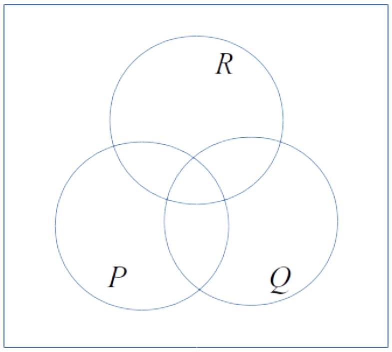
Midterm, 2020-02-17

Question 1 (Boolean Expressions).
Consider Boolean expression:

$$E_0 = (p \to q \to r) \wedge (q \to r \to p) \wedge (r \to p \to q)$$



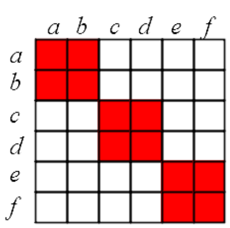
(A) Copy the Venn diagram's circles in your solution and shade those regions in the diagram that make E_0 true (being inside each circle P, Q, R means that the respective variable p, q, r is true; being outside the circle means that the variable is false).

(B) In the truth table of E_0 how many entries are `True`?
(*Note.* Building the truth table is optional. Regardless whether you build one or not, you should justify your answer.)

(C) Rewrite the Boolean expression E_0 into an equivalent one, using only conjunctions ($\wedge$) and negations ($\neg$).

Assume that implication ($\to$) is right-associative and conjunction ($\wedge$) has higher precedence than implication.

Question 2 (Nested Quantifiers).
Verify, if the following predicate/quantifier expressions are true for the given predicate. The predicate P is defined on $A \times A$, where $A = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}$. Predicate $P(\mathtt{a}, \mathtt{b})$ is true iff the square on row a and column a is shaded (and the predicate $P(\mathtt{a}, \mathtt{b})$ is false, if that square is white).



(A) Does the predicate P satisfy the logic formula:

$$\forall i \in A,\ P(i, i).$$

(B) Does the predicate P satisfy the logic formula:

$$\forall i \in A,\ \forall j \in A,\ P(i, j) \to P(j, i).$$

(C) Does the predicate P satisfy the logic formula:

$$\forall i, j, k \in A,\ P(i, j) \wedge P(j, k) \to P(i, k).$$

(D) Does the predicate P satisfy the logic formula:

$$\forall i, j \in A,\ P(i, j) \vee P(j, i).$$

(E) Does the predicate P satisfy the logic formula:

$$\forall i \in A,\ \exists j \in A,\ P(i, j).$$

Question 3 (Estimate with Big-O Notation).
Define the sequence $S(n)$ as a sum of squares from 1^2 to n^2:

$$S(n) = \sum_{i=1}^{n} i^2.$$

We have $S(1) = 1^2 = 1$, $S(2) = 1^2 + 2^2 = 5$, $S(3) = 1^2 + 2^2 + 3^2 = 14$, and so on.

(A) Is the function $S(n)$ in $O(n^1)$? Is it in $O(n^2)$? Is it in $O(n^3)$? Is it in $O(n^4)$? Explain your reasoning.

(B) Pick any one of the notations from the previous items ($g(n)$ is either $O(n^1)$, or $O(n^2)$, or $O(n^3)$, or $O(n^4)$). Check the definition of Big-O notation: Find the *witness*: the value k and the constant C such that the absolute value of $S(n)$ does not exceed $C \cdot |g(n)|$ for all $n > k$.

Question 4 (Chinese Remainder Theorem).
Consider the following system of three congruences:

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 2 \pmod{7}, \\ x \equiv 3 \pmod{9}. \end{cases}$$

(A) Does it have a solution? Will it have solution, even if we replace $1, 2, 3$ with other numbers on the right sides of the equation.

(B) Find an arithmetic progression (what is its first member A, difference B) where all members satisfy the first two congruences from the system.

(C) Find an arithmetic progression (what is its first member C, difference D) where all members satisfy all three congruences in the system.

Note. Arithmetic progression is an infinite sequence where every next member can be obtained by adding the same number (the difference) to the previous one. For example,

$$A,\ A+B,\ A+2B,\ A+3B,\ldots$$

is an arithmetic progression with the first member A and the difference B.

Question 5 (Binary notation).
Somebody has written two binary fractions on the board: α is infinite, β is finite (just 6 digits after the point):

$$\begin{cases} \alpha = 0.(011110)_2 = 0.011110011110011110\ldots_2 \\ \beta = 0.011110_2. \end{cases}$$

(A) Express the number β as a sum of some negative powers of 2; namely, show how to add up some of the numbers

$$\{2^{-1}, 2^{-2}, 2^{-3}, \ldots\}$$

to get β.

(B) Express β as an irreducible fraction `P/Q`; write this in the regular decimal notation.

(C) Write the product $64_{10} \cdot \alpha = 1000000_2 \cdot \alpha$ in the binary notation.

(D) Express α as an irreducible fraction `P/Q` in decimal notation.

Question 6 (Truth-tellers and Liars). Among the people A, B, C one is a truth-teller, the other two are liars. Every person (A, B, and C) has a closed box in front of himself/herself. Exactly one of the boxes has a candy inside. A, B, C know everything about each other and the location of candy.
Someone else (person D) approaches all of them. D knows, who are people A,B, and C (it is written on their name-cards), but D does not know anything about their lying behavior or the location of the candy. D is allowed to ask YES/NO questions to one or more people.

(A) Can D find out who has the candy by asking three questions?

(B) Can D find out who has the candy by asking two questions?

(C) Can D find out who has the candy by asking one question?

Justify your answers (by construction or by showing that it is impossible).

Question 7 (Time Complexity of Truth Tables).
Assume that there is a Boolean expression E with n variables:

$$E = E(a_1, a_2, \ldots, a_n).$$

The expression E contains $2n$ Boolean operators (such as $\neg$, $\wedge$, $\vee$). Variables $a_1, a_2, \ldots, a_n$ can independently take values `True` or `False`.
Consider the following algorithm to find, if E is a tautology by building the truth table. We will either find a false value, or establish that all values were true (in this case E is a tautology).

(1) For each assignment of n truth values to $a_1, \ldots, a_n$:
(2) For each of the $2n$ Boolean operators in E:
(3) Compute the value of that Boolean operator
(4) If E has value `False`:
(5) Return "E is not a tautology."
(6) If E has value `True`:
(7) Continue loop on Line **(1)**.
(8) Return "E is a tautology."

(A) Find the worst-case runtime $T(n)$ for this algorithm as an expression of n. (Assume that evaluating one Boolean operator $\neg$, $\wedge$, $\vee$ takes 1 unit of time.)

(B) Find a function $g(n)$ such that $T(n)$ is in $O(g(n))$.

Question 8 (About Rational and Irrational).
We denote two real numbers by p and q. Prove or disprove statements about the rational and irrational numbers.

(A) If $p + q$ is rational, then either both p, q are rational, or both are irrational.

(B) If pq is rational, then either both p, q are rational, or both are irrational.

(C) If p^2 and q^2 are both rational, then the product $(p+q)(p-q)$ is rational.

(D) If p^3 and p^5 are both rational, then p is rational.

(E) If pq and $p + q$ are both rational, then p and q are both rational.