# Math 1064 Review

## Useful Website

- Logic calculator: https://www.erpelstolz.at/gateway/formular-uk-zentral.html
- Mathway: https://www.mathway.com/Algebra
- Base calculator: https://www.rapidtables.com/calc/math/base-calculator.html
- Recurrences relation calculator: https://www.wolframalpha.com/examples/mathematics/discrete-mathematics/recurrences/
- Matrices calculator: https://matrixcalc.org/en/
- Sequence generator: http://oeis.org/

## Week 1

### The pigeonhole principle

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

---

### Proposition (Definition)

> **A proposition is a sentence that is true or false but not both**

---

### Negation, Conjunction, Disjunction

- Negation: ¬ p
- Conjunction: p ∧ q
- Disjunction: p ∨ q

p ∨ q is the "inclusive or", p ⊕ q is the "exclusive or"

---

### Logical equivalence (Definition)

> **Two compound propositions P and Q are logically equivalent**
>
> $$P \equiv Q$$
>
> **if they have identical truth values for every possible combination of truth values for their proposition variables**

---

### Contradiction (Definition)

> **Always false**

$$p \wedge (contradiction) \equiv (contradiction)$$
$$p \vee (contradiction) \equiv p$$

## Tautology (Definition)

> Always true

$$p \wedge (tautology) \equiv p$$
$$p \vee (tautology) \equiv (tautology)$$

---

## The conditional

the conditional from p to q:

$$p \to q$$

p is the **hypothesis** and q is the **conclusion**

> p $\to$ q is false if and only if the **hypothesis is true but the conclusion is false**

$$p \to q \equiv \neg p \vee q$$

---

## Logical equivalences

- Commutative laws

$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$

- Associative laws

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$

- Distributive laws

$$(p \wedge q) \vee r \equiv (p \wedge q) \vee (p \wedge r)$$
$$(p \vee q) \wedge r \equiv (p \vee q) \wedge (p \vee r)$$

- Identity laws

$$p \wedge (tautology) \equiv p$$
$$p \vee (contradiction) \equiv p$$

- Universal bound laws

$$p \vee (tautology) \equiv (tautology)$$
$$p \wedge (contradiction) \equiv (contradiction)$$

- Negation laws

$$p \vee \neg p \equiv (tautology)$$
$$p \wedge \neg p \equiv (contradiction)$$

- Double negative laws

$$\neg(\neg p) \equiv p$$

- Idempotent laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

- De Morgan's laws

$$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$$
$$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$$

- Absorption laws

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

- Negations

$$\neg(tautology)\ is\ a\ contradiction$$
$$\neg(contradiction)\ is\ a\ tautology$$

---

## More constructions in additional

$$(p \wedge q) \to r \equiv (p \to q) \vee (q \to r)$$

### Contrapositive

The contrapositive of $p \to q$ is $\neg q \to \neg p$

$$p \to q \equiv \neg q \to \neg p$$

### Converse

The converse of $p \to q$ is $q \to p$

### Inverse

The inverse of $p \to q$ is $\neg p \to \neg q$

---

## The biconditional

The biconditional from p to q is $q \leftrightarrow p$

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

---

## Satisfiability

> **A compound proposition is satisfiable if it isn't a contradiction**

- Consistent: If the conjunction **is a contradiction**, it is not cont consistent

---

## Predicates (Definition)

> **A sentence that contains finitely many variables, if the variables are given specific values it will becomes a proposition**

### Domain (Definition)

> **The set of all possible values that may be assigned to a predicate**

### Truth set (Definition)

> **The set of all values in the domain that when assigned to x, make predicate P(x) a true statement**

### Common domains

$$\begin{gathered} The\ natural\ numbers:\ N = \{0, 1, 2, 3, \ldots\} \\ The\ integers:\ Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, ..\} \\ The\ rationals:\ Q = all\ fractions = \{\frac{a}{b} | a, b \in Z \land b \neq 0\} \\ The\ real\ number:\ R = the\ entire\ number\ line \end{gathered}$$

---

# Week 2

## The universal quantifier

For all: $\forall$ is the universal quantifier

## The existential quantifier

There exists: $\exists$ is the existential quantifier

`:` is such that

---

## Negation of quantified statements

### Universal statement

$$\begin{gathered} \forall x \in D, Q(x) \\ \downarrow \\ \exists x \in D, \neg Q(x) \end{gathered}$$

### Existential statement

$$\begin{gathered} \exists x \in D : R(x) \\ \downarrow \\ \forall x \in D, \neg R(x) \end{gathered}$$

---

## Valid and invalid arguments

> **An argument form is valid if, whenever all of the premises are true, then the conclusion is true also**

