Fatima Irfan

LANGUOSTYLE

Big O, complexity of code

- $O(n^2+3n-1)=n^2$

  meaning exists an integer m and a positive constant c such that for every $n \geq m$

  $|n^2+3n-1| \leq c|n^2|$

- Polynomials always have +ve integer exponents

Examples

$\sqrt{n}+3$ is not a polynomial

$\frac{n^2+1}{n+1}$ is not a polynomial

$\frac{1}{x^3}+2x$ is not a polynomial (because -3 is not positive)

$x^{\frac{3}{2}}+2x-1$ is not a polynomial (because $\frac{3}{2}$ is not an integer)

- Polynomials must be of the form:

  $f(n)=a_n n^{k_n}+a_{n-1}n^{k_{n-1}}+\ldots+a_1 n+a_0$

  where $a_n, a_{n-1}, \ldots, a_0$ are any real no.s and $(n^{k_n}, \ldots)$ must be positive whole no.s

- Degree – highest exponent of the polynomial
  For a function: $f(n)=5$
  degree of the function $=0$

- $O(\text{polynomial}) = n^{\text{degree of polynomial}}$

- $O(2n^5+7n^3-n+3)=n^5$. Explain
  at some value m for every $m \geqslant n$
  $|f(n)| \leqslant c|k(n)|$
  <u>meaning</u> exists m and fixed constant c
  such that for every $m \geqslant n$
  $|f(n)| \leqslant c|n^5| = cn^5$

- Mickey polynomial
  ↳ positive (no restriction on being a whole no.)
  e.g. $f(n) = 3n^{10/3} + 26n^{5/3} + \frac{2}{3}n^{32} + n^3 + 4$
  degree $= \frac{10}{3}$
  * every polynomial is a mickey polynomial

Properties of O

① $O(f_1(n) \cdot f_2(n)) = O(f_1(n)) \cdot O(f_2(n))$

② $O(f_1(n) \pm f_2(n)) = \max\{O(f_1(n), f_2(n))\}$

③ $O\left(\frac{f_1(n)}{f_2(n)}\right) = \frac{O(f_1(n))}{O(f_2(n))}$

Sum of arithmetic sequence: $\left(\frac{1^{st}\text{ term} + \text{Last term}}{2}\right) \times n$
no. of terms

For i=2 to (3n+1)
x=a*b+1
For k=1 to i
y= X÷3+b²−1
next k
next i

i) Find the exact number of computation that is executed by the code

no. of iterations in outer loop $=(3n+1)-2+1$
$=3n$ times

$\boxed{x = a \overset{1}{\circledast} b \overset{2}{\oplus} 1}$ no. of operations in outer loop $=2$

no. of iterations in inner loop $= i-1+1 = i$ times

no. of operations in inner loop $=4$

1st term

No. of operations in:

$i=$	Outer loop	Inner loop
2	2	$4i = 4 \times 2 = 8$
$3n+1$	2	$4(3n+1)$

Last term

Total # of operations

$$= 2(3n) + (3n)\left(\frac{8 + 4(3n+1)}{2}\right)$$

(ii) Find the complexity of code

$O(\text{code}) = n^2$

For $k=4$ to n^3-1

$S = k^3 * 10 + 3 * k + 7$ $\quad 2+1+1+1+1=6$

For $i=2$ to $2k+1$

$L = s^3 + i^2 - 3 * i + 2$ $\quad 2+1+1+1+1+1=7$

next i

next k

no. of iterations in outer loop $= (n^3-1) - 4 + 1$

$= n^3 - 4$ times

no. of operations in outer loop $= 6$

no. of iterations in inner loop $= (2k+1) - 2 + 1$

$= 2k$ times

no. of operations in inner loop $= 7$

~~no. of iterati~~

LANGUOSTYLE

No. of operations in:

$k=$	Outer loop	Inner loop
4	6	$14k = 14(4) = 56$
n^3-1	6	$14(n^3-1)$

Total no. of operations:

$$= 6(n^3-4) + \left(\frac{56 + 14(n^3-1)}{2}\right)(n^3-4)$$

$O(\text{code}) = n^6$

LANGUOSTYLE

Planet Z_n

Z_n integers module n, $n \geq 1$ (must be positive)

- $5 \bmod 3 = 2$ //meaning if we divide 5 by 3, the remainder is 2
- $10 \bmod 7 = 3$
- $-4 \bmod 3 = 2$ (Fundamental theorem in Number Theory)

Let a in $\mathbb{Z}$ (i.e a is an integer), $b>0$ (also an int) then exists unique integers q, r, such that

$$a = bq + r, \text{ where } 0 \leq r \leq b$$

- $-13 \bmod 5 = 2$

assume a is negative integer and b is positive, then if b is a factor of a, then

$$a \bmod b = 0$$

if b is not a factor of a, then

$$a \bmod b = b - ((-a) \bmod b)$$

e.g. $-7 \bmod 10 = 10 - (7 \bmod 10) = 10 - 7 = 3$

note:

if a is positive and b is positive and $b > a$ then $a \bmod b = a$

$-12 \bmod 17 = 17 - (12 \bmod 17) = 17 - 12 = 5$

LANGUOSTYLE

Rule: $a \bmod b + (-a \bmod b) = b$

$52 \bmod 9 = 7$, $-52 \bmod 9 = 9 - 7 = 2$

$7 + 2 = 9$

In these, operations can be addition and multiplication

Addition on Z_n is called addition mod n

Multiplication on Z_n is called multiplication mod n

Construct the ~~addition~~ multiplication mod 5 (in Z_5)

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Construct the ~~multiplication~~ addition mod 5 (in Z_5)

*	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Def $a \in \mathbb{Z}_n$ i.e a belongs in $\mathbb{Z}_n$, we say a is invertible if $a.\square = 1$ in $\mathbb{Z}_n$
called inverse of a

Is 3 invertible in $\mathbb{Z}_5$?

$3x = 1$ 	$3 \bmod 5 = 3$

$3 \times 2 = 6$ 	$6 \bmod 5 = 1$

then $x = 2$, 2 is the inverse of 3 or 3^{-1} in $\mathbb{Z}_5$

Is 3 invertible in $\mathbb{Z}_6$?

$3x = 1 \pmod 6$

$3 \bmod 6 = 3$
$6 \bmod 6 = 0$
$9 \bmod 6 = 3$

3 is not invertible in $\mathbb{Z}_6$ 	$12 \bmod 6 = 0$

Is 3 invertible in $\mathbb{Z}_8$?

$3x = 1 \pmod 8$ 	$3 \bmod 8 = 3$

$3^{-1} = 3$ 	$6 \bmod 8 = 6$

$9 \bmod 8 = 1$

$\gcd(a,b) = d$ is the biggest factor

$d \mid a$ - means d is a factor of a

$d \mid b$ - means d is a factor of b

If c exists such that $c \mid a$ & $c \mid b$, then $c \mid d$.

Number Theory - $ax = b$ in $\mathbb{Z}_n$, solve over planet $\mathbb{Z}_n$

$ax = b$ in $\mathbb{Z}_n$ has a solution iff $\gcd(a,n) \mid b$
&
# of all distinct solutions in $\mathbb{Z}_n = \gcd(a,n)$

Q. Is 23 invertible in $\mathbb{Z}_{32}$?

means $23x = 1 \pmod{32}$

$a = 23, b = 1, n = 32$

$\gcd(23, 32) = 1$, therefore it is invertible and $1 \mid 1$? Yes

Q. Solve over planet $\mathbb{Z}_{12}$, $4x = 6$

$a = 4, b = 6, n = 12$

$\gcd(4, 12) = 4$

Is $4 \mid 6$? No, hence no solution

$\gcd(4, 12) = -4$ is also correct

Solve over planet Z_{21}, $6x=9$

$\gcd(6,21)=3$

Is $3|9$? Yes

so $x_1=5$

To find other 2,

$d=\frac{n}{\gcd(a,n)}=\frac{21}{3}=7$

$5+7=12=x_2$

$12+7=19=x_3$

"26" = "5" in Z_{21}

$6 \bmod 21 = 6$

$12 \bmod 21 = 12$

$18 \bmod 21 = 18$

$24 \bmod 21 = 3$

$30 \bmod 21 = 9$

Solve $10x=5$ over Z_{15}

$\gcd(10,15)=5$

Is $5|15$? Yes

$x_1=2$

$d=\frac{15}{5}=3$

$x_2=5$, $x_3=8$, $x_4=11$, $x_5=14$

$10 \bmod 15 = 10$

$20 \bmod 15 = 5$

$30 \bmod 15 = 0$

$40 \bmod 15 = 10$

Solve over Z, $10x \equiv 5 \pmod{15}$

$10x \pmod{15} = 5$

First $10x=5$ in planet 15

set of solutions $=\{2+3k, k\in Z\}$

Solve over planet Z, $2x \pmod{10} = 7$

$2x = 7 \pmod{10}$

$\gcd(2,10)=2$ Is $2|7$? No, hence no solution

Solve over planet Z, $3x \pmod{10} = 2$

$\gcd(3,10)=1$ Is $1|10$? Yes

$x=4$

now, over Z, $d=\frac{10}{1}=10$

set of solutions: $\{4+10k, k\in Z\}$

$9 \bmod 10 = 9$

$12 \bmod 10 = 2$

* $a \in Z_n$, $a \neq 0$, a^{-1} exists iff $\gcd(a,n)=1$

e.g. 3^{-1} in Z_{10}, $\gcd(3,10)=1$, invertible

3^{-1} in Z_9, $\gcd(3,9)=3 \neq 1$, not invertible

Find all integers with the properties, say x,

$x \pmod 7 = 6$ $\qquad x \equiv 6 \pmod 7$

$x \pmod 4 = 2$ $\qquad x \equiv 2 \pmod 4$

$x \pmod 9 = 1$ $\qquad x \equiv 1 \pmod 9$

Chinese Remainder Theorem

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$\vdots$

$x \equiv a_K \pmod{n_K}$

Assume gcd(between every two distinct n_i's) = 1

Then the above system has a solution

In fact, over $\mathbb{Z}_{\underbrace{n_1 \cdot n_2 \cdot n_3 \cdots n_K}_{n_1 \times n_2 \times \cdots \times n_K}}$ the system has a unique solution gcd(every) = 1

← Question $\overbrace{n_1 \cdot n_2 \cdot n_3}= 7 \times 4 \times 9 = 252$

$a_1, a_2, a_3 = 6, 2, 1$

By CRT, the system has atleast one solution ~~because~~ however over $\mathbb{Z}_{252}$, the system has a unique solution.

$n_1 = 7 \quad n_2 = 4 \quad n_3 = 9$

$m_1 = \frac{n}{n_1} = 36 \quad m_2 = \frac{n}{n_2} = 63 \quad m_3 = 28$

Find $(m_1)^{-1}$ in $\mathbb{Z}_{n_1}$

$(36)^{-1}$ in $\mathbb{Z}_7 = 1^{-1}$ in $\mathbb{Z}_7 = 1$

Find $(m_2)^{-1}$ in $\mathbb{Z}_{n_2}$

$(63)^{-1}$ in $\mathbb{Z}_4 = 3^{-1}$ in $\mathbb{Z}_4 = 3$

Find $(m_3)^{-1}$ in $\mathbb{Z}_{n_3}$

$(28)^{-1}$ in $\mathbb{Z}_9 = 1^{-1}$ in $\mathbb{Z}_9 = 1$

The unique solution over planet $\mathbb{Z}_{252}$

$x = [a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + a_3 m_3 m_3^{-1}] \bmod 252$

$= [(6)(36)(1) + (2)(63)(3) + (1)(28)(1)] \bmod 252$

$= 118$

To find all solutions in $\mathbb{Z}$, $\{118 + 252k, k \in \mathbb{Z}\}$

Q. Find all integers with these properties

$x \equiv 3 \pmod 8$

$x \equiv 5 \pmod 7$

$x \equiv 7 \pmod{11}$, Is CRT applicable?

