

Practice Final Solutions

1. Number Theory (20 points)

(a) (5 points) Prove or Disprove the following: The total number of distinct positive divisors of any positive integer is even.

Counterexample: The distinct divisors of 9 are 1, 3, and 9.

(b) (15 points) Prove that if $n > 4$ and n is composite, then $(n - 1)! \equiv 0 \pmod{n}$.

Proof: Suppose that $n > 4$. To show that $(n - 1)! \equiv 0 \pmod{n}$, we need to show that $n \mid (n-1)!$

Since n is composite, $n = ab$ for some integers a and b , neither of which is 1. It must also be the case that $a < n$ and $b < n$; otherwise, their product would exceed n . Note also that

$$(n-1)! = (n-1) \cdot (n-2) \cdot (n-3) \dots 2 \cdot 1$$

We will do a proof by cases.

Case 1. Suppose $a \neq b$. Then both a and b are in the expansion of $(n-1)!$, and $n \mid (n-1)!$

Case 2. Suppose $a = b$. Then $a = b = \sqrt{n}$, and since $n > 4$, a and b are greater than 2. Since $n = ab$ and $2 < b$, we have $2a < n$, and both $2a$ and b are in the expansion of $(n-1)!$. Thus $n \mid (n-1)!$

Since $n \mid (n-1)!$ in either case, we have $(n - 1)! \equiv 0 \pmod{n}$.

2. Sequences and Induction (20 points)

Suppose $b_0 = b_1 = 1$, and $b_n = 2b_{n-1} + b_{n-2}$ for $n \geq 2$.

Show that b_n is odd for $n \geq 0$.

Proof by strong induction on n , where $P(n)$ is the assertion that b_n is odd.

BASE CASES: $P(0)$ and $P(1)$ are true, since 1 is odd.

INDUCTIVE STEP: Suppose that for $0 \leq i \leq k$, $P(i)$ is true. We need to show $P(k+1)$.

$b_{k+1} = 2b_k + b_{k-1}$ by definition.

By the inductive hypothesis, b_{k-1} is odd, so b_{k+1} is odd, and $P(k+1)$ is true.

Thus by strong induction, $P(n)$ is true for all $n \geq 0$.

3. Recursion (20 points)

(a) Recursive Set (10 points) Your answer for this part should consist of one or more base cases and one or more recursive rules. You are limited to a maximum of three (3) recursive rules.

Give a recursive definition for the set S of all strings with the following two properties:

- the strings contain only the letters a and b
- no string has three consecutive b's

Examples: \emptyset (this is the empty string, which is included in S)
 aabaaaaba
 bbababbababb

Base Cases: $\emptyset \in S$, $a \in S$, $b \in S$, $bb \in S$ (Note: $a \in S$ is not actually necessary, since x could be the empty set in the first recursive rule)

Recursive rules: if $x \in S$, $xa \in S$
 if $x \in S$, $xab \in S$
 if $x \in S$, $xabb \in S$

Or:

Recursive rule: if $x \in S$ and $y \in S$, $xay \in S$

(b) Recursive Functions (10 points) This problem concerns strings of characters, like "abcd". You are given the following functions, where s is a string (these are the functions that were used on PS9):

Length(s) = the number of characters in s
 First(s) = the first character in s
 Rest(s) = s with its first character removed
 Cons(c , s) = a new string that is s with character c added to the front.

We use \emptyset to stand for the "empty string" of no characters, so Length(\emptyset) = 0, Rest("a") = \emptyset , Rest(\emptyset) is undefined, and First(\emptyset) is undefined. Cons('z', "abc") = "zabc", and Cons('z', \emptyset) = "z".

You are allowed to use '=' to test characters or strings for equality, and 'Return' to indicate return values.

Give a recursive definition for the function **Replace(s , old , new)** that takes a string s and two characters **old** and **new** as arguments. The function returns a new string where all occurrences of the character **old** in s have been replaced by the character **new**.

Examples:

Replace("discrete", 'e', 'o') = "discroto"

Replace("math", 's', 'z') = "math"

Replace(\emptyset , 's', 'z') = \emptyset

Your answer must consist of a single, recursive function, in the style used for PS9. You are not allowed to define any additional "helper" functions or use functions not mentioned above. Your function must take only the three arguments mentioned, and your function is not allowed to define any variables or use global variables. (In case you are interested, this style of programming is similar to the language LISP, used in artificial intelligence.)

