Midterm

Discrete Structures
Wednesday, February 24, 2021

You must justify all your answers to recieve full credit

---

1. (a) Write the following sentence as a Boolean expression: "To get an early vaccine it is sufficient to be a public servant involved in the continuous operation of government or a senior citizen with a referral from a family doctor."
Use the following atomic propositions:
V := "One can get an early vaccine"
G := "One is a public servant involved in the continuous operation of government"
S := "One is a senior citizen"
R := "One has a referral from a family doctor."

   (b) Write an equivalent Boolean expression – the contrapositive of the previous one.

(a) Sufficient condition is the one that implies the needed result (but not the other way round: There may be other reasons to get an early vaccine):

$$(G \vee (S \wedge R)) \to V.$$

(b) Contrapositive exchanges both sides of an implication and adds negation:

$$\neg V \to \neg(G \vee (S \wedge R)).$$

□

2. Let A, B, C be subsets in the same universe U. Draw a Venn diagram for these sets and shade all the regions corresponding to the set S:

$$S = (A \cup B \cup \overline{C}) \cap (A \cup \overline{B} \cup C) \cap (\overline{A} \cup B \cup C).$$

Consider clause/subexpression $(A \cup B \cup \overline{C})$. It includes everything, except the points that belong only to the set C (they are neither in the union $A \cup B$ nor in $\overline{C}$. Therefore the intersection will not contain region that is only covered by the set C. Other subexpressions can be analyzed similarly - so the intersection will not contain regions covered with just the set A and just the set B either. See Figure 1.

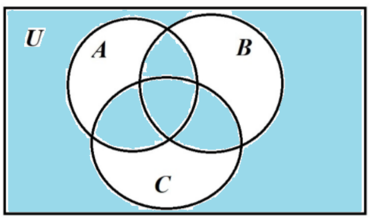

Figure 1: Venn Diagram for Q2 (Regions belonging to S are shaded blue).

Note. This set expression behaves somewhat similarly to the CNF (Conjunctive Normal Form) in Boolean logic - it lists all those regions that we do not want. And then intersects them (or, in case of CNF - they are joined by a conjunction). □

3. Let A, B, C be three arbitrary subsets of the same universe U. Prove or disprove the following set identity:
$$(B \oplus C) \cup A = (B \cup C) \oplus (A - C).$$

This set identity is false in the general case.

Consider an element x that belongs to A and B, but does not belong to C.
Then $x \in (B \oplus C) \cup A$ (since it is a union with set A: should contain all $x \in A$).
On the other hand, $x \notin (B \cup C) \oplus (A - C)$, since x belongs to both $(B \cup C)$ and $(A - C)$, but not to their symmetric difference $\oplus$.

Note. Just like any other set expression, there may be cases when the equality holds (if you pick A, B, C in a special way), but it is not an *identity*; it is not true in the general case. □

4. Let $P(x, y)$ and $Q(x, y)$ be two predicates defined on pairs of integers. Simplify the expression so that all negations are applied directly to the predicate symbols:
$$\neg(\forall y \in \mathbf{Z}\ (\neg Q(x, z) \vee P(x, y)) \wedge \exists z \in \mathbf{Z}\ \forall x \in \mathbf{Z}\ (Q(y, z) \to \neg P(x, y))).$$

Apply De Morgan's law to the outermost operation: $\wedge$.

$$\neg(\forall y \in \mathbf{Z}\ (\neg Q(x, z) \vee P(x, y)) \wedge \exists z \in \mathbf{Z}\ \forall x \in \mathbf{Z}\ (Q(y, z) \to \neg P(x, y))) \equiv$$
$$\equiv \neg(\forall y \in \mathbf{Z}\ (\neg Q(x, z) \vee P(x, y))) \vee \neg(\exists z \in \mathbf{Z}\ \forall x \in \mathbf{Z}\ (Q(y, z) \to \neg P(x, y))).$$

