BRONX COMMUNITY COLLEGE

of The City University of New York

DEPARTMENT OF MATHEMATICS and COMPUTER SCIENCE

FINAL EXAMINATION SAMPLE. Solutions.

PART I. Do all problems. Each problem is worth 4 points.

1. Show that $p \to (q \vee \neg(p \to q))$ is a tautology.

   (using truth tables or logical equivalences - the choice is yours)

   Solution: done in class

2. Translate these statements into English, where $R(x)$ is"x is a rabbit" and $H(x)$ is"x hops" and the domain consists of all animals.

   a) $\forall x(R(x) \to H(x))$

   b) $\exists x(R(x) \wedge H(x))$

   Solution: done in class

3. Re-write the statement

$$\neg\left(\forall x \exists y(P(x,y) \vee Q(y)) \wedge \exists x(\neg R(x))\right)$$

   so that negations appear only within predicates

   Solution: done in class

4. For the sets $A = \{1,2,3,4,d\}$, $B = \{1,a,3,d\}$, $C = \{1,2,3,a,b,c,d\}$ and the universal set is $U = \{1,2,3,4,5,a,b,c,d,e\}$. Find

   (a) $A \bigcap B \bigcap C$

   (b) $A \bigcup (B - C)$

   (c) $\overline{A} \bigcap (B \bigcap \overline{C})$

   Solution: done in class

5. Determine whether the given function is bijective, and **explain why**.

   $f : \{a,b,c,d,e,f\} \to \{1,2,3,4,5,6\}$,

   with $f(a) = 6$, $f(b) = 1$, $f(c) = 4$, $f(d) = 2$, $f(e) = 6$, $f(f) = 3$

   Solution: done in class

6. Determine which statements are false or true. **Justify your answer**.

   1. $\{0\} \in \{0, \{0\}\}$ **2.** $\{0\} \subset \{0, \{0, 1\}\}$ **3.** $\{\emptyset\} \subseteq \{\emptyset\}$
   4. $\{\{a\}, b\} \subseteq \{a, \{a, b\}, \{a\}\}$ **5.** $b \in \{a, \{a, b\}, \{b\}, \{\{a\}, b\}\}$

   Solution: done in class

7. Take a look at the following algorithm:

   Input: x: real number

   Output: won't say

```
procedure n(x)
If (x = 9), Return("A")
If (x < 9 and x > 1), Return("B")
If (x <= 1), Return("not C")
Else Return("D")
```

   a) what is returned by the algorithm on the input 7, i.e. x = 7?

   b) what is returned by the algorithm on the input 17, i.e. x = 17?

   Solution: done in class

8. Binary search was used to find 8 in the following list: 2, 6, 7, 8, 11.

   How many comparison operations (of 8 with an element of the list) is performed until 8 is located?

   Solution: done in class

9. Determine whether each of these integers is congruent to 7 modulo 11

   a) 84 **Answer:** congruent

   b) -26 **Answer:** congruent

   Solution:

   we will use a theorem that says that $a \equiv b(\ \texttt{mod}\ n)$ **iff** (is and only if) $a\ \texttt{mod}\ n = b\ \texttt{mod}\ n$

   a) $84\ \texttt{mod}\ 11 = 7$ (because $84 \div 11 = 7\ \texttt{R}\ 7$), hence $84 \equiv 7(\ \texttt{mod}\ 11)$

   b) $-26\ \texttt{mod}\ 11 = 7$, hence $-26 \equiv 7(\ \texttt{mod}\ 11)$

   computation: $-26 \div 11 = -2.(36)$, take 1 less (-3)

   $(-26) - 11(-3) = -26 + 33 = 7$ or how to get from -33 back to -26...need +7

10. Find the expansion base 3 of 16

    Solution: $16 \div 3 = 5$ `R 1`

    $5 \div 3 =$ `1 R 2`

    STOP

    starting with the last quotient, list the quotient (1) and all remainders (we can call it reverse order): 121

    Answer: $16 = (121)_3$

11. Compute decimal representation of $(167)_8$

    Solution: $(167)_8 = 7 \times 8^0 + 6 \times 8^1 + 1 \times 8^2 = 7 + 48 + 64 = 119$

    Answer: $(167)_8 = 119$

12. Compute $(23 \times 14 + 25)$ `mod 7` using modular arithmetic (without use of calculator)

    Solution: $(23 \times 14 + 25)$ `mod 7` $=$

    $=$ $([(23$ `mod 7`$) \times (14$ `mod 7`$)]$ `mod 7` $+ 25$ `mod 7`$)$ `mod 7` $=$

    $=$ $([2 \times 0]$ `mod 7` $+ 4)$ `mod 7` $= (0$ `mod 7` $+ 4)$ `mod 7` $= 4$

13. How many different four-digit pin numbers, using digits from 0 to 9, can people have if no digits are repeated

    Solution: _ _ _ _

    For the first position we have 10 options to choose from $(0, \ldots, 9)$, for the second one we will have only 9 options left (because we do not want repetitions of digits), for the third one 8, and for the last one 7.

