MATH1064

Usyd Mingyuan Ba

November 18, 2023

1 Week1

(i) **Definitions**

- Propositions : A proposition is a sentence that is true or false but not both.
- Variables and Compound Propositions : We use capital letters for compound propositions, which are made up from proposition variables (e.g. p, q,r, ...) and the symbols with $\wedge, \vee, \neg$ and unambiguous parentheses.
- Logical equivalence : 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 : A contradiction is a compound proposition which takes the value false for all possible truth values (true/false in all combinations) of its variables.
  Examples: $p \wedge \neg p$,$(q \wedge p) \wedge \neg p$
- Tautology : A tautology is a compound proposition which takes the value true for all possible truth values (true/false in all combinations) of its variables.
  Examples: $p \vee \neg p$

  ==========

==========

- The conditional : Let p and q be proposition variables; the conditional from p to q, p $\rightarrow$ q, is defined by the following truth table:

p	q	p $\rightarrow$ q
T	T	T
T	F	F
F	T	T
F	F	T

p is the hypothesis and q is the conclusion.

Different ways of saying p $\rightarrow$ q:
1 p implies q
2 if p, then q
3 q if p
4 p only if q
5 p is sucient for q
6 q is necessary for p

p $\rightarrow$ q is false if and only if it describes a counterexample; that is, the hypothesis is true but the conclusion is false.

$p \rightarrow q \equiv \neg p \vee q$

- Converse : The converse of $p \rightarrow q$ is $q \rightarrow p$.
- Inverse : The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.
- The biconditional : Let p and q be proposition variables; the biconditional from p to q, p $\Leftrightarrow$ q, is defined by the following truth table:

p	q	p $\Leftrightarrow$ q
T	T	T
T	F	F
F	T	F
F	F	T

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

- Satisfiability : A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true. Otherwise it is unsatisfiable.

==========

==========

- Predicates : A predicate is a sentence that contains finitely many variables, and which becomes a proposition (aka statement) if the variables are given specific values.
  Definition (Domain) : The domain of a variable in a predicate is the set of all possible values that may be assigned to it.
  Definition (Truth set) : The truth set of a predicate P(x) is the set of all values in the domain that, when assigned to x, make P(x) a true statement.

(ii) **Technological skills in Latex**

- The conjunction symbol: $p \wedge q$
- The disjunction symbol: $p \vee q$
- The negation symbol: $\neg p$
- The Logical equivalence symbol: $p \equiv q$

(iii) **Logical equivalence**

- Commutative Laws
  - $p \wedge q = q \wedge p$
  - $p \vee q = q \vee p$
- Associative laws
  - $(p \wedge q) \wedge r = p \wedge (q \wedge r)$
  - $(p \vee q) \vee r = p \vee (q \vee r)$
- Distributive laws
  - $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee q)$
- De Morgan's laws
  - $\neg(p \wedge q) = \neg p \vee \neg q$
  - $\neg(p \vee q) = \neg p \wedge \neg q$
- Absorption laws
  - $p \vee (p \wedge q) = \mathrm{p}$
  - $p \wedge (p \vee q) = \mathrm{p}$

==========

==========

- Equivalences OF implies
  - $p \to q = \neg p \vee q$
  - Prove:$(p \to r) \vee (q \to r) = (p \vee q) \to r$:
    $(p \to r) \wedge (q \to r) = (\neg p \vee r) \wedge (\neg q \vee r)$
    $= (\neg p \wedge \neg q) \vee r$ distributive laws
    $= \neg(p \vee q) \vee r$
    $= (p \vee q) \to r$

==========

==========

2 Week2

(i) **Definitions**

- The universal quantifier : $\forall$ For all
  Every real number is non-negative or non-positive
  $\equiv$ For all r$\in \mathbb{R}$, r≥ 0 or $r \leq 0$
  $\equiv \forall$ r$\in \mathbb{R}$, r≥ 0 or $r \leq 0$

- The existential quantifier : $\exists$ There exists
  There is a real number whose square equals 2.
  $\equiv \exists r \in \mathbb{R}$ such that $r^2 = 2$
  $\equiv \exists r \in \mathbb{R} : r^2 = 2$

- Negation of quantified statements :

  - Universal statement :$\forall x \in D : Q(x)$
    The negation of this statement is logically equivalent to: $\exists x \in D, \neg Q(x)$
  - Existential statement :$\exists x \in D : R(x)$
    The negation of this statement is logically equivalent to: $\forall x \in D, \neg R(x)$

- Negating multiple quantifiers :
  $\exists x \in \mathbb{R} : \forall y \in \mathbb{R}, xy = 0$
  The negation of this statement is logically equivalent to:
  $\forall x \in \mathbb{R} : \neg(\forall y \in \mathbb{R}, xy = 0)$

- Valid and invalid arguments :An argument form is valid if, whenever all of the premises are true, then the conclusion is true also.
  Otherwise the argument form is invalid.

  - Valid
    1.$p \to q$ ——(premise)
    2.p ——(premise)
    c.. . . q ——(conclusion)
  - Invalid (converse error)
    1.$p \to q$ ——(premise)
    2.q ——(premise)
    c.. . . p ——(conclusion)
  - Invalid (inverse error)
    1.$p \to q$ ——(premise)
    2.$\neg p$ ——(premise)
    c.. . . $\neg q$ ——(conclusion)

==========

==========

To be valid, in every row where the premises are all true , the conclusion must be true. It does not matter what happens in rows where some of the premises are false.
The argument form with premises $p1, ..., pk$ and conclusion c is valid if and only if $p1\wedge, ..., \wedge pk \implies c$ is a tautology

- Rules of inference :
  - Modus ponens and Modus tollends(method of denying)
    - Modus Ponens :
      If $p \to q$ and p
      then q.
    - Modus Tollens :
      If $p \to q$ and $\neg q$
      then $\neg p$.
  - Hypothetical Syllogism and Disjunctive Syllogism
    - Hypothetical Syllogism:
      If $p \to q, q \to r$
      then $p \to r$
    - Disjunctive Syllogism:
      If $p \vee q$ and $\neg p$
      then q.
  - Addition (generalisation) and Simplification (specialisation):
    - Addition (generalisation) :
      If P
      then $P \vee Q$
    - Simplification (specialisation):
      If $P \wedge Q$
      then P
  - resolution(uncompleted)

==========

==========

- Vacuous truth : A vacuous truth is a statement that asserts that all members of an empty set have a certain property. Because the set is empty, the statement is considered true regardless of the property being discussed. This might sound confusing at first, but it's a logical convention that has been accepted in mathematics and formal logic.

  Example 1 :
  For all real numbers r such that $r^2 = 1$,we have $r > r$.
  There is no real number for which $r^2 = -1$.
  This means that $r^2 = 1$ is always false, and so the conditional:
  $(r^2 = -1) \rightarrow anything$ is always true.
  In symbols:
  $\forall r \in \mathbb{R}, (r^2 = -1) \rightarrow (r > r)$
  is a true proposition.
  There is no real number for which $r^2 = -1$, so the conditional is always true since its hypothesis is always false. Hence the conditional is a tautology. We call this vacuous truth.

  Example 2 :
  Premises : $(\neg R \vee P), (\neg J \rightarrow \neg P), (R \wedge \neg J)$

(1)	$\neg R \vee P$		(1)
(2)	$\neg J \rightarrow \neg P$		(2)
(3)	$R \wedge \neg J$		(3)
(4)	R	(Specialisation from (3))	(4)
(5)	$R \vee G$	(Generalisation from (4))	(5)
(6)	$\neg J$	(Specialisation from (3))	(6)
(7)	$\neg P$	(Modus ponens from (6) and (2))	(7)
(8)	$\neg R$	(Elimination from (7) and (1))	(8)
(9)	G	(Elimination from (8) and (5))	(9)

  but

==========

==========

1.$\neg R \vee P$
2.$\neg J \rightarrow \neg P$
3.$R \wedge \neg J$
4.R (Specialisation from (3))
5.$R \vee \neg G$ (Generalisation from (4))
6.$\neg J$ (Specialisation from (3))
7.$\neg P$ (Modus ponens from (6) and (2))
8.$\neg R$ (Elimination from (7) and (1))
9.$\neg G$ (Elimination from (8) and (5))

Problem: The conjunction of the premises is a contradiction.

$$(\neg R \vee P) \wedge (\neg J \rightarrow \neg P) \wedge (R \wedge \neg J)$$

In other words: the premises are inconsistent.
We have seen that one can derive anything from this contradiction:

$$(\neg R \vee P) \wedge (\neg J \rightarrow \neg P) \wedge (R \wedge \neg J) \wedge p4 \wedge \ldots \wedge p8$$

$\rightarrow X$, where X = your favourite statement.

- Implicit quantification:
  Mathematicians often say things like:
  If x is larger than 3, then x^2 is larger than 9.

  This is not a statement, since we do not know the value of x. We are just being lazy: there is an implicit $\forall$ in here.
  $\forall x \in \mathbb{R}, x > 3 \rightarrow x^2 > 9$

- Methods of proof :
  - **Direct Proof** :
    To show that $P(x) \rightarrow Q(x)$, 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 :**
    To show that p is true,
    assume that p is false
    and use logical inference to prove a contradiction.

    Example :
    Lemma : For all $n \in \mathbb{N}$,n is either even or odd.

Proof: Assume the lemma is false. Choose the **smallest** $n \in \mathbb{N}$ that is neither odd nor even.
If $n > 0$, then it follows that n - 1 is either odd or even.

(i)If $n - 1$ is odd,
then $n - 1 = 2k + 1$ for some $k \in \mathbb{Z}$.
Thus $n = 2k + 2 = 2(k + 1)$, and so n is even.

(ii)If $n - 1$ is even,
then $n - 1 = 2k$ for some $k \in \mathbb{Z}$.
Thus $n = 2k + 1$, and so n is odd.

In all cases, n is either odd or even, contradicting our choice of n. Therefore every $n \in \mathbb{N}$ is either odd or even.

