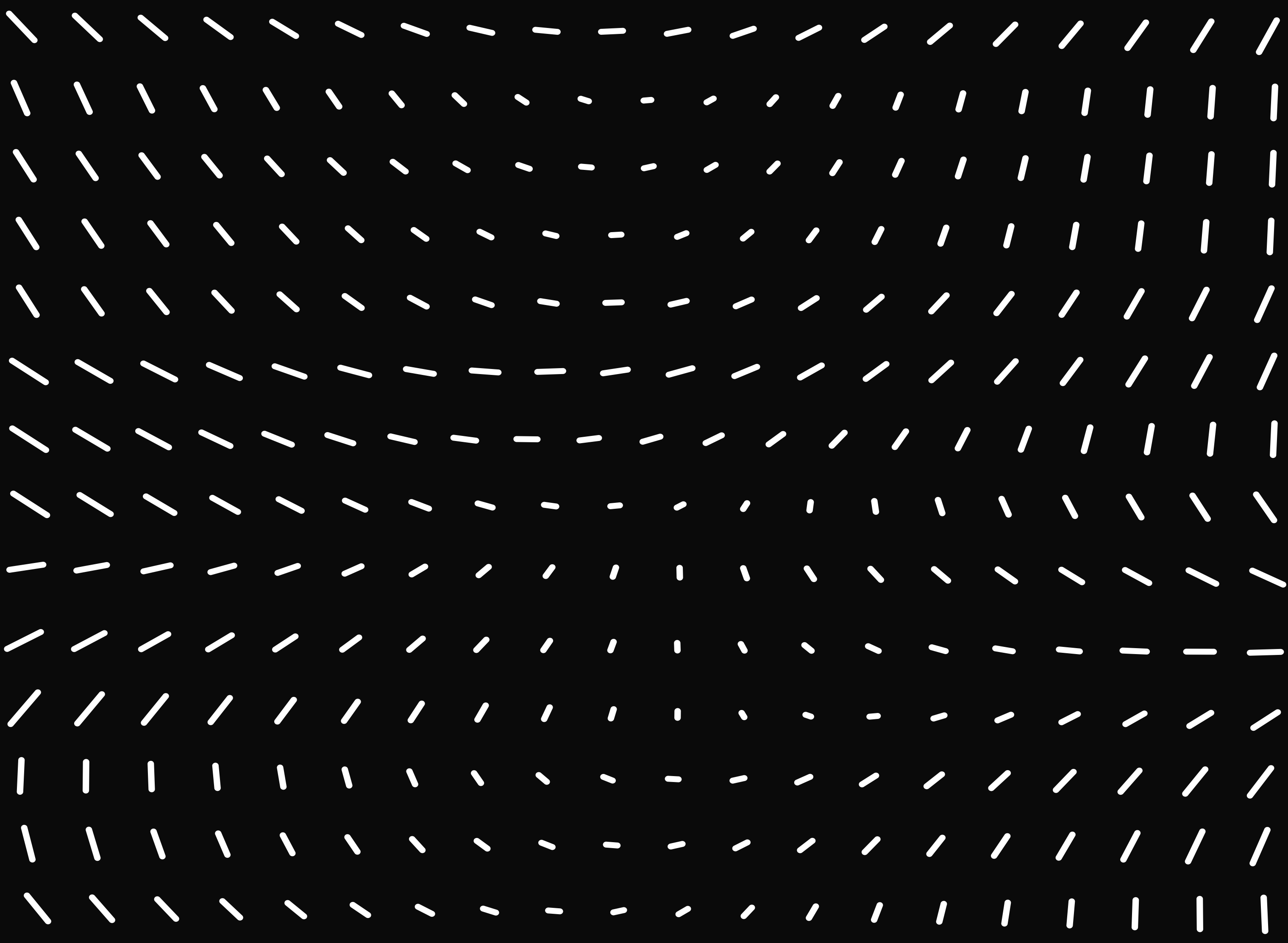


Euclidean Division

$n|m \rightarrow$ n divides m

$m = x_1(n)$

Modulo n

$a \equiv b \pmod{n} \Rightarrow a - b = x_1(n)$

Example: $\underbrace{\underbrace{\underbrace{-8 \equiv 2}_{-8-2=-10} \equiv 7}_{-8-7=-15} \equiv 12}_{-8-12=-20} \pmod 5$

$(a \bmod n) + (b \bmod n) = (a+b) \bmod n$

Example: $(17 \bmod 5) + (-8 \bmod 5) \equiv 4 \bmod 5$

$(2 \bmod 5) + (2 \bmod 5) \equiv 4 \bmod 5$

$(a \bmod n) \times (b \bmod n) = (ab) \bmod n$

Example: $(12 \bmod 5) \times (-3 \bmod 5) \equiv 4 \bmod 5$

$(-36 \bmod 5) \equiv 4 \bmod 5$

$4 \bmod 5 \equiv 4 \bmod 5$

Example: Is $1234567 = x^2$ (x is integer)

Table (mod 10)

x	x^2
0	0
1	1
2	4
3	9
4	6
5	5
6	6
7	9
8	4
9	1

NO 7, $x^2 \not\equiv 7 \bmod 10$

WTS: $1234567 \equiv 7 \bmod 10$

Can $x^2 \equiv 7 \bmod 10$?

Example: Is $9 | 4653$? let $4653 = N$

$N = 4 \times 10^3 + 6 \times 10^2 + 5 \times 10^1 + 3$

WTS: $N - S = 0 \pmod 9$

$N - S = 4(10^3 - 1) + 6(10^2 - 1) + 5(10 - 1) + 3(1-1)$

$= 4(1^3 - 1) + 6(1^2 - 1) + 5(1 - 1) \pmod 9$

$= 0 \bmod 9$

Example: Is $1234567 = x^2 + y^2$

$1234500 + 67 \equiv 67 \bmod 4$

$\equiv 3 \bmod 4$

x	x^2
0	0
1	1
2	0
3	1

$x^2 \backslash y^2$	0	1
0	0	1
1	1	2

Operator Closure

Sets [S] are number variants

Operator [Δ] is stuff like ×, ÷, +, −, +mod

Example:

$\mathbb{R}$ [Real no.] is closed under Δ = + & Δ = − $(2+3=5)$

$\mathbb{Z}$ [integer] is not closed under Δ = ÷ $(5 \div 2 = 2.5)$

Example:

Is set of even numbers closed when Δ = ÷	Is the set of odd integers closed when Δ = ×	Is the set of prime numbers closed when Δ = +
When $x = 6, y = 4$ $x \Delta y = 3/2$ is not even	odd integers, $x = 2(t) - 1$, $t \in \mathbb{Z}$ $y = 2(k) - 1$, $k \in \mathbb{Z}$ $(2(t) - 1) \Delta (2(k) - 1) = 4tk - 2k - 2t + 1$ $= 2\underbrace{(2tk - k - t)}_{\mathbb{Z}} + 1$	

Proposition & Paradox

Is this statement true/false

is a proposition	not a proposition
"1+2=3" is true	"1+2>x"
"1+2<2" is false	"What a great book"
"Singapore is in Asia"	"Is Singapore in Asia"

Paradoxes are not propositions

"This statement is false"

if T, becomes F

if F, becomes T

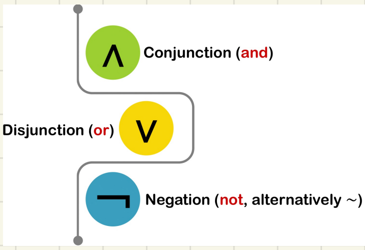
Symbolic Logic

P: "dogs are mammals"

$\hookrightarrow$ $P = T$ as dogs = mammals

if dogs $\neq$ mammals,

$P \neq T$



Negation (not)

p	$\neg p$
T	F
F	T

Disjunction (or)

p	q	$p \vee q$	$q \vee p$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

$q \vee p \equiv p \vee q$
equivalent,
$\vee$ commutes

Conjunction (and)

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

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

$\wedge$ is also commutative

De-morgan's Law

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\quad (p+q)' = p'q'$

$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\quad (pq)' = p'+q'$

Contradiction vs Tautology

always wrong

$P \vee (\neg p) \equiv F$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

always true

$P \wedge (\neg p) \equiv T$

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

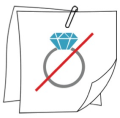
$\left.\begin{matrix} \\ \end{matrix}\right\}$ Always true!

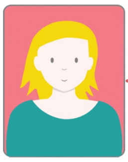
Equivalent Expressions

Equivalent Expressions: Bob and Alice

1. Alice is not married but Bob is not single.
   $\neg h \wedge \neg b$
2. Bob is not single and Alice is not married.
   $\neg b \wedge \neg h$
3. Neither Bob is single nor Alice is married.
   $\neg(b \vee h)$

Bob





Alice

These three statements are equivalent.

$\neg h \wedge \neg b \equiv \neg b \wedge \neg h \equiv \neg(b \vee h)$

b. Bob is single

$\neg b$: Bob is not single

h : Alice is married

$\neg h$: Alice is not married

Logical Equivalence laws

Axioms

$T \equiv$ Tautology
$C \equiv$ Contradiction

- $\neg T \equiv F$
- $\neg F \equiv T$
- $\neg T \equiv C \equiv F$
- $\neg C \equiv T \equiv T$

De Morgan

- $\neg(p \land q) \equiv \neg p \lor \neg q$
- $\neg(p \lor q) \equiv \neg p \land \neg q$

Commutativity

- $p \land q \equiv q \land p$
- $p \lor q \equiv q \lor p$

Double Negation

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

Idempotent

- $p \land p \equiv p$
- $p \lor p \equiv p$

Absorption

- $p \lor (p \land q) \equiv p$
- $p \land (p \lor q) \equiv p$

Distributivity

- $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$
- $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$

Conditional Operator

If p then q: $P \to q$

$p \to q$

implies

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

aka, $p \to q$ is F when
$p = T$ but $q = F$

Converse, Inverse & Contrapositive Theorem

$$\boxed{p \to q \equiv \neg p \lor q}$$

Proof

p q	$p \to q$	$\neg p$	$\neg p \lor q$
T T	T	F	T
T F	F	F	F
F T	T	T	T
F F	T	T	T

Statement	$p \to q$
Converse	$q \to p$
Inverse	$\neg p \to \neg q$
Contrapositive	$\neg q \to \neg p$

If statement T, contrapositive T

If converse T, inverse T

Only If operator

p only if q $\triangleq \neg q \to \neg p$

$\triangleq$ means "defined as"

- $\neg q \to \neg p$ is the contrapositive of $p \to q$
- (If not q then not p) $\equiv$ ($p \to q$) (why?)

Example

"Bob pays taxes only if his income $\geq \$1000$"
(b) (m)

$\triangleq$ "if Bob's income $< \$1000$ then he does not pay taxes"
($\neg m \to \neg b$)

$\equiv$ "if Bob pays tax then his income $\geq \$1000$"

b only if m $\triangleq \neg m \to \neg b \equiv b \to m$

"If you do not fix my ceiling, then I won't pay my rent."

$\neg f \to \neg p \equiv p \to f$

"I will pay my rent only if you fix my ceiling."

$\neg f \to \neg p \equiv p \to f$

means the same thing

Biconditional Operator

The biconditional of p and q: $p \leftrightarrow q \triangleq (p \to q) \land (q \to p)$

– True only when p and q have identical truth value

If and only if (iff)

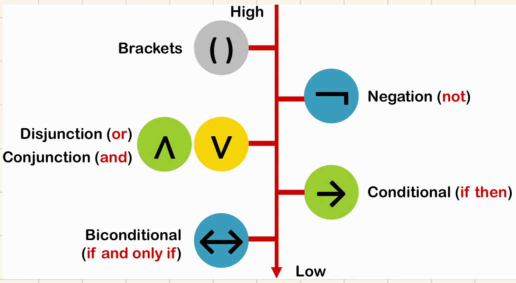
p q	$p \to q$	$q \to p$	$p \leftrightarrow q$
T T	T	T	T
T F	F	T	F
F T	T	F	F
F F	T	T	T

XNOR

Example. Show $p \lor q \to r \equiv (p \to r) \land (q \to r)$

LHS: $p \lor q \to r = (p \lor q) \to r$
$= \neg(p \lor q) \lor r$
$= (\neg p \land \neg q) \lor r$
$= (\neg p \lor r) \land (\neg q \lor r)$
$= (p \to r) \land (q \to r)$

Operator Precedence



Leftmost Precedence

When equal priority instances of binary connectives are not separated by (), the leftmost one has precedence.

E.g., $p \to q \to r \equiv (p \to q) \to r$

High → Low

Argument

A series of statements form a valid argument if and only if "the conjunction of premises implying the conclusion" is a tautology.

((Premise) ∧ (Premise)) → Conclusion

$p \to q;$
$p;$
$\therefore q$

Premises / Conclusion

By definition, a valid argument satisfies: "If the premises are true, then the conclusion is true".

To check if the above argument is valid, we need to check that $((p \to q) \wedge p) \to q$ is a tautology.

All statements True

$p \to q;$
$p;$
$\therefore q$

Premises / Conclusion

Critical rows are rows with all premises true.

