DMMR Condensed Summary Notes For Quick In-Exam Strategic Fact Deployment

Maksymilian Mozolewski

December 10, 2019

Topic	**Page**
Boolean Logic	2
Proof Techniques	2
Induction	3
Sets	3
Cardinality	4
Relations	5
Functions	6
Sequences	7
Sums	8
Number Theory	9
Counting	13
Graphs	17
Graph Colouring	22
Trees	22
Discrete Probability	24
Expected Value and Variance	26
Examples in Probability	28

Boolean Logic

Equivalence of prepositional statements

$P \equiv Q$ denotes a logical **equivalence** between the propositional statements P and Q. Two equivalent propositions have the same truth tables

Contrapositive

let S be a statement of the form $P \to Q$ then the **Contrapositive** of S is $\neg Q \to \neg P$. The Contrapositive of S is logically equivalent to S

Boolean Logic Laws

Identity Law:	$P \wedge T \equiv P$	$P \vee F \equiv P$
Domination Law:	$P \wedge F \equiv F$	$P \vee T \equiv T$
Idempotency Law:	$P \wedge P \equiv P$	$P \vee P \equiv P$
Double Negation:	$\neg(\neg P) \equiv P$	
Commutativity Law:	$P \wedge Q \equiv Q \wedge P$	$P \vee Q \equiv Q \vee P$
Associativity law:	$P \wedge (Q \wedge R) \equiv (Q \wedge P) \wedge R$	$P \vee (Q \vee R) \equiv (Q \vee P) \vee R$
Distributive Law:	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
De Morgan's Law:	$\neg(P \wedge Q) \equiv \neg P \wedge \neg Q$	

Negation of Quantifiers

$\neg(\forall x(P(x))) \equiv \exists x \neg P(x) \quad \neg(\exists x P(x)) \equiv \forall x \neg P(x)$

Proof Techniques

Direct Proof

use existing propositions and rules of inference to prove the given proposition

Proof by Contraposition

just like direct proof but we use prove contraposition of the given proposition

Proof by Contradiction

let P be the proposition to be proven, then assume $\neg P$ is true and show that $\neg P \to C$ where C is some logical contradiction of an earlier assumption or fact

Induction

Normal Induction

if P(n) is a predicate on $\mathbb{Z}^+$ we follow this process:
Base Case: we prove P(1) is true
Inductive Hypothesis: we assume $P(k)$ is true and we set to prove $P(k) \rightarrow P(k+1)$ is true
Inductive Step: we show that $P(k) \rightarrow P(k+1)$ is true

Strong Induction

same as normal induction however instead of assuming P(k) is true, we assume $P(1) \wedge ..P(k)$ is true and show that it being true implies P(k + 1)

Sets

Set

an **unordered** collection of objects, called members/elements.
A multi-set is a set which holds the multiplicity of objects as well as the objects

Important Sets

B	$\{true, false\}$	Boolean values
N	$\{0, 1, 2, 3, ..\}$	Natural numbers
Z	$\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$	Integers
Z^+	$\{z \in Z \mid z > 0\}$	Positive Integers
R		Real Numbers
R^+	$\{r \in R \mid r > 0\}$	Positive Real Numbers
Q	$\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}^+\}$	Rational Numbers
Q^+	$\{\frac{a}{b} \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+\}$	Positive Rational Numbers
C		Complex numbers

Power Set

the **power set** of a set A consists of all the possible subsets of A including the empty set. if A has n elements, then P(A) will contain 2^n elements

Complement

the **complement** of A is the set $\bar{A}$ which contains all the elements which are not in A, relative to the universe of discourse

Proofs with sets

to prove a set is a **subset** of another, show that an element in the first one must be in the other one, to prove two sets are equal, prove that they are both subsets of each other

Set Identities

Identity Law:	$A \cap U = A$	$A \cup \emptyset = A$
Idempotency Law:	$A \cap A = A$	$A \cup A = A$
Commutativity Law:	$A \cap B = B \cap A$	$A \cup B = B \cup A$
De Morgan's Law:	$\overline{A \cap B} = \bar{A} \cap \bar{B}$	$\overline{A \cup B} = \bar{A} \cup \bar{B}$
Absorption Law:	$A \cup (A \cap B) = A$	$A \cap (A \cup B)$
Domination Law:	$A \cap \emptyset = \emptyset$	$A \cup U = U$
Complementation law:	$\overline{(\overline{A})} = A$	
Associative Law:	$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$
Distributive Law:	$A \cup (B \cup C) = (A \cup B) \cap (A \cup B)$	$A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$
Complement Law:	$A \cap \overline{A} = \emptyset$	$A \cup \overline{A} = U$

Cartesian Product

$A \bigtimes B$ is the set of **all ordered pairs** (a,b) such that $a \in A \wedge b \in B$

Cardinality

Cardinality

the set A has **cardinality** $|A|$ which is the number of elements in A

Sets comparisons

for all sets, $|X| \leq |Y|$ iff there is an injection $f : X \to Y$

$$|X| = |Y| \text{ iff there is a bijection } f : X \to Y$$
$$|X| < |Y| \text{ iff } |X| \leq |Y| \wedge |X| \neq |Y|$$

Countability

A set S is called **countably infinite**, iff it has the same **cardinality** as the positive integers, $|\mathbb{Z}^+| = |S|$ we then say it has cardinality $\aleph$
A set is called **countable** iff it is either **finite** or **countably infinite**, otherwise it's called **uncountable**

Countability and Union

if A and B are countable sets, then $A \cup B$ is countable

Countability of Big Union

if I is countable and for each $i \in I$ the set A_i is countable then $\bigcup_{i \in I} A_i$ is countable

Cardinality of Finite Strings

The set $\sum^*$ of all finite strings over a finite alphabet $\sum$ is **countably infinite**

Uncountable sets

The set of infinite binary strings is **uncountable**
The set $[0,1] \subseteq R$ is **uncountable**
The set of functions $F = \{f | f : \mathbb{Z} \to \mathbb{Z}\}$ is **uncountable**

Schroder-Bernstein Theorem

$$\text{if } |A| \leq |B| \wedge |B| \leq |A| \text{ then } |A| = |B|$$

Cantor's theorem

$$|A| < |P(A)|$$

Continuum

the cardinality of the set $\mathbb{R}$ is $\mathfrak{c}$, and $\aleph < \mathfrak{c}$, there exists an infinite hierarchy of cardinalities of infinite sets

