-0

92

March 26, 2019

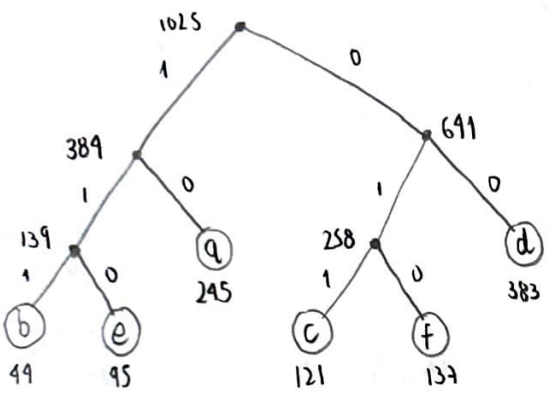
Name Paula Olaya

Computer Science 581 – Exam 2

1. Greedy Algorithms. Design a Huffman code for a text file in which "a" occurs 245 times, "b" occurs 44 times, "c" occurs 121 times, "d" occurs 383 times, "e" occurs 95 times, and "f" occurs 137 times.

-0

a: 245 b: ~~44~~ c: ~~121~~ d: 383 e: ~~95~~ f: ~~137~~

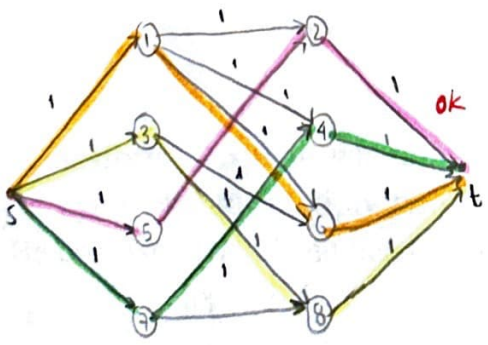


a = 10
b = 111
c = 011
d = 00
e = 110
f = 010

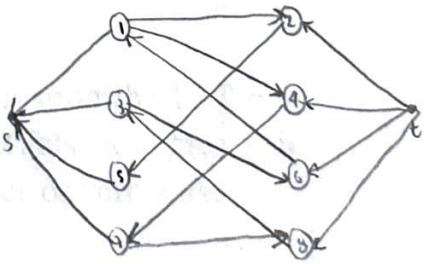
2. Network Flow. Define G by the following adjacency matrix. Note that G is bipartite, with its two partite sets comprised of odd- and even-numered vertices. Use a maximum flow algorithm to find a perfect bipartite matching for G.

-0

	1	2	3	4	5	6	7	8
1	0	1	0	1	0	0	1	0
2	1	0	0	0	1	0	0	0
3	0	0	0	0	0	1	0	1
4	1	0	0	0	0	0	1	0
5	0	1	0	0	0	0	0	0
6	1	0	1	0	0	0	0	0
7	0	0	0	1	0	0	0	0
8	0	0	0	0	0	0	1	0



Residual



There is no more augmenting path so we have found the maximum flow and the pairs.

Solution:

