

# Theory of Computations, Final Exam for the course CS 5315, Spring 2017

Name: \_\_\_\_\_

You can use up to 5 handwritten pages of notes. Feel free to use extra sheets of paper if needed, but if you do, do not forget to put your name on each of these sheets.

## 1. Primitive recursive and mu-recursive functions:

4/2  
10

1a. Why do we need to study primitive-recursive and mu-recursive functions in the first place? What programming concepts do they correspond to?

1b. Translate, step-by-step, the following double loop into a mu-recursive expression:

8  
10

```
int s = 2;
while(s < a) {
    for(int i = 1; i <= b; i++)
        {s = s + i;}
}
```

You can use the multiplication function is this description. What is the result of this program when a = b = 3?

10/10

1c. Prove, from scratch, that the remainder function  $a \% b$  is primitive recursive. Provide a simpler proof that this function is mu-recursive.

10/10

1d. Is Kolmogorov complexity primitive recursive? mu-recursive? Explain your answers.

1 a) we need to study primitive recursive functions in the first place because they are the important building blocks on the way to a full formalization of computability. Also, important in proof theory.

⊙ mu-recursive  $\neq$   $\rightarrow$  computable in intuitive sense.  
 $\rightarrow$  only functions computed by Turing Machine

⊙ primitive recursive  $\rightarrow$  for-loops.

⊙ mu-recursive  $\rightarrow$  while loops.

```
> int s = 2;
while(s < a) {
    for(int i = 1; i <= b; i++)
        {s = s + i;}
}
```

$\rightarrow$  for-loop

```
int a = 2;
for(int i = 1; i <= b; i++) {
    for(int i = 1; i <= b; i++) {
        s = s + i;
    }
}
```

Inner loop:  $Q(a, b)$   
 $S'(a, 0) = S_0$   
 $S'(a, m+1) = S'(a, m) + (m+1)$   
 $\therefore f(n, 0) = n; g(n) \rightarrow g = \pi_1^1$   
 $f(n, m+1) = f(n, m) + (m+1)$   
 $= f(n, m) + (m+1)$   
 $\rightarrow h(n, m, f(n, m))$   
 $= \pi_3^3 + (\pi_2^3 + 1)$   
 $= \pi_3^3 + \sigma(\pi_2^3) = add(\pi_3^3, \sigma(\pi_2^3))$

```

Outer loop: int a = 2; for (int j = 1; j <= a; j++) { S = G(S, b); }
S(b, 0) = 2; S(b, m+1) = G(S(b, m), b).
f(n, 0) = 2 -> g(n, 1) = 1+1 = sigma(0) + sigma(0) = sigma(sigma(0))
f(n, m+1) = G(f(n, m), n) -> h(n, m, f(n, m)) = G(pi_2^3, pi_1^3)
    
```

$\therefore f \equiv PR(\sigma(\sigma(0)), G(\pi_2^3, \pi_1^3))$  where  $G \equiv PR(\pi_1^3, \text{add}(\pi_2^3, \sigma(\pi_2^3)))$ .  
 --- (I)

(#) Conversion to  $\mu$ -recursive:  
 We stop at smallest 'm' for which

$\mu m (!s < a)$   
 $\rightarrow \mu m (!f(m) < a)$ .

where  $f(m)$  is given by (I)

So what is the final expression?  
 $f(n, \mu m. !f(n, m) < a)$

where:

```

a = b = 3;
int s = 2;
while (2 < 3) {
  for (int i = 1; i <= 3; i++)
    { S = S + i; }
}
    
```

$i = 1;$   
 $S = 2 + 1 = 3$   
 $i = 2$   
 $S = 3 + 2 = 5$   
 $i = 3$   
 $S = 5 + 3 = 8$

$i = 4$  out of for loop  
 $S = 8$  now  
 $S > 3$ .  
 out of while loop.

$S = 8 \rightarrow$  Ans.

- 1 a) No. Kolmogorov complexity is not primitive recursive
- No. Kolmogorov complexity is not  $\mu$ -recursive.

Since, Kolmogorov complexity is not computable, It is neither primitive recursive nor it is  $\mu$ -recursive.

1 c) Proof:

Remainder;  $a \div b$  is P.R.

$a \div b \equiv \begin{cases} \text{rem}(a, 0) = 0; \\ \text{rem}(a, b+1) = \begin{cases} \text{rem}(a, b) + 1 & \text{when } \text{rem}(a, b) + 1 < a \\ 0 & \text{otherwise} \end{cases} \end{cases}$

i.e. if  $\text{rem}(a, b) + 1 < a$   
 then  $\text{rem}(a, b) + 1$   
 else 0.  $\rightarrow$  0 is P.R. by definition

- $\rightarrow$  Need to prove:
- i) If-then-else is P.R.
- ii) less than is P.R.
- iii) add is P.R.