Relations

Binary relation

a **binary relation** R on sets A and B is a subset $R \subseteq AxB$. e.g. a set of tuples (a,b) with $a \in A \wedge b \in B$

n-ary relation

given sets $A_1, ..., A_n$ a subset $R \subseteq A_1, ..., A_n$ is an **n-ary relation**

Relation Union and Intersection

if R_i are relations on $AxB \forall i \in I$ then $\bigcup_{i \in I} R_i$ and $\bigcap_{i \in I} R_i$ are relations on AxB

Relation composition

let $R \subseteq BxC$ and $S \subseteq AxB$ the **composition relation** $(R \circ S) \subseteq AxC$ is $\{(a,c) | \exists b (a,b) \in S \wedge (b,c) \in R\}$

Closures

Closure R is a relation on A:

- R^0 is the identity relation ($\mathbf{i}_A$)
- $R^{n+1} = R^n \circ R$
- $R^* = \bigcup_{n \geq 0} R^n$

R^* is the **reflexive and transitive closure** of R

Properties of binary relations

the relation R on A is:
reflexive iff $\forall x \in A.(x,x) \in R$
symmetric iff $\forall x,y \in A.((x,y) \in R \rightarrow (y,x) \in R)$
antisymmetric iff $\forall x,y \in A(((x,y) \in R \wedge (y,x) \in R) \rightarrow x = y)$
transitive iff $\forall x,y,z \in A(((x,y) \in R \wedge (y,z) \in R) \rightarrow (x,z) \in R)$

Equivalence relations

A relation R on a set A is an **equivalence relation** iff it is reflexive, symmetric and transitive

Equivalence classes

let R be an equivalence relation on a set A and $a \in A$. Then

$$[a]_R = \{s|(a,s \in R)\}$$

is the **equivalence class** of a w.r.t R

Properties on equivalent relations

let R be an equivalence relation on A and a,b $\in A$ the following three statements are equivalent:

- aRb
- $[a]_R = [b])r$
- $[a]_R \cap [b])r \neq \emptyset$

Partitions of a set

A **partition** of a set A is a collection of disjoint, nonempty subsets that have A as their union.

Equivalence To Partition

If R is an equivalence on A, then the equivalence classes of R form a partition of A. Conversely, given a partition $A_i|i \in I$ of A there exists an equivalence relation R that has exactly the sets A_i for $i \in I$ as its equivalence classes

Functions

Function

let A and B be a non-empty set, then a **function** f maps exactly one element of B to each element of A. so every element in the function must be defined on all elements in A and there cannot be more than one element of B associated with any element of A

function Composition

if f and g are functions then $f \circ g = f(g(x))$

Injective Functions (one-to-one)

$f : A \rightarrow B$ is **injective** iff $\forall a,c \in A(f(a) = f(c) \rightarrow a = c)$

Surjective Functions (onto)

$f : A \to B$ is **surjective** iff $\forall b \in B \exists a \in A(f(a) = b)$

Bijective Functions (One-to-one correspondence)

$f : A \to B$ is a **bijection** iff it is both injective and surjective

New Functions from old functions

if f and g are functions then $f + g$ and $f \circ g$ is also a function

if f and g are both injective/surjective/bijective then $f \circ g$ is also injective/surjective/bijective (respectively)

Inverse Functions

let $f : A \to B$ be a bijection, then the inverse of f, $f^{-1} : B \to A$ is $f^{-1}(b) = a$ iff $f(a) = b$. So the inverse function exists only for bijections, and it exists for only the elements in B which are mapped to by some element $a \in A$ by f

Sequences

Sequences

Sequences are ordered lists of elements,
Example: $f : \mathbb{Z}^+ \to \mathbb{Q} f(n) = \frac{1}{n}$ defines the sequence $1, 1/2, 1/3, 1/4, ...$ assuming $a_n = f(n)$
the sequence is also written $a_1, a_2, a_3...$ or as $\{a_{n \in \mathbb{Z}^+}\}$

Sequence over a Set

a **sequence over a set** S is a function f from a subset of the integers to the set S. If the domain of f is finite then the sequence is finite.

Geometric and Arithmetic progressions

A **geometric progression** is a sequence of the form $a, ar, ar^2, ...ar^n, ..$

An **arithmetic progression** is a sequence of the form $a, a + d, a + 2d, ..., a + nd$, where the initial elements a, the common ratio r and the common difference d are real numbers

Reccurence relations

A **reccurence relation** for $\{a_n\}_{n \in \mathbb{N}}$ is an equation that expresses a_n in terms of one or more of the elements $a_0, a_1, ..., a_{n-1}$
the initial conditions specify the first elements of the sequence, before the recurrence relation applies
A sequence is called a solution of a recurrence relation iff its terms satisfy the recurrence relation

Fibonnaci Sequence

$$f(x) = \begin{cases} 1 & n = 1 \\ 1 & n = 2 \\ f(n-1) + f(n-2) & n > 2 \end{cases}$$

Solving recurrence relations with iteration

$a_n = a_{n-1} + 3$ for $n \geq 2$ with $a_1 = 2$

Forward Substitution Method:
$a_2 = 2 + 3$
$a_3 = (2 + 3) + 3 = 2 + 3 \cdot 2$
$a_4 = (2 + 2 \cdot 3) + 3 = 2 + 3 \cdot 3$
$\vdots$
$a_n = a_{n-1} + 3 = (2 + 3 \cdot (2 - 2)) + 3 = 2 + 3 \cdot (n - 1)$

Backward Substitution Method:
$a_n = a_{n-1} + 3$
$= a_{n-2} + 3 = a_{n-2} + 3 \cdot 2$
$= a_{n-3} + 3 \cdot 2 = a_{n-2} + 3 \cdot 3$
$\vdots$
$= a_2 + 3(n - 2) = (a_1 + 3) + 3 \cdot (n - 2) = 2 + 3 \cdot (n - 1)$

Common Sequences

nth Term	First 10 terms
n^2	$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, ...$
n^3	$1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, ...$
n^4	$1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, ...$
2^n	$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...$
3^n	$3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, ...$
$n!$	$1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, ...$
f_n	$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...$