- 1 - 6
- 3 - 8 ok
- 5 - 2
- 7 - 4

-0

 Name Paula Olaya

3. Linear Programming. Solve the following using the simplex method. -0

maximize: $x_1 + 2x_2 + 2x_3$

subject to: $x_1 - 2x_2 + x_3 \leq 6$

$x_2 \leq 4$

$x_3 \leq 5$

$2x_1 + x_3 \leq 9$

$x_1, x_2, x_3 \geq 0$

$z = x_1 + 2x_2 + 2x_3$

$x_4 = 6 - x_1 + 2x_2 - x_3$

$x_5 = 4 - x_2$ $(0,0,0,6,4,5,9)$

$x_6 = 5 - x_3$

$x_7 = 9 - 2x_1 - x_3$

1) We pivot x_3 with x_6

- $x_3 = 5 - x_6$

$z = x_1 + 2x_2 + 10 - x_6$

$x_4 = 1 - x_1 + 2x_2 + x_6$ $(0,0,5,1,4,0,4)$

$x_5 = 4 - x_2$

$x_3 = 5 - x_6$

$x_7 = 4 - 2x_1 + x_6$

2) We pivot x_2 with x_5

- $x_2 = 4 - x_5$

$z = 18 + x_1 - 2x_5 - x_6$

$x_4 = 9 - x_1 - 2x_5 + x_6$ $(0,4,5,9,0,0,4)$

$x_2 = 4 - x_5$

$x_3 = 5 - x_6$

$x_7 = 4 - 2x_1 + x_6$

3) We put x_1 with x_7

$x_1 = 2 - \frac{x_3}{2} - \frac{x_6}{2}$

$z = 20 - \frac{x_3}{2} - \frac{3x_6}{2} - 2x_5$

$x_4 = 7 + \frac{x_7}{2} + \frac{3x_6}{2} - 2x_5$

$x_2 = 4 - x_5$

$x_3 = 5 - x_6$

$x_1 = 2 - \frac{x_7}{2} - \frac{x_6}{2}$

$(2,4,5,7,0,0,0)$

✓

$z = 20$

$x_1 = 2$

$x_2 = 4$

$x_3 = 5$

} Solution

4. The Fast Fourier Transform. Explain where in its derivation the FFT employs mathematical symmetry to multiply two polynomials of degree n in $O(n \log n)$ time. Be concise. There's no need for pictures or verbosity. -0

Sorry for the verbosity, that's how I learnt it!

Due Halving lemma (Symmetry of the nth roots of unity)

If $n > 0$ and even, the square of the n complex nth roots are the $n/2$ complex $(n/2)$th roots of unity $(w_n^k)^2 = w_{n/2}^k$ → This leads to having $n/2$ of $(n/2)$th root of unity.

Also, $(-w^j) = w^{j+n/2}$ ✓

$(-w^j)^2 = w^{2j}$ $(w^{j+n/2})^2 = w^{2j} w^n$

$= w^{2j}$

- Applying divide and conquer with the even and odd indexed

$A^{[0]}(x) = A_0 + A_2 x + A_4 x^2 + \dots + A_{n-2} x^{\frac{n}{2}-1}$

$A^{[1]}(x) = A_1 + A_3 x + A_5 x^2 + \dots + A_{n-1} x^{\frac{n}{2}-1}$ } $A(x) = A^{[0]}(x^2) + x A^{[1]}(x^2)$

Then instead of evaluating $w_n^0, w_n^1, \dots, w_n^{n-1}$ we evaluate $(w_n^0)^2, (w_n^1)^2, \dots, (w_n^{n-1})^2$ on $A(x)$ which has the same form of the problem but half size

(on the other page) →

-8

$C = M^E \bmod (n)$

Page 3

Name Paula Olaya

5. Cryptology. Consider an RSA crypto scheme with $n = 35$ and $E = 5$. $p=5$ $q=7$ $\phi(n) = 24$ -4

   a. List a valid value for D. $D=5$ $25 = 1 \pmod{24}$

   b. Encode messages 3, 4 and 5. $3^5 \bmod 35 = 33$ ($3 \to 33$) $4^5 \bmod 35 = 9$ ($4 \to 9$) $5^5 \bmod 35 = 10$ ($5 \to 10$)

   c. List two messages that are always unencryptable. → 0 and 1

   d. List another message unencryptable under this scheme.

   If C is equal to p, q or D. $6^5 \bmod 35 = 6$, $7^5 \bmod 35 = 7$ } Real Answer

6. Complexity Theory.

   a. What is the Satisfiability Problem? All expunential (NO) problems can be adapted to a boolean satisfability problem.

   $X = \{x_1, x_2, \dots, x_n\}$

   variables? clauses? CNF?

   2^n operations NO

   Ex: $X = \{x_1, x_2, x_3\}$

   $Out = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \wedge x_2 \wedge x_3)$

x_1	x_2	x_3
0	0	0
0	0	1
0	1	1
0	1	0
1	0	0
1	1	0
1	0	1
1	1	1

   b. What does it mean to say that a problem is $\mathcal{NP}$-hard?

   R is "NP-hard" if $L \propto R$ $\forall L \in NP$

   R is NP-hard if it is as hard as the hardest NP-Problems.

   c. What does it mean to say that a problem is $\mathcal{NP}$-complete?

   R is "NP-complete" iff
   1) $R \in NP$
   2) R is NP-hard

   -4

   d. State the Cook-Levin Theorem.

   States that the Boolean Satisfiability Problem is NP-Complete.

   Any NP problem can be reduced by SAT.

Notes: This exam is *closed* book. Place your name at the top right of each page. Show your work where needed; your final answers must be justified and legible. It's generally better to leave an occasional question blank than to give poor responses to every question.