$n_1 = 8 \quad n_2 = 7 \quad n_3 = 11$

gcd(between every two n_i's) = 1, CRT is applicable

$m_1 = 77 \quad m_2 = 88 \quad m_3 = 56$

Find $(77)^{-1}$ in $\mathbb{Z}_8$	Find $(88)^{-1}$ in $\mathbb{Z}_7$	Find $(56)^{-1}$ in $\mathbb{Z}_{11}$
$(5)^{-1}$ in $\mathbb{Z}_8$	$(4)^{-1}$ in $\mathbb{Z}_7$	1^{-1} in $\mathbb{Z}_{11}$
$= 5$	$= 2$	$= 1$

$x = \big((3)(77)(5) + (5)(88)(2) + (7)(56)(1)\big) \bmod 616$

$= (579) \bmod 616$

Verify $579 \bmod 8 = 3$

$579 \bmod 7 = 5$

$579 \bmod 11 = 7$

gcd of big numbers

$82\overline{)216}$ → 2, -164, 52

$52\overline{)82}$ → 1, -52, 30

$30\overline{)52}$ → 1, -30, 22

$22\overline{)30}$ → 1, 22, 8

$8\overline{)22}$ → 2, -16, 6

$6\overline{)8}$ → 1, -6, 2

$2\overline{)6}$ → 3, -6, 0

For each of the numbers, gcd(#) = 2

Find gcd(32, 128)

$32\overline{)128}$ → 4, -128, 0

gcd = 32

Find gcd(32, 136)

$32\overline{)136}$ → 4, 128, 8

$8\overline{)32}$ → 4, -32, 0

gcd(32, 136) = 8

~~LCM~~

$30 = 16 \times 1 + 14$

gcd(16, 30) = gcd(16, 14)

gcd also has to be factor of 14

LCM[n, m] = k, k is the least positive integer when n|k and m|k

LCM[4, 12] = 48

$$\mathrm{LCM}[n,m] = \frac{nm}{\gcd(n,m)}$$

$$\mathrm{LCM}[82,216] = \frac{82 \times 216}{2} = 8856$$

gcd(32, 27) = c. Find two integers a, b s.t. $c = 32a + 27b$

$27\overline{)32}$ → 1, -27, 5

$5\overline{)27}$ → 5, -25, 2

$2\overline{)5}$ → 2, -4, 1

$1\overline{)2}$ → 2, -2, 0

$32 = 27.1 + 5$ $\qquad 5 = 32 - 27.1$

$27 = 5.5 + 2$ $\qquad 2 = 27 - 5.5$

$5 = 2.2 + 1$ $\qquad 1 = 5 - 2.2$

$1 = 5 - 2(27 - 5.5) = 5 - 2.27 + 10.5$

$= 11.5 - 2.27 = 11(32 - 27.1) - 2.27$

$= 11.32 - 27.11 - 27.2 = 11.32 - 27.13$

$b = -13,\ a = 11$

$\gcd(121, 38) = d$. Find a, b such that

$$d = 121a + 38b$$

$$38 \overline{)121}^{\,3} \quad 7\overline{)38}^{\,5} \quad 3\overline{)7}^{\,2} \quad 1\overline{)3}^{\,3}$$

$$\begin{array}{r} 121 \\ -114 \\ \hline 7 \end{array} \quad \begin{array}{r} 38 \\ -35 \\ \hline 3 \end{array} \quad \begin{array}{r} 7 \\ -6 \\ \hline 1 \end{array} \quad \begin{array}{r} 3 \\ -3 \\ \hline 0 \end{array}$$

$121 = 38.3 + 7 \qquad 7 = 121 - 38.3$

$38 = 7.5 + 3 \qquad 3 = 38 - 7.5$

$7 = 3.2 + 1 \qquad 1 = 7 - 3.2$

$1 = 7 - 2(38 - 7.5) = 7 - 2.38 + 10.7$

$= 11.7 - 2.38 = 11.(121 - 38.3) - 2.38$

$= 11.121 - 33.38 - 2.38 = 11.121 - 35.38$

$a = 11 \quad b = -35$

Numbers with different bases

digits of base $7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$\begin{array}{r} (2\,3\,5\,6)_8 \\ +(4\,2\,1\,7)_8 \\ \hline (6\,5\,7\,5)_8 \end{array} \qquad \begin{array}{r} (1\,1\,1\,1)_2 \\ +(0\,1\,0\,1)_2 \\ \hline (1\,0\,1\,0\,0)_2 \end{array}$$

Subtraction in base 8

$$\begin{array}{r} (2\,4\,1)_8 \\ -(1\,2\,7)_8 \\ \hline (1\,1\,2)_8 \end{array}$$

Q.

$$\begin{array}{r} (3\,2\,4)_5 \\ \times(\,\,3\,2)_5 \\ \hline 1\,2\,0\,3 \\ 2\,0\,3\,2\,+ \\ \hline (2\,2\,0\,2\,3)_5 \end{array}$$

Conversion from one base to another

Q. $(2\ 3\ 6)_8$ to Base 10

$2 \times 8^2 + 3 \times 8^1 + 3 \times 8^0 = 158_{10}$

Q. $(F\ 3\ A\ 1)_{16}$ to Base 10

$15 \times 16^3 + 3 \times 16^2 + 10 \times 16 + 1 \times 16^0 = (62369)_{10}$

Conversion from base 10 to another

9 to base 2

$9 = 2\,\boxed{} + r$

$9 = 2\,\boxed{4} + 1$

$4 = 2\,\boxed{2} + 0$

$2 = 2\,\boxed{1} + 0$

$1 = 2\,\boxed{0} + 1$

read backwards

$(1001)_2$

Convert 245 → base 8

$245 = 8\boxed{30} + 5$
$30 = 8\boxed{3} + 6$ $\quad 365_8$
$3 = 8\boxed{0} + 3$

Convert 378 to base 7

$378 = 7\boxed{54} + 0$
$54 = 7\boxed{7} + 5$
$7 = 7\boxed{1} + 0$ $\quad 1050_7$
$1 = 7\boxed{0} + 1$

Find all integers < 32 s.t. gcd (each integer & 32) = 2
(2, 6, 10, 14, 18, 22, 26, 30) = 8

Q. $n = 48.72$, find $\phi(n)$

Solution $n = 12.4 \cdot 8.9 = 2.2.3.2.2.2.2.2.2.3.3$
$= 2^7 . 3^3$

$\phi(n) = (2-1)2^6.(3-1) \cdot 3^2 = 1152$

meaning we have exactly 1152 positive integers such that gcd (between each & n) = 1

Q. $n = 7^9 . 5^3 11^4 . 3^{10}$
$= (7-1)7^8 (5-1)5^2 (11-1)11^3 (3-1)3^9$
$= 1.81 \times 10^{18}$

Q. $n = 12$ where gcd (between each & 12) = 1
$n = 2^2 . 3$
$\phi(n) = (2-1)2.(3-1) = 4$

Result: choose n positive integer, let $d|n$ then # of all positive integers below n where gcd (each, n) = d is $\phi\left(\frac{n}{d}\right)$

Q. $n = 32$ find all positive integers below 32 such that gcd (each integer, n) = 2
$\frac{32}{2} = 16$

$n = 2^4$
$\phi(n) = (2-1)2^3 = 8$

Q. $n = 108 = 3^2 . 2^2 . 3 = 3^3 . 2^2$
$\phi(n) = (3-1)3^2 . (2-1)2 = 36$

find $\phi(n)$ where gcd (each, 108) = 4
$\frac{108}{4} = 27 = 3^3 \quad \phi(n) = (3-1)3^2 = 18$

Q. $n = 55.100$. Find all positive integers s.t. gcd (each, n) = 5
$\frac{55}{5} . 100 = 11.100$
$= 11 . 5^2 . 2^2$

$\phi(n) = (11-1)(5-1)5(2-1)2 = 400$

<u>Fact</u> Let Q be a prime number

$\phi(Q) = Q-1$

<u>Euler format theorem</u>

n, m any positive integer such that gcd(n & m) = 1

$n^{k\phi(m)} (\text{mod } m) = 1$

or

$n^{\phi(m)} = 1 (\text{mod } m)$

Q. gcd(2, 105) = 1 n = 2 m = 105

$m = 105 = 5.21 = 5.7.3$

$\phi(m) = (5-1)(7-1)(3-1) = 48$

$2^{48} = 1 (\text{mod } 105)$

Q. Find $3^{12} (\text{mod } 13)$

n = 3 m = 13

$\phi(m) = 12$

$3^{12} (\text{mod } 13) = 1$

Q. Find $5^{15} (\text{mod } 13)$

n = 5 m = 13

$\phi(m) = 12$

$5^{12}.5^{3} (\text{mod } 13) = 5^{12} (\text{mod } 13) = 1$

$= 1.5^{3} (\text{mod } 13) = 8$

Q. Find $5^{128} (\text{mod } 13)$

n = 5 m = 13

$\phi(m) = 12$

$\frac{128}{12} = 10\frac{8}{12}$, $5^{10.12}.5^{8} (\text{mod } 13)$

$1.5^{8} (\text{mod } 13) = 1$

Q. n = 300.89

1) Find all integers 0 < n s.t gcd(each, n) = 1

$\phi(n) = 100.3.89 = 5^2.2^2.3.89$

$= (5-1)5(2-1)2.(3-1).(89-1)$

$= 7040$

2) Find all integers < n s.t gcd(each, n) = 3

$\frac{300.89}{3} = 100.89 = 5^2.2^2.89$

$\phi(n) = 5^2.2^2.89 = (5-1).5.(2-1)2.(89-1)$

$= 3520$

3) $7^{27} (\text{mod } 15)$

n = 7 m = 15

$m = 5.3$ $\phi(m) = (5-1).(3-1) = 8$

~~$7^{3.8}$ (mod~~ $\frac{27}{8} = 3\frac{3}{8}$

$7^{3.8}7^{3} (\text{mod } 15) = 1.7^{3} (\text{mod } 15)$

$= 13$

Boolean Algebra

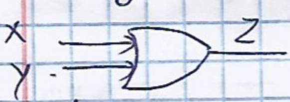
V – OR (+)
Λ – AND (*)

```
   1 0 1
 + 0 1 1
 -------
   1 1 1  → In Boolean Algebra, not in binary
 -------
```

logic
1 → True
0 – False

In Boolean Algebra, + here means OR not addition

OR gate

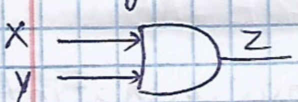


x and y are binary sequence ~~both~~

x	y	(x + y)
1	1	1
1	0	1
0	1	1
0	0	0

(x OR y)(x V y)

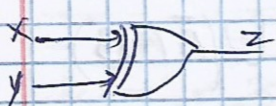
AND gate



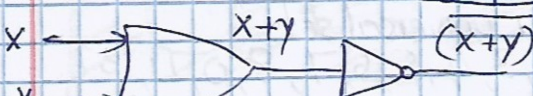
x	y	(x * y)
1	1	1
1	0	0
0	1	0
0	0	0

(x AND y)(x Λ y)

Exclusive OR (XOR)



x	y	$x \oplus y$
1	1	0
1	0	1
0	1	1
0	0	0



$A=\{2,3,4\}$ In a set,
↳ repitition not allowed, order not important

* $|A|$ = cardinality of A = number of elements in set

$|A|=3$

$B=\{4,5,7,2,3\}$

* $A\cup B=\{2,3,4,5,7\}$ (no repitition)

