Math 189 section 3 Fall 2021 Take-Home Exam: ERROR CORRECTED 12/10/2023 and DUE DATE EXTENDED

Dr Holmes

December 10, 2021

This paper contains the cumulative part of the final exam and a couple of questions from Test III. The rest of Test III (the grade on which is also part of the final examination grade) will be given in class in the final exam period, Monday Dec 13 12-2 pm. This exam is due at the end of the final examination period for the university: I will accept it electronically up to 11:55 pm on Thursday of finals week.

You are required to do this examination on your own, using course materials and tools, and not consulting any other person but the instructor. Please show calculations that are requested, and if you use some computer support to solve a problem, describe it and if possible attach printouts.

1. Verify that $((P \to Q) \vee (P \to R)) \to (P \to (Q \vee R))$ is a theorem of propositional logic by giving a truth table verifying that it is a tautology.

   If you did the original version, that is perfectly acceptable (I had the converse of this statement originally, which is fine for this truth table problem but does not match the hint in problem 2).

2. Verify that $((P \to Q) \vee (P \to R)) \to (P \to (Q \vee R))$ is a theorem of propositional logic by giving a proof following the manual of style. The method of proof by cases is suggested.

   This is where the error was: I had the converse of this implication (I wrote it backward) and the converse is true but considerably harder to prove, and proof by cases is not a good approach.

3. Verify that $((Q \vee \neg P) \wedge (R \vee \neg Q)) \rightarrow (P \rightarrow R)$ is a theorem of propositional logic, giving a proof following the style manual. The rule of disjunctive syllogism might be useful.

4. Prove that the square of an odd integer is odd.

5. Let a and b be integers. Let x and y be integers. Prove that if $d|a$ and $d|b$, then $d|(ax + by)$.

   In the language of a later section, any linear combination of two integers divisible by d, with integer coefficients, is itself divisible by d.

6. Rewrite the following negations of quantified sentences into forms in which negations are moved to the right as far as possible.

   (a) $\neg(\forall x \in A : P(x) \to Q(x))$

   (b) $\neg(\forall x \in \mathbb{N} : (\exists y \in \mathbb{N} : y < x))$

7. Contrast membership and subset: indicate for each part whether the membership relation $\in$, the subset relation $\subseteq$, both or neither make the indicated statements true if they replace the underlined blank.