If in all critical rows the conclusion is true, then the argument is valid (otherwise it is invalid).

p	q	$p \to q$	$(p \to q) \wedge p$	$((p \to q) \wedge p) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

No need to calculate

Counter Example

"If it is falling and it is directly above me then I'll run"
"It is falling"
"It is not directly above me"

Premises

"I will not run"

Conclusion

$S = (f \wedge a \to r);$
$f;$
$\neg a;$
$\therefore \neg r$

Premises / Conclusion

$S = (f \wedge a \to r);$
$f;$
$\neg a;$
$\therefore \neg r$

Premises / Conclusion

a r	f	$\neg a$	$f \wedge a$	S	$\neg r$
~~T T~~	~~T~~	~~F~~	~~T~~	~~T~~	~~F~~
~~T T~~	~~F~~	~~F~~	~~F~~	~~T~~	~~F~~
~~T F~~	~~T~~	~~F~~	~~T~~	~~F~~	~~T~~
~~T F~~	~~F~~	~~F~~	~~F~~	~~T~~	~~T~~
F T	T	T	F	T	F
~~F T~~	~~F~~	~~T~~	~~F~~	~~T~~	~~F~~
F F	T	T	F	T	T
~~F F~~	~~F~~	~~T~~	~~F~~	~~T~~	~~T~~

Counterexample

Critical rows

Fallacy !

Example ō Counter example

Arguments: Fallacy 1 (Converse Error)

p	q	p >
~~T~~	~~F~~	~~F~~
T	T	T
~~F~~	~~F~~	~~T~~
F	T	T

Example

- If it is Christmas then it is a holiday.
- It is a holiday. Therefore, it is Christmas!

$p \to q;$
$q;$
$\therefore p$

Arguments: Fallacy 2 (Inverse Error)

q	p	p→q	¬p	¬q
T	F	T	T	F
~~T~~	~~T~~	~~T~~	~~F~~	~~F~~
F	F	T	T	T
~~F~~	~~T~~	~~F~~	~~F~~	~~T~~

Example

- If it is raining then I will stay at home.
- It is not raining. Therefore, I will not stay at home

$p \to q;$
$\neg p;$
$\therefore \neg q$

① we can try set conclusion to false and move from there. If conclusion is F and premise are all T, it is a counterexmp

p	c	¬p	¬p → c
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

② If no counterexmp is found, look for a path. Need to use inference rules.

$p \to q;$
$p;$
$\therefore q$

Modus Ponens
(Method of Affirming)

$p \to q;$
$\neg q;$
$\therefore \neg p$

Modus Tollens
(Method of Denying)

Rule of Contradiction

$\neg p \to C;$
$\therefore p$

Alternative Rule of Contradiction

$\neg p \to F;$
$\therefore p$

Dillema : Solve thru case by case

$p \vee q;$
$p \to r;$
$q \to r;$
$\therefore r$

if $p \vee q$ is true

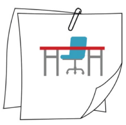
p true or q true

$p \to r$ is true | $q \to r$ is true

$\therefore$ r is true (modus ponens) | $\therefore$ r is true (modeus ponens)

Hypothetical Syllogism

$p \to q;$
$q \to r;$
$\therefore p \to r$



Example

- If I do not wake up, then I cannot go to work.
  p → q
- If I cannot go to work, then I will not get paid.
  q → r
- Therefore, if I do not wake up, then I will not get paid
  $\therefore$ p → r

Proof

nference Rules: Proof Hypothetical Syllogism

$(p \to q) \wedge (q \to r)$	(Hypotheses; Assumed True)
$\equiv (p \to q) \wedge (\neg q \vee r)$	(Conversion Theorem)
$\equiv [(p \to q) \wedge \neg q] \vee [(p \to q) \wedge r]$	(Distributive)
$\equiv [((p \to q) \wedge \neg q) \vee (p \to q)] \wedge [((p \to q) \wedge \neg q) \vee r]$	(Distributive)
$\equiv (p \to q) \wedge [((p \to q) \wedge \neg q) \vee r]$	(Recall absorption law: $a \vee (a \wedge b) \equiv a$, hence $[((p \to q) \wedge \neg q) \vee (p \to q)] \equiv p \to q$)
$\equiv (p \to q) \wedge [((\neg p \vee q) \wedge \neg q) \vee r]$	(Conversion)
$\equiv (p \to q) \wedge [((\neg p \wedge \neg q) \vee (q \wedge \neg q)) \vee r]$	(Distributive)
$\equiv (p \to q) \wedge [((\neg p \wedge \neg q) \vee F) \vee r]$	(Contradiction)
$\equiv (p \to q) \wedge [(\neg p \wedge \neg q) \vee r]$	(Unity)
$\equiv (p \to q) \wedge [(\neg p \vee r) \wedge (\neg q \vee r)]$	(Distributive)
$\equiv [(p \to q) \wedge (\neg q \vee r)] \wedge (\neg p \vee r)$	(Commutative; Associative)
$\therefore (\neg p \vee r) \equiv p \to r$	(Conjunctive Simplification; Conversion)

→ Chap 3

Predicatives

→ Something with an unknown, that becomes substantiated

Each predicate has a domain; $P(x)$, $x \in \mathbb{R}$ or $x \in \mathbb{Z}$

Let $P(x, y)$ = "$x > y$"

Domain: integers (i.e., both x and y are integers)

$P(4, 3)$	$P(1, 2)$	$P(3, 4)$
This means "$4 > 3$", so $P(4, 3)$ is TRUE.	This means "$1 > 2$", so $P(1, 2)$ is FALSE.	This means "$3 > 4$", so $P(3, 4)$ is FALSE.

In general, $P(x, y)$ and $P(y, x)$ are not equal.

$P(x)$ = "$x > 2$"
$P(1)$ is F
$P(2)$ is F
$P(3)$ is T
$P(10)$ is T

Quantifiers : Universal

any, for all : $\forall$

for all x in D

E.g., "$\forall x \in D$, $P(x)$ is true" iff "$P(x)$ is true for every x in D"

$\forall$	Universal quantifier, "for all", "for every"
$\in$	"Is a member (or) element of", "belonging to"
D	Domain of predicate variable

The square of any real number is non-negative.

$\forall x \in \mathbb{R}, x^2 \geq 0$

for all x in real numbers, $x^2 \geq 0$

Existential Quantifiers

There exists, for some : $\exists$

for some x in D

E.g., "$\exists\, x \in D$, $P(x)$ is true" iff "$P(x)$ is true for at least one x in D"

$\exists$	Existential quantifier, "there exists"
$\in$	"Is a member (or) element of", "belonging to"
D	Domain of predicate variable

Some birds are angry.

$\exists\, x \in$ {birds}, x is angry

for some value of x birds

- A proposition may contain multiple quantifiers:
  - "All rabbits are faster than all tortoises."
  - Domains: R = {rabbits}, T = {tortoises}
  - Predicate $C(x,y)$: Rabbit x is faster than tortoise y

In Symbols	$\forall x \in R$, ($\forall y \in T$, $C(x, y)$) or $\forall x \in R$, $\forall y \in T$, $C(x, y)$
In Words	For any rabbit x, and for any tortoise y, x is faster than y.

- "Every rabbit is faster than some tortoise."
- Domains: R = {rabbits}, T = {tortoises}
- Predicate $C(x,y)$: Rabbit x is faster than tortoise y

In Symbols	$\forall x \in R$, ($\exists y \in T$, $C(x, y)$) or $\forall x \in R$, $\exists y \in T$, $C(x, y)$
In Words	For any rabbit x, there exists a (some) tortoise y, such that x is faster than y.

$\neq$ Some tortoise are faster

Order of nesting

Is $\forall x \in D, \exists y \in D, P(x,y) \equiv \exists y \in D, \forall x \in D, P(x,y)$ in general?

LHS	RHS
$\forall x \in D, \exists y \in D, P(x,y)$	$\exists y \in D, \forall x \in D, P(x,y)$
y can vary with x	y is fixed, but x varies

Let $P(x,y)$ = "x admires y"

"Every person admires someone" | "Some people are admired by everyone"

Negation of quantified statement

Statement	When True	When False
$\forall x \in D, P(x)$	$P(x)$ is true for every x in D.	There is one x for which $P(x)$ is false.
$\exists x \in D, P(x)$	There is one x in D for which $P(x)$ is true.	$P(x)$ is false for every x in D.

Assume that D consists of $x_1, x_2, \ldots, x_n$

$\forall x \in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$ and

$\exists x \in D, P(x) \equiv P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$ or

Example 1

"Not all SCSE students study hard." = "There is at least one SCSE student who does not study hard."

$\neg(\forall x \in D, P(x)) \equiv \exists x \in D, \neg P(x)$

D = {SCSE students}

$P(x)$ = "x studies hard"

Negation of a universal quantification becomes an existential quantification.

"It is not the case that some students in this class are from NUS." = "All students in this class are not from NUS."

$\neg(\exists x \in D, P(x)) \equiv \forall x \in D, \neg P(x)$

D = {Students}

$P(x)$ = "x is from NUS"

Negation of an existential quantification becomes an universal quantification.

Example 2

$\neg(\forall x \in D, P(x) \wedge Q(x))$

$\equiv \exists x \in D, \neg(P(x) \wedge Q(x))$

$\equiv \exists x \in D, (\neg P(x) \vee \neg Q(x))$ → De morgan

Determine Truth

① Exhaustion

Let $D = \{5,6,7,8,9\}$

Is $\exists x \in D, x^2 = x$ true or false?

x	x^2	$x^2 = x$
5	$5^2 = 25$	False
6	$6^2 = 36$	False
7	$7^2 = 49$	False
8	$8^2 = 64$	False
9	$9^2 = 81$	False

Check all values manually

② Case

Positive Example to Prove Existential Quantification

Let $\mathbb{Z}$ denote all integers.

Is $\exists x \in \mathbb{Z}, x^2 = x$ true or false?

Take $x = 0$ or 1 and we have it.

True!

Counterexample to Disprove Universal Quantification

Let $\mathbb{R}$ denote all reals.

Is $\forall x \in \mathbb{R}, x^2 > x$ true or false?

Take $x = 0.3$ as a counterexample.

False!

Find the separate case

③ Logical Derivation

Consider an (arbitrary) domain X with n members.

Is $\exists x \in X, (P(x) \vee Q(x)) \equiv (\exists x \in X, P(x)) \vee (\exists x \in X, Q(x))$?

$\exists x \in X, (P(x) \vee Q(x))$

$\equiv [P(x_1) \vee Q(x_1)] \vee \ldots \vee [P(x_n) \vee Q(x_n)]$

$\equiv [P(x_1) \vee \ldots \vee P(x_n)] \vee [Q(x_1) \vee \ldots \vee Q(x_n)]$

$\equiv (\exists x \in X, P(x)) \vee (\exists x \in X, Q(x))$

Conditional Quantification

For any real number x, if $x > 1$ then $x^2 > 1$ (i.e., any real number greater than 1 has a square larger than 1).

- Let $P(x)$ denote "$x > 1$".
- Let $Q(x)$ denote "$x^2 > 1$".
- Recall: $\mathbb{R}$ is the collection of all real numbers.

In Symbolic Form: $\forall x \in \mathbb{R}, (P(x) \rightarrow Q(x))$

Consider the statement "lions are fierce animals".

- Let A denote the collection of all animals.
- Let $P(x)$ denote "x is a lion".
- Let $Q(x)$ denote "x is fierce".
- The statement can be rephrased as: "If an animal x is a lion then x is fierce".

In Symbolic Form: $\forall x \in A, (P(x) \rightarrow Q(x))$

$\forall x \in A \, (P(x) \rightarrow Q(x))$

Then, we define…

Contrapositive	$\forall x \in A, \neg Q(x) \rightarrow \neg P(x)$
Converse	$\forall x \in A, Q(x) \rightarrow P(x)$
Inverse	$\forall x \in A, \neg P(x) \rightarrow \neg Q(x)$

Same

What is $\neg(\forall x \in X, P(x) \rightarrow Q(x))$?

$\neg(\forall x \in X, P(x) \rightarrow Q(x))$

$\equiv \exists x \in X, \neg(P(x) \rightarrow Q(x))$ — Negation of Quantified Statements

$\equiv \exists x \in X, \neg(\neg P(x) \vee Q(x))$ — Conversion of Conditionals

$\equiv \exists x \in X, P(x) \wedge \neg Q(x)$ — De Morgan

Basic Inference Rules

① Universal Generalization

$P(c)$ for **any arbitrary** c from the domain D. is T
$\therefore \forall x \in D, P(x)$

x^2 is non-negative

- $P(x)$ = "x^2 is non-negative"
- $P(c)$ for an arbitrary real c
- Therefore $P(x)$ for all x in $\mathbb{R}$

Domain = $\mathbb{R}$

$P(x)$ = "x^2 is non-negative"

1	$P(c)$ for an arbitrary real c	Hypothesis
2	$\forall x \in \mathbb{R}, P(x)$	Universal Generalisation on 1

② Universal Instantiastion

if $\forall x \in D, P(x)$ is T
$\therefore P(c)$ is T
where c is **any** element of the domain D.

Tom and Jerry

- No cat can catch Jerry.
- Tom is a cat.
- Therefore, Tom cannot catch Jerry.

D = {all animals}

Cat(x) = x is a Cat

Catch(x) = x can catch Jerry

1	$\forall x \in D$, [Cat(x) → ¬ Catch(x)]	Hypothesis
2	Cat(Tom)	Hypothesis
3	Cat(Tom) → ¬ Catch(Tom)	Universal Instantiation on 1
4	¬ Catch(Tom)	Modus Ponens on 2 and 3

→ sub Tom into x
→ Cat(tom) → ¬Catch(tom) is T
Cat(tom) is T
∴ By modeus poneus,
¬Catch(tom) is T

③ Existential Generalization

$P(c)$
$\therefore \exists x \in D, P(x)$
for c **some** specific element of the domain D.