Union

* $A\cap B=\{\underbrace{2,3,4}_{\text{basically } A}\}=B\cap A$

intersection - elements that are in A and in B.
(common elements)

* $B-A=\{$elements in B that are not in A$\}$
$=\{5,7\}$

* $A-B=\{\ \}=\phi$ (empty set)

* $A\uplus B$ exclusive union

different from $\cup$

$$A\uplus B=(A\cap\bar{B})\cup(\bar{A}\cap B)$$

Assume W is our universal set
$W=\{2,3,4,5,6,7,8,0,11,13\}$

A "lives" in W

$A = \{2, 3, 4\} \rightarrow$ in W

and

B also "lives" in W

each element of A is an element of W

* $\bar{A} = W - A$

↳ also means (all elements in W not in A)

$\bar{A} = \{5, 6, 7, 8, 0, 11, 13\}$

$\bar{B} = W - B = \{6, 0, 11, 13, 8\}$ = (elements in universal set not in B)

- 11111

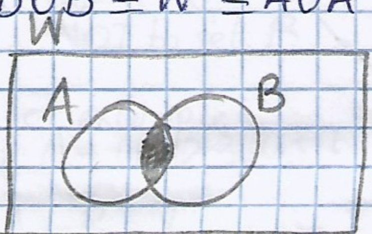
$x = 01011$ In Boolean

$\bar{x} = 10100$ $x + \bar{x}$ = always gives string of 1s

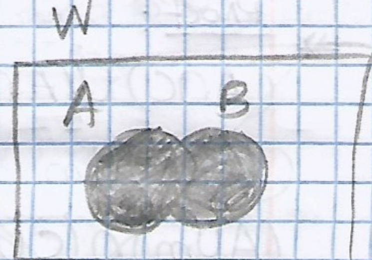
$x + \bar{x} = 11111$

- $B \cup \bar{B} = W = A \cup \bar{A}$

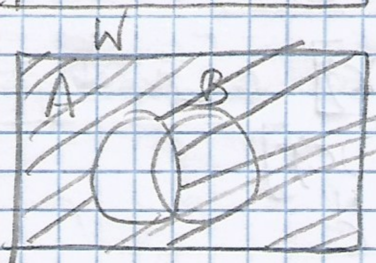
$A \cap B$



$A \cup B$



$\bar{A}$



$\vee$ — +

$\wedge$ — ·

x

Sets	Boolean Algebra
$\cup$	$+ (\vee)$
$\cap$	$\cdot (\wedge)$
$\uplus$	$\oplus$

exclusive union

Properties of set	Properties of Boolean Algebra
$(A\cap B)\cup C = (A\cup C)\cap(B\cup C)$	$AB + C$ $(A+C)(B+C)$
$(A\cup B)\cap C = (A\cap C)\cup(B\cap C)$	$(A+B).C = AC + BC$ $\boxed{\text{can prove results by truth table}}$
$(A\cap C)\cup(\bar{A}\cap C) = C$	$AC + \bar{A}C = C$
$A\uplus B = (\bar{A}\cap B)\cup(A\cap\bar{B})$	$A\oplus B = \bar{A}B + A\bar{B}$

Proof:

$(A\cap C)\cup\underbrace{(\bar{A}\cap C)}_{m}$

$(A\cap C)\cup m$

$(A\cup m)\cap(C\cup m)$

$[A\cup(\bar{A}\cap C)]\cap[C\cup(\bar{A}\cap C)]$

$[(A\cup\bar{A})\cap(A\cup C)]\cap[(C\cup\bar{A})\cap\underbrace{(C\cup C)}_{=C}]$

$= (A\cup C)\cap[(C\cup\bar{A})\cap C]$

$A \quad \cap[(C\cap C)\cup(\bar{A}\cap C)]$

Intersection of Sets

The intersection of sets A and B, denoted as $A \cap B$, is the set of elements common to both A AND B

For example:-

$A = \{1, 2, 3, 4, 5\}$ $B = \{2, 4, 6, 8, 10\}$

$A \cap B = \{2, 4\}$

Union of sets

The union of sets A and B, written as $A \cup B$, is the set of elements that appear in A OR B

For example:-

$A = \{1, 2, 3, 4, 5\}$ $B = \{2, 4, 6, 8, 10\}$

$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$

Difference of sets

The difference of sets A and B, written as $A - B$ is the set of elements belonging to set A and NOT to set B.

For example:

$A = \{1, 2, 3, 4, 5\}$ $B = \{2, 3, 5\}$

$A - B = \{1, 4\}$.

<u>NOTE</u>: $A - B \neq B - A$

$A = \{\phi, \{2\}, 2, 5, \{2,5\}, 30, a, \frac{1}{2}\}$

$|A| = n(A) = 8$

cardinality

T or F

- $\{2\} \in A$ T (set $\{2\}$ is an element of A)
- $\{2\} \subseteq A$ T, because 2 is an element of A

stare

$\boxed{\text{subset}}$

For $\subseteq$, start with $\{\ \}$

- If $A = \{\phi, \{2\}, 5, \{2,5\}, 30, A, \frac{1}{2}\}$ then,

  $\{2\} \subseteq A$ F (because 2 is not an element of A but $\{2\}$ is an element)

In general, $B \subseteq A$ this means each element in B is an element of A

- $\{5\} \subseteq A$ T
- $\{5, \{A\}\} \subseteq A$ F (because $\{A\}$ is not an element of A)

By default, $\{\} =$ empty set / $\boxed{\phi \subseteq \text{ of any set}}$

- $\phi \in A$ T (not by default, it is actually there)
- $\phi \subseteq A$ T (by default)
- $\{\phi\} \subseteq A$ T (not by default)

- $30 \in A$ T
- $\{30\} \subseteq A$ T
- $\{2,5\} \subseteq A$ T (because $2 \in A$ & $5 \in A$)

Powerset

Q. $A = \{1, 2, \{5\}\}$

Find all elements of $\wp(A)$ (powerset of A)

$\wp(A) = \{$each element is a subset of A$\}$ = set of all subsets of A

$= \{\phi, A, \{\{5\}\}, \{1\}, \{2\}, \{1,2\}, \{1,\{5\}\}, \{2,\{5\}\}\}$

- each subset of $A \in \wp(A)$

T, F

Q $2 \in \wp(A)$ F

$2 \in A$ T

$\{1,2\} \in \wp(A)$ T

$\{1,2\} \subseteq A$ T

$\{1\} \in \wp(A)$ T

$\{\{1\}, \{2,5\}\} \subseteq \wp(A)$ T

$\phi \in A$ F

$\phi \subseteq A$ T (by default)

$\{\phi\} \in \wp(A)$ F

$\phi \in \wp(A)$ T

$\wp(A) = \{\phi, A, \{1\}, \{2\}, \{\{5\}\}, \{1,2\}, \{2,\{5\}\}, \{1,\{5\}\}\}$

$\phi \subseteq \wp(A)$ T (by default)

Result: A is a set with n elements
then $|\wp(A)| = 2^n$ $= n(\wp(A))$ cardinality of $\wp(A)$

Extra questions
$A = \{3, x, 4, \{x, 2\}, 7, 2\}$

$\subset \rightarrow$ compare between 2 sets (subsets)

$\in \rightarrow$ between element and a set (belong)

$x \in A$ T "x belongs to A"
"x is an element of A"

$\{x, 2\} \in A$ T "$\{x, 2\}$ is an element of A"

$7 \in A$ T "7 is an element of A"

$\{4, x\} \subseteq A$ T "set of 2 elements, 4 and x, is a subset of A"

Eg. $A = \{\{3, 2\}, x, \{x\}, 3, 2, \phi\}$

$\{x\} \in A$ T "$\{x\}$ is an element of A. Things on the left must be exactly inside A

$\phi \in A$ T "ϕ is an element of A"

$\{2, x\} \in A$ "$\{2, x\}$ does not exist as a set in A"

by default
$\boxed{\phi \text{ is } \subseteq \text{any set}}$

$\{2,3\} \in A$ T "$\{2,3\}$ exists exactly as a set in A"

$\{2,3\} \subseteq A$ T "elements 2 and 3 exist in A"

$\{\{3,2\}, 3, 2\} \subset A$

$\{3,2\} \in A$ ✓
$2 \in A$ ✓
$3 \in A$ ✓

$\underline{\underline{T}}$

$\{\phi, 2\} \subset A$ T, ϕ and 2 are elements of A

e.g. ~~AccC~~ $A = \{2, 3, \{5\}, 7, \{5,2\}\}$

$B = \{5, 2, \{3,7\}, \phi\}$

$A \cup B$ (union) $\rightarrow$ similar to OR $\vee$

$A \cap B$ (intersection) $\rightarrow$ similar to AND $\wedge$

$A \cup B = \{2, 3, \{5\}, 7, \{5,2\}, 5, \{3,7\}, \phi\}$

$A \cap B = \{2\}$

$A - B$ = elements of A not in B

$= \{3, \{5\}, 7, \{5,2\}\}$

$B - A$ = elements of B not in A

$= \{5, \{3,7\}, \phi\}$

$B - A \neq A - B$

Universal set

Assume $U = \{2, 3, \{5\}, 7, \{5, 2\}, 5, \{3, 7\}, \phi, Z,$
$\{\theta, 2\}, \{7, Z\}, 22, 0\}$

$\bar{A} = U - A$

$A = \{2, 3, \{5\}, 7, \{5, 2\}\}$

$A = \{5, \{3, 7\}, \phi, Z, \{\theta, 2\}, \{7, Z\}, 22, 0\}$

$\{\theta, 2\} \in U$ T

$\{\theta, 2\} \subseteq U$ T

$\{\{5, 2\}\} \in U$ T

$\{\{5, 2\}\} \subseteq U$ T

---

iii) Let $A = \{0, \{0, y\}, y, \{6\}, x, \phi\}$

$B = \{\{0\}, \{\phi\}, \{6\}, \{6, x\}, 6, y, 23, 10,$
$\{\{0\}, \{6, x\}\}\}$

Write T or F

a) $\{\{0\}, \{6, x\}\} \in B$ T

b) $\{\{0\}, \{6, x\}\} \cancel{\in} \subseteq B$ T

c) $\{\phi\} \in A$ ~~T~~ F

d) $\{\phi\} \in B$ T

e) $\{\phi\} \subset B$ F

f) $\{\phi\} \subseteq A$ T

g) $\phi \in A$ T

h) $\{23, 10, y\} \in B$ F

i) $\{23, 10, y\} \subseteq B$ T

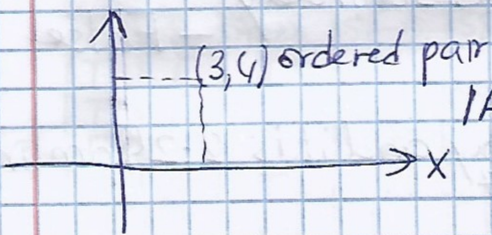
j) $\{6\} \in (A \cap B)$ T

k) $\{6\} \subseteq (A \cap B)$ F

l) Find $A \cap B = \{\{6\}, y, \phi\}$

m) Find $B - A = \{\{0\}, \{\phi\}, \{6, x\}, \emptyset, 23, 10, \{\{0\}, \{6, x\}\}\}$

A is a set



$|A| = A \times B = \{(a, b) \mid a \in A, b \in B\}$

x-y plane

Quantifier

Q. Convince me that $\underbrace{(x+y)z}_{\text{3 variables}} = xz + yz$

\# of possibilities $= 2^3 = 8$

$(x \vee y) \wedge z$

x	y	z	$(x+y)z$	$xz+yz$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	0	0
0	1	1	1	1
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