- Modus ponens (valid)

$$\begin{gathered} p \to q \\ p \\ \therefore q \end{gathered}$$

- Converse error (invalid)

$$\begin{gathered} p \to q \\ q \\ \therefore p \end{gathered}$$

- Inverse error (invalid)

$$
\begin{gathered}
p \to q \\
\neg p \\
\therefore \neg q
\end{gathered}
$$

Conjunction of the premises must be satisfy

---

## Valid arguments

- Modus ponens

$$
\begin{gathered}
p \to q \\
p \\
\therefore q
\end{gathered}
$$

- Modus tollens

$$
\begin{gathered}
\neg q \\
p \to q \\
\therefore \neg p
\end{gathered}
$$

- Hypothetical syllogism

$$
\begin{gathered}
p \to q \\
q \to r \\
\therefore p \to r
\end{gathered}
$$

- Disjunctive syllogism

$$
\begin{gathered}
p \vee q \\
\neg p \\
\therefore q
\end{gathered}
$$

- Addition

$$
\begin{gathered}
p \\
\therefore p \vee q
\end{gathered}
$$

- Simplification

$$
\begin{gathered}
p \wedge q \\
\therefore p
\end{gathered}
$$

- Conjunction

$$
\begin{gathered}
p \\
q \\
\therefore p \wedge q
\end{gathered}
$$

- Resolution

$$
\begin{gathered}
p \vee q \\
\neg p \vee r \\
\therefore p \vee r
\end{gathered}
$$

---

## Vacuous truth

For conditional, the **hypothesis** is **always false**, hence the conditional is a **tautology**

---

## Methods of proof

- **Direct proof**

  To show that P(x) $\to$ Q(x), choose an **arbitrary x** from the domain for which P(x) is true and use logical inference to show that **Q(x) is true also**

- **Proof by contradiction**

  Assume that p is false and use logical inference to prove a **contradiction**
- **Proof by contraposition**

  based on $p \to q \equiv \neg q \to \neg p$

  Choose some arbitrary x for which **Q(x) is false**, and argue by logical inference that **P(x) must be false also**
- **Disproof by counterexample**

---

## Without loss of generality (WLOG)

Use symmetry in the statement to reduce the number of cases to consider

---

# Week 3

## Set theory

A set S is a collection of object, which are called the elements of S

- If x is in S, $x \in S$, else, $x \notin S$
- $S = \{1, 2, 3\}$ is a finite set
- $S = \{0, 1, 2, 3, \dots\}$ is an infinite set
- Two set are equal if they contain the same elements

  $$S = T\ means\ \forall x,\ x \in S \leftrightarrow x \in T$$

  Order doesn't matter, repetition is ignored
- The empty set $\emptyset = \{\}$
- $x \neq \{x\}$

---

## Union

For sets S and T, their **union** is written $S \cup T$, contains all elements that belong to S or T

$$\bigcup_{i=1}^{5}\{i, 2i\} = \{0\} \cup \{1, 2\} \cup \{2, 4\} \cup \{\dots\}$$

## Intersection

For set S and T, their **intersection** is written $S \cap T$, contains all elements that belong to both S and T

$$\bigcap_{i=1}^{5}\{i, 2i\} = \{0\} \cap \{1, 2\} \cap \{2, 4\} \cap \{\dots\}$$

---

## Subsets

> **For sets S and T, S is a subset of T if every element of S belongs to T also**

$$S \subseteq T \; means \; \forall x, \; x \in S \rightarrow x \in T$$

### Proper subset

If $S \subseteq T$ and $S \neq T$

---

## Cardinality

> **If S is a finite set, then the cardinality of S is the number of distinct elements that S contains**

For **infinite set**, $|S| = \infty$, but two infinite sets might not have the same cardinality, $|R| \neq |Z|$

---

## Difference

For set S and T, their difference is written $S \backslash T$ or $S - T$, contains all elements that belong to S but not T

$$S \backslash T = \{x | x \in S \land x \notin T\}$$

---

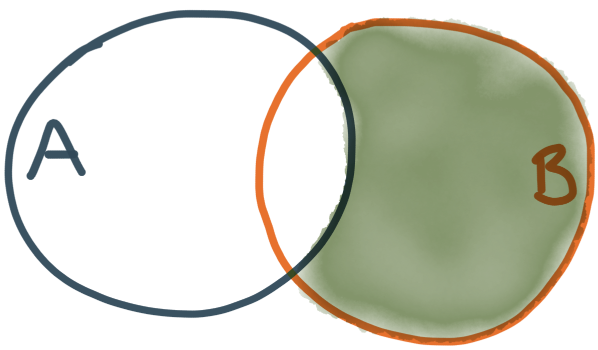
## Complement

Let U be some universal set, for any set S $\subseteq$ U, the **complement** of S is written $\bar{S}$

$$\bar{S} = \{x \in U | x \notin S\}$$

---

## Venn Diagrams



## Set identities

Same as logic equivalences

## Interval notation

- $[a, b] = \{x \in R | a \leq x \leq b\}$, a **square** bracket means **include** the endpoint
- $(a, b) = \{x \in R | a < x < b\}$, a **round** bracket means **exclude** the endpoint
- Never allowed to include $\infty$ or $-\infty$

