# MATH 132

# Discrete and Combinatorial Mathematics

Spring 2017 (Özgün Ünlü)

Lecture Notes

*Emin Bahadır Tülüce*

Subject: Date: ..../..../....

## Section 1.1) Fundamental Principles of Counting

The Rule of Sum: If the first task can be performed in $n$-ways and the second task can be performed in $m$-ways, then performing either task can be accomplished in $(n+m)$-ways.

↳ First or second but not both.

The Rule of Product: $\underbrace{\text{Procedure}} = \underbrace{\text{First Stage}} + \underbrace{\text{Second Stage}}$

If there are $m$ possible outcomes of first stage and for each of these outcomes there are $n$ possible outcomes for the second stage. Then, the procedure can be carried out in $(m \cdot n)$-ways.

Ex| Count the number of times print() is executed.

a. for i=1 to 5 do
   for j=1 to 7 do
   print("Math 132")

$5 \cdot 7 = 35$ by the Rule of Product.

b. for i=1 to 4 do
   for j=2i to 2i+8 do
   print()

$2i+8-2i+1 = 9$

$4 \cdot 9 = 36$ by the Rule of Product.

c. for i=1 to 2 do
   for j=2i to 4i do
   print()

$4i - 2i + 1 = 2i + 1$

$(2+1) + (4+1) = 8$ by the Rule of Sum.

Exercise| Write the generalized versions of the rule of sum and product.

If there are $n$ many tasks which can be performed in $t_1, t_2, \dots t_3$ many ways, then either task can be accomplished in $\sum_{i=1}^{n} t_n$ many ways.

If there are $n$ many stages of a procedure which has $s_1, s_2 \dots s_n$ outcomes, then the procedure can be carried out in $\prod_{i=1}^{n} s_i$ many ways.

## Section 1.2)

Definition: Given a collection of distinct objects, any arrangement of $r$ many of these objects is called a permutation of size $r$. ↳ Order is important.

Notation: $P(n, r) = n \cdot (n-1) \dots (n-r+1)$

Ex) $P(5, 0) = 5 \cdot 4 \cdot \dots 6 = 1$ — empty multiplication gives the identity element of multiplication which is 1.

Fact: There are $P(n, r)$ many different permutations of size $r$ of $n$ elements.

Proof: $\underbrace{\text{Write an arrangement of size } r}_{} = \underbrace{\text{Write 1. obj}}_{n \text{ outcomes}} + \underbrace{\text{Write 2. obj}}_{n-1 \text{ outcomes}} + \dots + \underbrace{\text{Write } r^{th} \text{ obj.}}_{n-r+1 \text{ outcomes}}$

by the Rule of Multiplication

$= n \cdot (n-1) \dots (n-r+1) = P(n, r)$

Ex) A license plate manifacturer wants to manifacture plates consisting of three letters follwed by two digits and no letter or digit can repeat for each plate. How many plates are there possible?

$\underbrace{\text{Manifacture Plate}}_{} = \underbrace{\text{Write Three Letters}}_{P(26,3)} + \underbrace{\text{Write Two Digits}}_{P(10,2)}$

↳ $= P(26,3) \cdot P(10,2) = 26 \cdot 25 \cdot 24 \cdot 10 \cdot 9$ } Enough for the exam.

⊛ $0! = 0 \cdot (-1) \cdot (-2) \cdot \dots \cdot 1 = 1$ (empty multiplication)

Fact: Assume there are $r$ many types of objects and $n_i$ many $i^{th}$ type object for $i$ in $\{1, 2, 3 \dots, r\}$, then: [Permutations with repetations]

The number of linear arrangement of these objects $= \dfrac{n!}{n_1! \cdot n_2! \cdots n_r!}$

Proof: Distinguish each object from each other by giving distinct indexes to all indistinguishable objects in a type, for all types.

$$\underbrace{\text{Write a linear arrangement of these } n \text{ distinct objects}} = \overbrace{\underbrace{\text{Write a linear arrangement of these objects without indexes}}}^{\text{We want to find this}} + \underbrace{\text{put indexes to indistinguishable objects of 1. type}} + \underbrace{\text{put indexes to indistinguishable objects of 2. type}} + \dots + \underbrace{\text{put indexes to indistinguishable objects of } r^{th} \text{ type}}$$

$$P(n,n) = X \cdot n_1! \cdot n_2! \cdots n_r!$$

$$n! = X \cdot n_1! \cdot n_2! \cdots n_r! \Rightarrow X = \frac{n!}{n_1! \cdot n_2! \cdots n_r!}$$

Ex| Find all the arrangements of aab by using the proof.

$a_1 a_2 b_1$, there are 2 types $(r=2)$, two a's $(n_1=2)$, one b $(n_2=1)$

$\underbrace{\text{Linear arr. of } a_1 a_2 b_1} = \underbrace{\text{First Stage}} + \underbrace{\text{Second Stage}} + \underbrace{\text{Third Stage}}$

| P(3, 3) | First Stage | Second Stage | Third Stage |
|---|---|---|---|
| | a a b | $a_1$ $a_2$ b | $a_1$ $a_2$ $b_1$ |
| | | $a_2$ $a_1$ b | $a_2$ $a_1$ $b_1$ |
| | a b a | $a_1$ b $a_2$ | $a_1$ $b_1$ $a_2$ |
| | | $a_2$ b $a_1$ | ⋮ |
| | b a a | b $a_1$ $a_2$ | |
| | | b $a_2$ $a_1$ | |

$$3! = X \cdot 2! \cdot 1! \Rightarrow X = \frac{3!}{2! \cdot 1!} = 3$$

Ex| Determine the number of staircase paths in the xy-plane from the point (1,3) to (5,6).

$5-1=4$ right moves

$6-3=3$ up moves

$$\overbrace{RRRRUUU}^{\text{Arrange this}} \Rightarrow \frac{7!}{4! \cdot 3!} = 35$$

## Section 1.3)

Definition: Given a collection of distinct object. A subcollection of r objects is called a combination / selection of size r. Order is not important

Notation: $C(n,r) = \frac{P(n,r)}{r!}$

Fact: There are $C(n,r)$ different combinations of size r of n elements.

Proof: $\underbrace{\text{Write a permutation}}_{P(n,\,r)} = \underbrace{\text{Write a combination}}_{X} + \underbrace{\text{Put on order}}_{r!}$

$$P(n,r) = X \cdot r! \Rightarrow X = \frac{P(n,r)}{r!} = C(n,r)$$

⊛ $P(n,r) = \dfrac{n!}{(n-r)!}$  $C(n,r) = C(n,n-r) = \dfrac{n!}{(n-r)!} \cdot \dfrac{1}{r!}$

Proof: $P(n,r) = n(n-1)\cdot\ldots\cdot(n-r+1) = n\cdot(n-1)\cdot\ldots\cdot(n-r+1)\dfrac{(n-r)(n-r-1)\cdots 1}{(n-r)(n-r-1)\cdots 1} = \dfrac{n!}{(n-r)!}$

Combinations of Repetations:

Ex| All combinations with repetations of size 2 among A and B: AA, AB, BB

Theorem: The following numbers are all equal.

i. The number of combinaton with repetitions of size $r$ among $n$ distinct objects

ii. The number of integer solutions to the equation $x_1 + x_2 + x_3 \cdots x_n = r$, $x_i \geq 0$

iii. The number of way $r$ identical objects can be distributed among $n$ distinct containers.

iv. The number of linear arrangements of $r$ many $x$'s and $(n-1)$ many $|$'s.

v. $C(n+r-1, r)$

Proof of i = ii: $x_i$ = number of ith object in the combination.

Proof of ii = iii: $x_i$ = number of objects in the ith container.

Proof of iii = iv: Put on $x$ for an object, on $|$ between containers.

Proof of iv = v: Number of linear arrangements of $r$ $x$'s and $(n-1)$ $|$'s with linear permutation of repetations. $= \dfrac{(r+(n-1))!}{r!\cdot(n-1)!} = C(n+r-1, r)$

| Ex | | $x_1+x_2=2$ | $\sqcup\sqcup$: | $x$'s and $|$'s | The formula |
|---|---|---|---|---|---|
| | AA | $x_1=2$, $x_2=0$ | $\overset{:}{\sqcup}\ \sqcup$ | $xx|$ | $C(n+r-1, r)=$ |
| | AB | $x_1=1$, $x_2=1$ | $\dot{\sqcup}\ \dot{\sqcup}$ | $x|x$ | $C(2+2-1, 2)=$ |
| | BB | $x_1=0$ $x_2=0$ | $\sqcup\ \overset{:}{\sqcup}$ | $|xx$ | $C(3,2) = 3$ |

Subject : Date :......./......./.......

Ex) In how many ways can one distrubute 4 identical marbles among 9 distinct containers. $\begin{matrix} 4 & x\text{'s} \\ 9\text{-}1 & 1\text{'s} \end{matrix}$ $\frac{(4+8)!}{4!\cdot 8!} = \frac{12\cdot 11\cdot 10\cdot 9\cdot 8!}{4\cdot 3\cdot 2\cdot 8!} = 495$

Solution with formula: $\begin{matrix} n=9 \\ r=4 \end{matrix}$ $C(9+4-1, 4) = 495$

Ex) Find the number of all non-negative integer solutions to the $x_1+x_2+x_3+x_4=18$

$\begin{matrix} 18\ x\text{'s} \\ 4\text{-}1\ 1\text{'s} \end{matrix}$ $\frac{(18+3)!}{18!\ 3!} = \frac{21\cdot 20\cdot 19\cdot 18!}{18!\ 3\cdot 2} = 1330$ With formula: $\begin{matrix} n=4 \\ r=18 \end{matrix}$ $C(18+4-1, 18) = 1330$

Ex) Find the number of all positive integer solutions to the $x_1+x_2+x_3+x_4=18$

We can say $x_i \geq 1$ and then, $y_1+y_2+y_3+y_4=14$ has the same answer.

$y_i = x_i+1$

$\begin{matrix} n=4 \\ r=14 \end{matrix}$ $C(4+14-1, 14) = C(17, 14)$

Ex) Find the number of integer solutions to the equation $x_1+x_2=6$, $\begin{matrix} 0 \leq x_1 \leq 3 \\ x_2 \geq 0 \end{matrix}$

Long Solution: $\underbrace{\text{NumberOfSolutions}} = \underbrace{x_1\geq 0,\ x_2 \geq 0}_{\text{numberOfSolutionsOf}} - \underbrace{x_1\geq 4,\ x_2\geq 0}_{\text{numberOfSolutionsOf}}$

$X = C(7,6) - C(3,2)$ $\quad X = C(2+6-1, 6) - \underbrace{y_1+y_2=2 \quad \begin{matrix} y_1\geq 0 \\ y_2 \geq 0\end{matrix}}_{\text{Number of solutions of}}$

$X = 7-3 = 4$

Ex) Let $\{a, b, c\}$ be a set of objects. For these objects find;

a) Find the number of permutations of size 2: $P(3,2) = 6$

b) Find the number of permutations with repetations of size 2: $3^2 = 9$

c) Find the number of combinations of size 2: $C(3,2) = \binom{3}{2} = 3$

d) Find the number of combinations with repetations of size 4: $C(3+4-1, 4) = 15$

Ex) Find the number of permutations of the letters in the word COMPUTER.

Since there's no size given, we should take it as 8: $P(8,8) = 8! = 40320$

Ex) Find the number of possible 4-letter sequences of the letters in word COMPUTER with repetations are allowed.

$8\cdot 8\cdot 8\cdot 8 = 8^4 = 4096$

Subject: Date ..../..../....

**Ex** Find the number of arrangements of letters in the word ANKARA.

Since there's 3 A's and 1 of each other: $\frac{6!}{3!\cdot 1!\,1!\,1!} = \frac{6!}{3!} = 6\cdot 5\cdot 4 = 120$

**Ex** How many arrangements in the previous ex. have no adjacent A's.

$\underbrace{\text{WriteSuchArrangement}}_{\hookrightarrow X = 6\cdot 4 = 24} = \underbrace{\text{WriteAnArrangementOf N, K, R}}_{P(3,3)=6} + \underbrace{\text{Put A's to the }{}_a N {}_a K {}_a R {}_a}_{C(4,3)=4}$

select 3 boxes of 4.

**Ex** If 6 people designated as A, B, C, D, E, F are seated about a round table, how many different circular arrangements are possible?

Two arrangements are considered to be same if one can be obtained by rotating another: ABCD = BCDA

$\underbrace{\text{Write Linear Arrangement}}_{P(6,6)} = \underbrace{\text{Write Circular Arrangement}}_{X} + \underbrace{\text{Choose A Starting Point}}_{C(6,1)}$

$X \rightarrow 6! = X\cdot 6 \Rightarrow X = 120$

**Ex** How many times is the print() statement executed in the following codes.

a.
```
for i=1 to 20 do
    for j=1 to 20 do
        for k=1 to 20 do
            if (i-j)^2 * (j-k)^2 * (i-k)^2 > 0
                print()
```
We observe that i, j, k should be distinct to execute print.

$P(20,3) = 20\cdot 19\cdot 18 = 6840$

b.
```
for i=1 to 20 do
    for j=1 to 20 do
        for k=1 to 20 do
            if (i-j)^2 * (j-k)^2 > 0
                print()
```
either $i \neq k$ or $i = k$

$P(20,3) + P(20,2) = 7220$

(as before)

c.
```
for i=1 to 20 do
    for j=i+1 to 21 do
        for k=j+1 to 22 do
            print()
```
Since $1 \leq i < j < k \leq 22$, $\{i,j,k\}$ is a combination of size 3 among $\{1,2,\ldots 22\}$

$C(22,3) = 1540$

d.
```
for i=1 to 20 do
    for j=i to 20 do
        for k=j to 20 do
            print()
```
* [we can observe this ex is same with c. so 1540]
* Since $1 \leq i \leq j \leq k \leq 20$ so $\{i,j,k\}$ is a combination with repetitions among $\{1,2,\ldots 20\}$

$C(20+3-1,\ 3) = C(22,3) = 1540$

Subject: Date: ....../....../......

*Another solution for d; Consider $X_1 = i-1$, $X_2 = j-i$, $X_3 = k-j$

Then $x_1 + X_2 + X_3 \leq 19 \Rightarrow \underbrace{\text{Answer}} = \underbrace{\substack{\text{Number of solutions} \\ X_1+X_2+X_3 \leq 19, \ X_i \geq 0}} = \underbrace{\substack{\text{Number of solutions} \\ X_1+X_2+X_3+Y_4 = 19, \ X_i \geq 0}}$

$C(4+19-1, 19) = C(22,19) = C(22,3) = 1540$

Ex) Determine the number of integer solutions of $x_1 + X_2 + X_3 + X_4 = 32$ where $X_1 > 0$, $X_2 > 0$, $X_3 > 0$, $0 < X_4 \leq 25$.

$$\underbrace{\text{Number Of Such Solutions}} = \underbrace{\substack{\text{Number Of Integer Solutions} \\ X_1+X_2+X_3+X_4=32, \ x_i > 0}} - \underbrace{\substack{\text{Number Of Integer Solutions} \\ X_1+X_2+X_3+X_4=32, \ X_1>0, X_2>0, X_3>0, \ X_4>25}}$$

$$= \underbrace{\substack{\text{Number Of Integer Solutions} \\ Z_1+Z_2+Z_3+Z_4 = 28 \\ \text{where } Z_i \geq 0}} - \underbrace{\substack{\text{Number Of Integer Solutions} \\ W_1+W_2+W_3+W_4 = 3 \\ \text{where } W_i \geq 0}} = C(28+4-1, 28) - C(3+4-1, 3) = C(31,28) - C(6,3)$$

$Z_i = X_i - 1$

$32-4 = 28$

$W_1 = X_1 - 1$, $W_2 = X_2 - 1$, $W_3 = X_3 - 1$, $W_4 = X_4 - 26$

$32-1-1-1-26 = 3$

Theorem: $(x_1 + x_2 + \cdots x_k)^n = \sum \frac{n!}{n_1! \cdot n_2! \cdots n_k!} x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$

Proof: $(x_1 + x_2 + \cdots x_k)^n = \underbrace{(x_1 + x_2 + \cdots x_k)}_{\text{1st factor}} \cdot \underbrace{(x_1 + x_2 + \cdots x_k)}_{\text{2nd factor}} \cdots \underbrace{(x_1 + x_2 + \cdots x_k)}_{n^{th}\text{ factor}}$

$=$

## Chapter 2)

Definition: A proposition or statement is a declarative sentence in which something is affirmed or denied so that it can therefore be significantly characterized as either true or false when it's interpreted in the context of a universe.

Ex) The Statement "$3 < 5$" is true when the universe is natural numbers.

Ex) "This statement is false" is hard to interpret.

Definition: Let p and q be two statements then we can obtain new statements called compound statement using the following logical connective or transformations.

Subject : Date : ...../...../.....

| Name | Notation | Reads | Definition |
|---|---|---|---|
| negation | $\neg p$ | not p | |
| conjunction | $p \wedge q$ | p and q | |
| disjunction | $p \vee q$ | p or q | |
| implication | $p \to q$ | if p, then q<br>p implies q<br>p only if q | q, if p<br>p is sufficent condition for q<br>p is necessary condition for q |
| biconditional | $p \leftrightarrow q$ | p, if and only if q<br>p is necessary and sufficent condition for q<br>p iff q | |

| p | q | $p \leftrightarrow q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

tables like this one

Definition: The contrapositive of $p \to q$ is $(\neg q) \to (\neg p)$

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

Definition: We say two compound statements $C_1$ and $C_2$ are logically equivalent and write $C_1 \Longleftrightarrow C_2$ if $C_1$ and $C_2$ have the same truth values in a complete truth table.

Ex)

| p | q | $p \to q$ | $(\neg q) \to (\neg p)$ | $q \to p$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 |

So we can say contrapositive of $p \to q$ is logically equivalent to $p \to q$. But the converse is not equivalent to $p \to q$

Laws of Logic: ① $p \to q \Longleftrightarrow (\neg p) \to (\neg q)$ (proof above)

② $\neg(\neg p) \Longleftrightarrow p$ Proof:

| p | $\neg p$ | $\neg\neg p$ |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 1 |

[Law of Negation]

③ $\neg(p \vee q) \Longleftrightarrow (\neg p) \wedge (\neg q)$ ④ $\neg(p \wedge q) \Longleftrightarrow (\neg p) \vee (\neg q)$

[De'Morgan's Law]

Proofs can be done with complete truth tables.

(5) $p \vee q \iff q \vee p$ (6) $p \wedge q \iff q \wedge p$ [Commutative laws]

(7) $(p \vee q) \vee r \iff p \vee (q \vee r)$ (8) $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$ [Associate laws]

(9) $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$
(10) $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ [Distrubutive Laws]

(11) $p \wedge p \iff p$ (12) $p \vee p \iff p$ [Independent Laws]

(13) $p \vee F_0 \iff p$ (14) $p \wedge T_0 \iff p$ [Indentity Laws]

(15) $p \vee T_0 \iff T_0$ (16) $p \wedge F_0 \iff F_0$ [Domination Laws]

(17) $p \vee \neg p \iff T_0$ (18) $p \wedge \neg p \iff F_0$ [Inverse Laws]

(19) $p \vee (p \wedge q) \iff p$ (20) $p \wedge (p \vee q) \iff p$ [Absorption Laws]

Ex| Show that $\neg(\neg((p \vee q) \wedge r) \vee (\neg q)) \iff q \wedge r$.

First proof: Draw a truth table for $p$, $q$, $r$, $(p \vee q)$, $(p \vee q) \wedge r$, $\neg((p \vee q) \wedge r)$, $(\neg q)$, the whole thing without $\neg$, the whole thing.

Second proof: Use De Morgan's rule: $\neg\neg((p \vee q) \wedge r) \wedge (\neg\neg q) \iff$

Use law of double negation: $((p \vee q) \wedge r) \wedge q \iff$

Use commutative rule: $r \wedge (q \wedge (p \vee q)) \iff$

Use absorption rule: $r \wedge q \xLeftrightarrow[\text{again}]{\text{commutative}} q \wedge r$

→ Names will be provided in the exam.

Ex|
```
counter1 = 0
counter2 = 0
for n=6 to 11 do
    for m= 4 to 7 do
        for k= 9 to 15 do
            if not (not (((n > 8) or (m>5)) and (k<12)) or (not (m>5)))
                counter1 = counter1 +1
            else counter2 = counter2 +1
```

Find the counter1 and counter2 after exec.

Assume $p = \text{"}n > 8\text{"}$ $q = \text{"}m > 5\text{"}$ $r = \text{"}k < 12\text{"}$

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

Since the expression is equivalent with $r \wedge q$ from the prev. ex!

| $q$ | $r$ | $q \wedge r$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

$\text{counter1} = \underset{6 \le n \le 11}{6} \cdot \underset{6 \le m \le 7}{2} \cdot \underset{9 \le k \le 11}{3} = 24$ $\text{counter2} = 6 \cdot 4 \cdot 7 - \text{counter1} = 132$

Subject :                                                                 Date ....../....../......

Definition: We write $(p_1 \wedge p_2 \wedge \cdots p_n) \Rightarrow q$ or we write $\dfrac{\begin{matrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{matrix}}{\therefore q}$

when $((p_1 \wedge p_2 \wedge \cdots p_n) \to q) \Longleftrightarrow T_0$. These means if we assume $p_1, p_2, \ldots p_n$ are all true then $q$ must be true.

Ex $\dfrac{\begin{matrix} p \\ p \to q \end{matrix}}{\therefore q}$

| $p$ | $q$ | $p \to q$ | $p \wedge (p \to q)$ | $(p \wedge (p \to q)) \to q$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 |

✓

Rules of Inference: (1) $\dfrac{\begin{matrix} p \\ p \to q \end{matrix}}{\therefore q}$ [Modus Ponens] (Proof at above)

(2) $\dfrac{\begin{matrix} p \to q \\ q \to r \end{matrix}}{\therefore p \to r}$

| $p$ | $q$ | $r$ | $p \to q$ | $q \to r$ | $(p \to q) \wedge (q \to r)$ | $p \to r$ | $((p \to q) \wedge (q \to r)) \to (p \to r)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

Always true

[Modus Tollens]
(3) $\dfrac{\begin{matrix} p \to q \\ \neg q \end{matrix}}{\therefore \neg p}$

(4) $\dfrac{\begin{matrix} p \\ q \end{matrix}}{\therefore p \wedge q}$ (5) $\dfrac{\neg p \to F_0}{\therefore p}$ (6) $\dfrac{p \wedge q}{\therefore p}$ (7) $\dfrac{p}{\therefore p \vee q}$ (8) $\dfrac{\begin{matrix} p \to r \\ q \to r \end{matrix}}{\therefore (p \vee q) \to r}$ Rule for proof by cases

Ex Show that $\dfrac{\begin{matrix} p \\ q \to r \\ r \to \neg p \end{matrix}}{\therefore \neg q}$. Solution 1: Write truth table for $(p \wedge (q \to r) \wedge (r \to \neg p)) \to \neg q$ is always 1.