Sums

Sums

given a sequence $\{a_n\}$, **the sum** of terms $a_m, a_{m+1}, ..., a_l$ is

$$a_m + a_{m+1} + ... + a_l \text{ or}$$
$$\sum_{j=m}^{\leqslant} a_j \text{ or } \sum_{m \leq j \leq l} a_j$$

more generally for an **index set S**:

$$\sum_{j \in S} a_j$$

Useful Summation Formulas

Sum	Closed Form
$\sum_{k=0}^{n} ar^k (r \neq 0)$	$\frac{ar^{n+1} - a}{r-1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Products

given a sequence $\{a_n\}$, the **product** of terms $a_m, a_{m+1}, ..., a_l$ is

$$a_m + a_{m+1} + ... + a_l \text{ or}$$

$$\prod_{j=m}^{\leqslant} a_j \text{ or } \prod_{m \leq j \leq l} a_j$$

more generally for an index set S:

$$\prod_{j \in S} a_j$$

Number Theory

Division

if a and b are integers with $a \neq 0$, then **a divides b**, written $a|b$, if there exists an integer c such that $b = ac$

Divisibility Results

if a, b, c are integers, then the following hold:

- $a|b \wedge a|c \rightarrow a|(b+c) \wedge a|(b-c)$
- $a|b \rightarrow a|bc$
- $a|b \wedge b|c \rightarrow a|c$

Division Algorithm

if a is an integer and d is a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
q is the **quotient**, r is the **remainder**, q = **a div b** and r = **a mod d**

Congruency

if a and b are integers and m is a positive integer, then
a is **congruent** to b modulo m, written $a \equiv b \pmod{m}$, iff $m|(a - b)$

Congruence is an equivalence relation

$a \equiv b \pmod{m}$ iff a mod m = b mod m

Congruence Result

$a \equiv b \pmod{m}$ iff there is an integer k such that $a = b + km$

Congruences of sums,differences and products

if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Corollary

- $(a + b) \pmod{m} = ((a \bmod m) + (b \bmod m)) \bmod m$
- $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Arithmetic modulo m

$\mathbb{Z}_m = \{0, 1, ..., m - 1\}$
$+_m$ on $\mathbb{Z}_m$ is $a +_m b = (a + b) \bmod m$
$\cdot_m$ on $\mathbb{Z}_m$ is $a \cdot_m b = (a \cdot b) \bmod m$

Primes

A positive integer $p > 1$ is called **prime** iff the only positive factors of p are 1 and p. otherwise it is called **composite**

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of non-decreasing size

Lemma

if p is prime and $p|a_1a_2...a_n$ where each a_i is an integer, then $p|a_j$ for some $1 \leq j \leq n$

Infinity of primes

Every natural number greater than one is either prime or it has a prime divisor and there are infinitely many primes

Trial Division

if n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

The Sieve of Eratosthenes

To find all primes between 2 and n:
try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

- write the numbers 2,..,n into a list. Let i := 2
- remove all strict multiples of i from the list
- let k be the smallest number present in the list s.t k ¿ i and let i:= k
- if $i > \sqrt{n}$ then stop else go to step 2

Greatest Common Divisor

Let a, b Z +.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written gcd(a, b)

Coprimes

The integers a and b are **relatively prime (coprime)** iff gcd(a, b) = 1

GCD from prime factors

gcd(a,b) = $p_1^{min(a_1,b_1)} p_2^{min(a_1,b_2)} ... p_n^{min(a_n,b_n)}$

Euclidian Algorithm

if x and y are integers and $x \geq y$ then
gcd(x,y) = gcd(y,x mod y) and
gcd(x,0) = x

Bezout's Theorem

If x and y are positive integers,then
there exist integers a and b such that gcd(x, y) = ax + by

Extended Euclidian algorithm

algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
        (d, a, b) := e-gcd(y, x mod y)
        return((d, b, a - ((x div y) * b)))
example:

e-gcd(22,4) ↓	= (2,1,0-(5 · 1)) = (2,1,-5)
e-gcd(4,2) ↓	↖= (2, 0, 1 − (2 ·0)) = (2,0,1)
e-gcd(2,0) →	↖= (2, 1, 0)

so gcd(22,4)= $2 = 1 \cdot 22 + (-5) \cdot 4$

Properties

if a,b,c are positive integers such that gcd(a,b) = 1 and $a|bc$ then $a|c$
i.e. if a has no common factors with b (except 1) but has common factors with bc then a has common factors with c

Further Properties

let m be a positive integer and let a,b,c be integers.
if $ac \equiv bc \pmod{m}$ and gcd(c,m) = 1, then $a \equiv b \pmod{m}$

Multiplicative Inverses

let x,y,m be integers, then y is a **multiplicative inverse** modulo m of x when $xy \equiv 1 \pmod{m}$

Existence of inverses

if m,x are positive integers and gcd(m,x) = 1 then x has a multiplicative inverse mod m (and it is unique mod m)

Chineese Reminder Theorem

Let $m_1, ..., m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, ..., a_n$ be arbitrary integers. Then the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$
here is a general construction to find such solution:

- Compute M = $m_1 m_2 \cdots m_n$
- for each i = 1,2,...,n, compute: $y_i = \dfrac{M}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$
- for each i = 1,2,...,n, compute $z_i \equiv y_i^{-1} \pmod{m_i}$ (the inverse of each y, can be found using the e-gcd algorithm by taking the result of $e - gcd(m_i, y_i) = (1 = a \cdot y_i + b \cdot m_i)$ and taking $\pmod{m_i}$ of both sides)
- the integer $x = \sum_{i=1}^{k} a_i y_i z_i$ is a solution to the system of congruences and x mod N is the unique solution modulo M

any other solutions will be multiples of M

Fermat's little Theorem

if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, for every integer a we have: $a^p \equiv a \pmod{p}$

RSA cryptography

Choose two distinct prime numbers pand q
let n = pq and k = (p-1)(q-1)
choose integer e where $1 < e < k$and gcd (e,k) = 1
(n,e) is released as the public key
let d be the multiplicative inverse of e modulo k, so $de \equiv 1 \pmod{k}$
(n,d) is the private key and kept secret
Encryption:

- Bob has public key (n,e) but no private key
- turns M into integer m, $0 \leq m < n$, using an agreed-upon reversible protocol - the padding scheme
- he computes the ciphertext c corresponding to $c = m^e$ mod n.
- Bob transmits c to alice