Negate all the quantifiers (negation switches $\exists$ into $\forall$ and vice versa). These are also called De Morgan's laws (for quantifiers rather than simple propositions):

$$\neg(\forall y \in \mathbf{Z}\ (\neg Q(x, z) \vee P(x, y))) \vee \neg(\exists z \in \mathbf{Z}\ \forall x \in \mathbf{Z}\ (Q(y, z) \to \neg P(x, y))) \equiv$$
$$\equiv (\exists y \in \mathbf{Z}\ \neg(\neg Q(x, z) \vee P(x, y))) \vee (\forall z \in \mathbf{Z}\ \exists x \in \mathbf{Z}\ \neg(Q(y, z) \to \neg P(x, y))).$$

Finally, apply negations to the innermost subexpressions (and drop double negations whenever they occur):

$$(\exists y \in \mathbf{Z}\ \neg(\neg Q(x, z) \vee P(x, y))) \vee (\forall z \in \mathbf{Z}\ \exists x \in \mathbf{Z}\ \neg(Q(y, z) \to \neg P(x, y))) \equiv$$
$$\equiv (\exists y \in \mathbf{Z}\ (\neg\neg Q(x, z) \wedge \neg P(x, y))) \vee (\forall z \in \mathbf{Z}\ \exists x \in \mathbf{Z}\ (Q(y, z) \wedge \neg\neg P(x, y))) \equiv$$
$$\equiv (\exists y \in \mathbf{Z}\ (Q(x, z) \wedge \neg P(x, y))) \vee (\forall z \in \mathbf{Z}\ \exists x \in \mathbf{Z}\ (Q(y, z) \wedge P(x, y))).$$

Here we also use the Boolean equivalence $\neg(A \to B) \equiv (A \wedge \neg B)$. □

5. Simplify the expression with negation so that negation is only applied to individual predicates or propositional variables (rather than larger subexpressions or quantifiers):

Inadvertently left without an expression. We skiped this exercise. □

6. Use the set-builder notation to describe the set of all positive odd integers n such that for every prime p dividing n, the number p^2 also divides n. Here is an (incomplete) list of the numbers in this set:

$$S = \{1, 9, 25, 27, 49, 81, 121, 125, 169, 225, 243, \ldots\}.$$

In the set-builder notation you can use $\mathbf{Z}^+$ (all positive integers), arithmetic operations, Boolean operations, quantifiers, and these two predicates:

Prime(x) is true iff x is a prime.

$(a \mid b)$ is true iff a divides b.

The proposition that "the number n is odd" translates as $\neg(2 \mid n)$, i.e. number 2 does not divide n.

The proposition that "the number n is divisible by a prime p" translates as $(p \mid n)$.

The proposition that "the number n is divisible by a prime square p^2" translates as $(p^2 \mid n)$.

We could combine the last two propositions like this:

$$\forall p \in \text{Primes}\ ((p \mid n) \to (p^2 \mid n)).$$

Unfortunately, we do not have the set Primes (but only the set $\mathbf{Z}^+$ of all positive integers. But we do have the predicate that always tells, if a number is prime or not. We can add this condition Prime(p) in front (to express the fact that $p^2 \mid n$ should be true only for primes dividing n.

The final expression looks like this:

$$S = \{n \in \mathbf{Z}^+ \mid \neg(2 \mid n) \wedge \forall p \in \mathbf{Z}^+(\text{Prime}(p) \to (p \mid n) \to (p^2 \mid n))\}.$$

Note. One can rewrite the last implication (using the fact that $\to$ is right-associative). So, these are also valid answers (they are all logically equivalent ways to write the same thing).

$$S = \{n \in \mathbf{Z}^+ \mid \neg(2 \mid n) \wedge \forall p \in \mathbf{Z}^+(\text{Prime}(p) \to ((p \mid n) \to (p^2 \mid n)))\}.$$

$$S = \{n \in \mathbf{Z}^+ \mid \neg(2 \mid n) \wedge \forall p \in \mathbf{Z}^+((\text{Prime}(p) \wedge (p \mid n)) \to (p^2 \mid n))\}.$$

Any other answers are fine too as long as they describe the same set.