Selling Stocks

If everyone is selling stocks, then someone is selling stocks.

D = {all people}

Sell(x) = "x is selling stocks"

$\forall x \in D$, Sell(x) → $\exists x \in D$, Sell(x)

1	$\forall x \in D$, Sell(x)	Hypothesis
2	Sell(c)	Universal Instantiation on 1
3	$\exists x \in D$, Sell(x)	Existential Generalisation on 2

④ Existential Instantiastion

$\exists x \in D, P(x)$
$\therefore P(c)$ **for some** c in the domain D.

Final Exam

- If any student scores > 80 in the final exam, then s/he receives an A.
- There are students who score > 80 in the final exam.
- Therefore, there are students who receive an A.

D = {all students}

$A(x)$ = "x receives an A"

$M(x)$ = "x scores > 80 in the final exam"

1	$\forall x \in D$, [$M(x)$ → $A(x)$]	Hypothesis
2	$\exists x \in D$, $M(x)$	Hypothesis
3	$M(c)$	Existential Instantiation on 2
4	$M(c)$ → $A(c)$	Universal Instantiation on 1
5	$A(c)$	Modus Ponens on 4 and 3
6	$\exists x \in D$, $A(x)$	Existential Generalisation on 5

→ Chapter4

Proof Techniques

Direct Proof

Proof by mathematical induction

Prove propositions of the form: $\forall n P(n)$

The proof consists of two steps.

Basis Step 1
The proposition $P(1)$ is shown to be true.

Inductive Step 2
Assume $P(k)$ is true (when $n = k$), then prove $P(k+1)$ is true (when $n = k+1$).

When both steps are complete, we have proved that "$\forall n P(n)$" is true.

From Step 2	$P(1) \rightarrow P(2)$ by Universal Instantiation
From Step 1	$P(1)$
Applying Modus Ponen	$P(2)$

Repeat the process to get $P(3)$, $P(4)$, $P(5)$, etc.

So, all $P(k)$ are true, i.e., $\forall n P(n)$.

Inductive step

$$[P(1) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow \forall n P(n)$$

Basis Step Hypothesis Valid Argument

Example: $\forall \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Let $P(n) = \left[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\right]$

Basic Step: $P(1)$ is true

$1 = \frac{(1)(1+1)}{2}$

Inductive Step: Assuming $P(k)$ is true, $k>0$

Imagine this like dominos!

$P(k+1)$ true: $\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$

$= \frac{(k+1)(k+2)}{2}$

$= \frac{(k+1)(k+1+1)}{2}$

So $P(n)$ is T for $n = k+1$,

$\therefore \forall n P(n)$ is T

for any n, $P(n)$ is T

Complete Induction

Prove propositions of the form: $\forall n P(n)$

The proof consists of two steps.

Basis Step 1
The proposition $P(1)$ is shown to be true.

Inductive Step 2
Assume for $k > 1$, $P(m)$ is true for every $m < k$, then prove $P(k)$ is true.

When both steps are complete, we have proved that "$\forall n P(n)$" is true.

Prove that every natural number $n > 1$ is either a prime, or a product of primes.

$P(n)$ = "($n = 1$) ∨ (n is prime) ∨ (n can be factored into primes)"

Basis Step 1
$P(1)$ is true because $n = 1$.

Inductive Step 2
Suppose $k > 1$, and $P(m)$ is true for all $m < k$. We must show that $P(k)$ is true.

If k is prime, $P(k)$ is T

Since $k > 1$, can factor $k = pq$

p is either prime or factors into prime, by induction hypothesis.

Same for q ... $\therefore$ k factors into primes

Proof by contradiction

Normal

- We want to prove $\boxed{P(n) \rightarrow Q(n)}$
- Assume by contradiction that $\boxed{\neg(P(n) \rightarrow Q(n))} = \neg(\neg P(n) \vee Q(n))$ $= P(n) \wedge \neg Q(n)$
- This happens exactly if $P(n)$ and $\neg Q(n)$
- Suppose that $P(n)$ and $\neg Q(n)$
- Prove that this gives a contradiction, namely $\boxed{\neg(P(n) \rightarrow Q(n)) \rightarrow C \wedge \neg C}$ False
- This is equivalent to $\boxed{P(n) \rightarrow Q(n)}$ (Truth table!)

Example

Prove that if n^2 is even, then n is even, for n integer.

Assume n^2 is even & n not even

$P(n)$ = "n^2 is even"

$Q(n)$ = "n is even"

$\neg Q(n)$ = "n is not even"

When n is odd, $n = 2k+1$, $k \in \mathbb{Z}$

$\therefore n^2 = (2k+1)^2$

$= 4k^2+4k+1$

$= 2(2k^2+2k)+1$

This means that n^2 is odd

However, we assumed that n^2 is even

This is a contradiction (C = "n^2 is even", $C \wedge \neg C$)

By contrapositive

We want to prove $\boxed{P(n) \rightarrow Q(n)}$ $= \neg P(n) \vee Q(n)$

equivalent to proving that $\boxed{\neg Q(n) \rightarrow \neg P(n)}$ $= Q(n) \vee \neg P(n)$

contra positive

Example 2

Prove that if n^2 is even, then n is even, for n integer.

Let $P(n)$ = "n^2 is even"

$Q(n)$ = "n is even"

By contrapositive, $\neg Q(n) \Rightarrow \neg P(n)$

n is not even aka $\neg Q(n)$

n is odd : $n = 2k+1$, $k \in \mathbb{Z}$

$n^2 = (2k+1)^2$

$= 2(2k^2+2k)+1$ (odd)

This means that $\neg P(n)$

Combinatorics

Principle of Counting

→ Simply counting permutations!

Also, $0! = 1$

Example

Create a yoghurt dessert with *1* fruit, *1* crunch, and *1* sauce.

- *11* fruits
- *16* crunches
- *15* sauces

→ 3 slot

$11 \times 16 \times 15 = 2640$

Principle of Counting: Cardinality of Power Set

- Consider a set $A = \{a_1,\ldots,a_n\}$ with n elements.
- List all subsets of A. Create a table.

All subsets of A	Binary vectors
$\{a_1\}$	10…0

- Each of these n elements are either in a subset of A or not: *2* choices.
- Such a choice needs to be made for each of the n elements.
- Thus $2*2*\ldots*2 = 2^n$ choices.

Principle of Counting: Filling r Slots With n Choices

There are n elements, with which to fill r slots.

Can Be Repeated

When elements can be repeated using the principle of counting: $n*n*\ldots*n = n^r$ choices.

→ Many marbles into bag

Cannot Be Repeated

When elements cannot be repeated:

- n choices for first slot
- $n - 1$ choices for second slot
- $n - (r - 1)$ choices for last slot
- In total: $n(n-1)(n-2)\ldots(n-r+1)$ choices

→ Cannot re-use marbles, put into bag

Permutation ; n!

A **permutation** is an arrangement of all or part of a set of objects, **with** regard to the order of the arrangement.

1^{st} position	*3* choices
2^{nd} position	*2* choices
3^{rd} position	*1* choice

Number of permutations of n objects

$n*(n-1)*(n-2)\ldots*2*1 = n!$

where $n!$ is called n **factorial**.

Number of permutations (order matters) of n things taken r at a time:

$$P(n,r)=\frac{n!}{(n-r)!}$$

Number of combinations (order does not matter) of n things taken r at a time:

$$C(n,r)=\frac{n!}{(n-r)!r!}$$

Number of different permutations of n objects where there are n_1 repeated items, n_2 repeated items, … n_k repeated items

$$\frac{n!}{n_1!n_2!\ldots n_k!}$$

Repeated

How many permutations are there of "MISSISSIPPI"?

M	Appears $k_1 = 1$
I	Appears $k_2 = 4$
S	Appears $k_3 = 4$
P	Appears $k_4 = 2$

$$\frac{11!}{(1!4!4!2!)}$$

11!/(1! 4! 4! 2!)

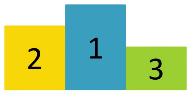
n choose r, ordered (P)

In how many ways can we award a 1^{st}, 2^{nd} and 3^{rd} prize to *8* contestants?

- For the 1^{st} prize, any of the *8*.
- Then for the 2^{nd} prize, any of the *7* left.
- And for the 3^{rd} prize, any of the *6* left.
- Hence $8*7*6 = 336$.

Alternatively: $\frac{8!}{(8-3)!} = 336$

or… $8P3$



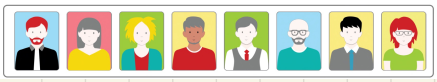


table seating permutation

6 people, around round table; Permutation $= \frac{6!}{6} = (6-1)! = 5!$

Combination

A **combination** is a selection of all or part of a set of objects, **without** regard to the order in which objects are selected.

Example

Team of *4* people from a group of *10*.

Number of combinations of n objects taken r at a time:

$\binom{n}{r} = C(n,r) = n!/r!(n-r)!$

There are $r!$ possible orderings within each combination.

So $r!\,C(n,r) = P(n,r)$ by definition of permutation.

From a committee of *8* people, in how many ways can you choose:

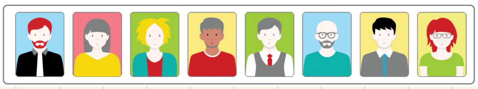
- A chairperson and vice-chairperson (one person cannot hold more than one position)?

P(8,2)

$8P2 = 56$

ordered

Chairperson Vice-chairperson



From a committee of *8* people, in how many ways can you choose:

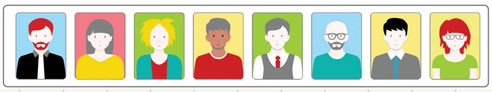
- A subcommittee of *2* people?

C(8,2)

$8C2 = 28$

No order

Subcommittee



Linear Recurrence Relation

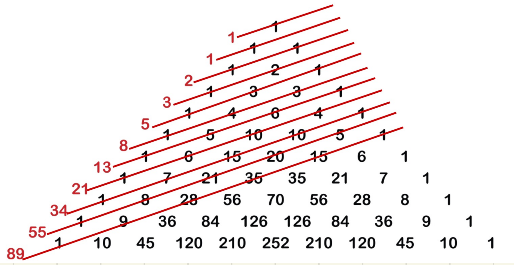
A **recurrence relation** is an equation that **recursively defines a sequence**, i.e., each term of the sequence is defined as a function of the preceding terms.

A recursive formula must be accompanied by **initial conditions** (information about the beginning of the sequence).

Example of recurrence:

Fibonacci Sequence

$$f_n = f_{n-1} + f_{n-2} \text{ with } f_0 = 0, f_1 = 1$$



How to solve?

1) Backtracking

Example

$a_n = a_{n-1} + 3$ and $a_1 = 2$

$a_{n-1} = a_{(n-1)-1} + 3$

$= a_{n-2} + 3$

$a_n = a_{n-1} + 3 = (a_{n-2} + 3) + 3 = a_{n-2} + 2*3$

$= (a_{n-3} + 3) + 2*3 = a_{n-3} + 3*3$

$= (a_{n-4} + 3) + 3*3 = a_{n-4} + 4*3$

...

Backtrack until a_1 Eq^n

$= a_1 + (n-1)*3$

$a_n = 2 + (n-1)*3$

Example:

Solve $a_n = 2a_{n-1} - a_{n-2}$ with initial conditions $a_1 = 3$, $a_0 = 0$

$a_n = 2a_{n-1} - a_{n-2}$ (− a_{n-1} on both sides)

$a_n - a_{n-1} = 2a_{n-1} - a_{n-2} - a_{n-1}$

$a_n - a_{n-1} = a_{n-1} - a_{n-2}$

$= a_{n-2} - a_{n-3}$

$=$ ⋮

$= a_1 - a_0$

$= 3 - 0$

$= 3$

$\therefore a_n - a_{n-1} = 3$

$a_n = a_{n-1} + 3$ (solved)

2) Characteristic Eq^n

A **linear homogeneous relation** of degree d is of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d}$$

E.g.,:

- The Fibonacci sequence
- The relation: $a_n = 2a_{n-1}$ (degree 1)
- But **not** the relation: $a_n = 2a_{n-1} + 1$

The **characteristic equation** of the above relation is:

$$x^d = c_1 x^{d-1} + c_2 x^{d-2} + \dots + c_d$$

If the **characteristic equation** $x^2 - c_1 x - c_2 = 0$ (of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$) has:

- two distinct roots s_1, s_2, then the explicit formula for the sequence a_n is

$$u*s_1^n + v*s_2^n$$

- a single root s, then the explicit formula for a_n is

$$u*s^n + v*n*s^n$$

where u and v are determined by initial conditions.

Example:

Solve $a_n = 2a_{n-1} - a_{n-2}$ with initial conditions $a_1 = 3$, $a_0 = 0$

Degree is 2, as there is n-1, n-2

Separate example: $a_n = a_{n-1} + a_{n-3}$

$\downarrow$

$x^3 = x^2 + 1$

The eq^n : $x^2 = 2x - 1$

$x^2 - 2x + 1 = 0$

$(x-1)^2 = 0$

Single Root: Use ; $a_n = U \cdot s^n + V \cdot n \cdot s^n$

$= U \cdot (1)^n + V \cdot n \cdot (1)^n$

$= U + V \cdot n$

Sub a_1, a_0

(1) — $a_0 = U + V \cdot (0)$

$0 = U$

(2) — $a_1 = U + V \cdot (1)$

$3 = U + V$

$\therefore a_n = 3n$ //

Example:

Determine the number of bit strings (i.e., comprising 0s and 1s) of length n that contains no adjacent 0s.