Solution 2:

| Step | A true statement | Reason |
|---|---|---|
| 1 | $p$ | Premise |
| 2 | $q \to r$ | Premise |
| 3 | $r \to \neg p$ | Premise |
| 4 | $\neg\neg p$ | Double negation applied on step 1. |
| 5 | $q \to \neg p$ | Rule of Syl. applied to step 2, 3. |
| 6 | $\neg q$ | Modus Tollens applied on step 4 and 5. |

$\dfrac{\begin{matrix} x \to y \\ \neg y \end{matrix}}{\therefore \neg x}$ $x = q$, $y = \neg p$

Solution 3:

| | | |
|---|---|---|
| 1 | $p$ | Premise |
| 2 | $r \to \neg p$ | Premise |
| 3 | $\neg r$ | Modus Tollens on 1, 2. |
| 4 | $q \to r$ | Premise |
| 5 | $\neg q$ | Modus Tollens on 3, 4. |

$\dfrac{\begin{matrix} x \\ y \to \neg x \end{matrix}}{\neg y}$ Second ver. of Modus Tollens

Subject: Date: ..../..../....

**Definition:** An open statement is a declarative sentence which is not a statement but contains one or more variables and it becomes a statement when the variables in it are replaced by certain allowable choices.

**Ex** $P(x) = $ "$x < 5$" and Universe = Integers $\Rightarrow$ $P(2)$ is true, $P(8)$ is false

**Definition:** Let $p(x)$ be an open statement, then we can use quantifiers to obtain two statements as follows:

| Name of quantifier | Notation | Read | Meaning |
|---|---|---|---|
| existential | $\exists x\, p(x)$ | there exist $x$ such that $p(x)$<br>for some $x$, $p(x)$ | $\exists x\, p(x)$ is true when for some (at least one) $a$ in the universe $p(a)$ is true. |
| universal | $\forall x\, p(x)$ | for all $x$, $p(x)$<br>for any $x$, $p(x)$<br>for every $x$, $p(x)$<br>for each $x$, $p(x)$ | $\forall x\, p(x)$ is true when for every $a$ in the universe $p(a)$ is true. |

**Ex** If Universe = Integers, $p(x) = $ "$x > 5$", $q(x) = $ "$x < 8$" then,

$\exists x\, p(x)$ is true because $p(6)$ is true and 6 is an integer.

$\forall x\, p(x)$ is false because $p(4)$ is false.

$\forall x\, (p(x) \vee \neg p(x))$ is true by Inverse Law.

$\exists x\, (p(x) \wedge q(x))$ is true because $p(6)$ and $q(6)$ are both true.

$\forall x\, (p(x) \vee q(x))$ is true because $x > 5$ or $x \leq 5 < 8$.

**Ex** $\exists x\; x^2 = -1$ is false when universe = real numbers

$\exists x\; x^2 = -1$ is true when universe = complex numbers

**Ex** If universe = integers then; $\forall x\, \exists y\, (y < x)$ is true because given $x$, we can take $y = x-1$

$\exists x\, \forall y\, (y < x)$ is false because $y = x+1$ can be given.

**Ex** Universe = Real Numbers $p(x) = $ "$x^2 - 4 = 0$" $q(x) = $ "$(x+5)(x-3) = 0$" $r(x) = $ "$(x-2)^2 = 0$"

$\exists x\, (p(x) \wedge q(x))$ is false $p(x)$ is true only $x = 2$, $x = -2$ however $q(2)$ is false and $q(-2)$ is false.

$(\exists x\, p(x)) \wedge (\exists x\, q(x))$ is true because we interprete this as true $\wedge$ true.

$\forall x\, (p(x) \rightarrow r(x))$ is false because if we take $x = -2$ true $\rightarrow$ false $\Leftrightarrow$ false

$\forall x\, (r(x) \rightarrow p(x))$ is true because $r(x)$ is true only $x = 2$, and $p(2) =$ true.

Subject :  Date ....../....../......

Ex Universe = Integers , $(\forall x\,(x<5)) \vee (\forall x\,(x \geq 5))$ is false. } Not equivalent.
$(\forall x\,(x<5)) \vee ((x\geq 5))$ is true.

⊛ $\forall x\,(p(x) \wedge q(x))$ is logically equivalent to $\forall x\, p(x) \wedge \forall x\, q(x)$.
⊛ $\exists x\,(p(x) \vee q(x))$ is logically equivalent to $\exists x\, p(x) \vee \exists x\, q(x)$. ] Vice versa is not log. eq.
⊛ $\neg \forall x\, p(x)$ is logically equivalent to $\exists x\, \neg p(x)$
⊛ $\neg \exists x\, p(x)$ is logically equivalent to $\forall x\, \neg p(x)$

Ex $\neg \forall x\, \exists y\; p(x,y) \wedge q(x,y) \Longleftrightarrow \exists x\, \forall y\, (\neg p(x,y)) \vee (\neg q(x,y))$

Notation: When the universe is a number system: $\exists x > a\; p(x)$ means $\exists x\, (x>a) \wedge p(x)$
$\forall x > a\; p(x)$ means $\forall x\, (x>a) \rightarrow p(x)$

$\boxed{\text{Fact}}$ $\neg(p \rightarrow q) \Longleftrightarrow (p \wedge \neg q)$ because, $(p \rightarrow q) \Longleftrightarrow (\neg p \vee q)$

⊛ Ex Show that $\neg \forall x > a\; p(x)$ is logically equivalent to $\exists x > a\; \neg p(x)$.

$\neg \forall x > a\; p(x) \Longleftrightarrow \neg \forall x\,(x>a) \rightarrow p(x) \Longleftrightarrow \exists x\,(x>a) \wedge \neg p(x) \Longleftrightarrow \exists x > a\; \neg p(x)$

⊛ Ex Show that $\neg \exists x > a\; p(x)$ is logically equivalent to $\forall x > a\; \neg p(x)$

$\neg \exists x > a\; p(x) \Longleftrightarrow \neg \exists x\, (x>a) \wedge p(x) \Longleftrightarrow \forall x\, \neg(x>a) \vee \neg p(x) \Longleftrightarrow \forall x\,(x>a) \Rightarrow \neg p(x)$
$\Longleftrightarrow \forall x > a\; \neg p(x)$

Ex Show that $\lim_{x\to 0} \frac{|x|}{x}$ doesn't exist. Universe = real numbers.

$\lim_{x\to a} f(x)$ exists means: $\exists L\; \forall \varepsilon > 0\; \exists d > 0\; \forall x\; 0<|x-a|<d \rightarrow |f(x)-L| < \varepsilon$

$\lim_{x\to 0} \frac{|x|}{x}$ doesn't exists means: $\forall L\; \exists \varepsilon > 0\; \forall d > 0\; \exists x\; 0<|x-0|<d \wedge \left|\frac{|x|}{x} - L\right| \geq \varepsilon$ is true. $d = \frac{1}{2}$ not

⊛ Remember $\forall x\, p(x) \vee \forall x\, q(x)$ is not logically equivalent to $\forall x\,(p(x) \vee q(x))$
$\exists x\, p(x) \wedge \exists x\, q(x)$ is not logically equivalent to $\exists x\,(p(x) \wedge q(x))$

Logical Implications:

① $\dfrac{\forall x\, p(x) \vee \forall x\, q(x)}{\therefore \forall x\,(p(x) \vee q(x))}$

② $\dfrac{\exists x\,(p(x) \wedge q(x))}{\therefore \exists x\, p(x) \wedge \exists x\, q(x)}$

Ex) Show that

Premises:
1. $\forall x\,(p(x) \vee q(x))$
2. $\exists x\, \neg p(x)$
3. $\forall x\, (\neg q(x) \vee r(x))$
4. $\forall x\, s(x) \rightarrow \neg r(x)$

$\therefore \exists x\, \neg s(x)$

③ Rule of Universal Specification: $\forall x\, p(x) \Rightarrow p(a)$
④ Rule of Universal Generalization: $\{p(a) \mid E\} \Rightarrow \forall p(x)$
⑤ Rule of Existential Specification: $\exists x\, p(x) \Rightarrow p(a_0)$
⑥ Rule of Universal Generalization: $p(a) \Rightarrow \exists x\, p(x)$

| Step | A true statement | Reason |
|---|---|---|
| 5 | $\neg p(a_0)$ | Existential specification applied on 2. |
| 6 | $p(a_0) \vee q(a_0)$ | Univeral specification applied on 1. |
| 7 | $\neg p(a_0) \rightarrow q(a_0)$ | Apply $[z \rightarrow w \Leftrightarrow \neg z \vee w]$ fact on 6. |
| 8 | $q(a_0)$ | Modus Ponens applied on steps 5 and 7. |
| 9 | $\neg q(a_0) \vee r(a_0)$ | Universal Specification applied on 3. |
| 10 | $q(a_0) \rightarrow r(a_0)$ | Apply the [if fact] on step 9. |
| 11 | $r(a_0)$ | Modus Ponens on 8 and 10. |
| 12 | $s(a_0) \rightarrow \neg r(a_0)$ | Universal Specification applied on 4. |
| 13 | $\neg s(a_0)$ | Modus Tollens applied on 11 and 12. |
| 14 | $\exists x\, \neg s(x)$ | Existential Generalization applied on 13. |

## Chapter 3)

Definition: A set is a well-defined collection of objects in a specified universe.

Notation: $\{a \mid p(a)\}$ = The set of objects in the universe whic satisfies $p(x)$.

Notation: $S = \{a_1, a_2, a_3 \ldots\}$ means $\forall x\,(x \in S) \longleftrightarrow ((x = a_1) \vee (x = a_2) \vee \cdots)$

Ex) If universe = Integers, then $\{x \mid 2 \leq x \leq 6\} = \{2, 3, 4, 5, 6\}$

| Notation | Read | Meaning |
|---|---|---|
| $A \cup B$ | A union B | $\{x \mid (x \in A) \vee (x \in B)\}$ |
| $A \cap B$ | A intersection B | $\{x \mid (x \in A) \wedge (x \in B)\}$ |
| $A - B$ | A minus B | $\{x \mid (x \in A) \wedge (x \notin B)\}$ |
| $A \times B$ | A times B | $\{(x, y) \mid (x \in A) \wedge (y \in B)\}$ |
| $P(A)$ | Power set of A | $\{u \mid u \subseteq A\}$ |
| $\bar{A}$ | comlement of A | $\{x \mid x \notin A\}$ |

Subject: Date: ..../..../....

(☆) If universe = sets, this means everything (reals, integers, tuples...).

Ex) Universe $= U = \{1, 2, 3, 4, 5\}$ and $A = \{2, 3\}$ then, $\{1, 4, 5\}$

Definition: Given two sets A, B. We define three statements as follows:

$A \subseteq B$ means $\forall x\ (x \in A) \rightarrow (x \in B)$

$A = B$ means $(A \subseteq B) \wedge (B \subseteq A)$

$A \subset B$ means $(A \subseteq B) \wedge (\neg(A = B))$

When $A \subseteq B$ is true we say A is subset of B.

When $A \subset B$ is true we say A is a proper subset of B.

Laws of Set Theory

① $\overline{\overline{A}} = A$ Law of double complement ② $\overline{A \vee B} = \overline{A} \wedge \overline{B}$ De'Morgans Law ... similar to Laws of Logic

Proofs are similar like $p \wedge q$ corresponds $x \in (A \wedge B)$.

Ex) Simplify the set $X = ((A \cap B) \cup (A \cap (B \cap (\overline{C} \cap D)))) \cup (\overline{A} \cap B)$

$$X \overset{\text{dist. law}}{=} (A \cap (\underbrace{B \cup (B \cap (\overline{C} \cap D))}_{\text{absorption laws} \Rightarrow = B})) \cup (\overline{A} \cap B) = (A \wedge B) \cup (\overline{A} \cap B)$$

$$X \overset{\text{dist. law}}{=} B \cap (\underbrace{A \cup \overline{A}}_{U}) \overset{\text{inverse law}}{=} B \wedge U \overset{\text{identity law}}{=} B$$

Definition: If A is a finite set then $|A|$ = number of elements in A.

Section 3.4 - 3.5) : universe $\longleftrightarrow$ sample space for an experiment

set $\longleftrightarrow$ event

Definition: Let S be a sample space for an experiment and assume for every event A, we have a $Pr(A)$. Then we say $Pr(A)$ is probability of A if:

① $Pr(S) = 1$ ② if $A \wedge B = \emptyset$ then $Pr(A \vee B) = Pr(A) + Pr(B)$ ③ $Pr(A) \geq 0$

These was the axioms of probability. (for every A, B events.)

Fact: $Pr(\overline{A}) = 1 - Pr(A)$ Proof: $\underbrace{1 = Pr(S)}_{1^{st}\text{ axiom}} \overset{\text{inverse law}}{=} Pr(\underbrace{\overline{A} \vee A}_{\overline{A} \wedge A = \emptyset}) \overset{2^{nd}\text{ axiom}}{=} Pr(\overline{A}) + Pr(A)$

Subject : Date : ....../....../......

Fact: $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$

Proof: $Pr(A \cup B) = Pr(A) + Pr(B - A\cap B)$ $\quad$ $Pr(B) = Pr(B - A\cap B) + Pr(A \cap B)$

$A \cup B = A \cup (B - A\cap B)$ $\quad$ $B = (B - A\cap B) \cup (A \cap B)$

$A \cap (B - A\cap B) = \emptyset$ $\quad$ $(B - A\cap B) \cap (A \cap B) = \emptyset$

So $Pr(B - A\cap B) = Pr(B) - Pr(A \cap B)$. Hence $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$

Ex| Suppose a coin is loaded to come up heads twice as often as it comes up tails. If we toss the coin once, find the probability of getting heads.

$S = \{H, T\}$ $\quad$ $A = \{H\}$ $\quad$ $B = \{T\}$ $\quad$ So we have $A \cap B = \emptyset$

$1 \overset{\text{1st Axiom}}{=} Pr(S) = Pr(A \cup B) \overset{\text{2nd Axiom}}{=} Pr(A) + Pr(B)$ , $Pr(A) = 2 \cdot Pr(B)$

Hence, $1 = Pr(B) + 2Pr(B) \implies Pr(B) = \frac{1}{3}$, $Pr(A) = \frac{2}{3}$. Then answer is $\frac{2}{3}$

Definition: Assume $S$ is the sample space for an expriment and $S$ is finite. For any event $A$, we define fair probability as: $Pr(A) = \frac{|A|}{|S|}$

Ex| Assume we have a fair die and let $A$ be the event that we get an even number and $B$ be the event that we get 4 or 5 when we roll once.

$S = \{1, 2, 3, 4, 5, 6\}$ $\quad$ $A = \{2, 4, 6\}$ $\quad$ $B = \{4, 5\}$

$Pr(A) = \frac{|A|}{|S|} = \frac{3}{6} = \frac{1}{2}$ $\quad$ $Pr(B) = \frac{|B|}{|S|} = \frac{2}{6} = \frac{1}{3}$

Ex| Assume that we have a fair coin. If we toss this coin four times, let $A$ be the event that we get two heads and two tails.

$S = \{HHHH, HHHT \ldots\ldots TTTT\}$ $\quad$ $|S| = 2^4 = 16$

$A = \{HHTT, HTHT \ldots\ldots TTHH\}$ $\quad$ $|A| = \frac{4!}{2!2!} = 6$ $\implies \frac{|A|}{|S|} = \frac{6}{16} = \frac{3}{8}$

Ex| If one number is selected at random from $\{1, 2, 3, 4, 5\}$, what is the probability the number is even? $\underbrace{\text{at random}}_{\text{Fair Probability}}$

$S = \{1, 2, 3, 4, 5\}$ , $A = \{2, 4\}$ $\implies \frac{|A|}{|S|} = \frac{2}{5}$

Subject : Date : ....../....../......

## Chapter 4)

The well-ordering principle: A non-empty subset of $\mathbb{Z}^+$ contains a smallest element.

Ex) $A = \{n \mid (n \in \mathbb{Z}^+) \wedge (n^2 > 3)\}$ has the smallest element 2.

Ex) $\{n \mid (n \in \mathbb{Z}^+) \wedge (n^2+1=0)\}$ has no smallest element because it's empty.

Ex) $\{x \mid (x \in \mathbb{R}) \wedge (x > 2)\}$ has no smallest element.

The principle of mathematical induction: Let $S(n)$ be an open statement.

Then
$$\begin{array}{l} S(1) \\ \forall n \in \mathbb{Z}^+ \quad S(n) \rightarrow S(n+1) \\ \hline \therefore \forall n \in \mathbb{Z}^+ \quad S(n) \end{array}$$

Proof: Assume $S(1)$ is true and $\forall n \in \mathbb{Z}^+ \; S(n) \rightarrow S(n+1)$ is true. Then define $A = \{n \mid (n \in \mathbb{Z}^+) \wedge (S(n) \text{ is false})\}$. We're trying to show that $A = \emptyset$. Then $A$ contains a smallest element say $n_0$. Now $n_0 \neq 1$ because $S(1)$ is true so $(n_0 - 1)$ is in $\mathbb{Z}^+$. But $(n_0-1) \notin A$ because $(n_0-1) < n_0$. Therefore $S(n_0 - 1)$ is true. Notice we know $S(n_0-1) \rightarrow S(n_0)$ is true because $\forall n \in \mathbb{Z}^+ \; S(n) \rightarrow S(n+1)$ is true. Hence $S(n_0)$ is not true. This is a contradiction. So $A = \emptyset$.

Use of mathematical induction: ① Define $S(n)$. ② Prove $S(1)$ is true. ③ Assume $S(n)$ is true. ④ Prove $S(n+1)$ is true. Say that "We are done by math. induction."

Ex) Prove that $1+2+\ldots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{Z}^+$

① $S(n) =$ "$1+2+\ldots+n = \frac{n(n+1)}{2}$". ② $S(1) =$ "$1 = \frac{1+1}{2}$" is true.

③ Assume $S(n)$ is true, then $1+2+\ldots+n = \frac{n(n+1)}{2}$

④ prove this

$S(n+1) =$ "$1+2+\cdots n+n+1 = \frac{(n+1)(n+2)}{2}$" $\Rightarrow$ "$\frac{n(n+1)}{2} + n+1 = \frac{(n+1)(n+2)}{2}$" $\Rightarrow$ "$\underbrace{n^2+3n+2 = n^2+3n+1}_{\text{true}}$"

We are done by mathematical induction.

Ex) Prove that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n$ in $\mathbb{Z}^+$.

Subject : Date : ...../...../......

① $S(n) = $ " $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ " ② $S(1) = $ " $1 = \frac{1 \cdot 2 \cdot 3}{6}$ " is true.

③ Assume $S(n)$ is true. ④ Prove $S(n+1)$ is true. $S(n+1) = $ " $\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+2)}{6}$ "

$\sum_{i=1}^{n} i^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6} \Rightarrow \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} = \frac{(n+1)(n(2n+1)+6(n+1))}{6} =$

$\frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$ --> So $S(n+1)$ is true. We can say that $S(n)$ is true for all $n$ in $Z^+$ by Mathematical induction.

A more general version of Mathematical Induction:

$$\frac{\begin{array}{l} S(n_0) \\ \forall n > n_0 \quad S(n) \to S(n+1) \end{array}}{\therefore \forall n \geq n_0 \quad S(n)}$$

Assume Universe $= Z^+$ and $n_0 \in Z^+$. Then;

⭐ To use this version, we just prove $S(n_0)$ instead of $S(1)$ at step ②. On step ③, also assume $n \geq n_0$ with $S(n)$

Ex| Prove that for all $n \in Z^+$ if $n \geq 5$ then $n^2 < 2^n$.

① $S(n) = $ " $n^2 < 2^n$ " ② $S(5) = $ " $5^2 < 2^5$ " is true.

③ Assume $n \geq 5$ and $S(n)$ is true. Then,

④ $(n+1)^2 = n^2 + 2n + 1 < 2^n + 2n + 1 \leq 2^n + 3n < 2^n + n^2 < 2^n + 2^n = 2^{n+1}$

because $S(n)$ is true; because $n \geq 5 \Rightarrow n > 1$; because $n \geq 5 \Rightarrow n > 3$; because $S(n)$

Since $(n+1)^2 < 2^{n+1}$ is true, $S(n)$ is true for all $n \geq 5$ by Math. Induction.

The most general version of Mathematical Induction:

$$\frac{\begin{array}{l} S(n_0) \wedge S(n_0+1) \cdots S(n_1) \\ \forall n > n_1 \ (S(n_0) \wedge S(n_0+1) \wedge \cdots S(n)) \to S(n+1) \end{array}}{\therefore \forall n \geq n_0 \quad S(n)}$$

Assume Universe $= Z^+$ and $n_0 \in Z^+$, $n_1 \in Z^+$, $n_0 < n_1$

To use this version, we prove $S(n_0), S(n_0+1), \ldots S(n_1)$ at step ②.

On step ③ also assume $n \geq n_1$ *, $S(n_0), S(n_0+1), \ldots S(n)$ is true.

Ex| Define $a_1 = 1$, $a_2 = 3$, $a_3 = 7$, $a_4 = 11$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3} + a_{n-4}$ when $n \geq 5$. Then show that $\underbrace{a_n \leq 2^n \text{ for all } Z^+}_{n \geq 1 \to n_0}$.

$n \geq 1$

$n_0 = 1$

① $S(n) = "a_n \leq 2^n"$

② $S(1) = "1 < 2"$ is true

$S(2) = "3 < 4"$ is true

$S(3) = "7 < 8"$ is true

$S(4) = "11 < 16"$ is true

③ Assume $n \geq 4$ and $S(1)$ is true, $S(2)$ is true ... $S(n)$ is true.

$a_{n+1} = a_n + a_{n-1} + a_{n-2} + a_{n-3} \leq 2^n + 2^{n-1} + 2^{n-2} + 2^{n-3} \leq \circledast$

because $n \geq 4 \rightarrow n+1 \geq 5$

because $S(n) \rightarrow a_n \leq 2^n$, $S(n-1) \rightarrow a_{n-1} \leq 2^{n-1}$, $S(n-2) \rightarrow a_{n-2} \leq 2^{n-2}$, $S(n-3) \rightarrow a_{n-3} \leq 2^{n-3}$

$\circledast = 2^n + 2^{n-1} + 2^{n-2} + 2^{n-3} + 2^{n-4} \cdots + 2^0 = 2^{n+1} - 1 \leq 2^{n+1}$ So $S(n+1)$ is true.

We can say that $S(n)$ is true for all $Z^+$ by Math. Induction.

Ex| Prove that its possible to write $n$ as sum of 3's and/or 8's for every $n \geq 14$ and $n \in Z^+$.

$n_0 = 14$

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

$n, n-1, n-2$

$n \geq 16$ $n_1 = 16$

① $S(n) =$ "$n$ can be written as a sum of 3's and/or 8's."

② $S(14)$ is true $14 = 8+3+3$

$S(15)$ is true $15 = 3+3+3+3+3$

$S(16)$ is true $16 = 8+8$

③ Assume $n \geq 16$ and $S(14) \wedge S(15) \wedge \cdots \wedge S(n)$ is true.

$S(n+1) \Rightarrow (n+1) = (n-2) + 3 \rightarrow$ Can be written as a sum of 3's and 8's because $S(n-2)$ is true.