Decryption:

- using her private key (n,d), computes $m = c^d$ mod n
- given m, she can recover the original message M by reversing the padding scheme

Counting

Counting Summary

Type	Repetition Allowed ?	Formula
r-permutations	No	$\frac{n!}{(n-r)!}$
r-combinations	No	$\frac{n!}{r!(n-r)!}$
r-permutations	Yes	n^r
r-combinations	Yes	$\frac{(n+r-1)!}{r!(n-1)!}$

Product Rule

if A and B are finite sets then: $|A \bigtimes B| = |A| \cdot |B|$

General Product Rule

if $A_1, A_2, ..., A_m$ are finite sets then: $|A_1, A_2, ..., A_m| = |A_1| \cdot |A_2| \cdots |A_m|$

Counting Subsets

A finite set, S, has $2^{|S|}$ distinct subsets

Counting Functions

For all finite sets A and B, the number of distinct functions, $f : A \to B$, mapping A to B is:

$$|B|^{|A|}$$

Sum Rule

if A and B are finite sets that are disjoint, then:

$$|A \cup B| = |A| + |B|$$

General Sum Rule

if $A_1, ..., A_m$ are finite sets that are pairwise disjoint, then:

$$|A_1, ..., A_m| = |A_1| + ... + |A_m|$$

Pigeonhole Principle

For any positive integer k, if k + 1 objects (pigeons) are placed in k boxes (**pigeonholes**), then at least one box contains two or more objects.

Generalized Pigeonhole Principle

If $N \geq 0$ objects are placed in k 1 boxes, then at least one box contains at least $\left\lceil \frac{N}{k} \right\rceil$ objects

Permutations

A permutation of a set S is an ordered arrangement of the elements of S. In other words, it is a sequence containing every element of S exactly once

R-Permutations

An r-permutation of a set S, is an ordered arrangement (sequence) of r distinct elements of S. (For this to be well-defined, r needs to be an integer with $0 \leq r \leq |S|$.)

Calculating r-permutations

let P(n,r) denote the number of r-permutations of an n-elements set. For all integers $n \geq 1$, and all integers r such that $1 \leq r \leq n$:
P(n,r) = $\frac{n!}{(n-r)!}$

How big is n!

$n! \leq n^n$ for all n bigger than 0
$2^n < n!$ for all n bigger or equal than 4

Stirling's approximation formula

$n! \approx \sqrt{2} \cdot (\frac{n}{e})^n$ or

$$\sqrt{2} \cdot (\frac{n}{e})^n \cdot e^{\frac{1}{12n+1}} \leq n! \leq \sqrt{2} \cdot (\frac{n}{e})^n \cdot e^{\frac{1}{12n}}$$

R-Combinations

An r-combination of a set S is an unordered collection of r elements of S. In other words, it is simply a subset of S of size r

Calculating R-Combinations

let C(n,r) denote the number of r-combinations of an n-element set, which is also written as $\binom{n}{r}$. Then for all integers $n \geq 1$, and for all integers r such taht $0 \leq r \leq n$:

$$C(n,r) = \binom{n}{r} = \frac{n!}{r! \cdot (n-r)!} = \frac{n \cdot (n-1) \cdots (n-r+1)}{r!}$$

Bounds for Combinations

using basic considerations and stirling's approximation formula, one can easilly estabilish the following bounds and approximations for $\binom{n}{r}$:

$$(\frac{n}{r})^r \leq \binom{n}{r} \leq (\frac{n \cdot e}{r})^r$$

$$\binom{2n}{n} \approx \frac{2^{2n}}{\sqrt{\pi n}}$$

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}$$

Combinations Identity

For all integers $n \geq 1$ and all integers r $1 \leq r \leq n$:

$$\binom{n}{r} = \binom{n}{n-r}$$

The Binomial Theorem

For all $n \geq 0$:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

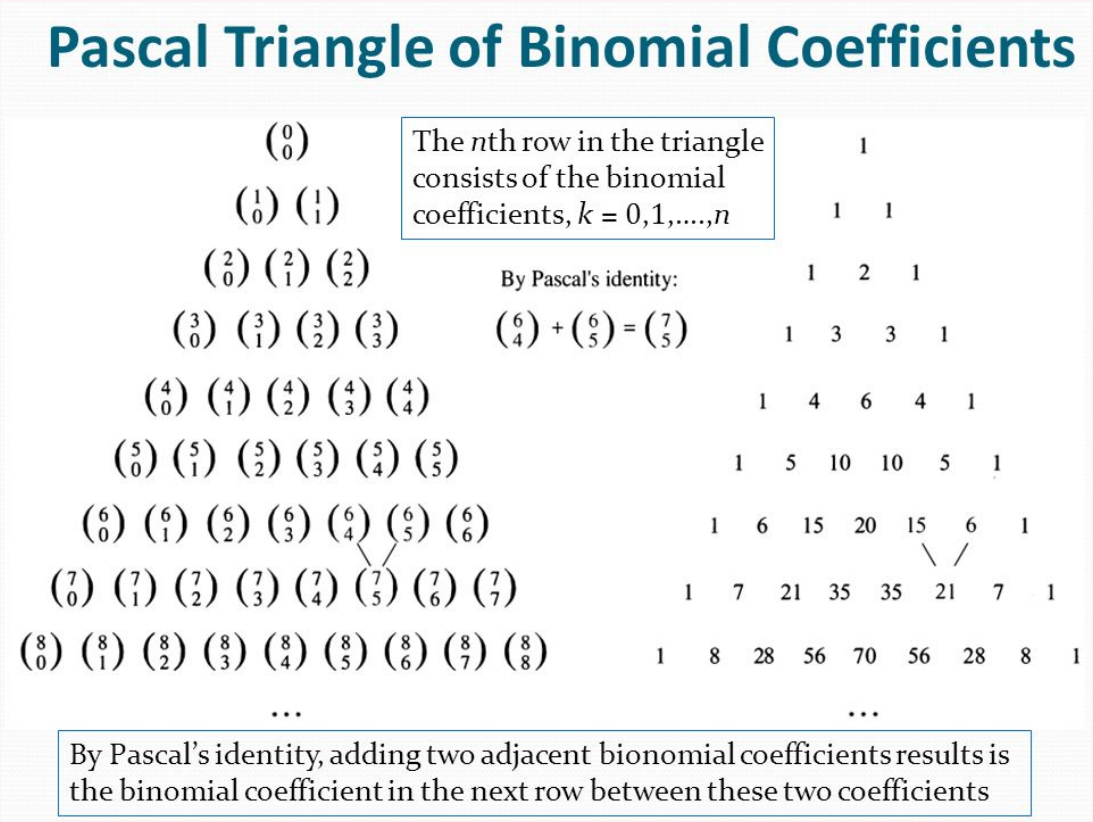
Corollary

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n$$

Pascal's Identity

For all integers $n \geq 0$, and all integers r, $0 \leq r \leq n+1$:

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$



Vandermonde's identity

for m,n,r ≥ 0, r $\leq m$ and r $\leq$ n, we have:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

R-Combinations with repetition

from a set S is simply a multi-set of size r over S (set which can contain multiple of each element)

counting r-combinations with repetition

For all integers n,r ≥ 1, the number of r-combs-w.r. from a set S of size n is

$$\binom{n+r-1}{r} = \binom{n+r-1}{n-1}$$

The number of permutations of n objects, with n_1 indistinguishable objects of Type 1, n_2 indistinguishable objects of Type 2,..., and n_k indistinuishable objects of Type k, is:

$$\binom{n}{n_1, n_2, ..., n_k} = \frac{n!}{n_1! n_2! ... n_k!}$$

Multinomial theorem

for all n $\geq$ 0 and all k $\geq$ 1:

$$(x_1 + x_2 + ... + x_k)^n = \sum_{0 \leq n_1, n_2, ..., n_k \leq n} \binom{n}{n_1, n_2, ..., n_k} x_1^{n_1} x_2^{n_2} ... x_k^{n_k}$$

Graphs

Graph Types

Type	Edges	Multi-Edges	Loops
(simple undirected) graph	Undirected	No	No
(undirected) multigraph	Undirected	Yes	No
(undirected) pseudograph	Undirected	Yes	Yes
directed graph	Directed	No	Yes
simple directed graph	Directed	No	No
directed multigraph	Directed	Yes	No
directed pseudograph	Directed	Yes	Yes
mixed graph	Both	Yes	Yes

Directed Graph Definition

A directed graph (digraph), G = (V, E), consists of a non-empty set, V, of vertices (or nodes), and a set $E \subseteq VV$ of directed edges (or arcs). Each directed edge $(u, v) \in E$ has a start (tail) vertex u, and a end (head) vertex v. Note: a directed graph G = (V, E) is simply a set V together with a binary relation E on V

Undirected Graph Definition

A (simple,undirected) graph, G = (V, E), consists of a non-empty set V of vertices (or nodes), and a set$E \subseteq [V]$ 2 of (undirected) edges. Every edge $u, v \in E$ has two distinct vertices u 6= v as endpoints, and such vertices u and v are then said to be adjacent in the graph G.

Degree of a vertex

The degree of a vertex v in a undirected graph is the number of edges incident with it. The degree of the vertex v is denoted by deg(v).

The Neighbourhood of a vertex

The neighborhood (neighbor set) of a vertex v in a undirected graph, denoted N(v) is the set of vertices adjacent to v.

Handshaking Theorem

If G=(V,E) is a undirected graph with m edges. let V_1 be the vertices of even degree and V_2 be the vertices of odd degree in G, then:

$$2m = \sum_{v \in V} deg(v) = \sum_{v \in V_1} deg(v) + \sum_{v \in V_2} deg(v)$$

In/Out degree

The in-degree of a vertex v, denoted $deg_-(v)$, is the number of edges directed into v. The out-degree of v, denoted $deg_+(v)$, is the number of edges directed out of v. Note that a loop at a vertex contributes 1 to both in-degree and out-degree.

Number of Edges of a Directed Graph

Let G = (V, E) be a directed graph. Then:

$$|E| = \sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v)$$

Complete Graphs

A **complete graph** on n vertices, denoted by K_n is the simple graph that contains exactly one edge between each pair of distinct vertices.

Cyclical Graphs

A cycle C_n for $n \geq 3$ consists of n vertices v_1, v_2, v_n and edges
$(v_1, v_2), (v_2, v_3), ..., (v_{n-1}, v_n), (v_n, v_1)$

n-Cubes

An n-dimensional hypercube, or n-cube, is a graph with 2^n vertices representing all bit strings of length n, where there is an edge between two vertices if and only if they differ in exactly one bit position.

Bipartite Graphs

An equivalent definition of a bipartite graph is one where it is possible to color the vertices either red or blue so that no two adjacent vertices are the same color.

Complete Bipartite Graphs

A complete bipartite graph is a graph that has its vertex set partitioned into two subsets V_1 of size m and V_2 of size n such that there is an edge from every vertex in V_1 to every vertex in V_2.

Subgraphs

A subgraph of a graph G = (V,E) is a graph (W,F), where $W \subseteq V$ and $F \subseteq E$. A subgraph H of G is a proper subgraph of G if $H \neq G$.

Induced Subgraphs

Let G = (V, E) be a graph. The subgraph induced by a subset W of the vertex set V is the graph H= (W,F), whose edge set F contains an edge in E if and only if both endpoints are in W.

Bipartite Graph alternative Definition

A bipartite graph is a (undirected) graph G = (V,E) whose vertices can be partitioned into two disjoint sets (V_1, V_2), with $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$, such that for every edge $e \in E$, e = {u, v} such that $u \in V_1$ and $v \in V_2$. In other words, every edge connects a vertex in V_1 with a vertex in V_2.
Equivalently, a graph is bipartite if and only if it is possible to color each vertex red or blue such that no two adjacent vertices are the same color.

Matchings

A **matching**, M, in a graph, G = (V,E), is a subset of edges, $M \subseteq E$, such that there does not exist two distinct edges in M that are incident on the same vertex. In other words, if $\{u, v\}, \{w, z\} \in M$, then either $\{u, v\} = \{w, z\}$ or $\{u, v\} \cap \{w, z\} = \emptyset$.

A **maximum matching** in graph G is a matching in G with the maximum possible number of edges.

Perfect/Complete Matchings

For a graph G = (V,E), we say that a subset of edges, $W \subseteq E$, **covers** a subset of vertices, $A \subseteq V$, if for all vertices $u \in A$, there exists an edge $e \in W$, such that e is incident on u, i.e., such that e = {u, v}, for some vertex v.

