

CS 5/7350 – Final Exam
May 12, 2021

Name: Answers

- This exam is **closed book** and **closed notes**.
- You MAY have a calculator and 1 page of notes that is 8.5 x 11 inches
- No cell phones, or other electronics except as required for zoom and only used for zoom or other proctoring.
- Pencil and/or pen are permitted.
- It is **3 hours** in duration plus time for scanning and uploading, etc.
- You should have 14 problems. Pay attention to the point value of each problem and dedicate time as appropriate.

On my honor, I have neither given nor received unauthorized aid on this exam.

SIGNED: _____

DATE: _____

Name: _____

ID: _____

1. [5 pts] The following numbers are in the number system $\beta = \frac{1}{\sqrt[3]{2}}$ (one over the cube root of 2) and $D = \{0,1\}$. Add the numbers and give the answer in the same number system:

$$\begin{array}{r} 1100010010.110011 \\ + 1010011000.110001 \\ \hline 0111001000.010100011 \end{array}$$

NOT on Test 3 Spring '23

2. [8 pts] You want to prove that some problem H is NP-Complete. You know that problem G is NP-Hard. Mark **True** for each of the following statements of things you need to prove. Mark **False** if you do not need to prove the statement.

(i) You need to prove that H can be verified in polynomial time.

(ii) You need to prove that G can be verified in polynomial time. *True*

(iii) You need to prove that a solver for G can also solve H. *False*

(iv) You need to prove that a solver for H can also solve G. *False*

(v) You need to prove that H is NP-Hard *True* ←

True (do this by iv.)

3. [7 pts] Compute the **integer** value for Z given that $((161 * Z) + 3879) \bmod 11609 = 11169$. Show your table for the Extended Euclidian Algorithm.

$$\frac{1}{161} \bmod 11609 = 10239$$

$$Z = 8049$$

4. [6 pts] Show the addition table required for addition that adds two numbers from the number system $\beta = 7$ and $D = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ giving a number in the same number system. Ensure the addition can be performed in parallel without having to “ripple” a carry. (You do not need to fill in the grey areas)

	-4	-3	-2	-1	0	1	2	3	4
-4	$\overline{11}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$0\overline{3}$	$0\overline{2}$	$0\overline{1}$	00
-3									01
-2									02
-1									03
0									$1\overline{3}$
1									$1\overline{2}$
2									$1\overline{1}$
3									10
4									11

NOT on Test 3 Spr 23

5. [8 pts] You have 3 dice. Each one is different.

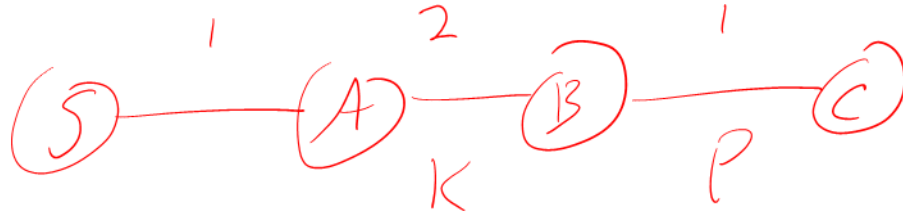
- Die #1 has sides { 0, 1, 2 } with a
 - 20% chance of rolling a 0, a
 - 30% chance of rolling a 1 and a
 - 50% chance of rolling a 2.
- Die #2 has sides { 2, 2, 0 } with a
 - 35% chance of rolling the first 2 and a
 - 35% chance of rolling the other 2 and a
 - 30% chance of rolling a 0
- Die #3 has sides {0, 1} with a
 - 25% chance of rolling a 0 and a
 - 75% chance of rolling a 1

(i) Fill in the table for the dynamic programming algorithm to solve the problem.

