87

VANESSA LAMA

-1

April 5, 2022

Computer Science 581 – Exam 2

1. Dynamic Programming

   a. State the Principle of Optimality.

   → For a given stage 'i', no matter what given the decision d_i on f_i that take, the following decisions $d_{i+1}, d_{i+2}, \ldots d_n$, (where, n is the total no. of decisions) must be optimal with respect to f_i and d_i.

   what is? states -1

   b. How long does it take to solve an n stage decision process with d decisions per stage?

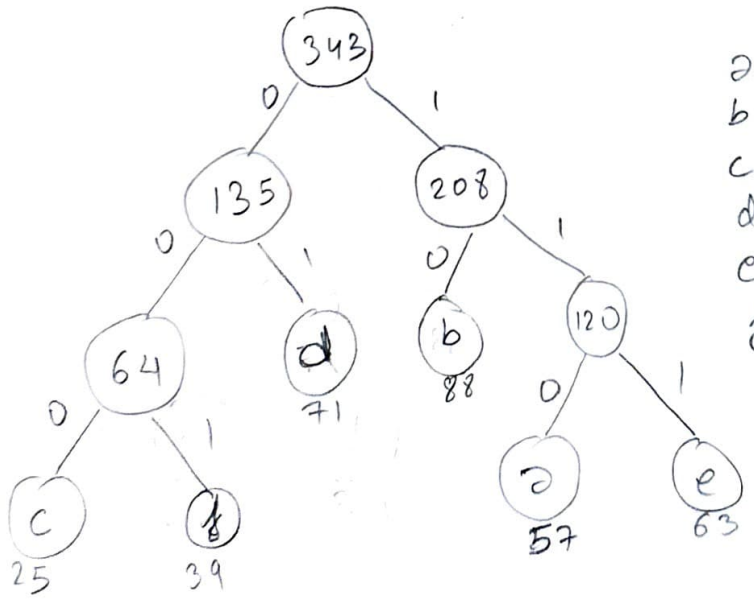
   $O(d^n)$

   -0

2. Greedy Algorithms

   Design a Huffman code for a text file in which "a" occurs 57 times, "b" occurs 88 times, "c" occurs 25 times, "d" occurs 71 times, "e" occurs 63 times, and "f" occurs 39 times.

   a: 57, b: 88, c: 25, d: 71, e: 63, f: 39



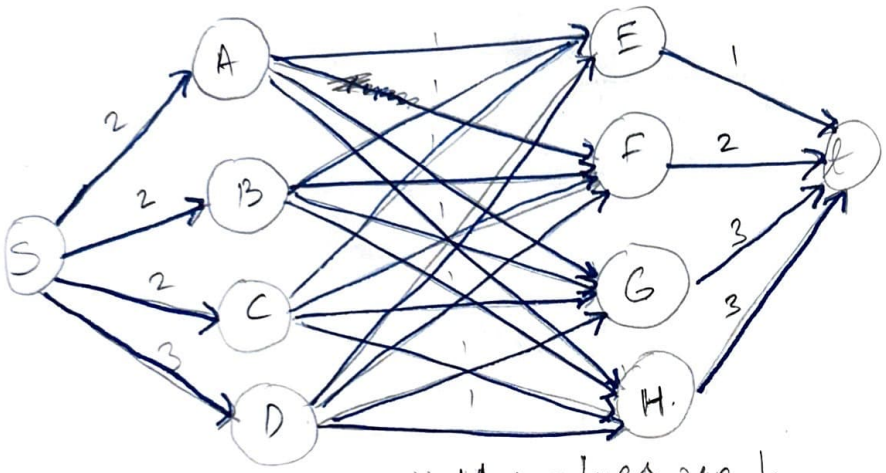
a = 110
b = 10
c = 000
d = 01
e = 111
f = 001

-0

VANESSA LAMA

-12

3. Network Flow
Use network flow (show your work) to find a 4 × 4 Boolean matrix whose row sums are (2,2,2,3) and whose column sums are (1,2,3,3), if any such a matrix exists.



all flow values are 1.

I've set it up, I think, but can't figure out the next steps.

The next step is to find a maximum flow.

which is the whole point of the exercise.