Set of all numbers (even and odd) with this property is also known as *Powerful numbers* - `https://bit.ly/3sEefft`, but one does not need to know anything about them (just translate their definition into set-builder notation). □

7. Prove or disprove by a counterexample the following two statements:

   (a) Statement$_1$: "Function $f\colon \mathbf{R} \to \mathbf{R}$ given by $f(x) = 3x - 7$ is surjective."

   (b) Statement$_2$: "Function $f\colon \mathbf{Z} \to \mathbf{Z}$ given by $f(x) = 3x - 7$ is surjective."

(a) The function $f(x) = 3x - 7$ is surjective as a real-valued function.
Indeed, pick any real number $y \in R$. Then the equation

$$f(x) = 3x - 7 = y \text{ has this solution: } x = \frac{y+7}{3}.$$

(b) The function $f(x) = 3x - 7$ is **not** surjective as an integer function.
For example, we cannot find any integer $x \in \mathbf{Z}$ that satsifies $3x - 7 = 0$. (Number 7 is not divisible by 3.) Therefore some integer numbers such as $0 \in \mathbf{Z}$ do not have any pre-image that would map to them. □

8. Is the number $\frac{2}{1+\sqrt{5}}$ rational or irrational? Prove your answer.
(If necessary, you can use the following Lemma: For any positive integer n, the square root $\sqrt{n}$ is either itself a positive integer or it is irrational.)

We prove that $\frac{2}{1+\sqrt{5}}$ is irrational.
Proof by contradiction. Assume that this number is a rational number $p/q \in \mathbf{Q}$. In this case

$$\frac{2}{1+\sqrt{5}} = \frac{p}{q}.$$

Since $1 + \sqrt{5} \neq 0$, we can flip both fractions:

$$\begin{aligned} \frac{1+\sqrt{5}}{2} &= \frac{q}{p}, \\ 1 + \sqrt{5} &= \frac{2q}{p}, \\ \sqrt{5} &= \frac{2q}{p} - 1 = \frac{2q-p}{p}. \end{aligned}$$

We have expressed $\sqrt{5}$ as a rational number $(2q - p)/p$. This is a contradiction. (We can either prove directly that $\sqrt{5}$ is irrational; or we can use Lemma, since $\sqrt{5}$ is clearly not an integer (since $2^2 = 4 < 5$, but $3^2 = 9 > 5$, so $\sqrt{5} \in (2; 3)$, so it cannot be an integer (and by Lemma it must be irrational). □

9. Consider set S defined by this set-builder expression:

$$S = \left\{ x \in \mathbf{Z}^+ \mid x \leqslant 80 \wedge \exists m \in \mathbf{Z}^+ \ \left(x = m^2\right) \right\}.$$

   (a) List the elements of the set S.
   (b) Find the size of its power set $|\mathcal{P}(S)|$.

(a) If we translate the set-builder notation back to human language, the set S consists of all positive full squares less or equal than 80. Let us list all these numbers:

$$S = \{1, 4, 9, 16, 25, 36, 49, 64\}.$$

(b) The powerset $\mathcal{P}(S)$ contains exactly $2^{|S|} = 2^8 = 256$ elements.
Any finite set S has exactly $2^{|S|}$ subsets, since we can make exactly $n = |S|$ choices when deciding, if some element $s_i \in S$ belongs or does not belong to some subset A. We can make these choices in 2^n ways. □

10. Let $f\colon \mathbf{N} \to \mathbf{N}$ be defined by $f(n) = \sum_{j=1}^{n} j(j+1)$.

    (a) Find the smallest k such that $f(n)$ is in $O(n^k)$.

    (b) Find C, n_0 so that $|f(n)|$ does not exceed $C \cdot |n^k|$ for all $n \geqslant n_0$.

(a) The smallest value k is $k = 3$. We can compute this sum:

$$\sum_{j=1}^{n} j(j+1) = (1^2 + 2^2 + \ldots + n^2) + (1 + 2 + \ldots + n) =$$

$$= \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} = \frac{n^3 + 3n^2 + n}{6} + \frac{n^2 + n}{2} = \frac{1}{3}n^3 + n^2 + \frac{2}{3}n.$$

This is a polynomial of degree 3, since it contains $\frac{1}{3}n^3$. Every polynomial grows as fast as its highest-order term which is n^3.

