1. Construct a truth table for each of these compound propositions. 12 分

a) $(p \vee q) \rightarrow (p \oplus q)$ **b)** $(p \oplus q) \rightarrow (p \wedge q)$
c) $(p \vee q) \oplus (p \wedge q)$ **d)** $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$
e) $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$
f) $(p \oplus q) \rightarrow (p \oplus \neg q)$

p	q	r	$(p \vee q) \rightarrow (p \oplus q)$	$(p \oplus q) \rightarrow (p \wedge q)$	$(p \vee q) \oplus (p \wedge q)$	$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$	$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$	$(p \oplus q) \rightarrow (p \oplus \neg q)$
T	T	T	F	T	F	T	F	T
T	F	T	T	F	T	T	T	F
F	T	T	T	F	T	T	F	F
F	F	T	T	T	F	T	T	T
T	T	F					T	
T	F	F					F	
F	T	F					T	
F	F	F					F	

2. Show that $(p \rightarrow r) \vee (q \rightarrow r)$ and $(p \wedge q) \rightarrow r$ are logically equivalent. 3 分

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

3. Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people. 10 分

a) Someone in your class can speak Hindi.
b) Everyone in your class is friendly.
c) There is a person in your class who was not born in California.
d) A student in your class has been in a movie.
e) No student in your class has taken a course in logic programming.

Let C(x) be the propositional function "x is in your class."
a) ∃xH(x) and ∃x(C(x) ∧ H(x)), where H(x) is "x can speak Hindi"
b) ∀xF(x) and ∀x(C(x) → F(x)), where F(x) is "x is friendly"
c) ∃x¬B(x) and ∃x(C(x)∧¬B(x)), where B(x) is "x was born in California"
d) ∃xM(x) and ∃x(C(x) ∧ M(x)), where M(x) is "x has been in a movie"
e) ∀x¬L(x) and ∀x(C(x) → ¬L(x)), where L(x) is "x has taken a course in logic programming"

4. Use rules of inference to show that if $\forall x(P(x) \rightarrow (Q(x) \wedge S(x)))$ and $\forall x(P(x) \wedge R(x))$ are true, then $\forall x(R(x) \wedge S(x))$ is true. 10 分

Step	Reason
1. ∀x(P(x) ∧ R(x))	Premise
2. P(a) ∧ R(a)	Universal instantiation from (1)
3. P(a)	Simplification from (2)
4. ∀x(P(x) →(Q(x) ∧ S(x)))	Premise
5. Q(a) ∧ S(a)	Universal modus ponens from(3) and (4)
6. S(a)	Simplification from (5)
7. R(a)	Simplification from (2)
8. R(a) ∧ S(a)	Conjunction from (7) and (6)
9. ∀x(R(x) ∧ S(x))	Universal generalization from (5)

5. Determine whether each of these statements is true or false. 6 分

a) $x \in \{x\}$ **b)** $\{x\} \subseteq \{x\}$ **c)** $\{x\} \in \{x\}$
d) $\{x\} \in \{\{x\}\}$ **e)** $\emptyset \subseteq \{x\}$ **f)** $\emptyset \in \{x\}$

a) T b) T c) F d) T e) T f) F

6. Suppose the universal set is {1,2,3,4,5,6,7,8} and A = {1,2,3,6,8}, B = {6,7,8}, C = {3,6} 8 分

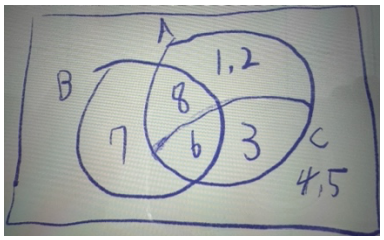
a) Depict the sets on a Venn diagram.

b) Write the set $(\overline{A \cup C}) \cup B$ in enumerated form.

c) Write the set $B \times C$ in enumerated form.

d) Write the set $C^2 \cap (A \times B)$ in enumerated form.

a)



b) $(\overline{A \cup C}) \cup B \equiv \bar{A} \cup B = \{4,5,7\} \cup \{6,7,8\} = \{4,5,6,7,8\}$

c) $B \times C$ = {(6,3),(6,6),(7,3),(7,6),(8,3),(8,6)}

d) $C^2 \cap (A \times B) = \{(3,3),(3,6),(6,3),(6,6)\} \cap (A \times B) = \{(3,6),(6,6)\}$

7. Determine whether f is a function from the set of all bit strings to the set of integers if 6 分

a) $f(S)$ is the position of a 0 bit in S.
b) $f(S)$ is the number of 1 bits in S.
c) $f(S)$ is the smallest integer i such that the ith bit of S is 1 and $f(S) = 0$ when S is the empty string, the string with no bits.

a) No (one to many) b) Yes c) No (what if S='00000'?)