- C_n = the number of such bit strings
- A binary string with no adjacent 0s is constructed by:
  - Adding "1" to any string w of length $n - 1$ satisfying the condition, or
  - Adding "10" to any string v of length $n - 2$ satisfying the condition
- Thus $C_n = C_{n-1} + C_{n-2}$ where $C_1 = 2$ $(0,1)$, $C_2 = 3$ $(01, 10, 11)$

Now solve $C_n = C_{n-1} + C_{n-2}$ where $C_1 = 2$, $C_2 = 3$

Eq^n is $x^2 = x + 1$

$x^2 - x - 1 = 0$

Roots are $x = \frac{1+\sqrt{5}}{2}$, $x = \frac{1-\sqrt{5}}{2}$

$\therefore$ $C_n = u \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + v \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n$

Initial conditions give us:

$$C_1 = u * \left(\frac{1+\sqrt{5}}{2}\right) + v * \left(\frac{1-\sqrt{5}}{2}\right) = 2$$

i.e., $\frac{u+v}{2} + \frac{(u-v)\sqrt{5}}{2} = 2$

$$C_2 = u * \left(\frac{1+\sqrt{5}}{2}\right)^2 + v * \left(\frac{1-\sqrt{5}}{2}\right)^2 = 3$$

i.e., $\frac{3(u+v)}{2} + \frac{(u-v)\sqrt{5}}{2} = 3$

Solving this we get:

$$u = \frac{\sqrt{5}+3}{2\sqrt{5}}$$

$$v = \frac{\sqrt{5}-3}{2\sqrt{5}}$$

$$C_n = \left(\frac{\sqrt{5}+3}{2\sqrt{5}}\right) * \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-3}{2\sqrt{5}}\right) * \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Set Theory

- Two common ways to specify a set:
  - **Explicit**: enumerate the members
    - E.g., $A = \{2, 3\}$
  - **Implicit**: description using predicates $\{x \mid P(x)\}$
    - E.g., $A = \{x \mid x$ is a prime number$\}$

$\in$ ··

We write $x \in S$ iff x is an element (member) of S.

E.g., $A = \{x \mid x$ is a prime number$\}$ then $A = \{2, 3, 5, 7, \dots\}$
$2 \in A$, $3 \in A$, $5 \in A$, ..., $1 \notin A$, $4 \notin A$, $6 \notin A$, ...

A set A **is a subset of the set** B, denoted by $A \subseteq B$ iff every element of A is also an element of B.

I.e.,:

equivilant

- $A \subseteq B \triangleq \forall x(x \in A \rightarrow x \in B)$
- $A \not\subseteq B \triangleq \neg (A \subseteq B)$

  $\equiv \neg \forall x(x \in A \rightarrow x \in B)$

  $\equiv \exists x(x \in A \wedge x \notin B)$

- E.g., $B = \{1, 2, 3\}$, $A = \{1, 2\} \subseteq B$ $\quad C = \{1, 2, 4\} \not\subseteq B$

NULL SET

The empty set is denoted by $\varnothing$ or by $\{\ \}$.

Note: $\varnothing \neq \{\varnothing\}$

$$A = B \triangleq \forall x(x \in A \leftrightarrow x \in B)$$

- Two sets A and B are equal iff they have the same elements.

  $A \neq B \triangleq \neg \forall x(x \in A \leftrightarrow x \in B)$

  $\equiv \exists x\, [(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)]$

- Two sets are not equal if they do not have identical members, i.e., there is at least one element in one of the sets which is absent in the other.
  - E.g., $\underbrace{\{1, 2, 3\}}_{A} = \underbrace{\{3, 1, 2\}}_{B} = \{1, 3, 2\} = \{1, 1, 1, 2, 3, 3, 3\}$ $\quad \therefore A = B$

Cardinality

The **cardinality** $|S|$ of S is the number of elements in S. (E.g., for $S = \{1, 3\}$, $|S| = 2$)

- If $|S|$ is finite, S is a finite set; otherwise S is infinite.
  - The set of **positive** integers is an infinite set.
  - The set of **prime** numbers is an infinite set.
  - The set of **even prime** numbers is a finite set. $\rightarrow \{2\}$
- Note: $|\varnothing| = 0$

Power Set

The **power set** $P(S)$ of a given set S is the set of all subsets of S: $P(S) = \{A \mid A \subseteq S\}$.

- E.g., for $S = \{1,2,3\}$

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

- If a set S has n elements, then $P(S)$ has 2^n elements.
  - Hint: Try to leverage the Binomial theorem.

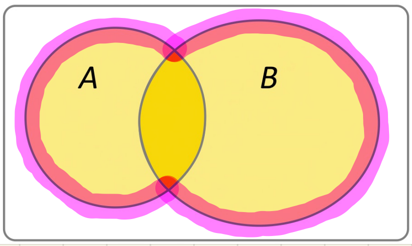
$$(x+y)^n = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \dots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n,$$

$P(S) = \{\phi, \}$ ✓

Union

The **union of sets A and B** is the set of those elements that are either in A, in B, or both.

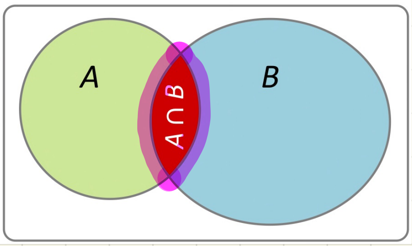
$$A \cup B \triangleq \{x \mid x \in A \vee x \in B\}$$



Intersection

The **intersection of the sets A and B** is the set of all elements that are in both A and B.

$$A \cap B \triangleq \{x \mid x \in A \wedge x \in B\}$$



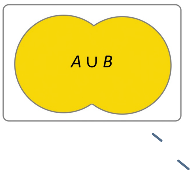
NO Intersect

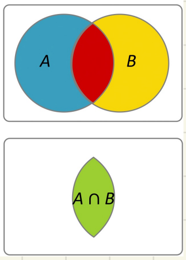
Sets A and B are **disjoint** iff $A \cap B = \varnothing$

$$|A \cap B| = 0$$

Venn Diagram: Cardinality of Union

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

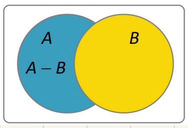




Venn Diagram: Set Difference and Complement

The **difference of A and B** (or **complement of B with respect to A**) is the set containing those elements that are in A but not in B.

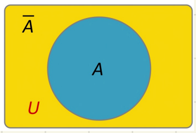
$$A - B \triangleq \{x \mid x \in A \wedge x \notin B\}$$



Venn Diagram: Set Difference and Complement

The **complement of A** is the complement of A with respect to U.

$$\overline{A} = U - A \triangleq \{x \mid x \notin A\}$$



Cartesian Product

The **Cartesian product $A \times B$** of the sets A and B is the set of all **ordered pairs** (a,b) where $a \in A$ and $b \in B$.

$$A \times B \triangleq \{(a,b) \mid a \in A \wedge b \in B\}$$

Example:

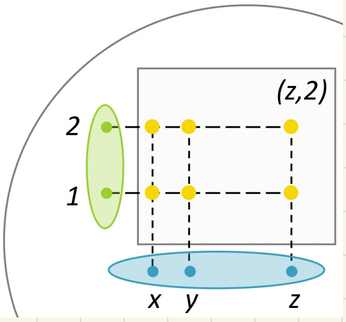
$A = \{1,2\}$, $B = \{x,y,z\}$

$A \times B = \{(1,x), (1,y), (1,z), (2,x), (2,y), (2,z)\}$

$B \times A = \{(x,1), (x,2), (y,1), (y,2), (z,1), (z,2)\}$

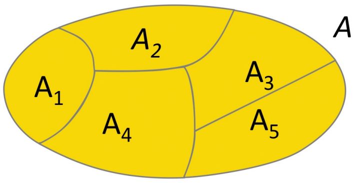
In general: $A_1 \times A_2 \times \ldots \times A_n \triangleq \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i$ **for** $i = 1, 2, \ldots, n\}$

$|A_1 \times A_2 \times \ldots \times A_n| = |A_1|\,|A_2| \ldots |A_n|$



Partition

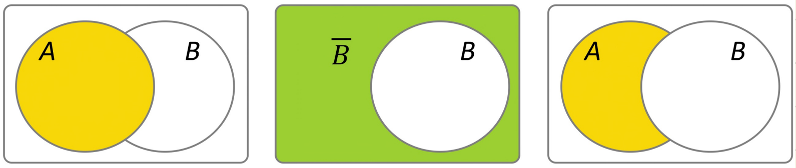
A collection of nonempty sets $\{A_1, A_2, \ldots, A_n\}$ is a **partition** of a set A, iff $A = A_1 \cup A_2 \cup \ldots A_n$ and $A_1, A_2, \ldots, A_n$ are **mutually disjoint**, i.e., $A_i \cap A_j = \varnothing$ for all $i, j = 1, 2, \ldots, n$, and $i \neq j$.



Set identity

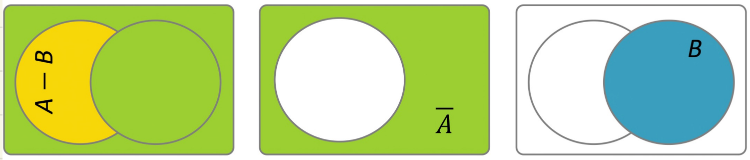
Identity	Name
$A \cup \varnothing = A$ $A \cap U = A$ universal set	Identity laws
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{\overline{A}} = A$	Double Complement laws
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A - B = A \cap \overline{B}$	Alternate representation for set difference

$A \cap \overline{B} = A - B$



Compare $A \cap \overline{B}$ with $A - B = \{x \mid x \in A \wedge x \notin B\}$

$\overline{A \cap \overline{B}} = \overline{A} \cup B$



- **Consider** $\overline{A - B} = \overline{A \cap \overline{B}}$
- **This is De Morgan's Law** $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$ **with** $X = A$ **and** $Y = \overline{B}$

Proving Set identity

a) Show that each set is a subset of the other

step 1 **Show that** $(B - A) \cup (C - A) = (B \cup C) - A$

For any $x \in$ LHS, $x \in (B - A)$ **or** $x \in (C - A)$ **(or both)**

When $x \in B - A$
- $\Rightarrow (x \in B) \wedge (x \notin A)$
- $\Rightarrow (x \in B \cup C) \wedge (x \notin A)$
- $\Rightarrow x \in (B \cup C) - A$

When $x \in C - A$
- $\Rightarrow (x \in C) \wedge (x \notin A)$
- $\Rightarrow (x \in B \cup C) \wedge (x \notin A)$
- $\Rightarrow x \in (B \cup C) - A$

Therefore LHS $\subseteq$ RHS

step 2 **Show that** $(B - A) \cup (C - A) = (B \cup C) - A$

For any $x \in$ RHS, $x \in (B \cup C)$ **and** $x \notin A$

When $x \in B$ **and** $x \notin A$: $(x \in B) \wedge (x \notin A)$
- $\Rightarrow x \in B - A$
- $\Rightarrow x \in (B - A) \cup (C - A)$

When $x \in C$ **and** $x \notin A$: $(x \in C) \wedge (x \notin A)$
- $\Rightarrow x \in C - A$
- $\Rightarrow x \in (B - A) \cup (C - A)$

Therefore RHS $\subseteq$ LHS

$\therefore$ **With LHS $\subseteq$ RHS and RHS $\subseteq$ LHS, we can conclude that LHS = RHS.**

b) Apply set identity theorems

Show that $(A - B) - (B - C) = A - B$

$$\begin{aligned}
(A-B)-(B-C) &= (A \cap \overline{B}) \cap (B \cap \overline{C}) && \textbf{(By alternate representation for set difference)} \\
&= (A \cap \overline{B}) \cap (\overline{B} \cup C) \; \text{open up} && \textbf{(By De Morgan's laws)} \\
&= [(A \cap \overline{B}) \cap \overline{B}] \cup [(A \cap \overline{B}) \cap C] && \textbf{(By Distributive laws)} \\
&= [A \cap (\overline{B} \cap \overline{B})] \cup [A \cap (\overline{B} \cap C)] && \textbf{(By Associative laws)} \\
&= (A \cap \overline{B}) \cup [A \cap (\overline{B} \cap C)] && \textbf{(By Idempotent laws)} \\
&= A \cap [\overline{B} \cup (\overline{B} \cap C)] && \textbf{(By Distributive laws)} \\
&= A \cap \overline{B} && \textbf{(By Absorption laws)} \\
&= A - B && \textbf{(By alternate representation for set difference)}
\end{aligned}$$

c) Use membership tables

Similar to truth table (in propositional logic):

- **Columns for different set expressions**
- **Rows for all combinations of memberships in constituent sets**
- **"*1*" = membership, "*0*" = non-membership**
- **Two sets are equal iff they have identical columns**

Prove that $(A \cup B) - B = A - B$

A	B	$A \cup B$	$(A \cup B) - B$	$A - B$
0	0	0	0 — same —	0
0	1	1	0 — same —	0
1	0	1	1 — same —	1
1	1	1	0 — same —	0

Binary Relations

Let A and B be sets. A **binary relation** R **from** A **to** B is a subset of $A \times B$. Given (x,y) in $A \times B$, x **is related to** y **by** R $(xRy) \leftrightarrow (x,y) \in R$.

