Name: David Crow

CSCE 531 Discrete Mathematics Fall 2018 Exam 1

Put your name on every page.

Your work must be your own.

The only permitted resources are:

- your personal notes,
- the course textbook, and
- the materials posted on the course Canvas site or linked directly from that site.

In particular,

- you may not use any other books or websites, and
- with the exception of the instructor, you may not communicate with another person in any way.

Tips:

- Read all questions prior to answering any, and budget your time accordingly.
- Leaving a question unanswered will result in zero points for that question.

Name: David Crow

Multiple Choice – 3 points each

For each of the following, choose the **BEST** answer.

1. Given the statement $\forall x(x^2 + x - 2 \neq 0)$, where the domain consists of the **NONNEGATIVE** integers, which **ONE** of the following is **TRUE**?
   a. $x = -2$ is the only counterexample.
   b. $x = 1$ is the only counterexample.
   c. Both $x = -2$ and $x = 1$ are counterexamples.
   d. None of the above.

2. Which **ONE** of the following statements is **FALSE** if the domain of each variable consists of all **REAL** numbers?
   a. $\forall x \forall y \exists z(x = y + z)$
   b. $\forall x \exists y \exists z(x = y + z)$
   c. $\exists x \forall y \exists z(x = y + z)$
   d. $\exists x \exists y \forall z(x = y + z)$

3. Which **ONE** of the rules of inference below is used in the following argument? "The Doctor is a Time Lord. If The Doctor is a Time Lord, then she can regenerate. Therefore, The Doctor can regenerate."
   a. Hypothetical syllogism
   b. Modus ponens
   c. Modus tollens
   d. None of the above.

p
$p \to q$
$\therefore q$

4. For which **ONE** of the theorems below is the following proof a valid argument?
   Proof: Assume the premise of the theorem holds. Then $i = 2m$ for some $m \in \mathbb{Z}$. Now assume that $i + j$ is odd. Then $i + j = 2k + 1$ for some $k \in \mathbb{Z}$, so
   $$\begin{aligned} j &= j + (i - i) \\ &= (i + j) - i \\ &= (2k + 1) - 2m \\ &= 2(k - m) + 1, \end{aligned}$$
   which contradicts the premise.
   a. Premise: i is even and j is even. Conclusion: $i + j$ is even.
   b. Premise: i is even and j is odd. Conclusion: $i + j$ is odd.
   c. Premise: i is odd and j is even. Conclusion: $i + j$ is odd.
   d. Premise: i is odd and j is odd. Conclusion: $i + j$ is even.
   e. None of the above.

i is even
$i+j$ is odd
$\therefore j$ is odd

5. Which **ONE** of the following is a valid definition of a function with the domain $\mathbb{N}$ and the range $\mathbb{Z}^+$?
   a. f assigns to each integer k the value of k mod 10.
   b. f assigns to each integer k the value of $k + 1$.
   c. f assigns to each nonnegative integer k the value of k mod 10.
   d. f assigns to each nonnegative integer k the value of $k + 1$.

Name: David Crow

6. Suppose $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is defined by $f(m,n) = m^2 - n$. Which **ONE** of the following is **TRUE**?
   a. $f(m,n)$ is both one-to-one and onto. $f(2,2) = 2$
   b. $f(m,n)$ is neither one-to-one nor onto. $f(-2,2) = 2$ not one-to-one
   c. $f(m,n)$ is not one-to-one but it is onto.
   d. $f(m,n)$ is one-to-one but not onto.

7. Which **ONE** of the following is countably infinite?
   a. The set of blog posts that could be generated by an immortal monkey with an indestructible keyboard.
   b. The set of passwords that include at least one upper case letter, at least one lower case letter, at least one digit, and at least one special character, as well as having lengths of at least 8 and no more than 30.
   c. The set of real numbers between zero and $10^{-10^{100}}$.
   d. The set of people who won the lottery without playing.

8. Consider the set F of functions mapping bit strings to Boolean values. Which **ONE** of the following is **TRUE**?
   a. F is countably infinite
   b. F is empty
   c. F is finite
   d. F is uncountably infinite

9. Let $\mathbb{X} = \mathbb{R} - \mathbb{Z}$. Which **ONE** of the following is **TRUE**?
   a. $\mathbb{Q} \subseteq \mathbb{X}$. $\frac{1}{1} \in \mathbb{Q}$, $\frac{1}{1} \notin X$
   b. $\mathbb{X}$ is countably infinite. uncountable
   c. $\mathbb{X}$ is finite.
   d. None of the above

10. Consider the cardinality of sets A, B, and C. If $(|A| \le |B|) \wedge (|B| \le |C|) \wedge (|C| \le |A|)$, which **ONE** of the following is **TRUE**?
    a. There cannot exist three sets that have these cardinality relationships.
    b. There exists a one-to-one function from A to B.
    c. All three sets are countable.
    d. None of the above

11. Suppose set F is finite, set C is countably infinite, and set U is uncountably infinite. Which **ONE** of the following statements is **ALWAYS TRUE**?
    ~~a.~~ There exists a one-to-one correspondence between U and $\mathbb{Z}^+$.
    b. There exists a one-to-one correspondence between $C \cap U$ and $\mathbb{Z}^+$.
    c. There exists a one-to-one correspondence between $(C \cup F) - (C \cap F)$ and $\mathbb{Z}^+$.
    d. None of the above statements is always true.