## Power sets

> **For any set S, the power set of S is the set of all subsets of S**

$$P(S) = \{X | X \subseteq S\}$$
$$* \, include \; \emptyset$$

**If |S|=n, |P{S}|=** $2^n$

## Cartesian product

The Cartesian product of A x B is $A \times B = \{(a, b) | a \in A, b \in B\}$

**If |A|=n, |B|=m, |AxB|=n*m**

## Function

Let X and Y be sets, if f assigns to each x $\in$ X a **unique** element y $\in$ Y, then f is called a function from X to Y, written f: X $\rightarrow$ Y, x $\mapsto$ y or y = f(x)

unique means one and only one

function is a **subset** of a Cartesian product

If f: X $\rightarrow$ Y, then

- X is called the **domain** of f
- Y is called the **co-domain** of f
- If x $\in$ X, then f(x) is called the **image** of x
- If A $\subseteq$ X, then f(A) is called the **image** of A, the entire f(X) is called the **range** of f
- If y $\in$ Y, then $f^{-1}$(y)={x $\in$ X|f(x) = y}$\subseteq$X is called the **preimage** of y
- If B $\subseteq$ Y, then $f^{-1}$(B)={x $\in$ X|f(x) $\in$ B } $\subseteq$X is called the **preimage** of B

# Week 4

# Equality of functions

Function f, g: X $\rightarrow$ Y are equal, written f = g, if and only if

$$f(x) = g(x) \ for \ all \ x \in X$$

$*$ f denotes a **function**, f(x) denotes an **element** of Y

---

# Floor and ceiling

## Floor (Definition)

> **Let x $\in$ R be a real number. The floor of x, denoted $\llcorner x \lrcorner$, is the unique integer n such that n $\leq$ x $<$ n+1**

## Ceiling (Definition)

> **Let x $\in$ R be a real number. The ceiling of x, denoted $\ulcorner x \urcorner$, is the unique integer n such that n -1$<$ x $\leq$ n**

- $\forall x \in R : \llcorner x - 1 \lrcorner = \llcorner x \lrcorner - 1$
- For all x $\in$ R and all n $\in$ Z, we have $\llcorner x + n \lrcorner$ = $\llcorner x \lrcorner + n$

---

# Properties of function

Let f: X $\rightarrow$ Y, then

1. f is **onto, surjective, surjection** if:

   $\forall y \in Y, \exists x \in X \ such \ that \ f(x) = y$

   Every y is the image of something

   - $|X| \geq |Y|$
2. f is **one-to-one, injective, injection** if:

   $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \rightarrow x1 = x2$

   Different elements of X have different images

   - $|X| \leq |Y|$
3. f is a **one-to-one correspondence, bijective, bijection** if f is both one-to-one and onto
   - $|X| = |Y|$

---

# Composition of function

If f: X $\rightarrow$ Y and g: Y $\rightarrow$ Z, then the composition

$$g \circ f : X \rightarrow Z = g(f(x)) \ for \ all \ x \in X$$

---

## The Tower of Hanoi

- Recursive definition: $T_0 = 0 \; and \; T_n = 2 \times T_{n-1} + 1$
- Explicit formula, closed formula: $T_n = 2^n - 1$

---

## Types of sequences

finite, infinite, index (subscript), alternating

To define a sequence recursively:

- **Initial conditions**
- **A recurrence relation**

---

## Notation of sums

$$\sum_{m}^{n} a_i = a_m + a_{m-1} + a_{m+2} + \ldots + a_{n-1} + a_n$$

- If m > n, $\sum_m^n a_i$ = 0
- $\sum_m^n a_i \pm \sum_m^n b_i = \sum_m^n (a_i + b_i)$
- $\sum_m^n ca_i = c \sum_m^n a_i$
- $\sum_{i=p}^q a_i + \sum_{i=p+1]}^r a_i = \sum_{i=p}^r a_i$
- $\sum_{i=p}^q a_i = \sum_{i=m+p}^{n+p} a_{i-p} = \sum_{i=m-q}^{n-q} a_{i+q}$
- $\sum_{i=p}^q (a_i - a_{i+1}) = a_m - a_{n+1}$ if m $\leq$ n

---

## Divisibility

> **If n, d $\in$ Z, then n is divisible by d if and only if there exists some k $\in$ Z such that n = kd, written d|n**

- $\forall a, b, m \in Z, (m|a) \wedge (m|b) \rightarrow m|(a+b)$
- Let n, d $\in$ Z. If $|n| \geq 1$ and d|n, then $0 < |d| \leq |n|$, **bounds on divisors**
- **The Quotient-Remainder Theorem**