Logic OR and AND

Logical statements

- Today is Wednesday or Tomorrow is Saturday — False

$S1 \vee S2 = F$

Today is Thursday and it is 2:24pm in NAB007

$S1 \wedge S2 = T$

- If S_1, then S_2

- If $\underbrace{\boxed{\text{today is Friday}}}_{S_1}$, then $\underbrace{\boxed{3^2 = 20.23}}_{S_2}$ — True

$S_1 \Rightarrow S_2$

implies if S_1, then S_2

S_1	S_2	$S_1 \Rightarrow S_2$
T	T	T
T	F	F
F	T	T
F	F	T

Linear Sequence (linear recurrence)

Q $a_n = 5a_{n-1} - 6a_{n-2} +$

$a_0 = 3 \quad a_1 = 5$ Find a general formula for a_n

$\{a_n\}_0^{+\infty} = 5a_{n-1} - 6a_{n-2}$

$a_n = 5a_{n-1} - 6a_{n-2}$

$x^n = 5x^{n-1} - 6x^{n-2}$

$x^2 = 5x - 6$

$x^2 - 5x + 6 = 0$

$(x-3)(x-2) = 0$

$x = 3, \ x = 2$

We find a general formula for the undetermined

$a_n = c_1(2)^n + c_2(3)^n$, find c_1, c_2

$a_2 =$

$b_2 =$

$b_2 =$

Q. $a_n = -6a_{n-1} - 9a_{n-2}$, for every $n \geq 2$
$a_0 = 2 \quad a_1 = 10$

$a_2 = -6(10) - 9(2) = -78$

$a_3 = -6(-78) - 9(10) =$

Find a general form for a_n

$x^n = -6x^{n-1} - 9x^{n-2}$

$x^2 = -6x - 9$
$x^2 + 6x + 9 = 0$
$(x+3)(x+3) = 0$
$x = -3 \quad x = -3$ repeated twice

$a_n = c_1(-3)^n + c_2 n(-3)^n$

$a_0 = 2$
$c_1 = 2$
$a_1 = 10$
$10 = c_1(-3) - 3c_2$
$-6 - 3c_2 = 10$
$c_2 = \frac{-16}{3}$

$a_n = 2(-3)^n - \frac{16}{3} n(-3)^n$

Suppose $a_n = 4a_{n-1} - 3a_{n-2}$, $a_1 = 2$
Find a formula for a_n $\quad a_2 = 10$

$x^n = 4x^{n-1} - 3x^{n-2}$
$x^2 = 4x - 3$
$x^2 - 4x + 3 = 0$
$(x-3)(x-1) = 0$
$x = 3 \quad x = 1$

$a_n = c_1(3)^n + c_2(1)^n \qquad 3c_1 + c_2 = 2$
$9c_1 + c_2 = 10 \qquad c_2 = 2 - 3c_1$
$c_2 = 10 - 9c_1$
$2 - 3c_1 = 10 - 9c_1$
$6c_1 = 8$
$c_1 = \cancel{1.5}\,\frac{4}{3} \qquad c_2 = -2$

$a_n = -2 + \frac{4}{3}(3)^n$

Suppose $\{a_n\}_{n=0}^{\infty}$, $a_n = 2a_{n-2} - a_{n-1}$
$a_0 = 2$ and $a_1 = 7$

Find a general formula for a_n

$a_n = 2a_{n-2} - a_{n-1}$
$x^n = 2x^{n-2} - x^{n-1}$
$x^2 = 2 - x$
$x^2 + x - 2 = 0$
$\cancel{x^2 - x = x - 2 = 0} \quad x^2 - x + 2x - 2 = 0$
$\cancel{x(x-1) - 1(x+2) = 0} \quad x(x-1) + 2(x-1) = 0$
$(x+2)(x-1) = 0$
$x = -2, 1$
$a_n = c_1(-2)^n + c_2(1)^n$

[illegible]

[illegible]

ar[illegible]

Quantifiers (logic)

$\mathbb{N}$ = set of all integers ≥ 0

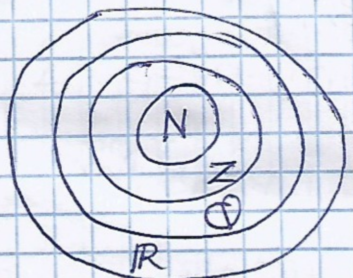
$\mathbb{Z}$ = set of all integers (including zero)

$\mathbb{Q}$ = set of all rational numbers

* rational number means $\frac{a}{b}$, $a, b \in \mathbb{Z}$

π is an approximation (irrational number)

$\mathbb{R}$ – set of all real numbers



A = set of numbers
$A^* = A - \{0\}$

$\mathbb{R}^*$ – all real numbers exc

$\mathbb{Q}^*$ – all rational numbers except 0

$\mathbb{N}^* = \mathbb{N} - \{0\}$ (set of all integers ≥ 1)

OR

$\exists \rightarrow$ exists / there exists
$\exists! \rightarrow$ exists unique
$\forall \rightarrow$ for all

T or F

- $\exists!\ x \in \mathbb{Q}$ s.t $\cancel{xy=}$ $x + y = y$ $\forall y \in \mathbb{Q}$ T

$\underline{\underline{x = 0}}$

- $\exists x \in \mathbb{Q}$ s.t. $x + y = y$ $\forall y \in \mathbb{Q}$ T

- If $\boxed{\exists x \in \mathbb{R} \text{ s.t } x^2+1=0}$ F, then $\boxed{y^2+2=e^3 \text{ for some } y \in \mathbb{R}}$ T

$S_1 \to F \quad S_2 \to T \quad S_1 \to S_2$ is T

- $\forall x \in \mathbb{R} \; \exists y \in \mathbb{R}$ s.t $x+y=0$ T

(for real numbers there exist real number where $x+y=0$)

- $\exists y \in \mathbb{R}$ s.t $\forall x \in \mathbb{R}$ we have $x+y=0$ F

(for any y we add x, we get 0)

- $\exists! \, x \in \mathbb{N}^*$ s.t. $x^2-3x=0$ T

$x(x-3)=0$

$x=0, x=3$

Because $x=0$ is not in $\mathbb{N}^*$ and only $x=3$ is a solution

- $\exists! \, x \in \mathbb{N}$ s.t. $x^2-3x=0$ F

- $\forall \underbrace{x \in \mathbb{R}}_{\text{could be } 0} \; \exists y \in \mathbb{R}$ s.t $xy=1$ F

$\downarrow$

$\forall x \in \mathbb{R}^* \; \exists y \in \mathbb{R}$ s.t $xy=1$ T

Equivalence relation & Partial order

Equivalence relation – we define what the normal "="

Def Let A be a set.
Define "=" on A, s.t.

1) (a–a) {symmetric}
$\forall a \in A$, a"="a

2) ($a \Leftrightarrow b$) {reflexive}
whenever a"="b for some $a,b \in A$,
then b"="a

3) (a–b–c) {transitive}
whenever a"="b and b"="c for some $a,b,c \in A$
then a"="c

Ex $A=\mathbb{Z}$, define "=" on Z s.t. $\forall a,b \in \mathbb{Z}$,
a"="b iff a(mod 5) = b(mod 5)
here, the normal equal

1)(a–a): Let $d \in \mathbb{Z}$. Is it true that
d(mod 5) = d(mod 5)?
Yes, hence 1st axiom hold

2)($a \Leftrightarrow b$): Assume a"="b for some $a,b \in A$,
show that b"="a.

a(mod 5) = b(mod 5)
this implies b(mod 5) = a(mod 5), then b"="a

3)(a–b–c): Assume a"="b & b"="c for some
$a,b,c \in \mathbb{Z}$
a(mod 5) = b(mod 5)
and b(mod 5) = c(mod 5),
hence a(mod 5) = c(mod 5) ⇒ implies a"="c

Find all equivalence classes for above.
$a \in \mathbb{Z}$, $[a] = \bar{a}$ = set of all elements of [a] that are equal ("=") to a

$[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$

→ try: 3"="−12 : 3(mod 5) = 3
−12(mod 5) = 5 − 2 = 3

3"="8 : 3(mod 5) = 3
8(mod 5) = 3

*note: [8] would be same as [3], [13], ...

$[0] = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$
$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$
other classes can be $\{1, 2\}$

Know: Assume "=" is an equivalence relation

1) Intersection of every two distinct equivalence classes $= \phi$

e.g. (above) $[3] \cap [4] = \phi$

2) Union of all equivalence classes $= A$

$[0] \cup [1] \cup [2] \cup [3] \cup [4] = Z$

Q. $A = \{1,2,3\}$ $B = \{-1,2,3\}$

Find $A \times B$ and $|A \times B|$

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

$|A \times B| = 9$ (by counting) &

$|A| = 3$ & $|B| = 3$ $3 \times 3 = 9$

Q. $A = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$B = \{0,4,8\}$

Define "=" on A s.t. $\forall a,b$ in A

a"="b if $(a-b) \bmod 12 \in B$

Given that this is an equivalence relation

1) Find all equivalence classes

2) View "=" as a subset of $A \times B$, how many elements does "=" have?

1. 8"="4 $(8-4) \bmod 12 = 4$ & $4 \in B$ ✓

4"="8 $(4-8) \bmod 12 = -4 \bmod 12$

$= 12-8 = 4$ & $4 \in B$ ✓

2. 5"="1 $(5-1) \bmod 12 = 4$ & $4 \in B$ ✓

1"="5 $(1-5) \bmod 12 = -4 \bmod 12$

$= 4$ & $4 \in B$

1) $[0] = \{0,4,8\}$

(by $0-0 \bmod 12 = 0 \in B$

$0-4 \bmod 12 = 4 \in B$

$0-8 \bmod 12 = 8 \in B$)

$[1] = \{1,5,9\}$

$[2] = \{2,6,10\}$

$[3] = \{3,7,11\}$

$([0] \cup [1] \cup [2] \cup [3] = A)$

2) $A \times A = \{(a,b) \mid a,b \in A\}$

$|A \times A| = 12^2 = 144$

"=" $\{(0,0),(4,4),(8,8),(1,1),(5,5),(9,9),(2,2),(6,6),(10,10),(3,3),(7,7),(11,11),(0,4),(4,0),(0,8),(8,0),(4,8),(8,4),(1,5),(5,1),(1,9),(9,1),(5,9),(9,5),(2,6),(6,2),(2,10),(10,2),(6,10),(10,6),(3,7),(7,3),(3,11),(11,3),(7,11),(11,7)\}$.

by counting, # of elements in "=" = 36

[0]=3 [2]=3

[1]=3 [3]=3

# of elements in "=": $3^2+3^2+3^2+3^2=36$

* note: if you remove one pair (2,6) from "=", would it be a set of "="?

No, because 2^{nd} axiom would fail, 2"="6 & 6"="2 should be there

Is 3"="7?
Is (3,7) ∈ "="?
} both mean same thing

Yes

Q. A={1,2,4} B={(1,2),(2,1),(2,4),(4,2),(1,4),(4,1)}

- Is B ⊆ A×A?

Yes, B has relations for 2^{nd} axiom

- Can we view this (B) as an equivalence relation on A?

No, doesn't contain {(1,1),(2,2),(4,4)}

* note: not every subset is an equivalence relation

• An equivalence relation on A can be viewed ~~on~~ as subset of A×A, but not every subset of A×A is an equivalence relation.

Q. M={1,2,3}, B={(1,1),(2,2),(3,3)}

Can we view B as an equivalence relation on M?

Yes.

Q. If M=normal equal then B={(1,1),(2,2),(3,3)}

because

[1]={1}

[2]={2}

[3]={3}

Q. If M={1,2,3}, B={(1,1),(2,2),(3,3),(1,3)}

Can we view B as an equivalence relation on M?