-12

VANESSA LAMA

-0

4. Linear Programming
Use the simplex algorithm (show your work) to solve the following.
maximize: $3x_1 + x_2$
subject to: $4x_1 + x_2 \leq 7$
$x_1 + x_2 \leq 5$
$x_1, x_2 \geq 0$

in slack form:

	x_1	x_2	S_1	S_2	Z	
→ R_1	(4)	1	1	0	0	7
R_2	1	1	0	1	0	5
R_3	−3	−1	0	0	1	0

$\frac{7}{4} = 1.75$, $\frac{5}{1} = 5$

↑ most-negative

pick pivot of 4 from x_1

operations:

$R_1 = \frac{1}{4}R_1$

$R_2 = R_2 - \frac{1}{4}R_1$

$R_3 = R_3 + \frac{3}{4}R_1$

	x_1	x_2	S_1	S_2	Z	
R_1	1	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$\frac{7}{4}$
→ R_2	0	(3/4)	$-\frac{1}{4}$	1	0	$\frac{13}{4}$
R_3	0	$-\frac{1}{4}$	$\frac{3}{4}$	0	1	$\frac{21}{4}$

$= 7$, $= 4.33$

↑ most-negative

pick pivot of $\frac{3}{4}$ from x_2,

operations:

$R_2 = \frac{4}{3}R_2$

$R_1 = R_1 - \frac{1}{3}R_2$

$R_3 = \frac{1}{3}R_2 + R_3$

x_1	x_2	S_1	S_2	Z	
1	0	$\frac{1}{3}$	$-\frac{1}{3}$	0	$\frac{2}{3}$
0	1	$-\frac{1}{3}$	$\frac{4}{3}$	0	$\frac{13}{3}$
0	0	1	0	1	$\frac{19}{3}$

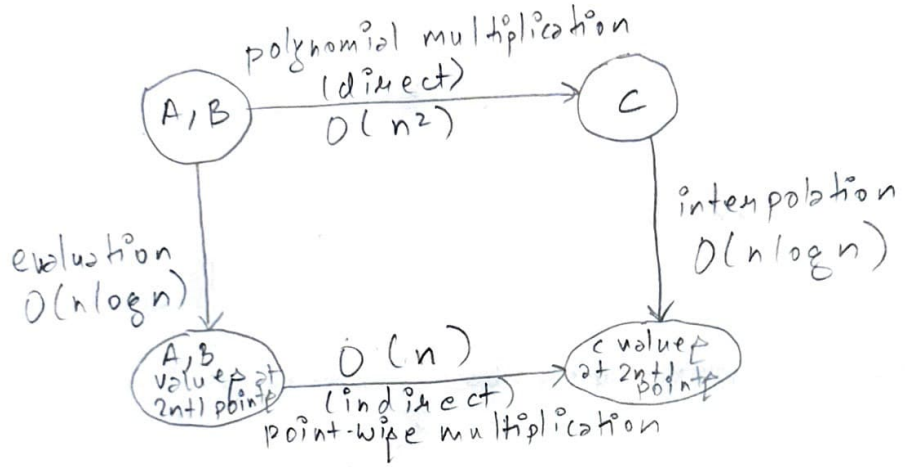
all positive, so optimal!

∴ max $Z = \frac{19}{3}$ at $(x_1, x_2) = (\frac{2}{3}, \frac{13}{3})$ ✓

VANESSA LAMA

-0

5. The Fast Fourier Transform
   Draw the figure for polynomial multiplication via the FFT as discussed in class. Include time complexities for the direct method versus pointwise evaluation, multiplication and interpolation.



-0

6. Cryptology

   a. State (do not prove) Fermat's Little Theorem.

If n is prime, then, $\forall\, b \not\equiv 0 \pmod n$,
$b^{n-1} \equiv 1 \pmod n$

-0

   b. Encode message 3 in an RSA crypto system with $n = 91$ and $E = 5$.

$C = 3^E \bmod n = 3^5 \bmod 91$
$= 243 \bmod 91$
$\therefore C = 61$

-0

Rough:
9×27
=270-27
=243
243-91-91
= 9+9+43
= 61

Important Notes:

- This exam is *closed* book.
- Use a separate page for each question, with your name at the *top right* of each page.
- Your final answers must be justified. They must also be readable. Illegible answers are wrong.
- Use your time wisely. When in doubt, it's generally better to leave an occasional question blank than it is to try to give poorly thought-out responses to every question.