CSE 15: Discrete Mathematics
Final Examination

Fall 2017

Name: Pedro Damian Sanchez Jr Lab Section: _____

Left Neighbor: N/A Right Neighbor: N/A

Instructions

- This is a closed book exam.
- There is a total of 140 points.
- There are 15 pages. including this page.
- You have 3 hours to complete this exam.
- A list of logical equivalences and inference rules can be found starting on page 14.
- If you are unsure about anything, please ask.

Section	Points Available	Points Earned
Logic and Set Theory	20	17
Complexity and Proofs	30	20
Counting Principles	25	13
Number Theory and Cryptography	65	51
TOTAL	**140**	101

1 Logic and Set Theory — 20 points

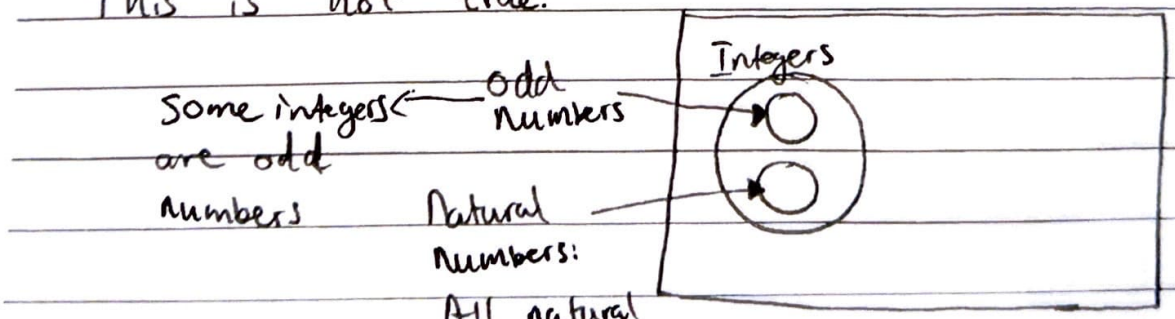
1. Use a truth table to verify the validity of *resolution*. *[8 points]*

p	q	r	$(p \vee q)$	$(\neg p \vee r)$	$(q \vee r)$	$[(p \vee q) \wedge (\neg p \vee r)]$	$\rightarrow (q \vee r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	T	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	F	T	T	F	T
F	F	F	F	T	F	F	T

2. Given the following premise: All natural numbers are integers, and Some integers are odd numbers, can we then conclude that Some natural numbers are odd numbers? Explain your answer. Points will be awarded for the explanation, not for guessing "Yes" or "No". *[4 points]*

Yes, if all natural numbers are defined as $\forall R \geq 1$, then it must follow that if, the $\forall \mathbb{Z} \geq 1$ every other number will be odd; therefore to say some natural numbers are odd is correct.

This is not true.



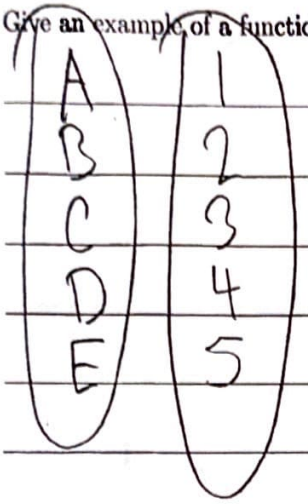
Nobody says odd numbers and natural numbers intersect.

~~Nobody said odd numbers and integers~~

3. Let $A = \{a, b, c\}$. and $B = \{x, y, x\}$. Compute $B \times A$. [6 points]

{xa, xb, xc, ya, yb, yc} 6

4. Give an example of a function that is not one-to-one, and also not onto. [2 points] 2



Note: No correlation occurs for any input given.

2 Complexity and Proofs — 30 points

1. Use a direct proof to show that the sum of an even integer and an odd integer is odd? *[4 points]*

Let $a=(2n)$ and $b=(2k+1)$ 4

$a+b = 2n+2k+1$

$= 2(n+k)+1$ ✓

2. Use a proof by contradiction to show that the sum of a rational number and an irrational number is irrational. *[6 points]*

Assume that the sum of a rational number and an irrational is rational

Let $a=\frac{p}{q}$ and $b=\pi$ in proofs, you can not set constant values,

$a+b=\frac{p}{q}+\pi$ by definition π is irrational.

No matter what p and q are, if add to π the result will always be irrational, and not rational.

what if I choose some other irrational number other than π?

3. Explain how do we go about establishing the truth of a statement by using mathematical induction? Describe the steps of the inductive process and explain why each one is necessary. *[5 points]*

1.) Base Case is establish where P(1) holds. 5

2.) State an Inductive Hypothesis where P(k+1) is assumed.