    Answer: Therefore there are $10 \times 9 \times 8 \times 7 = 5040$ different 4-digit pin numbers, using digits from 0 to 9, with no digits repeated.

14. Given a set $S = \{x, y, z, 8, 9, 10\}$, how many 3-element subsets does S have?

    Solution: First thing to note is that we are not asked for the powerset!

    We are interested in three-elements subsets (order is not important in sets). Therefore, this is the case of 3-combinations (3-subsets).

    $$C(6,3) = \binom{6}{3} = \frac{6!}{3!(6-3)!} = \frac{6 \times 5 \times 4}{3 \times 2 \times 1} = 20$$

    Answer: 20 3-element subsets

15. How many integers from 1 to 300 are only multiples of 5 or 7?

    Solution: Let's look at the first 10: $1, \ldots, 10$: only two numbers (5 and 10) are multiples of 5.

    The second ten: $11, \ldots, 20$: only two numbers (15 and 20) are multiples of 5 and so forth...

    Therefore, in the first hundred: $1, \ldots, 100$ there are 2×10 numbers that are multiples of 5.

    Hence, in 300, there are $2 \times 10 \times 3 = 60$ numbers that are multiples of 5.

    Note that we will get the same answer if we just get the quotient of the division of 300 by 5 and : 300 `div` $5 = 60$

    Now let's check multiples of 7:

    there are 300 `div` $7 = 42$ - this is how many numbers that are multiples of 7 in interval $[1, 300]$.

    Don't forget to exclude those we counted twice, like 35, 70, ...

    There are 300 `div` $35 = 8$ of them.

    So our answer would be $60 + 42 - 8 = 94$

    Answer: 94 integers from 1 to 300 are multiples of 5 and 7.

PART II. Do any four (4) problems. Each problem is worth 10 points.

1. Show that the compound propositions $\neg p \vee (r \rightarrow \neg q)$ and $\neg(p \wedge q \wedge r)$ are logically equivalent using logical equivalences (do not use truth tables).

   Solution:

   $\neg p \vee (r \rightarrow \neg q) \equiv$ by law (11)

   $\equiv \neg p \vee (\neg r \vee \neg q) \equiv$ by commutative and associative laws

   $\equiv \neg p \vee \neg q \vee \neg r \equiv$ by DeMorgan's laws

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

2. For the sets $A = \{1, 3, 4, d\}$, $B = \{1, 3, d\}$

   (a) Find the *powerset* of A, $P(A)$, and give its cardinality.
   Solution: $|P(A)| = 2^{|A|} = 2^4 = 16$
   $P(A) = \{\emptyset, \{1\}, \{3\}, \{4\}, \{d\}, \{1,3\}, \{1,4\}, \{1,d\}, \{3,4\}, \{3,d\}, \{4,d\}, \{1,3,4\}, \{1,3,d\}, \{1,4,d\}, \{3,4,d\}, \{1,3,4,d\}\}$

   (b) Find the *Cartesian Product* $B \times A$, and give its cardinality.
   Solution: $|B \times A| = |B| \times |A| = 4 \times 3 = 12$
   Pay attention to the order of the elements!
   First element comes from set B, and the second one from set A.
   The result of Cartesian product is a **set of tuples**.
   $B \times A = \{(1,1), (1,3), (1,4), (1,d), (3,1), (3,3), (3,4), (3,d), (d,1), (d,3), (d,4), (d,d)\}$

   (c) Is $A \subset B$?
   Answer: no, because $4 \in A$, but $4 \notin B$

   (d) Is $B \subset A$?
   Answer: yes, because every element of B is also an element of A.

3. Determine whether the function $f(x) = 2x^3 + 1$, where $f(x)$: `R` $\rightarrow$ `R` is

   a) one-to-one (injective)?

   Solution: the function $f(x)$ is one-to-one, because no two different elements are mapped to the same one.

   reasoning:

   Let's assume that $x \neq y$ and see if $f(x) = f(y)$

   $2x^3 + 1 = 2y^3 + 1$

   $-1 \qquad -1$

   $2x^3 = 2y^3$

   $\div 2 \quad \div 2$

$x^3 = y^3$ the odd power preserves the sign, hence for the two sides to be equal, x must be equal to y, but we assumed that it isn't so.