- **Proof by contraposition :**
  Key idea: To prove $\forall x, P(x) \rightarrow Q(x)$: Choose some arbitrary x for which Q(x) is false, and argue by logical inference that P(x) must be false also.(logically depends on $p \rightarrow q \equiv \neg q \rightarrow \neg p$)

  Example :
  Lemma,For all $n \in \mathbb{N}$, if n^2 is odd then n is odd.

  Proof : choose any $n \in \mathbb{N}$ that is not odd, which means n is even.
  Therefore,n = 2k for some $k \in \mathbb{Z}$,and so $n^2 = (2k)^2 = 2 * (2k)^2$
  Therefore,n^2 is even ,which also indicates n is not odd.
  So: if n^2 is not odd, then n is not odd. By the contrapositive, this means that if n^2 is odd then n is odd.
- **Disproof by counterexample :**
  Key idea: To disprove a statement $\forall x, P(x)$ – that is, to show that the statement is false – we simply need to show one example of an x for which P(x) is false. This x is called a counterexample.

- Prime and composite :
  - prime : The natural number n is prime if and only if n $>$ 1 and, for all $r, s \in \mathbb{N}$, if n = r $\cdot$ s then r = 1 or s = 1.
    which is : $\forall r, s \in \mathbb{N}, (n = r * s) \rightarrow (r = 1 \vee s = 1)$
  - composite:
    The natural number n is composite if and only if n ¿ 1 and n = r $\cdot$ s for some $r, s \in N$ with $r \neq 1$ and $s \neq 1$.
    which is $\exists r, s \in \mathbb{N}$ such that $n = r * s \wedge r \neq 1 \wedge s \neq 1$

    If n $>$ 1, then n is either prime or composite, but not both.
    proof : $\neg(\forall r, s \in \mathbb{N}, (n = r * s) \rightarrow (r = 1 \vee s = 1))$

$\equiv \exists r, s \in \mathbb{N}, \neg((n = r * s) \rightarrow (r = 1 \vee s = 1))$ ——**(negation of quantified statements)**
$\equiv \exists r, s \in \mathbb{N}, \neg(\neg(n = r * s) \vee (r = 1 \wedge s = 1))$ ——**(condition to disconjunction)**
$\equiv \exists r, s \in \mathbb{N}, (n = r*s) \wedge \neg(r = 1 \vee s = 1)$ ——**(De Morgan's laws)**
$\equiv \exists r, s \in \mathbb{N}\ , n = r * s \wedge r \neq 1 \wedge s \neq 1$ ——**(De Morgan's laws)**

- Prime factorisation :
  Proof : Every natural number n > 1 can be written as a product of primes. Suppose the theorem is false. Then there exists a natural number n > 1 that is not a product of primes.

  Choose the smallest such number n. From the previous lemma, either n is prime or n is composite. We take cases:

  If n is prime, then n is trivially a product of primes (n = n).
  If n is composite, then n = r · s for natural numbers $r \neq 1$ and $s \neq 1$.
  This implies that $1 < r < n$ and $1 < s < n$.

  ==========

==========

Because we chose n to be the smallest natural number that is not a product of primes, both r and s (which are smaller) must be products of primes. Therefore $n = r \cdot s$ is a product of primes also.
So, regardless of whether n is prime or composite, we find that n is a product of primes. This contradicts our choice of n.

Therefore every natural number $n > 1$ is a product of primes.

- Without loss of generality (WLOG) :
Key idea: Use symmetry in the statement to reduce the number of cases to consider.
WLOG means that no generality is lost by making a simplifying assumption: If the simple case is true then trivially all cases must be true.

Example :

For all $a, b \in \mathbb{Z}$, if ab and $a + b$ are even, then both a and b are even.

By contraposition suppose not both a and b are even.

Without loss of generality we may assume a is odd.

So $a = 2k + 1$ for some $k \in \mathbb{Z}$.

Case 1: b is even. Then $b = 2l$ for some $l \in \mathbb{Z}$. This gives

$$a + b = (2k + 1) + 2l = 2(k + l) + 1.$$

Hence $a + b$ is odd.

Case 2: b is odd. Then $b = 2l + 1$ for some $l \in \mathbb{Z}$. This gives

$$ab = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1.$$

Hence ab is odd.

In each case, not both $a + b$ and ab are even.

This completes the proof by contraposition.

==========

==========

3 W3

(i) Defintion

- Set theory:
  A set S is a collection of objects, which are called the elements of S If x is in S, we write $x \in S$ If not, we write x $\notin$ S.
  We can list the elements of S with curly braces: $S = \{x1, x2, ...\}$

  Example1:
  $S = \{2, 3, 4, 5\} = \{5, 4, 3, 2\}$ = {2,2,2,2,3,4,5}
  $3 \in \mathbb{S}$,but $1 \notin \mathbb{S}$
  This is a finite set.

  Example2:
  $\mathbb{N} = \{0, 1, 2, 3, ...\}$
  This is a infinite set.

- Empty set
  The empty set, written $\emptyset$, contains no elements at all: $\emptyset = \{\}$
  Formally, when we say that $\emptyset$ is the empty set, we mean:
  $\forall x, x \notin \emptyset$

  A one-element set $\{x\}$ is not the same as x: $2 \neq \{2\}$

- Union
  For sets S and T, their union is written S $\cup$ T. It contains all elements that belong to S or T (possibly both):
  $\forall x, x \in S \cup T \leftrightarrow (x \in S \vee x \in T)$

- Intersection
  For sets S and T, their intersection is written $S \cap T$. It contains all elements that belong to both S and T:
  $S \cap T = \{x | x \in S \wedge x \in T\}$

- Subsets
  For sets S and T, we say that S is a subset of T if every element of S belongs to T also.
  We write this as $S \subseteq T$.
  Formally: $S \subseteq T$ means $\forall x, x \in S \rightarrow x \in T$

==========

==========

- Sets of Sets
  Sets can contain other sets: $\{1, \{2, 3\}, \{1, \{\{4\}\}\}\}$
  What about: $S = \{x | x \notin x\}$
  Is $S \in S$?

  - If S $\in$ S, then (by definition of S) we have S $\notin$ S.
  - If S $\notin$ S, then (by definition of S) we have S $\in$ S.
    This is Russell's paradox

    we can use "the" empty set $\emptyset$ as a starting point. From here we can build other sets:
    $\{\emptyset\} = \{\{\}\}$
    $\{\emptyset, \{\emptyset\}\} = \{\{\}, \{\{\}\}\}$
    $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
    . . . and so on

    We can, if we like, give these sets names:
    $0 = \emptyset$
    $1 = \{\emptyset\} = \{0\}$
    $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
    $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$

  To avoid problems such as Russell's paradox, we can attempt to define all sets recursively:
  1.Base : $\emptyset$ is a set
  2.Recursion: We define several operations that build new sets from old
  This is very delicate, and is another topic for another course. However, we will see some of these operations in a moment.

- Cardinality
  If S is a finite set, then the cardinality of S is the number of distinct elements that S contains.
  We write this as $|S|$.
  If S is an infinite set, we often write $|S| = 1$. However, cardinality is more interesting and more subtle: there are many different infinities, and two infinite sets might not have the same cardinality.
  For example, $|R| \neq |Z|$, even though both are infinite.

==========

==========

For sets S and T, their difference is written S \ T (or sometimes written S \ T).
It contains all elements that belong to S but not T:
$S \backslash T = \{x | x \in S \wedge x \notin T\}$

- Complement:
  Let U be some universal set in which we are working.
  For example, the universal set might be:
  - R if we are doing calculus
  - Z if we are doing number theory
  - the set of all points on the plane if we are doing geometry

  For any set $S \subseteq U$, the complement of S is written $\bar{S}$.
  It contains all elements of U that do not belong to S:
  $\bar{S} = \{x \in U | x \notin S\}$

- Summary: Relationships and operations
  - $S \subseteq T \leftrightarrow (x \in S \rightarrow x \in T)$
  - $S = T \leftrightarrow (x \in S \leftrightarrow x \in T)$
  - $S = T \leftrightarrow (S \subseteq T \wedge T \subseteq S)$

  - $S \cup T = \{x | x \in S \vee x \in T\}$
  - $S \cap T = \{x | x \in S \wedge x \in T\}$
  - $S \backslash T = \{x | x \in S \wedge x \notin T\}$
  - $\bar{S} = \{x \in U | x \notin S\}$

- Venn diagrams

- Power Sets
  For any set S, the power set of S is the set of all subsets of S. We write this as $P(S)$:
  $P(S) = \{X | X \subseteq S\}$
  If $S = \{3, 5\}$: $P(S) = \{\emptyset, \{3\}, \{5\}, \{3, 5\}\}$

- The cardinality of the power set
  Suppose S is a finite set with n elements, i.e., $|S| = n$.
  What is $|P(S)|$? — 2^n

==========

==========

- Cartesian product
  For sets, order does not matter: {a, b} = {b, a}
  We write (a, b) for an ordered pair.
  Here order and repetition do matter:
  (a, b) = (c, d) if and only if a = c and b = d.

  Example: $(3, 5) \neq (5, 3)$
  Example: $(3, 3) \neq 3$

  The Cartesian product A × B of sets A and B is:
  $A \times B = \{(a, b) | a \in A, b \in B\}$
  Example: If A = $\{a, b\}$ and B = $\{2, 3\}$, then
  $A \times B = \{(a, 2), (a, 3), (b, 2), (b, 3)\}$.

- Suppose X and Y are finite sets with $|X| = n$ and $|Y| = m$. What is $|X \times Y|$?
  $|X \times Y| = n \cdot m$

  - If $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset$
  - $A \times B = B \times A$ if and only if $A = B$

- Function:
  Let X and Y be sets. Then f is called a function from X to Y , written f : $X \to Y$, if it assigns to each $x \in X$ a unique element $y \in Y$. In mathematics, "unique" means "one and only one". We write $y = f(x)$ and sometimes abbreviate this to $x \mapsto y$.
  Examples:

  - f : $\mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$
  - g : $\mathbb{N} \to \mathbb{N}$ defined by $n \mapsto 2^n$
  - sin: $\mathbb{R} \to \mathbb{R}$

  Are these functions?