3.) Proceed to the Inductive Step to determine if P(k+1) holds.

4.) If all cases hold, the Inductive Hypothesis becomes a Mathematical Theorem.

4. Use a proof by mathematical induction to show that the following holds true: *[10 points]*

$$1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4}n^2(n+1)^2$$

5

Base Case when $n=2$:

$\frac{1}{4}(2)^2((2)+1)^2 = 9$; $1^3+2^3 = 9$; ~~P(2)~~ holds!

Induction, Let $K=n+1$:

Assume $1^3+2^3+3^3+\cdots+K^3 = \frac{1}{4}K^2(K+1)^2$

$\Rightarrow 1^3+2^3+3^3+\cdots+(n+1)^3 = \frac{1}{4}\cancel{(n+1)^2}((n+1)+1)^2$

Let ~~$n=2$~~: $1^3+2^3+3^3 = \frac{1}{4}(3)^2((3)+1)^2 = 36$;

$\therefore$ LHS = RHS, $\forall n \geq 0$;

You have to show that LHS equals that. You have just assumed it.

Base case and I.H are correct

5. What is the best case for insertion sort? Provide a sample input that will force the algorithm to behave it its best case. *[2 points]* 2

In the best case, Insertion Sort operates in O(1) when the item being searched is a the front of the list.

Find 7:

7	3	5	9	4	2	8	6

Right Here! Otherwise, the list must be mostly sorted to operate in O(n).

6. Prove that the complexity function $f(n) = 5n + 7$ belongs to $O(n^2)$.* *[3 points]*

$5n^2 + 7n^2 \geq 5n+7$ 3

$\Rightarrow 12n^2 \geq 5n+7, \quad \forall n \geq 1;$

#5 cont... Fuck it, why not create an algorithm that does find a sorted list, with the object being searched always in the front that give us operations in O(0);

Do not write stuff like that in future. You can get 0 for the whole exam because of this.

*There is no typo in this question.

3 Counting Principles — 25 points

1. A bicycle is locked with a combination lock of 3 dials, each ranging from 0 to 9. What is the maximum number of combinations I would have to attempt in order unlock the chain? [2 points] 2

|0-9|0-9|0-9| implies 10 numbers for every slot.
$10 \cdot 10 \cdot 10 = 10^3 = 1000$ possible combinations

2. Suppose the chairs in an auditorium are labelled with an uppercase English letter followed by a number not exceeding 100. What is the maximum amount of chairs that can be labelled uniquely? [4 points] 4

26 Upper Case English Letters, 100 numbers if the count begins from 1 to 100 give $26 \cdot 100 = 2600$ different ways to uniquely label seats.

3. A certain airline has 3 chicken dishes and 2 seafood dishes. How many different ways can you have dinner on that airline, if you are only allowed one dish? [4 points] 0

3 chicken dishes and 2 seafood dishes gives $3 \cdot 2 = 6$ possible meal options

$2 + 3 \neq 5$ not product rule

4. Use the basic counting principles covered in class to determine how many odd numbers there are between 1000 and 100000? [5 points] 2

100,000 − 1,000 = 99,000 numbers total. Since every other number is odd, with the last number being even, $(99{,}000 \div 2) - 1 = 49499$ odd numbers exist from 1,000 to 109000.

Correct answer is 49500. It's an example from a textbook

5. In a version of BASIC, the name of a variable is a string of 1 or 2 alphanumeric characters. An alphanumeric character is either an uppercase English letter or one of the 10 decimal digits. An additional requirement is that variable names must start with a letter. Finally, variable names can not be equal to any of the 5 two-character keywords in the BASIC language. How many different variable names are possible? *[10 points]*

5

Position one is fix with only 26 characters as an option, however, since Position 2 is optional, this leaves us with 26 combination without a second character and 26 with a number character. If the string has a decimal digit from 0 to 9 and 5 of those possibilities are ruled out, that gives

$$(26 \cdot 10) + 26 - 5 = 281;$$

That's 281 alphanumeric character combinations.

2 letter

$$26 + 26 \cdot 36 - 5$$

936

1 letter $= 26 + [redacted] - 5$

$= 26 + 731$

$= 957$

4 Number Theory and Cryptography — 65 points

1. Compute $42^{17} \bmod 143$. [12 points]

$17 \div 2 = 8$ rem 1 ^ $= 10001_2$ 10

$8 \div 2 = 4$ rem 0

$4 \div 2 = 2$ rem 0 $\Rightarrow 2^4 + 0^3 + 0^2 + 0^1 + 2^0$

$2 \div 2 = 1$ rem 0

$1 \div 2 = 0$ rem 1 $42^{2^4} \bmod 143 = ?$ what is this?