To prove: (i) If-then-else is P.R.:

If  $Q(u)$   
 then  $g(u)$   
 else  $h(u)$

$\Rightarrow Q(u) \text{ AND } g(u) \text{ OR } (1-Q(u)) \text{ AND } h(u)$   
 AND is recursive which is P.R.  
 OR in P.R. proved below  
 sub is P.R. proved below

# OR is P.R.  $\rightarrow$   
 $a \vee b = 1 - (1-a) * (1-b)$   
 $= a + b - a * b$

# sub is P.R.  $\rightarrow$   
 $(a-b) = a - 1 - 1 \dots - 1$   
 $\rightarrow \text{sub}(a,0) = a; \text{sub}(a,m+1) = \text{prev}(\text{sub}(a,m))$

$\rightarrow$  add and mult is P.R. - proved below.  
 # AND is multiplication which is P.R. proved below.

# prev is P.R.  $\rightarrow$   
 $\text{prev}(u) = \begin{cases} u-1 & \text{if } u > 1 \\ 0 & \text{otherwise} \end{cases}$

$\text{prev}(0) = 0 \rightarrow f(0) = 0 \rightarrow g() \rightarrow g = 0$   
 $\text{prev}(m+1) = m \rightarrow f(m+1) = m \rightarrow h(m, f(m)) = m$   
 $\rightarrow h = \pi_1^2$   
 $\text{prev} = \text{PR}(0; \pi_1^2)$

# add is P.R.:  
 $\text{add}(a,0) = 0$   
 $\text{add}(a,i+1) = \text{add}(a,i) + 1$   
 $f(u,0) = g(u) = g = u_1 = \pi_1^1$   
 $f(u,m+1) = h(u,m, f(u,m))$   
 $= f(u,m) + 1$   
 $\rightarrow h = \pi_1^2 + 1 = \sigma(\pi_1^2)$   
 $\therefore \text{add} = \text{PR}(\pi_1^1, \sigma(\pi_1^2))$

(ii) # less than is P.R.  
 $a < b \Leftrightarrow a \leq b \wedge \neg (a=b)$  — (1)  
 Again,  $a = b \equiv a \leq b \wedge b \leq a$  — (2)  
 Also,  $a \neq b \equiv \neg (a=b)$  — (3)

# mult is P.R.:  
 $\text{mult}(a,0) = 0; \text{mult}(a,i+1) = \text{mult}(a,i) + a$   
 $f(u,0) = 0; \rightarrow g = 0$   
 $f(u,m+1) = f(u,m) + u_1 \rightarrow h(u,m, f(u,m)) = \pi_1^2 + \pi_1^1$   
 $\rightarrow h = \text{add}(\pi_1^2, \pi_1^1)$   
 $\therefore \text{mult} = \text{PR}(0, \text{add}(\pi_1^2, \pi_1^1))$

Again,  $a \leq b \rightarrow \text{eval } 0(a-b)$  — (1)  
 $\rightarrow a-b = \begin{cases} a-b & \text{if } a > b \\ 0 & \text{otherwise} \end{cases}$   
 $\text{eval } 0(u) = \begin{cases} \text{true if } u = 0 \\ \text{false if otherwise} \end{cases}$   
 $\text{eval } 0(0) = 1; f(0) = 1; g() = 1$   
 $\text{eval } 0(m+1) = 0$   
 $h(m, f(m)) = 0$   
 $\text{eval } 0(u) = \text{P.R.}(0,0,0)$   
 (1) is P.R. from which 3, 2, 1 is P.R. follows.

$\therefore$  (i) is P.R. proved.

So, (i) - If-then-else is P.R. }  $\therefore a \% b \rightarrow$  remainder is P.R.

#  $a \% b$  is  $\mu$ -recursive as it can be expressed in  $\mu$ -recursive terms.

$a \% b \equiv \begin{cases} a & ; a < a \\ 0 & \text{otherwise} \end{cases}$   
 $\Rightarrow a \% b \equiv \mu x; a < x < a$

$a/b = m + \frac{r}{b}$   
 $\Rightarrow a = bm + r; 0 \leq r < b$   
 $(b * m) \leq a < (b * m) + b$   
 $\Rightarrow (b * m) \leq a < (b * m) + b$   
 $\rightarrow$  smallest  $m$ ; for which  $\mu m (a < b * (m+1))$   
 $\therefore a \% b \equiv \mu m (a < b * (m+1)) \rightarrow$  hence,  $\mu$ -recursive.