So $S(n)$ is true for all $n \geq 14$ by Mathematical Induction

Ex| Consider the following program segment. Prove that the output is $(n-1)!$ when the input is $n \geq 1$.

```
n = input
x = 1
y = 1
while y ≠ n do
    x = x * y
    y = y + 1
output x
```

① $S(n) =$ "output is $(n-1)!$ when input is $n$"

② $S(1)$ is true because $0! = 1$.

③ Assume $S(n)$ is true. Before we go into while loop last time, we have $x = (n-1)!$ and $y = n$ because $S(n)$ is true. So at the end of the last while loop, we will have $x = (n-1)! \cdot n = n!$ and $y = n+1$ Hence $S(n+1)$ is true

Therefore $S(n+1)$ is true for all $n \geq 1$.

Subject : Date :

Ex) Consider the following program segment.

```
n = input
i = 0
j = -1
while (j < 0)
    if (3 divides n) and (n >= 0) then j = n/3
    else i = i+1 ; n = n-8
Output (i, j)
```

Show that this program segment always stops in finite time when input $\geq 14$

$S(n)$ = " the prog. seg. stops in finite time when input is $n$ "

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

we want this to be true

$n-7 \geq 14$

$n \geq 21$

$S(14)$ is true
$S(15)$ is true
⋮
$S(21)$ is true

Proven. Then

Assume $n \geq 21$ and $S(14) \wedge S(15) \wedge \dots S(n)$ is true. Then $S(n+1)$ is true because $S(n+1-8) = S(n-7)$ is true. ✓

Ex) Assume $f$ is a computer procedure which takes an input $n$ and gives an output denoted $f(n)$ as follows.

$n$ = input

if $n > 0$ then output $n^5 + \sum_{i=1}^{n-1} f(i)$

else output 1.

Prove that

$f(n) \leq n^{6+n}$ for all $n \geq 1$

① $S(n)$ = " $f(n) \leq n^{6+n}$ " ②

Section 4.3, 4, 5)

Definition: Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then we say $b$ divides $a$ and write $b \mid a$ if $\exists n \in \mathbb{Z}$ $b \cdot n = a$.

Ex) $3 \mid 6$ is true because $3 \cdot 2 = 6$ and 2 is an integer.

$-5 \mid 10$ is true because $(-5)(-2) = 10$ and $(-2)$ is an integer.

$6 \mid 0$ is true because $6 \cdot 0 = 0$ and 0 is an integer.

$5 \mid 7$ is false. $3 \mid 4$ is false.

Subject :

Date : ....../....../......

Fact: Assume $a$, $b$, $c$ are integers. Then,

(i) $1 \mid a$ (ii) $(a \neq 0) \rightarrow (a \mid 0)$ (iii) $((a \mid b) \wedge (b \mid c)) \rightarrow (a \mid c)$

(iv) $((a \mid b) \wedge (a \mid c)) \rightarrow (\forall x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ (a \mid bx + cy))$

Ex) Can we find two integers $x$, $y$ such that $107 = 6x + 15y$

No, because by Fact (iv), $3 \mid 6x + 15y$ however $3 \nmid 107$. → $b \nmid a \iff \neg(b \mid a)$

Notation: $D(n) = \{m \in \mathbb{Z}^+ \mid m \mid n\}$

Definition: We say a positive integer $p$ is a prime number if $|D(p)| = 2$

Definition: We say a positive integer $n$ is a composite number if $|D(p)| \geq 3$

Fact: ($n$ is not a prime) $\iff$ ($n$ is composite) when $n \in \mathbb{Z}^+$ and $n \neq 1$

Lemma: $\forall n \in \mathbb{Z}^+$ ($n$ is composite) $\longrightarrow$ ($\exists p$ prime $p \mid n$) $\quad \neg(x \rightarrow y)$, $\neg(\neg x \vee y)$, $x \wedge \neg y$

Proof: Suppose not: $\exists n \in \mathbb{Z}^+$ ($n$ is composite) $\wedge$ ($\forall p$ prime $p \nmid n$)

Lets consider these: $S \neq \emptyset$; $S = \{n \in \mathbb{Z}^+ \mid (n \text{ is composite}) \wedge (\forall p \text{ prime } p \nmid n)\}$

By well-ordering principle there's a smallest element say $n_0$. So there exist $m_0 \in D(n_0)$ such that $1 < m_0 < n_0$ because $|D(n_0)| \geq 3$.

Notice $m_0 \notin S$ because $m_0 < n_0$. In case $m_0$ is a prime, we get a contradiction because $m_0 \mid n_0$. In case $m_0$ is not a prime, we know that there exist $p_0$ a prime number which divides $m_0$ because $m_0 \notin S$. This give contradiction since $p_0 \mid m_0$ and $m_0 \mid n_0$ implies $p_0 \mid n_0$.

Theorem (Euclid): There are infinitely many primes.

Proof: Suppose not: There exist $n$ a (finite) positive integer and $\{p_1, p_2 \cdots p_n\}$ is the set of all prime numbers. Then $p_1 p_2 \cdots p_n + 1$ is not a prime. So $p_1 p_2 \cdots p_n + 1$ is a composite number. By lemma, there exist a $p_i$ which divides $p_1 p_2 \cdots p_n + 1$. This is a contradiction because $\forall i\ p_i \nmid p_1 p_2 \cdots p_n + 1$ since $p_i \mid p_1 p_2 \cdots p_n$ but $p_i \nmid 1$.

Notation: $\exists! x\ p(x)$ means there exists a unique $x$ such that $p(x)$ is true.

Theorem (Division Algorithm):

$\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ (b>0) \rightarrow (\exists! q \in \mathbb{Z}\ \exists! r \in \mathbb{Z}\ (a = bq + r) \wedge (0 \leq r < b))$

Proof: Define $S = \{a - bx \mid (x \in \mathbb{Z}) \wedge (a - bx \geq 0)\}$ Then $S \neq \emptyset$ ← exercise, use $b \neq 0$

So $S$ has a smallest element say $r$. Then $r = a - bq$ for some $q$ in $\mathbb{Z}$.

Suppose $r \geq b$, then $0 \leq r - b = a - bq - b = a - b(q+1) = r - b < r$

because $r \geq b$ — because $b > 0$

This is a contradiction

$a - b(q+1) \notin S$. So $r < b$. Hence $a = bq + r$ and $0 \leq r < b$.

Assume $bq_1 + r_1 = a = bq_2 + r_2$ and $0 \leq r_1, r_2 < b$

Then $(bq_1 + r_1) - (bq_2 + r_2) = a - a = 0$ so $bq_1 - bq_2 = r_2 - r_1$

Therefore $b \cdot |q_1 - q_2| = |r_1 - r_2| < b$ because $0 \leq r_1, r_2 < b$. Therefore $q_1 = q_2$ and $r_1 = r_2$.

(*) $\begin{array}{c|c} a & b \\ \hline -\ \ r & q \end{array}$ } $a$ and $b$ are inputs. Division algorithm always gives unique outputs $r$ and $q$.

(*) If $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ and $b \geq 2$ then there exist unique $n, r_0, r_1, \dots, r_n$ such that $\forall i\ 0 \leq r_i < b$ and $a = r_0 + r_1 b + r_2 b^2 + \dots + r_n b^n$

Idea of Proof: $a = r_0 + q_1 b$ $q_1$ is unique, $r_0$ is unique.

$q_1 = r_1 + q_2 b$ $q_2$ is unique, $r_1$ is unique.

Note: In the above example we say $a$ is equal to $r_n r_{n-1} r_{n-2} \cdots r_2 r_1 r_0$ in base $b$.

Definition: For $a, b$ in $\mathbb{Z}$ we say $c$ is a common divisor of $a$ and $b$ if ($c$ is a positive integer) and $(c \mid a)$ and $(c \mid b)$.

Definition: For $a, b$ in $\mathbb{Z}$ we say $c$ is the greater common divisor of $a, b$ and write $\gcd(a, b) = c$.

if (i) $c$ is a common divisor of $a$ and $b$

and (ii) if $d$ is a common divisor of $a$ and $b$ then $d \mid c$.

Subject :

Date :......./......./.......

Why there's only one greatest common divisor of $a, b$.

Assume $c_1 = \gcd(a,b)$ , $c_2 = \gcd(a,b)$ Then we know by definition:

$c_1 \mid c_2$ and $c_2 \mid c_1 \implies c_1 = c_2$ by the following fact:

$\rightarrow x_1 \mid x_2 \wedge x_2 \mid x_1 \implies |x_1| = |x_2|$ and $c_1 > 0$ $c_2 > 0$

Why there's alway a gcd of $a, b$.

Define $S = \{ax + by \mid (x \in \mathbb{Z}) \wedge (y \in \mathbb{Z}) \wedge (ax+by>0)\}$

Notice $S \neq \emptyset$ because $a \in S$ consider $x=1$ and $y=0$

We have $S \subseteq \mathbb{Z}^+$. So there exist a smallest element $c$ in $S$.

If $d \mid a$ and $d \mid b$ then $d \mid ax_0 + bx_0$ where $c = ax_0 + by_0$. This means $d \mid c$

Suppose $c \nmid a$. Then $a = qc + r$ where $0 < r < c$ by Division alg.

This is a contradiction $r = a - qc = a - q(ax_0 + by_0) = (1 - qx_0)a + (-qy_0)b \in S$ and $r < c$

Ex $\exists x \exists y \; 15x + 13y = 10151$ is true because $\gcd(15, 13) = 1$

So we know $\exists x_0 \exists y_0 (x_0 + y_0 = 1)$. Take $x = x_0 \cdot 10151$ , $y = y_0 \cdot 10151$

Theorem (Euclidean Algorithm): Let $a, b \in \mathbb{Z}^+$. Assume $b < a$.

Define $r_0 = a$ , $r_1 = b$ , $r_n = q_{n+1} r_{n+1} + r_{n+2}$ and $0 < r_{n+2} < r_{n+1}$ for $n \geq 0$.

If $r_k \neq 0$ and $r_{k+1} = 0$ then $\gcd(a, b) = r_k$

Ex $\gcd(250, 111) \implies$

$$250 = 2 \cdot 111 + 28 \qquad r_2 = 28$$
$$111 = 3 \cdot 28 + 27 \qquad r_3 = 27$$
$$28 = 1 \cdot 27 + 1 \qquad r_4 = 1 \rightarrow \gcd = 1$$
$$27 = 27 \cdot 1 + 0 \qquad r_5 = 0$$

Ex Does there exist a positive integer $n$ such that $\gcd(8n+3, 5n+2) \neq 1$

$\gcd(11, 7) = 1 \implies n \neq 1$

$\gcd(19, 12) = 1 \implies n \neq 1$

$$8n+3 = 1 \cdot (5n+2) + (3n+1)$$
$$5n+2 = 1 \cdot (3n+1) + (2n+1)$$
$$3n+1 = 1 \cdot (2n+1) + n$$
$$\left.\begin{aligned} 2n+1 &= 2 \cdot n + 1 \\ n &= n \cdot 1 + 0 \end{aligned}\right\} \underbrace{\gcd(8n+3, 5n+2) = 1}_{\text{There isn't any.}}$$

Subject : Date : ...../...../.....

Exercise: Define lcm$(a,b)$ as least common multiple.
Show $a \cdot b = \text{lcm}(a,b) \cdot \gcd(a,b)$ for every $a, b \in \mathbb{Z}^+$

Lemma: $\forall a \in \mathbb{Z}^+ \ \forall b \in \mathbb{Z}^+ \ \forall p$ prime $(p \mid ab) \to ((p \mid a) \vee (p \mid b))$

Proof: Assume $p \mid ab$ and $p \nmid a$. Then we need to show $p \mid b$.

$A \to (B \vee C) \iff (\neg A) \vee (B \vee C) \iff \neg(A \wedge \neg B) \vee C \iff (A \wedge \neg B) \to C$

Notice $\gcd(p,a) = 1$ because $p \nmid a$ and $p$ is prime.

So there exist $x_0, y_0 \in \mathbb{Z}$ such that $px_0 + ay_0 = 1$

So $b = b(px_0 + ay_0) = pbx_0 + aby_0$. We also know $p \mid p$ and $p \mid ab$ so $p \mid b$.

Theorem: Every integer $n > 1$ can be written as product of primes uniquely up to the order of the primes. [Fundamental Theorem of Arithmetic]

Idea of proof: Existance: $S = \{n > 1 \mid n$ cannot be written as product of primes$\}$

Suppose $S \neq \emptyset$. Then there exist a smallest element $n_0$ in $S$.

Case $n_0$ is prime: $n_0 = n_0$, then this is a contradiction.

Case $n_0$ is not prime: $n_0 = m_1 \cdot m_2$ and $1 < m_1 < n_0$, $1 < m_2 < n_0$

$m_1 \notin S$, $m_2 \notin S$. So $m_1 = \underbrace{p_1 \cdot p_2 \cdots p_l}_{\text{product of primes}}$ $m_2 = \underbrace{q_1 q_2 \cdots q_s}_{\text{product of primes}}$

This is a contradiction because $n_0 = m_1 \cdot m_2 = p_1 \cdots p_l \cdot q_1 \cdots q_s$

Uniqueness: $p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_s$. By previous lemma, $p_1 \mid q_i$ for some $i$, $p_2 \mid q_j$ for some $j$

Ex) Find the number of positive divisors of $2^3 \cdot 5^2 \cdot 7^4$.

By the f.t.a., every divisor of $2^3 5^2 7^4$ is in form $2^i \cdot 5^j \cdot 7^k$ where $0 \le i \le 3$, $0 \le j \le 2$, $0 \le k \le 4$.

So the answer is $(3+1) \cdot (2+1) \cdot (4+1) = 4 \cdot 3 \cdot 5 = 60$

Ex) Show that $\forall m \in \mathbb{Z}^+ \ \forall n \in \mathbb{Z}^+ \ m(m+1)(m+2) \neq n^2$

by Euc. Alg.

Suppose $m(m+1)(m+2) = n^2$ for some $m, n$. Notice $\gcd(m, m+1) = 1$, $\gcd(m+1, m+2) = 1$

If $p \mid m+1$ and $p$ is prime, then $p \nmid m$ and $p \nmid m+2$. This means $p^2 \mid m+1$ should be true because of "$= n^2$" part.

Subject : Date ..../..../....

Then divide both sides with all prime that divide $(m+1)$ we get $m(m+2) = s^2$ for some $S$ in $\mathbb{Z}^+$. This is a contradiction: $m^2 < m(m+1) < (m+1)^2$

(iii) $\exists x \exists y \; ax + by = 1 \Leftrightarrow \gcd(a,b) = 1$ | $\gcd(a,b) = c \Rightarrow \exists x \exists y \; ax + by = c$

any number $(1 \cdot k)$

## Chapter 5)

Definition: A relation from A to B is a subset of $A \times B$.

Definition: A relation on A is a relation from A to A.

Notation: If R is relation and $(a, b) \in R$ then we write $aRb$.

Ex) $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$

$\{(1,2), (3,4)\}$ is not a relation from A to B because $2 \notin B$

$\{(1,4), (3,5)\}$ is a relation from A to B.

$R = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$ is a relation A.

$1R2$ is true because $(1,2) \in R$ is true.

$3R1$ is false because $(3,1) \notin R$.

Notice $R = \leqslant$

Definition: A function from A to B is a relation f from A to B, which satisfies these following: (i) $\forall a \in A \; \exists b \in B \; (a, b) \in f$

(ii) $\forall a \in A \; \forall b_1 \in B \; \forall b_2 \in B \; ((a, b_1) \in f) \land ((a, b_2) \in f) \rightarrow (b_1 = b_2)$

Notation: If f is a function and $(a,b) \in f$ then we write $f(a) = b$

Note: If you consider f as a procedure then statement (i) in above definition says "for every input in A, there exist an output B" and statement (ii) says "for every input, the output is unique".

Ex) If $A = \{1, 2\}$ $B = \{3, 4, 5\}$ then

$f_1 = \{(1,3)\}$ is not a function from A to B because $2 \in A$ and $\forall x B \; (2, x) \notin f_1$

$f_2 = \{(1, 3), (1, 4), (2, 3)\}$ is not a function from A to B because $(1,3) \in f_2$ and $(1,4) \in f_2$ however $3 \neq 4$

$f_3 = \{(1,3), (2,3)\}$ is a function because the output, can be same.

Subject : Date : ...../...../.....

— Review —

**Ex** Given $n$ many cities. How many round-trip routes are there that visits each city exactly once and returns to the starting city?

Case we have two: $C1 — C2$ $\quad c1 \to c2 \to c1$, $c2 \to c1 \to c2$ $\quad$ 2 routes.

Case we have three: $(c1 \to c2 \to c3 \to c1,\ c1 \to c3 \to c2 \to c1) \times 3 = 6$ routes.

We observe these routes corresponds to permutations $(12, 21), (123, 132 \ldots)$

So in general, number of such routes are $P(n, n) = n!$

**Ex** In how many ways can one select five cards from a deck of 52 such that selection contains ① no hearts: $\binom{52-13}{5} = \binom{39}{5}$ ⓘⓘ At least one hearths: $\binom{52}{5} - \binom{39}{5}$

**Ex** In how many ways can one choose 3 CD's from Top10 List if repeats are allowed.

$n = 10 \quad r = 3 \qquad C(10+3-1, 3) = C(12, 3) = 220 \qquad (x_1 + x_2 + x_3 + \cdots + x_{10} = 3)$

**Ex** For a network system assume that a password consists of 7 chars, the first of which is a letter chosen from $\{A, B, C, D, E, F, G\}$ and the remaining chars can be chosen from Eng alphabet or a digit. Possible passwords: $7 \cdot (26 + 10)^6$

**Ex** How many different seven-person committes can be formed each containing four women from an available set of 30 women and three men from available set of 20 men. $\binom{30}{4} \cdot \binom{20}{3} = 31241700$

**Ex** In how many ways can one go from $(0,0)$ to $(6,6)$ if the only move permitted are $R: (x, y) \to (x+1, y)$ and $U: (x, y) \to (x, y+1)$. $6R, 6U \Rightarrow \frac{(6+6)!}{6! \cdot 6!} = 924$

**Ex** Find the coefficent of $x^5 y^4$ in the expansion $(x+y)^9$. $\frac{9!}{5! \cdot 4!} = 126$

**Ex** counter1 = counter2 = counter3 = 0

```
for n=6 to 11
   for m=4 to 7
      for k=9 to 15
         if (not(n<9) or (m<6)) and (not(k<12) or not(m<6)) and k<12
            if not (n<9)
               counter1++
            else
               counter2++
         else
            counter3++
```

Let $\overset{p}{(n<9)}, \overset{q}{(m<6)}, \overset{r}{(k<12)}$

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

$$(p \to q) \wedge (r \to \neg q) \wedge r$$

First notice counter2 will be 0 after execution.

$$\begin{array}{l} p \to q \\ r \to \neg q \\ r \\ \hline \therefore \neg p \end{array}$$

Then draw a truth table to see $\neg p \wedge \neg q \wedge r$ is logic. equiv...

Then find the numbers of this statement is true. It will be counter1.

Ex) $\forall x \forall y\ x-y=y-x$ is false. $\exists x \exists y\ x-y=y-x$ is true.

$\forall x \exists y\ x-y=y-x$ is true. $\exists x \forall y\ x-y=y-x$ is false.

Ex)
1 $p \to (q \vee r)$
2 $q \to s$
3 $(r \vee t) \to (s \wedge u)$
4 $\neg p \to (t \wedge \neg t)$
$\therefore s \vee t$

$t \wedge \neg t = \text{false}$ (4)
$\neg p = \text{false}$ (4)
$p = \text{true}$ (4)
$(q \vee r)$ is true (1)
$r \to (r \vee t)$ (*)

$(s \wedge u) \to s$ (**)
$r \to s$ (*, 3, **)

Proof by cases: $\begin{array}{l} q \to s \ (2) \\ r \to s \\ q \vee r \\ \hline \therefore s \end{array} \Rightarrow s \vee t$

Ex) Suppose a die is loaded unfairly and probability a given number $i \geq 2$ turns up twice to the number $(i-1)$. If the die is rolled, what is the prob of an even outcome.

$Pr(1)=x$ $Pr(4)=8x$
$Pr(2)=2x$ $Pr(5)=16x$
$Pr(3)=4x$ $Pr(6)=32x$

$1 = Pr(\{1,2,\dots 6\}) = x+2x \dots 32x = 63x \Rightarrow x = \frac{1}{63}$

So $Pr(\{2,4,6\}) = \frac{2}{63} + \frac{8}{63} + \frac{32}{63} = \frac{42}{63}$

— End of Review —

Ex) Count all functions from $\{1,2\}$ to $\{3,4,5\}$. $3 \cdot 3 = 9$

⇒ Number of functions from A to B is $|B|^{|A|}$.

Ex) Number of functions from $\emptyset$ to $\emptyset$ is $0^0 = 1$.

⇒ $\emptyset$ is a function from $\emptyset$ to $\emptyset$, in fact from $\emptyset$ to any set.

⊗ Number of relations from A to B = Subsets of $A \times B = 2^{|A| \cdot |B|}$

<u>Definition</u>: Let f be a function from A to B. Then we say f is one-to-one if $\forall a_1 \in A\ \forall a_2 \in A\ \forall b \in B\ ((a_1,b) \in f \wedge (a_2,b) \in f) \to (a_1 = a_2)$

Ex) Count all functions from $\{1,2\}$ to $\{3,4,5\}$ $3 \cdot 2 = 6$

⇒ Number of one-to-one functions from A to B is $P(|B|, |A|)$

Ex) Number of one-to-one functions from $\emptyset$ to $\emptyset$ is $P(0,0)=1$

Ex) Number of one-to-one functions from $\{1,2,3,4\}$ to $\{5,6\} = P(2,4) = 2 \cdot 1 \cdot 0 \cdot 0$
$= 0$

Subject : Date : ....../....../......

<u>Definition:</u> Let $f$ be a function from $A$ to $B$, then we say $f$ is onto if $\forall b \in B \ \exists a \in A \ (a, b) \in f$.

