $\{v, w\} \subseteq V(G)$ The vertices v and w are endpoints of the edge
Loop edge	$\{v, v\} = \{v\}$ 
Parallel edges	$\{v, w\}$ 
Simple graph	A graph with no loops or parallel edges 
Incidence	Edge e and vertex v are incident if v is an endpoint e
Adjecence	Vertices u, v are adjacent if there is an edge with endpoints $\{u, v\}$. A vertex u is adjacent to itself if there is a loop with endpoints $\{u\}$
Degree	Degree of a vertex v is the number of edges incident with v, where we count each loop twice. We write this as deg(v)  In simpler terms: deg(v) counts the ends of edges that meet v
Directed graph	Let G be a directed graph and $v \in V(G)$  - The **indegree** $\deg^-(v)$ is the no. of edges terminating in v. - The **outdegree** $\deg^+(v)$ is the no. of edges starting in v.

Terminology	**Definition**
Complete graph	The complete graph on n vertices is a simple graph with exactly one edge between any pair of vertices. 
Cycle	A cycle C_n for $n \geq 3$ is a graph that looks like a loop.  C_5
Wheel	You get a wheel W_n from cycle C_n by adding a vertex that connects to each of the vertices  W_5
Trees	Graphs without cycles 
Path	An alternating sequence of vertices and edges with a starting and ending vertices.
Simple path	A path with no repeating vertices
Connected & disconnected graphs	A graph G is connected if $\forall x, y \in V(G)$, there is a path from x to y. Otherwise G is a disconnected graph.  Connected  Disconnected
Circuit	A path that starts and ends at the same vertex
Eulerian circuit	A path that starts and ends at the same vertex and uses every edge exactly once Necessary conditions for an Eulerian circuit to exist: (1) If we ingore any isolated vertices (vertices with degree 0), then the remaining graph must be connected (because we must traverse all edges) (2) The degree of every vertex must be even (otherwise you will be retracing!)
Eulerian trail/path	A path that uses each path exactly once, but whose start and end vertices can be different. For it to exist, it requires exactly two vertices of odd degree
Hamiltonian circuit/cycle	circuit that traverses every vertex exactly once
Bipartite graph	A simple graph G is bipartite if it has at least 2 vertices and satisfies one (and hence all) of the following equivalent conditions: (1) The set of vertices $V(G)$ has a partition $\{V_1, V_2\}$ such that every edge is of the form $\{v_1, v_2\}$ where $v_k \in V_k$ (2) The vertices can be coloured with 2 colours such that no 2 adjacent vertices have the same colour. (3) Every circuit in G has even length. 

8.2 Handshake theorem

Handshake theorem
Let G be a graph with n vertices $V(G) = \{v_1, ..., v_n\}$ then $\sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \deg(v_2) + ... + \deg(v_n) = 2 \times \lvert E(G) \rvert$
Corollary
In any graph, the sum of all vertex degrees must be even and the number of vertices of odd degree is even.

Handshake theorem for directed graphs
Let G be a directed graph with n vertices $V(G) = \{v_1, ..., v_n\}$ then $\sum_{i=1}^{n} \deg^-(v_i) = \sum_{i=1}^{n} \deg^+(v_i) = \lvert E(G) \rvert$

8.3 Matrices, matrix multiplication, adjacency matrix

Matrix definition

Let $n_r, n_c \in \mathbb{N}$. An $n_r \times n_c$ matrix is just a $n_r \times n_c$ grid of numbers where n_r is the no. of rows and n_c is the no. of columns.

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n_c} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n_c} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n_r,1} & m_{n_r,2} & \dots & m_{n_r,n_c} \end{bmatrix}$$

Given a $n_r \times n_c$ matrix M we write $M = (m_{i,j})$ where for each $i = 1, 2, ..., n$ and $j = 1, 2, ..., n$ the symbol $m_{i,j}$ denotes the entry in row i, column j

Matrix multiplication

Let $A = (a_{i,j})$ and $B = (b_{i,j})$ be $n \times n$ matrices.
Their product AB is an $n \times n$ matrix $AB = (m_{i,j})$ with entries:

$$m_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j} = a_{i,1} b_{1,j} + \dots + a_{i,n} b_{n,j}$$

Example:

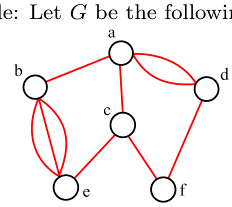
$$A = \begin{bmatrix} 1 & 2 \\ 4 & 6 \end{bmatrix}, B = \begin{bmatrix} 7 & 3 \\ 2 & 8 \end{bmatrix}$$

$$AB = \begin{bmatrix} (1)(7) + (2)(2) & (1)(3) + (2)(8) \\ (4)(7) + (6)(2) & (4)(3) + (6)(8) \end{bmatrix} = \begin{bmatrix} 11 & 19 \\ 40 & 60 \end{bmatrix}$$

Adjacency matrix

The adjacency matrix of graph G is a $n \times n$ matrix $M_G = (m_{i,j})$ where each entry $m_{i,j}$ is the no. of edges with endpoints $\{i, j\}$ (counted with multiplicity)

Example: Let G be the following graph



The adjacency matrix of G is defined by

$$M_G = \begin{bmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

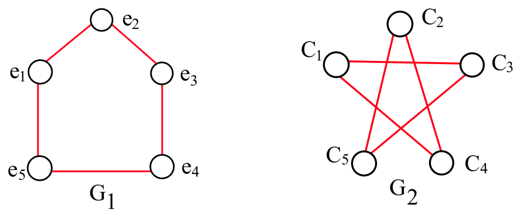
where the rows and columns are from a to f

8.4 Graph isomorphism

Graph isomorphism

Two graphs are isomorphic when you can map connections from G_1 to G_2 completely

Example: G_1 and G_2 are isomorphic



Graph G_1		**Graph G_2**		
Vertex	Connections	Vertex	Connections	Conclusion
e_1	e_2e_5	c_1	c_3c_4	$\phi(e_1) = c_1$
e_2	e_3e_1	c_3	c_5c_1	$\phi(e_2) = c_3$
e_3	e_4e_2	c_5	c_2c_3	$\phi(e_3) = c_5$
e_4	e_5e_3	c_2	c_4c_5	$\phi(e_4) = c_2$
e_5	e_1e_4	c_4	c_1c_2	$\phi(e_5) = c_4$