$42^{2^3} \bmod 143 = 113$

$42^{2^2} \bmod 143 = 16$

$42^{2^1} \bmod 143 = 48$

$42^{2^0} \bmod 143 = 42$

$\therefore 42^{17} \bmod 143 = 2.75360663407 \times 10^{25}$

$42^{17} \bmod 143 = 42^{2^4} \cdot 42^{2^0} \bmod 143$

$= 48$

2. What does it mean for two integers to be relatively prime? [3 points]

When two integers are relatively prime, the only factor they share in common is the number one, GCD(x, y) = 1. 3

3. Find the least positive integer that is a multiplicative inverse of 17 modulo 120. [5 points]

$17 \cdot x \equiv 1 \bmod 120$; $x = 137$ 2

Extended Euclid

4. Describe an algorithm for verifying the primality of an integer. That is, given an integer input n, your algorithm should return True if n is prime, and False otherwise. [5 points]

```
def Prime(n)
    if n factors to 1 or n:
        return True
    return False
```

check all numbers below $\sqrt{n}$ for divisibility 2

5. How much work is needed in general to find out if a number is prime? [5 points]

First check is number is odd or even, if odd continue, since the only even prime is 2. Then look for prime factors of that number, if none can be found, then it is prime

$O(\sqrt{n})$

6. Describe an algorithm for producing prime factorizations of integers. [5 points]

Use the Sieves of Erathostanes to find all primes from 2 to the integer, then test if the integer is divisible by any of those primes starting from the smallest on to the the integer. 5

7. What are the properties that an integer should have in order to force your factorization algorithm from the last question to do as much work as possible? [5 points]

The worst case is if the integer itself is prime and therefore can not be factored into smaller primes. 4

Correct answer is when n is a product of two large primes.

8. Suppose I am setting up RSA keys and I select my two prime numbers p and q, and I compute $n = pq$. How much work is required for me to compute $\varphi(n)$? [2 points]

$\varphi(n) = (p-1)(q-1)$; if you can't subtract one from two numbers and then multiply those two number together, then you have no business in math or science, so (all) 2

9. How much work would be needed to compute $\varphi(n)$ if I only know n. but not p and q? [3 points]

The larger that n is, the harder it is to factor out p and q, after a while it becomes pointless, unless you can solve for the n-th prime. 3

10. Suppose I let $p = 13$ and $q = 11$, so $n = 13 \times 11 = 143$? Suppose also that I pick my encryption exponent $e = 17$. Compute my decryption exponent d. [5 points]

Hint: Question 3 of this section will be useful.

$\varphi(n) = \varphi(143) = (p-1)(q-1) = (13-1)(11-1) = (12)(10) = 120$;

$d = \frac{(1+\varphi(n))}{e} = \frac{121}{7}$; $\varphi(n) = 120$

You got points for this. 2

now we need $ed \equiv 1 \pmod{\varphi(n)}$

$17d \equiv 1 \pmod{120}$

$d = \overline{17} \pmod{120}$

This is what Q3 asked you for

11. Now encrypt the message 42 with the public key computed in the last question. [3 points]

Hint: Question 1 of this section will be useful.

$C = M^e \bmod(n) \Rightarrow C = (42)^{(17)} \bmod(143)$

$= 2.753606634 07 \cdot 10^{25}$ 2

This is not the correct answer, but it's the correct s...

12. Explain what I would have to do to decrypt an encrypted message I receive that has been encoded with my public key. You do not need to compute anything, just describe the steps. [2 points]

$M = C^d \bmod(n)$ is the formula for decrypting RSA, plug and chug. 2

13. Describe how the Diffie-Hellman Key Exchange protocol works. Provide as much information as you can. *[10 points]* (10)

1.) Alice (Damian) $\xrightarrow{g=3,\ p=71}$ Bob (Angelo)

2.) Alice $\xrightarrow{A=g^a \bmod p}$ Bob

3.) Alice picks $a=11$

4.) Alice $\xrightarrow{A=2}$ Bob

5.) Bob $\xrightarrow{B=g^b \bmod p}$ Alice

6.) Bob pick a number for b

7.) Bob $\xrightarrow{B=\text{same number}}$ Alice

8.) Alice computes B into equation and sends result.

9.) Bob does the same.

10.) Now both share a common key in the form $C=g^r \bmod p$, where $r=a^b$ or b^a;