BRONX COMMUNITY COLLEGE

of The City University of New York

DEPARTMENT OF MATHEMATICS and COMPUTER SCIENCE

FINAL EXAMINATION SAMPLE

Instructions: Do all problems from PART I and **four** (4) problems from PART II. Please **clearly show all your work** to receive full credit, i.e. you must **justify your answers by the work shown** on this exam.

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)

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

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

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

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

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.** $b \in \{a, \{a, b\}, \{b\}, \{\{a\}, b\}\}$

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?

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?

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

   a) 84 **b)** -26

10. Find the expansion base 3 of 16

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

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

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

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

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

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.

   (b) Find the *Cartesian Product* $B \times A$, and give its cardinality.

   (c) Is $A \subset B$?

   (d) Is $B \subset A$?

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

   a) one-to-one (injective)?

   b) onto (surjective)?

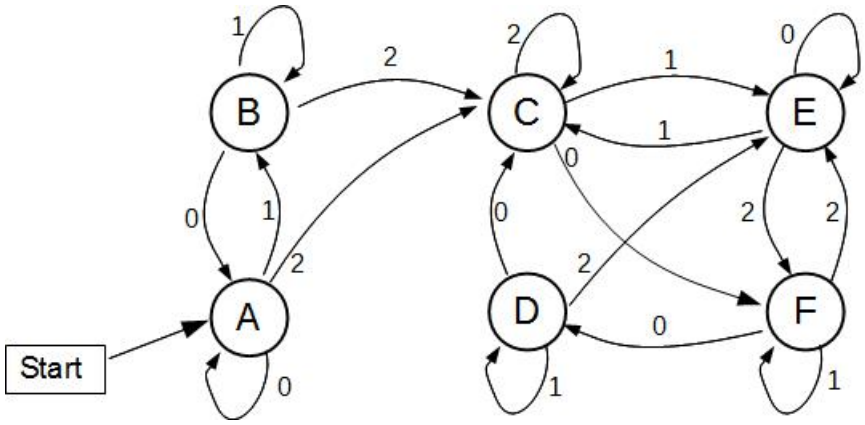
   c) one-to-one correspondence (bijection)?

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

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

   Show all the passes, with interchanges.

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?

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

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?

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

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

   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.

7. How many bit-strings of length 9 contain

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

   (b) at least two 1's?

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