Therefore no two different values are mapped to the same one.

b) onto (surjective)?

The domain and codomain (target) are the sets of all real numbers. The function is well defined on R, i.e. no divisions by zero. Therefore, for any value y from the codomain(target set) we will be able to find a pre-image x such that $f(x) = y$

Answer: $f(x)$ is onto

c) one-to-one correspondence (bijection)?

Answer: yes, because $f(x)$ is both one-to-one and onto.

d) Has inverse? If yes, give the inverse function.

Solution:

Yes it does, because it is **onto**.

To find the inverse we need to solve $y = 2x^3 + 1$ for x:

$x = \sqrt[3]{\frac{y-1}{2}}$, hence $f^{-1}(x) = \sqrt[3]{\frac{x-1}{2}}$

4. Sort the list of integers $\{9, 0, 2, 7, 4, 3\}$ using the *bubble sort*.

   Show all the passes, with interchanges.

   Solution: there will be $n - 1 = 6 - 1 = 5$ passes

   the values that are compared are underlined

   pass one

3	3	3	3	$\underline{3}$	**9**
4	4	4	$\underline{4}$	$\underline{9}$	3
7	7	$\underline{7}$	$\underline{9}$	4	4
2	$\underline{2}$	$\underline{9}$	7	7	7
$\underline{0}$	$\underline{9}$	2	2	2	2
$\underline{9}$	0	0	0	0	0

   pass two

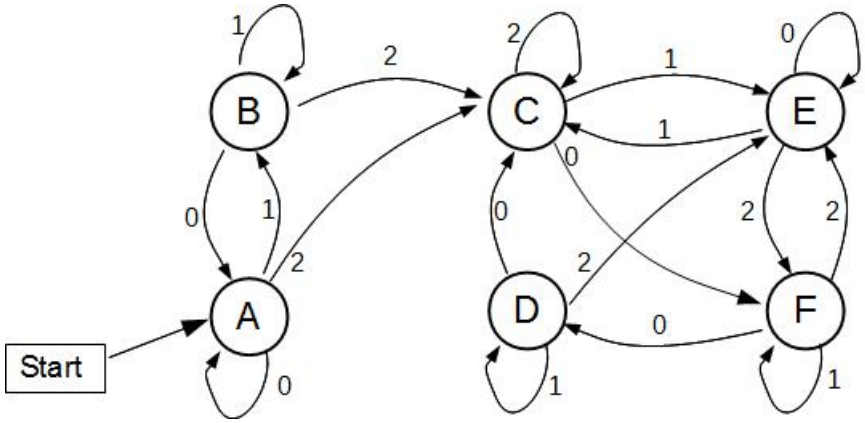
9	**9**	**9**	**9**	**9**
3	3	3	$\underline{3}$	**7**
4	4	$\underline{4}$	$\underline{7}$	3
7	$\underline{7}$	$\underline{7}$	4	4
$\underline{2}$	$\underline{2}$	2	2	2
$\underline{0}$	0	0	0	0

   pass three

9	**9**	**9**	**9**
7	**7**	**7**	**7**
3	3	3	**4**
4	4	4	3
2	2	2	2
0	0	0	0

there will be two more passes, but no interchanges, since the elements are already sorted.

5. For the following Finite State Machine (FSM)



a) What is the current state after the FSM has processed the following input sequence: 0 1 2 1 0 2 1?

Answer: state **F**

reasoning: from **A** input 0 will bring us to state **A**, then input 1 will send us to state **B**, then input 2 will forward us to state **C**, the next input value 1 will take us to **E**, 0 will keep us at state E, input 2 will send us to state F, and finally input 1 will keep us in state F.

b) Give the shortest input that gives the shortest path (in terms of state changes) from start state **A** to state **D** ?

Answer: 200

6. Consider a simple ***cryptosystem*** in which the set of all possible *plaintexts* m come from Z_N for some integer N. Alice and Bob share a secret number $k \in Z_N$. The security of their encryption scheme rests on the assumption that no one besides them knows the number k. To encrypt a *plaintext* $m \in Z_N$, Alice computes:

$c = (m + k)$ `mod` N (encryption)

Alice sends the *ciphertext* c to Bob. When Bob receives the *cyphertext* c, he decrypts c as follows:

$m = (c - k)$ `mod` N (decryption)

Assume that $N = 1347$, and Alice and Bob agreed on key $k = 423$

a) Alice wants to send the *plaintext* message $m = 245$ to Bob.

What will be the encrypted message, *cyphertext* c?

