CSC165H1: Problem Set 3

Due November 15, 2017 before 10pm

General instructions

Please read the following instructions carefully before starting the problem set. They contain important information about general problem set expectations, problem set submission instructions, and reminders of course policies.

- Your problem sets are graded on both correctness and clarity of communication. Solutions which are technically correct but poorly written will not receive full marks. Please read over your solutions carefully before submitting them. Proofs should have headers and bodies in the form described in the course note.
- Each problem set may be completed in groups of up to three. If you are working in a group for this problem set, please consult `https://github.com/MarkUsProject/Markus/wiki/Student_Groups` for a brief explanation of how to create a group on MarkUs.

  Exception: Problem Sets 0 and 1 must be completed individually.
- Solutions must be typeset electronically, and submitted as a PDF with the correct filename. **Hand-written submissions will receive a grade of ZERO.**

  The required filename for this problem set is **problem_set3.pdf**.
- Problem sets must be submitted online through MarkUs. If you haven't used MarkUs before, give yourself plenty of time to figure it out, and ask for help if you need it! If you are working with a partner, you must form a group on MarkUs, and make one submission per group. "I didn't know how to use MarkUs" is not a valid excuse for submitting late work.
- Your submitted file should not be larger than 9MB. This may happen if you are using a word processing software like Microsoft Word; if it does, you should look into PDF compression tools to make your PDF smaller, although please make sure that your PDF is still legible before submitting!
- The work you submit for credit must be your own; you may not refer to or copy from the work of other groups, or external sources like websites or textbooks. You may, however, refer to any text from the Course Notes (or posted lecture notes), except when explicitly asked not to.

Additional instructions

- For each proof, clearly define the predicate ($P(n)$) that is relevant for your proof.
- You may not use forms of induction we have not covered in lecture.
- Please follow the same guidelines as Problem Set 2 for all proofs.

1. **[12 marks] extend some results...**

Definition 1 (sequence a_n, $\mathcal{S}$). Let $a : \mathbb{N} \mapsto \mathbb{Z}$. Denote $a(n) = a_n$, and a is identified with the sequence $a_0, a_1, a_2, \ldots$. Let $\mathcal{S} = \{f \mid f : \mathbb{N} \mapsto \mathbb{Z}\}$ be the set of integer sequences.

(a) **[3 marks]** Use induction on n to prove that if m is some non-zero integer, and $a, b \in \mathcal{S}$ are arbitrary integer sequences, and n is an arbitrary natural number greater than 0, then

$$(\forall k \leq n, a_k \equiv b_k \pmod{m}) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k \pmod{m}$$

Hint: You may assume 2.18(c) from the course notes as a starting point.

(b) **[3 marks]** Use induction on n to prove that if $d \in \mathbb{N}$, $d > 1$, and b is an integer sequence with $b_m > 0$ for all natural numbers m, and n is an arbitrary natural number, then

$$(\forall i \in \mathbb{N}, i \leq n \Rightarrow \gcd(d, b_i) = 1) \Rightarrow d \nmid \prod_{i=0}^{i=n} b_i$$

Hint: You may assume 2(g) from problem set 2 as a starting point.

(c) **[3 marks]** Consider the sums

$$\frac{1}{2+1} + \frac{1}{2 \times 2} = \frac{14}{24} > \frac{13}{24} \qquad \frac{1}{3+1} + \frac{1}{3+2} + \frac{1}{2 \times 3} = \frac{37}{60} > \frac{13}{24}$$

Use induction to prove that for all natural numbers n, if $n > 1$ then:

$$\sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$$

(d) **[3 marks]** Define integer sequence $c \in \mathcal{S}$ by

$$c_n = \begin{cases} 0, & \text{if } n = 0 \\ c_{n-1} + 3n^2 - 3n + 1, & \text{if } n > 0 \end{cases}$$

Use induction on n to prove that for all $n \in \mathbb{N}, c_n = n^3$.

2. **[8 marks] Counting subsets**

(a) **[3 marks]**

Definition 2 ($\binom{n}{k}$). Let $n, k \in \mathbb{N}$, $k \leq n$, and S be a set with $|S| = n$. Then $\binom{n}{k}$ denotes the number of subsets S of size k.

Use induction on n to prove

$$\forall n, k \in \mathbb{N}, k \leq n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Hint: Notice that no induction is required when $k = 0$ or $k = n$, and look for a connection between $\binom{n+1}{k}$ and both $\binom{n}{k}$ and $\binom{n}{k-1}$. This approach requires you to introduce k **after** n. **Anti-Hint**: You may **not** use results from combinatorics such as the Binomial Theorem, since they are, essentially, what you are proving.

Definition 3 (S_n). Let $n \in \mathbb{N}$. Define $S_n = \{1, 2, \ldots, n\}$

Definition 4 (DTP_n). Let $n \in \mathbb{N}$. Define the set of **disjoint two-set partitions** of S_n as follows:

$$DTP_n = \{\{A, B\} \mid A, B \subseteq S_n \text{ and } A \cup B = S_n \text{ and } A \cap B = \emptyset\}$$

Notice that $DTP_0 = \{\{\emptyset, \emptyset\}\}$ and $DTP_1 = \{\{\{1\}, \emptyset\}\}$.

(b) **[2 marks]** Write out all the elements of DTP_2 and DTP_3 explicitly.

(c) **[3 marks]** Find a closed-form expression for $|DTP_n|$ in terms of n. Use induction on n to prove your formula correct.

3. **[11 marks] asymptotics**

(a) **[3 marks]** Use the definition of big-Theta from the course notes to prove Theorem 5.8.

(b) **[3 marks]** Use the definition of big-Oh from the course notes to prove that for all $a, b \in \mathbb{R}^+$

$$(b > a \wedge a > 1) \Rightarrow b^n \notin O(a^n)$$

You may **not** use limits or other techniques of calculus.

(c) **[5 marks]** Read over function xgcd, which calculates the extended gcd(n, m), below:

```
1 def xgcd(n, m):
2     s1, s0, t1, t0, r1, r0 = 0, 1, 1, 0, m, n
3     while r1 != 0:
4         quotient = r0 // r1
5         r0, r1 = r1, r0 - quotient * r1
6         s0, s1 = s1, s0 - quotient * s1
7         t0, t1 = t1, t0 - quotient * t1
8     return (r0, s0, t0)
```

Let the input size be n. Assume that the loop body, lines 4–7, is 1 “step”. Prove that the runtime of xgcd, $\mathrm{RT}_{\texttt{xgcd}} \in O(\lg n)$. **Hint:** Can you show that every two iterations of the loop reduces r0 by at least half?