35/40 = 8.8/10.0

2. Computable sets, computable functions, and Turing machines:

2a. Why do we need to study decidable and recursively enumerable (r.e.) sets?

2b. Is the intersection of two r.e. sets always r.e.? If yes, prove it, if no, provide a counterexample.

2c. Prove that it is not possible, given a program that always halts, to check whether this program always computes  $2 * n + 1$ .

2d. Design a Turing machine that computes  $2 * n + 1$  in binary code. Trace this machine on the example of  $n = 10_2$ .

10/10  
10/10  
10/10  
10/10

2a) Computations ...  $\rightarrow$  math-wise complicated.  
 but Maths has simple, basic concepts of "sets" to represent these computations in clear, concise terms, easy to understand.  
 We need to study decidable set to have an algo. to check whether  $n \in A$  at a moment of time.  
 We need to study recursively enumerable set to prove that there is an algo. which eventually prints all of its elements.

2b) Yes intersection of 2 r.e. sets is always r.e.  
 $A, B \rightarrow r.e.$   
 $A, B \rightarrow$  let each run for  $k$  hrs.  
 1hr.  $A \rightarrow$  print  $n$ .  
 1hr.  $B \rightarrow$  print  $y$ .  
 Assuming it is okay to repeat, the computer can print the elements from  $A$  for  $k$  hrs,  $B$  for  $k$  hrs search for elements in common, print them as  $A \cap B$ . Repeat until finished. Hence, all elements gets eventually printed.  
 $A \cap B \rightarrow r.e.$

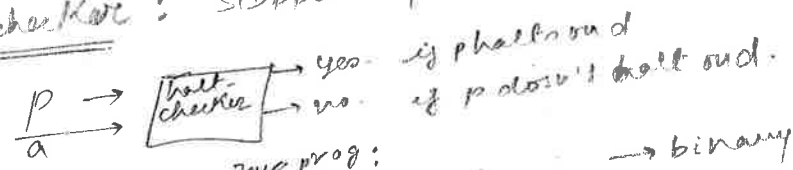
2c) By contradiction, let a program is possible which always checks whether this program computes  $2 * n + 1$ .  
 $2 * n + 1$  - checker (p) =  $\begin{cases} 1 & \text{if } \forall n (p(n) = 2 * n + 1) \\ 0 & \text{if } \exists n (p(n) \neq 2 * n + 1) \end{cases}$   
 whatever if p doesn't always halt.  
 We build a zero-checker on this:  
 $q \rightarrow \forall n (q(n) = 0)$   
 $\downarrow$   
 $p(n) = q(n) + 2 * n + 1$   
 $\xrightarrow{\text{checker}} \forall n (p(n) = 2 * n + 1)$   
 $\text{Zero-checker}(n) = [2 * n + 1 \text{ checker}] [q(n) + 2 * n + 1]$   
 $= \begin{cases} \text{Yes} & \text{if } \forall n (q(n) = 0) \Leftrightarrow p(n) = q(n) + 2 * n + 1 = 2 * n + 1 \\ \text{no} & \text{if } \exists n (q(n) \neq 0) \Leftrightarrow p(n) = q(n) + 2 * n + 1 \neq 2 * n + 1 \end{cases}$   
 $=$  whatever if  $q$  sometimes doesn't halt.

zero-checker  $(f, p, d) = \text{true}$  if  $\forall t (f(p, d)(t) = 0)$   
 false if  $\exists t (f(p, d)(t) > 0)$

halt-checker  $(f, p, d) = ! \text{zero-checker } f(p, d) \rightarrow \text{true if } p \text{ halts and}$   
 $\rightarrow \text{false if } p \text{ doesn't halt and.}$

Best halt-checker is not possible, zero-checker not possible  $\rightarrow$   
 hence, our assumption wrong and said algo. not possible.

⊕ halt-checker: suppose possible.

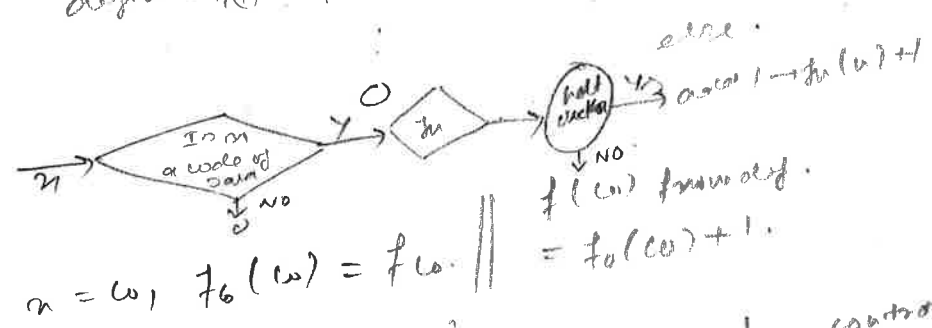


code of Java 'c'  $\xrightarrow{\text{Java prog:}}$  ASCII  $\rightarrow$

lemma:  $\exists$  an algo that given returns one file, etc.