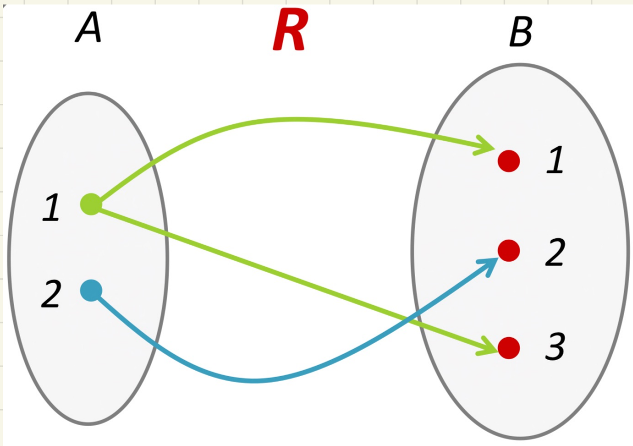
Example

$A = \{1,2\}$, $B = \{1,2,3\}$, $(x,y) \in R \leftrightarrow (x-y)$ is even

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

$(1,1) \in R$, $(1,3) \in R$, $(2,2) \in R$

$x > y$, x **owes** y, x **divides** y



Inverse Binary R/S

Let R be a relation from A to B. The **inverse relation** R^{-1} from B to A is defined as: $R^{-1} = \{(y,x) \in B \times A \mid (x,y) \in R\}$.

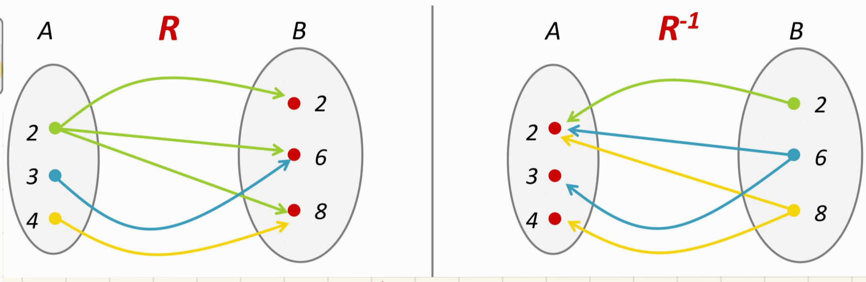
$A = \{2,3,4\}$, $B = \{2,6,8\}$, $(x,y) \in R \leftrightarrow x$ **divides** y

$A \times B = \{(2,2), (2,6), (2,8), (3,2), (3,6), (3,8), (4,2), (4,6), (4,8)\}$

$(2,2) \in R, (2,6) \in R, (2,8) \in R, (3,6) \in R, (4,8) \in R$

$(2,2) \in R^{-1}, (6,2) \in R^{-1}, (8,2) \in R^{-1}, (6,3) \in R^{-1}, (8,4) \in R^{-1}$ These are in R^{-1}

$(y,x) \in R^{-1} \leftrightarrow y$ **is a multiple of** x



MATRIX Representation

$A = (a_1, a_2, a_3)$, $B = (b_1, b_2, b_3, b_4)$,

$R = \{(a_1, b_2), (a_2, b_1), (a_3, b_1), (a_3, b_4)\}$

(i,j)th **entry is** T **if** $a_i R b_j$:
$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{cccc} b_1 & b_2 & b_3 & b_4 \end{array} \\ \begin{bmatrix} F & T & F & F \\ T & F & F & F \\ T & F & F & T \end{bmatrix} \end{array}$$

Example

$A = \{2,3,4\}$, $B = \{2,6,8\}$, $(x,y) \in R \leftrightarrow x$ **divides** y.

A\B	2	6	8
2	T	T	T
3	F	T	F
4	F	F	T

normal

$$a_i R b_j: \quad \begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{cccc} b_1 & b_2 & b_3 & b_4 \end{array} \\ \begin{bmatrix} F & T & F & F \\ T & F & F & F \\ T & F & F & T \end{bmatrix} \end{array}$$

R^{-1}

$$b_i R^{-1} a_j: \quad \begin{array}{c} \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{array}\begin{array}{c} \begin{array}{ccc} a_1 & a_2 & a_3 \end{array} \\ \begin{bmatrix} F & T & T \\ T & F & F \\ F & F & F \\ F & F & T \end{bmatrix} \end{array}$$

$$R = \{(a_1, b_2), (a_2, b_1), (a_3, b_1), (a_3, b_4)\}$$

$$R^{-1} = \{(b_2, a_1), (b_1, a_2), (b_1, a_3), (b_4, a_3)\}$$

TRANSPOSE

Composition of relations

Given R in $A \times B$, and S in $B \times C$, the **composition** of R and S is a relation on $A \times C$ defined by $R \circ S = \{(a,c) \in A \times C \mid \exists\, b \in B, aRb \text{ and } bSc\}$.

Example

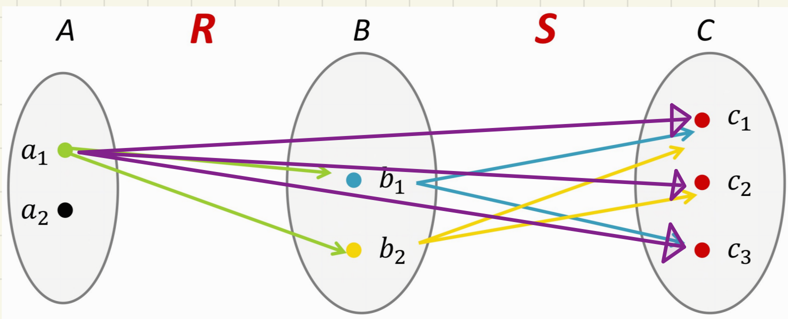
$A = \{a_1, a_2\}, B = \{b_1, b_2\}, C = \{c_1, c_2, c_3\}$

$R = \{(a_1, b_1), (a_1, b_2)\}$

$S = \{(b_1, c_1), (b_2, c_1), (b_1, c_3), (b_2, c_2)\}$

What is $R \circ S$?

$R \circ S = \{(a_1, c_1), (a_1, c_3), (a_1, c_2)\}$



* b is a "station" or "path"

Reflexivity

A relation R on a set A is **reflexive** if every element of A is related to itself: $\forall x \in A, xRx$.

Example 2

$A = \mathbb{Z}$, $xRy \leftrightarrow x = y$: reflexive

$A = \mathbb{Z}$, $xRy \leftrightarrow x > y$: not reflexive

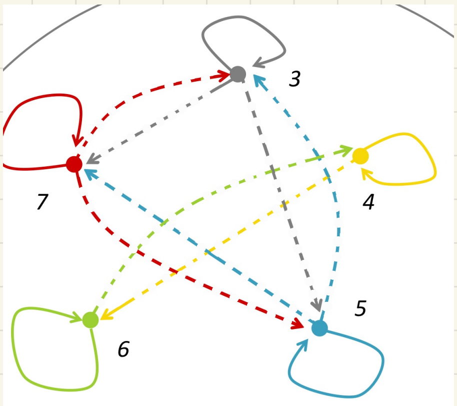
What is the reflexivity on the matrix representing R? → Diagonal of matrix

Example 1

$A = \{3,4,5,6,7\}$, $xRy \leftrightarrow (x - y)$ is even

R reflexive

- Check for self loop, everything must be loopable



X	a_1	a_2	a_3	a_4
a_1	T	F	T	F
a_2	F	T	F	T
a_3	F	T	T	F
a_4	F	F	F	T

$xRy \leftrightarrow (x-y = \text{even})$

Symmetry

A relation R on a set A is **symmetric** if $(x,y) \in R$ implies $(y,x) \in R$: $\forall x \in A\ \forall y \in A, xRy \rightarrow yRx$.

Not Symmetric Relationship

E.g., $A = \mathbb{Z}$, $xRy \leftrightarrow x > y$: not symmetric

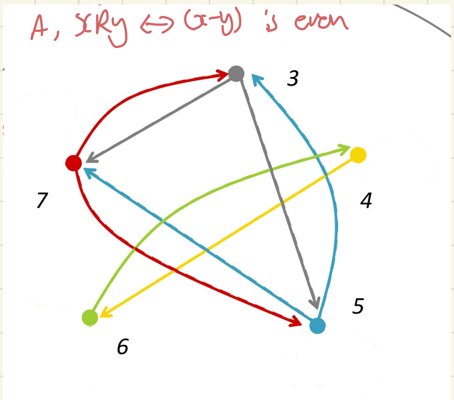
$x > y$

? $y \not> x$

Symmetric Relationship

E.g., $A = \mathbb{Z}$, $xRy \leftrightarrow x = y$: symmetric

$x = y$
$y = x$



Transitivity (basically checking the composition of R/s)

A relation R on a set A is **transitive** if $(x,y) \in R$ and $(y,z) \in R$ implies $(x,z) \in R$: $\forall x\ \forall y\ \forall z\ xRy \land yRz \rightarrow xRz$.

$A = \mathbb{Z}$, $xRy \leftrightarrow x = y$: **transitive** →

$xRa \land aRy$

$x = a \land a = y$

$\therefore x = y$

$(x, y) \in R$

$A = \mathbb{Z}$, $xRy \leftrightarrow x > y$: **transitive**

$xRa \land aRy$

$x > a \land a > y$

$\therefore x > y$

$(x, y) \in R$

Equivalence Relation ????

A relation R on a set A is **an equivalence relation** if:

1. R is reflexive: $\forall x \in A, xRx$
2. R is symmetric: $\forall x \forall y\ xRy \rightarrow yRx$
3. R is transitive: $\forall x \forall y \forall z\ xRy \wedge yRz \rightarrow xRz$

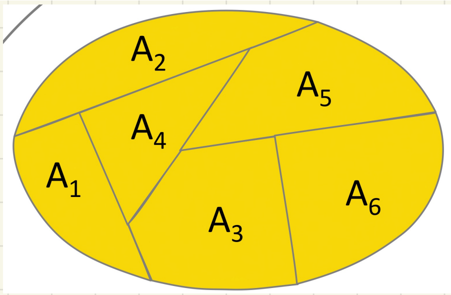
Equivalence class of a in A: $[a] = \{x \in A \mid aRx\}$ for R an equivalence relation.

Partition of a set A:

$A_i \cap A_j = \varphi$ whenever $i \neq j$

$A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6 = A$

Equivalence classes of A form a partition of A.



Example:

$a \equiv b \pmod n \leftrightarrow a = qn + b$

$\equiv \pmod n$ is **an equivalence relation**:

1. $\equiv \pmod n$ is reflexive: $\forall x \in A$, $x \equiv x \bmod n$
2. $\equiv \pmod n$ is symmetric: $\forall x \forall y\ x \equiv y \pmod n \rightarrow y \equiv x \pmod n$
3. $\equiv \pmod n$ is transitive: $\forall x \forall y \forall z\ x \equiv y \pmod n \wedge y \equiv z \pmod n \rightarrow x \equiv z \pmod n$

$x = q(n) + y$

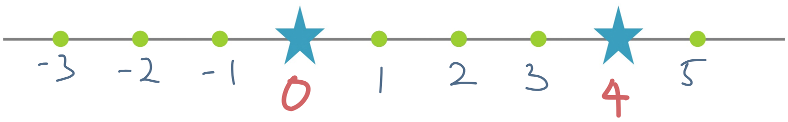
$y = (-q)(n) + x$

$\left.\begin{array}{l} x = q_1(n) + y \\ y = q_2(n) + z \end{array}\right\} \begin{array}{l} x = q_1(n) + q_2(n) + z \\ x = (q_1 + q_2)(n) + z \end{array}$

Equivalence class of $[0] = \{0, n, 2n, 3n, \ldots, -n, -2n, -3n \ldots\}$

Equivalence class of $[1] = \{1, n+1, 2n+1, 3n+1, \ldots, -n+1, -2n+1 \ldots\}$

Example: Integers mod 4



Integers mod n can be represented as elements between 0 and $n-1$: $\{0, 1, 2, \ldots, n-1\}$

☆ Any integer will be a part of one of the 4 equivalence classes here, as this is the nature of mod (4)

Example

Let A be the set of all integers, and $x\,R\,y$ if and only if $x - y$ is even. R is equivalence relation.

R : $x - y$ is even

1) Reflexive? : $x - x$ will be even, $x \in \mathbb{Z}$

2) Symmetry? : $y - x$ is even, $x - y$ is even

3) Trans? : yes

True, as the equivalence classes are $[0]$ and $[1]$, where 0 denotes even numbers & 1 denotes odd numbers

Anti-symmetry

A relation R on a set A is **antisymmetric** if $(x,y) \in R$ and $(y,x) \in R$ implies $x = y$: $\forall x \forall y\ xRy \wedge yRx \rightarrow x = y$.

Example

$A = \mathbb{Z}$, $xRy \leftrightarrow x = y$: antisymmetric

$A = \mathbb{Z}$, $xRy \leftrightarrow x \geq y$: antisymmetric

$\left.\begin{array}{l} (x,y) \in R \Rightarrow x \geq y \\ (y,x) \in R \Rightarrow y \geq x \end{array}\right\}$

$x = y$

$BRC \leftrightarrow B \subseteq C$: antisymmetric

$\left.\begin{array}{l} (B,C) \in R \Rightarrow B \subseteq C \\ (C,B) \in R \Rightarrow C \subseteq B \end{array}\right\} B = C$

Basically, if $aRb \wedge bRa \Rightarrow a = b$

Partial Order

R is **a partial order** on A if R is reflexive, antisymmetric and transitive.