  Given any integer n and positive integer d, there exist **unique** integers q and r such that

  $$n = qd + r \; and \; 0 \leq r < d$$

  q is the **quotient**, r is the **remainder**
- $If \; n = qd + r, \; then \; n \equiv r(mod \; d)$
- $n \equiv m(mod \; d) \; if \; and \; only \; if \; d|(n-m)$
- $n \equiv 0(mod \; d) \; if \; and \; only \; if \; d|n$
- $$\begin{gathered} If \; a \equiv b(mod \; d) \; and \; n \equiv m(mod \; d) \\ 1. an \equiv bm(mod \; d) \\ 2. a \pm n \equiv b \pm m(mod \; d) \end{gathered}$$

---

# Week 5

# Prime factorization (Definition)

> **A product of primes is the product of prime numbers $p_1, p_2, p_3, ..., p_m$**
>
> $$n = p_1 * p_2 * ... * p_m = \prod_{k=1}^{m} p_k$$

- Every natural number n>1 can be written as a product of primes

# GCD and LCM

- The greatest common divisor of the integers a and b, is the **largest $d \in N$ for which d|a and d|b**
- The least common divisor of the positive integers a and b, is the **smallest $n \in N$ for which a|n and b|n**

If a and b are integers that are not both equal to zero, then gcd(a, b) exists

Two Integers $a, b \in Z$ are called **coprime** if gcd(a, b) =1

- If $a, b \in Z$ are coprime and $ab = c^3$ for some $c \in Z$, then $a = d^3$ and $b = e^3$ for some $d, e \in Z$

For all $a, b \in Z$

1. $$gcd(a, b) = gcd(b, a - b)$$
2. If a = bq +r

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

---

# Base b expansion (Definition)

> **Let b be an integer greater than 1, every positive integer n can be expressed uniquely in the form**
>
> $$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

---

# Running time

number of steps required for it to finish, running time is a function:

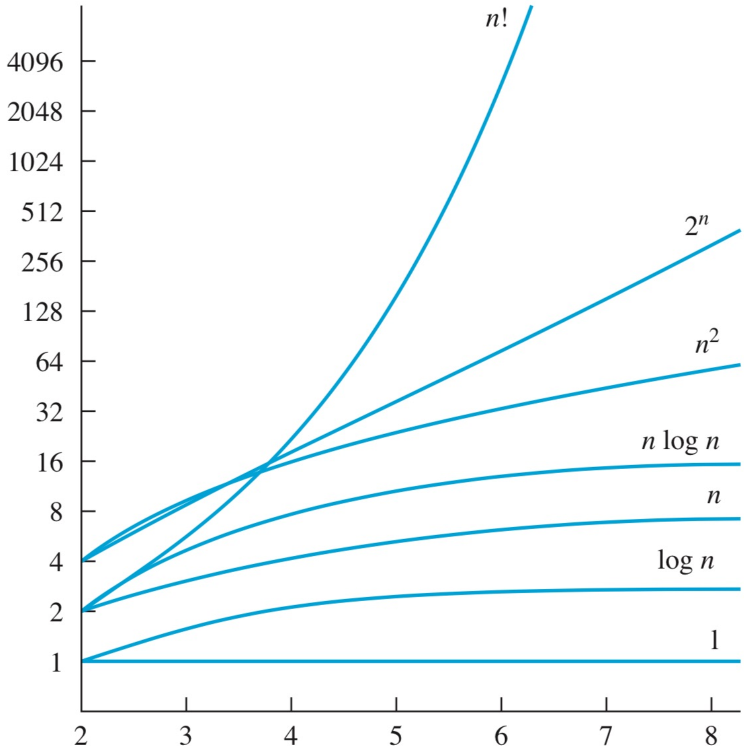
$$f : N \to N; Input\ size \mapsto Number\ of\ steps\ required$$

## O-notation (Definition)

> **Let f and g be functions from a subset of R to R. Then f(x) is in O(g(x)) if there exist constants C and k such that for all $x \in A, x \geq k$**
>
> $$|f(x)| \leq C|g(x)|$$

C and k are the **witnesses** of the statement "f(x) is in O(g(x))"

- $f(x) \in O(g(x))$ or $g(x) \in O(f(x))$ or $f(x) = O(g(x))$
- $f(n) \in O(f(n))$
- $O(c * f(n)) = O(f(n))$
- $O(f(n) + f(n)) = O(f(n))$
- $O(f(n)g(n)) = f(n) * O(g(n))$




$$n^d \in O(b^n) \; if \; d > 0 \; and \; b > 1$$
$$b^n \in O(c^n) \; and \; c \notin O(b^n) \; if \; c > b > 1$$
$$n! \in O(n^n)$$
$$log(n!) \in O(nlog(n))$$
$$log(x) \in O(x^\alpha)$$
$$3^n \notin O(2^n)$$