natural no. c, checks whether 'c' consists of 0's and 1's  $\rightarrow$  append '1'

define  $f(n)$ :  $f_u(u) + 1$   $n$  is a code of Java



$n = c_0, f_0(c_0) = f_{c_0} \parallel = f_0(c_0) + 1$

$\therefore f_{c_0}(c_0) = f_0(c_0) + 1 \Rightarrow 0 = 1$ . contradiction. halt-checker not possible.  $\therefore f$  is computable.

$2 * n + 1$

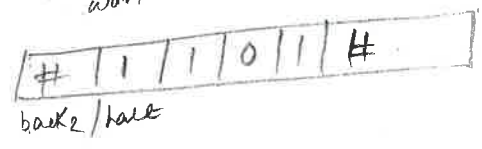
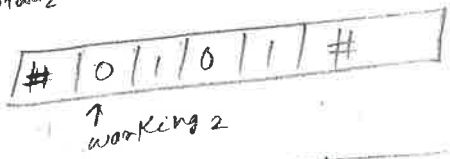
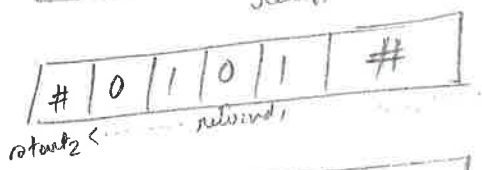
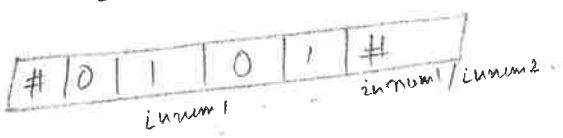
$f(n) \rightarrow$  Computation Turing Machine:  
 $g(n) = 2 * n = (n + n)$

- (start<sub>1</sub>, #)  $\rightarrow$  innum<sub>1</sub>, R
- innum<sub>1</sub>, 1  $\rightarrow$  R; innum<sub>1</sub>, 0  $\rightarrow$  R
- innum<sub>1</sub>, #  $\rightarrow$  1, R; innum<sub>2</sub>
- innum<sub>2</sub>, 1  $\rightarrow$  R; innum<sub>2</sub>, 0  $\rightarrow$  R
- innum<sub>2</sub>, #  $\rightarrow$  L, ready<sub>1</sub>
- ready<sub>1</sub>, 1  $\rightarrow$  L; #  $\rightarrow$  rewind<sub>1</sub>
- rewind<sub>1</sub>, 1  $\rightarrow$  L; rewind<sub>1</sub>, 0  $\rightarrow$  L
- rewind<sub>1</sub>, #  $\rightarrow$  start<sub>2</sub>

$f(n) = n + 1$

- start<sub>2</sub>, #  $\rightarrow$  working<sub>2</sub>, R
- working<sub>2</sub>, 0  $\rightarrow$  1, back<sub>2</sub>, R
- working<sub>2</sub>, 1  $\rightarrow$  0, R
- working<sub>2</sub>, #  $\rightarrow$  1, back<sub>2</sub>, L
- back<sub>2</sub>, 1  $\rightarrow$  L; back<sub>2</sub>, 0  $\rightarrow$  L
- back<sub>2</sub>, #  $\rightarrow$  halt