Solution: $c = (245 + 423)$ `mod` $1347 = 668$

b) Bob received *cyphertext* $c = 137$ from Alice.

What will be the *plaintext* message m after he decrypts the *cyphertext*?

Solution: $m = (137 - 423)$ `mod` $1347 = -286$ `mod` $1347 = 1061$

c) Suppose that Eve somehow found out that $N = 2347$ and also managed to learn that message $m = 1234$ corresponds to $c = 310$. Can she infer/deduce the value for key k? Show how.

Solution:

Eve knows $N = 2347$, $m = 1234$ and $c = 310$.

She also knows the formulas for the simple encryption: $c = (m + k)$ `mod` N.

Therefore she will get $310 = (1234 + k)$ `mod` 1347 - from here she can deduce key k:

$(1234 + k) - 1347 = 310$ after solving this linear equation we will get that $k = 310 + 1347 - 1234 = 423$.

"Hooray!" (for Eve) and "Oh, my!" for Bob and Alice.

7. How many bit-strings of length 9 contain

   (a) three 0's in the beginning and two 1's at the end?

   Solution: the order of bits is important,

   in addition, we have three 0's in the beginning with two 1's at the end

   9-bit string: $\underline{0}\ \underline{0}\ \underline{0}\ \_\ \_\ \_\ \_\ \underline{1}\ \underline{1}$

   choices : 1 1 1 2 2 2 2 1 1

   $1 \times 1 \times 1 \times 2 \times 2 \times 2 \times 2 \times 1 \times 1 = 2^4 = 16$ bit strings

   Answer: 16 bit strings

   (b) at least two 1's?

   in this case the position of 1's is not fixed, all we know is that there should be at least two of them. Hence we cannot use the method employed in item (a) to find the answer. We will have to use combinations (the order of 1's in their positions is not important to us, because we believe that 1s are distinguishable).

   two 1's in the bit string: $C(9, 2) = \binom{9}{2} = \ldots$

   three 1's in the bit string: $C(9, 3) = \binom{9}{3} = \ldots$

   four 1's in the bit string: $C(9, 4) = \binom{9}{4} = \ldots$

five 1's in the bit string: $C(9,5) = \binom{9}{5} = \ldots$

six 1's in the bit string: $C(9,6) = \binom{9}{6} = \ldots$

seven 1's in the bit string: $C(9,7) = \binom{9}{7} = \ldots$

eight 1's in the bit string: $C(9,8) = \binom{9}{8} = \ldots$

nine 1's in the bit string: $C(9,9) = \binom{9}{9} = \ldots$

After we find all of them we will add them up to get the answer, but it is too many computations of binomial coefficient we will have to perform.

Let's use complement property!

The complement will be " at most one 1, meaning that no 1's or one 1.

one 1 in the bit string: $C(9,1) = \binom{9}{1} = \frac{9!}{1!(9-1)!} - \frac{9!}{8!} = 9$

no 1's in the bit string: $C(9,0) = \binom{9}{0} = \frac{9!}{0!(9-0)!} - \frac{9!}{9!} = 1$

$C(9,1) + C(9,0) = 9 + 1 = 10$

Finaly, there 2^9 bit strings of length 9.

Therefore, our answer is $2^9 - 10 = 512 - 10 = 502$

Answer: 502 bit strings

comment: try to find $C(9,2)+C(9,3)+C(9,4)+C(9,5)+C(9,6)+C(9,7)+C(9,8)+C(9,9)$ on your own, for practice.

It should be equal to 502.

(c) number of 1's is more than the number of 0's?

the case when the requirement will fulfilled:

5 1's, 4 0's: $C(9,5) = C(9,4) = \binom{9}{5} = \frac{9!}{5!(9-5)!} = \frac{9!}{5!4!} = 126$

6 1's and 3 0's: $C(9,6) = C(9,3) = \binom{9}{6} = \frac{9!}{6!(9-6)!} = \frac{9!}{6!3!} = 84$

7 1's and 2 0's: $C(9,7) = C(9,2) = \binom{9}{7} = \frac{9!}{7!(9-7)!} = \frac{9!}{7!2!} = 36$

8 1's and 1 0: $C(9,8) = C(9,1) = \binom{9}{8} = \frac{9!}{8!(9-8)!} = \frac{9!}{8!1!} = 9$

9 1's and no 0's: $C(9,9) = C(9,0) = \binom{9}{9} = \frac{9!}{9!(9-9)!} = \frac{9!}{9!0!} = 1$

Adding them up (sum rule): $126 + 84 + 36 + 9 + 1 = 256$

Answer: 256 bit strings