Example

check
reflexive, $\forall x \in A$, $(x,x) \in R \Rightarrow x \le x$

anti-symmetry, $\left.\begin{array}{l}(x,y) \in R \Rightarrow x \le y \\ (y,x) \in R \Rightarrow y \le x\end{array}\right\}$ $x = y$ → only when $x=y$ can this be valid

trans, $\left.\begin{array}{l}(x,y) \in R \Rightarrow x \le y \\ (y,z) \in R \Rightarrow y \le z\end{array}\right\}$ $x \le z$, $(x,z) \in R$

$A = \mathbb{Z}$, $xRy \leftrightarrow x \le y$

Notion of partial order is useful for scheduling problems across possibly different domains.

Transitive Closure

Let A be a set and R a binary relation on A.

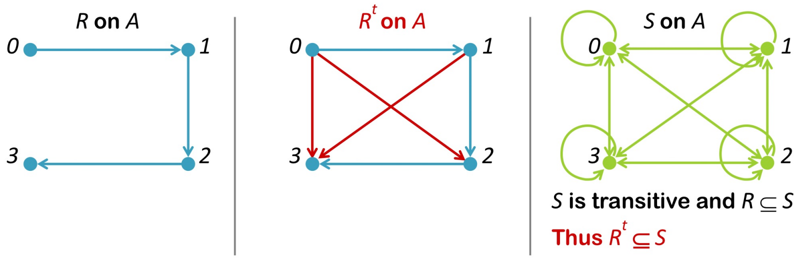
The **closure of a relation** $R \subseteq A \times A$ with respect to a property P (P being reflexive, symmetric, or transitive) is the relation obtained by adding the minimum number of ordered pairs to R to obtain property P.

Let A be a set and R a binary relation on A. The **transitive closure** of R is the binary relation R^t on A that satisfies the following three properties:

1. R^t is transitive
2. $R \subseteq R^t$
3. If S is any other transitive relation that contains R then $R^t \subseteq S$

Let $A = \{0,1,2,3\}$

Consider a relation $R = \{(0,1),(1,2),(2,3)\}$ on A



S is transitive and $R \subseteq S$

Thus $R^t \subseteq S$

$R^t = \{(0,1),(1,2),(2,3),(0,2),(0,3),(1,3)\}$

Transitive Closure: Construction

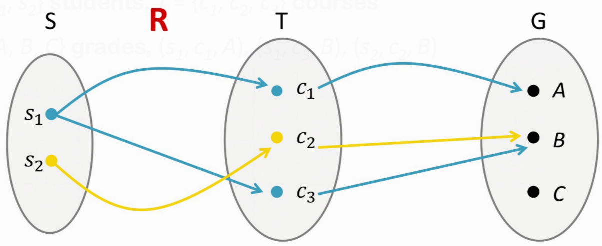
- Let A be a set and R a binary relation on A.
- Start with R, and do the following: $\forall x, y, z \in A$, if $(xRy \wedge yRz \wedge x\cancel{R}z)$ then add (x,z).
- Repeat until the obtained relation is transitive (will stop if $|A|$ is finite).
- The ordering in which the edges are added does not matter.

Non-Binary R/S

Let $A_1, \ldots, A_n$ be sets. A *n-ary* **relation** R is a subset of $A_1 \times \cdots \times A_n$. $a_1, \ldots, a_n$ are related if $(a_1, \ldots, a_n) \in R$.

$S = \{s_1, s_2\}$ students, $T = \{c_1, c_2, c_3\}$ courses

$G = \{A, B, C\}$ grades, (s_1, c_1, A), (s_1, c_3, B), (s_2, c_2, B) $\in R$



Complement of a R/S

Let $R \subseteq A_1 \times \cdots \times A_n$ be a relation.
$\bar{R} = (A_1 \times \cdots \times A_n - R)$ is **the relational complement of R**,
i.e., $(a_1, a_2, a_3, \ldots, a_n) \in \bar{R} \Leftrightarrow (a_1, a_2, a_3, \ldots, a_n) \notin R$.

$A = \{1,2\}$, $B = \{3,5\}$ and $R = \{(1,3), (2,5)\}$

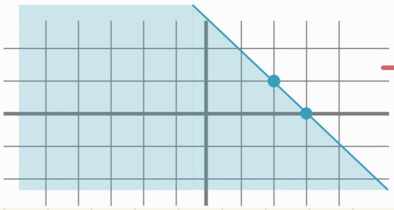
Then $\bar{R} = A \times B - R = \{(1,5), (2,3)\}$ anything not in R/S

Operations on R/S

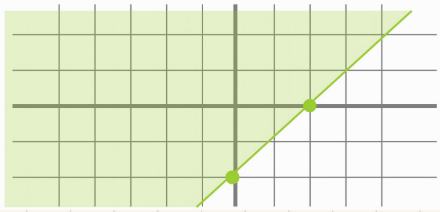
Union / intersection ⇒ ∪ / ∩ ⇒ Combine all / same x,y

$T = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x + y \leq 3 \}$

real number

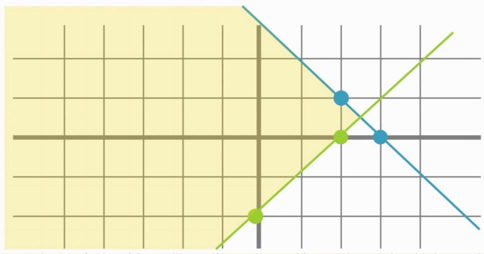


$S = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid x - y \leq 2 \}$



∩

$T \cap S = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid (x + y \leq 3) \land (x - y \leq 2)\}$



Functions

$f(x)$ Let X and Y be sets. A **function** f from X to Y is a rule that assigns every element x of X to a unique y in Y. We write $f: X \to Y$ and $f(x) = y$.

$$(\forall x \in X\ \exists y \in Y, y = f(x)) \land (\forall x_1, x_2 \in X, f(x_1) \neq f(x_2) \to x_1 \neq x_2)$$

X =	Domain
Y =	Codomain
y =	**Image** of x under f
x =	**Preimage** of y under f
Range =	Subset of Y with preimages

Domain $X = \{a,b,c\}$

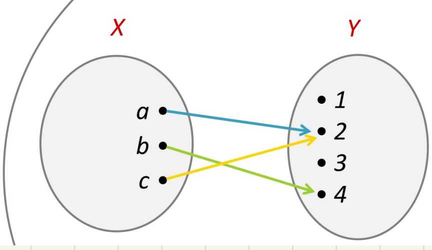
Codomain $Y = \{1,2,3,4\}$

$f = \{(a,2), (b,4), (c,2)\}$

Preimage of 2 is $\{a,c\}$

Range = $\{2,4\}$

Arrow Diagram of f:

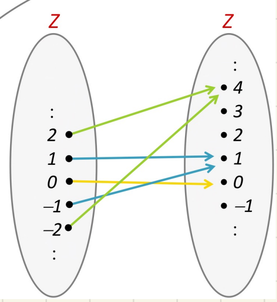


Let f be the function from Z to Z that assigns the square of an integer to this integer.

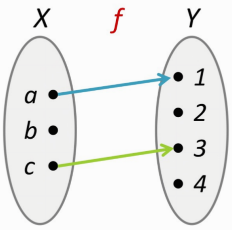
Then $f: Z \to Z, f(x) = x^2$

Domain and codomain of f: Z

Range (f) = $\{0, 1, 4, 9, 16, 25, ...\}$

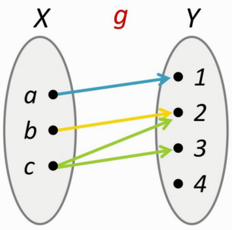


$X = \{a,b,c\}$ to $Y = \{1,2,3,4\}$



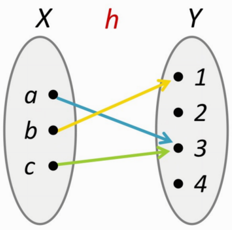
No!

(b has no image)



No!

(c has two images)

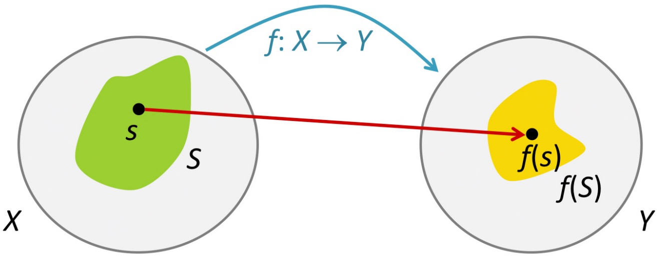


Yes!

(Each element of X has exactly one image)

Image of a set

Let f be a function from X to Y and $S \subseteq X$. The **image of S** is the subset of Y that consists of the images of the elements of S: $f(S) = \{f(s) \mid s \in S\}$.



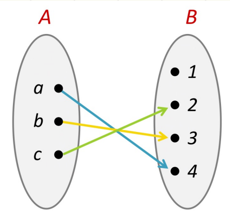
Injective

Injectivity: One-to-one Function

A function f is **one-to-one** (or **injective**), if and only if $f(x) = f(y)$ implies $x = y$ for all x and y in the domain of f.

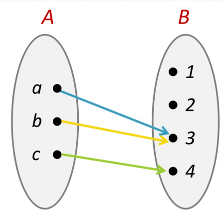
In words…

"All elements in the domain of f have different images".



One-to-one

(All elements in A have a different image)



Not one-to-one

(a and b have the same imag

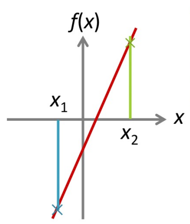
Mathematical Description

$f: A \to B$ is one-to-one $\Leftrightarrow \forall x_1, x_2 \in A\ (f(x_1) = f(x_2) \Longrightarrow x_1 = x_2)$

or

$f: A \to B$ is one-to-one $\Leftrightarrow \forall x_1, x_2 \in A\ (x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2))$

$f: R \to R,\ f(x) = 4x - 1$



Does each element in R have a different image?

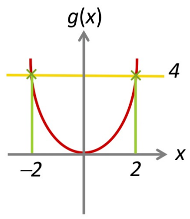
Yes!

To show $\forall x_1, x_2 \in R\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$,

take some $x_1, x_2 \in R$ with $f(x_1) = f(x_2)$.

Then $4x_1 - 1 = 4x_2 - 1 \Rightarrow 4x_1 = 4x_2 \Rightarrow x_1 = x_2$.

$g: R \to R,\ g(x) = x^2$



No!

Take $x_1 = 2$ and $x_2 = -2$.

Then $g(x_1) = 2^2 = 4 = g(x_2)$ and $x_1 \neq x_2$.

Surjective (onto)

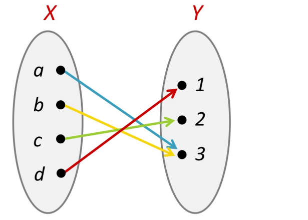
$f(x)$ A function f from X to Y is **onto** (or **surjective**), if and only if for every element $y \in Y$ there is an element $x \in X$ with $f(x) = y$.

In words…

"Each element in the codomain of f has a preimage".

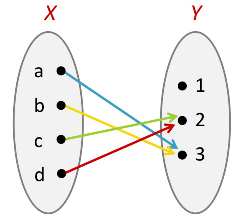
Mathematical Description

$f: X \to Y$ is onto $\Leftrightarrow \forall y \in Y \; \exists x \in X, \; f(x) = y$



Onto

(All elements in Y have a preimage)



Not onto

(1 has no preimage)

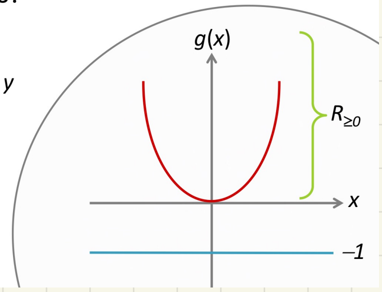
$g: R \to R, \; g(x) = x^2$

Does each element in R have a preimage?

No!

- To show $\exists y \in R$ such that $\forall x \in R \; g(x) \neq y$
- Take $y = -1$
- Then any $x \in R$ holds $g(x) = x^2 \neq -1 = y$

But $g: R \to R_{\geq 0}$, $g(x) = x^2$ (where $R_{\geq 0}$ denotes the set of non-negative real numbers) is onto!



→ write x in terms of y!

$$y = \frac{x+1}{x}$$

$$xy = x + 1$$

$$x = \frac{1}{y-1} \leftarrow$$ Tells us how to find preimage of y

Bijectivity

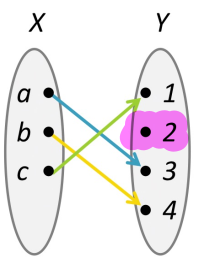
$f(x)$ A function f is a **one-to-one correspondence** (or **bijection**), if and only if it is both one-to-one and onto.