No, since we have (1,3) we should have (3,1)

Q. M={1,2,3}, B={(1,1),(2,2),(3,3),(1,3),(3,1)}

Whenever we have a"="b, we should have b"="a, hence it is an equivalence relation.

Equivalence classes: [1]={1,3}

[2]={2}

Partial order = A relation "$\leq$" on A is a partial order iff,

1) symmetric (a-a) : $\forall a \in A$, a"$\leq$"a

~~a"$\leq$"a since a=a~~

2) anti-reflexive : whenever a and b are distinct and a"$\leq$"b, then b"$\nleq$"a

3) transitive (a-b-c) : whenever a"$\leq$"b and b"$\leq$"~~a~~c, then a"$\leq$"c

Q. ~~A=N*~~ Define "$\leq$" on Z such that $\forall a,b \in Z$, a"$\leq$"b iff $a|b$ i.e ($b=ca$ for some ~~$c \in N^*$~~) $c \in Z$

1) symmetric : every integer is a factor of itself $c \in Z$

2) antireflexive :

~~5"$\leq$"7~~ 5 $\quad 2|-2 \quad$ 2 is a factor of -2

$-2=2(-1) \quad c=-1 \in Z$

and $-2|2 \quad$ -2 is a factor of 2

$2=-2(1) \quad c=1 \in Z$

-1 is in Z, whenever you have both reflexive, you cannot have partial order.

FIX: $b=ca$ for some N^*, then

$2|-2 \quad -2=2(-1)$ but $c=-1 \notin N^*$

then it becomes anti-reflexive

Q. $A=\{1,2,5\}$, we have $B=\{(1,1),(2,2),(5,5),(1,5),(2,5)\}$

Is B a partial order on A?

Yes, first axiom works, second axiom & third axiom hold

- (1,5) present and not (5,1) hence 2nd axiom hold
  (2,5) present and not (5,2) hence 2nd axiom hold
- $(a,b) \ (b,c) \Rightarrow (a,c)$ ← 3rd axiom

Q. $L=\{2,4,10,7\}$

$B=\{(2,2),(4,4),(10,10),(7,7),(2,4),(4,10),(10,7)\}$

Is B a partial order on L?

No, first axiom hold, second axiom hold (no reflexive), third axiom not hold

(2,4),(4,10), which means you should have (2,10)

(4,10),(10,7), and (4,7)

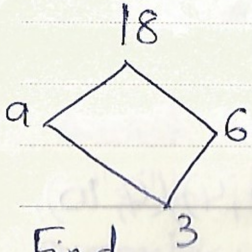
LANGUOSTYLE

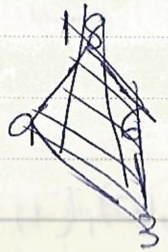
Q. $A=\{3,6,9,18\}$

"$\leq$" defined on A s.t. $\forall a,b \in A$, a"$\leq$"b iff $a|b$ in $\mathbb{N}^*$ ($b=ac$ for some $c\in \mathbb{N}^*$)

Then "$\leq$" is a partial order on A

3"$\leq$"6	$6=3c$ $c=2$	6"$\leq$"18	$18=6c$ $c=3$
3"$\leq$"9	$9=3c$ $c=3$	9"$\leq$"18	$18=9c$ $c=2$
3"$\leq$"18	$18=3c$ $c=6$		





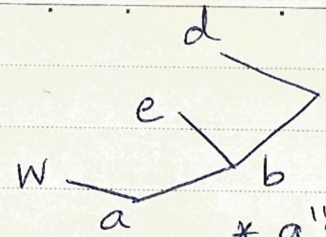
Find

1) $9\wedge 18 = 9$
2) $6\vee 9 = 18$
3) $9\wedge 6 = 3$
4) Find min element if it exist $= 3$
5) Find max element if exist $= 18$

* $9\wedge 18$ = greatest lower bound
  $9\vee 18$ = lowest/least upper bound

LANGUOSTYLE

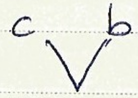
E.g.



here a"$\leq$"b, b"$\leq$"c, c"$\leq$"d, b"$\leq$"e, a"$\leq$"w, a"$\leq$"d, a"$\leq$"c

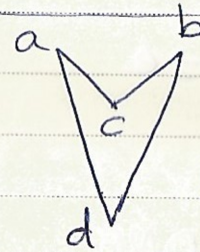
* a"$\leq$"d → assume transitive, do not draw it

E.g.



here b"$\not\leq$"c and c"$\not\leq$"b

E.g.

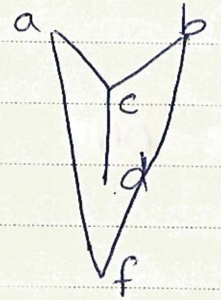


- c"$\leq$"a, c"$\leq$"b, d"$\leq$"a, d"$\leq$"b
- $a\wedge b$ = DNE

because anything less than C is not _"$\leq$"c then DNE

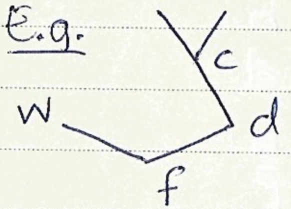
- c and d must be connected

E.g.



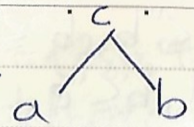
- $a\wedge b$ = DNE
  since ~~d~~ f"$\not\leq$"d

E.g.



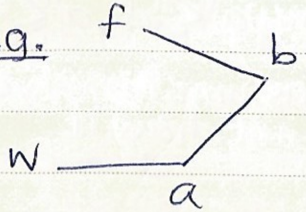
$w\wedge d = f$

E.g.



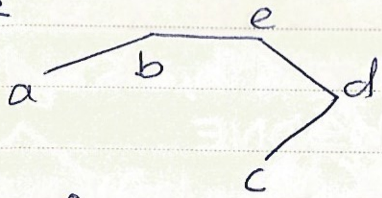
$a \vee b = c$

E.g.



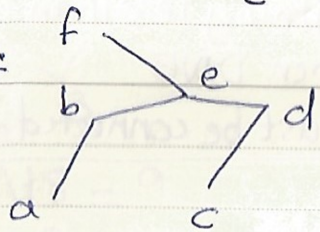
$a \wedge b = a$
$a \vee b = b$

E.g.



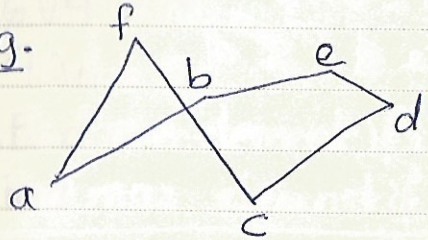
$a \vee c = e$

E.g.



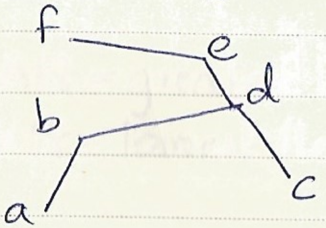
$a \wedge c = DNE$
$a \vee c = e$

E.g.



$a \vee c = DNE$

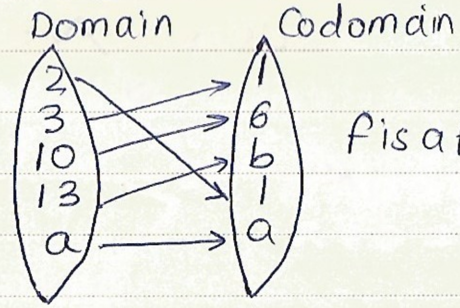
E.g.



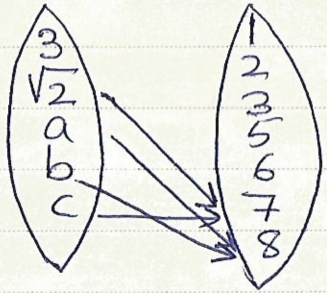
$b \wedge d = b$
$b \vee d = d$
$b \wedge f = b$
$b \vee f = f$

LANGUOSTYLE

Functions



f is a function



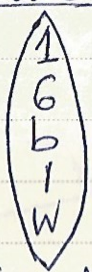
f is not a function

Def f: domain → codomain is a function iff

1) each element in the domain should have an output in the codomain
2) an element in the domain cannot have 2 different output

Difference b/w codomain & range

codomain



range = {b, l, w}

range $\subseteq$ codomain

- if range = codomain, function is ONTO

LANGUOSTYLE

Def f: Domain → codomain. Assume range = codomain then f is onto (surjective)

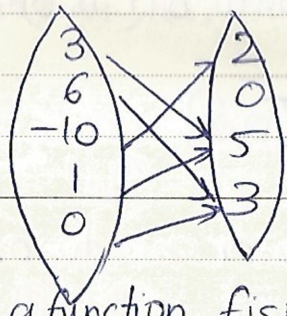
$f: \underbrace{[-4,4]}_{\text{domain}} \rightarrow \underbrace{\mathbb{R}}_{\text{codomain}}$, range [0,4]

since codomain ≠ range, function not onto

if

$f: [-4,4] \rightarrow [0,4]$, then f is onto

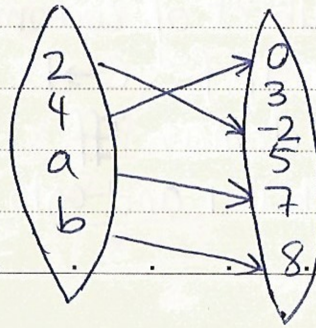
f:



f is a function, f is not onto or one-to-one

Def f is one-to-one iff each element in the range is assigned to one and only one element in the domain (injective)

f:



f is a function, not onto but one-to-one

Def f: Domain $\to$ codomain is called bijective if it is both one-to-one and onto.

x^2 → onto $(-\infty,\infty)$ range $=(-\infty,\infty)$ codomain)
→ one-to-one X $((-2)^2=4=(2)^2)$

Q. $f:[0,\infty)\to\mathbb{R}$, range $=[0,\infty)$
$f(x)=x^2$
$\mathbb{R}\neq[0,\infty]$, hence not onto but is one-to-one

Q. $f:[-2,\infty)\to\mathbb{R}$, range $=[0,\infty)$
$f(x)=x^2$
f is a function, not onto or one-to-one

Q. $f(x):[0,\infty]\to[0,\infty]$, range $[0,\infty]$
$f(x)=x^2$
f is onto and one-to-one

If $f: D\to C$, range is a subset of codomain,
then f is invertible if $f^{-1}: C\to D$
inverse from codomain to domain iff
f is bijective function (both 1-1 and onto)

• $(f\circ k)(x)=f(k(x))$
f composition k / f after k

Q. Imagine $f=2x^2+x-1$
$k=\sqrt{x}+3$
Find $(f\circ k)(x)=2(\sqrt{x}+3)^2+(\sqrt{x}+3)-1$
$=2(\sqrt{x}+3)^2+\sqrt{x}+2$
Find $(k\circ f)(x)=\sqrt{(2x^2+x-1)}+3$

• If f is invertible then $f\circ f^{-1}$ is the same as $(f^{-1}\circ f)=x$

Q. $f:\mathbb{R}\to\mathbb{R}$
$y=f(x)=2x^3-7$
f is invertible, find the inverse.

A. Substitute x for y, and y for x and solve for y
$y=2x^3-7$
$x=2y^3-7 \Rightarrow$ make y the subject
$y^3=\frac{x+7}{2}$
$y=\sqrt[3]{\frac{x+7}{2}}$, $f^{-1}(x)=\sqrt[3]{\frac{x+7}{2}}$