  1. $f\colon \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$
  2. $f\colon \mathbb{N} \to \mathbb{N}$ where $f(n) = n!$
  3. $f\colon \mathbb{N} \to \mathbb{N}$ where $f(n) = \frac{(n+1)(n+3)}{3}$
     No, since $f(n) \notin \mathbb{N}$ for some n.
  4. $f\colon \mathbb{N} \to \mathbb{N}$ where $f(n) = \frac{(n+1)(n+2)}{2}$
  5. $f\colon \mathbb{R} \to \mathbb{R}$ where $f(x) = 42$
  6. $f\colon \mathbb{Q} \to \mathbb{Z}$ where for all $m, n \in \mathbb{Z}$ with $n \neq 0$, $f(m/n) = m$
     No, since each rational has many different expressions m/n.
  7. $f\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ where $f((x, y)) = |x - y|$
  8. $f\colon \mathbb{R} \to \mathbb{R}$ where $f(x)$ is the solution $z \in \mathbb{R}$ to $3x + 1 = z$
  9. $f\colon \mathbb{R} \to \mathbb{R}$ where $f(x)$ is the solution $z \in \mathbb{R}$ to $z^2 = x$
     No, since $z^2 = x$ might have two solutions, or none.

==========

==========

- Formal definition of funtion
  We can think of a function as a subset of a Cartesian product:
  A function $f : X \to Y$ is a subset $\neg \subseteq X \times Y$ such that, for each $x \in X$, there is a unique $y \in Y$ such that $(x, y) \in \neg$. We write $f(x)$ to denote this unique y.
  Example: For $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$
  $\neg = \{(1, 1), (2, 4), (3, 9), (4, 16), ...\}$

  The subset :
  $\neg = \{(x, y) | x \in X \wedge f(x) = y\} \subseteq X \times Y$

  is the graph of the function f. We have :
  $\neg = \{(x, f(x)) | x \in X\} \subseteq X \times Y$

  If f: $X \to Y$ is a function, then:
  1. X is called the domain of f.
  2. Y is called the co-domain of f.
  3. If $x \in X$, then $f(x)$ is called the image of x.
  4. If $A \subseteq X$, then

     $$f(A) = \{f(x) \mid x \in A\} = \{y \mid \exists x \in A : f(x) = y\} \subseteq Y$$

     is called the image of A.
     The entire set $f(X)$ is called the range of f.
  5. If $y \in Y$, then $f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$
     is called the preimage of y.
  6. If $B \subseteq Y$, then $f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subseteq X$
     is called the preimage of B.

  Don't confuse f^{-1} with $\frac{1}{f}$.

==========

==========

4 W4

(i) Definitions

- Equality of functions:
  Functions $f, g : X \to Y$ are equal, written $f = g$, if and only if:
  $f(x) = g(x), \forall x \in X$
  Note: f denotes a function and $f(x)$ denotes an element of Y.

  Example: sin is a function; $sin(x)$ is just some number.

- Floor :
  Let $x \in \mathbb{R}$ be a real number. The floor of x, denoted $\lfloor x \rfloor$, is the unique integer n such that $n \leq x < n + 1$.

- Ceiling :
  Let $x \in \mathbb{R}$ be a real number. The ceiling of x, denoted $\lceil x \rceil$, is the unique integer n such that $n - 1 < x \leq n$.

- Properties of functions
  Let $f : X \to Y$. Then:

  - Surjective(onto) : $\forall y \in Y, \exists x$ in X such that $f(x) = y$
    Every element of Y is the image of something.
  - Injective(one - to- one): $\forall x1, x2 \in X, f(x1) = f(x2) \to x1 = x2$
    Different elements of X have different images
  - Bijective f is a one-to-one correspondence, or bijective, or a bijection, if f is both one-to-one and onto. The elements of X are "paired off" with the elements of Y

==========

Proving that a function is onto

Let $f: \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = \lfloor n/2 \rfloor$.

To show that f is onto, we need to show:

$$\forall y \in \mathbb{Z},\ \exists x \in \mathbb{Z} \text{ such that } f(x) = y.$$

Proof: Consider any $y \in \mathbb{Z}$. Let $x = 2y$.
Then:

- $x \in \mathbb{Z}$; that is, x belongs to the domain;
- $\lfloor x/2 \rfloor = \lfloor 2y/2 \rfloor = \lfloor y \rfloor = y$, and so $f(x) = y$.

Therefore f is onto. □

Proving that a function is one-to-one

Let $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$.

Is f one-to-one? Yes.

We need to show: $\forall x_1, x_2 \in X,\ f(x_1) = f(x_2) \ \to\ x_1 = x_2$.
Proof: Suppose $n, m \in \mathbb{N}$ such that $f(n) = f(m)$.

Then $n^2 = m^2$.

This implies $n = m$ or $n = -m$.

But $-m \notin \mathbb{N}$ unless $m = 0$. So we make two cases:

Case 1: If $m \neq 0$, then $-m \notin \mathbb{N}$ and so $n = m$.

Case 2: If $m = 0$, then $n = 0$, and so $n = m$.

Since in either case $n = m$, it follows that f is one-to-one.

==========

- Finite sets Suppose X and Y are finite sets
  - If $|X| > |Y|$, then there is no injective function $X \to Y$.
  - If $|X| < |Y|$, then there is no surjective function $X \to Y$.
  - There is bijective funtion $X \to Y$ if and only if $|X| = |Y|$

  Put differently:
  - If $f : X \to Y$ is injective , then $|X| \leq |Y|$.
  - If $f : X \to Y$ is surjective ,then $|X| \geq |Y|$.
  - If $f : X \to Y$ is bijective ,then $|X| = |Y|$.

  For finite sets with $|X| = |Y|$, the following statements are equivalent:
  - $f : X \to Y$ is injective
  - $f : X \to Y$ is bijective
  - $f : X \to Y$ is surjective
- Composition of functions If $f : X \to Y$ and $g : Y \to Z$, then the composition :
  $g \circ f : X \to Y$ is defined by:
  $(g \circ f)(x) = g(f(x)), \forall x \in X$
- Types of sequences Sequences can be finite:
  $5, 5, 20, 5, 5, 60$ can be written as $(a_n)_{n=1}^{6}$, where $a_1 = 5, a_2 = 5.....a_6 = 60$
  or infinite:
  $0, 1, 3, 6, 10, 15, 21.....$ can be written as $(g_n)_{n\geq 0}$ where $g_0 = 0, g_1 = 1.....$

  The index (the subscript) does not need to start at 0, and does not need to be called n:
  $1, 5, 15, 35, 70.....$ can be written as $(f_i)_{i\geq 4}$,where $f_4 = 1, f_5 = 5, f_6 = 15$ and so on
  An alternating sequence alternates between positive and negative:
  $((-\frac{1}{2})^n)_{n\geq 0} = 1, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{8}, ...$
- Define a sequence recursively
  - Initial conditions, which directly specify one or more terms that begin the sequence:
    $F_0 = 0, F_1 = 1$
  - A recurrence relation, which defines every other term using earlier terms:
    $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

==========

==========

- Notation for sums: For a sequence (a_i), we can add some or all of its terms:

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

  Dummy variables The i in $\sum_{i=m}^{n}$ is a dummy variable, like the x in $\forall x$

  - You can use any letter here (as long as it is not already taken):
  - The dummy variable is only relevant inside the sum, which means you can reuse it outside the sum:
    $\sum_{i=1}^{3} i + \sum_{i=1}^{4} i^2 = 1 + 2 + 3 + 1 + 4 + 9 + 16$
  - You can also perform a change of variable. If k = i + 1, then:
    $3! + 4! + 5! = \sum_{i=3}^{5} i! = \sum_{k=4}^{6} (k-1)!$

- Arithmetic with finite sums
  - Adding / subtracting 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:
    $\sum_{i=p}^{q} a_i + \sum_{i=q+1}^{r} a_i = \sum_{i=p}^{r} a_i$, if $p \leq q \leq r$
  - Index shift:
    $\sum_{i=m}^{n} a_i = \sum_{i=m+p}^{n+p} a_{i-p}$
  - Telescoping sums:
    $\sum_{i=m}^{n} (a_i - a_{i+1}) = a_m - a_{n+1}$ if $m \leq n$

- Divisiblity
  If $n, d \in \mathbb{Z}$,then n is divisible by d if and only if there exists some $k \in \mathbb{Z}$ such that $n = kd$
  We write $d \mid n$.We also say 'd divides n' or 'd is a divisor of n'.

- Lemma (Bounds for divisors)
  Let $n, d \in \mathbb{Z}$, If $|n| > 1$ and $d \mid n$, then $0 < |d| \leq |n|$.
  Proof of lemma: Suppose $n, d \in \mathbb{Z}$ with $|n| \geq 1$ and $d \mid n$.Then there is some $k \in \mathbb{Z}$ such that $n = kd$.

  The key steps in this proof were to:

  - prove $0 < |d|$ by contradition
  - prove $|d| \leq |n|$ in the special case where $n, d \in \mathbb{N}$
  - reduce the general case $n, d \in \mathbb{Z}$ to an instance of our special case.

==========

==========

- The Quotient-Remainder Theorem Given any integer n and positive integer d,
  there exist unique integers q and r such that:
  $n = q(quotient) * d(divisor) + r(remainder)$ and $0 \leq r < d$
  We call q the quotient, and r the remainder.

- Modular arithmetic:
  If n and m leave the same remainder after division by d, we say that they are congruent modulo d.
  We write: $n \equiv m(\text{mod d})$
  If $n \equiv m$ (mod d), then $m \equiv n$ (mod d). So the relationship is symmetric.