12. Consider two countably infinite sets, J and K. Which **ONE** of the following is **FALSE**?
    a. There exists a function that maps J to $\mathbb{Z}^+$.
    b. The exists a one-to-one correspondence between J and K.
    c. Every function that maps J to K is invertible.
    d. None of the above

Name: David Crow

Short answer – Various point values

Present your work clearly and in an organized manner. If you need to do scratch work, do it elsewhere.

13. [6 pts] Refer to the rules of the island of knights and knaves described in Example 7 in Section 1.2. Suppose that you meet Anita, Boris, and Carmen. Anita says "I am a knave and Boris is a knight." Boris says "Exactly one of us is a knave." Determine whether each of the three people is a knight or a knave.

All 6 rows eliminated by Anita; Boris's statement doesn't give new info

A	B	C
~~0~~	~~0~~	~~0~~
~~0~~	~~0~~	~~1~~
~~0~~	~~1~~	~~0~~
~~0~~	~~1~~	~~1~~
~~1~~	~~0~~	~~0~~
~~1~~	~~0~~	~~1~~
1	1	0
1	1	1

0 is knight
1 is knave

Anita is a knave.

Boris is a knave.

We can not determine whether Carmen is a knight or a knave.

The information we've been given is not sufficient to decide whether or not Carmen is a knight.

14. [10 pts] Prove the following theorem: if n is a perfect square, then $n+2$ is not a perfect square.
Hint: $i^2 - j^2 = (i+j)(i-j)$.

$n = k * k = k^2$ $\quad (k+1)^2 - k^2 = (k+1+k)((k+1)-k)$

$= (2k+1)(1)$

$= 2k+1$

That is, the difference between consecutive perfect squares is $2k+1$. In other words, the next perfect square after n is $n + (2k+1)$. Because $k \in \mathbb{Z}$, $2 \neq 2k+1$ for any k, and so $n+2$ can't be a perfect square.

15. [10 pts] Explain the error in the following "proof":
"Theorem": In any set of $n \in \mathbb{Z}^+$ coffee mugs, all the mugs are the same size.
"Proof": Let $P(n)$ be the proposition that "in any set of n coffee mugs, all the mugs are the same size." Then $P(1)$ holds trivially. Now adopt the inductive hypothesis $P(k)$ for some $k \in \mathbb{Z}^+$, i.e. for any set of k coffee mugs, all the mugs have the same size. Next, let $C = \{m_0, m_1, m_2, \ldots, m_{k-1}, m_k\}$ be a set of $k+1$ coffee mugs. Also, define $C_0 = \{m_0, m_1, \ldots, m_{k-1}\}$ and $C_k = \{m_1, m_2, \ldots, m_{k-1}, m_k\}$, each of which is by construction a set of k coffee mugs. Thus, according to the inductive hypothesis, all the mugs in C_0 must have the same size, and similarly for C_k. Now choose any mug $m_i \in C_0 \cap C_k = \{m_1, m_2, \ldots, m_{k-1}\}$. Then, because all the mugs in C_0 have the same size, so do m_0 and m_i, and because all the mugs in C_k have the same size, so do m_i and m_k. By transitivity, m_0 and m_k have the same size, and therefore so do all the mugs in C. We have shown that $P(k) \to P(k+1)$, which completes the proof by induction. ∎

The base case doesn't span a large enough range.
Let $k=2$. Here, $C = \{m_0, m_1\}$, $C_0 = \{m_0\}$, and $C_k = \{m_1\}$. It's obvious that $C_0 \cap C_k = \emptyset$.
We thus can't find an $m_i \in C_0 \cap C_k$ to show that $P(k+1) = P(3)$ is true.

Because induction gets us to the next step,
we can't get to 3 → we can't get to 4 → " " to 5 → ...
We'd need to also prove $P(2)$ to make this a valid proof.

Name: David Crow

16 [10 pts] Suppose that a restaurant offers gift certificates in denominations of \$5 and \$8. Use strong induction to prove that any integer value greater than \$32 can be formed.

Proof:

Base case:

$P(32): 4*8 + 0*5 = 32$

$P(33): 1*8 + 5*5 = 33$

$P(34): 3*8 + 2*10 = 34$

$P(35): 0*8 + 7*5 = 35$

$P(36): 2*8 + 4*5 = 36$

Inductive hypothesis:

Assume that, for all n such that $36 \le n \le k$, $P(n)$ holds.

Inductive step:

We know $k+1 = (k-4)+5$ and, if $k \ge 36$, then $k-4 \ge 32$.

Since $k-4 \ge 32$, by the inductive hypothesis $P(k-4)$ is true.