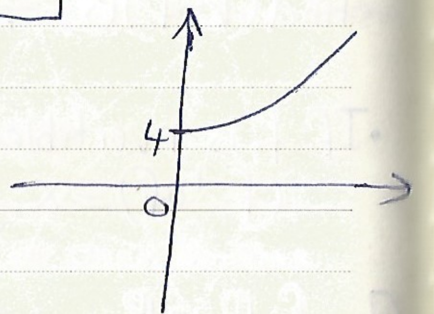
Q. $f: [0,\infty] \Rightarrow \mathbb{R}$, s.t. $f(x) = x^2+4$

Is f invertible? If yes, find f inverse, if not change the codomain so that f is invertible.

$$\boxed{\begin{array}{l} f(x) = ax^2+bx+c \\ \text{Vertex} = \left(\frac{-b}{2a}, f\left(\frac{-b}{2a}\right)\right) \end{array}}$$

$f(x) = x^2+4$

$f(0) = 4$



* by horizontal line test, the function 1-1
* function is not onto because codomain $\neq$ range $(\mathbb{R} \neq [4,\infty))$

hence f is not invertible, so change f

$f: [0,\infty) \Rightarrow [4,\infty)$

now f is onto and one-to-one

↳ $f^{-1}: [4,\infty] \rightarrow [0,\infty]$

$y = x^2+4$

$x = y^2+4$

$y = \sqrt{x-4}$

$f^{-1} = \sqrt{x-4}$

try $(f \circ f^{-1})(x) = x^2+4 = (\sqrt{x-4})^2+4$

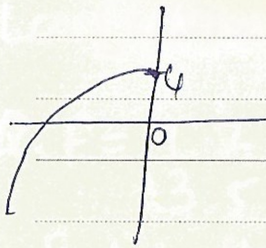
$= x-4+4 = x$

$(f^{-1} \circ f)(x) = \sqrt{(x^2+4)-4} = \sqrt{x^2+0} = x$

$(f \circ f^{-1}) = (f^{-1} \circ f) = x$

Q. $f: (-\infty,0] \rightarrow (-\infty,4)$, $f = -x^2+4$

If the inverse of f exists, find f^{-1}



f is 1-1 and onto

$f^{-1}: [-\infty,4] \rightarrow [-\infty,0]$

$y = -x^2+4$

$x = -y^2+4$

$y^2 = 4-x$

$y = \sqrt{4-x}$

$f^{-1} = -\sqrt{4-x}$

Q. $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 2 & 5 & 6 & 4\end{pmatrix}$ $\rightarrow$ domain, $\rightarrow$ codomain = range

a function from a finite set to itself

$f:\{1,2,3,4,5,6\} \rightarrow$ domain

$f(1)=3,\ f(3)=2,\ f(4)=5,\ f(5)=6,\ f(6)=4$

$f(2)=1$

f is 1-1 & onto, f is invertible

Find $f^2=(f \circ f)(x)$

$f^3=(f^2 \circ f)(x)$

$f^k=(f^{k-1} \circ f)(x)$

$$f^2=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 3 & 1 & 6 & 4 & 5\end{pmatrix}$$

$$f^3=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 2 & 3 & 4 & 5 & 6\end{pmatrix}$$

Q. $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 2 & 3 & 4 & 1 & 6 & 7 & 5\end{pmatrix}$

f is bijective

Find smallest positive integer n s.t $f^n(a)=a \ \forall a \in$ domain

$f=\underbrace{(1\ 2\ 3\ 4)}_{4\text{-cycle}} \circ \underbrace{(5\ 6\ 7)}_{3\ \cancel{4}\text{-cycle}}$ meaning $f^n=I=$ Identity function

$$f^n=\begin{pmatrix}1 & 2 & 3 & \ldots & 8\\ 1 & 2 & 3 & \ldots & 8\end{pmatrix}$$

$$LCM[3,4]=\frac{3\times4}{gcd(3,4)}=\frac{12}{1}=12$$

Q. $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 1 & 4 & 2\end{pmatrix}$

Find smallest positive integer n s.t $f^n=I$

$f=\underbrace{(1\ 3)}_{2\text{-cycle}} \circ \underbrace{(2\ 5)}_{2\text{-cycle}} \circ \underbrace{(4)}_{1\text{-cycle}}$

$$n=LCM[2,1]=\frac{2}{1}=2$$

Q. $f=\underbrace{(1\ 2\ 3\ 4)}_{4\text{-cycle}} \circ \underbrace{(5\ 7\ 8)}_{3\text{-cycle}} \circ \underbrace{(9\ 10\ 11\ 12\ 13)}_{5\ \cancel{8}\text{-cycle}}$

$LCM[4,3,5]=LCM[4,3]=12$

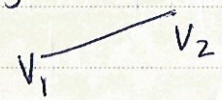
$$LCM[12,5]=\frac{12\times5}{gcd(12,5)}=60$$

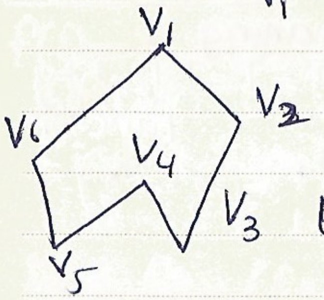
LANGUOSTYLE

Graphs

Def $G(V,E)$ V-set of vertices
E-set of edges

- an edge is a line segment that connects 2 vertices





$V=\{V_1,V_2,V_3,V_4,V_5,V_6\}$
$|V|=6$
$E=\{V_1-V_2, V_2-V_3, V_3-V_4, V_4-V_5, V_5-V_6, V_6-V_1\}$
(V_1-V_2 same as V_2-V_1)

- path: a sequence of edges that connect two vertices
  e.g. $V_1-V_2-V_3$ is a path/walk
  $V_1-V_6-V_5-V_4-V_3$ is another path

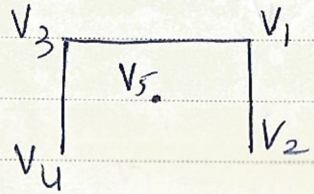
$V_1-V_2-V_3$ of length 2 (2 edges)
$V_1-V_6-V_5-V_4-V_3$ of length 4

so a path is $V_i-V_{i_1}-V_{i_2}-V_{i_3}-\cdots V_{in}$
where i_n are distinct vertices

LANGUOSTYLE

- every edge is a walk but not vice versa

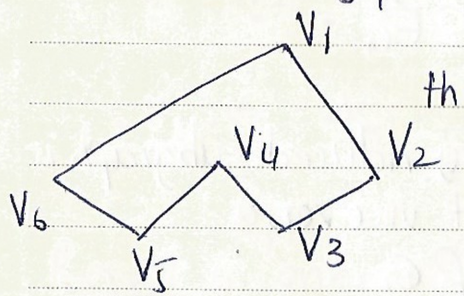
Connected graph - a graph is a connected graph if it $\exists$ a path between every 2 distinct vertices



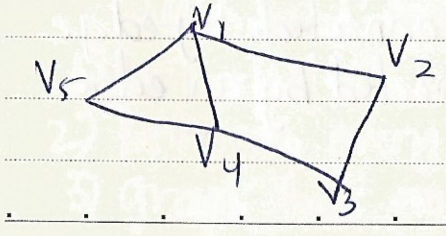
not connected
V_5 is not connected by any vertex by a path

Cycle: $V_i-V_{i_1}-V_{i_2}-V_{i_3}-\cdots V_{in}-V_i$
where $V_{i_1}-V_{in}$ are distinct vertices

difference b/w cycle and path
the starting point V_i is repeated twice

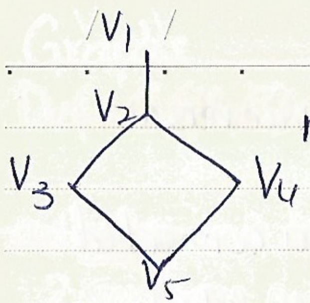


this graph is a cycle

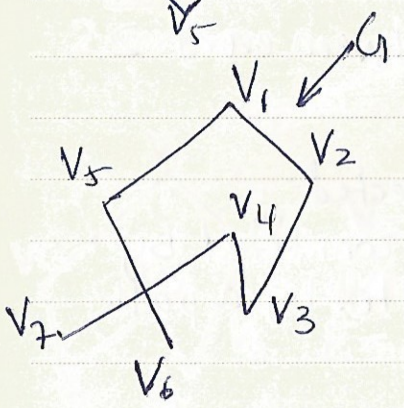


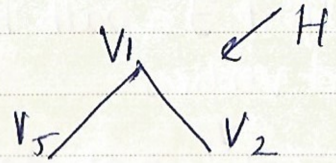
this graph is not a cycle but has a cycle

LANGUOSTYLE



not a cycle but has a cycle





H is a subgraph of G:

V_1, V_2, V_5 are also vertices of G

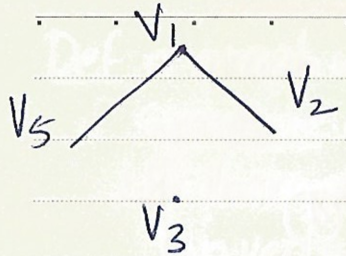
edges $V_1 - V_2$ and $V_1 - V_5$ belong in G

$= V_H \subseteq V_G$ and $E_H \subseteq E_G$

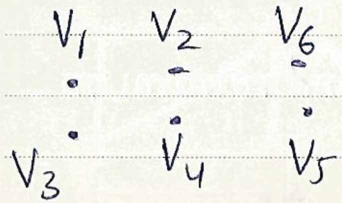
Induced subgraph - every induced subgraph is a subgraph but not vice versa

1) H is a subgraph of G
2) vertices in H are connected by edge iff they are connected by an edge in G

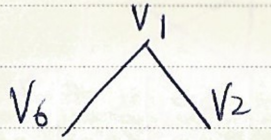
LANGUOSTYLE



not induced because $V_2 - V_3$ are not connected by an edge

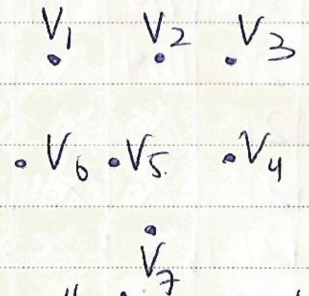


this is a subgraph but not induced



this is not a subgraph

Def H is a spanning subgraph of G iff $V_H = V_G$

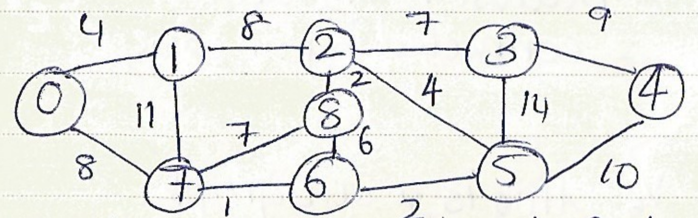


is a spanning subgraph since $V_H = V_G$

Result A connected graph is called a tree iff one of the following holds:

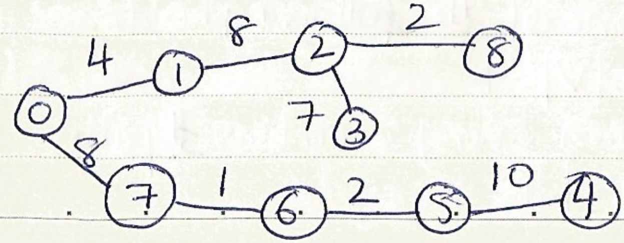
1) $|E| = |V| - 1$
2) between every 2 vertices $\exists!$ path
3) graph has no cycles

Weighted graph

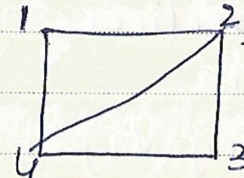


Use Dijkstraw algorithm to find minimum spanning tree
(starts with 0)