  If $a \equiv b(\text{mod d})$ and $n \equiv m(\text{mod d})$,then

  - $an \equiv bm(\text{mod d})$
  - $a + n \equiv b + m(\text{mod d})$
  - $a - n \equiv b - m(\text{mod d})$

==========

==========

5 W5

- **Prime factorisation** :
  The natural number $n \in \mathbb{N}$ is said to be writthen as a product of primes if there is a natural number $m \in \mathbb{N}$ and prime numbers $p_1, ..., p_m$ such that:
  $n = p_1 * p_2 * ... * p_n = \Pi_{k=1}^{m} p_k$
  every natural number $n > 1$ can be written as a product of primes.

- The fundamental Theorem of Arithmetic
  Given any integer $n > 1$,there exists a natural number k ,pairwise distinct prime numbers $p_1, p_2, ..., p_k$, and natural numbers $e_1, e_2, ..., e_k$ such that:
  $n = p_1^{e_1} * p_2^{e_2} * ..... * p_k^{e_k} = \Pi_{i=1}^{k} p_i^{e_i}$
  and any other expression for n as a product of prime numbers is identical to this except possibly for the order in which the factors are written.

- greatest common divisor of two integers a and b(not both zero)is the largest $d \in \mathbb{N}$ for which $d|a$ and $d|b$

- least common mutiple of two positive integers a and b is the smallest $n \in \mathbb{N}, n > 0$,for which $a|n$ and $b|n$ (we exclude zero here because this is always a solution).

- compute gcd without prime factorisation:
  $\forall a, b \in \mathbb{Z}, gcd(a, b) = gcd(b, a - b)$. Why?

  - if $d|a$ and $d|b$, then $d|a - b$
  - if d b and $d|a - b$,then $d|b + (a - b) = a$

  So: the common divisors of a and b are the same as the common divisors of b and a-b.
  In particular, the greatest common divisor of a and b is the same as the greatest common divisor of b and a - b.
  Speed way:$\forall a, b \in \mathbb{Z}$, if $a = bq + r$,then gcd(a,b) = gcd(b,r)

==========

==========

- **The Euclidean algorithm**
  To find gcd(a,b) where $a, b \in \mathbb{Z}$ and $a \geq b > 0$
  - Write $a = qb + r$ as in the quotient-remainder theorem
  - if r=0, then terminate with gcd(a,b) = b
  - otherwise, replace (a,b) by (b,r) and repeat

  Notice that the gcd is the last none-zero remainder.

  We've only discussed $a, b \geq 0$.What about arbitrary $a, b \in \mathbb{Z}$?
  - If one or both of a,b are negative, then just ignore the negative signs: $gcd(a, b) = gcd(|a|, |b|)$
  - if a=0 and b=0, then gcd(a,b) is not defined
  - if $a \neq 0$ and b=0 , then gcd(a,b) = $|a|$.
  - if a = 0 and $b \neq 0$, then gcd(a,b) = $|b|$.

- Representation of integers(Base b expansion):
  Let b be an integer greater than 1.Every positive integer n can be expressed uniquely in the form:
  $n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$
  where k is a none-negative integer, $a_0, ..., a_k$ are none-negative integers less than b and $a_k \neq 0$

- O-notation:
  O-notation is a mathematical notation that describes how quickly a function f grows compared to some function g when both their arguments tend towards infinity.
  For a given g it assigns a (large) set of functions which all grow at roughly the same rate, or slower. The comparison is done by checking whether f is an element of this set.
  Definition:

  Let f and g be functions from a subset $A \in \mathbb{R}$ to $\mathbb{R}$. Then f (x) is in O(g(x)) if there exist constants C and k such that for all $x \in \mathbb{A}, x \geq k$:

  $$|f(x)| \leq C|g(x)|$$

  For this to make sense f must have the following properties
  - $f, g : A \subset \mathbb{R} \to \mathbb{R}$
  - A is unbounded(for all $k \in A$ there exist infinitely many $x \in \mathbb{A}$such that $x \geq k$)

==========

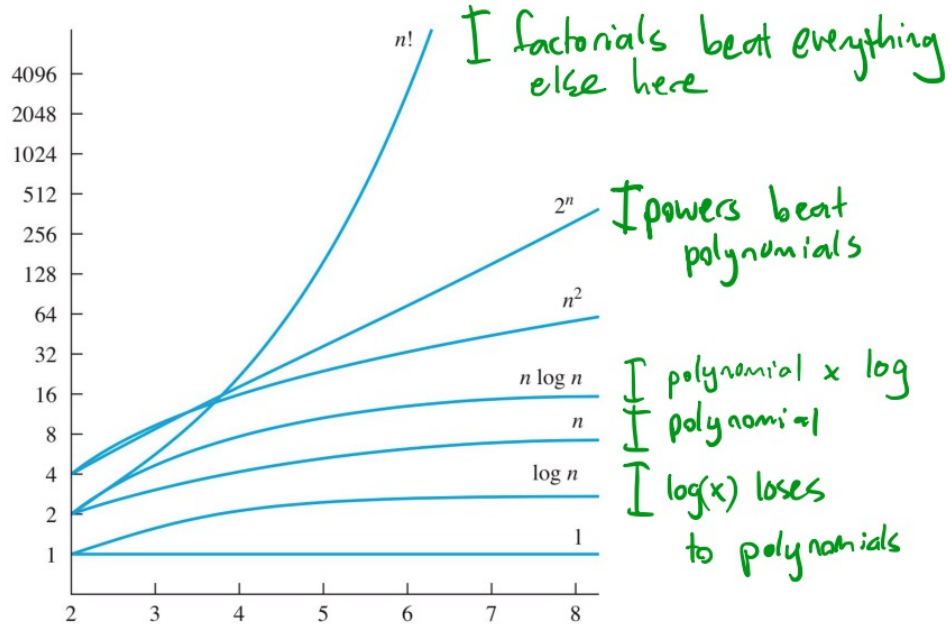
==========

Operations

- $f(n) \in O(f(n))$
- $O(c \cdot f(n)) = O(f(n))$ if c is a constant
- $O(f(n) + f(n)) = P(f(n))$
- $O(f(n)g(n)) = f(n) \cdot O(g(n))$

Note: Here, we use '=' to mean set equality

Important examples



==========

==========

- Lower bound and exact order

  Definition $[\Omega - notation]$:Let f and g be functions from a subset $A \in \mathbb{R}to\mathbb{R}$.Then f(x) is in $\Omega(g(x))$ if there are positive constants C and k such that for all $x \geq k$:

  $$|f(x)| \geq C|g(x)|$$

  Definition $[\Theta - notation]$:let f and g be functions from asubset $A \in \mathbb{R}to\mathbb{R}$. Then f(x) is in $\Theta(g(x))$ if $f(x) \in O(g(x))$ and $f(x) \in \Theta(g(x))$.
  f(x) is $\Theta(g(x))$ means that f(x) and g(x) are of the same order(within a constant of each other).

==========

==========

6 W6

- **Number of operations: Best-case, worst-case, average-case**

  Search integers $a_1, \ldots, a_n$ for presence of integer called key.

```
procedure LinearSearch(key, n: integer; a1, a2, a3, ..., an: integers)
begin
  i := 1                              {initializes the counter}
  while (i ≤ n and key ≠ ai) do
    i := i + 1
  if i ≤ n then location := i         {successful search}
  else location := 0                  {unsuccessful search}
end {location is the subscript of the first array entry that equals key;
     location is 0 if key is not found}
```

  - Best-case scenario: $key = a_1$, complexity of algorithm is O(1) , O(n) (in fact, $\Theta(nx)$).
  - Worst-case scenario: $key = a_n$, complexity of algorithm is O(n)
  - Average scenario : Assume key is in the list and equal to a_k with probability p = 1/n
    $f(n) = 1 * p + 2 * p + 3 * p + ... + n * p = (n + 1)/2$

- **Number of operations: Euclidean algorithm**

```python
def Euclidean(a,b):

    if b == 0:
        return a
    else:
        return Euclidean(b, a % b)

```

INPUT: 2 none negative integers
OUTPUT: gcd(a,b)

A call of Euclidean has

- 2 operations if b = 0 (check b , return a)
- 3 operations if b > 0 (check b,a mod b,return function output)

==========

==========

How many steps are necessary until b = 0?
Idea: look at first argument every second step

- $r_i = k \cdot r_{i+1} + r_{i+2}$
- $k \geq 1$
- $r_i = k \cdot r_{i+1} + r_{i+2} \geq r_i = r_{i+1} + r_{i+2} > 2r_{i+2}$
- $r_{i+2} < r_i/2$

After at most 2log2(a) calls of Euclid, the arguments must be gcd(a, b) and 0.

Running time: $3(2log2(a)) - 1 \in O(log(a))$.

- **Mathmatical induction**
  Let P(n) be a predicate that is defined for all integers $n \geq a, a \in \mathbb{N}$, Suppose:
  - P(a) is true
  - For all integers $n \geq a, P(n) \rightarrow P(n+1)$

  Then P(n) is true for all integers $n \geq a$(We just assume P(n),we never directly proof P(n) is true)

- **How to use mathematical induction**
  - Prove P(a) (This is called basic step)
  - Prove that for all integers $n \geq a, P(n) \rightarrow P(n+1)$
    (i) Assume P(n) is true for some particular but arbitrary $n \geq a$;
    (ii) using this, show that P(n + 1) is also true.
    This is called the inductive step. The assumption that P(n) is true is called the inductive hypothesis.

==========

==========

7 W7

- Case1 : **Order matters, repetition allowed**
  If a decision process can be broken down into a finite number of independent steps, and there are ni possible outcomes for the ith step, then the entire process can be carried out in Πni possible ways.
  In particular: for finite sets $S_1, S_2, ...S_k$,

$$|S_1 * S_2 * ... * S_k| = \Pi_{i=1}^{k} |S_i|$$

- Case2 : **Order matters, repetition not allowed**
  If you choose k elements from a set S with n elements, and order matters and repetition is not allowed, then there are:

  n possiblities for the first choice, then n - 1 for the second, then n - 2 for the third, ... then n - k + 1 for the kth.