### $\Omega$-notation (Definition)

> **Let f and g be functions from a subset of R to R. Then f(x) is in $\Omega(g(x))$ if there are positive constants C and k such that for all x > k**
>
> $$|f(x)| \geq C|g(x)|$$

### $\Theta$-notation (Definition)

> **Let f and g be functions from a subset of R to R. Then f(x) is in $\Theta$(g(x)) if $f(x) \in O(g(x))$ and $f(x) \in \Omega(g(x))$**

---

# Week 6

## P vs NP

A decision problem is a yes/no question, for which we wish to find an algorithm

P: solve quickly

NP: inherently difficult

An algorithm is considered **fast** if its running time is bounded by a polynomial

- Fast: $O(n), O(n \log n), O(n^c)$
- Slow: $O(C^n) \; when \; C > 1, O(n!), O(e^{e^n})$

---

## The principle of mathematical induction

> **Let P(n) be a predicate that is defined for all integers** $n \geq a, a \in N$
>
> Suppose:
>
> 1. **Basis step: P(a) is true**
> 2. **Inductive step: For all integers** $n \geq a, P(n) \rightarrow P(n+1)$

### Bernoulli's inequality

> For all real x>0 and all integers $n \geq 2, (1+x)^n > 1+nx$

---

# Week 7

## Counting and probability

- Sample space S
- Event E
- Probability

$$P(E) = \frac{number\ of\ outcomes\ in\ E}{number\ of\ outcomes\ in\ S}$$

### Order matters, repetition allowed

$$|S_1 \times S_2 \times S_3 \times \ldots \times S_k| = \prod |Si|$$

Example: telephone number

### Order matters, repetition not allowed

choose k elements from a set S with n elements

$$P(n,k) = n*(n-1)*(n-2)*\ldots*(n-k+1) = \frac{n!}{(n-k)!}$$

Example: ranking

### Order does not matters, repetition not allowed

n choose k

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n*(n-1)*(n-2)*\ldots*(n-k+1)}{k!}$$

For all $n, k \in Z\ with\ 0 \leq k \leq n$

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

Example: n people shake hands at a party. What is the total number of handshakes?

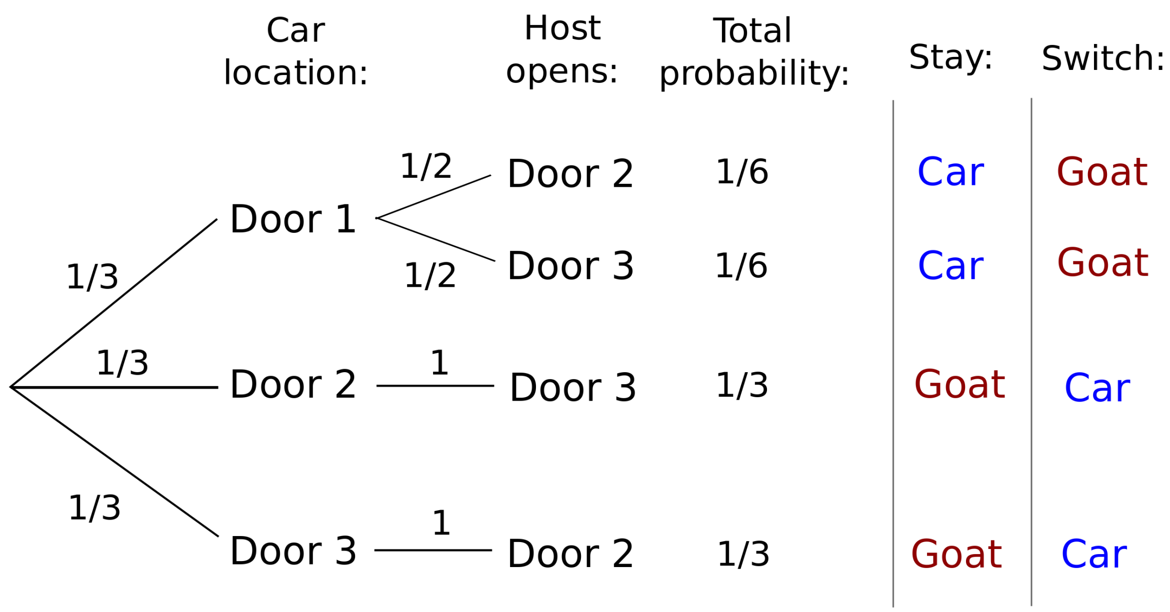
### Order does not matter, repetition allowed

$$\frac{(k+n-1)!}{k!(n-1)!} = \binom{n+k-1}{n-1}$$

Example: How many ways are there to put 2 balls (not distinguished) into 3 boxes (distinguished)?