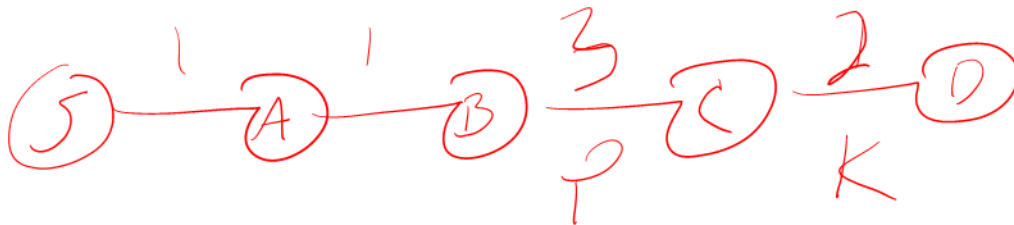
- (ii) What is the probability of rolling a 0? 1.5% 6.75%
- (iii) What is the probability of rolling a 1? 14% 27%
- (iv) What is the probability of rolling a 2? 24.5%
- (v) What is the probability of rolling a 3? 26.25%
- (vi) What is the probability of rolling a 4? 26.25%
- (vii) What is the probability of rolling a 5? 26.25%

	D1	+D2	+D3	
0	.2	.06	.015	
1	.3	.09	.0675	
2	.5	.29	.14	
3	0	.21	.27	
4	0	.35	.245	
5	0	0	.2625	

6. [8 pts] Create a graph with a starting vertex of "S" (when required) where:
- The weight of the third edge chosen with Prim's Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen by Kruskal's algorithm with a "K".



- The weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Prim's Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen by Kruskal's algorithm with a "K".



7. [8 pts] Answer the following questions.:

- A program requires 3s to brute force attack an encryption key of 64 bits. If the running time is $\Theta(2^n)$ about how many years would it take to brute force attack an encryption key of 256 bits? (note there are about 32 million seconds in a year)

$$3 \cdot 2^{192}$$

- A program requires 3s to brute force attack an encryption key of 64 bits. If you have access to a quantum computer where the running time is $\Theta(n^2)$ about how many seconds would it take to brute force attack an encryption key of 256 bits?

$$3 \left(\frac{256}{16} \right)^2 = 3 \cdot 4^2 = 48$$

8. [7 pts] Use the DGT algorithm discussed in class to determine how to represent the value 282 using the number system $\beta=5$, $D = \{-2, -1, 0, 7\}$. Show your work.

$$\begin{array}{r}
 282 \div 5 = 56 \text{ use } 7 \\
 \underline{-7} \\
 275 \\
 \underline{-5} \\
 55 \\
 \underline{-0} \\
 55 \\
 \underline{-5} \\
 11 \div 5 = 2 \text{ use } 7
 \end{array}$$