  So the total number of choices is :

$$n \cdot (n-1) \cdot (n-2)...(n-k+1) = \frac{n!}{(n-k)!}$$

- Case3: **Order does not matter, repetition not allowed**

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

- Case4 : **Order does not matter, repetition allowed**
  Choosing k items from a set of n items such that order does not matter and repetition is allowed is the same as counting all possible arrangements of k crosses and n 1 bars, and this number is

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

==========

==========

8 W8

- **The inclusion-exclusion principle**

$$\begin{aligned}|A_1 \cup A_2 \cup \ldots \cup A_n| = &\sum_{i=1}^{n} |A_i| \\ &- \sum_{1 \le i < j \le n} |A_i \cap A_j| \\ &+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \\ &\vdots \\ &+ (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n| ,\end{aligned}$$

  where $A_1, A_2, \ldots, A_n$ are the sets in question. The principle alternates between addition and subtraction to account for overcounting in the intersections of the sets.

  Example:I have 10 students, and I wish to give back their marked quizzes. If I give the quizzes to students at random (without asking for student numbers, but ensuring that everybody receives a quiz), what is the probability that nobody receives their own quiz?

  - Step1 Total permutations : 10!
  - Step2 Permutations of at least 1 student gets right quiz:
    Assume A_i is the set of all permutations that i student(s) get right quizes Where at least one student gets the right exam :
    $|A_1 \cup A_2 \cup .... \cup A_{10}|$
  - Probability: $\frac{10! - |A_1 \cup A_2 \cup .... \cup A_{10}|}{10!}$(using inclusion-exclusion principle to calculate)

- **The 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.

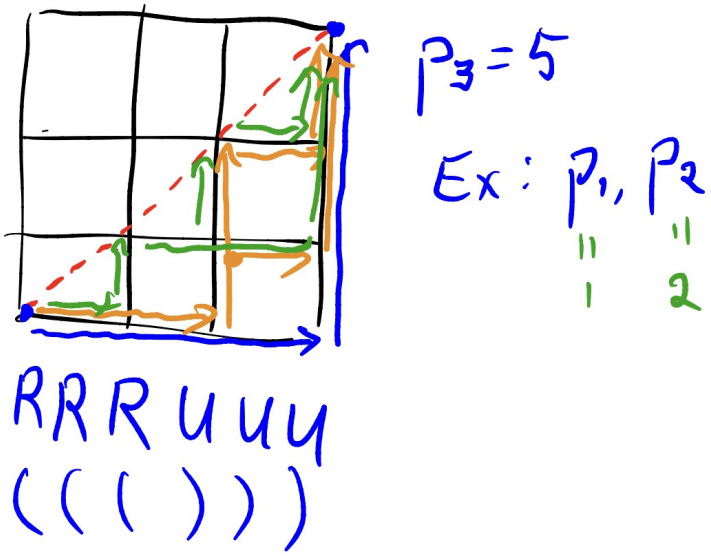
  Example:
  Suppose we have n = 101 pigeons to fit into k = 20 holes. Then, using the generalised pigeonhole principle with m = 5, we can conclude that some hole contains ≥ 6 pigeons.

==========

==========

- **Balanced String**
  String means a sequence of brackets where order matters
  Balanced means that in each initial substring, there are no more ")" than there are "("
  Examples: Let bn be the number of balanced strings on n left-brackets and n right-brackets.
  - $b_0 = 1$
  - $b_1 = 1$ ()
  - $b_2 = 1$ ()(),(())
  - $b_3 = 5$((())),(()()),(())(),()(()),()()()

- **Monotonic lattice paths**
  Let's count special paths on an n x n grid going from the bottom left corner to the top right corner. Namely, paths that only step right or up, and stay below the diagonal.Let p_n be the number of such paths.



  Each monotonic lattice path is a sequence of n R's and n U's such that in each initial subsequence there are no more U's than R's (since otherwise the path would cross the diagonal). We therefore have a well-defined map from monotonic lattice paths to balanced strings defined by
  $R \to$ (and $L \to$)
  This map is bijective, with inverse defined by
  $($ → R and) → U

==========

==========

- **Catalan Number**
  - Recurrence Relation: $C_0 = 1, \quad C_{n+1} = \sum_{i=0}^{n} C_i \cdot C_{n-i}$ for $n \geq 0$
  - Direct Formula: $C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!}$

- **Recurrences revisited**
  Consider a linear homogeneous recurrence relation of order 2:

$$a_n = \alpha a_{n-1} + \beta a_{n-2}$$

method

  - Step1 Factor $x_2 - \alpha x - \beta = (x - \alpha_1)(x - \beta_1)$
  - Step2($\lambda_1 \neq \lambda_2$) then $a_n = A\lambda_1^n + B\lambda_2^n$
  - Step2($\lambda_1 = \lambda_2$) then $a_n = C\lambda^n + Dn\lambda^n$

Solutions in (2a) and (2b) are the general solution of the rec. relation. Initial conditions (values of a_0 and a_1) determine constants A, B or C, D.

Eample
Let $f : \mathbb{N} \to \mathbb{Z}$ be a function defined recursively by f(0) =-1, f(1) =5 and for all $n \geq 2$ by

$$f(n) = 10f(n-1) - 25f(n-2)$$

  - Step1 Factor $x_2 - 10x + 25 = 0$
  - Step2($\lambda_1 = \lambda_2 = 5$) then $f_n = A5^n + B5^n$
  - Step3 $f(0) = A + 0 = -1, f(1) = -5^1 + B5^1 = 5 \to B = 2$

linear non-homogeneous recurrence relation of order 2:

$$a_n = \alpha a_{n-1} + \lambda a_{n-2} + F(n)$$

method

  - Step1 Find a paticular solution $a_n^{(p)}$ by poking around
  - Step2 Determine the general solution $a_n^{(h)}$ to the homogeneous equation

$$a_n = \alpha a_{n-1} + \lambda a_{n-2}$$

    The general solution of the non-homogeneous recurrence relation is then given by a $a_n^{(p)} + a_n^{(h)}$

When we are given initial conditions, i.e. values of a0 and a1, then these determine the constants A, B or C, D.

==========

==========

Example

$$a_n = 10a_{n-1} - 25a_{n-2} + 3^n$$

From before, the homogeneous equation $a_n = 10a_{n-1} - 25a_{n-2}$ has the general solution $a_n^{(h)} = C \cdot 5^n + D \cdot n5^n$

- Try $a_n^{(p)} = E3^n$
- $E3^n = 10E3^{n-1} - 25E3^{n-2} + 3^n$
- $E = \frac{9}{4}$

solution $a_h = a_n^{(h)} + a_n^{(n)} = C \cdot 5^n + Dn5^n + \frac{9}{4}3^n$

==========

9 W9

- Setup
  - Sample Space S (also called probability space). Here: $|S| < \infty$
  - $x \in S$ is called an outcome,or an elementary event
  - $E \subseteq S$ is called an event
  - Set of events $\mathbb{E}$ is a subset of the power set of S, so $\mathbb{E} \subseteq P(S)$
  - For $x \in S$.{x} is called an elementary event
- Random A random variable is a function $X : S \to R$ defined on the outcomes of a sample space.
  Example:
  S outcomes of the roll of two fair dice, so $|S| = 36$. $X : S \to R$, X(s) = "sum of the values of the two dice in outcome $s \in S$" Then X(S) = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}.
- Distribution of random variable

  $$\text{Set of all pairs (r, p(X = r))}$$

  X refers to random variable which is a function that assigns a real number to each outcome in a sample space.
- **Conditional probability** Let E and F be events with $p(F) > 0$. The conditional probability of E given F is

  $$p(E|F) = \frac{p(E \cup F)}{p(F)}$$

  Example
  In your local juggling club, 1/3 of all members are computer scientists. Exactly 1/4 of all members pass clubs, 2/5 of these are computer scientists.
  i) What is the percentage of computer scientists who pass clubs amongst all members?
  $p(E \cap F)$
  ii) What is the percentage of computer scientists who pass clubs amongst the computer scientists?
  $p(F|E)$
- **Independent**: If any of the following hold, E and F are called independent.(The following are equivalent)
  - $p(E|F) = p(E)$
  - $p(E \cap F) = p(E)p(F)$

Bayes' theorem

We had:

$$p(E) = p(E \mid F) \cdot p(F) + p(E \mid \overline{F}) \cdot p(\overline{F})$$

$$p(F \mid E) = \frac{p(F)}{p(E)} \cdot p(E \mid F)$$

Hence:

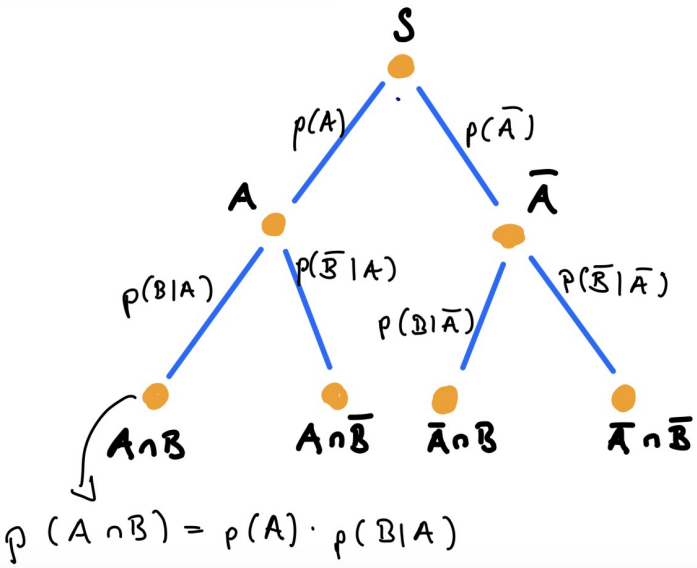
Bayes' theorem

Suppose E and F are events from a sample space S with $p(E) > 0$ and $p(F) > 0$. Then:

$$p(F \mid E) = \frac{p(F)}{p(E \mid F) \cdot p(F) + p(E \mid \overline{F}) \cdot p(\overline{F})} \cdot p(E \mid F)$$