<u>Ex</u> Count all onto functions from $\{1, 2, 3\}$ to $\{4, 5\}$ $\quad 2^3 - 2 \cdot 1^3 = 6$

$\Rightarrow$ $U$ = set of all functions from $\{1, 2, 3\}$ to $\{4, 5\}$

$A_C = \{f \in U \mid \forall (a, b) \in f \ \ b \notin C\}$ So $A_\emptyset = U$, $A_{\{4\}} = \{\{(1,5), (2,5), (3,5)\}\}$

$A_{\{4,5\}} = A_{\{4\}} \cap A_{\{5\}}$ $\qquad A_{\{4,5\}} = \emptyset$, $A_{\{5\}} = \{\{(1,4), (2,4), (3,4)\}\}$

Set of all onto functions from $\overset{A}{\{1,2,3\}}$ to $\{4, 5\}$ $= A_\emptyset - A_{\{4\}} \cup A_{\{5\}}$

$= |U| - |A_{\{4\}} \cup A_{\{5\}}|$

$= |U| - (\underbrace{|A_{\{4\}}| + |A_{\{5\}}|}_{C(2,1)} - |A_{\{4\}} \cap A_{\{5\}}|$ $\Rightarrow$ $|U| - \binom{2}{1} \cdot |A_{\{4\}}| + |A_{\{4\}} \cap A_{\{5\}}|$

$2^3 - 2 \cdot 1^3 + 0^3 = \ldots$

Number of onto functions from $A$ to $B$: $\displaystyle\sum_{k=0}^{|B|} (-1)^k \cdot \binom{|B|}{|B|-k} \cdot (|B|-k)^{|A|}$

<u>Stirling Numbers:</u> $S(m, n) = \dfrac{1}{n!} \cdot \displaystyle\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{n-k} \cdot (n-k)^m$

$\Rightarrow$ We can say now number of onto funcions from $A$ to $B$: $|B|! \cdot S(|A|, |B|)$

<u>Definition:</u> Let $f$ be a function from $A$ to $B$ and $C \subseteq A$ and $D \subseteq B$

Then (i) $f(C) = \{b \in B \mid \exists a \in C \ \ (a, b) \in f\}$ [image of $C$ under $f$]

(ii) $f^{-1}(D) = \{a \in A \mid \exists b \in D \ \ (a, b) \in f\}$ [preimage of $D$ under $f$]

(iii) $f|_C = \{(a, b) \in f \mid a \in C\}$ [restriction of $f$ to $C$]

<u>Ex</u> $A = \{1, 2, 3\}$ $\quad B = \{4, 5\}$ $\quad f = \{(1, 4), (2, 5), (3, 5)\}$

$f(\{2, 3\}) = \{5\}$ $\qquad f^{-1}(\{5\}) = \{2, 3\}$ $\qquad f|_{\{1,2\}} = \{(1,4), (2,5)\}$

$f(\{1, 2\}) = \{4, 5\}$ $\qquad f(\emptyset) = \emptyset$

$f^{-1}(\{4\}) = \{5)$ $\qquad f^{-1}(\emptyset) = \emptyset$ $\qquad f|_{\{1\}} = \{(1, 4)\}$

$A \xrightarrow{f} B \xrightarrow{g} C$ onto

$g \circ f$

Subject : Date ....../....../......

Facts: Let $f$ be a function from $A$ to $B$. Then;

(i) $f$ is onto $\iff f(A) = B$

(ii) $f$ is one-to one $\iff \forall b \in B \ |f^{-1}(\{b\})| \leq 1$

(iii) $f$ is onto $\iff \forall b \in B \ |f^{-1}(\{b\})| \geq 1$

Theorem: Let $f$ be a function from $A$ to $B$, $C_1 \subseteq A$, $C_2 \subseteq A$, $D_1 \subseteq B$, $D_2 \subseteq B$

(i) $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$

(ii) $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$ → ! Not equals.

Ex) $A = \{1, 2\}$ $C_1 = \{1\}$ $C_2 = \{2\}$ $B = \{3\}$

$f = \{(1,3), (2,3)\}$

$f(C_1 \cap C_2) = f(\emptyset) = \emptyset$ → $\emptyset \neq \{3\}$

$f(C_1) \cap f(C_2) = \{3\}$ → $\emptyset \subseteq \{3\}$

(iii) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$

(iv) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$

(v) $f^{-1}(B - D_1) = A - f^{-1}(D_1)$

Proof of v: Assume $a \in f^{-1}(B - D_1)$. Then $f(a) \in B - D_1$ in other words $f(a) \in B$ and $f(a) \notin D_1$. Suppose $a \in f^{-1}(D_1)$ Then $f(a) \in D_1$. This is a contradiction because $f(a) \notin D_1$. So $a \notin f^{-1}(D_1)$ Hence $a \in A - f^{-1}(D_1)$. This proves $f^{-1}(B - D_1) \subseteq A - f^{-1}(D_1)$. Assume $a \in A - f^{-1}(D_1)$ Then $f(a) \notin D_1$ because $a \notin f^{-1}(D_1)$. So $f(a) \in B - D_1$ because $f(a) \in B$ Hence $a \in f^{-1}(B - D_1)$ This proves $A - f^{-1}(D_1) \subseteq f^{-1}(B - D_1)$. Therefore $f^{-1}(B - D_1) = A - f^{-1}(D_1)$

Definition: Let $f$ be a function from $A$ to $B$ and $g$ be a function from $B$ to $C$. Then $g \circ f = \{(a, c) \mid (a \in A) \wedge (c \in C) \wedge (\exists b \in B \ ((a,b) \in f) \wedge ((b,c) \in g))\}$

Notice $g \circ f$ (composition of $g$ and $c$) is a function from $A$ to $C$.

Theorem: Let $f$ be a function from $A$ to $B$, let $g$ be from $B$ to $C$.

(i) if $g \circ f$ is onto then $g$ is onto.

(ii) if $g \circ f$ is one-to-one then $f$ is one-to-one.

Subject : Date :....../....../......

Question: Can we say f is onto in part i, g is one-to one in part ii? NO.

Definition: Let R be a relation from A to B. Then we define $R^c$ a new relation from B to A as follows: $R^c = \{(b,a) \mid (a,b) \in R\}$

Definition: We say a function f from A to B is invertible if $f^c$ is a function from B to A.

Notation: If A is a set then, $I_A = \{(a,a) \mid a \in A\}$ is the identity function on A.

Theorem: Let f be a function from A to B. Then following are equivalent:

(i) f is invertible.

(ii) There exist g such that g is a function from B to A and $g \circ f = I_A$ and $f \circ g = I_B$

(iii) f is one-to-one and onto. (which we call bijection)

Proof of i→ii: Take $g = f^c$

Proof of ii→iii: $\left.\begin{array}{l} g \circ f = I_A \text{ is one-to-one} \Rightarrow f \text{ is one-to-one} \\ f \circ g = I_B \text{ is onto} \Rightarrow f \text{ is onto} \end{array}\right\}$ f is bijection.

Proof of iii→i: ---

Notation: If f is invertible then instead of $f^c$ we write $f^{-1}$.

Theorem: Let f be a function from A to B. Assume $|A| = |B|$. Then following are equivalent:

(i) f is bijection. (ii) f is one-to-one (iii) f is onto.

Idea of proof: we only show that ii→iii and iii→ii because i↔(ii and iii)

Pigeonhole Principle: If m pigeons occupy n pigeonholes and $m > n$ then at least one pigeonhole has two or more pigeons roosting it.

Note: If you want to use pigeonhole principle, then you have to:

1. Define the set of pigeons
2. Define the set of pigeonholes.
3. Say which pigeon occupies which hole.
4. Show that [no. of pigeons] > [no. of holes]
5. Say "by Pigeonhole Principle".

Subject : Date ..../..../....

Ex) Assume that an office employs 13 file clerks. Show that at least two of them must have birthdays during the same month.

Define the set of pigeons as the set of file clerks.

Define the set of pigeonholes as the set of months.

Say pigeon X roosts in pigeonhole y if the birthday of the file clerk x has birthday during the month y.

We have Number of pigeons = 13 > 12 = number of pigeonholes.

So by Pigeonhole Principle, we can say that at least two of the file clerks have birthdays during the same month.

Ex) Given a tape that contains 500'000 words of four or fewer lowercase letters. (Note: letters from Eng. alphabet and consecutive words on tape are seperated by a blank character.) Can it be that 500'000 words are all distinct?

Define the set of pigeons as words on the tape.

Define the set of pigeonholes as words of four or fewer lowercase letters

Say pigeon x roosts in pigeonhole y where $x = y$

Number of pigeons = 500'000

Number of pigeonholes = $26^4 + 26^3 + 26^2 + 26^1 = 475'254$

No. Of. Pigeons > No. Of. P.Holes

So we are done by pigeonhole principle.

Ex) Let $S \subseteq \mathbb{Z}^+$ where $|S| = 37$. Show that S contains two elements that have the same remainder upon division by 36.

Pigeons = S Pigeonholes = $\{0, 1, 2, \ldots 35\}$

Pigeon x ~~goes to~~ roosts in pigeonhole y if, $x = 36p + y$ where $q \in \mathbb{Z}$.

Number of pigeons = 37 > 36 = number of pigeonholes.

So we're done by Pigeonhole principle.

Subject : Date : ......./......./.......

Ex| Prove that if 101 integers are selected from the set $S = \{1, 2, 3, \ldots 200\}$ then there are two integers such that one divides the other.

Pigeons = Selected 101 integers  Pigeonholes: $\{1, 3, 5, 7, 9, \ldots 199\}$ (odd nums)

Pigeon $x$ roosts in pigeonhole $y$ if, $x = 2^q \cdot y$ where $q \in \mathbb{N}$

Number of pigeons $= 101 > 100 =$ number of pigeonholes

So by pigeonhole principle, there exist $x_1$, $x_2$ such that $x_1 = 2^{q_1} y$, $x_2 = 2^{q_2} y$

If $q_1 < q_2$, then $x_2$ divides $x_1$.
If $q_2 < q_1$, then $x_1$ divides $x_2$.
} So in any case, one divides other.

→ We couldn't prove the previous example with 100 integer selections: $\{101, 102, \ldots 200\}$

Ex| Show that any subset of size 6 from the set $S = \{1, 2, 3, 4, 5, 6\}$ must contain two elements whose sum is 10.

Pigeons = the subset of size 6  Pigeonholes: $\{\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}\}$

Pigeon $x$ roosts in pigeonhole $y$ if, $x \in y$.

Number of pigeons $= 6 > 5 =$ Number of pigeonholes.

So by pigeonhole principle, there exits two pigeons $x_1, x_2$, such that:

$x_1 \neq x_2$ and $x_1 \in y$ and $x_2 \in y$. Notice $y \neq \{5\}$

So $y = \{1, 9\}$ or $\{2, 8\}$ or $\{3, 7\}$, $\{4, 6\}$. } In all cases $x_1 + x_2 = 10$

Ex| Let $S$ be a set of six positive integers whose maximum is at most 14. Show that the sums of the elements in all subsets of $S$ cannot be all distinct.

Wrong Solution: Pigeons = Non-empty subsets of $S$ | $x$ goes to $y$ if sum of $x$ is equal to $y$.

Pigeonholes $= \{1, 2, 3 \ldots 69\}$

$\{1\}$  $\{9, 10, 11, 12, 13, 14\}$

$2^6 - 1 = 63 \not> 69$ Then we decrease the No. of pigeons and pigeonholes.

Subject :

Date :....../....../......

Correct Solution: Pigeons = non-empty subsets of $S$ with at most five elements.

X goes to y if sum of x is y.

Pigeonholes = $\{1, 2, 3, \dots, 60\} \to \{10, 11, 12, 13, 14\}$

No. Of Pigeons $= 2^6 - 1 - 1 = 62 > 60 =$ No. Of Pigeonholes.

So by pigeonhole principle there exist two subsets $X_1$, $X_2$ of $S$ such that sum of elements of them are the same.

Ex] Find a positive integer $A$ so that the following is true: Let $S \subseteq \mathbb{Z}^+$, where $|S| = A$. Then $S$ contains two elements that same remainder upon division by 8. [We can choose any number $A \geq 9$]

Pigeons = $S$ Pigeonholes: Remainders upon division by 8: $\{0, 1, 2, 3, 4, 5, 6, 7\}$

Pigeon $x$ goes to pigeonhole $y$ if $y$ is the remainder of $x$ upon division by 8.

Number of pigeons $= A \geq 9 > 8 =$ Number of pigeonholes.

So by pigeonhole principle, we can say there exist two numbers in $S$ which has the same remainder upon division by 8 if $A \geq 9$.

Ex] Let $m \in \mathbb{Z}^+$ with $m$ is odd. Prove that there exist a positive integer $n$ such that $m$ divides $2^n - 1$.

Pigeons $= \{2^1 - 1, 2^2 - 1, 2^3 - 1, 2^4 - 1, \dots, 2^{m+1} - 1\}$

Pigeonholes $= \{0, 1, 2, \dots, (m-1)\}$

Pigeon $x$ goes pigeonhole $y$ if $y$ is the remainder of $x$ upon division by $m$.

Number of pigeons $= m + 1 > m =$ Number of pigeonholes.

So by pigeonhole principle $y$ has two or more pigeons roosting it.

Say $2^{n_1} - 1$ and $2^{n_2} - 1$ have the same remainder upon division by $m$:

$$\left.\begin{aligned} 2^{n_1} - 1 &= q_1 m + y \\ 2^{n_2} - 1 &= q_2 m + y \end{aligned}\right\} \quad \begin{aligned} &2^{n_1} - 2^{n_2} = (q_1 - q_2) \cdot m \\ &\text{Without loss of generality, we can assume } n_1 > n_2; \end{aligned}$$

So we can say $m$ divides $2^{n_1} - 2^{n_2} = 2^{n_2}(2^{n_1 - n_2} - 1)$ Remember $m$ is odd. Therefore $m$ divides $2^{n_1 - n_2} - 1$.

Subject : Date : ....../....../......

Ex/ While on a 4-week vacation, Herbert will play at least one set of tennis each day, but he won't play more than 40 sets total during the day. Prove that no matter how he distributes his sets during the four 4 weeks, there is a span of consecutive days during which he'll play exactly 15 sets.

Let $x_i$ = the total number of sets played from start to the end of $i$th day.

We know $[1 \leqslant x_1 < x_2 < x_3 < \cdots < x_{28} \leqslant 40]$

We want to show $[x_j - x_i = 15]$ exist for some $i, j$.

Pigeons $= \{(i, n) \mid i \in \{1, 2, 3, \ldots, 28\},\ n \in \{0, 1\}\}$

Pigeonholes $= \{1, 2, 3, \ldots, 55\} \rightarrow (40+15)$

Pigeon $(i, n)$ roosts in pigeon hole $y$ if; $y = \begin{cases} x_i & \text{if } n=0 \\ x_i + 15 & \text{if } n=1 \end{cases}$

Pigeon number $= 2 \cdot 28 = 56 > 55$ = Pigeon hole number

By, pigeonhole principle, there exist two pigeons $(i, n)$ and $(j, m)$ such that $(i, n)$ and $(j, m)$ roosts in same pigeonhole $y$.

We have $n \neq m$ because if $n = m = 0$ then we have $x_i = x_j$ or $n = m = 1$ and we have $x_i + 15 = x_j + 15$, this is impossible because $i \neq j$ means $x_i \neq x_j$

Without loss of generality, we have $n = 0$ and $m = 1$ which means $x_i = x_j + 15 = y$. So we are done.

---

Definition: Let $R$ be a relation on $A$. Then we say; $(a,b) \in A \rightarrow (b,a) \in A$

(i) $R$ is reflexive if $\forall a \in A\ (a, a) \in R$

(ii) $R$ is symmetric if $\forall a \in A\ \forall b \in A\ (a, b) \in R \rightarrow (b, a) \in R$

(iii) $R$ is antisymmetric if $\forall a \in A\ \forall b \in A\ ((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b)$

(iv) $R$ is transitive if $\forall a \in A\ \forall b \in A\ \forall c \in A\ ((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$

Subject : Date ...../...../.....

Ex| The operation $|$ (→ divides.) is reflective on $\mathbb{Z}^+$.

(*) Antisymmetric is not negation of symmetric.

Ex| $\leq$ is antisymmetric because $a \leq b$ and $b \leq a$ implies $a = b$

Ex| $<$ is antisymmetric because $a < b$ and $b < a$ is always false.

Ex| $|$ is not antisymmetric on $\mathbb{Z}$ because $2 | -2$ and $-2 | 2$ but $2 \neq -2$

Ex| $\leq$ is transitive because $a \leq b$ and $b \leq c$ implies $a \leq c$.

Ex| $<$ is transitive because $a < b$ and $b < c$ implies $a < c$.

Ex| $|$ is transitive because $a | b$ and $b | c$ implies $a | c$.

Ex| $R = \{(a,b) \mid a, b \in \mathbb{Z}^+ \text{ and } \gcd(a,b) > 1\}$

Then $R$ is not transitive because $(2,6) \in R$, $(6,3) \in R$, $(2,3) \notin R$

$R$ is not reflective on $\mathbb{Z}^+$ because $(1,1) \notin R$

$R$ is symmetric because $\gcd(a,b) = \gcd(b,a)$

$R$ is not antisymmetric because $(2,6) \in R$ and $(6,2) \in R$, $2 \neq 6$

Ex| $=$ is reflexive, symmetric, antisymmetric and transitive.

Definition: A relation is called an equivalence relation if it is reflexive, symmetric and transitive. Ex| $=$ is an equivalence relation.

Ex| $R = \{(a,b) \mid 3 | a-b\}$ on $\mathbb{Z}$. $R$ is reflexive because $3|0$. $R$ is symmetric because $3 | a-b$ implies $3 | b-a$. $R$ is transitive because $3|a-b$, $3|b-c$ implies $3|a-c$.
So $R$ is an equivalance relation. In fact: $aRb \iff a \equiv b \pmod 3$

Definition: Let $A$ be a set and $R$ be a relation on $R$. Then we say

(*)
1. $R$ is a partial order if $R$ is reflexive, antisymmetric, transitive.
2. $R$ is a total order if $R$ is partial order and $\forall a \in A\ \forall b \in A\ (a,b) \in R \vee (b,a) \in R$
3. $R$ is an equivalance relation if $R$ is reflexive, symmetric, transitive.

Ex| $\leq$ on $\mathbb{Z}$ is a total order. (also a partial order.)

$\subseteq$ on sets is a partial order. (not a total: $\{2,3\} \nsubseteq \{4,5\}$, $\{4,5\} \nsubseteq \{2,3\}$)

Subject : Date : ...../...../.....

Ex| $|$ on $\mathbb{Z}^+$ is a partial order. (Not a total order: $2 \nmid 3$, $3 \nmid 2$)

Definition: Let $R$ be an equivalence relation on $A$ and $x \in A$. Then we define equivalence class of $x$ as follows: $[x] = \{y \mid y \in A \text{ and } (x,y) \in R\}$

Ex| If $A = \mathbb{Z}$ and $R = \{(a,b) \in A \times A \mid 3 \mid a-b\}$ $\equiv$ (mod 3) Then;

$[0] = \{\ldots -6, -3, 0, 3, 6 \ldots\}$ $[-3] = [0] = [3] = [6] = \cdots$

$[1] = \{\ldots -5, -2, 1, 4, 7 \ldots\}$ $[1] = [4] = [7] \cdots$ $A/_R = 3$

$[2] = \{\ldots -4, -1, 2, 5, 8 \ldots\}$ → Notice we have only 3 different eq. classes.

Notation: If $R$ is an equivalence relation on $A$ then $A/_R = \{[x] \mid x \in A\}$

Definition: Let $A$ be a set and $F$ be a subset of the power set of $A$. Then we say $F$ is a partition of $A$ if;

① $\forall u \in F \quad u \neq \emptyset$, ② $\forall x \in A \ \exists u \in F \quad x \in u$ and

③ $\forall u \in F \quad \forall w \in F \quad u \cap w = \emptyset$ or $u = w$ $\boxed{\text{Eq. Relation}} \rightarrow \boxed{\text{Partition}}$

Theorem: If $R$ is an equivalence relation on $A$ then $A/_R$ is a partition of $A$.

Proof: $F = A/_R$ ①: Then given any $u$ in $F$ there exist $x \in u$, $u = [x] \Rightarrow u \neq \emptyset$ because $x \in [x]$

②: Given $x \in A$ we have $x \in [x] \in F$, since $R$ is reflexive.

③: Given $u = [x]$ and $w = [z]$ in $F$. Assume $u \cap w \neq \emptyset$. Then there exist $t \in [x]$ and $t \in [z]$ which means $(x,t) \in R$, $(z,t) \in R$. Since $R$ is symmetric, $(t,z) \in R$, and since $R$ is transitive $(x,z) \in R$ ..... $[x] = [z]$

Natural numbers in sets: $N = \{0, 1, 2, 3\}$

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

$= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$

Question:

So how do we define $-1, -2, \ldots$

Subject : Date ...../...../.....

Answer: Let $A = N \times N$ , $R = \{((a,b),(c,d)) \mid a+d = b+c\}$

R is reflexive because $a+b = b+a$

R is symmetric because $a+d = b+c \Rightarrow b+c = a+d$

R is transitive because $a+d = b+c$ and $c+f = d+e \Rightarrow a+f = b+e$

So R is equivalence relation. Instead of $A/R$ we write $\mathbb{Z}$.

$\rightarrow 0 = [(0,0)] = \{(0,0),(1,1),(2,2)\ldots\}$

$1 = [(1,0)] = \{(1,0),(2,1),(3,2)\ldots\}$

$2 = [(2,0)] = \{(2,0),(3,1),(4,2)\ldots\}$

$-1 = [(0,1)] = \{(0,1),(1,2),(1,3)\ldots\}$

$-2 = [(0,2)] = \{(0,2),(1,3),(2,3)\ldots\}$

Definition of substraction

$[(a,b)] - [(c,d)] = [(a+d, b+c)]$

Ex) $2-4 = [(2,0)] - [(4,0)] = [(2,4)]$
$= [(0,2)] = -2$

Question: How do we define rational numbers, $\frac{1}{2} = ?$ , $\frac{2}{3} = ?$

Answer: Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ and $R = \{((a,b),(c,d)) \mid ad = bc\}$

R is an equivalence relation. Instead of $A/R$ we write $Q$

Definition: $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ , Instead of $[(a,b)]$ we write $\frac{a}{b}$

Ex) $\frac{1}{2} = [(1,2)] = \{(1,2),(-1,-2),(3,6),(8,16)\ldots\}$

Ex) $\frac{1}{4} + \frac{2}{8} = [(1,4)] + [(2,8)] = [(8+4\cdot 2, 4\cdot 8)] = [(16,32)] = [(1,2)]$

Exercise: Define real numbers as equivalence classes of sequences. (Math 102)

Theorem: If F is a partition of A, then $R = \{(a,b) \in A \times A \mid \exists u \in F \; a \in u, b \in u\}$ is an equivalence relation on A. $\boxed{\text{Partition}} \rightarrow \boxed{\text{Equivalence Relation}}$

Theorem: For any set A, there is a bijection (one-to-one and onto) function between the set of partitions of A and the set of equivalence relations on A.

Proof: Use previous two theorems.

Subject : Date : ....../....../......

**Ex**

| Partition of $\{1,2,3\}$ | Equivalence relation on $\{1,2,3\}$ |
|---|---|
| $F_1=\{\{1\},\{2\},\{3\}\}$ | $R_1=\{(1,1),(2,2),(3,3)\}$ |
| $F_2=\{\{1,2\},\{3\}\}$ | $R_2=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ |
| $F_3=\{\{1,2,3\}\}$ | $R_3=\{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2),(1,3),(3,1)\}$ |

## Chapter 6) (back)

Definition: A finite set of symbols is called an alphabet if symbols are all distinct even after any juxtaposition.

**Ex** $\{0,1,2,3,4\}$ is an alphabet $\{a,b,c\}$ is an alphabet.
$\{c, a, r, car\}$ is not an alphabet because first 3 make the 4th.

Definition: Let $\Sigma$ be an alphabet, then a string of length $n \in \mathbb{N}$ is a juxtaposition in the form $a_1 a_2 a_3 \dots a_n$ where $a_i \in \Sigma$.