(b) We can pick $C = 2$, $n_0 = 1$. In this case for each $n \geq 1$ we have

$$\left|\frac{1}{3}n^3 + n^2 + \frac{2}{3}n\right| \leq \left|\frac{1}{3}n^3 + n^3 + \frac{2}{3}n^3\right| = 2\left|n^3\right|.$$

In this inequality we use the fact that $n^2 \leq n^3$ and $n \leq n^3$ whenever $n \geq n_0 = 1$.

Note. We can make a conclusion that the function f is in $O(n^3)$ (and this result can be shown by the definition and cannot be improved; i.e. we cannot replace this by $O(n^k)$ for any $k < 3$, since f contains a cubic term. □

11. (a) Use Euclidean algorithm to find $\gcd(426, 156)$ (*the greatest common divisor*).

    (b) Use the GCD found in the previous step to compute $\mathrm{lcm}(426, 156)$ (*the least common multiple*).

(a) We divide 426 by 156 to get remainder 114. Then divide 156 by 114 to get remainder 42 and so on. Euclidean algorithm can be written as a chain of equalities:

$$\gcd(426, 156) = \gcd(156, 114) = \gcd(114, 42) = \gcd(42, 30) =$$

$$= \gcd(30, 12) = \gcd(12, 6) = \gcd(6, 0) = 6.$$

(b) The LCM (least common multiplier) for any two numbers a, b satisfies this identity: $\gcd a, b \cdot \mathrm{lcm}(a, b) = a \cdot b$. Therefore we can express

$$\mathrm{lcm}(426, 156) = \frac{426 \cdot 156}{\gcd(426, 156)} = \frac{426 \cdot 156}{6} = 426 \cdot 26 = 11076.$$

□

12. Consider the system of congruences

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

(a) Find one solution to this system of congruences.

(b) Describe all the solutions to this system.

(b) First we do part **(b)** to get all the solutions, then take a specific one for part **(a)**. Since 5,7,9 are all coprime, we apply the Chinese Remainder Theorem, which guarantees the existence of a solution. First use Bezout's identity on three pairs of numbers:

$$\begin{array}{lllll} 5 \text{ and } 7\cdot 9 & \Longrightarrow & \exists\, a_1, b_1 \text{ with } 5a_1 + 63b_1 = 1 & \Longrightarrow & 63b_1 \equiv 1 \pmod 5 \\ 7 \text{ and } 5\cdot 9 & \Longrightarrow & \exists\, a_2, b_2 \text{ with } 7a_2 + 45b_2 = 1 & \Longrightarrow & 45b_2 \equiv 1 \pmod 7 \\ 9 \text{ and } 5\cdot 7 & \Longrightarrow & \exists\, a_3, b_3 \text{ with } 9a_3 + 35b_3 = 1 & \Longrightarrow & 35b_3 \equiv 1 \pmod 9 \end{array}$$

By trial and error (checking 5 values for b_1, 7 values for b_2, 9 values for b_3), we find:

$$b_1 \equiv 2 \pmod 5, \qquad b_2 \equiv 5 \pmod 7, \qquad b_3 \equiv 8 \pmod 9.$$

The Chinese Remainder Theorem tells us that a solution to the given system is

$$\begin{aligned} & 1\cdot 63\cdot 2 + 2\cdot 45\cdot 5 + 3\cdot 35\cdot 8 \pmod{5\cdot 7\cdot 9} \\ &= 126 + 450 + 840 \pmod{315} \\ &= 1416 \pmod{315}. \end{aligned}$$

We are technically done, as all solutions to this system may be expressed as $1416 + 315k$ for any $k \in \mathbf{Z}$. Since $1416 > 315$, we can simplify the first term as $1416 \equiv 156 \pmod{315}$, to get that all solution are of the form $156 + 315k$, for any $k \in \mathbf{Z}$.

(a) One solution is for $k = 0$, so $x = 156$.