In a bipartite graph G = (V,E) with bipartition (V_1, V_2), a **complete matching** with respect to V_1, is a matching $M^{'} \subseteq E$ that covers V_1, and a **perfect matching** is a matching, $M_* \subseteq E$, that covers V.

Hall's Marriage Theorem

For a bipartite graph G = (V,E), with bipartition (V_1, V_2), there exists a matching $M \subseteq E$ that covers V_1 if and only if for all $S \subseteq V_1, |S| \leq |N(S)|$.

Corollary

Corollary A bipartite graph G = (V,E) with bipartition (V_1, V_2) has a perfect matching if and only if $|V_1| = |V_2|$ and $\forall S \subseteq V_1, |S| \leq |N_G(S)|$.

New Graphs From Old

The union of two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the simple graph with vertex set $V_1 \cup V_2$ and edge set $E_1 \cup E_2$. The union of G_1 and G_2 is denoted by $G_1 \cup G_2$.

Representing Graphs: Adjacency Lists

An **adjacency list** represents a graph (with no multiple edges) by specifying the vertices that are adjacent to each vertex.

Adjacency Matrix

Suppose that G = (V, E) is a simple graph where $|V| = n$. Arbitrarily list the vertices of G as $v_1, v_2, ..., v_n$. The adjacency matrix, A, of G, with respect to this listing of vertices, is the n x n 0-1 matrix with its (i, j)th entry = 1 when v_i and v_j are adjacent, and = 0 when they are not adjacent

Isomorphism of graphs

Definition: Two (undirected) graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a bijection, , with the property that for all vertices $a, b \in V_1$

$$\{a, b\} \in E_1 \text{ if and only if } \{f(a), f(b)\} \in E_2$$

Such a function f is called an isomorphism. Intuitively, isomorphic graphs are "THE SAME", except for "renamed" vertices.

Paths

For an undirected graph(same definition for directed graphs) G = (V,E), an integer $n \geq 0$, and vertices $u, v \in V$, **a path (or walk) of length n from u to v** in G is a sequence:
$x_0, e_1, x_1, e_2, ..., x_{n1}, e_n, x_n$
of interleaved vertices $x_j \in V$ and edges $e_i \in E$, such that $x_0 = u$ and $x_n = v$, and such that $e_i = \{x_{i1}, x_i\} \in E$ for all $i \in 1, ..., n$.
Such a path **starts** at u and **ends** at v. A path of length $n \geq 1$ is called a **circuit (or cycle)** if $n \geq 1$ and the path starts and ends at the same vertex, i.e., u = v.
A path or circuit is called **simple** if it does not contain the same edge more than once.(And we call it **tidy** if it does not contain the same vertex more than once, except possibly the first and last in case u = v and the path is a circuit (cycle))

Connectedness in Undirected Graphs

An undirected graph G = (V,E) is called connected, if there is a path between every pair of distinct vertices. It is called disconnnected otherwise.

There is always a simple, and tidy path between any pair of vertices u,v of a connected undirected graph G.

Connected Components

A connected component $H = (V', E')$ of a graph G = (V,E) is a maximal connected subgraph of G, meaning H is connected and $V' \subseteq V$ and $E' \subseteq E$, but H is not a proper subgraph of a larger connected subgraph R of G.

Connectedness in Directed Graphs

A directed graph G = (V,E) is called **strongly connected**, if for every pair of vertices u and v in V, there is a (directed) path from u to v, and a directed path from v to u.

(G = (V,E) is **weakly connected** if there is a path between every pair of vertices in V in the underlying undirected graph (meaning when we ignore the direction of edges in E.)

A **strongly connected component (SCC)** of a directed graph G, is a maximal strongly connected subgraph H of G which is not contained in a larger strongly connected subgraph of G

Directed Acyclic Graph (DAG)

A Directed Acyclic Graph (DAG), is a directed graph that contains no circuits or loops.

Euler Path

An **Euler path** in a multigraph G is a simple path that contains every edge of G. (So, every edge occurs exactly once in the path.)

An **Euler circuit**in an multigraph G is a simple circuit that contains every edge of G. (So, every edge occurs exactly once in the circuit.)

Euler's Theorem (Euler's Circuits)

A connected undirected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.

Euler's Theorem (Euler's Paths)

A connected undirected multigraph G has an Euler path which is not an Euler circuit if and only if G has exactly two vertices of odd degree.

Hamiltonian Paths

A **Hamiltonian path** in a (undirected) graph G is a simple path that visits every vertex exactly once. (In other words, it is a tidy path that visits every vertex.)

A **Hamiltonian circuit** in a (undirected) graph G is a simple circuit that passes through every vertex exactly once (except for the common start and end vertex, which is seen exactly twice).

Graphs With Edge Weights

An edge-weighted directed graph, G = (V,E, w), has a length/weight/cost function, $w : E \to \mathbb{N}$, which maps each edge $(u, v) \in E$ to a non-negative integer "length" (or "weight", or "cost"): $w(u, v) \in \mathbb{N}$.

We can extend the "length" function w to a function $w : V\ x\ V \to \mathbb{N} \cap \{\infty\}$, by letting w(u, u) = 0, for all u ∈ V, and letting $w(u, v) = \infty$ for all $(u, v) \notin E$.

Dijkstra's Algorithm

Input: Edge-weighted graph, G = (V,E, w), with (extended) weight function $w : V\ x\ V \to N$, and a source vertex $s \in V$.
Output: Function $L : V \to N \cup \{\}$, such that for all $v \in V$, L(v) is the length of the shortest path from s to v in G.
Algorithm:
Initialize: S := {s}; L(s) := 0;
Initialize: L(v) := w(s, v), for all $v \in V - \{s\}$;
while (S ≠ V)**do**
u :=arg $\min_{z \in V-S}\{L(z)\}$
$S := S \cap \{u\}$
for all $v \in V - S$ such that $(u, v) \in E$ **do**
L(v) := min{L(v), L(u) + w(u, v)}
end for
end while
Output function L(·).

Graph Colouring

K-Colouring

Suppose we have k distinct colours with which to colour the vertices of a graph. Let $[k] = \{1, ..., k\}$. For an undirected graph, $G = (V, E)$, an admissible vertex **k-colouring** of G is a function $c : V \to [k]$, such that for all u, $v \in V$, if $\{u, v\} \in E$ then $c(u) \neq c(v)$.