Notation: $\lambda$ denotes empty string.
$\Sigma^n$ denotes the set of strings of length $n$.
$\Sigma^*$ denotes the set of all strings. (infinite)

**Ex** $\Sigma=\{0,1\} \Rightarrow \Sigma^0=\{\lambda\}$, $\Sigma^2=\{00,01,10,11\}$, $\Sigma^*=\{\lambda,0,1,00,01,\dots\}$

(*) Definition: A finite state machine is a five tuple:

$$M=(S,\Sigma_i,\Sigma_o,f_{next},f_{output})$$

$S$ is a set, $\Sigma_i$ and $\Sigma_o$ are alphabets. $f_{next}$ is a function from $S \times \Sigma_i$ to $S$. $f_{output}$ is a function from $S \times \Sigma_i$ to $\Sigma_o$.

Fact: Given a finite state machine and $s_0 \in S$ we obtain a function from $\Sigma_i^*$ to $\Sigma_o^*$ as following algorithm;

Subject :                                                    Date : ....../....../......

$s = s_0$

while (true)

  $i$ = get an input

  write the output: $f_{output}(s, i)$

  $s = f_{next}(s, i)$

end

**Ex** Define $S = \{s_0, s_1\}$, $\Sigma_i = \left\{ \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{1} \right\}$, $\Sigma_o = \{0, 1\}$

$$
\begin{array}{ll}
f_{next}\left(s_0, \binom{0}{0}\right) = s_0 & f_{output}\left(s_0, \binom{0}{0}\right) = 0 \\
f_{next}\left(s_0, \binom{0}{1}\right) = s_0 & f_{output}\left(s_0, \binom{0}{1}\right) = 1 \\
\quad\left(s_0, \binom{1}{0}\right) = s_0 & \quad = 1 \\
\quad\left(s_0, \binom{1}{1}\right) = s_1 & \quad = 0 \\
\quad\left(s_1, \binom{0}{0}\right) = s_0 & \quad = 1 \\
\quad\left(s_1, \binom{0}{1}\right) = s_1 & \quad = 0 \\
\quad\left(s_1, \binom{1}{0}\right) = s_1 & \quad = 0 \\
\quad\left(s_1, \binom{1}{1}\right) = s_1 & \quad = 1
\end{array}
$$

$$
\begin{array}{r}
1\,0\,0\,1\,0\,0\,1\,1 \\
+\;0\,1\,0\,1\,1\,0\,0\,1 \\
\hline
0\,0
\end{array}
$$

State is $s_0$ → input $\binom{1}{1}$ → output $0$ → state $s_1$ → input $\binom{1}{0}$ → output $0$ → state $s_1$ ...

$f_{output}\left(s_0, \binom{1}{1}\right) = 0$ $f_{next}\left(s_0, \binom{1}{1}\right) = s_1$

$s_0$ is the state of carrying 0, $s_1$ is the state of carrying 1.

$s_0 \to$ dse topla
$s_1 \to$ elde var 1

Question: How can we optimize* finite state machines?

*: We say $M_1$ is better than $M_2$ if $M_1$ and $M_2$ both give the same function from $\Sigma_i^*$ to $\Sigma_o^*$ and $M_1$ has less states than $M_2$.

Step 1: Define a relation on the set of states as follows:

$$E_1 = \{(s_1, s_2) \in S \times S \mid \forall i \in \Sigma_i \quad f_{output}(s_1, i) = f_{output}(s_2, i)\}$$

Notice $E_1$ is an equivalence relation since it's reflexive, symmetric and transitive.

Step 2: Given an equivalence relation $E_k$ on the set of states. Define a new equivalence relation $E_{k+1}$ as follows:

$$E_{k+1} = \{(s_1, s_2) \in E_k \mid \forall i \in \Sigma_i \quad (f_{next}(s_1, i), f_{next}(s_2, i)) \in E_k\}$$

Step 3: If $E_k = E_{k+1}$ then write the new finite state machine using equivalence classes of states as the set of states.

Subject : Date : ....../....../......

**Ex**

| state \ input | $f_{next}$ 0 | $f_{next}$ 1 | $f_{output}$ 0 | $f_{output}$ 1 |
|---|---|---|---|---|
| $s_1$ | $s_2$ | $s_4$ | 1 | 0 |
| $s_2$ | $s_3$ | $s_1$ | 1 | 1 |
| $s_3$ | $s_1$ | $s_4$ | 1 | 0 |
| $s_4$ | $s_2$ | $s_1$ | 1 | 0 |

$S = \{s_1, s_2, s_3, s_4\}$ $\quad \Sigma_i = \{0,1\}$ $\quad \Sigma_o = \{0,1\}$

Assume initial state $s_0 = s_1$, then

Input $= 1011$ $\quad$ Output $= 0110$

| Equivalence Relation | Partition |
|---|---|
| $E_1$ | $\{\{s_1, s_3, s_4\}, \{s_2\}$ |
| $E_2$ | $\{\{s_1, s_4\}, \{s_3\}, \{s_2\}$ |
| $E_3$ | $\{\{s_1, s_4\}, \{s_3\}, \{s_2\}$ |

So $E_2 = E_3$ which means a better machine is

| | $f_{next}$ 0 | $f_{next}$ 1 | $f_{output}$ 0 | $f_{output}$ 1 |
|---|---|---|---|---|
| $[s_1]$ | $[s_2]$ | $[s_1]$ | 1 | 0 |
| $[s_2]$ | $[s_3]$ | $[s_1]$ | 1 | 1 |
| $[s_3]$ | $[s_1]$ | $[s_1]$ | 1 | 0 |

**Definition:** Let $f$ and $g$ be two functions from $\mathbb{Z}^+$ to $\mathbb{R}$ then we say $g$ dominates $f$ or we say $f$ is in "big-Oh" of $g$ and we write $f \in O(g)$ if $\exists C \in \mathbb{R}^+ \; \exists k \in \mathbb{Z}^+ \; \forall n \in \mathbb{Z}^+ \; (n \geq k) \rightarrow (|f(n)| \leq C \cdot |g(n)|)$

Note that we can consider $O(g)$ as a set of functions.

**Ex** $f(n) = 10^8 n + 500$, $g(n) = n^2$. Show that $f \in O(g)$

Take $C = 10^8 + 1$, $k = 500$, then given any $n \in \mathbb{Z}^+$ if $n \geq k$

$$|f(n)| = 10^8 n + 500 \underset{(n \geq 500)}{\leq} 10^8 n + n = (10^8+1)n \underset{(C = 10^8+1)}{\leq} Cn \underset{(n \geq 1)}{\leq} Cn^2 = C \cdot |g(n)|$$

**Ex** If $f(n) = 1000n^2 + 5n + 100$ and $g(n) = n^2$, show that $f \in O(g)$

Take $C = 2000$, $k = 1$, then given any $n \in \mathbb{Z}^+$, $n \geq k$

$$|f(n)| = 1000n^2 + 5n + 100 \underset{\substack{(5n+100 \leq 1000n^2) \\ 1 \leq n}}{\leq} 1000n^2 + 1000n^2 = 2000n^2 = Cn^2 = C|g(n)|$$

**Ex** Show that $n^3 \notin O(n^2)$. {Negate the statement $\exists \exists \forall \; p \rightarrow q$}

We need to show $\forall C \in \mathbb{R}^+ \; \forall k \in \mathbb{Z}^+ \; \exists n \in \mathbb{Z}^+ \; (n \geq k) \wedge (|f(n)| > C|g(n)|)$

Take $n = \max\{k, [\![C]\!]^* + 2\}$, then we get; $\quad$ *: $[\![x]\!] = (\text{int})\, x$

$n \geq k$ and $|f(n)| = n \cdot n^2 \geq ([C]+2)n^2 > Cn^2 = C \cdot |g(n)|$

Subject : Date : ..../..../....

Some sets of functions: $O(1)$: constant | $O(\log_2 n)$: logarithmic | $O(n)$: linear
$O(n^2)$: quadratic | $O(n^3)$: cubic | $O(n^m)$: polynomial | $O(c^n)$: exponential | $O(n!)$: factorial

Definition: Given a computer program P, we define three functions:
$f_{best}(n)$ = [least number of operations program P has to perform to calculate the output when the size of input is n.
$f_{worst}(n)$ = [greatest number of...]
$f_{average}(n)$ = [average number of...] $= \sum_{k \in \mathbb{Z}^+} k \cdot Pr(A_k)$ where the sample space S is the set of all possible inputs and $A_k$ is the event that we got an input for which program P has to perform k operations to calculate the output and $Pr(A_k)$ = [probability of the event $A_k$]

Ex/ Procedure Search $(a, \{a_1, a_2, \dots, a_n\})$

```
i = 1
while (i ≤ n and a ≠ a_i)
    i = i + 1
If i ≤ n then print(i)
else print(0)
```

$f_{best}(n) = 1+1+1+1+1 = 5$
$f_{worst}(n) = 1 + 3n + 1 = 3n+2 \quad f_{worst} \in O(n)$
$f_{average}(n) = \sum_{s=1}^{n} (3s+2)\frac{1}{N} + (3n+2)\frac{N-n}{N} \in O(n)$

Chapter 8) S set $\longleftrightarrow$ universe $\mathcal{U}$
c condition $\longleftrightarrow$ open statement $p(x)$

Notation: $N(c)$ = (the number of elements in S which satisfy the condition c)

Ex/ $S = \{1,2,3,4,5,6,7\}$, $c_1$ = the number is even ; $c_2$ = the number is odd. $N(c_1)=3$ $N(c_2)=4$

Notation: $c_1 c_2$ means $c_1$ **and** $c_2$.

Ex/ $N(c_1\, c_2) = 0$ because a number can't be both even and odd.

Notation: $\overline{c}$ means not c.

Ex/ $N(\overline{c_1}) = 4 \quad N(\overline{c_2}) = 3$ Careful: $N(\overline{c_1}\ \overline{c_2}) = 0$
$N(\overline{c_1\ c_2}) = 7$

Subject : Date : ...../...../.....

Notation: $S_r = \sum_{\substack{I \subseteq \{1,2,\dots n\} \\ |I|=r \\ I=\{i_1,i_2,\dots i_r\}}} N(c_{i_1} c_{i_2} \dots c_{i_r})$ when there are n many conditions

$S_0 = |S|$

Ex) Assume $c_1$ and $c_2$ are conditions. Then,

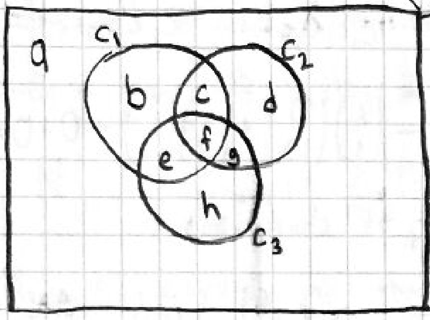
$S_1 = N(c_1) + N(c_2)$ $\qquad$ $S_2 = N(c_1 c_2)$

Ex) Assume $c_1$, $c_2$ and $c_3$ are conditions. Then,

$S_1 = N(c_1) + N(c_2) + N(c_3)$ $\qquad$ $S_2 = N(c_1 c_2) + N(c_1 c_3) + N(c_2 c_3)$ $\qquad$ $S_3 = N(c_1 c_2 c_3)$

(Principle of Inclusion and Exclusion) Theorem: Assume $c_1, c_2, \dots, c_n$ are conditions. Then,

$$N(\bar{c}_1 \bar{c}_2 \cdots \bar{c}_n) = \sum_{r=0}^{n} (-1)^r \cdot S_r = S_0 - S_1 + S_2 - \cdots \pm S_n$$




$N(c_1) = b+c+e+f$ $\qquad$ $N(c_1 c_2) = c+f$

$N(c_2) = c+d+f+g$ $\qquad$ $N(c_2 c_3) = f+g$ $\qquad$ $N(c_1 c_2 c_3) = f$

$N(c_3) = e+f+g+h$ $\qquad$ $N(c_1 c_3) = e+f$

$$S_0 - S_1 + S_2 - S_3 = [(a+b+c+d+f+g+h)] - [(b+c+e+f)+(c+d+f+g)+(e+f+g+h)] + S_2 - S_3$$

$$S_0 - S_1 + S_2 - S_3 = a - c - e - g - 2f + [(c+f)+(e+f)+(f+g)] - [f] = \underbrace{a}_{N(\bar{c}_1 \bar{c}_2 \bar{c}_3)} \checkmark$$

Ex) Determine the number of positive integers n where $1 \leq n \leq 100$ and n is not divisible by 2, 3 or 5.

Note that (not divisible by 2, 3 or 5) $= \neg(2 \vee 3 \vee 5) = (\neg 2) \wedge (\neg 3) \wedge (\neg 5)$

= (not divisible by 2) and (not divisible by 3) and ...

Define $S = \{1, 2, 3 \dots 100\}$

Define $c_1$ = the number is divisible by 2

" $c_2$ = " " " " by 3

" $c_3$ = " " " " by 5

$N(c_1) = 50$ $\qquad$ $N(c_1 c_2) = 16$

$N(c_2) = 33$ $\qquad$ $N(c_1 c_3) = 10$

$N(c_3) = 20$ $\qquad$ $N(c_2 c_3) = 6$

$N(c_1 c_2 c_3) = 3$

$$N(\bar{c}_1 \bar{c}_2 \bar{c}_3) = \sum_{r=0}^{3} (-1)^r \cdot S_r = S_0 - S_1 + S_2 - S_3 = (100) - (50+33+20) + (16+10+6) - (3) = 26$$

Subject : Date :

Ex) Find the number of non-negative integer solutions to the equation;

$$x_1 + x_2 + x_3 + x_4 = 18 \quad \text{where} \quad \forall i \; x_i \leq 7$$

Define $S = $ (set of all nonnegative solutions)

Define $c_i = (x_i \geq 8)$, so we have 4 conditions.

$$N(c_1) = \begin{pmatrix} \text{the number of solutions} \\ x_1+x_2+x_3+x_4=18 \quad \cancel{0\leq x_i \leq 8} \\ 0 \leq x_i \end{pmatrix} \underset{z_1 = x_1 - 8}{=} \begin{pmatrix} \text{the number of solutions} \\ z_1+z_2+z_3+z_4=10 \end{pmatrix} = \binom{n+r-1}{r} = \binom{4+10-1}{10} = \binom{13}{10} = 13 \cdot 15$$

$$N(c_1 c_2) = \begin{pmatrix} \text{the number of solutions} \\ x_1+x_2+x_3+x_4=18 \quad \cancel{0\leq x_i \leq 8} \\ 0 \leq x_i \end{pmatrix} \underset{\substack{z_1 = x_1 - 8 \\ z_2 = x_2 - 8}}{=} \begin{pmatrix} \text{the number of solutions} \\ z_1+z_2+z_3+z_4=2 \end{pmatrix} = \binom{n+r-1}{r} = \binom{4+2-1}{2} = \binom{5}{2} = 10$$

$c_1 c_2 c_3 = 0 \qquad c_1 c_2 c_3 c_4 = 0$

By symmetry, $c_1 = c_2 = c_3 = c_4$

$c_1 c_2 = c_1 c_3 = \dots \qquad c_1 c_2 c_3 = \dots \qquad \cancel{c_1 c_2 c_3 c_4 =}$

$$N(\bar{c}_1 \bar{c}_2 \bar{c}_3 \bar{c}_4) = S_0 - S_1 + S_2 - S_3 + S_4 = \binom{21}{18} - \binom{4}{1}\binom{13}{10} + \binom{4}{2}\binom{5}{2} - 0 + 0 = 246$$

$$S_0 = |S| = \binom{n+r-1}{r} = \binom{4+18-1}{17} = \binom{21}{18}$$

number of conditions

Remember the Theorem:

$$\begin{pmatrix} \text{The number of onto} \\ \text{function from } A \text{ to } B \end{pmatrix} = \sum_{r=0}^{|B|} (-1)^r \binom{|B|}{|B|-r} (|B|-r)^{|A|}$$

Proof: Define $S = $ (set of all functions from $A$ to $B$)

Assume $B = \{b_1, b_2, \dots, b_n\}$ where $|B| = n$. Then $c_i = $ ($b_i$ is not in the range of function)

So $\bar{c}_1$ means $b_1$ is in the range. Then $\bar{c}_1 \bar{c}_2 \bar{c}_3 \cdots \bar{c}_n$ means function is onto.

$$N(\bar{c}_1 \bar{c}_2 \bar{c}_3 \cdots \bar{c}_n) = \sum_{r=0}^{n} (-1)^r S_r = \sum_{r=0}^{n} (-1)^r \cdot \binom{n}{r} \cdot N(c_1 c_2 \cdots c_r)$$

Number of functions from $A$ to $B - \{b_1, b_2, \dots, b_r\}$

$$= \sum_{r=0}^{n} (-1)^r \binom{n}{r} |B - \{b_1, b_2, \dots, b_r\}|^{|A|} = \sum_{r=0}^{n} (-1)^r \binom{|B|}{|B|-r} \cdot (|B|-r)^{|A|}$$

Ex) In how many ways can the 26 letters of the alphabet be permutated so that non of the patterns car, dog, fun or byte occurs?

Subject : Date : ...../...../.....

$S=$ (set of all permutations of 26 letters)

$c_1=$ car occurs $c_2=$ dog occurs $c_3=$ fun occurs $c_4=$ byte occurs

$N(\bar{c}_1\ \bar{c}_2\ \bar{c}_3\ \bar{c}_4) = S_0 - S_1 + S_2 - S_3 + S_4$

$= |S| - [3\cdot N(c_1) + N(c_4)] + [3\cdot N(c_1c_2) + 3\cdot N(c_1c_4)] - [N(c_1c_2c_3) + 3\cdot N(c_1c_2c_4)] + [N(c_1c_2c_3c_4)]$

$= 26! - [3\cdot 24! + 23!] + [3\cdot 22! + 3\cdot 21!] - [20! + 3\cdot 19!] + [17!]$ think the pattern as a letter

**Ex** Assume there are 5 villages. An engineer is to devise a system of two-way roads so that after the system is completed, no village will be isolated. In how many ways can he do this?

$S=$ (all possible two-way road systems)
$c_i=$ the $i^{th}$ village is isolated
$\Big\}\ N(\bar{c}_1\ \bar{c}_2\ \bar{c}_3\ \bar{c}_4\ \bar{c}_5) = ?$

$N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4\bar{c}_5) = \sum_{r=0}^{5} (-1)^r \cdot S_r = S_0 - S_1 + S_2 - S_3 + S_4 - S_5$

$S_0 =$ (for every pair, there's a road or not.) $= 2^{C(5,2)}$

$S_1 = N(c_1) + N(c_2) + N(c_3) + N(c_4) + N(c_5) = 5\cdot N(c_1) = 5\cdot 2^{C(4,2)}$

$S_2 = \binom{5}{2}\cdot N(c_1c_2) = 10\cdot 2^{C(3,2)}$ $\quad S_3 = \binom{5}{3}\cdot N(c_1c_2c_3) = 10\cdot 2^{C(2,2)}$

$S_4 = \binom{5}{4}\cdot N(c_1c_2c_3c_4) = 5\cdot 1$ $\quad S_5 = N(c_1c_2c_3c_4c_5) = 1$

$= 2^{10} - 5\cdot 2^6 + 10\cdot 2^3 - 20 + 5 - 1 = 1024 - 320 + 80 - 20 + 5 - 1 = 768$

**Ex** 6 married couples are to be seated at a circular table. In how many ways they can arrange themselves so that no wife sits next to her husbands.

$S=$ (set of all circular arrangements of 12 people)

$c_i =$ (ith couple sits together) $\Rightarrow N(\bar{c}_1\ \bar{c}_2\ \bar{c}_3\ \bar{c}_4\ \bar{c}_5\ \bar{c}_6) = ?$

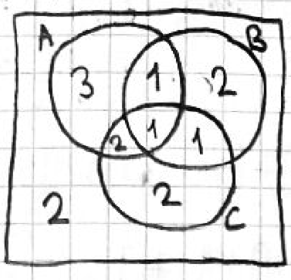
$S_0 = 11!$ $\quad S_1 = \binom{6}{1}\cdot N(c_1) = \binom{6}{1}\cdot \underbrace{10!\cdot 2}_{WH/HW}$ $\quad S_2 = \binom{6}{2}\cdot N(c_1c_2) = \binom{6}{2}\cdot \underbrace{9!\cdot 2\cdot 2}_{WH/HW\ \cdot\ WH/HW}$

So the answer is in general: $\sum_{r=0}^{6} (-1)^r \cdot \binom{6}{r}\cdot (11-r)!\cdot 2^r$

Subject : Date : ....../....../......

**Notation:** $E_m =$ number of elements in $S$ that satisfy exactly $m$-conditions of the $n$-conditions.

**Ex**



$c_1 =$ element is in A $\quad c_2 =$ element is in B $\quad c_3 =$ element is in C

$N(c_1) = 7 \quad N(c_2) = 5 \quad N(c_3) = 6 \quad N(c_1c_2c_3) = 1$

$N(c_1c_2) = 2 \quad N(c_1c_3) = 3 \quad N(c_2c_3) = 2$

$N(\bar{c}_1\bar{c}_2\bar{c}_3) = 14 - 18 + 7 - 1 = 2$

$S_0 = |S| = 14 \quad S_1 = 7+5+6 \quad S_2 = 2+3+2 \quad S_3 = 1$

$E_0 = N(\bar{c}_1\bar{c}_2\bar{c}_3) = 2 \quad E_1 = 3+2+2 = 7 \quad E_2 = 1+2+1 = 4 \quad E_3 = 1$

**Generalization of Inclusion - Exclusion:**
$$E_m = \sum_{r=m}^{n} (-1)^{r-m} \cdot \binom{r}{r-m} \cdot S_r$$
the before version is $m=0$

**Ex** $E_1 = \sum_{r=1}^{3} (-1)^{r-1} \cdot \binom{r}{r-1} \cdot S_r = \binom{1}{0} \cdot 18 - \binom{2}{1} \cdot 7 + \binom{3}{2} \cdot 1 = 18 - 2 \cdot 7 + 3 \cdot 1 = 7$

**Ex** Consider the village example given before. (5 villages.) Now find the number of systems of two-way roads so that exactly 2 villages are isolated.

$$E_2 = \sum_{r=2}^{5} (-1)^{r-2} \cdot \binom{r}{r-2} \cdot S_r = S_2 - 3S_3 + 6S_4 - 10S_5$$

**Definition:** Derangement is an arrangement where nothing is in its right place.

**Ex** Derangements of 123 are 231 and 312. 213 is not, for example.

**Notation:** $d_n =$ the number of derangements of $123\ldots n$.

**Theorem:**
$$d_n = \sum_{r=0}^{n} (-1)^r \cdot \binom{n}{r} \cdot (n-r)!$$

**Proof:** $S =$ all arrangements of $123\ldots n$ $\qquad c_i = i$ is in $i^{th}$ position

$$N(\bar{c}_1\bar{c}_2\bar{c}_3\ldots\bar{c}_n) = \sum_{r=0}^{n} (-1)^r \cdot S_r = \sum_{r=0}^{n} (-1)^r \cdot \binom{n}{r} \cdot (n-r)!$$

$S_r = \binom{n}{r} \cdot N(c_1c_2\ldots c_r) = \binom{n}{r} \cdot (n-r)!$

**Rook Polynomials:** (in Chapter 8 and 9)

Let $C$ be a region on a $(n \times n)$-chessboard. Then, $r_0(C) = 1$

$r_k(c) =$ (number of ways $k$ rooks can be placed on $C$) without being on the same row or column

$$r(C, x) = \sum_{k=0}^{\infty} r_k(c) \cdot x^k$$ } is called rook polynomial.