□

13. Consider the two numbers in binary notation

$$\begin{aligned} \alpha &= 111001110_2, \\ \beta &= 1110_2. \end{aligned}$$

(a) Express β as a sum of powers of 2.

(b) Show how to multiply the two binary numbers α and β on paper (similar to the "school algorithm". It would look like this – with 0s and 1s instead of asterisks:

```
 111001110
 ×    1110
 ---------
 *********
*********
...   ...
```

(a) We can express by the definition of binary notation for positive integer numbers:

$$\beta = \mathtt{1110}_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 8 + 4 + 2 = 14.$$

(b) We complete the numeric multiplication. Filling in the digits is straightforward (since multiplication by digits 0 and 1 is easy; we just need to remember to shift them accordingly). The only unusual part is adding together the digits position-by-position (as there may be large carries to the next binary position). □

```
    111001110
    ×    1110
    ---------
    000000000
   111001110
  111001110
 111001110
-------------
1100101000100
```

14. Express the periodic decimal fraction $3.378378378\ldots = 3.(378)$ as an irreducible rational number $\frac{p}{q}$. Show the formulas (infinite geometric progression or some other arithmetic manipulation) that can be used to get your answer.

First we note that

$$0.(378) = \frac{378}{1000} + \frac{378}{1000 \cdot 1000} + \cdots = \sum_{n=0}^{\infty} \frac{378}{1000} \cdot \left(\frac{1}{1000}\right)^n.$$

Recall that the sum of a geometric series is

$$\sum_{n=1}^{\infty} ar^n = \frac{a}{1-r},$$

whenever $|r| < 1$. Hence in this case

$$3.(378) = 3 + \sum_{n=0}^{\infty} \frac{378}{1000} \cdot \left(\frac{1}{1000}\right)^n = 3 + \frac{378/1000}{1 - 1/1000} = 3 + \frac{378}{999} = \frac{3 \cdot 999 + 378}{999}.$$

This answer may be simplified to $\frac{125}{37}$, but the expression above is an acceptable answer, in the absence of caclulcators. □

15. Prove by mathematical induction that for all $n \in \mathbf{Z}^+$ the following equality holds:

$$\sum_{j=1}^{n} \left(\frac{1}{2j-1} - \frac{1}{2j+1}\right) = \frac{2n}{2n+1}.$$

Statement: Let $P(n)$ be the statement "$\sum_{j=1}^{n}\left(\frac{1}{2j-1}-\frac{1}{2j+1}\right)=\frac{2n}{2n+1}$".

Base case: When $n=1$, we have

$$\sum_{j=1}^{1}\left(\frac{1}{2j-1}-\frac{1}{2j+1}\right)=\frac{1}{2-1}-\frac{1}{2+1}=1-\frac{1}{3}=\frac{2}{3},$$

and

$$\frac{2n}{2n+1}=\frac{2}{2+1}=\frac{2}{3}.$$

Hence $P(1)$ holds.

Inductive hypothesis: Suppose that $P(n)$ holds for some $n \geqslant 1$.

Inductive step: Applying the inductive hypothesis in the second line below, the sum for $P(n+1)$ is

$$\begin{aligned}
\sum_{j=1}^{n+1}\left(\frac{1}{2j-1}-\frac{1}{2j+1}\right) &= \left(\sum_{j=1}^{n}\left(\frac{1}{2j-1}-\frac{1}{2j+1}\right)\right)+\left(\frac{1}{2(n+1)-1}-\frac{1}{2(n+1)+1}\right) \\
&= \frac{2n}{2n+1}+\frac{1}{2n+1}-\frac{1}{2n+3} \\
&= \frac{2n(2n+3)+(2n+3)-(2n+1)}{(2n+1)(2n+3)} \\
&= \frac{4n^2+6n+2n+3-2n-1}{(2n+1)(2n+3)} \\
&= \frac{4n^2+6n+2}{(2n+1)(2n+3)} \\
&= \frac{(2n+1)(2n+2)}{(2n+1)(2n+3)} \\
&= \frac{2(n+1)}{2(n+1)+1}.
\end{aligned}$$

Hence $P(n+1)$ holds.

Conclusion: By the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbf{N}$. $\square$