For an integer $k \geq 1$, we say an undirected graph $G = (V, E)$ is **k-colourable** if there exists a **k-colouring** of G. The chromatic number of G, denoted $\chi(G)$, is the smallest positive integer k, such that G is k-colourable.

Every Graph with n vertices is n-colourable

N-Clique

The **n-Clique**, K_n, i.e., the complete graph on n vertices, has chromatic number $\chi(K_n) =$ n. All its vertices must get assigned different colours in any admissible colouring.

The **clique number** $\omega(G)$, of a graph G is the maximum positive integer $r \geq 1$, such that K_r is a subgraph of G.
Note that for all graphs G, $\omega(G) \leq \chi(G)$: if G has an r-clique then it is not (r - 1)-colorable. However in general:
$\omega(G) \neq \chi(G)$. For instance, The 5-cycle, C_5, has $(C_5) = 2 < \chi(C_5) = 3$.

Trees

Trees

A **tree** is a connected simple undirected graph with no simple circuits.
A **forest** is a (not necessarily connected) simple undirected graph with no simple circuits.

Facts

A graph G is a tree if and only if there is a unique simple (and tidy) path between any two vertices of G.

Every tree, T = (V,E) with $|V| \geq 2$, has at least two vertices that have degree = 1.

Every tree with n vertices has exactly $n - 1$ edges.

Rooted Trees

A rooted tree, is a pair (T, r) where T = (V,E) is a tree, and $r \in V$ is a chosen root vertex of the tree. Often, the edges of a rooted tree (T,r) are viewed as being directed, such that for every vertex v the unique path from r to v is directed away from (or towards) r.

Terminology:

- For each node $v \neq r$ the **parent**, is the unique vertex u such that $(u, v) \in E$. v is then called a **child** of u. Two vertices with the same parent are called **siblings**.
- **A** leaf is a vertex with no children. Non-leaves are called **internal vertices**
- The **height** of a rooted tree is the length of the longest directed path from the root to any leaf.
- **The ancestors (descendants,** respectively) of a vertex v are all vertices u $\neq$ v such that there is a directed path from u to v (from v to u, respectively).
- The **subtree** rooted at v, is the subgraph containing v and all its descendants, and all directed edges between them.

M-ary Trees

For $m \geq 1$, A rooted tree is called a m-ary tree if every internal node has at most m children. It is called a full m-ary tree if every internal node has exactly m children. An m-ary tree with m = 2 is called a binary tree.

Rooted Ordered Tree

A **trooted ordered tree** is a rooted tree (T, r) where in addition the children of each internal vertex v are linearly ordered according to some ordering $\leq_v$. When drawing the tree, we usually write ordered children (from least to greatest) from left to right. If the rooted ordered tree is a **binary** tree, then the first child is called **left child** and the second child is called **right child**.

Counting Nodes 1

For all $m \geq 1$, every full m-ary tree with i internal vertices has exactly $n = m \cdot i + 1$ vertices.

Counting Nodes 2

For all $m \geq 1$, a full m-ary tree with:

- n vertices has $i = \dfrac{n-1}{m}$ internal vertices and $l = \dfrac{(m-1)n+1}{m}$ leaves
- i internal vertices has $n = m \cdot i + 1$ vertices and $l = (m-1)i + 1$ leaves
- if $m \geq 2$, then if the m-ary tree has l leaves then it has $n = \dfrac{ml-1}{m-1}$ vertices and $i = \dfrac{l-1}{m-1}$ internal vertices.

Counting Leaves

There are at most m^h leaves in an m-ary tree of height h.

Height of trees

If an m-ary tree has l leaves, and h is its height, then $h \geq \lceil \log_m l \rceil$.

Number of Comparisons in a sort

You have to sort a list of distinct unknown numbers: $a_1, ..., a_n$, using only the operation of comparing two numbers:$a_i <_? a_j$. How many comparisons do you need, in the worst case, in order to sort all the numbers correctly? Answer:

$$n \log_2 n$$

Spanning Trees

For a simple undirected graph G, a spanning tree of G is a subgraph T of G such that T is a tree and T contains every vertex of G.

Existence of Spanning Trees

Every connected graph G has a spanning tree.

Prim's Algorithm for a minimum spanning tree

Input: Connected, edge-weighted, undirected graph G = (V,E, w).
Output: A minimum-cost spanning tree T for G.
Algorithm:
Initialize: T := {e}, where e is a minimum-weight edge in E.
for i := 1 to n 2 **do**
Let $e^{'}$:= a minimum-weight edge incident to-
some vertex in T, and not forming a circuit if added to T;
T := $T \cup \{e^{'}\}$;
end for
Output the tree T.

Discrete Probability

Sample Space

For any probabilistic experiment or process, the set Ω of all its possible outcomes is called its **sample space**.

Probability Distribution

A probability distribution over a finite or countable set Ω, is a function:

$$P : \Omega \to [0, 1]$$

such that $\sum_{s \in \Omega} P(s) = 1$.

Event in a countable sample space

For a countable sample space Ω, an **event**, E, is simply a subset $E \subseteq \Omega$ of the set of possible outcomes. Given a probability distribution $P : \Omega \to [0, 1]$, we define the probability of the event $E \subseteq \Omega$ to be $P(E) = \sum_{s \in E} P(s)$.

Facts about Probability of events

Suppose $E_0, E_1, E_2, ...$ are a (finite or countable) sequence of pairwise disjoint events from the sample space Ω. In other words, $_i \in \Omega$, and $E_i \cap E_j = \emptyset$ for all $i, j \in \mathbb{N}$. Then

$$P(\bigcup_i E_i) = \sum_i P(E_i)$$

Furthermore, for each event $E \subseteq \Omega, P(\bar{E}) = 1 - P(E)$.

Conditional Probability

Let $P : \Omega \to [0, 1]$ be a probability distribution, and let $E, F \subseteq \Omega$ be two events, such that $P(F) > 0$. The conditional probability of E given F, denoted $P(E|F)$, is defined by:

$$P(E|F) = \frac{P(E \cap F)}{P(F)}$$

Independent Events

Events A and B are called independent if $P(A \cap B) = P(A)P(B)$.
Note that if $P(B) > 0$ then A and B are independent if and only if

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

Pairwise and Mutual Independence

Events $E_1, ..., E_n$ are called **pairwise independent**, if for every pair $i, j \in 1, ..., n, i \neq j$, E_i and E_j are independent(i.e., $P(E_i \cap E_j) = P(E_i)P(E_j)$).