Ex|

| | | |
|---|---|---|
| 1 | 2 | 3 |
| ▨ | ▨ | 4 |
| ▨ | ▨ | 5 |

$C =$ union of squares $1, 2, 3, 4, 5$

$r_1(c) = 5 \quad r_2(c) = 4 \quad r_3(c) = 0 \quad r_4(c) = 0 \ldots\ldots$

rook poly of C.

$$r(c, x) = r_0(c) \cdot x^0 + r_1(c) \cdot x^1 + r_2(c) \cdot x^2 + r_3(c) \cdots = (1 + 5x + 4x^2)$$

**Theorem:** If $C_1$ and $C_2$ have no common row or column. Then $r(C, x) = r(C_1, x) \cdot r(C_2, x)$ where $C = C_1 \cup C_2$

Ex|

| | | |
|---|---|---|
| 1 | ▨ | ▨ |
| 2 | ▨ | ▨ |
| ▨ | ▨ | 3 |

$C_1 = 1, 2$ $\quad r(C_1, x) = 1 + 2x$

$C_2 = 3$ $\quad r(C_2, x) = 1 + x$

$\Big\}\ r(C, x) = (1 + 2x)(1 + x) = 1 + 3x + 2x^2$

Ex| Assume we have 4 people $P_1\ P_2\ P_3\ P_4$ and 5 seats $X_1\ X_2\ X_3\ X_4$ and $X_5$.

$P_1$ doesn't want to sit on $X_1$ or $X_2$

$P_2$ " " $X_2$

$P_3$ " " $X_3$ or $X_4$

$P_4$ " " $X_4$ or $X_5$

In how many ways these people can seat?

Notice every $P_i$ can sit only one $X$ and every $X$ can hold only one $P$.

| | $X_1$ | $X_2$ | $X_3$ | $X_4$ | $X_5$ |
|---|---|---|---|---|---|
| $P_1$ | 1 | 2 | ▨ | ▨ | ▨ |
| $P_2$ | ▨ | 3 | ▨ | ▨ | ▨ |
| $P_3$ | ▨ | ▨ | 4 | 5 | ▨ |
| $P_4$ | ▨ | ▨ | ▨ | 6 | 7 |

We place our rooks to the places they don't want to sit to count the negation

$S =$ (all possible seatings)

$c_i = i^{th}$ person is unhappy

$$N(\overline{c_1}\,\overline{c_2}\,\overline{c_3}\,\overline{c_4}) = S_0 - S_1 + S_2 - S_3 + S_4 = ?$$

$S_0 = P(5, 4)$

$S_1 = r_1(c) \cdot P(4, 3)$

$S_2 = r_2(c) \cdot P(3, 2)$

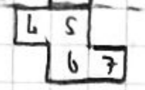
$S_3 = r_3(c) \cdot P(2, 1)$

$S_4 = r_4(c)$

We should compute $r(c, x)$ to find $r_1(c), r_2(c) \ldots$

Subject : Date ...../...../.....

$C_1 =$  $r(C_1, x) = 1 + 3x + x^2$

$C_2 =$  $r(C_2, x) = 1 + 4x + 3x^2$

$\Big\} (1+3x+x^2)(1+4x+3x^2) = \underbrace{1 + 7x + 16x^2 + 13x^3 + 3x^4}_{\text{So we found } r(C,x)}$

$\circledast\ S_0 - S_1 + S_2 - S_3 + S_4 = 120 - 7\cdot 24 + 16\cdot 6 - 13\cdot 2 + 3 = 25$

## Chapter 9)

Definition: A formal as follows: $\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \ldots$ is called the generating function for $\{a_n\}_{n=0}^{\infty}$.

Ex) The generating function for $\{n!\}_{n=0}^{\infty} = 1 + x + 2x^2 + 6x^3 + 24x^4 + \ldots = \sum_{n=0}^{\infty} n! \cdot x^n$

Ex) $r(C,x)$ was a generating function for $\{r_n(C)\}_{n=0}^{\infty}$

–Math 102– Definition: $\left(\begin{matrix}\text{Maclurin Series}\\ \text{of } f(x)\end{matrix}\right) = \overbrace{\sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} \cdot x^n}\ = f(x)$

Ex) $\left(\begin{matrix}\text{The Maclurin}\\ \text{Series of}\end{matrix}\ f(x) = \frac{1}{1-x}\right) = \sum_{n=0}^{\infty} x^n$ Proove this.

Assume $f(x) = \frac{1}{1-x}$. Then, $f^{(0)}(x) = \frac{1}{1-x}$ $f^{(1)}(x) = \frac{(-1)}{(1-x)^2} \cdot (-1) = \frac{1}{(1-x)^2}$

$f^{(2)}(x) = \frac{2}{(1-x)^3}$ $f^{(3)}(x) = \frac{6}{(1-x)^4}$ Then, Claim $f^{(n)}(x) = \frac{n!}{(1-x)^{n+1}}$ for $n \in \mathbb{N}$

Proof of claim: Step 1) Define $P(n) =$ " $f^{(n)}(x) = \frac{n!}{(1-x)^{n+1}}$ ".

Step 2) $P(0)$ is true because " $f^{(0)}(x) = f(x) = \frac{0!}{(1-x)^1}$ " is true.

Step 3) Assume $P(n)$ is true. $f^{(n+1)} = \frac{d}{dx}\left(f^{(n)}(x)\right) = \cdots = \frac{(n+1)!}{(1-x)^{n+2}}$ so we are done by Math. induction

So the result: $\left(\text{Maclurin series of } \frac{1}{1-x}\right) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} = \sum_{n=0}^{\infty} x^n$ $\quad f^{(n)}(0) \to \frac{n!}{(1-0)^{n+1}}$

**Notation:** If $\sum_{n=0}^{\infty} a_n x^n$ is the Maclurin Series of $f(x)$, then we can say the generating function for $\{a_n\}$ is $f(x)$.

Ex) $\left(\text{Generating function for } \{1\}_{n=0}^{\infty}\right) = \frac{1}{1-x}$

Subject : Date : ....../....../......

$\to f(x)=e^x \Rightarrow f^{(n)}(x)=e^x$, $n\in\mathbb{N}$

Ex| (The generating function for $\{\frac{1}{n!}\}_{n=0}^{\infty}) = e^x$ So $\frac{f^{(n)}(0)}{n!} = \frac{e^0}{n!} = \frac{1}{n!}$

Theorem ① If $f(x)=\sum_{n=0}^{\infty} a_n x^n$ for all $x\in(-\varepsilon,\varepsilon)$ for some $\varepsilon>0$ then the Maclurin series of $f(x)$ is $\sum_{n=0}^{\infty} a_n x^n$

Theorem ② $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ for all $x$ in $(-1,1)$.

Theorem ③ $e^x = \sum_{n=0}^{\infty} \frac{1}{n!}x^n$ for all $x$ in $(-\infty,\infty)$.

Ex| Find the generating for $\{(-1)^n\}_{n=0}^{\infty}$

$$\frac{1}{1+x} = \frac{1}{1-(-x)} \overset{\text{by ②}}{=} \sum_{n=0}^{\infty}(-x)^n = \sum_{n=0}^{\infty}(-1)^n x^n \text{ for all } x \text{ in } (-1,1)$$

By theorem ①, (the Maclurin for $\frac{1}{1+x}$) $= \sum_{n=0}^{\infty}(-1)^n x^n$, hence, Gen for $\{(-1)^n\}_{n=0}^{\infty} = \frac{1}{1+x}$

Ex| If $a_n = \begin{cases} 1, & n \text{ is even.} \\ 0, & n \text{ is odd.}\end{cases}$ Gen. for $\{a_n\}_{n=0}^{\infty} = 1+x^2+x^4+x^6\ldots = \frac{1}{1-x^2}$

Definition: Partition of a number $n$ is a sum in the following:

$$n = n_1+n_1+\ldots+n_1+n_2+n_2+\ldots+n_2+n_3+n_3+n_3+\ldots+n_k+n_k+\ldots+n_k$$

where $k\geq 1$ and $n_1>n_2>\ldots>n_k\geq 1$

Ex| Partition of 4: $4=4$, $4=3+1$, $4=2+2$, $4=2+1+1+1$, $4=1+1+1+1$

Ex| $P(4)=5$

Notation: $P(0)=0$ $P(n)=$ the number of partitons of $n$.

Fact: (Generating for $\{P(n)\}_{n=0}^{\infty}) = \prod_{k=1}^{\infty}\frac{1}{1-x^k}$

$4=4$
$4=3+1$

Notation: $P_{distinct}(0)=1$ $P_{distinct}(n)=$ the number of partitions with different summands

Ex| $P(4)=2$

Fact; (Generating for $\{P_{distinct}(n)\}_{n=0}^{\infty}) = \prod_{k=1}^{\infty}(1+x^k)$

Subject : Date : ..../..../....

$4=4$
$4=2+2$

**Ex** $P(4)=2$

**Notation:** $P_{even}(0)=1$ $P_{even}(n)=$ number of partitions with even summands

**Fact:** (Generating for $\{P_{even}(n)\}$) $= \prod_{k=1}^{\infty} \frac{1}{1-x^{2k}}$

**Notation** $P_{odd}(0)=1$ $P_{odd}(n)=$ number of partitions with odd summands

**Fact:** (Generating for $\{P_{odd}(n)\}$) $= \prod_{k=1}^{\infty} \frac{1}{1-x^{2k-1}}$

☆

| n | $P_{odd}$ | | $P_{distinct}$ |
|---|---|---|---|
| 0 | 1 | = | 1 |
| 1 | 1 | = | 1 |
| 2 | 1 | = | 1 |
| 3 | 2 | = | 2 |

| n | $P_{odd}$ | | $P_{distinct}$ |
|---|---|---|---|
| 4 | 2 | = | 2 |
| 5 | 3 | = | 3 |
| 6 | 4 | = | 4 |

**Theorem:** $P_{odd}(n) = P_{distinct}(n)$ for all $n \in \mathbb{N}$

Proof: (Generating for $P_{distinct}(n)$) $= (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$

$$= \frac{(1-x^2)}{(1-x)} \cdot \frac{(1-x^4)}{(1-x^2)} \cdot \frac{(1-x^6)}{(1-x^3)} \cdot \frac{(1-x^8)}{(1-x^4)} = $$

$$= \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^3}\right)\left(\frac{1}{1-x^5}\right)\cdots = \text{(Generating for } P_{odd}(n)).$$

**Ex** For $n \in \mathbb{N}$ define $a_n = |\{(x_1,x_2,x_3) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} \mid x_1+2x_2+3x_3=n \text{ and } \forall i\ x_i \geq 0\}|$

$a_1 = 1$ $(x_1=1,\ x_2=0,\ x_3=0)$ $a_3 = 3$ $((3,0,0),(1,1,0),(0,0,1))$

$a_2 = 2$ $((2,0,0),(0,1,0))$ $a_4 = 4$ $((4,0,0),(1,0,1),(0,2,0),(2,1,0))$

$a_5 = 5$ $((5,0,0),(1,2,0),(3,1,0),(2,0,1),(0,1,1))$ $a_6 = 7$ $((6,0,0),(4,1,0),(3,0,1),(0,3,0),(0,0,2),(2,2,0),(1,1,1))$

$\{a_n\}_{n=0}^{\infty} =$ (We can consider $a_n$ as number of partitions of $n$ with summands equal to 1 or 2 or 3) $= \underbrace{\left(\frac{1}{1-x}\right)}_{1+x^1+x^2\cdots}\underbrace{\left(\frac{1}{1-x^2}\right)}_{1+x^2+x^4\cdots}\underbrace{\left(\frac{1}{1-x^3}\right)}_{\cdots}$

~~So we take only first 3 part of the formula $\{P(n)\}$ generating~~

**Theorem:** If $\sum_{n=0}^{\infty} a_n x^n$ is a real number for all $x$ in $(-\varepsilon, \varepsilon)$ for some $\varepsilon > 0$. Then, $\frac{d}{dx}\left(\sum_{n=0}^{\infty} a_n x^n\right) = \sum_{n=1}^{\infty} a_n n x^{n-1}$

**Ex** We know (- from last lecture -) $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$ when $x$ is in $(-1,1)$

So we can say $\frac{d}{dx}\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2} = \frac{d}{dx}\left(\sum_{n=0}^{\infty} x^n\right) = \sum_{n=1}^{\infty} n x^{n-1}$

Subject : Date : ....../....../......

Ex] (Generating function for $\{n\}_{n=0}^{\infty}$) $= \sum_{n=0}^{\infty} n x^n = \sum_{n=1}^{\infty} n x^n = x \cdot \overbrace{\sum_{n=1}^{\infty} n \cdot x^{n-1}}^{\frac{1}{(1-x)^2}} = \frac{x}{(1-x)^2}$

↳ Lets see if its true: $\frac{x}{(1-x)^2} = x \cdot \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x}\right) = x(1+x+x^2+x^3 \dots)(1+x+x^2+x^3 \dots) = 1x + 2x^2 + 3x^3 + 4x^4 \dots$ ✓

(GOOD) Ex] $\left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\left(\frac{1}{1-x^3}\right) = 1 + 1x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6$ see the previous example

$(1+x+x^2+x^3 \dots)(1+x^2+x^4+x^6 \dots)(1+x^3+x^6+x^9 \dots)$

New Chapter

old generating function

**Definition:** (The exponential generating func for $a_n$) $= \sum_{n=0}^{\infty} \frac{a_n}{n!} \cdot x^n$

Ex] (The exp. generating for $\{1\}_{n=0}^{\infty}$) $= e^x$

Note: If we want to count something and the order is not important (e.g number of partitions $\begin{smallmatrix} 3=3 \\ 3=2+1 \\ 3=1+1+1 \end{smallmatrix}$) then, we use generating functions. If the order is important, then use exponential generating functions.

Ex] In how many ways can 3 of the letters TALLAHASSEE be arranged?

→ The old counting method takes too long since the combinations of 3 are too many.

Define $a_n$ = (number of arrangements of n letters in TALLAHASSEE), $a_3 = ?$

⊛ = Exp. Gen. For $\{a_n\}_{n=0}^{\infty} = \underset{(3\ A\text{'s})}{\left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!}\right)}\underset{(2L,\,2S,\,2E)}{\left(1+x+\frac{x^2}{2!}\right)^3}\underset{(1T,\,1H)}{(1+x)^2}$ We are taking the first terms of $\{1\}_{n=0}^{\infty}$ generating.

⊛ $= 1 + 6x + 17x^2 + \frac{181}{6}x^3 + \frac{112}{3}x^4 \dots + x^{?}$ (finite) $\Rightarrow \frac{a_3}{3!} = \frac{181}{6} \Rightarrow a_3 = 181$

Ex] Lets find for 4 letters: $\frac{112}{3} = \frac{a_4}{4!} \rightarrow \frac{a_n}{n!} \Rightarrow \frac{112}{3} \cdot 4! = 896$

Ex] $a_n$ = (number of functions from $\{1,2,3 \dots n\}$ to $\{1,2,3,4,5\}$)

Then find the exponential generating function for $\{a_n\}_{n=0}^{\infty}$.

Solution 1]

$a_n = |\{1,2,3,4,5\}|^{|\{1,2,3 \dots n\}|} = 5^n$

$\sum_{n=0}^{\infty} \frac{5^n}{n!} \cdot x^n = \sum_{n=0}^{\infty} \frac{(5x)^n}{n!} = e^{5x}$

Solution 2) $= \underbrace{\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}\dots\right)}_{|\{x \mid f(x)=1\}|}\underbrace{\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}\dots\right)}_{|\{x \mid f(x)=2\}|}\cdots$ [5 times] $= e^x \cdot e^x \cdot e^x \cdot e^x \cdot e^x = e^{5x}$

Ex) $b_n$ = (Number of onto functions from $\{1,2,3,\dots,n\}$ to $\{1,2,3,4,5\}$)
Find the exponential generating function for $\{b_n\}_{n=0}^{\infty}$

→ We eliminate the 1's from the previous solutions because those 1's means there's no element that goes to that value.

$$= \underbrace{\left(x+\frac{x^2}{2!}+\frac{x^3}{3!}\dots\right)}_{|x \mid f(x)=1| \geq 1}\underbrace{\left(x+\frac{x^2}{2}+\frac{x^3}{3}\dots\right)}_{|x \mid f(x)=2| \geq 1}\cdots \text{[5 times]} = (e^x-1)^5$$

## Chapter 10)

Definition: Let $m \in \mathbb{Z}^+$ and $C_0, C_1, \dots, C_m$ be real numbers if $C_0 \neq 0$ and $C_m \neq 0$ then an equation in form $[C_0 a_n + C_1 a_{n-1} \dots + C_m a_{n-m} = f(n)]$ is called a linear recurrence relation of order $m$. Moreover if $f(n)=0$ for all $n$, then it's called homogeneous, otherwise it's non-homogeneous.

→ (Informal Def) Linear means all coefficients of $a_n, a_{n-1}$ things are real.

Ex)

| Equation | Is Linear | Order | Is Homogeneous |
|---|---|---|---|
| $7a_n + a_{n-1} = 0$ | Yes | 1 | Yes |
| $a_n + a_{n+3} + a_{n-4} = n$ | Yes | 7 | No |
| $n^2 a_{n+3} + 5a_n = 0$ | No | 3 | Yes |
| $a_n + a_{n+3} + n^3 = 0$ | Yes | 3 | No |
| $a_{n+5} = a_{n-1} + a_{n-3}$ | Yes | 8 | Yes |

Definition: The polynomial $C_0 r^m + C_1 r^{m-1} + \dots + C_{m-1} r + C_m$ is called the characteristic polynomial for the equation $C_0 a_n + C_1 a_{n-1} + \dots + C_m a_{n-m} = 0$.
Moreover, roots of this polynomial are called characteristic roots for the equations.

Subject : Date :......./......./.......

Ex) Equation | Characteristic Polynomial | Characteristic Roots

| Equation | Characteristic Polynomial | Characteristic Roots |
|---|---|---|
| $a_n - 5a_{n-1}$ | $r-5$ | $5$ |
| $a_n - 3a_{n-1} + 2a_{n-2} = 0$ | $r^2 - 3r + 2 = 0$ | $1, 2$ |
| $a_{n+2} = 6a_{n+1} - 9a_n$ | $r^2 - 6r + 9 = 0$ | $3$ |
| $4a_n + a_{n+2} = 0$ | $r^2 + 4$ | $-2i, 2i$ |

① If $r_0$ is a char. root for $C_0 a_n + \cdots + C_m a_{n-m} = 0$ then, $a_n = K \cdot r_0^n$ is a solution for $C_0 a_n + C_1 a_{n-1} + \cdots + C_m a_{n-m} = 0$.

**Proof:** If we substitute $a_n = K \cdot r_0^n$, we get: $K r_0^{n-m} \underbrace{(C_0 r_0^m + C_1 r_0^{m-1} + \cdots + C_m)}_{=0 \text{ because its the char poly.}} = 0$

② If $(r - r_0)^s$ divides the char. poly. for $C_0 a_n + \cdots + C_m a_{n-m} = 0$ then, $a_n = K \cdot n^{s-1} \cdot r_0^n$ is a solution for $C_0 a_n + \cdots + C_m a_{n-m} = 0$.

③ If $\overline{a}_n$ and $\overline{\overline{a}}_n$ are two solutions for $C_0 a_n + \cdots + C_m a_{n-m} = 0$, then, $\overline{a}_n + \overline{\overline{a}}_n$ is also a solution for it.

**Theorem:** If $\prod_{i=1}^{k} (r - r_i)^{s_i}$ is char polynomial for $C_0 a_n + \cdots + C_m a_{n-m} = 0$ then, the general solution for $C_0 a_n + \cdots + C_m a_{n-m} = 0$ is $a_n = \sum_{i=1}^{k} \sum_{j=0}^{s_i - 1} K_{ij} n^j r_0^n$.

⊛⊛
⊛ Method for solving homogeneous linear rec. relation $C_0 a_n + \cdots + C_m a_{n-m} = 0$ with initial values $a_0 = A_0$, $a_1 = A_1, \ldots, a_{m-1} = A_{m-1}$:

Step 1) Find the general solution for $C_0 a_n + \cdots + C_m a_{n-m} = 0$.

Step 2) Use initial values.

Ex) Solve $a_n - 5a_{n-1} = 0$ and $a_0 = 3$? Char poly is: $r - 5$. So the general solution is: $a_n = K \cdot 5^n$, Then use this: $3 = a_0 = K \cdot 5^0 \Rightarrow K = 3$

$a_n = 3 \cdot 5^n$

Subject : Date : ..../..../....

Ex| Solve $a_n - 3a_{n-1} + 2a_{n-2} = 0$ where $n \geq 2$, $a_0 = 0$, $a_1 = 1$

The char poly for it: $r^2 - 3r + 2 = (r-1)(r-2)$

The general solution: $a_n = K_1 \cdot 1^n + K_2 \cdot 2^n$

Then we use initials: $0 = a_0 = K_1 \cdot 1^0 + K_2 \cdot 2^0 \Rightarrow K_1 + K_2 = 0$

So answer: $a_n = -1 + 2^n$ $\quad 1 = a_1 = K_1 \cdot 1^1 + K_2 \cdot 2^1 \Rightarrow K_1 + 2K_2 = 1$ $\Big\}$ $K_1 = -1$, $K_2 = 1$

Ex| Solve $a_n - 6a_{n-1} + 9a_{n-2} = 0$ where $n \geq 2$ and $a_0 = 1$, $a_1 = 1$

The char poly for it: $r^2 - 6r + 9 = 0 = (r-3)^2 = 0$ $\qquad 3^n - 2n3^{n-1}$

The general solution: $a_n = K_1 \cdot 3^n + K_2 \cdot n \cdot 3^n$ comes from $2^{nd}$ I sign.

Then we use initials: $1 = a_0 = K_1 \cdot 3^0 + K_2 \cdot 0 \cdot 3^0 \Rightarrow K_1 = 1$

So answer: $3^n - 2n \cdot 3^{n-1}$ $\quad 1 = a_1 = K_1 \cdot 3^1 + K_2 \cdot 1 \cdot 3^1 \Rightarrow 3K_1 + 3K_2 = 3 \Rightarrow K_2 = \frac{-2}{3}$

Ex| Fibonacci numbers: $F_n = F_{n-1} + F_{n-2}$. $F_0 = 0$, $F_1 = 1$. Find $F_n$.