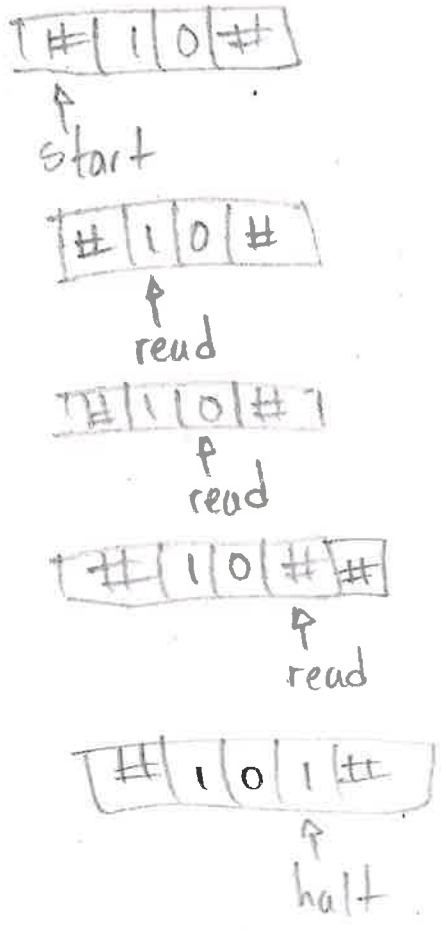
$f(n) \rightarrow 102 = n$



# Turing Machine $2 \times n + 1$

Given  $n = 10_2$   
 Want  $10_2$

start, #  $\rightarrow$  R, read  
 read, 1  $\rightarrow$  R  
 read, 0  $\rightarrow$  R  
 read, #  $\rightarrow$  L, halt



2a. So we can understand other concepts such as when will the intersections of two sets print a number. If they are not r.e. that (printing number) can't be done.

$$\frac{67}{70} = \frac{9.6}{10}$$

3. NP-hardness:

3a-d. Reduce the satisfiability problem for the formula  $(a \vee \sim c) \& (\sim b \vee c) \& (a \vee b \vee c)$  to:

- a) 3-coloring,  $10/10$
- b) clique,  $10/10$
- c) subset sum problem, and  $10/10$
- d) interval computations.  $10/10$

$10/10$   
 $7/10$

3e. In proofs of what results are these reductions used? What do we gain by proving that a problem is NP-hard?

3f. Use the definitions of the classes P, NP, NP-hard, and NP-complete to describe, for each of these four classes, whether this class contains 3-coloring, 2-SAT, sorting, and subset sum. Explain your answers.

3g. Give two examples of why the current definition of a feasible algorithm is not perfect:

- an example when an algorithm is feasible according to this definition but not practically feasible, and
- an example when an algorithm is not feasible according to this definition but is practically feasible.

$10/10$

3.9) Eg. practically not feasible by def<sup>n</sup> feasible:

$$T_A(n) = 10^{200 \log(n)}$$

② practically feasible, by definition not feasible:

$$T_A(n) = \exp(10^{-80} \log(n))$$

3.2) These reductions are used in the proof of NP-hardness. Gain by proving a problem is NP-hard:

i) If a problem is NP-hard, unless  $P = NP$ , no feasible algo. is possible for solving all particular cases of this problem. Thus, we should not waste time looking for a solution.

ii) By def<sup>n</sup>, a problem is NP-hard  $\rightarrow$  every prob. of class NP can be reduced to it. Thus, we have a good heuristic feasible algo. for solving some particular cases of this problem.



3.1

3-colouring: cannot be solved in poly. time, unless P=NP  
 : 3-SAT is reduced to it  $\rightarrow$  NP-hard  
 : each node has 3 colours to choose from  $\rightarrow$  NP.  
 $\therefore$  NP, NP-hard  $\rightarrow$  NP-complete

2-SAT: solve in polynomial time  $\rightarrow$  P.

SAT reduced to it  $\rightarrow$  NP-hard

$P \neq NP$ ; not NP

$\therefore$  not NP-complete.

2-SAT is polynomial time  
 it is in NP

Sorting:  $\rightarrow$  polynomial time sol<sup>n</sup>  $\rightarrow$  P.

$\rightarrow$  represented as a graph of correct order  $\rightarrow$  NP

$P \neq NP$ ; not NP-hard, not NP-complete

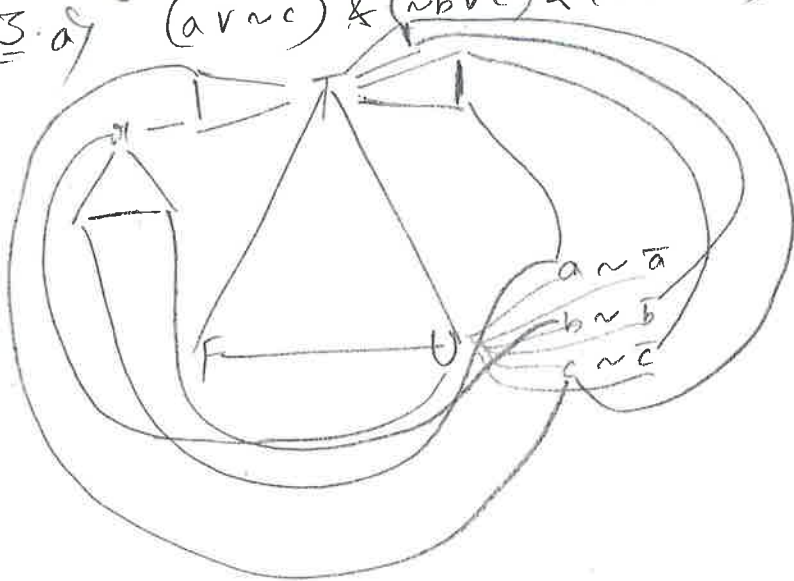
Subset Sum: polynomial time solution  $\rightarrow$  P.  
 3-CNF reduced to it  $\rightarrow$  NP-hard.

not a single solution  $\rightarrow$  not NP.

not NP-complete.