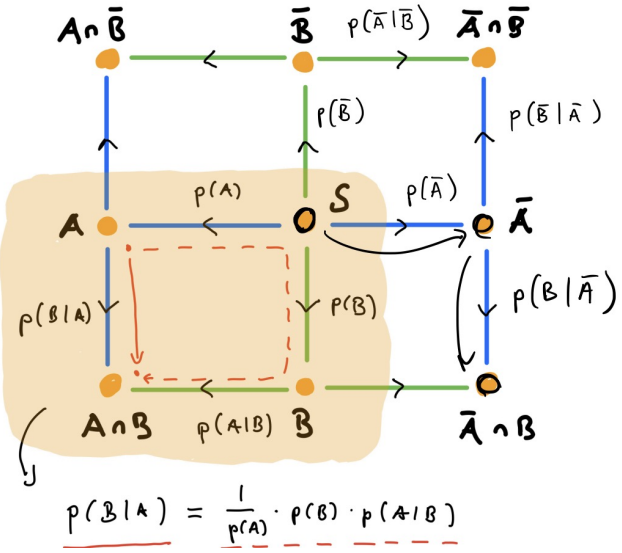
Independence and conditional probability

Decision tree for a pair of arbitrary events A and B



Independence and conditional probability

Bayes' theorem



==========

10 W10

- Relation
  - Let X and Y be sets. A relation R from X to Y is a subset of $X \times Y$
  - We write $(x, y) \in R$ also as xRy and say that x is related to y.
  - The complementary relation to R is $\overline{R} = (X \times Y) \backslash R$
  - If $X = Y$ we say that R is a relation on X.
- Properties
  Let R be a relation on the non-empty set X. Then:
  - Reflexive : $\forall x \in X, (x, x) \in \mathbb{R}$
  - Symmetric : $(x, y) \in \mathbb{R} \rightarrow (y, x) \in \mathbb{R}$
  - Transitive : $(x, y) \in \mathbb{R} \wedge (y, z) \in \mathbb{R} \rightarrow (x, z) \in \mathbb{R}$
- Combining Relations The relations R_1 and R_2 from X to Y are a subsets of $X \times Y$ We can use operations on subsets to create new relations:
  - $R_1 \cup R_2$
  - $R_1 \cap R_2$
  - $R_1 \backslash R_2$

  We can compose relations R from X to Y and S from Y to Z to get a new relation $S \circ R$ from X to Z by defining:

$$S \circ R = \{(a, c) | \exists b \in Y : aRb \wedge bSc \subseteq X \times Y\}$$

- Equivalence relation If the relation R on the non-empty set X is **reflexive, symmetric and transitive**, then R is an equivalence relation on X.
- 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.

==========

Example
$(m, n) \in R$ if and only if $3|(m-n)$ these are 3 equivalence classes

- $\{..., -6, -3, 0, 3, 6, ...\}$
- $\{..., -5, -2, 1, 4, 7, ...\}$
- $\{..., -4, -1, 2, 5, 8, ...\}$

We can (if we like) call these [0], [1] and [2].

If R is an equivalence relation on the non-empty set X, then:

$$[x] \neq \emptyset \quad \text{for all} \quad x \in X$$

$$X = \bigcup_{x \in X} [x]$$

$$[x] \cap [y] = \begin{cases} \emptyset & \text{if } (x, y) \notin R \\ [x] = [y] & \text{if } (x, y) \in R \end{cases}$$

A partition

==========

- Partition
  A set $\{S1, S2, ...\}$ is a partition of S if:
  - $S_i \neq \emptyset$
  - $S = S_1 \cup S_2 \cup .....S_i$ The sets cover S
  - $S_i \cap S_j = \emptyset$ whenever $i \neq j$ The sets are disjoint

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

  Suppose $\{X_1, X_2, ...\}$ is a partition of X. Then the relation R defined by

  $$xRy \leftrightarrow \exists i \text{ such that } x \in X_i \text{ and } y \in X_i$$

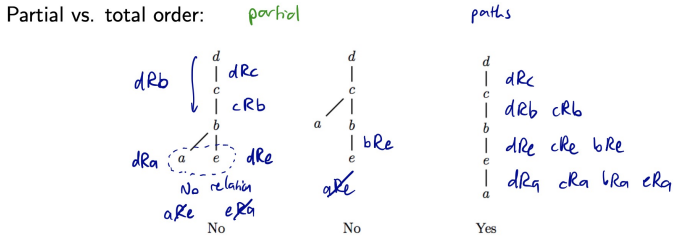
  is an equivalence relation.
  In other words : **If two elements belong to the same subset, then they are related.**

- Anti-symmetric
  The relation R is anti-symmetric if and only if :

  $$\forall a, b \in X, (a, b) \in R \text{ and } (b, a) \in R \text{ implies } a = b$$

  - can not have both (1,3) and (3,1)
  - may not have either
  - anti-symmetric $\neq$ not symmetric
    Example: symmetric and anti-symmetric $\{(1, 1), (2, 2), (3, 3)\}$

- Partial and total orders
  A relation R on a set X which is reflexive, transitive, and anti-symmetric is called a partial order on X. If in addition, $\forall a, b \in X$,aRb or bRa, then R is called a total order on X.

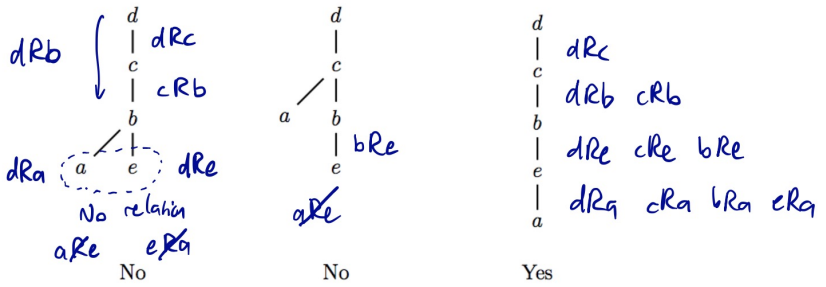


==========

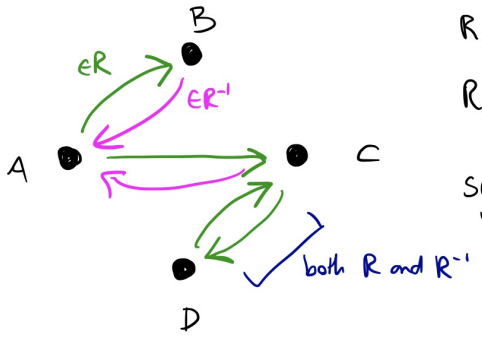
==========

- Reflexive closure
  $ref(R) = R \cup \{(x, x)|x \in X\} = R \cup \Delta$
  For a digraph representation: add a loop at each vertex

Partial vs. total order: partial paths



- Symmetric closure
  $R \cup \{(y, x)|(x, y) \in R\} = R \cup R^{-1}$
  For a digraph representation: Add edges in the opposite direction



$R = \{(A,B), (A,C), (C,D), (D,C)\}$

$R^{-1} = \{(B,A), (C,A), (D,C), (C,D)\}$

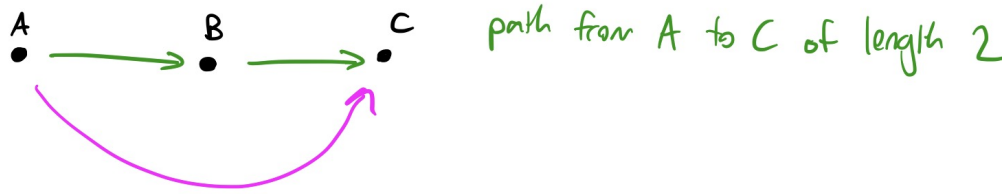
$sym(R) = \{(A,B), (A,C), (C,D), (D,C), (B,A), (C,A)\}$

$sym(R) = R \cup R^{-1}$

==========

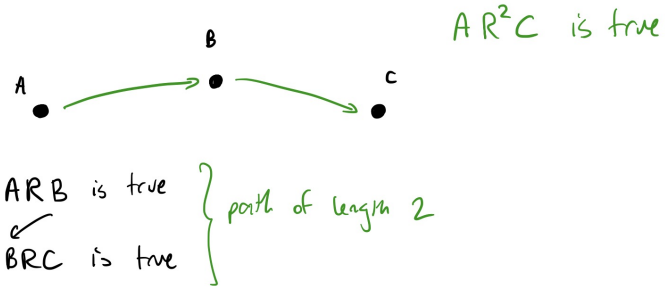
==========

- Transitive closure
  For a digraph representation: If there is a path from x to y, add an edge from x to y.



There is a path of length k from x to y in R if there are $x = x_0, ..., x_k = y$ such that $xRx_1, x_0Rx_1, ..., x_{k1}Ry$.