---

## Monty Hall problem




---

## Binomial coefficients

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

The Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

> **For any finite set S, the number of subsets of S with an even number of elements is equal to the number of subsets of S with an odd number of elements**
>
> with even number: $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots$
>
> with odd number: $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots$

## Another equation

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

---

# Week 8

## The inclusion-exclusion principle

> **For any sets A and B**
>
> $$|A \cup B| = |A| + |B| - |A \cap B|$$

> **For sets** $A_1, A_2, \ldots, A_n$
>
> $$|A_1 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j|$$
> $$+ \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots \pm |A_1 \cap A_2 \cap \ldots \cap A_n|$$

## The generalized pigeonhole principle

> **If n pigeons sitting in k pigeonholes, and if n > k*m, then at least one of the pigeonholes contains at least m+1 pigeons**

## Ramsey theory

> Every graph on six vertices has at least a triangle or has an independent set of size three

---

## Catalan number

$$b_n = p_n = t_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!} < 4^n \ for \ n \geq 1$$

---

## Recurrences revisited

- $$a_n = \alpha a_{n-1} + \beta a_{n-2}$$
  $$1. Factor \ x^2 - \alpha x - \beta = (x - \lambda_1)(x - \lambda_2)$$
  $$2a. If \ \lambda_1 \neq \lambda_2, then \ a_n = A\lambda_1^n + B\lambda_2^n \ for \ some \ constants \ A \ and \ B$$
  $$2b. If \ \lambda_1 = \lambda_2, then \ a_n = C\lambda^n + Dn\lambda^n, \ where \ \lambda = \lambda_1 = \lambda_2 \ and \ C \ and \ D \ are \ some \ constants$$
- $$a_n = \alpha a_{n-1} + \beta a_{n-2} + f(n)$$
  $$1. Find \ one \ particular \ solution \ a_n^{(p)} \ by \ assume \ a_n = Af(n) \ and \ calculate \ the A$$
  $$2. Determine \ the \ general \ solution \ a_n^{(h)} \ to \ the \ homogeneous \ equation \ a_n = \alpha a_{n-1} + \beta a_{n-2}$$
  $$3a. \ LHS: a_n = A\lambda_1^n + B\lambda_2^n + A' f(n)$$
  $$3b. \ LHS: a_n = C\lambda^n + Dn\lambda^n + A' f(n)$$

---

# Week 9

## Random variable (Definition)

> **A random variable is a function X:** $S \rightarrow R$ **defined on the outcomes of a sample space**

- Sample space S, $|S| < \infty$
- $x \in S$ is called an outcome, {x} is called an elementary event
- $E \subseteq S$ is called an event

---

## Conditional probability

> **Let E and F be events with p(F) > 0, The conditional probability of E given F is**
>
> $$p(E|F) = \frac{p(E \cap F)}{p(F)}$$

---

## Independence

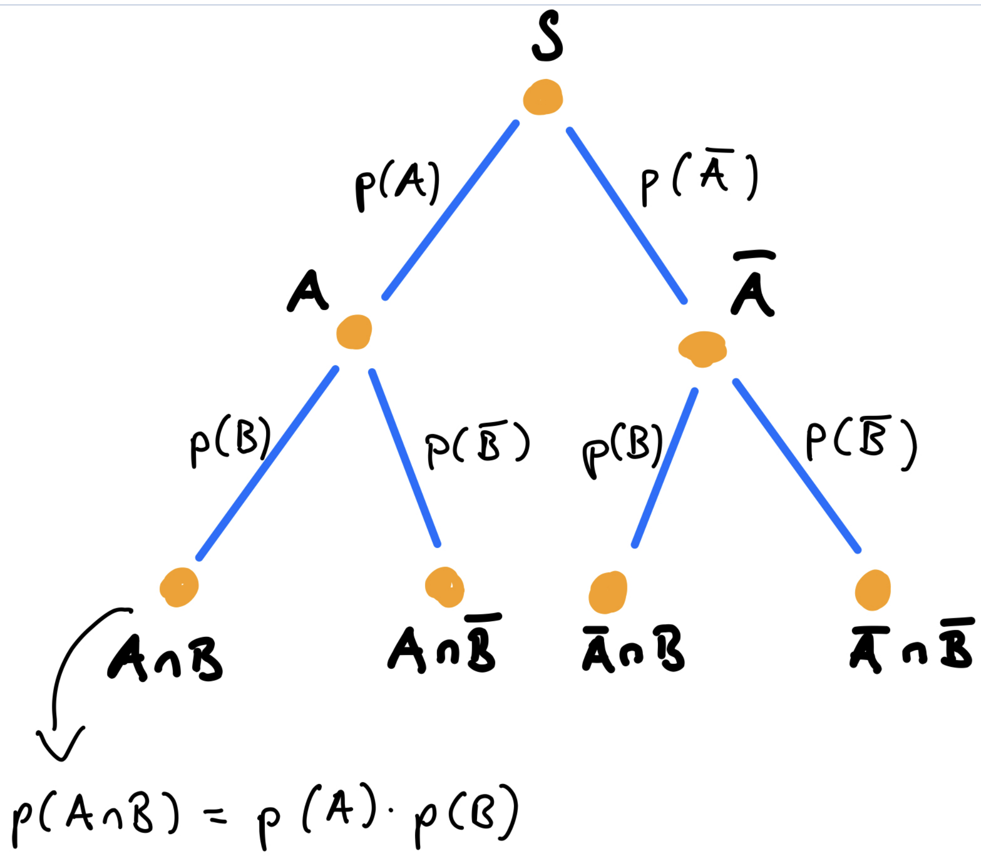
1. $p(E|F) = p(E)$
2. $p(E \cap F) = p(E)p(F)$