NP it is in NP  
 so it is NP-complete

3.1 a)  $(a \vee b \vee c) \wedge (\neg b \vee c) \wedge (a \vee b \vee c)$



3-colouring

or solving one particular case of this problem then reduction automatically generates algorithm for solving particular cases of all NP-hard problems.

3f)

	3-coloring	clique	2-SAT	interval scheduling
P	no, unless $P=NP$	no, unless $P=NP$	yes	no, unless $P=NP$
NP	yes	yes	yes	no one knows
NP-hard	yes	yes	no, unless $P=NP$	yes
NP-complete	yes	yes	<del>no one knows</del> no unless $P=NP$	no one knows.

3g) Some algorithms are feasible, they are, usually polynomial time, so, an algorithm is feasible if it takes polynomial time. There exist a polynomial  $p(n)$  such that for input  $x$

$$t_A(x) \leq p(\text{len}(x))$$

\* Example of when algorithm is feasible according to the above definition but not practically feasible.

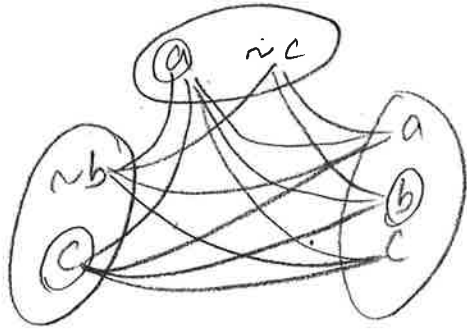
$t_A(x) = 10^{40} \cdot \text{len}(x)$  This is feasible in the view point of the definition but not practically.

\*  $t_A(x) = \exp(10^{50} \cdot \text{len}(x))$ : Feasible in practical

3b) clique:

$(a \vee \neg b) \wedge (\neg b \vee c) \wedge (a \vee b \vee c)$

→ connect all nodes other than variable & negation



solution:

$a = T$

$b = T$

$c = T$

clique: connected.

3c)

Subset problem.

	a	b	c	c1	c2	c3
a	1	0	0	1	0	1
$\bar{a}$	1	0	0	0	0	0
b	0	1	0	0	1	0
$\bar{b}$	0	1	0	0	1	1
c	0	0	1	1	0	0
$\bar{c}$	0	0	1	1	0	0
$\bar{c}$				1	0	0
$\bar{c}$				0	1	0
$\bar{c}$				0	1	0
$\bar{c}$				0	0	0
$\bar{c}$				0	0	0
				3	3	3
	1	1	1			

$a = T$   
 $b = T$   
 $c = T$

Interval computations:

$$(a \vee c) \& (b \vee c) \& (a \vee b \vee c)$$

$$\equiv [1 - (1-a)(1-c)] [1 - (1-b)(1-c)] [1 - (1-a)(1-b)(1-c)]$$

$$= [1 - (1-a)c] [1 - (b)(1-c)] [1 - (1-a)(1-b)(1-c)]$$

$$\therefore F \equiv 1.$$

$$\Rightarrow 1 - (1-a)c = 1$$

$$\Rightarrow 1 - a = 0 \text{ or } c = 0$$

$$a = 1 \text{ or } c = 0$$

$$1 - (b)(1-c) = 1$$

$$\Rightarrow b = 0 \text{ or } c = 1$$

$$1 - (1-a)(1-b)(1-c) = 1$$

$$\Rightarrow a = 1 \text{ or } b = 1 \text{ or } c = 1$$

Hence,  $\underbrace{a = 1, b = 1, c = 1}_{\text{chosen solution}}$  satisfies the problem.

$$\frac{36}{40} = \frac{9.0}{10}$$

4. Parallelization:

- 10/10 4a. matrices (2-D arrays) are added component-wise. Does the problem of adding  $n$  matrices belong to the class NC? Explain your answer.
- 8/10 4b. If we parallelize and take into account communication time, what is the fastest that we can compute the sum of two matrices? Explain your answer.
- 8/10 4c. Where are similar arguments used in the proof that satisfiability is NP-hard?
- 10/10 4d. What are the physical assumptions behind these arguments? Give two examples of how non-standard physics -- in which these assumptions are not satisfied -- can be used to solve NP-hard problems in polynomial time.