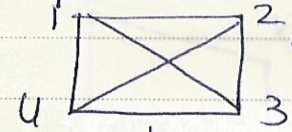
	0	1	2	3	4	5	6	7	8
0	$\boxed{0}$	4^{0}	∞	∞	∞	∞	∞	8^{0}	∞
1	X	$\boxed{4^{0}}$	12^{1}	∞	∞	∞	∞	8^{0}	∞
7	X	X	12^{1}	∞	∞	∞	9^{7}	$\boxed{8^{0}}$	15^{7}
6	X	X	12^{1}	∞	∞	11^{6}	$\boxed{9^{7}}$	X	15^{7}
5	X	X	12^{1}	25^{5}	21^{5}	$\boxed{11^{6}}$	X	X	15^{7}
2	X	X	$\boxed{12^{1}}$	19^{2}	21^{5}	X	X	X	14^{2}
8	X	X	X	19^{2}	21^{5}	X	X	X	$\boxed{14^{2}}$
4	X	X	X	$\boxed{19^{2}}$	$\boxed{21^{5}}$	X	X	X	X
3	X	X	X	$\boxed{19^{2}}$	X	X	X	X	X



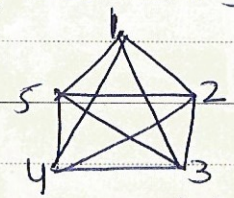
<u>Def</u> a graph with n vertices is called <u>complete</u> and it is denoted by K_n iff there ~~are~~ is an edge between every two vertices



this is connected but not complete



connected and now completed



there is an edge between every two vertices

* for a complete graph - deg(each vertex) $= n-1$
degree - no. of edges that meet at v

<u>Def</u> a graph is called <u>regular</u>, if degrees of all vertices are equal

<u>Result</u> $\sum$ all ~~edges~~ degrees $= 2|E|$ (for any graph)

$$|E| = \frac{\text{sum of } \cancel{\text{(all edges)}} \text{ degrees}}{2}$$

Q. 4,4,3,3,3,2,2,1,1

Is there are graph with 9 vertices, say $v_1, v_2, \ldots, v_9$ such that the $deg(v_1)=4, deg(v_2)=4, \ldots, deg(v_9)=1$?

step 1: ~~4~~ 4, 3, 3, 3, 2, 2, 1, 1

3, 2, 2, 2, 2, 2, 1, 1

step 2: 1, 1, 1, 2, 2, 1, 1

2, 2, 1, 1, 1, 1, 1

step 3 1, 0, 1, 1, 1, 1

1, 1, 1, 1, 1, 0

~~step~~ 0, 1, 1, 1, 1, 0

step 4 1, 1, 1, 1, 0, 0

0, 1, 1, 0, 0

step 5 1, 0, 0, 0, 0

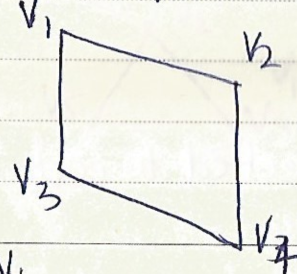
~~0, 0, 0, 0~~

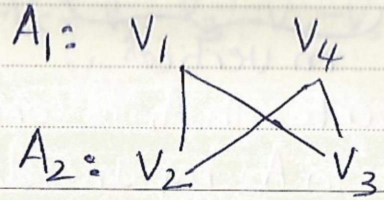
no such graph exists

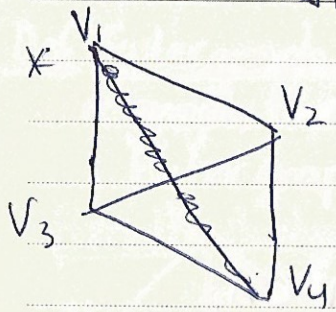
hence by algorithm, cannot be constructed

Bi partite graph: a graph is bipartite graph if the set of vertices can be partitioned into 2 sets A_1, A_2 such that every two vertices in the same set (A_1 or A_2) are not connected by an edge

* for a complete graph, A_1 or A_2 cannot be formed





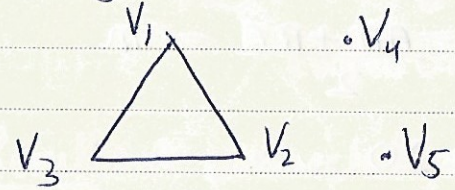


cannot be bipartite

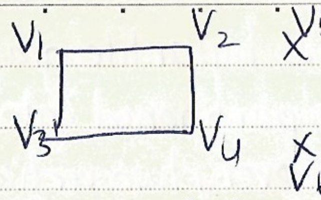
A_1: V_1 V_4

A_2: (cannot be formed)

a graph is bipartite iff the graph has no odd cycles



not bipartite



A_1: V_5 V_6 V_1 V_4

A_2: V_2 V_3

K_n complete graph with n vertices

$K_{n,m}$ is a connected bipartite where

A_1: $\underbrace{x \ x \ x \ x \ x \ldots x}_{n \text{ vertices}}$

A_2: $\underbrace{x \ x \ x \ x \ldots x}_{m \text{ vertices}}$

each vertex in A_1 is connected to each vertex in A_2 by an edge

e.g

$K_{3,2}$ A_1: V_1 V_2 V_3

A_2: V_4 V_5

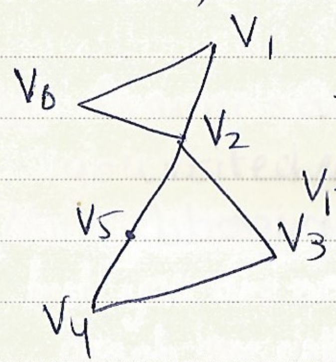
$$\text{degree}(\overset{=v}{\text{vertex}}) = \begin{cases} m & \text{if } v \in A_1 \\ n & \text{if } v \in A_2 \end{cases}$$

$$|E| = \frac{\sum \text{degrees}}{2} = \frac{nm+mn}{2} = nm$$

$K_{5,4} = |E| = 5 \times 4 = 20$

Def Circuit

a walk (vertices can be repeated) but in the walk, each edge of the graph must be only visited once and then return to v_0, such walk is called a circuit.



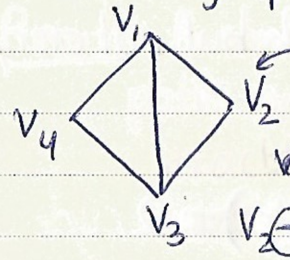
Is this graph a circuit?

$V_1 - V_6 - V_2 - V_3 - V_4 - V_5 - V_2 - V_1$

Yes

Def Euler graph / Euler circuit

a graph that is connected is called an Euler graph if it is a circuit



connected graph

$\underbrace{V_2 - V_1 - V_4 - V_3 - V - V_2}_{\text{edges are the same}}$

Result: A connected graph is an Euler graph iff deg(each vertex) is an even integer.

LANGUOSTYLE

$K_{4,3}$ is not an Euler because deg of vertex in A_1 is 3

$K_{n,m}$ is an Euler graph iff n,m both are even integers

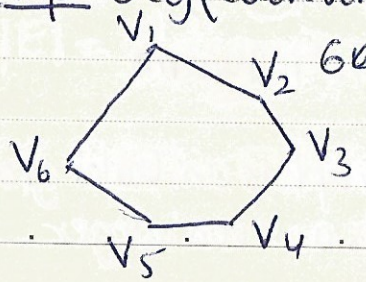
K_4 degree(each vertex) $= 3$

K_n is an Euler graph if n is odd
$\boxed{\deg(K_n) = n-1}$

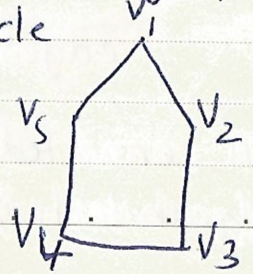
<u>Def</u> C_n – n cycles
C_6 – 6-cycles

C_n is always an Euler graph but not every Euler graph is a cycle

<u>Imp</u>. deg(each vertex of cycles) $= 2$

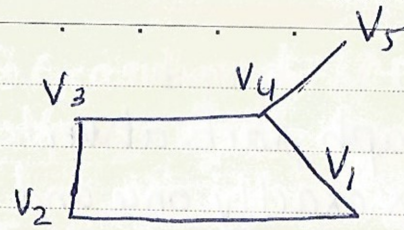


6-cycle



5-cycle

LANGUOSTYLE



not Euler
$\deg(V_5) = 1$

This is an Euler path but not Euler circuit

<u>Def</u> Assume you start at a vertex V_i and you visited each edge exactly once (Note: you may visit more than once) but you are not able to return to V_i, such graph we call it <u>Euler path</u>/trail

example: $V_5 - V_4 - V_1 - V_2 - V_3 - V_4$

<u>Result</u> A connected graph is an Euler path not Euler circuit iff exactly two vertices are of odd degrees

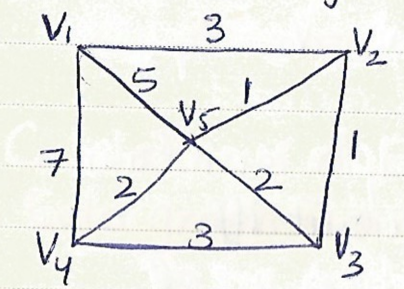
Def **Hamiltonian**

when a connected graph starts at vertex v, then visit each vertex exactly once and return to v (opposite of euler circuit, where we visit each edge exactly once)

Result connected graph D with n vertices is hamiltonian iff C_n is a subgraph of D (contains all the vertices)

eg. 10 vertices with C_{10} is a subgraph

cycle of degree 10 vertices



Is it hamiltonian?

List all possible (distinct) hamiltonian cycle

$V_5 \overset{5}{-} V_1 \overset{7}{-} V_4 \overset{3}{-} V_3 \overset{1}{-} V_2 \overset{1}{-} V_5$ $T_W = 17$

$V_5 \overset{5}{-} V_1 \overset{3}{-} V_2 \overset{1}{-} V_3 \overset{3}{-} V_4 \overset{2}{-} V_5$. $T_W = 14$. shortest hamiltonian cycle

LANGUOSTYLE

Is C_5 a subgraph of D?

$V_1 - V_2 - V_3 - V_4 - V_1$ Yes

Is it a cycle? No

Contains a cycle? ~~No~~ Yes

Hamiltonian? Yes

Euler circuit? No (deg of all vertices not all even)

Euler trail? No, more than 2 vertices have odd degrees

Math induction

$w = mc_1$ $\quad m|w$

$\searrow$ some integer

$k = mc_2$ $\quad m|k$

$mc_1 + mc_2 = w + k$

$m(c_1 + c_2) = w + k$

$m(c_1 \pm c_2) = w \pm k$

$\therefore m|(w \pm k)$ or $mc = (w \pm k)$

$m|ak$ for every integer a

$\cancel{mc_1 =}$ $mc_1 a = ak$

$m\left(\frac{c_1 a}{a}\right) = k$

$m|k$

- m is a factor of a & b then $m|(a \pm b)$
- m is a factor of n then $m|na$

$\uparrow$ a is an integer

LANGUOSTYLE

Show that $15|(7^{8n} - 1), \forall n \geq 1$

Solution:

1^{st} step: prove it for $n=1$

$15|7^8 - 1 = 15|5764801 - 1$

$= 15|5764800$

$5764800 = 38432 \times 15$

$\therefore \frac{7^8 - 1}{15}$ = integer by calculation

2^{nd} step: assume $15|7^{8n} - 1$ for some $n \geq 1$

3^{rd} step: prove it for $(n+1)$

substitute $(n+1)$ for n

then, back to step 2 then $n=3$

(called recursion)

Use algebra manipulation and then you are done

$$7^{(n+1)8} - 1 = 7^{8n}7^8 - 1 = 7^{8n}7^8 - 1 + \underline{7^8 - 7^8}$$

$$= \underbrace{(7^8 - 1)}_{*} + \underbrace{7^8(7^{8n} - 1)}_{**}$$

by step1 $\quad$ by step2 (multiple) 15 is a factor of $(7^{8n} - 1)$

① $15|*$ $\quad$ ② $15|**$

Since $15|*$ and $15|**$ then $15|(* + **)$

hence done.