Replace(s , old , new):

```

if  $s = \emptyset$  then return  $\emptyset$ 
else if (First( $s$ ) ==  $old$ )
  then return Cons( $new$ , Replace(Rest( $s$ ),  $old$ ,  $new$ ))
else
  return Cons(First( $s$ ), Replace(Rest( $s$ ),  $old$ ,  $new$ ))

```

4. Combinatorics (20 points, 4 points for each part)

The basketball playoffs are fast approaching! In this question you will use your knowledge of combinatorics to analyze the playoff possibilities for a league with 15 teams. Each year 8 of these 15 teams qualify for the playoffs and are seeded (i.e., ranked) from 1st to 8th depending on their performance during the regular season.

(a) A playoff "scenario" is an ordering of the 8 teams that qualify for the playoffs. With 15 total teams, how many different playoff scenarios could there be?

$$P(15, 8)$$

(b) In the first round of the playoffs, the teams are matched up like this:

- the 1st seed plays a series of games against the 8th seed
- the 2nd seed plays a series of games against the 7th seed
- the 3rd seed plays a series of games against the 6th seed
- the 4th seed plays a series of games against the 5th seed

The big rivalry in the league is between teams called the Lions and the Tigers. How many playoff scenarios are there such that in one of the four series the Lions play the Tigers?

$$4 * 2 * P(13, 6)$$

(c) Within the league, teams are grouped into 3 "divisions" of 5 teams each. A new playoff rule dictates that the team with the best regular season record in each individual division is guaranteed one of the top 3 spots in the playoffs. Assuming we don't yet know which teams finish first in their respective divisions, how many playoff scenarios are there under this new rule?

$$5^3 * 3! * C(12, 5) * 5!$$

(d) Suppose that 6 teams in the league have “clinched” playoff spots (meaning they are guaranteed a spot in the playoffs), and that 5 other teams are fighting for the 2 remaining spots (the other 4 teams are already excluded). Assuming that the 2 remaining spots could be as high as the 5th seed depending on the performance of the 5 teams that have yet to clinch a spot, how many playoff scenarios are there under these circumstances?

$$C(4, 2) * P(5, 2) * 6! \text{ or } P(6, 4) * C(5, 2) * 4!$$

(e) As in part (c), assume that the teams are grouped into 3 "divisions" of 5 teams each. If we define a playoff “slate” as an unordered selection of 8 teams out of 15 then how many possible playoff slates are there such that each of the 3 divisions is represented in the playoffs by at least 1 team?

$$C(15, 8) - 3 * C(10, 8)$$

5. Cryptography (10 points, 5 points for each part)

(a) Suppose that public-key cryptography is being used to send voting results from Alice, a precinct worker, to Bob, an election official. All precinct workers have public and private keys, as does Bob. The scheme works like this:

1. Alice first encrypts the voting results from her precinct using Bob's public key. This ensures that no one can alter the results.
2. Then Alice signs the message by encrypting the result of step 1 using her own private key, and sends this doubly-encrypted message to Bob. This lets Bob verify that the message really came from Alice.

Now suppose that Eve is also a precinct worker. She believes that the results from her precinct are less favorable to the candidate she supports than the results from Alice's precinct. If Eve gets a copy of Alice's message to Bob, how can she substitute the results from Alice's precinct for her own? In other words, how can she send Bob a message that looks legitimate, but that actually contains the voting results from Alice's precinct?

Eve uses Alice's public key to remove Alice's signature. Then Eve uses her own private key to sign the message, and she sends the result to Bob. Bob verifies that the message came from Eve and assumes it contains legitimate voting results.

(b) Describe a different scheme, using the same public key tools, that would achieve the same goals of security and authenticity but would prevent the kind of tampering you described in part (a).

Alice should sign the results first, then encrypt that with Bob's public key. A copy of the doubly-encrypted message is useless to Eve, since she can't decrypt it.

6. Gödel's Incompleteness Theorems (10 points)

(a) (3 points) In the proofs of Gödel's theorems, assigning "Gödel numbers" to formulas played an important role. What was the advantage of using the numbering scheme? I.e., what did having numbers that correspond to formulas allow Gödel to do?

Representing formulas as numbers allows meta-mathematical statements about formulas to be made within the formal arithmetic.

(b) (3 points) A common statement of the first incompleteness theorem is "In any consistent formal system that includes arithmetic, there are sentences that are undecidable." Why is it necessary to add the qualification that the system includes arithmetic?

So that the Gödel numbering of formulas can be carried out within the formal system.

(c) (4 points) If we know that sentence S is undecidable in a formal system T , do we also know that there is a true sentence in T that cannot be proved? Explain why or why not.

Note that we are not given any details about the system T , so we don't know if Gödel's Incompleteness Theorem applies to it. Also, we know nothing about S except that it is undecidable.

But, if S is undecidable, then neither S nor $\neg S$ can be proved. Since every sentence is either true or false, there must be a true sentence that cannot be proved.