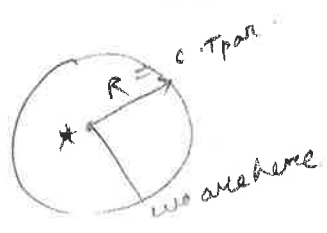
4a)

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}$$

$c_{ij} = a_{ij} + b_{ij} + a_{12}b_{ij} + \dots + a_{in}b_{ij}$  // elements in matrix =  $n^2$ .  
 Adding 'n' matrices:  $O(\log(n))$  time. For each matrix,  $n$  processors.  $n \cdot n^2 \times n \rightarrow n^3$  no. of processors.

Yes, it belongs to the class NC. Since it is solvable in polynomial time and NC is the class of problems solved in polylog time by polynomial processors.

4b) Parallelize, processing time  $\rightarrow T(\text{par}(n))$  with communication.  
 Sequential processing time  $\rightarrow T(\text{seq}(n))$ .



Assuming communication delay is almost as fast as speed of light, the diagram.  
 Volume of sphere,  $V = \frac{4}{3} \pi R^3 = \frac{4}{3} \pi c^3 T_{\text{par}}(n)^3$ .  
 $\Rightarrow$  Sphere can fit 'n' processors.  
 $N_{\text{processors}} \leq \frac{V}{\Delta V} = \frac{4/3 \pi c^3 T_{\text{par}}(n)^3}{\Delta V}$   
 $\Rightarrow T(\text{seq}(n)) \leq N_{\text{processors}} \leq c_1 T_{\text{par}}^3, T_{\text{par}} \leq c_2 T^4_{\text{par}}(n)$   
 $\Rightarrow T^4_{\text{par}}(n) \geq c \cdot T_{\text{seq}}(n)$   
 $\Rightarrow T_{\text{par}}(n) \geq c [T_{\text{seq}}(n)]^{1/4}$

This is the fastest assuming Euclidean physics.  
 In this case what is it?  $T_{\text{seq}}(n) = n$   
 so  $\geq c \cdot n^{1/4}$

4c) Similar arguments used in the proof that satisfiability is NP-hard. Argument of using speed of light as the maximum transfer of speed is used in the proof of NP-hardness of SAT to show that at any given case depends on a finite no. of neighbours & they only depend on finite polynomial no. of states which can be computed in binary way.

All  
 it  
 is  
 a  
 proof  
 that  
 over  
 the  
 # of  
 process  
 in  
 polynomial

4d) Physical assumptions based on Euclidean arguments: we state that  $v \leq c$  &  $v = \frac{4}{3} \pi r^3$ ,  $\epsilon_0$  because info. can't travel faster, we can only use polynomial no. of processors which are not enough to solve exponential time problems.

Non-Euclidean physics can help solve NP-hard problems in polynomial time:

- 1) Let a computer sum & send signal back in time when done.
- 2) Use of Lobachevsky space: allows us to fit an exponential no. of processors in the sphere which would allow to compute exponential time algo in polynomial time.
- 3) Exploit causality by having random no. generators try to find a path  $\epsilon_0$  trying to provoke very low probability events (much lower than finding the correct area) by travelling back in time & trying to disrupt causality.

$$\frac{30}{20} = \left( \frac{15}{10} \right)$$

5. How to solve NP-hard problems?

5a. Suppose that a probabilistic algorithm for checking the program correctness misses the program's mistake 20% of the time. How many times do we need to repeat this algorithm to achieve reliability of 99%? And why do we need probabilistic algorithms in the first place?

5b. Apply both greedy algorithms to solve the following particular case of the knapsack problem: we have 4 objects with weights 20, 30, 40, and 50, values 1000, 1200, 1200, and 1500, and the overall weight of 50. Why do we need to use these algorithms, if they do not produce optimal results?

5c. (For extra credit) Give an example of how quantum computing can speed up computations.

5a) prob. of missing a mistake  $\rightarrow 20\% \rightarrow \frac{20}{100} = 0.2$   $p_0 = 0.2$ .  
 Reliability  $\rightarrow 99\%$  means probability of missing ~~not~~ ~~error~~ ~~error~~  $(100-99)\%$   
 $= 1\%$ .  $\therefore \epsilon = \frac{1}{100} = 0.01$ .  
 $K \rightarrow$  no. of times algo is to be repeated.

$$\text{Now, } p_0^K \leq \epsilon.$$

$$\Rightarrow K \ln p_0 \leq \ln \epsilon.$$

$$\Rightarrow K \geq \frac{\ln \epsilon}{\ln p_0} \quad [ : p_0 \leq 1 ]$$

$$\Rightarrow K = \frac{\lceil \ln \epsilon \rceil}{\ln p_0}$$

$$= \frac{\lceil \ln 0.01 \rceil}{\ln 0.2}$$

$$= 2.86.$$

$$= 3.$$

$\therefore$  No. of times algo. is to be repeated  $\rightarrow 3$ .