There is a path of length k from x to y if and only if xR^ky.



connectivity closure:

$$R^* = \bigcup_{k=1}^{\infty}$$
or
$$R \cup R^2 \cup R^3 \cup R^4 .....$$

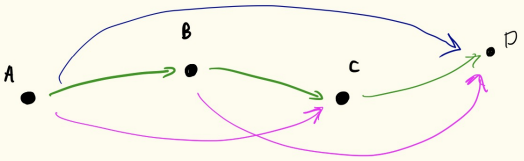
Short summary

- The connectivity closure R^* is the transitive closure tra(R).
- If X has only n elements, then $R^* = \bigcup_{k=1}^{n} R^k$

==========

==========

Example



$R = \{(A,B), (B,C), (C,D)\}$

$R^2 = \{(A,C), (B,D)\}$

$R^3 = \{(A,D)\}$

$tra(R) = R \cup R^2 \cup R^3$

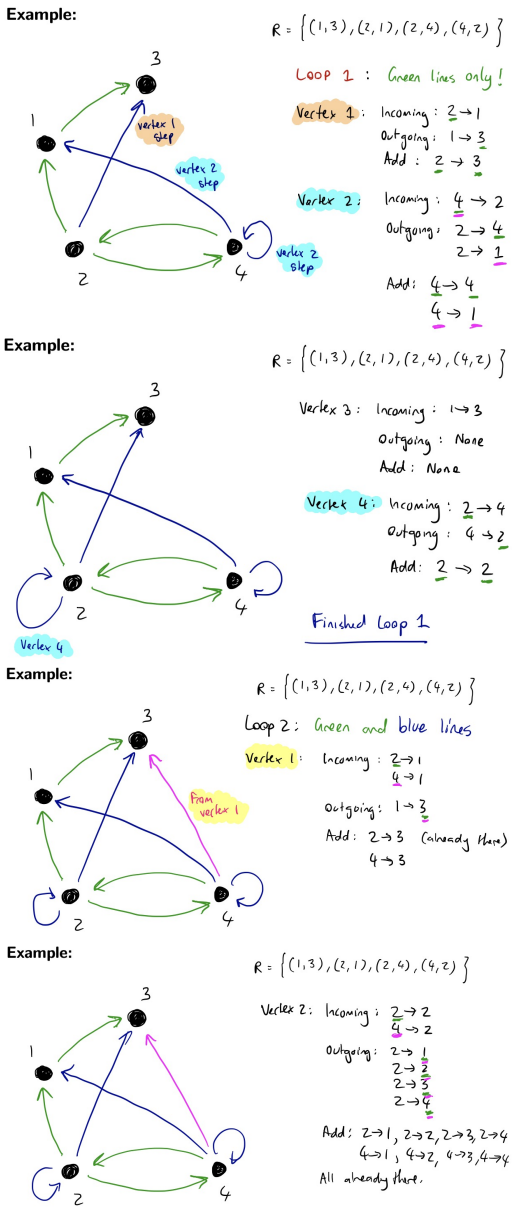
$= \{(A,B), (B,C), (C,D), (A,C), (B,D), (A,D)\}$

R R^2 R^3

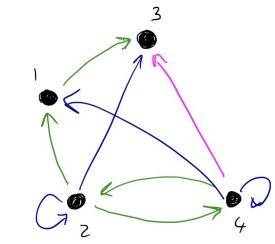
- Warshall's algorithm Main idea: A path exists between vertices x and y if and only if:
  - there is an edge from x to y; or
  - there is a path from x to y going through vertex 1; or
  - there is a path from x to y going through vertices 1 and/or 2; or
  - ...
  - there is a path from x to y going through any of the other n 2 vertices.

==========

Example


Example:
R = {(1,3),(2,1),(2,4),(4,2)}
Loop 1 : Green lines only!
Vertex 1: Incoming : 2→1
Outgoing : 1→3
Add : 2→3
Vertex 2: Incoming : 4→2
Outgoing : 2→4
2→1
Add: 4→4
4→1
vertex 1 step
vertex 2 step
vertex 2 step
Example:
R = {(1,3),(2,1),(2,4),(4,2)}
Vertex 3: Incoming : 1→3
Outgoing : None
Add : None
Vertex 4: Incoming : 2→4
Outgoing : 4→2
Add: 2→2
Finished Loop 1
Vertex 4
Example:
R = {(1,3),(2,1),(2,4),(4,2)}
Loop 2: Green and blue lines
Vertex 1: Incoming : 2→1
4→1
Outgoing : 1→3
Add: 2→3 (already there)
4→3
From vertex 1
Example:
R = {(1,3),(2,1),(2,4),(4,2)}
Vertex 2: Incoming : 2→2
4→2
Outgoing: 2→1
2→2
2→3
2→4
Add: 2→1, 2→2, 2→3, 2→4
4→1, 4→2, 4→3, 4→4
All already there.

Example:



$R = \{(1,3),(2,1),(2,4),(4,2)\}$

Vertex 3: Incoming: $1\to3$, $2\to3$
Outgoing: None

Vertex 4: Incoming: $2\to4$, $4\to4$
Outgoing: $4\to1$, $4\to2$, $4\to3$, $4\to4$

Add: $2\to1$, $2\to2$, $2\to3$, $2\to4$
$4\to1$, $4\to2$, $4\to3$, $4\to4$
All already present

END LOOP

Do one more loop: Nothing changes

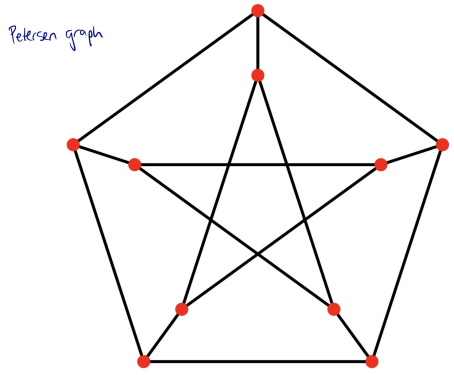
- Order of taking closures
  - ref(sym(R)) = sym(ref(R))
  - ref(tra(R)) = tra(ref(R))
  - tra(sym(R)) = sym(tra(R))

==========

==========

11 W11

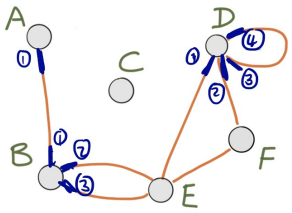
- Graph theory
  A graph G consist of 2 finite sets:
  - a non-empty set V(G) of vertices
  - a possibly empty set E(G) of edges, where associated with a set $\{v, w\} \subseteq V(G)$
    The vertices v and w are called the endpoints of the edge.
  - A graph G is defined purely in terms of sets V(G) and E(G). The drawing is just a visual aid.
  - An edge may have endpoints v, v
    We call such an edge a loop
  - 2 edges may have the same endpoints $\{v, w\}$. We call these parallel edges.
  - A graph with no loops or parallel edges is called a simple graph.
- Peterson Graph
  most famous counter example



==========

==========

- Terminologies
  - **Incident** : For an edge e and a vertex v , v is an endpoint of e
  - **adjacent** : For vertices u, v, there is an edge with endpoints $\{u, v\}$
    A vertex u is adjacent to itself if there is a loop with endpoints $\{u\}$.
  - **Degree** : the degree of vertex v is the number of edges incident with v , where we count each loop twice ,we write this as deg(v).



Informally, deg(v) counts the "ends of edges" that meet v.

deg(A) = 1 , deg(B) = 3 , deg(D) = 4 , deg(C) = 0 .

- **Handshake Theorem**
  Let G be a graph with n vertices $V(G) = \{v_1, v_2 ... v_n\}$,Then

$$\sum_{i=1}^{n} deg(v_1) = deg(v_1) + ... + deg(v_n) = 2 \cdot |E(G)|$$

  In particular, in any graph, the sum of all vertex degrees must be even.

- Directed graphs
  Let G be a digraph (directed graph), and $v \in V(G)$
  - The in-degree $def^{-}(v)$ is the number of edges terminating in v.
  - The out-degree $deg^{+}(v)$ is the number of edges starting in v.

  Let G be a directed graph with n vertices $V(G) = \{v_1, ..., v_n\}$ Then:

$$\sum_{i=1}^{n} deg^{-}(vi) = \sum_{i=1}^{n} deg^{-}(vi) = |E(G)|$$

- Path
  Let G be a graph and let $x, y \in V(G)$. A path in G from x to y is an alternating sequence of vertices and edges:

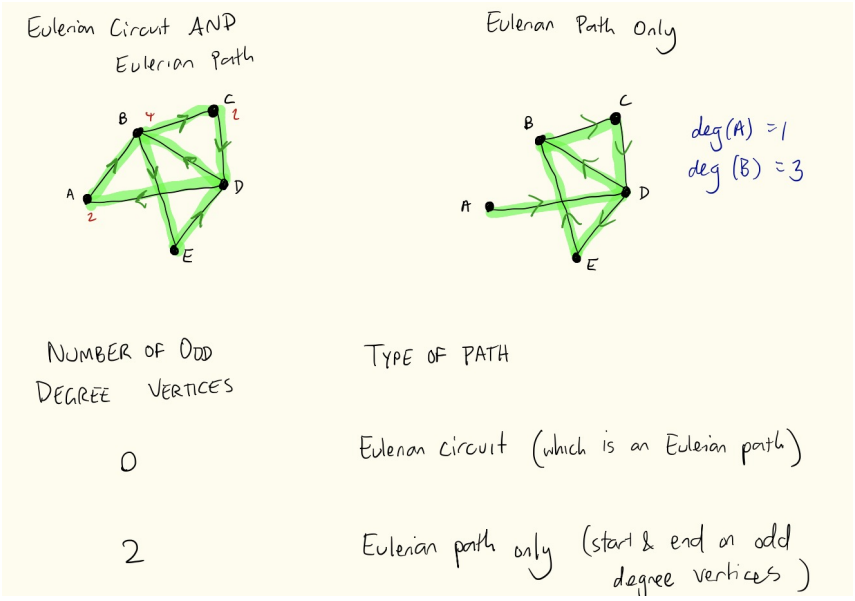
$$v_0(\text{starting vertex}), e_1, v_1, e_2, ..., v_{n-1}, e_n, v_n(\text{end vertex})$$

  where $v_0 = x, v_n = y$, and each edge e_i has endpoints $\{v_{i-1}, v_i\}$

==========

==========

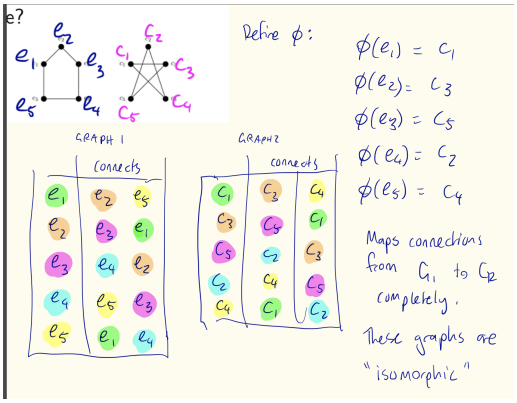
- More on path
  - Connected graph and Disconnected : for a graph G, $\forall$ vertices $x, y \in V(G)$, there is a path from x to y. Otherwise G is called disconnected.
- Circuit
  A path is called a circuit if it does not repeat any edge, and it starts and ends at the same vertices.
- **Eulerian circuits**
  A Eulerian circuit is a path that starts and ends at the same vertex, and that uses every edge exactly once.
  - If we ignore isolated vertices(degree = 0), the the remaining graph must be connected.
  - Let G be a connected graph. Then G has a Eulerian circuit if and only if every vertex of G has even degree .
- **Eulerian trail**
  A Eulerian trail is a path using each edge exactly once, but whose start and end vertices can be different.