In words…

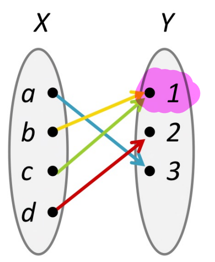
"No element in the codomain of f has two (or more) preimages" (one-to-one)

and

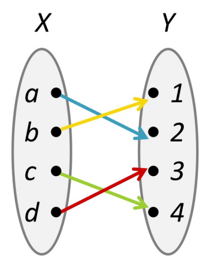
"Each element in the codomain of f has a preimage" (onto)



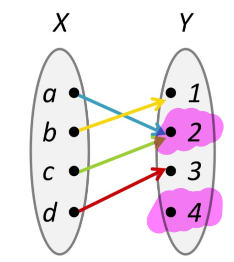
No!
(Not onto as 2 has no preimage)



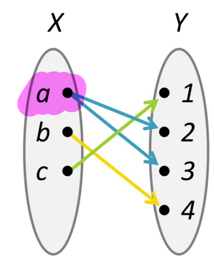
No!
(Not one-to-one as 1 has two preimages)



Yes!
(Each element has exactly one preimage)



No!
(Neither one-to-one nor onto)



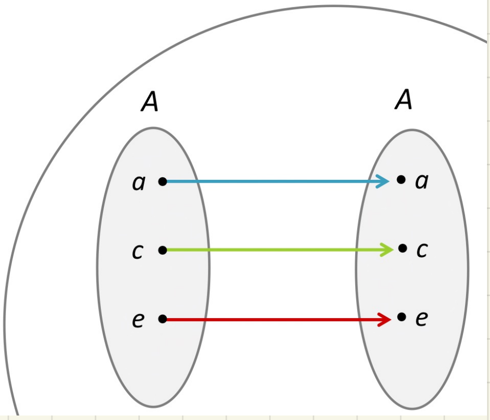
No!
(Not a function as a has two images)

Identity (it is bijective)

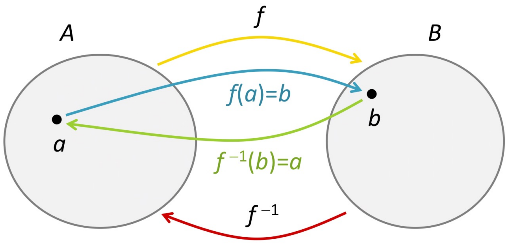
The identity function on a set A is defined as:
$i_A: A \to A$, $i_A(x) = x$.

Example

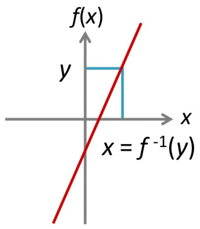
All identity functions are bijections (e.g., for $A = \{a, c, e\}$).



Let $f: A \to B$ be a one-to-one correspondence (bijection). Then the inverse function of f, $f^{-1}: B \to A$, is defined by: $f^{-1}(b)$ = that unique element $a \in A$ such that $f(a) = b$. We say that f is invertible.



What is the inverse of
$f: R \to R$, $f(x) = 4x-1$?

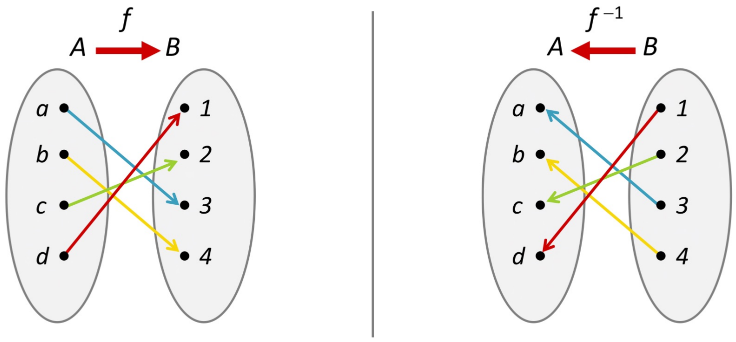


Let $y \in R$.

Calculate x with $f(x) = y$: $y = 4x-1 \Leftrightarrow (y+1)/4 = x$.

Hence $f^{-1}(y) = (y+1)/4$.

Find the inverse function of the following function:



domain swap to b
codomain now a

Let $f: A \to B$ be a one-to-one correspondence and $f^{-1}: B \to A$ its inverse.
Then $\forall b \in B\ \forall a \in A\ (f^{-1}(b) = a \Leftrightarrow b = f(a))$.

How to show inverse is bijective?

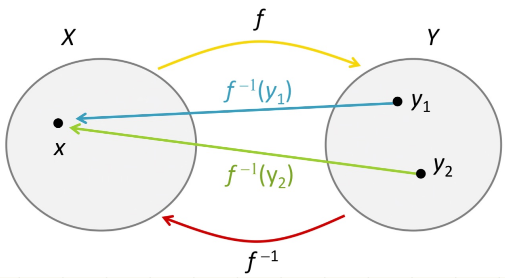
1

Theorem 1: If $f: X \to Y$ is a one-to-one correspondence, then $f^{-1}: Y \to X$ is a one-to-one correspondence.

Proof: f^{-1} is one-to-one

Take $y_1, y_2 \in Y$ such that $f^{-1}(y_1) = f^{-1}(y_2) = x$.

Then $f(x) = y_1$ and $f(x) = y_2$, thus $y_1 = y_2$.



→ Take y_1 & y_2

Assume not one to one

$f^{-1}(y_1) = x_1 \quad f^{-1}(y_2) = x_1$

$y_1 = f(x_1) \quad y_2 = f(x_1)$

$\therefore y_1 \neq y_2$, $\therefore$ One-one

2

Theorem 1: If $f: X \to Y$ is a one-to-one correspondence, then $f^{-1}: Y \to X$ is a one-to-one correspondence.

Take some x

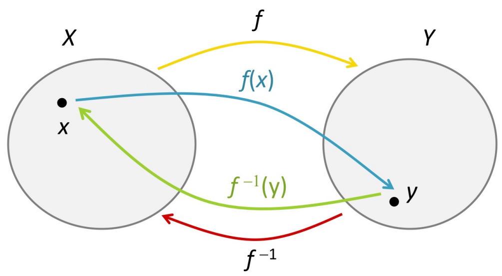
find $y = f(x)$

if $f^{-1}(y) = x$, is onto

Proof: f^{-1} is onto

Take some $x \in X$, and let $y = f(x)$.

Then $f^{-1}(y) = x$.

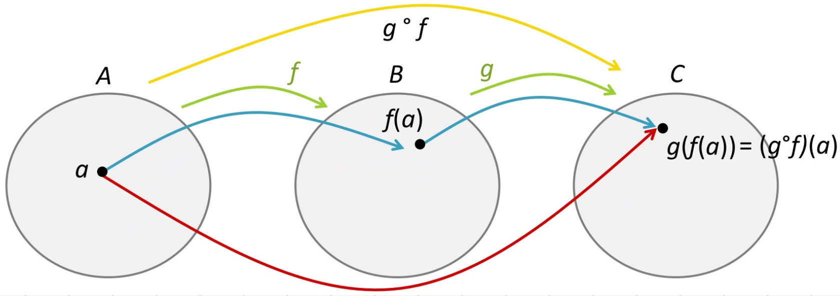


Composition

Composition and Properties: Composition of Functions

codomain of first must be domain of second

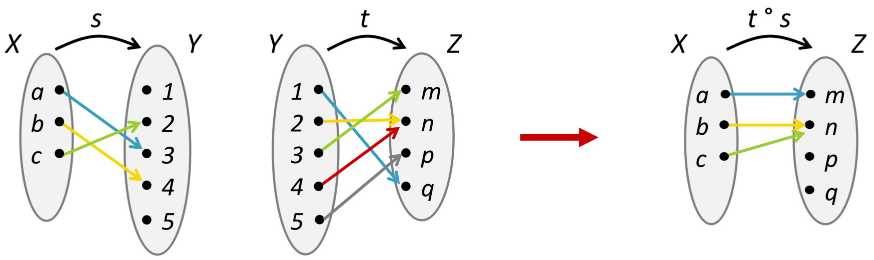
Let $f: A \to B$ and $g: B \to C$ be functions. The **composition** of the functions f and g, denoted as $g \circ f$, is defined by: $g \circ f: A \to C$, $(g \circ f)(a) = g(f(a))$.



Given functions $s: X \to Y$ and $t: Y \to Z$. Find $t \circ s$ and $s \circ t$.

$t \circ s$ is well defined

$s \circ t$ not well defined



$f: Z \to Z$, $f(n) = 2n + 3$, $g: Z \to Z$, $g(n) = 3n + 2$

What is $g \circ f$ and $f \circ g$?

$(f \circ g)(n) = f(g(n)) = f(3n + 2) = 2(3n + 2) + 3 = 6n + 7$

$(g \circ f)(n) = g(f(n)) = g(2n + 3) = 3(2n + 3) + 2 = 6n + 11$

$f \circ g \neq g \circ f$ (No **commutativity** for the composition of functions!)

Proving One-One for Composition

Theorem 2: Let $f: X \to Y$ and $g: Y \to Z$ be both one-to-one functions. Then $g \circ f$ is also one-to-one.

Proof: $\forall x_1, x_2 \in X\ ((g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow x_1 = x_2)$

Suppose $x_1, x_2 \in X$ with $(g \circ f)(x_1) = (g \circ f)(x_2)$.

Then $g(f(x_1)) = g(f(x_2))$.

Since g is one-to-one, it follows $f(x_1) = f(x_2)$.

Since f is one-to-one, it follows $x_1 = x_2$.

for any x_1 / x_2

if $(g \circ f)(x_1) = (g \circ f)(x_2)$

$x_1 = x_2$

Theorem 3: Let $f: X \to Y$ and $g: Y \to Z$ be both onto functions. Then $g \circ f$ is also onto.

Proof: $\forall z \in Z\ \exists x \in X$ such that $(g \circ f)(x) = z$

Let $z \in Z$.

Since g is onto, $\exists y \in Y$ with $g(y) = z$.

Since f is onto, $\exists x \in X$ with $f(x) = y$.

Hence, with $(g \circ f)(x) = g(f(x)) = g(y) = z$.

Floor / Ceiling

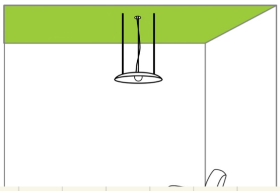
Ceiling and Floor: Definition

The **floor function** assigns to the real number x, the largest integer $\lfloor x \rfloor$ that is less than or equal to x. The **ceiling function** assigns to the real number x, the smallest integer $\lceil x \rceil$ that is greater than or equal to x.

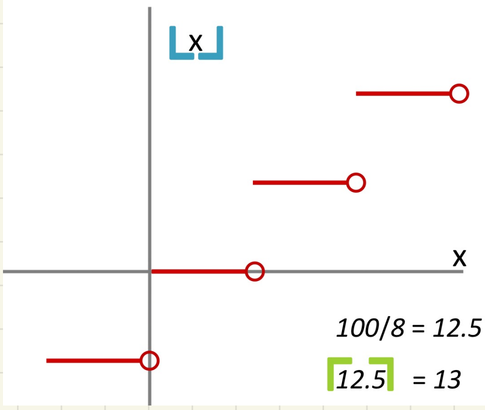
Example

$\lfloor ½ \rfloor = 0$ $\lceil ½ \rceil = 1$

$\lfloor -½ \rfloor = -1$ $\lceil -½ \rceil = 0$

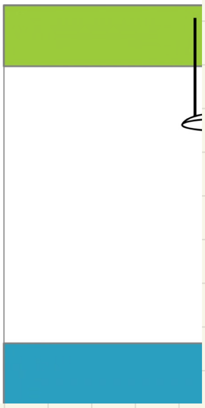


How many bytes are required to encode 100 bits of data?

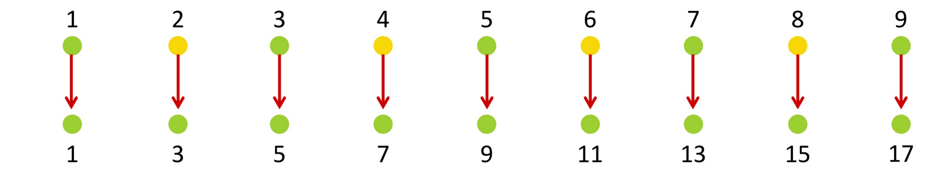


$100/8 = 12.5$

$\lceil 12.5 \rceil = 13$



A set that is either finite, or has the same cardinality as the set of positive integers is called **countable**.
A set that is not countable is called **uncountable**.

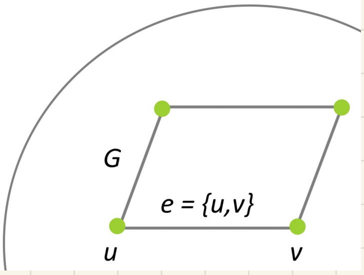


- $f(n)$ is one-to-one: suppose $f(n) = f(m)$, then $2n - 1 = 2m - 1$. Hence, $n = m$.
- $f(n)$ is onto: take m as an odd positive integer. Then m is less than an even integer $2k$ (k a natural number). Thus $m = 2k - 1 = f(k)$.

Graph

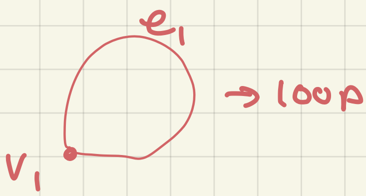
A **graph** $G = (V,E)$ is a structure consisting of a set V of vertices (nodes) and a set E of edges (lines joining vertices).

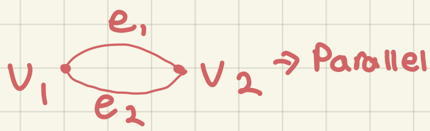
- Two vertices u and v are **adjacent** in G if $\{u,v\}$ is an edge of G.
- If $e = \{u,v\}$, the edge e is called **incident** with the vertices u and v.



Graphs are useful to represent data.