Q. Show that $11 \mid 2^{10n}-1$ for every $n \geq 1$

Solution 1) Prove it for $n=1$ (or whatever starting value)
by calculation, check if $11 \mid 2^{10}-1$

$$11 \times \underbrace{93}_{\text{an integer}} = 2^{10}-1$$

2) Assume $11 \mid 2^{10}-1$ for some $n \geq 1$
3) Prove it for $n+1$
Show that $11 \mid 2^{10(n+1)}-1$
$2^{10n}2^{10}-1+2^{10}-2^{10}$
$\underbrace{(2^{10}-1)}_{*} + \underbrace{2^{10}(2^{10n}-1)}_{**}$

① $11 \mid *$ by step 1
② $11 \mid **$ by step 2 (because we assume $11 \mid 2^{10n}-1$)
$11 \mid (* + **)$, hence done.

Irrational – means no. cannot be written as $\frac{\text{integer}}{\text{integer}}$

irrational #s are infinite $= \mathbb{R}-\mathbb{Q}$
π is irrational whereas $\frac{22}{7}$, 3.14 is not

all terminated decimal no.s are rational

terminated – 3.1666666...
other irrational numbers – $e, \pi, \sqrt[x]{q}$
q is a prime

Rational – written in reduced form
if $x=\frac{a}{b}$, $\gcd(a,b)=1$

$\frac{\text{even}}{\text{odd}}, \frac{\text{odd}}{\text{odd}}, \frac{\text{odd}}{\text{even}}$ are reduced forms

but $\frac{\text{even}}{\text{even}}$ is NOT reduced

Q. Use the 4-method to convince me that $\sqrt{7}$ is irrational

Proof We use contradiction:
Deny (deny what we need to prove), then we reach to a conclusion i.e caused by our denial

Start ~~eg.~~ hence assume $\sqrt{7}$ is rational (Deny)
hence $\exists$ positive integers, a, b s.t.
$\sqrt{7}=\frac{a}{b}$, $\gcd(a,b)=1$

note: claim a and b are odd integers

$$7 = \frac{a^2}{b^2}$$

$7b^2 = a^2$ (here $7 \times (\text{odd})^2 = \cancel{\text{odd}}$ even)

~~odd~~ even $\neq$ odd

Def $n = \frac{a}{b}$ is reduced form n is odd, then a,b are odd

Def An integer w is called an odd integer if $w = 2k+1$ for some $k \in \mathbb{Z}$

An integer w is called an even integer if $w = 2k$ for some $k \in \mathbb{Z}$

since a,b are odd, $a = 2k+1$ and $b = 2m+1$ $k \in \mathbb{Z}, m \in \mathbb{Z}$

$$7 = \frac{(2k+1)^2}{(2m+1)^2}$$

$$7 = \frac{4k^2+4k+1}{4m^2+4m+1}$$

$$7(4m^2+4m+1) = 4k^2+4k+1$$

$$7m^2+7m+\frac{7}{4} = k^2+k+\frac{1}{4}$$

$$7m^2+7m+\frac{6}{4} = k^2+k$$

contradiction: integer + fraction $\neq$ integer

hence our denial is invalid, $\sqrt{7}$ is irrational

Q Convince me $\sqrt{17}$ is irrational

Deny $\sqrt{17}$ is rational, hence

$\sqrt{17} = \frac{a}{b}$ where a is ~~even~~ odd and b is odd and $\gcd(a,b) = 1$

$17 = \frac{(2m+1)^2}{(2k+1)^2}$ where $m, k \in \mathbb{Z}$

$$17(4k^2+4k+1) = 4m^2+4m+1$$

$$17k^2+17k+\frac{17}{4} = m^2+m+\frac{1}{4}$$

$$17k^2+17k+\frac{17-1}{4} = m^2+m$$

$$17k^2+17k+4 = m^2+m$$

assume m is even and k is odd

$(17 \times \text{odd}) + (17 \times \text{odd}) + 4 = \text{even} + \text{even}$

$\rightarrow$ even + 4 = even

note: $\frac{n-1}{4}$ works for any integer except 17

Q Convince me $\sqrt{5}$ is irrational

Deny, $\sqrt{5}$ is irrational hence $\sqrt{5} = \frac{a}{b}$, where a is ~~even~~ odd and b is odd & $\gcd(a,b) = 1$

$\sqrt{5} = \frac{a}{b}$, $5 = \frac{a^2}{b^2}$, where $a = 2m+1$, $b = 2n+1$, $m, n \in \mathbb{Z}$

$5(2n+1)^2 = (2m+1)^2$

$5(4n^2+4n+1) = 4m^2+4m+1$

$5n^2+5n+\frac{5}{4} = m^2+m+\frac{1}{4}$

$5n^2+5n+\frac{5-1}{4} = m^2+m$

$5n^2+5n+1 = m^2+m$

(assume m and n to be odd: $(5 \times \text{odd}) + (5 \times \text{odd}) = \text{even}$ and RHS: odd + odd = even)

works

$\underbrace{5n^2+5n}+1 = \underbrace{m^2+m}$

even + 1 = odd even

contradiction odd ≠ even

hence $\sqrt{5}$ is irrational

Q. $\sqrt{45}$ is irrational

→ same method, replace 5 by 45

→ works even though 45 is not prime

$45(4n^2+4n+1) = 4m^2+4m+1$

$45n^2+45n+\frac{45-1}{4} = 4m^2+4m$

$\underbrace{45n^2+45n+11}_{\text{even + odd = odd}} = \underbrace{4m^2+4m}_{\text{even}}$

even ≠ odd, hence contradiction and $\sqrt{45}$ is irrational

Q. $\sqrt{2}$ is irrational

Deny, $\sqrt{2}$ is rational hence $\sqrt{2} = \frac{a}{b}$ where a is even, b is odd, $\gcd(a,b) = 1$

(reason: $2 = \frac{a^2}{b^2}$ iff $\frac{\text{odd}}{\text{odd}}$ then $2 \times \text{odd} = \text{even}$ then even $= a^2$ (which is odd))

$2 = \frac{a^2}{b^2}$, $a = 2k$, $b = 2m+1$ $(k, m \in \mathbb{Z})$

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

$2(4m^2+4m+1) = 4k^2$

$2m^2+2m+\frac{2}{4} = k^2$

integer + fraction ≠ integer.

contradiction, hence $\sqrt{2}$ is irrational

rational ± rational = rational (direct) proof by

rational ± irrational = irrational (contradiction)

irrational ± irrational = could be rational/irrational (by example)

<u>Proof</u> (1) x, y are rational, Show that x+y rational

since x, y are rational

$x = \frac{a}{b}$ (a, b are integers; $b \neq 0$)

and $y = \frac{c}{d}$ (c, d are integers, $d \neq 0$)

<u>Now</u> $x+y = \frac{a}{b} + \frac{c}{d}$

$$\frac{ad+cb}{bd} = \frac{\overset{\text{integer}}{ad} + \overset{\text{integer}}{cb}}{\underset{\text{integer}}{bd}}$$

since integer + integer = integer then

$x+y = \frac{\text{integer}}{\text{integer}}$, hence rational

<u>Proof</u> (2) x be rational and y be irrational.

We show that x+y is irrational.

1) deny: hence x+y is irrational

<u>i.e</u> $x+y = W$ is irrational

$y = W - x$

by (1), W−x is rational, then <u>y is rational</u>

contradiction, our denial is invalid,

x+y is irrational

<u>Proof (3)</u> Example:

$\sqrt[n]{Q}$, $n \geq 2$, Q is prime

$\underbrace{x = \sqrt{7}}_{\text{irrational}}$, $\underbrace{y = 5 - \sqrt{7}}_{\text{irrational by(2)}}$

$x+y = \sqrt{7} + 5 - \sqrt{7} = 5$ (rational)

irrational ± irrational = could be rational ~~irrational~~

Example: $\overset{\text{irrational}}{\sqrt{2}} + \overset{\text{irrational}}{\sqrt{3}}$ = irrational

in this case, could be irrational

Q. Convince me x, y are odd, then x+y is ~~odd~~ even

<u>since</u> $x = 2k+1$, $k \in \mathbb{Z}$

$y = 2m+1$, $m \in \mathbb{Z}$

then $x+y = 2k+1+2m+1$

$= 2(k+m)+2$

$= 2(k+m+1)$

2(any integer) = even

Q. Convince me x ~~you even~~ is even and y is odd, then $x+y=$ ~~even~~ odd

Proof $x=2k, k\in \mathbb{Z}$

$y=2m+1, m\in\mathbb{Z}$

$x+y=2k+2m+1=2\underbrace{(k+m)}_{\text{integer}}+1$

$= 2\times \text{integer}+1 = \text{odd (by def)}$

note $W=\sqrt[n]{Q_1^{\alpha_1}\cdot Q_2^{\alpha_2}\cdot Q_3^{\alpha_3}\cdots Q_m^{\alpha_m}}, n\geq 2$

where $Q_1, Q_2, Q_3, \ldots, Q_m$ are distinct prime

If one of the exponent is not divisible by n, then W is irrational

e.g. $\sqrt[5]{\underset{\substack{\downarrow\\ \text{not divisible by } 5}}{3^{7}}\cdot 5^{10}\cdot 7^{12}\cdot 13}$ = irrational

Pigeonhole principle

Ceiling function

$\lceil 3.1\rceil=4$ $\lceil\;\rceil$ is ceiling function

$\lceil -2.7\rceil=-2$ ($x\in\mathbb{R}$, $\lceil x\rceil$ = least integer $\geq x$)

$\lceil -2\rceil=-2$, $\lceil \frac{9}{4}\rceil=3$

Floor function

$\lfloor -5.2\rfloor=-6$ $\lfloor x\rfloor$ = greatest integer $\leq x$

* $\lceil -3\rceil=\lfloor -3\rfloor=-3$

pigeonhole principle : f: Domain $\to$ Codomain

$|\text{codomain}|\leq|\text{domain}|$

there are atleast n elements in the domain that map to the same element in the codomain. Find max. value of n.

$f:\{1,2,4,5\}\to\{3,10\}$

$|D|=\cancel{3}\,4$ $|C|=2$

Construct all possible functions. you have $2^4=16$

statement true for all 16 functions

To find n, $n=\left\lceil\frac{|D|}{|C|}\right\rceil=\frac{4}{2}=2$

Q. In 5000 students, there exist atleast n students who were born on the same day of the week and on the same year (2000–2019). Find the max value of n.

$|D|=5000$ $|C|=19-0+1=(20\times\underset{\text{week}}{7})=140$

$n=\left\lceil\frac{5000}{140}\right\rceil=36$

Q. In a class of 19 students, how many n of the same gender?

$|D| = 19 \quad |C| = 2$ (male/female)

$n = \left\lceil \frac{19}{2} \right\rceil = 10$

Q. You have 900 balls which can be thrown into 3 different holes, how many balls can be thrown in the same hole?

$n = \left\lceil \frac{900}{3} \right\rceil = 300$, atleast 300

Q. There are 1,000,000 people, born between 1980 and 2005 and atleast n that have the same month, day, year of birth?

$D \longrightarrow C \qquad |D| = 1000000 \quad |C| = 2005 - 1980 + 1$

$= \begin{pmatrix} 26 & 30 & 12 \\ Y & D & M \end{pmatrix}$

year, day, month

$n = \left\lceil \frac{1000000}{9360} \right\rceil = 107 \qquad = 26 \times 30 \times 12 = 9360$