Assignment - 2 (submission deadline: 12 April, 2018)

Note: Unless otherwise stated, notation used is as defined in the class.

1. Apply the **Chinese Remainder Theorem** to solve the following system of congruences:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}$$

2. Use the **Extended Euclidean algorithm** to compute $886^{-1} \pmod{1353}$.

3. What is the converse, inverse and contrapositive for the following propositions?

   (a) A right implies a responsibility.

   (b) The right to search for the truth implies also a duty.

   (c) Speak only if it improves upon the silence.

4. Find the negation of the proposition:
   "Alexander the Great was a Roman leader and $2 + 1 = 3$"

5. Rewrite the quote by Benjamin Franklin (1706-1790) as a conditional proposition:
   "Never put off till tomorrow what you can do today".

6. Construct a truth table for each of the following propositions, and classify if each proposition as either a tautology, a contradiction, or a contingencies:

   (a) $(p \to q) \vee (q \to p)$

   (b) $(p \vee q) \wedge (p \vee \neg q)$

   (c) $(p \vee q) \wedge (\neg p \wedge \neg q)$

7. Use the rules of inference to show that $\neg(p \vee \neg(p \wedge q))$ is a contradiction.

8. Prove that $[(p \wedge \neg(\neg p \vee q)) \vee (p \wedge q)] \longrightarrow p$ is a tautology. Do not use truth table.

9. Find the negation of the implication:
   "If you are from the state of New York, then you will receive a scholarship."

10. For the following argument, translate it into symbolic logic, and determine whether or not the argument is valid.
    "If a country is devoloping, it cannot devote much of its financial resource to technology development. However, if a country cannot devote much of its financial resource to technology development, then its economy will not grow. Therefore, a developing country will not have an economic growth. "

11. Using modus ponens, what can you conclude from the following premises?
    "My improvement upon silence is necessary when I need to speak the truth. And after seeing these grave atrocities, I cannot restrain my tongue."

12. Construct an argument, on any subject of your choosing, with only two premises, having the following characteristics:

    (a) An invalid argument with two true premises, and a true conclusion.

    (b) An invalid argument with two true premises, and a false conclusion

13. When the Roman Emperor Marcus Aurelius (121-180) persecuted early Christians, Tertullian (155-240) argued against the methods Aurelius employed.

Either Christians have committed crimes or not. If they are guilty of crimes, your refusal to permit a public inquiry is irrational. If they have committed no offence, it is unjust to punish them.
Therefore, your conduct is either unjust or irrational.

Show that Tertullian's arguments is valid.

14. Sir Richard Empson (c. 1450-1510) minister to king Henry VII of England, reportedly was able to demonstate that any person was capable of paying a heavy tax.

If the accused lives at a small rate, his savings must make him rich. If the accused maintains a large household, his expenditures proves he is rich. But, either he lives at a small rate, or he maintains a large expenditure.
Therefore, he is rich, and consequently can play heavily to the king.

This argument has been given the title of the Emperor's fork: whoever was found in the cross hairs of this argument was impaled on the prongs of this dilemma.
Determine whether Sir Empson's argument is valid and explain why?

15. Show that the following is a valid argument:

Everyone shouts or cries. Not everyone cries.
So some people shout and does not cry.

Which rules of inference are used to established the above conclusion?

16. Use resolution to show that the following is a valid argument:

All students go to parties. Some students drink too much.
Therefore, some people who drink too much must go to parties.

17. Write down the converse of the following statement.
"If n is a multiple of 3 then n is not a multiple of 7."
Say whether the original statement and its converse are true or false, and justify your answers.

18. Consider the statement:
u : if n is the square of an even integer then n is the sum of two successive odd integers. (Here "successive odd integers" means odd integer of the form $k, k+2$.)

    (a) Show that u is true by using a construction based on the following examples:
    $4^2 = 7 + 9, 6^2 = 17 + 19, 8^2 = 31 + 33, 10^2 = 49 + 51$

    (b) Write down the converse of the statement u and show that it is false.

    (c) Write down the contrapositive of the statement u. Is it true or false?

19. Obtain disjunctive normal form, conjunctive normal form, principal disjunctive normal form and principal conjunctive normal form of $(\neg P \vee \neg Q) \longrightarrow (P \longleftrightarrow \neg Q)$.

20. Given the Boolean function

$$F = x\overline{y}z + \overline{x}\ \overline{y}z + xyz$$

(a) List the truth table of the function.

(b) Draw the logic diagram using the original Boolean expression.

(c) Simplify the algebraic expression using Boolean algebra.

(d) List the truth table of the function from the simplified expression and show that it is the same as the truth table in part (a).

(e) Draw the logic diagram from the simplified expression and compare the total number of gates with the diagram of part (b).