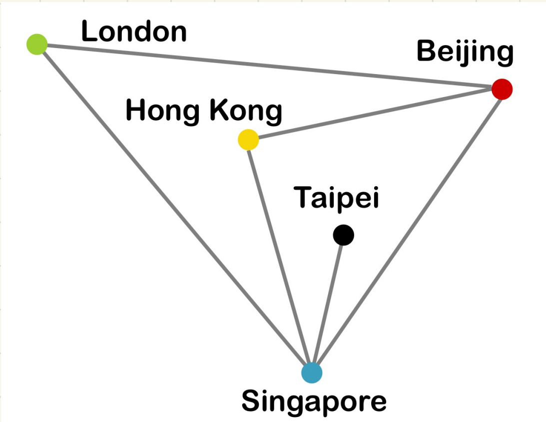
A **simple** graph is a graph that has no **loop** (= edge $\{u,v\}$ with $u = v$) and no parallel edges between any pair of vertices.





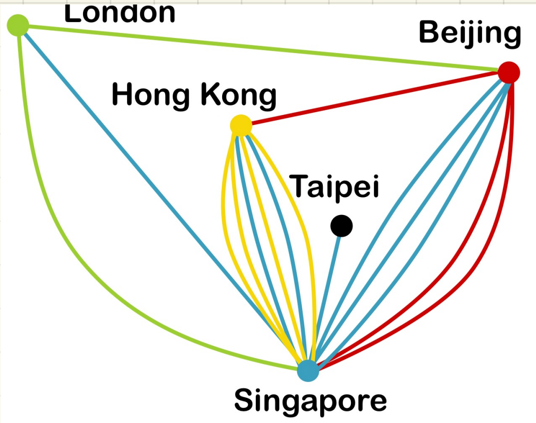
From\To	Hong Kong	Singapore	Beijing	Taipei	London
Hong Kong		4 Flights			
Singapore	2 Flights		3 Flights	1 Flight	1 Flight
Beijing	1 Flight	2 Flights			
Taipei					
London		1 Flight	1 Flight		1 Flight

Draw a graph to see whether there are direct flights between any two cities (in either direction).



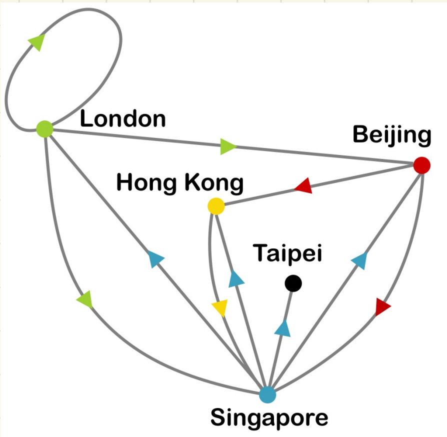
Simple

A **multigraph** is a graph that has no loop and at least 2 parallel edges between some pair of vertices.



multigraph

A **directed** graph is a graph where edges $\{u,v\}$ are ordered, that is, edges have a direction. Parallel edges are allowed in **directed multigraphs**. Loops are allowed for both.



directed multigraph

Euler Circuit: Definitions

A **Euler path** (Eulerian trail) is a walk on the edges of a graph which uses each edge in the original graph exactly once.

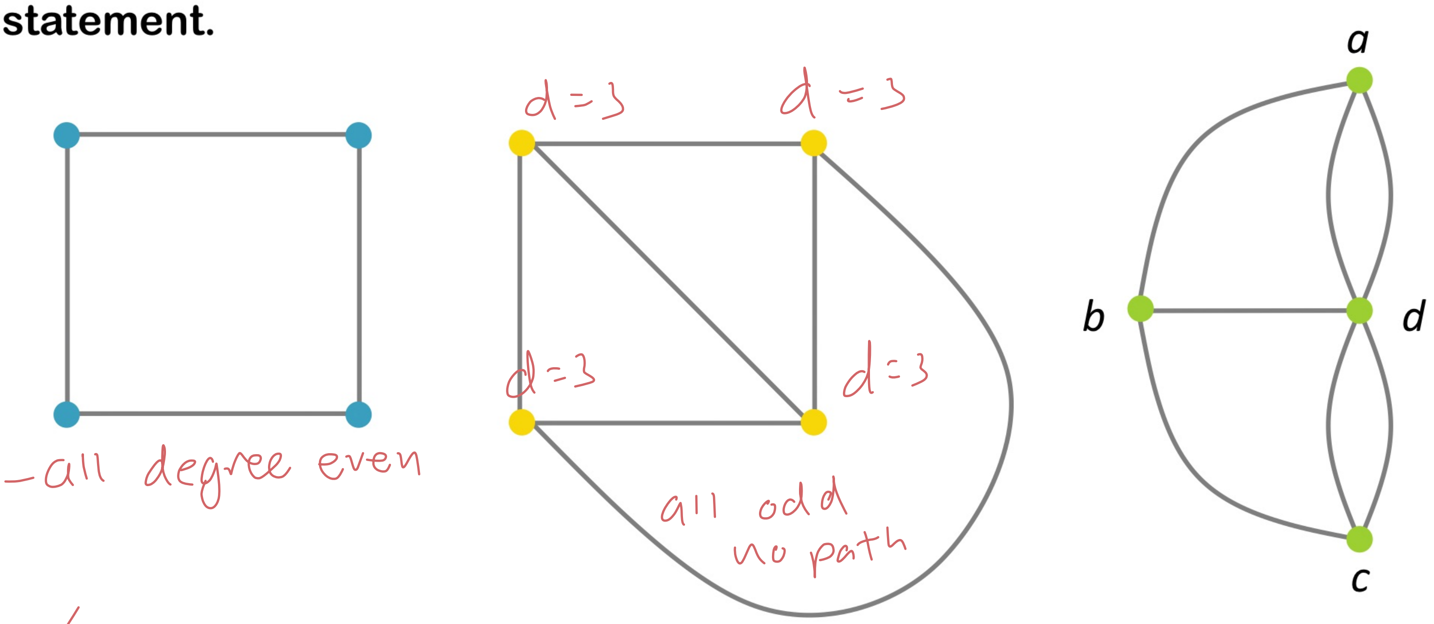
The beginning and end of the walk may or may not be the same vertex.

A **Euler circuit** (Eulerian cycle) is a walk on the edges of a graph which starts and ends at the same vertex, and uses each edge in the original graph exactly once.

If all node have odd degree, no path

- Suppose G has an Euler path, which starts at v and finishes at w.
- Add the edge $\{v,w\}$.
- Then by the first part of the theorem, all nodes have even degrees, except for v and w which have odd degrees.

Note: Euler Theorem actually states an "if and only if" statement.



✓ Euler Circuit | No Euler Path | No Euler Path

Theorem: consider a connected graph G.

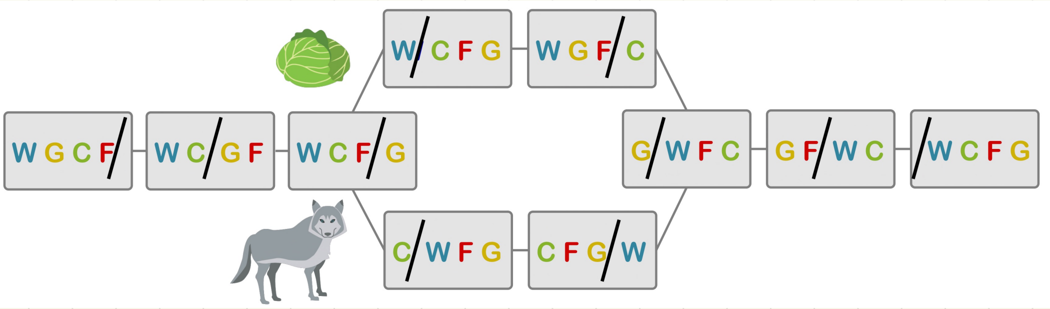
1. If G contains an Euler path that starts and ends at the same node, then all nodes of G have an even degree. → all even
2. If G contains an Euler path, then exactly two nodes of G have an odd degree. → only 2 odd

Graphs: Wolf, Goat and Cabbage

1. The ferryman takes the goat (no other choice)
2. The ferryman returns
3. Either he takes the cabbage or the wolf

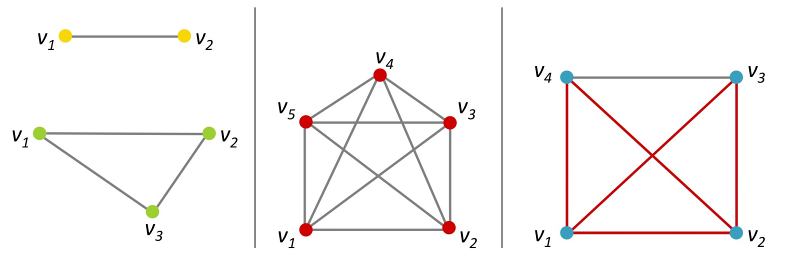
F = ferryman
G = goat
W = wolf
C = cabbage

4. Either he takes:
   a. The cabbage, brings back the goat, leaves the goat and takes the wolf across, returns, and takes the goat across.
   b. The wolf, brings back the goat, leaves the goat and takes the cabbage across, returns, and takes the goat across.



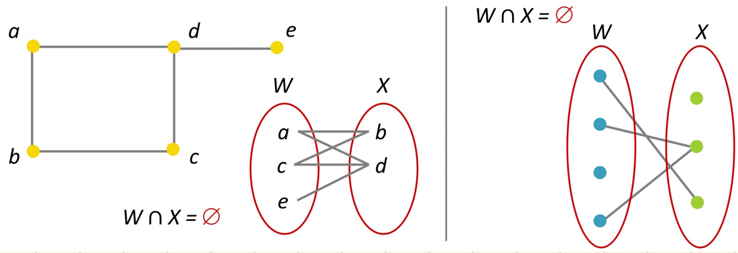
Complete

A **complete graph with n vertices** is a simple graph that has every vertex adjacent to every other distinct vertex.



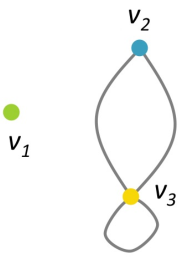
Bipartite

A **bipartite graph** is a graph whose vertices can be partitioned into 2 (disjoint) subsets W and X such that each edge connects a $w \in W$ and a $x \in X$.



Mode on Node Degree: Definitions

The **degree deg(v)** of a vertex v in an undirected graph is the number of edges incident with it (a loop at a vertex contributes twice). In-degree and out-degree are distinguished for directed graphs.



Total degree = $\deg(v_1) + \deg(v_2) + \deg(v_3) = 0 + 2 + 4 = 6$

The **total degree deg(G)** of an undirected graph G is the sum of the degrees of all the vertices of G: $\sum_{v \in V} \deg(v)$

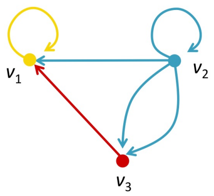
Then

$$\boxed{2e = \sum_{v \in V} \deg(v)}$$

→ One edge has to "hit" twice, always

Adjacent Matrix

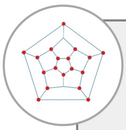
A graph can be represented by a matrix $A = (a_{ij})$ called **adjacency matrix**, with a_{ij} = the number of arrows from v_i to v_j.



$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$$

What is the adjacency matrix of a complete graph?

Hamiltonian Circuit: Definition

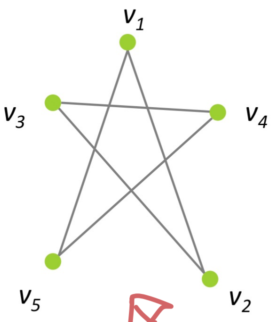


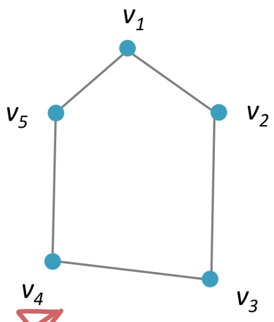
A **Hamiltonian path** of a graph *G* is a walk such that every vertex is visited exactly once.

A **Hamiltonian circuit** of a graph *G* is a closed walk such that every vertex is visited exactly once (except the same start/end vertex).

Graph Isomorphism: Pictorial Representations

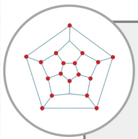
A graph can have many pictorial representations.





$$
\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}
\begin{array}{c}
\begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\
\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}
\end{array}
$$

Isomorphic

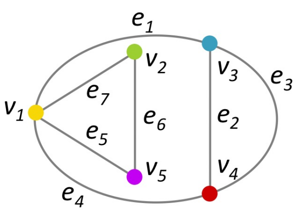


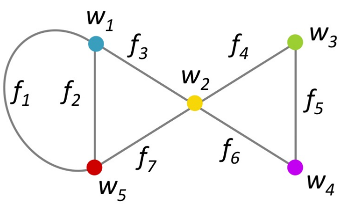
A graph $G = (V_G, E_G)$ **is isomorphic** to a graph $H = (V_H, E_H)$ if and only if there exists two bijections mapping the vertex sets and edge sets, respectively:

$g: V_G \to V_H$, $h: E_G \to E_H$

such that an edge $e \in E_G$ is incident on $v, w \in V_G \Leftrightarrow$ the edge $h(e) \in E_H$ is incident on $g(v), g(w) \in V_H$.

Graph Isomorphism: Example





Vertex and edge bijections:

$g = \{(v_1, w_2), (v_2, w_3), (v_3, w_1), (v_4, w_5), (v_5, w_4)\}$

$h = \{(e_1, f_3), (e_2, f_2), (e_3, f_1), (e_4, f_7), (e_5, f_6), (e_6, f_5), (e_7, f_4)\}$

mapping