Because we can always add one \$5 gift certificate,

we can reach $k+1$ dollars in value; in other words,

we can always reach a value of at least \$32.

By the principle of mathematical (strong) induction,

the theorem is proved

17 [10 pts] Show how to use Fermat's Little Theorem and the Chinese Remainder Theorem to calculate $7^{3208} \bmod 2431 = 152$.

$11*13*17 = 2431$

FLT: $a^p \equiv a \pmod p$, $a^{p-1} \equiv 1 \pmod p$

Compute $7^{3208} \bmod 11$, $7^{3208} \bmod 13$, $7^{3208} \bmod 17$

$7^{3208} \bmod 11 = (7^{10})^{320} \cdot 7^8 \bmod 11 = 1^{320} \cdot 7^8 \bmod 11$

$= 7^8 \bmod 11 = ((((((7 \cdot 7 \bmod 11) \cdot 7 \bmod 11) \cdot 7 \bmod 11) \cdot 7 \bmod 11) \cdot 7 \bmod 11) \cdot 7 \bmod 11) \cdot 7 \bmod 11$

$= 9$

$7^{3208} \bmod 13 = (7^{12})^{267} \cdot 7^4 \bmod 13 = 1^{267} \cdot 7^4 \bmod 13 = 7^4 \bmod 13$

$= ((7 \cdot 7 \bmod 13) \cdot 7 \bmod 13) \cdot 7 \bmod 13 = 9$

$7^{3208} \bmod 17 = (7^{16})^{200} \cdot 7^8 \bmod 17 = 1^{200} \cdot 7^8 \bmod 17 = 7^8 \bmod 17$

$= ((((((7 \cdot 7 \bmod 17) \cdot 7 \bmod 17) \cdot 7 \bmod 17) \cdot 7 \bmod 17) \cdot 7 \bmod 17) \cdot 7 \bmod 17) \cdot 7 \bmod 17$

$= 16$

$x = 7^{3208} \equiv 9 \bmod 11 \equiv 9 \bmod 13 \equiv 16 \bmod 17$

$9 \bmod 11 \equiv 1 \cdot 9 \bmod 11$

$9 \bmod 13 \equiv 5 \cdot 7 \bmod 13$

$16 \bmod 17 \equiv 7 \cdot 12 \bmod 17$

$x = 13 \cdot 17 \cdot 9 + 11 \cdot 17 \cdot 7 + 11 \cdot 13 \cdot 12 \bmod 2431$

$\equiv 1989 + 1309 + 1716 \bmod 2431$

$\equiv 5014 \bmod 2431$

$\equiv 152 \bmod 2431$

$\therefore 7^{3208} \bmod 2431 = 152$

Name: David Crow

18. [10 pts] Consider a collection of m distinguishable n-sided dice where $n > m$. Assuming that m and n are both even, express the number of ways to roll the following.

a. Even numbers on all the dice.

$$\left(\frac{n}{2}\right)^m$$

b. An even number on exactly one die and odd numbers on the remaining dice.

$$\left(\frac{n}{2}\right)\left(\frac{n}{2}\right)^{m-1} = \left(\frac{n}{2}\right)^m$$

c. An even number on at least one die.

ways to roll all odds = $\left(\frac{n}{2}\right)^m$

$$n^m - \left(\frac{n}{2}\right)^m$$

d. Even numbers on exactly half the dice.

$$\left(\frac{n}{2}\right)^{m/2}\left(\frac{n}{2}\right)^{m/2} = \left(\frac{n}{2}\right)^m$$

e. Distinct values on all the dice.

$$n(n-1)(n-2)\cdots(2)(1) = n!$$

19. [4 pts] Let A and B be finite sets.

a. How many distinct functions from A to B exist?

Each of $|A|$ elements can map to each of $|B|$ elements

All are unique

$\therefore |B|^{|A|}$

b. How many of those functions are one-to-one?

$(|B|)(|B|-1)(|B|-2)\ldots(|B|-|A|+1)$

0 if $|B| < |A|$; otherwise, $\dfrac{|B|!}{|B|-|A|!}$

20. [2 pts] At the end of Beggar's Night (a.k.a. Halloween) a boy makes his little sister an offer. He tells her that he has a total of n candy items, each of which is either a pack of gum, a lollipop, a chocolate bar, or a piece of taffy. If she can guess correctly how many of each type of item he has, he will give it all to her and do her chores for a year. Otherwise, she has to give him an item from her bag. How many possibilities does she have to choose from?

partition n into 4 nonempty subsets

n is indistinguishable, 4 is distinguishable $\rightarrow$ $C(n+r-1, r-1)$

$\therefore \binom{n+3}{3}$

21. [2 pts] What is the term involving x^2 in $(3x + 2y)^9$?

doesn't say coefficient of...

binomial theorem gives $\binom{9}{2}(3x)^2(2y)^{9-2}$

$= \binom{9}{2}(3^2)(2^7)x^2y^7$

(still, the coefficient of the term involving x^2 is $\binom{9}{2}(3^2)(2^7)$)