Digits $-2 \times 5 = 3$
 $-1 \times 5 = 4$
 $0 \times 5 = 0$
 $7 \times 5 = 2$

NO Digit $\times 5 = 1$,
 so 282 can not be
 represented in this
 number system

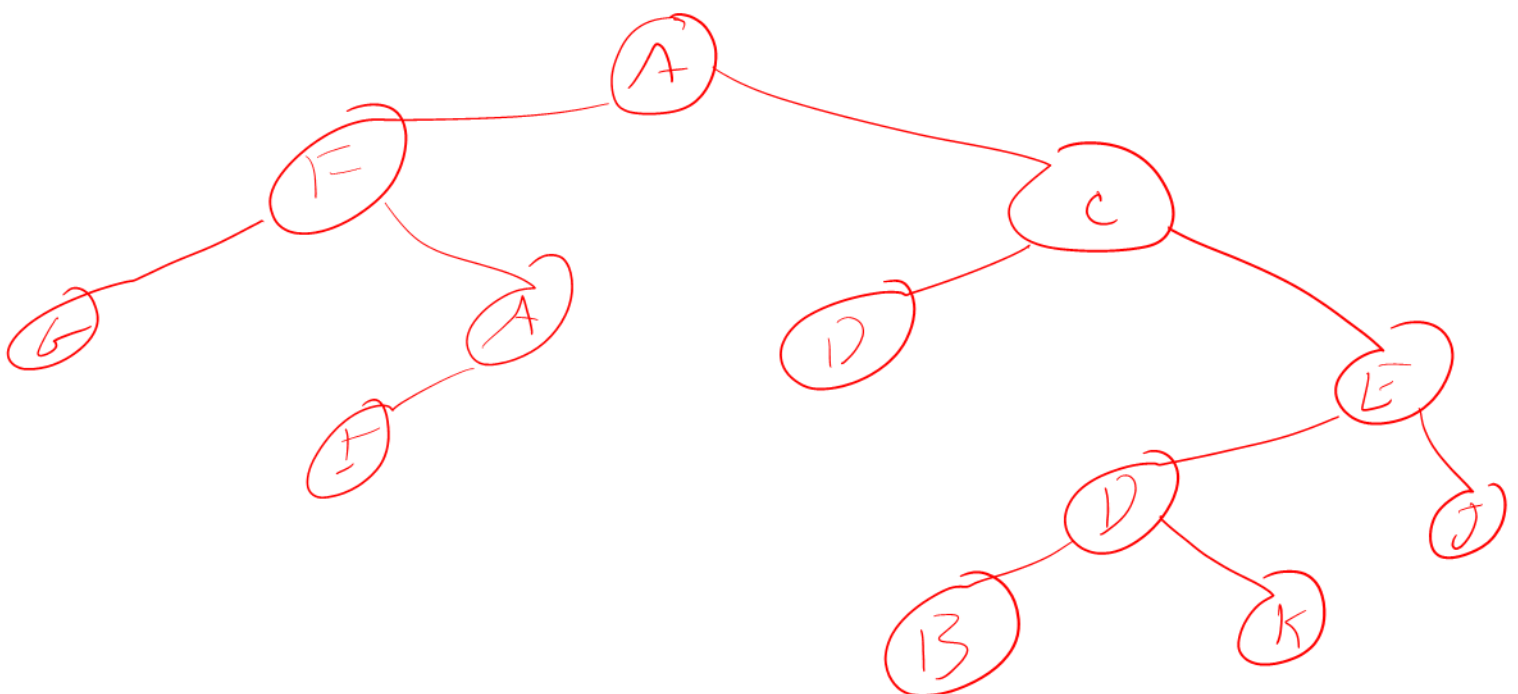
07

least
 significant
 Digit

9. [7 pts] A tree has the following pre-order and in-order traversals. Draw the tree and give the post-order traversal.

In-Order: GFIHABDKCEJ

Pre-Order: AFGHICDBKEJ



10. [8 pts] You have two strings, A and B.
- String A has a length of 8.
 - String B has an unknown length.
 - The Lowenstein Edit Distance between the two strings is 5.
- (i) What is the minimum length of String B?

3

- (ii) What is the maximum length of String B?

13

- (iii) What is the minimum length of the Longest Common Subsequence of String A and String B

3

- (iv) What is the maximum length of the Longest Common Subsequence of String A and String B?

8

11. [8 pts] You run different programs for various values of “n” and sometimes “m” and create 4 tables of the runtimes. Give the asymptotic bounds that each table supports?

a.	n	time (ms)	b.	n	time (ms)	c.	m	n	time (ms)	d.	m	n	time (ms)
	5	11		100	12156		100	100	104		100	100	52
	6	66		200	12156		100	200	156		100	200	104
	7	462		300	12156		100	300	208		100	400	208
	8	3696		400	12156		100	400	260		100	800	416
	9	33264		500	12156		200	100	156		200	100	104
	10	332640		600	12156		200	200	208		200	200	208
	11	3659040		700	12156		200	300	260		200	400	416
	12	43908480		800	12156		200	400	832		200	800	832

$\theta(n!)$

$\theta(1)$

$\theta(m+n)$

$\theta(m \cdot n)$

12. [6 pts] Two people need to establish a secret key for encrypting communications. They agree to use a Diffie-Hellman key exchange with a modulus of 13 and decide on 2 as the base. Person A chooses a random value of 4 and person B chooses a random value of 9.

a. What is the value Person A sends to Person B

3

b. What is the value Person B sends to Person A

5

c. What is the shared secret key between Person A and Person B

1

13. [6 pts] Using n_0 equal to 10, determine the maximum value for c_1 and the minimum value for c_2 , required to show that $f(n) = 7n^2 + 3n + 5$ is $\Theta(n^2)$.

$$0 < c_1 n^2 \leq 7n^2 + 3n + 5 \leq c_2 n^2$$

$$0 < c_1 \leq 7 + \frac{3}{n} + \frac{5}{n^2} \leq c_2$$

$$c_1 \leq 5$$

@ $n \rightarrow \infty$

$$7.35 \leq c_2$$

@ $n = 10$

14. [8 pts] Determine a Huffman encoding for each symbol in a message that contains:

20 A's, 7 B's, 7 C's, 5 D's, 2 E's and 2 F's.

How many bits are in the entire message if each symbol is encoded with 3 bits?

$$43 \times 3 = 129$$

How many bits are in the entire Huffman coded message?

93

How much entropy does each “B” have in the message?

$$\log_2 \frac{4^3}{7} = 2.68$$