21. Simplify the following expression in (a) sum-of-product form, and (b) product-of-sum form.

$$A\overline{C} + \overline{B}D + \overline{A}CD + +ABCD$$

22. Simplify the following Boolean function in sum-of-products form by means of a four-variable map. Draw the logic diagram with (a) AND-OR gates; (b) NAND gates.

$$F(A, B, C, D) = \sum(0, 2, 8, 9, 10, 11, 14, 15)$$

23. Simplify the following Boolean function in product-of-sum form by means of a four-variables map. Draw the logic diagram with (a) OR-AND gates; (b)NOR gates

$$F(w, x, y, z) = \sum(2, 3, 4, 5, 6, 7, 11, 14, 15)$$

24. Simplify the Boolean function F together with the don't care conditions d in (a) sum-of-products form, and (b) product-of-sums form

$$F(w, x, y, z) = \sum(0, 1, 2, 3, 7, 8, 10)$$

$$d(w, x, y, z) = \sum(5, 6, 11, 15)$$

25. Use the tabulation procedure to generate the set of prime implicants and to obtain all minimal expressions for the following functions:

(a) $f(w, x, y, z) = \sum(0, 1, 5, 7, 8, 10, 14, 15)$

(b) $f(w, x, y, z) = \sum(0, 1, 2, 5, 7, 8, 9, 10, 13, 15)$

26. Simplify the sum-of-products expression for the function

$$f(x, y, z) = xyz + x\overline{y}z + x\overline{y}\ \overline{z} + \overline{x}yz + \overline{x}y\overline{z} + \overline{x}\ \overline{y}\ \overline{z}$$

using (a) a k-map, (b)the Quine-McCluskey method.

27. Determine the cannonical sum-of-products representation of the following functions:

(a) $f(x, y, z) = z + (\overline{x} + y)(x + \overline{y})$

(b) $f(x, y, z) = x + \overline{(\overline{x}\ \overline{y} + \overline{x}z)}$

28. Simplify the algebraic expression:

$$(\overline{x} + xy\overline{z}) + (\overline{x} + xy\overline{z})(x + \overline{x}\ \overline{y}z)$$

29. Find the complement of
$$\overline{w} + (\overline{x} + y + \overline{y}\ \overline{z})(x + \overline{y}z)$$
and then simplify it.

30. Given $A\overline{B} + \overline{A}B = C$, show that $A\overline{C} + \overline{A}C = B$

31. Show that $F^d(x_1, \ldots, x_n) = \overline{F(\overline{x}_1, \ldots, \overline{x}_n)}$ for a Boolean function $F(x_1, \cdots, x_n)$, where F^d stands for the dual of F.

32. Which of the following groupoids are semigroups? Which are groups?

   (a) $(\mathbb{N}, \star)$ where $a \star b = ab$ for all $a, b \in \mathbb{N}$.
   (b) $(\mathbb{N}, \star)$ where $a \star b = b$ for all $a, b \in \mathbb{N}$.
   (c) $(\mathbb{Z}, \star)$ where $a \star b = a - b$ for all $a, b \in \mathbb{Z}$.
   (d) $(\mathbb{Z}, \star)$ where $a \star b = a + b + ab$ for all $a, b \in \mathbb{Z}$.
   (e) $(\mathbb{R}, \star)$ where $a \star b = a|b|$ for all $a, b \in \mathbb{R}$.
   (f) $(\mathbb{R}, \star)$ where $a \star b = 2^a b$ for all $a, b \in \mathbb{R}$.

33. Let $(G, \star)$ be a group and $a, b \in G$. Suppose that $a^2 = e$ and $a \star b \star a = b^7$. Show that $b^{48} = e$.

34. Let G be a group generated by the elements a and b such that $o(a) = 4, a^2 = b^2$, and $ba = a^3 b$. Find $o(b)$ and $|G|$.

35. If $G = \langle g \rangle$ is a cyclic group of order 30, then find all distinct elements of (a) order 5 (b) order 6.

36. Let G be a group, then prove that G is abelian when $a^2 = a \quad \forall a \in G$ holds.

37. Justify your answer: $(Q^+, \star)$ is not a abelian group where $a \star b = \frac{ab}{2} \quad \forall a, b \in \mathbb{Q}$

38. Which of the following algebraic structures $(R, +, \cdot)$ form a ring?

   (a) Let X be any set and $R = P(X)$, the power set of X. Define $A + B = A \triangle B$ and $A \cdot B = A \cap B$ for all $A, B \in R$ (where $A \triangle B = (A - B) \cup (B - A)$)
   (b) In the above set R, define $A + B = A \cup B$ and $A \cdot B = A \cap B$ for all $A, B \in R$.
   (c) Let R be the set of all real-valued continuous functions defined on $\mathbb{R}$. Define $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(g(x))$ for all $f, g \in R$ and for all $x \in \mathbb{R}$.
   (d) Let R be the set of all twice differentiable real-valued functions having second derivative zero at $x = 0$. Define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$ for all $f, g \in R$ and for all $x \in \mathbb{R}$.

39. Let R be a commutative ring with characteristic p, where p is a prime number. Prove that $(a + b)^p = a^p + b^p$.

40. Find all c such that $\mathbb{Z}_3[x]/\langle x^3 + cx^2 + 1 \rangle$ is a field.

41. Show that (a) $\mathbb{Z}$ is not a field, (b) $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ is not a field.

42. Let E be the modular elliptic curve defined by $y^2 = x^3 + 3x \pmod{17}$. (a) Find all points of E (including the point at infinity), (b) find $2(8, 14)$.

43. The field $\mathsf{GF}(2^5)$ can be constructed as $\mathbb{Z}_2[x]/(x^5+x^2+1)$. (a) Compute $(x^4+x^2)\times(x^3+x+1)$, (b) using the **Extended Euclidean algorithm**, compute $(x^3 + x^2)^{-1}$.

——-END———