   (a) $\{3\} \_\_\_ \mathbb{N}$

   (b) $\{1, 3\} \_\_\_ \{1, 2, 3, \{1, 3\}\}$

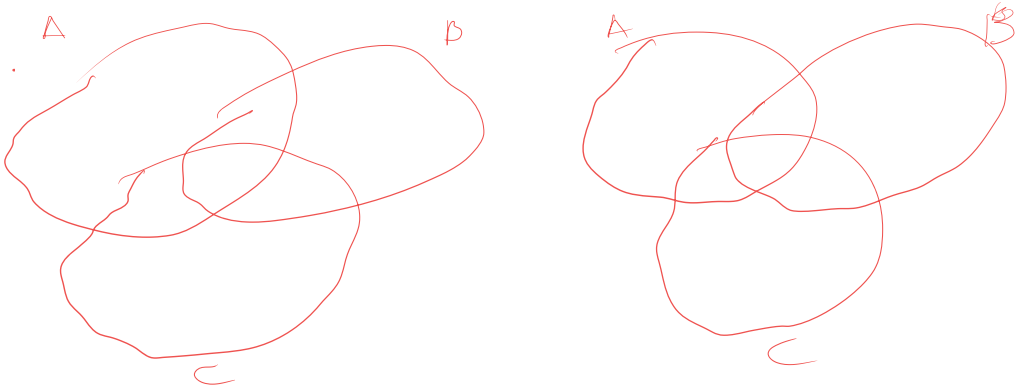
   (c) $1 \_\_\_ \{\{1, 2\}\}$

   (d) $\frac{1}{2} \_\_\_ \{1, \frac{1}{2}, \frac{3}{4}\}$

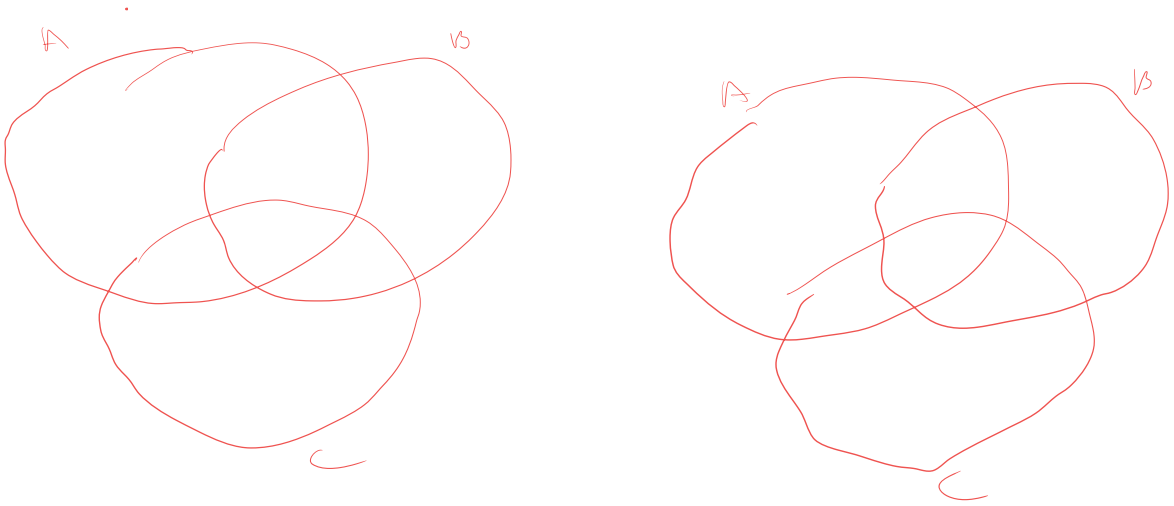
8. Venn diagram proof and counterexample

   One of the following statements is a theorem of Boolean algebra. One is not. Give a Venn diagram illustration (with appropriate use of shadings with explanatory keys) of the one that is true, and give an explicit counterexample with calculations to show that the other is false.

   (a) $A - (B \cap C) = (A - B) \cup (A - C)$

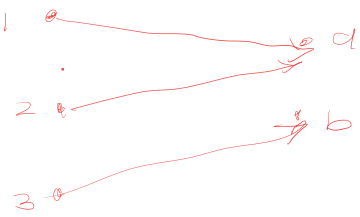


(b) $(A \cap B) - C = (A - B) \cup (A - C)$

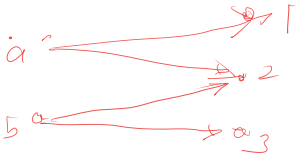


9. A number of finite diagrams of relations are given. For each diagram, indicate whether it is a diagram of a function or not, and if not why not (with reference to specific values). If it is a diagram of a function, indicate whether it is a one-to-one function or not (and if not, why not, with reference to specific values). If it is a diagram of a one-to-one function, draw a diagram of its inverse and indicate what its domain and target are.

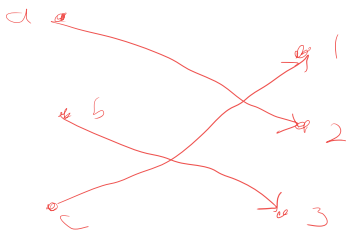
   (a) :



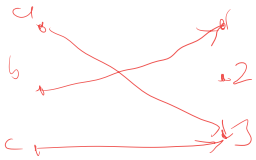
   (b) :



(c) :



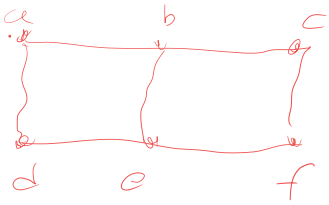
(d) :



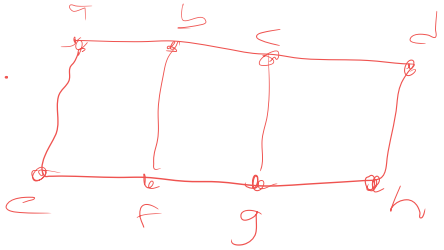
10. An Eulerian walk in an undirected graph is a graph which visits each vertex in the graph and traverses each edge in the graph exactly once.

    One of the two graphs pictured has an Eulerian walk and one does not. For the one which does, give this walk as an ordered list of vertices (arrows on the diagram absolutely do not give enough information); for the one which does not, describe features of the graph which make it clear that it cannot have an Eulerian walk.

    (a)



(b)



11. (Test 3: proof by induction) Define $a_0 = 6; a_1 = 13; a_{n+2} = 5a_{n+1} - 6a_n$

    Compute the terms of this sequence up to a_6.

    Prove by strong induction that for each non-negative integer n, $a_n = (5)(2^n) + 3^n$

12. (Test 3) RSA example which you may work using the spreadsheets: please print out or transcribe displays from the spreadsheets (or if you used a different method to do the calculations, give similar evidence of your work).

    Your public key is

    $N = 28907$

    $r = 11$

    A friend sends you the important message 42 (the answer to the question of the meaning of life the universe and everything): he encrypts 42 using your key and sends it to you:

    (a) what number do you receive?

    (b) Your closely guarded secret is that N is the product of the primes 137 and 211.

    Verify that 11 satisfies the required condition to be your encryption exponent.

    (c) Compute your decryption exponent.

    (d) Verify that decryption of the message sent to you gives the expected value 42.