The char poly for $F_n - F_{n-1} - F_{n-2} = 0$ is: $r^2 - r - 1 = 0 = \left(r - \frac{1-\sqrt{5}}{2}\right)\left(r - \frac{1+\sqrt{5}}{2}\right)$

The general solution: $F_n = K_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n + K_2 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n$

Then we use initials: $0 = F_0 = K_1 + K_2$

$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$ $\quad 1 = F_1 = K_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right) + K_2 \cdot \left(\frac{1+\sqrt{5}}{2}\right)$ $\Big\}$ $K_1 = \frac{-1}{\sqrt{5}}$ $\quad K_2 = \frac{1}{\sqrt{5}}$

Ex| $a_n = \left(\text{The number of binary sequences of length } n \text{ that have no consecutive 0's}\right)$. Find $a_n$

$a_n = \left(\begin{array}{c}\text{the ones with} \\ \text{ends with 0}\end{array}\right) + \left(\begin{array}{c}\text{the ones with} \\ \text{ends with 1}\end{array}\right)$

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

And we have $a_0 = 1$ ("")
$a_1 = 2$ ("0", "1")

Hence $a_n = F_{n+2}$ shifted two elements $=$

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

Subject : Date :

(*) (*)

(*) **Method** for solving non-homogeneous linear rec. relations $C_0 a_n + \cdots + C_m a_{n-m} = f(n)$ with initial conditions $a_0 = A_0$, $a_1 = A_1$, ...: $A_{m-1} = A_{m-1}$

Step 1) Find the general solution for $C_0 a_n + \cdots + C_m a_{n-m} = 0$. call it $a_n^{(h)}$

Step 2) Find one solution for $C_0 a_n + \cdots + C_m a_{n-m} = f(n)$, call it $a_n^{(p)}$

Step 3) Use initial conditions by considering $a_n = a_n^{(h)} + a_n^{(p)}$ (particular solution)

Hints for Step 2: If $f(n) = C \cdot n^k$, try $a_n^{(p)} = \bar{A}_0 + \bar{A}_1 n + \cdots \bar{A}_k n^k$

If $f(n) = C \cdot r^n$, try $a_n^{(p)} = A r^n$

If $f(n) = C \cdot \cos(n\theta)$, try $a_n^{(p)} = K_1 \cdot \cos(n\theta) + K_2 \cdot \sin(n\theta)$

Ex) Solve $a_n - 2a_{n-1} = n$ and $a_0 = 1$.

Step 1) The char poly for $a_n - 2a_{n-1} = 0$ is $r-2$

So the general solution is $a_n^{(h)} = K \cdot 2^n$

Step 2) $f(n) = n$ so, we can try $a_n^{(p)} = \bar{A}_0 + \bar{A}_1 n$.

We want $n = (\bar{A}_0 + \bar{A}_1 n) - 2(\bar{A}_0 + \bar{A}_1(n-1)) = (-\bar{A}_1)n + (-\bar{A}_0 + 2\bar{A}_1)$

So we found $\bar{A}_1 = -1$, $\bar{A}_0 = -2$. So $a_n^{(p)} = -2-n$

Step 3) $a_n = a_n^{(h)} + a_n^{(p)} = K \cdot 2^n - 2 - n$, we know $1 = a_0 = K - 2 \Rightarrow K = 3$

So the answer is $a_n = 3 \cdot 2^n - 2 - n$

Ex) Solve $a_n - 5a_{n-1} = 8 \cdot 3^n$ and $a_0 = 8$

Step 1) the char poly for $a_n - 5a_{n-1} = 0$ is $r - 5$

So the general solution is $a_n^{(h)} = K \cdot 5^n$

Step 2) $f(n) = 8 \cdot 3^n$ so, we can try $a_n^{(p)} = A \cdot 3^n$

$24 \cdot 3^{n-1} = 8 \cdot 3^n = a_n^{(p)} - 5a_{n-1}^{(p)} = A \cdot 3^n - 5 \cdot A \cdot 3^{n-1} = (3A - 5A) \cdot 3^{n-1} \Rightarrow A = -12$

Step 3) $a_n = a_n^{(h)} + a_n^{(p)} = K \cdot 5^n - 12 \cdot 3^n$  $a_0 = 8 = K - 12 \Rightarrow K = 20$

So the answer is $a_n = 20 \cdot 5^n - 12 \cdot 3^n$

Subject : Date : ....../....../......

Ex| Solve $a_n - 5a_{n-1} = 6n^2$ and $a_0 = 1$

Step 1) As in previous example $a_n^{(h)} = K\cdot 5^n$

Step 2) Try $a_n^{(p)} = A_0 n + A_1 n + A_2 n^2$

$6n^2 = a_n^{(p)} - 5a_{n-1}^{(p)} = (A_0 + A_1 n + A_2 n^2) - 5(A_0 + A_1(n-1) + A_2(n-1)^2)$ $\to$ $A_0 = \frac{-45}{16}$, $A_1 = \frac{-15}{4}$, $A_2 = \frac{-3}{2}$

Step 3) $a_n = a_n^{(h)} + a_n^{(p)}$ , $1 = a_0 = K - \frac{45}{16} \Rightarrow a_n = \frac{61}{16}5^n - \frac{3}{2}n^2 - \frac{15}{4}n - \frac{45}{16}$

Note: Sometimes the hint does not work (step 2) so try multiplying with a power of n. $\to a_n^{(p)}$

Ex| Solve $a_n - 3a_{n-1} = 5\cdot 3^n$ and $a_0 = 2$

Step 1) $r - 3 = 0 \Rightarrow a_n^{(h)} = K\cdot 3^n$

Step 2) Try $a_n^{(p)} = A\cdot 3^n \Rightarrow 5\cdot 3^n = A\cdot 3^n - 3\cdot A\, 3^{n-1} = 0 \to$ impossible

Then try, $a_n^{(p)} = A\cdot n\cdot 3^n \Rightarrow 5\cdot 3^n = a_n^{(p)} - 3a_{n-1}^{(p)} = A\cdot n 3^n - 3A(n-1)3^{n-1} \Rightarrow A = 5$

Step 3) $a_n = a_n^{(h)} + a_n^{(p)} = K\cdot 3^n + 5n\cdot 3^n$ $\quad 2 = a_0 = K \Rightarrow \quad a_n = 2\cdot 3^n + 5n3^n$

Ex| Let $a_n = f_{worst}(n)$ for the procedure Bubble Sort.

$\to a_n = a_{n-1} + (n-1)$ $\to$ swapping through from last index to first $\qquad a_2 = 1$ $\to$ One swap

Step 1) The char. polynomial for $a_n - a_{n-1} = 0$ is $r - 1 \Rightarrow a_n^{(h)} = K\cdot 1^n = K$

Step 2) Try $a_n^{(p)} = A_0 + A_1 n \Rightarrow n - 1 = a_n^{(p)} - a_{n-1}^{(p)} = A_0 + A_1 n - A_0 + A_1(n-1) = A_1$ [impossible]

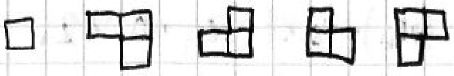
Try $a_n^{(p)} = (A_0 + A_1 n)n \qquad n - 1 = (A_0 + A_1 n)n - (A_0 + A_1(n-1))(n-1) \to A_1 = \frac{1}{2}, \; A_0 = -\frac{1}{2}$

Step 3) $a_n = a_n^{(h)} + a_n^{(p)} = K + \frac{n(n-1)}{2}$

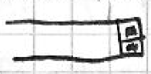
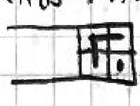
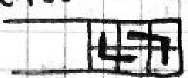
Ex| $a_n = \begin{pmatrix} \text{number of ways we can} \\ \text{cover a } 2\times n \text{ chessboard} \\ \text{with tiles } ⊟ \text{ and } ◫ \end{pmatrix}$ Find $a_n$.

$a_n = \underbrace{a_{n-2}}_{\text{Number of cases}} + \underbrace{a_{n-1}}_{\text{Number of cases}} \Rightarrow a_n = F_{n+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$

$\hookrightarrow$ Fibonacci numbers

$a_n = \left( \begin{array}{l} \text{Number of ways we can cover} \\ \text{a } 2\times n \text{ chessboard with tiles} \end{array} \right.$  $)$

$a_1 = 1 \quad a_2 = 5 \quad a_3 = 11$ (We find them by drawing)

$a_n = \Big($ ends with  $\Big) + 4 \cdot \Big($ ends with  $\Big) + 2 \cdot \Big($ ends with  $\Big)$

$$a_n = a_{n-1} + 4a_{n-2} + 2a_{n-3}$$

Step 1) $a_n - a_{n-1} - 4a_{n-2} - 2a_{n-3} = 0$

$r^3 - r^2 - 4r - 2 = 0 = (r+1)(r^2 - 2r - 2) \to r = -1, \; r = 1 \pm 3$

The general solution for $a_n - a_{n-1} - 4a_{n-2} - 2a_{n-3}$ : $a_n = K_1 \cdot (-1)^n + K_2 (1+\sqrt{3})^n + K_3 (1-\sqrt{3})^n$

Step 2)
$$\left.\begin{array}{l} 1 = a_1 = -K_1 + K_2(1+\sqrt{3}) + K_3(1-\sqrt{3}) \\ 5 = a_2 = K_1 + K_2(1+\sqrt{3})^2 + K_3(1-\sqrt{3})^2 \\ 11 = a_3 = -K_1 + K_2(1+\sqrt{3})^3 + K_3(1-\sqrt{3})^3 \end{array}\right\} \begin{array}{l} K_1 = 1 \\ K_2 = \frac{1}{\sqrt{3}} \\ K_3 = \frac{-1}{\sqrt{3}} \end{array} \Bigg| \; a_n = (-1)^n + \frac{1}{\sqrt{3}}(1+\sqrt{3})^n - \frac{1}{\sqrt{3}}(1-\sqrt{3})^n$$

(*) We solved linear rec. relations. Use the following method for non-linear recursion relations

Ex) Solve $a_n - 3a_{n-1} = 0$ and $a_0 = 5$ with non-linear method instead.

Define $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Then $0 = \sum_{n=1}^{\infty} (a_n - 3a_{n-1}) \cdot x^n = *$

$\frac{1}{1-\alpha} = \sum_{n=0}^{\infty} \alpha^n$

$* = \sum_{n=1}^{\infty} a_n x^n - 3 \cdot \sum_{n=1}^{\infty} a_{n-1} x^n \Rightarrow \left( \sum_{n=0}^{\infty} a_n x^n - a_0 \right) - 3 \left( x \cdot \sum_{n=1}^{\infty} a_{n-1} x^{n-1} \right) \Rightarrow$

$(f(x) - 5) - 3 \left( x \cdot \sum_{n=0}^{\infty} a_n x^n \right) \Rightarrow 0 = (f(x) - 5) - 3(x \cdot f(x)) \Rightarrow f(x) = \frac{5}{1-3x} \to 5 \cdot \frac{1}{1-3x}$

$= 5 \cdot \sum_{n=0}^{\infty} (3x)^n = \sum_{n=0}^{\infty} 5 \cdot 3^n \cdot x^n$ , $a_n$

-Review

Ex) Prove that $\sum_{i=0}^{n} F_i^2 = F_n \cdot F_{n+1}$ for all $n \geq 1$.

$F_n$ is fibonacci numbers

$F_0 = 0 \quad F_1 = 1 \quad F_2 = 1 \ldots$

① $S(n) = " \sum_{i=0}^{n} F_i^2 = F_n \cdot F_{n+1} "$

② $S(1)$ is true because $0^2 + 1^2 = 1 \cdot 1$

$S(2)$ is true because $0^2 + 1^2 + 1^2 = 1 \cdot 2$

Subject : Date : ....../....../......

③ Assume $S(n)$ is true, $n \geq 2$. Then:

$$\sum_{i=0}^{n+1} F_i^2 = \sum_{i=0}^{n} F_i^2 + F_{n+1}^2 = F_n \cdot F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1} \cdot F_{n+2}$$

④ So we are done by Math. Induction

Ex) Prove that 57 divides $7^{n+2} + 8^{2n+1}$ for all $n$ in $\mathbb{Z}^+$.

① Define $S(n) =$ " $57 \mid (7^{n+2} + 8^{2n+1})$ "

② $S(1)$ is true because $7^{1+2} + 8^{2+1} = 343 + 512 = 855$ and $\frac{855}{57} = 15$

③ Assume $S(n)$ is true. We want to prove for $7^{(n+1)+2} + 8^{2(n+1)+1}$

$$7^{n+3} + 8^{2n+3} = 7 \cdot 7^{n+2} + 64 \cdot 8^{2n+1} =$$

$$64 \cdot 7^{n+2} + 64 \cdot 8^{2n+1} - 57 \cdot 7^{n+2} = 64\underbrace{(7^{n+2} + 8^{2n+1})}_{57 \mid} - \underbrace{57 \cdot 7^{n+2}}_{57 \mid}$$

④ By Math Induction, $S(n)$ is true for all $n \in \mathbb{Z}^+$

Ex) Show that if we select 101 integers from the $S = \{1, 2, 3, \ldots, 200\}$ there exist $m, n$ in the selection such $\gcd(m, n) = 1$

① Pigeons = selected 101 integers

Pigeonholes = $\{\{1,2\}, \{3,4\}, \{5,6\}, \ldots, \{199, 200\}\}$

② Pigeon $x$ goes to pigeonhole $y$ if $x \in y$.

③ Number of pigeonholes $= 100 < 101 =$ Number of pigeons

④ By pigeon principle there exist $m, n$ in the selected 101 integers which go to the same pigeonhole $\{k, k+1\}$. Without loss of generality, we can assume $m = k$ and $n = k$. So $\gcd(m, n) = (k, k+1) = 1$

Ex) Show that if any 14 integers are selected from the set $S = \{1, 2, 3 \ldots 25\}$, there are at least two integers whose sum is 26.

Subject : Date :....../....../......

Pigeons = Selected 14 integers

Pigeonholes = $\{\{1,25\}, \{2,24\}, \dots, \{12,14\}, \{13\}\}$

Send pigeon $x$ to pigeonhole $y$ if $x \in y$

Number of pigeons $= 14 > 13 =$ Number of pigeonholes.

So by pigeonhole principle, there exist two pigeons $x_1, x_2$ and a pigeonhole $y$ such that $x_1 \in y$ and $x_2 \in y$.

Notice $y \neq \{13\}$ because $|\{13\}| = 1$ but $|y| = 2$. So $y = \{x_1, x_2\}$ is either $\{1,25\}$ or $\{2,24\}$ or ... $\{12,14\}$. So we have $x_1 + x_2 = 26$

Ex| Let $S \subset (\mathbb{Z}^+ \times \mathbb{Z}^+)$. Find the minimum value of $|S|$ that guarantees the existance of distinct ordered pairs $(x_1, x_2), (y_1, y_2) \in S$ such that $x_1 + y_1$ and $x_2 + y_2$ are both even.

$|S| = m_0 = 5$ by following two facts:

1) $m_0 > 4$. Proof: Take $S = \{(1,1), (1,2), (2,1), (2,2)\}$

2) $m_0 \leqslant 5$. Proof: We should show that assuming $|S| \geqslant 5$ guarantees the condition.

Assume $|S| \geqslant 5$; Pigeons $= S$ Pigeonholes $= \{(odd, odd), (odd, even), (even, even), (even, odd)\}$

Pigeon $(x, y)$ goes to $(u, v)$ if $x$ is $u$
$y$ is $v$.

Number of pigeons $= |S| \geqslant 5 > 4 =$ Number of pigeonholes.

So by pigeonhole principle, there exist $(x_1, x_2), (y_1, y_2) \in S$ and there exist a pigeonhole $(u, v)$. So $x_1, y_1$ are both even are both odd. Also, $x_2, y_1$ are both even or both odd. Hence $(x_1 + y_1)$ and $(x_2 + y_2)$ are both even.

Ex| If 11 integers are selected from $S = \{1, 2, 3, \dots 100\}$, prove that there are two numbers such $0 < |\sqrt{x} - \sqrt{y}| < 1$.

Pigeons = Selected 11 integers

Pigeonholes = $\{(0,1], (1,2], (2,3], \dots, (9,10]\}$

Pigeon $x$ goes to pigeonhole $I$, $\sqrt{x} \in I$

Number of pigeons = 11 > 10 = Number of pigeonholes

By pigeonhole principle, there exist two numbers $x$ and $y$ and $\sqrt{x}$, $\sqrt{y}$ are in the same pigeonhole interval, $I = (n, n+1]$ Hence $0 < |\sqrt{x} - \sqrt{y}| < 1$

Ex) Let $f, g, h$ denote the following closed binary operations on $P(\mathbb{Z}^+)$. → power set

For $A, B \subseteq \mathbb{Z}^+$, $f(A,B) = A \cap B$, $g(A,B) = A \cup B$, $h(A,B) = A \Delta B$

where closed binary operation on $X$ means a function from $X \times X$ to $X$.

and $U \Delta V = (U \setminus V) \cup (V \setminus U)$.

→ $f$ is not one-to-one: $\{1\} \cap \{2\} = \emptyset = \{3\} \cap \{4\}$

$g$ is not one-to-one: $\{1\} \cup \{2\} = \emptyset = \{1,2\} \cup \emptyset$

$h$ is not one-to-one: $\{1\} \Delta \{1\} = \emptyset = \emptyset \Delta \emptyset$

→ $f$ is onto: For any $A \in P(\mathbb{Z}^+)$ we have $A \cap A = A$

$g$ is onto: For any $A \in P(\mathbb{Z}^+)$ we have $A \cup \emptyset = A$

$h$ is onto: For any $A \in P(\mathbb{Z}^+)$ we have $A \Delta \emptyset = A$

— End of Review —

## Chapter 11)

nothing means undirected.

Definition: A graph is a pair $(V, E)$ such that $V$ is a non-empty set and $E \subseteq \{e \subseteq V \mid |e| = 1 \text{ or } |e| = 2\}$.

Elements of $V$ are called verticles (vertex).

Elements of $E$ are called edges.

Ex) If $V = \{1, 2, 3\}$ and $E = \{\{1\}, \{2,3\}, \{1,3\}\}$

then $(V, E)$ is a graph.

★ points for verticles

★ arcs for edges

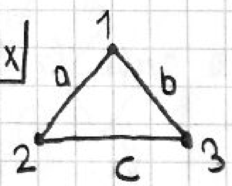
Subject : Date : ....../....../......

Definition: A directed graph is a pair $(V, E)$ such that $V$ is a non-empty set and $E \subseteq V \times V$

Ex) $V = \{1, 2, 3\}$ $E = \{(1,1), (2,3), (1,3), (3,1)\}$


Definition: A walk on a graph $(V, E)$ from $x$ to $y$ is a sequence in the following form $v_0 e_1 v_1 e_2 v_2 e_3 \dots v_{n-1} e_n v_n$ where $v_0 = x$ and $v_n = y$ and $\forall i$ $v_i \in V$, $e_i \in E$, $e_i = \{v_{i-1}, v_i\}$

Ex)



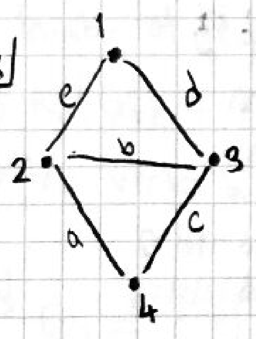

1a2b1c3 is not a walk; $2 \notin b$, $1 \notin c$.

1a2c3 is a walk.

⊛ We say the length of the walk is $n$ (number of edges).

⊛ The walk is;
1. a path if no vertex is repeated other than $v_0 = v_n$.
2. a cycle if is a path and $v_0 = v_n$.
3. a trail if no edge is repeated
4. a circuit if no edge is repeated and $v_0 = v_n$

Ex)

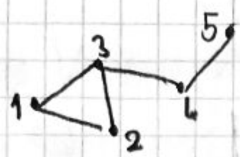
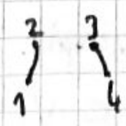



| Walk | path | cycle | trail | circuit |
|---|---|---|---|---|
| 1e2a4c3b2 | | | Yes | |
| 1e2b3c4 | Yes | | Yes | |
| 1e2a4c3b2e1 | | | | |
| 1e2a4c3d1 | Yes | Yes | Yes | Yes |
| 1e2e1 | Yes | Yes | | |

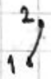
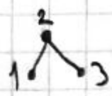
Definition: A graph $(V, E)$ is called connected if,

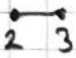
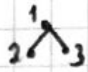
$\forall v_1 \in V$ $\forall v_2 \in V$ if $v_1 \neq v_2$ then there is a path $v_1$ to $v_2$ in $(V, E)$

Subject : Date : ...../...../.....

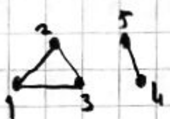
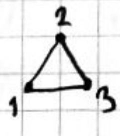
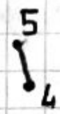
Ex  is connected. Ex  is not connected. (No path 1 to 3).

Definition: We say $(W, F)$ is a subgraph of $(V, E)$ if $W \subseteq V$ and $F \subseteq E$ and $(W, F)$ is a graph.

Ex  is a subgraph of  ; $(\{1\}, \{\{2,3\}\})$ is not a subgraph of $(\{1,2,3\}, \{\{2,3\}\})$.

 is not a subgraph of 

Definition: We say $H$ is a connected component of a graph $G$ if,
(i) $H$ is subgraph of $G$. (ii) $H$ is connected.
(iii) $\forall \bar{H}$ if $H$ is a subgraph of $\bar{H}$ and $\bar{H}$ is a subgraph of $G$ and $\bar{H}$ is connected then, $H = \bar{H}$

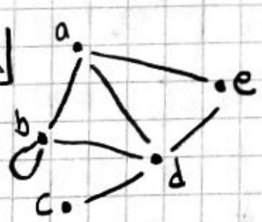
Ex Connected components of  are  and 

Notation: $K(G)$ is the number of connected components of $G$.

Ex $K(\triangle) = 1$ $\quad K(\triangle\ \backslash) = 2$ $\quad K(\square\ \cdot\ \cdot) = 3$

Notation: Let $(V, E)$ be a graph and $v \in V$. Then,

$$\deg(v) = \sum_{e \in E} r_e \quad \text{where} \quad r_e = \begin{cases} 0 & \text{if } v \notin e \\ 1 & \text{if } v \in e \text{ and } |e| = 2 \\ 2 & \text{if } v \in e \text{ and } |e| = 1 \end{cases}$$

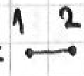
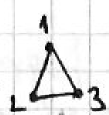
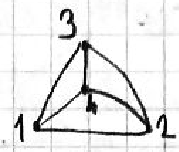
Ex 

$\deg(a) = 3$ $\quad \deg(d) = 4$
$\deg(b) = 4$ $\quad \deg(e) = 2$
$\deg(c) = 1$

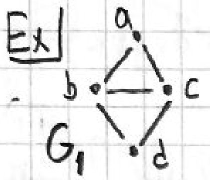
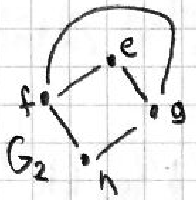
Notation: $K(V) =$ (complete graph on $V$.)

$K(V) = (V, E)$ where $E = \{e \subseteq V \mid |e| = 2\}$

Notation: $K_n = K(\{1, 2, 3, \dots, n\})$

Ex] $K_1 =$  $K_2 =$  $K_3 =$  $K_4 =$ 

Definition: A bijection $f$ from $V_1$ to $V_2$ is called a graph isomorphism from $(V_1, E_1)$ to $(V_2, E_2)$ if $\forall v \in V_1$ $\forall w \in V_1$ $\{v, w\} \in E_1 \iff \{f(v), f(w)\} \in E_2$.