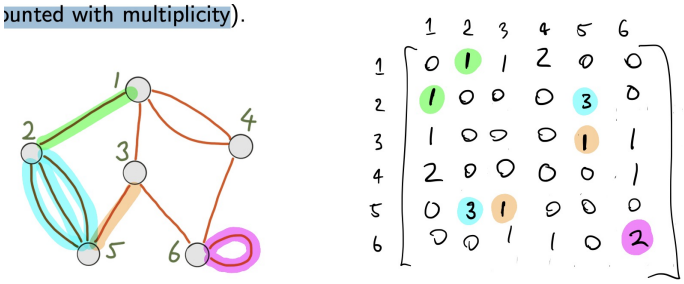
- Hamiltonian circuits
  circuit using every vertex exactly once. (Except for start = end vertex, which must appear twice.)

- Graph isomorphism
  Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are said to be isomorphic written $G_1 \cong G_2$, if there exists a bijective function $f : V_1 \to V_2$ such that:

$$f(E_1) = \{\{f(v_1), f(v_2)\} | \{v_1, v_2\} \in E_1\} = E_2$$



- **Representing graphs using Matrices**
  Let G a graph with n vertices, and suppose we label these vertices $V(G) = \{1, 2, ..., n\}$
  The adjacency matrix of G is the $n \cdot n$ matrix $\mathbb{A} = (a_{i,j})$, where each entry $a_{i,j}$ is the number of edges with endpoints $\{i, j\}$(counted with multiplicity)



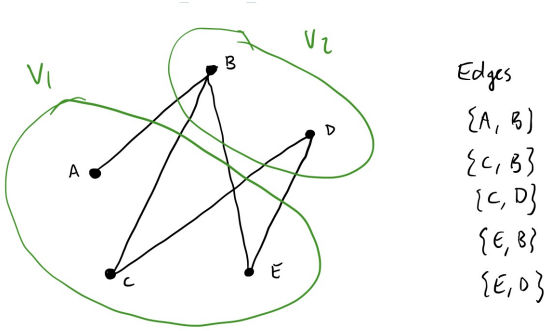
Theorem

Let G be a graph with vertices $V(G) = \{1, 2, ..., n\}$, and **adjacency matrix** $\mathbb{A}$.
Then the number of paths of length k from vertex i to vertex j is the entry in row i, column j of the kth power $A_k = A \cdot A \cdot ...A$.

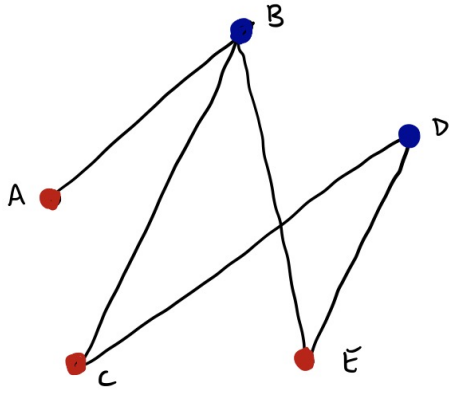
==========

12 W12

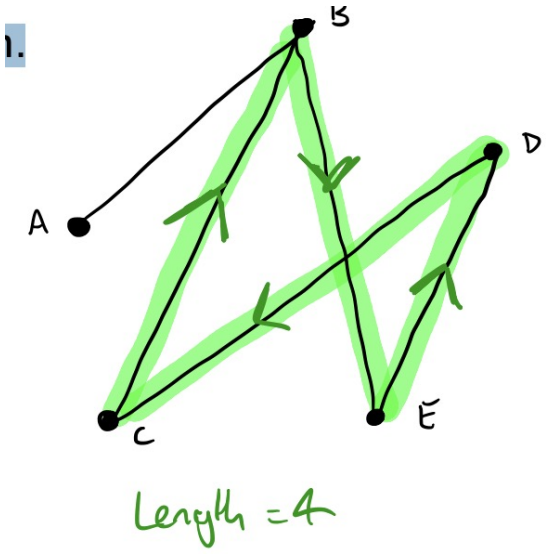
- **Bipartite graph**
  The simple graph G is bipartite if it has at least 2 vertices and satisfies one (and hence all) of the following equivalent conditions:
  - The set of vertices $V(G)$ has a partition $\{V_1, V_2\}$ such that every edge is of the form $\{v_1, v_2\}$ where $v_k \in V_k$



  - The vertices can be coloured with two colours such that no two adjacent vertices have the same colour



– Every circuit in G has even length.



==========

- **Finite state machine (with output)**
  A finite state machine (with output) M = (S, I, O, f , g,s0) consists of
  - a finite set S of states
  - a finite input alphabet I
  - a finite output alphabet O
  - transition function $f : S \times I \to S$
  - an output function $g : S \times I \to O$
  - an initial state s_0
- Representing finite state machines: State diagrams
  A more visual representation of a finite state machine $M = (S, I, O, f, g, s0)$, is via a digraph, with one vertex per state and one directed edge per transition, each decorated with input and output.
  Example
  - $S = \{s_0, s_1, s_2, s_3, s_4, s_5, s_6\}$
  - $I = \{5, 10, 25, O, R\}$
  - $O = \{n, 5, 10, 25, orangejuice, applejuice\}$
  - f
  - g
  - s_0
- Formal languages
  Let **A** be a finite set called the alphabet.
  A formal language **L** is set of strings with symbol in **A**.
  The empty string is denoted λ.
  Example
  - $A = \{0, 1\}, L = \{0^n 1^m | m, nin\mathbb{N}\}$
  - $A = \{0, 1\}, L = \{0^n 1^n | nin\mathbb{N}\}$
  - $A = \{a, b, c, d, ..., z\}$,L = all English words

==========

==========

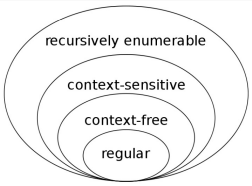
- **Phrase-structure grammar**
  A phrase-structure grammar $G = (V, T, S, P)$ consists of
  - a vocabulary (or alphabet) V
  - a subset $T \subseteq V$ of terminal symbols
  - a start symbol $S \in V$
  - a finite set of productions P
    The non-terminal symbols are N = V - T. Every production in P must have at least one non-terminal symbol on its left side.

  The language generated by G is the set L(G) of all words in terminals that can be derived from S using the productions P.
  The set of all sentences (or words) over V is V^*. So $L(G) \subseteq T^* \subseteq V^*$.

  Example
  G = (V,T, S, P) where
  V = 0, 1, S, A (vocabulary or alphabet),
  T = 0, 1 (terminal symbols),
  P = $S \to 0A, S \to 0S, A \to 1A, A \to 1$ (productions)
  So that
  V^* is the set of all words in V, e.g 01AAA1,SSA101, λ(empty string)
  T^* is the set of all words i T. e.g. 001,101,λ
  $L(G) \subseteq T^* \subseteq V^*$.

==========

- **Types of grammars: The Chomsky Hierarchy**



Type 0: no restrictions
Type 1: context-sensitive
$L = \{0^n1^n2^n \mid n > 0\}$ has a context-sensitive grammar
Type 2: context-free
$L = \{0^n1^n \mid n > 0\}$ has a context-free grammar
Type 3: regular
$L = \{0^n1^m \mid m, n > 0\}$ has a regular grammar

T	characterisation	Restrictions on productions
0		No restrictions
1	context-sensitive	(a) $lAr \to lwr$, $A \in N$ non-terminal, $l, r, w \in V^*$ arbitrary words over V, $w \neq \lambda$; (b) $S \to \lambda$, S not RHS of any prod. rule
2	context-free	$A \to w$, $A \in N$ non-terminal, $w \in V^*$ arbitrary
3	regular	$A \to aB$ or $A \to a$, $A, B \in N$ non-terminal, $a \in T$ terminal; or $S \to \lambda$.

13 W13

- *

Finite state machine (without output) – Finite state automaton

A finite state machine (without output) $M = (S, I, f, s_0, F)$ consists of

- a finite set S of states,
- a finite input alphabet I,
- a transition function $f\colon S \times I \to S$,
- an initial state s_0,
- a subset $F \subseteq S$ if final or accepting states.

- Extended transition function and Recognised language

Let $M = (S, I, f, s_0, F)$ be a finite state machine without output.

Extended transition function

Extend the transition function $f\colon S \times I \to S$ to

$$f\colon S \times I^* \to S$$

by defining $f(s, x)$ to be the state obtained by starting at s and reading x from left to right.

$x \in I^*$ is recognised (or accepted) by M if $f(s_0, x) \in F$.

Recognised language

The string $x \in I^*$ is recognised (or accepted) by M if $f(s_0, x) \in F$.
The language $L(M) = \{x \in I^* \mid f(s_0, x) \in F\}$ is the language recognised (or accepted) by M