8. Determine whether each of these functions is a bijection from **R** to **R**. 8 分

a) $f(x) = 2x + 1$
b) $f(x) = x^2 + 1$
c) $f(x) = x^3$
d) $f(x) = (x^2 + 1)/(x^2 + 2)$

a) Y b) N c) Y d) N

9. What are the terms a_0, a_1, a_2, and a_3 of the sequence $\{a_n\}$, where a_n equals 8 分

a) $2^n + 1$? **b)** $(n+1)^{n+1}$?
c) $\lfloor n/2 \rfloor$? **d)** $\lfloor n/2 \rfloor + \lceil n/2 \rceil$?

a) $a_0 = 2, a_1 = 3, a_2 = 5, a_3 = 9$

b) $a_0 = 1, a_1 = 4, a_2 = 27, a_3 = 256$

c) $a_0 = 0, a_1 = 0, a_2 = 1, a_3 = 1$

d) $a_0 = 0, a_1 = 1, a_2 = 2, a_3 = 3$

10. Find $\sum_{k=100}^{200} k$ 4 分

15150

11. Describe an algorithm that takes as input a list of n integers and finds the location of the last even integer in the list or returns 0 if there are no even integers in the list. 5 分

procedure last even location(a1 ,a2 , ... ,an: integers)
k := 0
for i := 1 to n
if a_i is even then k: = i
return k {k = 0 if there are no evens}

12. Give a big-O estimate for each of these functions. For the function g in your estimate that $f(x)$ is $O(g(x))$, use a simple function g of the smallest order. 6 分

a) $n \log(n^2 + 1) + n^2 \log n$
b) $(n \log n + 1)^2 + (\log n + 1)(n^2 + 1)$
c) $n^{2^n} + n^{n^2}$

a) $O(n^2 \log n)$ **b)** $O(n^2 (log\ n)^2)$ **c)** $O(n^{2^n})$

13. Convert the octal expansion of each of these integers to a binary expansion. 8 分

a) $(572)_8$ **b)** $(1604)_8$
c) $(423)_8$ **d)** $(2417)_8$

a) 101 111 010 b)~~00~~1 110 000 100 c) 100 010 011 d) ~~0~~10 100 001 111

14. Find the solutions x to the following system of congruences 6 分

$$x \equiv 1(mod\ 4)$$
$$x \equiv 2(mod\ 5)$$
$$x \equiv 3(mod\ 7)$$

$$r_1 = 1, r_2 = 2, r_3 = 3, n_1 = 4, n_2 = 5, n_3 = 7, n = n_1 n_2 n_3 = 140$$
$$N_1 = \frac{n}{n_1} = 35, N_2 = \frac{n}{n_2} = 28, N_3 = \frac{n}{n_3} = 20$$
$$M_i = N_I^{-1}(mod\ n_i), i = 1,2,3$$
$$\because 35 \times 3 \equiv 1(mod\ 4)\ \therefore M_1 = 3$$
$$\because 28 \times 2 \equiv 1(mod\ 5)\ \therefore M_2 = 2$$
$$\because 20 \times (-1) \equiv 1(mod\ 7)\ \therefore M_3 = -1$$
$$x \equiv r_1 M_1 N_1 + r_2 M_2 N_2 + r_3 M_3 N_3 \equiv 1 \times 3 \times 35 + 2 \times 2 \times 28 + 3 \times (-1) \times 20 \equiv 157 \equiv 17(mod\ 140)$$
$$\therefore x = 17 + 140k, \forall k \in Z$$

15. For a RSA public key system, to encrypt a text, x, is to perform the formula: $y = x^n\ mod\ z$, where n is the public key and z is call the "public modulus". Suppose that you are give two prime numbers, 17 and 23, and n = 31. Use RSA algorithm to

a) Derive the z. 3 分

b) Prove or disprove that s = 159 is a private key. 3 分

c) Encrypt x = 31 using public key n and z. 4 分

a) $y = x^n\ mod\ z, z = pq = 17 \times 23 = 391$

b) $sn \equiv 1\big(mod(p-1)(q-1)\big),\ (p-1)(q-1) = 16 \times 22 = 352$
$$sn = 159 \times 31 = 4929\ \because 4929 = 14 \times 352 + 1$$
$$=> 4929 \equiv 1\ (mod\ 352), sn \equiv 1\big(mod\ (p-1)(q-1)\big)$$
$$\therefore s = 159 = private\ key$$

c) $y = x^n\ mod\ z = 31^{31}\ (mod\ 391)$
$$y \equiv 31^{31} \equiv 31^{16} \cdot 31^8 \cdot 31^4 \cdot 31^2 \cdot 31 \equiv 154 \cdot 50 \cdot 370 \cdot 179 \cdot 31 \equiv 147\ (mod\ 391)$$