If any of the above hold, E and F are called independent

---

## Bayes' theorem

> **Suppose E and F are events from a a sample space S with p(E) > 0 and p(F) > 0**
>
> $$p(F|E) = \frac{p(F)}{p(E|F) * p(F) + p(E|\bar{F}) * p(\bar{F})} * p(E|F)$$
> $$p(E) = p(E|F) * p(F) + p(E|\bar{F}) * p(\bar{F})$$




---

## Expected value

> **The expected value, also called the expectation or mean**
>
> $$E(X) = \sum_{s \in S} p(s)X(s)$$

- $E(aX + b) = aE(X) + b$

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

## Variance

> $$V(X) = \sum_{s \in S}(X(s) - E(X))^2 p(s)$$

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

---

# Week 10

## Relation (Definition)

> **Let X and Y be sets, a relation R from X to Y is a subset of $X \times Y$**
>
> Written $(x, y) \in R, xRy, x \sim y$
>
> **The complementary relation to R is $\bar{R} = (X \times Y) \backslash R$**
>
> **If X=Y we say that R is a relation on X**
>
> **Compose relations**
>
> $$S \circ R = \{(a, c) | \exists b \in Y : aRb \wedge bSc\} \subseteq X \times Z$$

## Reflexive, Symmetric, Transitive

- **Reflexive** provided that $(x, x) \in R \; for \; all \; x \in X$
- **Symmetric** provided that if $(x, y) \in R \; then \; (y, x) \in R$
- **Transitive** provided that if $(x, y) \in R \; and \; (y, z) \in R, then \; (x, z) \in R$

---

## Equivalence relation and Partition

### Equivalence relation

If set X is reflexive, symmetric and transitive

- 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

  - $[x] \neq \emptyset \; for \; all \; x \in X$
  - $X = \bigcup_{x \in X} [x]$
  - $$[x] \cap [y] = \begin{cases} \emptyset & \text{if} \quad (x, y) \notin R \\ [x] = [y] & \text{if} \quad (x, y) \in R \end{cases}$$

  Example:

  - $$\begin{gathered} (m, n) \in R \; if \; and \; only \; if \; 3 | (m - n) \\ [0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ [1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ [2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{gathered}$$

### Partitions

If $A \cap B = \emptyset$, then A and B are disjoint

> **A set $\{S_1, S_2, ...\}$ is a partition of S if**
>
> $$1. S_i \neq \emptyset \; for \; all \; i$$
> $$2. S = S_1 \cup S_2 \cup ...$$
> $$3. S_i \cap S_j = \emptyset \; whenever \; i \neq j$$

- An equivalence relation on X gives a partition of X
- A partition of X gives an equivalence relation on X

---

## Anti-symmetric

- Symmetric

$$\forall a, b \in X, (a, b) \in R \; implies \; (b, a) \in R$$

- Anti-Symmetric

$$\forall a, b \in X, (a, b) \in R \; and \; (b, a) \in R \; implies \; a = b$$

- Partial order

  A relation on a set X which is reflexive, transitive, and anti-symmetric

- Total order

$$\forall a, b \in X, aRb \; or \; bRa$$

---

## Closure

### Reflexive closure

$$ref(S) = R \cup \Delta = R \cup \{(x, x) | x \in X\}$$

### Symmetric closure

$$sym(R) = R \cup R^{-1} = R \cup \{(y, x) | (x, y) \in R\}$$

### Transitive closure

$$tra(R) = R \cup R^{\star} = \bigcup_{k=1}^{\infty} R^k$$

---

# Week 11

## Graph theory

A graph G consists of two finite sets:

1. a non-empty set V(G) of **vertices**
2. a (possibly empty) set E(G) of **edges**

- **Loop**: An edge may have endpoints {v, v} = {v}
- **Parallel edges**: Two edges may have the same end points {v, w}