Need of Probabilistic Algo.:

- i) Many practical problems are NP-hard.
- ii) This means that unless  $P = NP$ , no feasible algo is possible that solves all instances of this problem.
- iii) In some cases, it is possible to solve some instances.

5. c) Quantum computing can speed up computations through superpositions.

Digital computers: everything 0 & 1

Quantum u: every 2 states 0 and 1 can also have a superposition on.

$c_0|0\rangle + c_1|1\rangle$ ;  $c_0, c_1$  are complex numbers.

$|c_0|^2 + |c_1|^2 = 1$ ;  $\rightarrow$  measure this qubit (quantum bit); states  
 Prob. of obtaining 0  $\rightarrow$  prob. of obtaining 1.  
 Faster computations

$\rightarrow$   $O(n^{1/2})$  time complexity.

5. b) 4 objects:

Max W = 50

	$x_1$	$x_2$	$x_3$	$x_4$
$w_i$	20	30	40	50
$v_i$	1000	1200	1200	1500

1st greedy algo: pick highest value first.

$x_4 = 1$ ;  $v_i = 1500$ ;  $w_2 = 50$  maximum weight is reached.  
 $\therefore x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1$  in the selection.  
 Gain is 1500/-

2nd greedy algo: pick highest ratio first

	$x_1$	$x_2$	$x_3$	$x_4$
$w_i$	20	30	40	50
$v_i$	1000	1200	1200	1500
$v_i/w_i$	50	40	30	30

$x_1 = 1$ ;  $v_1 = 1000, w_1 = 20, W = 20$   
 then  $x_2 = 1$ ;  $v_1 = 1200, w_2 = 30, W = 20 + 30 = 50$ . Maximum weight is reached.  
 $\therefore$  Sol<sup>n</sup> is  $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0$   
 $\therefore$  Gain is  $1000 + 1200 = 2200/-$ .

$\rightarrow$  Need to use these algos, because program in 1 problem immediately enhances program in all others.



30/30 = 10/10

6. Beyond NP: polynomial hierarchy:

70/10 6a. Which class of the polynomial hierarchy contains optimization problems? The problem of winning in 3 moves? Explain your answers.

10/10 6b. Which class of polynomial hierarchy contains  $\Sigma_4^{\text{PI}}$ ?

10/10 6c. Give an example of an oracle A for which  $P^A = NP^A$ . Explain your answer.

6/10 a) Optimization problems:  
 $(x, y) \in P \iff \exists p \forall q C(p, q)$   
 $\rightarrow$  belongs to class  $\Sigma_2 P$

$\left[ \begin{array}{l} NP: \exists y C(m, y) \\ co-NP: \forall y C(m, y) \end{array} \right.$

Winning in 3-moves:  
 $\exists p_1 \forall p_2 \exists p_3 \forall p_4 \exists p_5$   
 $\rightarrow$  belongs to class  $\Sigma_5 P$

b)  $\Sigma_4^{\text{PI}} \equiv \exists x_1 \forall x_2 \exists x_3 \forall x_4 \exists x_5 P(x_1, \dots, x_5)$   
 $\equiv \exists x_1 \forall x_2 \exists x_3 \forall x_4 \exists x_5 Q(x_1, \dots, x_5)$   
 $\equiv \exists x_1 \forall x_2 \exists x_3 \forall x_4 \exists x_5 R(x_1, \dots, x_5)$   
 $\equiv \Sigma_4 P$

6c)  $P^A = NP^A$  for oracle  $A = PSPACE$

$P^A \rightarrow$  relative to an oracle class.  
 $NP^A \rightarrow NP \in P^{\text{SAT}} \rightarrow$  we can reduce every NP - problem to satisfiability.

$NP: \exists y C(m, y): \Sigma_1 P$   
 $co-NP: \forall y C(m, y): \Pi_1 P$   
 $P(SPACE) \equiv \exists x_1 \forall x_2 \dots P$  ... polynomial no. of quantifiers  
 $P^{PSPACE} \equiv \exists x_1 \forall x_2 \dots \exists [PSPACE] \dots$   
 $NP^{PSPACE} \equiv \exists x_1 \forall x_2 \dots \exists [PSPACE] \dots$   
 $\approx PSPACE$   
 $\therefore PSPACE = NP^{PSPACE}$