Ex]  

$\{(a,e), (b,f), (c,g), (d,h)\}$ is a graph isomorphism from $G_1$ to $G_2$

Definition: If there exist an isomorphism from $G_1$ to $G_2$ then we say $G_1$ is isomorphic to $G_2$

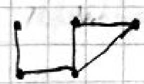
Theorem: If $G_1$ is isomorphic to $G_2$ then;

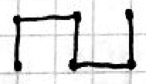
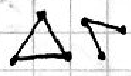
(i) (number of verticles $G_1$) = (number of verticles in $G_2$)

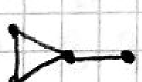
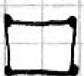
(ii) (number of edges in $G_1$) = (number of edges in $G_2$)

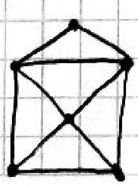
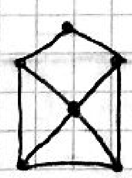
(iii) $K(G_1) = K(G_2)$

(iv) $\forall v$ vertex in $G_1$, $\deg(v) = \deg(f(v))$ where $f$ is an isomorphism $G_1$ to $G_2$.

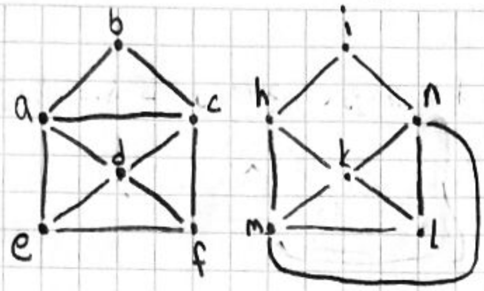
Ex] $G_1 =$  $G_2 =$  $G_1$ is not isomorphic to $G_2$ by i.

$G_1 =$  $G_2 =$  $G_1$ is not isomorphic to $G_2$, $K(G_1) = 1$, $K(G_2) = 2$ ) ii

$G_1 =$  $G_2 =$  $G_1$ is not isomorphic to $G_2$ by iv. because there's a $\deg(v) = 3$ in $G_1$ but not in $G_2$.

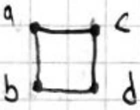
$G_1 =$   $= G_2$ i, ii, iii, iv are satisfied but $G_1$ is still not isomorphic to $G_2$ by following:

$G_1$ $G_2$




**Ex** Proof of $G_1$ is not isomorphic to $G_2$:
Suppose they are isomorphic. Then, $f(a) = i$ must be true because $\deg(a) = 2$ and b is the only vertex with degree 2. $\{a, b\}$ is an edge of $G_1$ so $\{i, f(b)\}$ must be an edge in $G_2$. Hence $f(b) = h$ or $f(b) = n$ but $f(b) \neq h$ because $\deg(b) = 4 \neq 3 = \deg(h)$. So $f(b) = n$. Now $\{a, c\}$ is also an edge in $G_1$ so $f(c) = h$ which is a contradiction, $\deg(c) = 4$ n/w $\deg(h) = 3$.

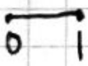
Definition: A graph $(V, E)$ is called bipartite if $V = V_1 \cup V_2$ with $V_1 \cap V_2 = \emptyset$ and $\forall e \in E \ \exists v_1 \in V_1 \ \exists v_2 \in V_2 \ e = \{v_1, v_2\}$

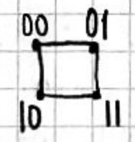
**Ex** 

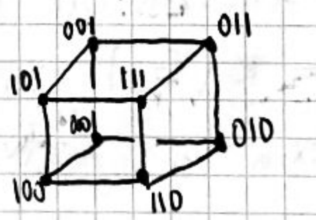
$V_1 = \{a, d\}$, $V_2 = \{b, c\}$

Notation: $Q_n$ = (hypercube) = $(V, E)$

$V$ = binary sequences of length $n$ $\quad E = \{\{v_1, v_2\} \subseteq V \mid v_1$ and $v_2$ differ in exactly one position$\}$

**Ex** $Q_1 =$ 

$Q_2 =$ 

$Q_3 =$ 

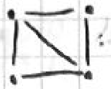

(*) $Q_n$ is bipartite; $V_1$ = (binary sequences of length $n$ with even num of 1's)
$V_2$ = (binary sequences of length $n$ with odd num of 1's)

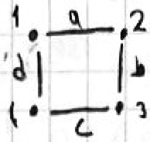
**Ex** Consider vertices as CPUs and edges as connections between CPU's

| graph | speed | cost |
|---|---|---|
| $K_N$ | very fast | very expensive |
|  | very slow | very cheap |
| $Q_N$ | OK | OK |

Subject : Date :....../....../......

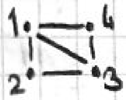
Euler Circuit: means a circuit which traverses every edge in the graph

Ex  } This has no euler circuit



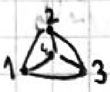

1a2b3c4d1 is an euler circuit.

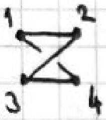
Theorem (Euler): Let $G(V, E)$ be a graph with no isolated verticles. Then $G$ has an Euler circuit if and only if $G$ is connected and every vertex of $G$ has even degree.

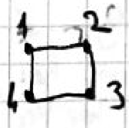
Ex 

This has no euler circuit since $\deg(1) = 3$ not even.

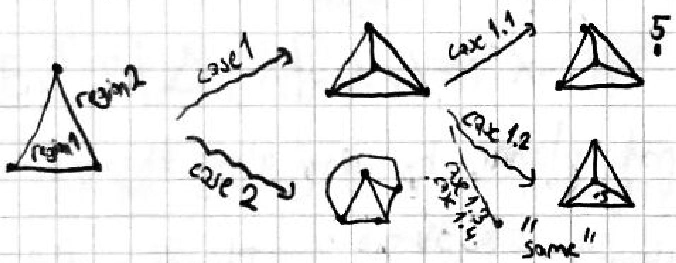
Definition: A graph $G$ is called planar if $G$ can be drawn in the plane with its edges intersecting only at verticles of $G$.

Ex $K_4$ is planar as follows; 


Ex 

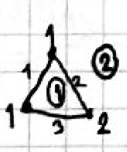
is planar because we can draw it as follows: 


Ex $K_5$ is not planar. First prof as follows:

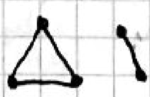



} Every case, there should be an intersection to draw edges to the 5. vertex.

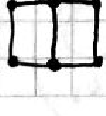
Theorem (Euler): Let $G(V, E)$ be a connected planar graph with $|V| = v$ and $|E| = e$. Assume $r$ is the number of regions determined by a planar graph of $G$. Then, $v - e + r = 2$ (Proof by induction)

Ex 

$3-3+2=2$

 $5-4+2=3 \neq 2$

because the graph is not connected.

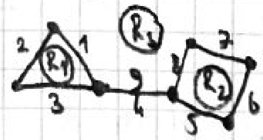
 $6-7+3=2$

Subject :

Date ....../....../......

Notation: Let R be a region in a planar drawing of a graph, then degree of R is; deg(R) = (number of edges around R)

Ex




$\deg(R_1)=3 \quad \deg(R_2)=4 \quad \deg(R_3)=9^*$ → some edges count twice.

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

(i) $\sum_{v\in V} \deg(v) = 2\cdot|E|$ (ii) $\sum_{R \text{ regions}} \deg(R) = 2\cdot|E|$

Proof: $v1 \xrightarrow{\text{edge}} v2$ Proof: r1 / r2

Theorem: Let $G=(V,E)$ be a loop-free connected planar graph with $|V|=v$, $|E|=e>2$ and $r$ = (number of regions). Then,

(i) $3r \leq 2e$ (ii) $e \leq 3v-6$

Proof: $\begin{matrix}\text{loop-free} \\ e>2\end{matrix} \Rightarrow \text{for all } R,\ \deg(R)\geq 3$

$\Downarrow$

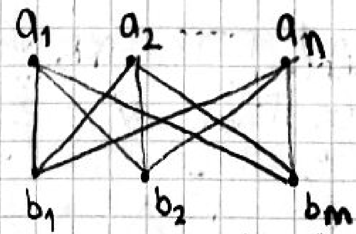
$3r \leq \sum_{R \text{ region}} \deg(R) = 2e$

Proof: $\left.\begin{matrix} v-e+r=2 \\ 3r\leq 2e \end{matrix}\right\} e\leq 3v-6$

Ex Another proof for $K_5$ is not planar, by using above theorem;

$\left.\begin{matrix} v=5 \\ e=\binom{5}{2}=10 \end{matrix}\right\}$ Suppose $K_5$ is planar, $\begin{matrix} e\leq 3v-6 \\ 10\leq 15-6 \end{matrix}$ → This is a contradiction.

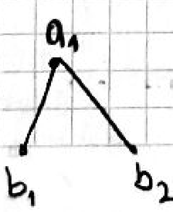
Notation: $K_{n,m}$ =



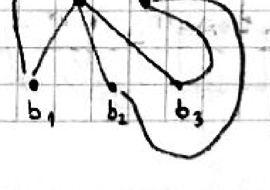

} all possible connections a—b

Ex $K_{1,1}$ =

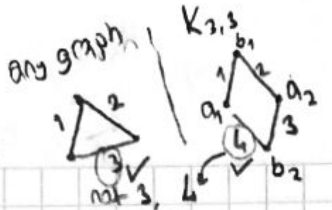

Ex $K_{1,2}$ =




Ex $K_{2,3}$ =




These graphs $K_{1,1}$, $K_{1,2}$ and $K_{2,3}$ are planar.




Theorem: $K_{3,3}$ is not planar. Proof: $v = 6$, $e = 3 \cdot 3 = 9$ } suppose $r$ is planar. $r = 2 - v + e = 5$

but $20 = \underbrace{4r}_{\text{because } K_{3,3} \text{ is bipartite}} \leqslant \sum_{R \text{ region}} \deg(R) = 2e = 18$ $\quad 20 \nleqslant 18$ is a contradiction.

Definition: If $G = (V, E)$ is a graph, a proper coloring of $G$ occurs when we color the verticles of $G$ so that if $\{v_1, v_2\}$ is an edge in $G$ then $v_1$ and $v_2$ are colored with different colors.

Notation: $\chi(G)$ = (minimum number of colors needed to properly color $G$) (chromatic number)

Ex $\chi(\text{—}) = 2$ $\quad \chi(\Delta) = 3$

Ex $\chi(K_n) = n$ $\quad \chi(K_{n,m}) = 2$ → Color $a_1, a_2 \dots a_n$ as one, color $b_1, b_2 \dots b_m$ as another one.

Notation: $P(G, \lambda)$ = (number of ways we can properly color $G$ using at most $\lambda$ colors)

Ex $P(\text{—}, 1) = 0$ $\quad P(\text{—}, 2) = 2$ $\quad P(\text{—}, \lambda) = \lambda \cdot (\lambda - 1)$

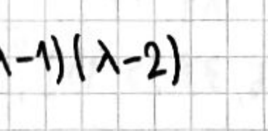
Ex $P(\Delta, \lambda) = \lambda(\lambda-1)(\lambda-2)$ $\quad$ Ex $P(\text{•—•—•}, \lambda) = \lambda \cdot (\lambda-1) \cdot (\lambda-1)$

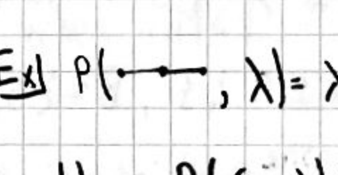
Theorem: Let $G$ be a loop-free graph, then $P(G, \lambda)$ is a polynomial, in the form; $C_n \lambda^n + C_{n-1} \lambda^{n-1} + \dots C_1 \lambda + C_0$ where $n$ = (number of verticles)

We say $P(G, \lambda)$ is the chromatic polynomial for $G$. $\quad C_n = 1$

Applications of Graph Coloring

Scheduling Problems:

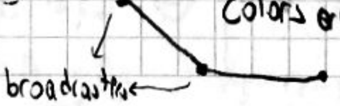



2, 4 red machine

1, 3, 5 blue machine

Broadcasting Networks:




colors are frequences

Subject :                                                     Date : ...../...../.....

Ex) Which of the following can be a chromatic polynomial?

a) $p(\lambda) = \lambda^3 + 5\lambda^2 - 7\lambda + 1$  c) $r(\lambda) = \lambda^4 + \lambda + 3\lambda^2$

b) $q(\lambda) = 7\lambda^5 + 2\lambda^4 - 9\lambda^2$  d) $k(\lambda) = \lambda^3 - 2\lambda^2 + \lambda$

a) $p(\lambda)$ is not a chr. poly; because $p(0)=1$ and it's impossible to color with 0 color.

b) $q(\lambda)$ is not a chr poly. because leading coefficient $C_n = 7 \neq 1$.

c) $r(\lambda)$ is not a chr poly. because $(r(1)=5) \Rightarrow$ (no edge) but $r(\lambda) \neq \lambda^n$ for any n.

d) $k(\lambda)$ is a chr. poly as follows; $k(\lambda) = P( \quad , \lambda)$

<u>Theorem</u>: Let $G=(V,E)$ be a connected graph and $e \in E$

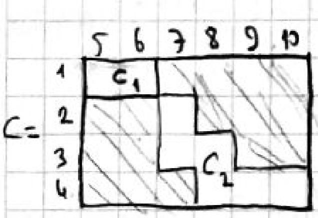
$P(G_e, \lambda) = P(G, \lambda) + P(G_e', d)$  $G_e = G - e$

$G_e' = G$ where e is identified to one vertex.

Ex) $P(\underset{G_e}{\quad}, \lambda) = P(\underset{G}{\quad}, \lambda) + P(\underset{G_e'}{\quad}, \lambda)$

<Review> (8-9-10 for final)

Ex) $A = \{1,2,3,4\}$, $B = \{5,6,7,8,9,10\}$, How many 1-1 functions satisfy ⓐ none ⓑ exactly one of the following conditions (i) $f(1) \in \{5,6\}$ (ii) $f(2)=7$ (iii) $f(3) \in \{7,8\}$ (iv) $f(4) \in \{8,9,10\}$




$r(C,x) = \underbrace{(1+2x)}_{r(C_1,x)}\underbrace{(1+6x+9x^2+2x^3)}_{r(C_2,x)} = 1 + 8x + 21x^2 + 20x^3 + 4x^4$

$C_1$ = condition (i)

$C_2$ = (ii)  $C_3$ = (iii)  $C_4$ = (iv)

Define $S$ = (set of all 1-1 functions from A to B)

$S_0 = |S| = P(6,4)$

$S_1 = 8 \cdot P(5,3)$

$S_2 = 21 \cdot P(4,2)$

$S_3 = 20 \cdot P(3,1)$

$S_4 = 4 \cdot P(2,0)$

ⓐ $E_0 = S_0 - S_1 + S_2 - S_3 + S_4 = 76$

ⓑ $E_1 = S_1 - 2S_2 + 3S_3 - 4S_4 = 140$

Ex] 13 cards are randomly chosen from a standard deck of cards. ($13 \times 4$)
What is the probability of these 13 cards include ⓐ At least one from each suit
ⓑ exactly 1 void (non-existing suit)
ⓒ exactly 2 voids.

$S = $ (set of all 13 combinations of 52 cards.)

$A =$ event ⓐ   $B =$ event ⓑ   $C =$ event ⓒ

$C_1 =$ (No spades)   $C_2 =$ (No hearths)   $C_3 =$ (No diamonds)   $C_4 =$ (No clubs)

$Pr(A) = \frac{|A|}{|S|} = \frac{E_0}{S_0}$   $Pr(B) = \frac{|B|}{|S|} = \frac{E_1}{S_0}$   $Pr(C) = \frac{|C|}{|S|} = \frac{E_2}{S_0}$

$S_0 = |S| = C(52, 3)$

$S_1 = N(C_1) + N(C_2) + N(C_3) + N(C_4) = C(4,1) \cdot N(C_1) = C(4,1) \cdot C(39, 13)$

$S_2 = C(4,2)\, C(26, 13)$

$S_3 = C(4,3)\, C(13, 13) = C(4,3)$

$E_1 = S_1 - 2S_2 + 3S_3 - 4S_4$

$E_0 = S_0 - S_1 + S_2 - S_3 + S_4$

$E_2 = S_2 - 3S_3$

Theorem: $(1-x)^{-n} = \sum_{i=0}^{\infty} \binom{n+i-1}{i} x^i$ when $|i| < 1$

Ex] Let $a_n =$ (number of 4 element subsets of $\{1, 2, 3, \dots, n\}$ that contain no consecutive integers.)

Find the generating function for $a_n$ and find $a_{15}$.

Notice, $a_n =$ (number of non-negative integer solutions to the equation
$x_1 + x_2 + x_3 + x_4 + x_5 = n - 1$ where $x_2 \geq 2$, $x_3 \geq 2$, $x_4 \geq 2$)

Given $\{n_1, n_2, n_3, n_4\}$, a four elements subset of $S$ without any consecutive integers we get a solution for the [equation] by considering $n_1 < n_2 < n_3 < n_4$ and $\underset{\geq 0}{x_1 = n_1 - 1}$, $\underset{\geq 2}{x_2 = n_2 - n_1}$ → no consecutive.
$\underset{\geq 2}{x_3 = n_3 - n_2}$, $\underset{\geq 2}{x_4 = n_4 - n_3}$, $\underset{\geq 0}{x_5 = n - n_4}$

Subject: Date: ...../...../.....

Define $b_n = \left( \begin{array}{l} \text{number of non-negative integer solutions to the} \\ x_1 + x_2 + x_3 + x_4 + x_5 = n \quad \text{where} \end{array} \begin{array}{l} x_2 \geq 2 \\ x_3 \geq 2 \\ x_4 \geq 2 \end{array} \right)$ So $b_n = a_{n+1}$

$$(\text{Gen. Fun. for } b_n) = (1+x+x^2+\dots)^2 (x^2+x^3+x^4\dots)^3$$

Last Theorem $= \left(\frac{1}{1-x}\right)^2 \cdot \left(x^2 \cdot \left(\frac{1}{1-x}\right)\right)^3 = x^6 \cdot (1-x)^{-5}$

$$= x^6 \cdot \sum_{i=0}^{\infty} \binom{5+i-1}{i} x^i = \sum_{i=0}^{\infty} \binom{i+4}{i} \cdot x^{i+6} \implies (\text{Gen. Fun. } a_n) = \sum_{i=0}^{\infty} \binom{i+4}{i} x^{i+6+1}$$

$$a_{15} = (\text{The coefficent of } x^{15}) \implies i=8; \dots + \binom{12}{8} x^{15} \dots \implies a_{15} = \binom{12}{8}$$

Ex) A ship carries 48 flags, 12 each of the colors red, white, blue and black. 12 of these flags are placed on a vertical pole in order to communicate a signal to other ships.

(a) How many of these signals use an even number of blue flags and an odd number of black flags?

(b) How many of them have at least 3 white flags or 0 white flags?

Since the order of flags is important, we should use exp. gen. functions.

$a_n$ = (number of such signals when we have $4n$ flags, $n$ for each color and put $n$ flags)

Solution (a)

$$(\text{exp. gen. for } a_n) = \underbrace{\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}\dots\right)^2}_{\text{red, white}} \cdot \underbrace{\left(1+\frac{x^2}{2!}+\frac{x^4}{4!}\right)}_{\text{blue}} \cdot \underbrace{\left(x+\frac{x^3}{3!}+\frac{x^5}{5!}\right)}_{\text{black}}$$

$$= (e^x)^2 \cdot \left(\frac{e^x+e^{-x}}{2}\right) \cdot \left(\frac{e^x-e^{-x}}{2}\right)$$

$$= \frac{1}{4}(e^{4x}-1) = \frac{-1}{4} + \frac{1}{4} \cdot \sum_{n=0}^{\infty} \frac{(4x)^n}{n!} \implies \text{coefficent of } x^{12} = \left(\frac{4^{11}}{12!}\right) \cdot x^{12}$$

exp. part

$$= \frac{-1}{4} + \sum_{n=0}^{\infty} \frac{4^{n-1} \cdot x^n}{n!}$$

(a) $= \boxed{a_{12} = 4^{11}}$

$$\underline{\text{solution (b)}} \quad (\text{exp. gen. for } a_n) = \underbrace{\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}\cdots\right)^3}_{\text{red, blue, black}} \cdot \left(\underbrace{1}_{0\text{ white}} + \underbrace{\frac{x^3}{3!}+\frac{x^4}{4!}+\cdots}_{\text{at least 3 white}}\right)$$

$$= e^{3x}\left(e^x - x - \frac{x^2}{2!}\right) = e^{4x} - x\cdot e^{3x} - \frac{x^2}{2}e^{3x}$$

$$= \sum_{n=0}^{\infty}\frac{4^n x^n}{n!} - \sum_{n=0}^{\infty}\frac{3^n\cdot x^{n+1}}{n!} - \sum_{n=0}^{\infty}\frac{3^n x^{n+2}}{2\,(n!)} = \cdots + \overbrace{\left(\frac{4^{12}}{12!} - \frac{3^{11}}{11!} - \frac{3^{10}}{2\cdot 10!}\right)}^{\text{coefficient } k}\cdot x^{12} + \cdots$$

So the answer for b is; $k = \frac{a_{12}}{12!} \Rightarrow a_{12} = 12!\cdot k$ ✓

$\underline{\text{Ex}}$ For the alphabet $\{0,1,2,3\}$ there are $4^{10}$ strings of length 10. How many of these strings contain an even number of 1's in them. ⟨Exercise⟩: Solve by using exponential gen. funcs.

Define $a_n =$ (number of strings of length $n$ containing even 1's)

$a_1 = 3 \qquad a_n = \begin{pmatrix}\text{number of such strings}\\ \text{ending with } 0,2,3\end{pmatrix} + \begin{pmatrix}\text{number of such strings}\\ \text{ending with } 1\end{pmatrix}$

$$a_n = 3\cdot a_{n-1} + \underbrace{\left(4^{n-1} - a_{n-1}\right)}_{n-1 \text{ part has odd 1's.}}$$

Solve; $a_1 = 3$, $a_n = 4^{n-1} + 2a_{n-1}$

$\underline{\text{Step 1)}}$ Solve the homogenous part. The char poly for $a_n - 2a_{n-1} = 0$ is $r-2$. So the general sol. for hom. part is $a_n^{(h)} = C\cdot 2^n$

$\underline{\text{Step 2)}}$ Find a particular solution. Try $a_n^{(p)} = A\cdot 4^{n-1}$

$$4^{n-1} = a_n^{(p)} - 2a_{n-1}^{(p)} = A\,4^{n-1} - 2\cdot A\cdot 4^{n-2} \Rightarrow 4 = 4A - 2A \Rightarrow a_n^{(p)} = 2\cdot 4^{n-1}$$

$\underline{\text{Step 3)}}$ Use initial values for $a_n = a_n^{(h)} + a_n^{(p)} = C\cdot 2^n + 2\cdot 4^{n-1}$

We have $3 = a_1 = C\cdot 2 + 2 = 2C + 2 \Rightarrow C = \frac{1}{2}$ $\}$ $a_n = 2^{n-1} + 2\cdot 4^{n-1}$

$a_{10} = 524800$ ✓