Events $E_1, ..., E_n$ are called **mutually independent**, if for every subset $J \subseteq 1, ..., n$:

$$P(\bigcap_{j \in J} E_j) = \prod_{j \in J} P(E_j)$$

Binomial Distribution Theorem

The probability of exactly k successes in n (mutually) independent Bernoulli trials, with probability p of success and q = (1 p) of failure in each trial, is

$$\binom{n}{k} p^k q^{n-k}$$

Binomial Distribution

The binomial distribution, with parameters n and p, denoted b(k; n, p), defines a probability distribution on $k \in 0, ..., n$, given b

$$b(k; n, p) = \binom{n}{k} \cdot p^k q^{n-k}$$

Random Variable

A **random variable**, is a function $X : \omega \to R$, that assigns a real value to each outcome in a sample space Ω.

For a random variable X, we write $P(X = r)$ as shorthand for the probability $P(\{s \in \Omega | X(s) = r\})$. **The distribution** of a random variable X is given by the set of pairs $\{(r, P(X = r)) | r$ is in the range of $X\}$.

Geometric Distribution

A random variable $X : \Omega \to \mathbb{N}$, is said to have a geometric distribution with parameter p, $0 \leq p \leq 1$, if for all positive integers $k \geq 1, P(X = k) = (1 - p)^{k-1}p$.

Baye's Theorem

Let A and B be two events from a (countable) sample space Ω, and $P : \Omega \to [0, 1]$ a probability distribution on Ω, such that $0 < P(A) < 1$, and $P(B) > 0$. Then

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|\bar{A})P(\bar{A})}$$

Generalised Baye's Theorem

Suppose that $E, F_1, ..., F_n$ are events from sample space Ω, and that $P : \Omega \to [0, 1]$ is a probability distribution on Ω. Suppose that $\cup_{i=1}^{n} F_j = \Omega$ and that $F_i \cap F_j = \emptyset$ for all $i \neq j$. Suppose $P(E) > 0$, and $P(F_j) > 0$ for all j. Then for all j:

$$P(F_j|E) = \frac{P(E|F_j)P(F_j)}{\sum_{i=1}^{n} P(E|F_i)P(F_i))}$$

Expected Value And Variance

Expected Value

The expected value, or expectation, or mean, of a random variable $X : \Omega \to R$, denoted by E(X), is defined by:

$$E(X) = \sum_{s \in \Omega} P(s)X(s)$$

Here $P : \Omega \to [0, 1]$ is the underlying probability distribution on Ω.

Better expression for Expectation

For a random variable $X : \Omega \to \mathbb{R}$

$$E(X) = \sum_{r \in range(X)} P(X = r) \cdot r$$

Linearity of Expectation

Theorem (**Linearity of Expectation**):For any random variables $X, X_1, ..., X_n$on Ω, $E(X_1 + X_2 + ... + X_n) = E(X_1) + ... + E(X_n)$.

Furthermore, for any $a, b \in R$, $E(aX + b) = aE(X) + b$.
(In other words, the expectation function is a linear function.)

Expectation on n Bernouli Trials

The expected no. of successes in n (**Not necessarily independent**) Bernoulli trials, with probability p of success in each, is

$$np$$

Expectation of a geometrically distributed r.v

the expected value E(X) of a geometrically distributed random variable with parameter p is

$$\frac{1}{p}$$

Independence of Random Variables

Two random variables, X and Y, are called **independent** if for all $r_1, r_2 \in \mathbb{R}$:

$$P(X = r_1 \text{ and } Y = r_2) = P(X = r_1) \cdot P(Y = r_2)$$

Expectation of Independent Variables

: If X and Y are independent random variables on the same space Ω. Then

$$E(XY) = E(X)E(Y)$$

Variance and Standard Deviation

For a random variable X on a sample space Ω, the **variance** of X, denoted by V(X), is defined by:

$$V(X) = E((X - E(X))^2) = \sum_{s \in \Omega} (X(s) - E(X))^2 P(s)$$

The **standard deviation** of X, denoted $\sigma(X)$, is defined by:

$$\sigma(X) = \sqrt{V(X)}$$

Variance Identity

For any random variable X.

$$V(X) = E(X^2) - E(X)^2$$

Markov's Inequality

For a nonnegative random variable, $X : \Omega \to R$, where $X(s) \geq 0$ for all $s \in \Omega$, for any positive real number $a > 0$:

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

Chebyshev's Inequality

Let $X : \Omega \to R$ be any random variable, and let $r > 0$ be any positive real number. Then:

$$P(|X - E(X)| \geq r) \leq \frac{V(X)}{r^2}$$

Birthday Paradox

Suppose that each of $m \geq 1$ pigeons independently and uniformly at random enter one of $n \geq 1$ pigeon-holes. If

$$m \geq (1.1775 \cdot \sqrt{n}) + 1$$

then the probability that two pigeons go into the same pigeon-hole is greater than $1/2$.

Examples in Probability

Friends and Enemies

Suppose that in a group of 6 people every pair are either friends or enemies. Then, there are either 3 mutual friends or 3 mutual enemies.

Ramsey's Theorem

For any positive integer, k, there is a positive integer, n, such that in any undirected graph with n or more vertices:
either there are k vertices that are all mutually adjacent, meaning they form a k-clique,
or, there are k vertices that are all mutually non-adjacent, meaning they form a k-independent-set.

For each integer $k \geq 1$, let R(k) be the smallest integer $n \geq 1$ such that every undirected graph with n or more vertices has either a k-clique or a k-independent-set as an induced subgraph.

Erdos,1947

For all $k \geq 3$

$$R(k) > 2^{k/2}$$

Probabilistic Method

To show the existence of a hard-to-find object with a desired property, Q, try to construct a probability distribution over a sample space Ω of objects, and show that with positive probability a randomly chosen object in Ω has the property Q.

Union Bound

For any (finite or countable) sequence of events $E_1, E_2, E_3, ...$

$$P(\bigcup_i E_i) \leq \sum_i P(E_i)$$