- **Simple graph**: A graph with no loops or parallel edges
- **Incident**: v is an endpoint of e
- **Adjacent**: There is an edge with endpoints {u, v}
- **Degree**: The number of edges incident with v, loop will be counted twice

---

## The handshake theorem

> **Let G be a graph with n vertices** $V(G) = v_1, \ldots, v_n$
>
> $$\sum_{i=1}^{n} deg(v_i) = deg(v_1) + \ldots + deg(v_n) = 2 * |E(G)|$$
>
> **In any graph, the number of vertices of odd degree is even**

---

## Directed graphs

- The **in-degree** $deg^-(v)$ is the number of edges terminating in v
- The out-degree $deg^+(v)$ is the number of edges starting in v
- $$\sum_{i=1}^{n} deg^-(v_i) = \sum_{i=1}^{n} deg^+(v_i) = |E(G)|$$

---

## Graph types

- Complete graphs: simple graph with exactly one edge between any pair of verties
- Cycles
- Wheels
- Cubes
- Trees
- Cactus graphs

---

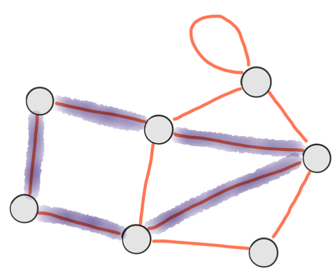
## Path

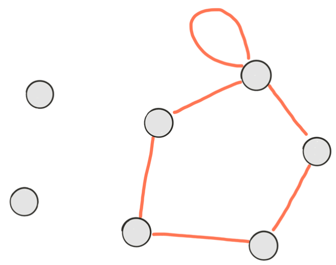
- **Connected**: $\forall x, y \in V(G),\ there\ is\ a\ path\ from\ x\ to\ y$
- **Disconnected**

---

## Eulerian circuit

> **Starts and ends at the same vertex, and uses every edge exactly once**
>
> **Connected graph and if and only if every vertex degree is even**





### Eulerian trail

> Using each edge exactly once, but whose start and end vertices **can be different**
>
> Except **two vertices** can have **odd** degree, every vertex degree is **even**

---

## Hamiltonian circuits

> Using every vertex exactly one (except for start = end vertex)

---

## Graph isomorphism

> Two graphs $G_1 = (V_1, E_1)$ and $G_1 = (V_2, V_2)$ are said to be isomorphic, written $G_2 \cong G_2$ if there exists a bijective function such that
>
> $$\phi(E_1) = \{\{\phi(v_1), \phi(v_2)\} | \{v_1, v_2\} \in E_1\} = E_2$$

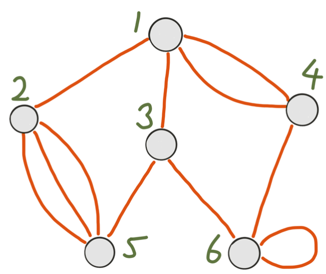
---

## Matrices

The product AB is an $n \times n$ matrix with entries

$$m_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j} = a_{i,1} b_{1,j} + a_{i,2} b_{2,j} + \ldots + a_{i,n} b_{n,j}$$

### Representing graphs using matrices




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

> **The adjacency matrix of G is the $n \times n$ matrix $A = (a_{i,j})$, where each entry $a_{i,j}$ is the number of edges with endpoints {i,j}**

> **Let G be a graph, the number of paths of length k from vertex i to vertex j is the entry in row i, column j of the $k^th$ power $A^k = A * A * \ldots * A$, a single path with k loop edges is counted $2^k$ times**

---

# Week 12

## Bipartite graphs

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 colored with two color such that no two adjacent vertices have the same color
3. Every circuit in G has even length

---

## Hall's marriage theorem

Complete matching from $V_1$ to $V_2$ if every vertex in $V_1$ is incident with an edge in M

> **Let G be a bipartite graph with partition $\{V_1, V_2\}$ of the vertices. There is a complete matching from $V_1$ to $V_2$ if and only if $|A| \leq |N(A)|$ for all $A \subseteq V_1$**

Hall violater: $|N(A)| < |A|$

---

## Finite state machine

A **finite state machine** $M = (S, I, O, f, g, s_0)$ consists of

- a finite set S of **states**
- a finite **input alphabet** I
- a finite **output alphabet** O
- a **transition function** $f : S \times I \to S$
- an **output function** $g : S \times I \to O$
- an initial state $s_0$

### Formal languages

- A formal language L is a set of strings with symbols in A
- The empty string is denoted $\lambda$

### Grammars

A phase-structure grammar $G = (V, T, S, P)$ consists of

- a vocabulary V
- a subset $T \subseteq V$ of terminal symbols
- a start symbol $S \in V$
- a finite set of productions P