CSC165H1: Problem Set 3 Sample Solutions

Due November 15, 2017 before 10pm

Note: solutions are incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

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

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

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

<u>**Solution**</u>

Claim:

$$\forall a, b \in \mathcal{S}, \forall m \in \mathbb{Z}, \forall n \in \mathbb{N}, (m \neq 0 \wedge [\forall k \in \mathbb{N}, k \leq n \Rightarrow a_k \equiv b_k \pmod m]) \Rightarrow \prod_{k=0}^{n} a_k \equiv \prod_{k=0}^{n} b_k \pmod m$$

Proof (induction on n): Let $a, b \in \mathcal{S}$ be arbitrary integer sequences, let m be an arbitrary integer, and let k be an arbitrary natural number. Assume $m \neq 0$. Define $P(n)$:

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

Base cases: $a_0 \equiv b_0 \pmod m$ is the same as $\prod_{k=0}^{0} a_k = \prod_{k=0}^{0} b_k \pmod m$, since this is a unary product, so $P(0)$ is true.* $a_0 \equiv b_0 \wedge a_1 \equiv b_1 \pmod m$ implies $a_0 a_1 \equiv b_0 b_1 \pmod m$ by Exercise 2.18(c) in the course notes, so $P(1)$ is true.

Inductive step: Let $n \in \mathbb{N}$ and assume $P(n)$ is true, that is if $\forall k \in \mathbb{N}, k \leq n \Rightarrow a_k \equiv b_k \pmod m$ then $\prod_{k=0}^{n} a_k \equiv \prod_{k=0}^{n} b_k \pmod m$. I will show that $P(n+1)$ follows.

Assume $\forall k \in \mathbb{N}, k \leq n+1 \Rightarrow a_k \equiv b_k \pmod m$. Then,

$$\begin{aligned}\prod_{k=0}^{n+1} a_k = [\prod_{k=0}^{n} a_k] \times a_{k+1} &\equiv [\prod_{k=0}^{n} b_k] \times b_{k+1} \pmod m \qquad \text{(by IH and 2.18(c))} \\ &\equiv \prod_{k=0}^{n+1} b_k \pmod m \qquad \blacksquare\end{aligned}$$

*Base case 0 is feasible, and sufficient provided the inductive step is done appropriately

(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.

Solution

Claim:

$$\forall d \in \mathbb{N}, \forall b \in \mathcal{S}, \forall n \in \mathbb{N}, (d > 1 \wedge [\forall i \in \mathbb{N}, i \leq n \Rightarrow \gcd(d, b_i) = 1]) d \nmid \prod_{i=0}^{n} b_i$$

*

Proof (induction on n): Let $d \in \mathbb{N}, b \in \mathcal{S}$ Assume $d > 1$ Define $P(n)$:

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

Base cases: Since $d > 1$, if $\gcd(d, b_0) = 1 < d$ means that $d \nmid b_0$, so $P(0)$ holds. If $\gcd(d, b_0) = 1 = \gcd(d, b_1)$, then the contrapositive of 2(g) from problem set 2 implies that $d \nmid b_0 b_1$, so $P(1)$ holds.

Inductive step: Let $n \in \mathbb{N}$ and assume $P(n)$, that is:

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

I will show that $P(n+1)$ follows. Assume $\forall i \in \mathbb{N}, i \leq n+1 \Rightarrow \gcd(d, b_i) = 1$.

Then,

$$\begin{aligned} &(\text{By IH and } \gcd(d, b_{n+1}) = 1) \quad & d \nmid \prod_{i=0}^{n} b_i \wedge d \nmid b_{n+1} \quad &\Rightarrow \quad d \nmid [\prod_{i=0}^{n} b_i] \times b_{n+1} \quad & \text{by 2(g)} \\ &&&= \quad \prod_{i=0}^{n+1} b_i \quad \blacksquare & \end{aligned}$$

*The requirement that $b_m > 0$ is implicit in $\gcd(d, b_i) = 1$ when $d > 1$.

(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:

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

<u>**Solution**</u>

Claim:

$$\forall n \in \mathbb{N}, n > 1 \Rightarrow \sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$$

Proof (induction on n): Define $P(n)$:

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

Base case: $P(2)$ was verified in the presentation of this question, above.

Inductive step: Let $n \in \mathbb{N}$. Assume $n > 1$ and $P(n)$. I will show that $P(n+1)$ follows. Then,

$$\begin{aligned}
\sum_{j=(n+1)+1}^{2(n+1)} \frac{1}{j} &= \left[\sum_{j=n+1}^{j=2n} \frac{1}{j}\right] + \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1} \\
&> \frac{13}{24} + \left[\frac{(2n+2)+(2n+1)-2(2n+1)}{2(n+1)(2n+1)}\right] \qquad \text{(by IH)} \\
&= \frac{13}{24} + \left[\frac{1}{2(n+1)(2n+1)}\right] > \frac{13}{24} \qquad \left(\frac{1}{2(n+1)(2n+1)} > 0\right) \qquad \blacksquare
\end{aligned}$$

(d) **[3 marks]** Define integer sequence $c \in S$ 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 $n \in \mathbb{N}, c_n = n^3$.

<u>**Solution**</u>

Claim:

$$\forall n \in \mathbb{N}, c_n = n^3$$

Proof (induction on n): Let $n \in \mathbb{N}$. Define $P(n)$:

$$P(n) : c_n = n^3$$

Base case: By the definition $c_0 = 0 = 0^3$, so $P(0)$ holds.

Inductive step: Let $n \in \mathbb{N}$ and assume $P(n)$, that is $c_n = n^3$. I will show that $P(n+1)$ follows.
From the definition:

$$\begin{aligned}
c_{n+1} &= c_n + 3(n+1)^2 - 3(n+1) + 1 \\
&= n^3 + 3(n^2 + 2n + 1) - 3n - 3 + 1 \qquad \text{(by IH)} \\
&= n^3 + 3n^2 + 6n - 3n + 3 - 3 + 1 = n^3 + 3n^2 + 3n + 1 = (n+1)^3 \qquad \blacksquare
\end{aligned}$$

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

(a) **[3 marks]**

Definition 2 ($\binom{n}{k}$). Let $n, k \in \mathbb{N}$, $k \le n$, 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

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

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.

Solution

Claim:

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

Proof (induction on n): Define $P(n)$

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

Base cases: There is exactly one way of choosing a subset of size 0 (the empty set) from any set, and in particular sets of size 0 or 1. There is exactly one way of choosing a subset of size n from a set of size n, and in particular the set of size 1. This means that

$$\frac{0!}{0!(0-0)!} = 1 = \binom{0}{0} = \binom{1}{0} = \binom{1}{1} = \frac{1!}{0!(1-0)!} = \frac{1!}{1!(1-1)!}$$

This verifies $P(0)$ and $P(1)$. (Recall that $0! = 1! = 1$).

Induction step: Let $n \in \mathbb{N}$. Assume $n > 0$ and also assume $P(n)$. I will show that $P(n+1)$ follows.

Assume $k \in \mathbb{N}$ and $k \le n$. Let S be an arbitrary set with $|S| = n + 1$.

Case $k = 0 \vee k = n + 1$: If $k = 0$ or $k = n + 1$ the result is immediate, since there is exactly one way to choose a subset of size 0 or a subset of size $n + 1$ from S, and

$$\binom{n+1}{0} = \frac{(n+1)!}{0!(n+1-0)!} = 1 = \frac{(n+1)!}{(n+1-0)!0!}$$

Case $0 < k \wedge k < n + 1$: Since S has at least 2 elements, let $x \in S$ be a particular element of S. The k-subsets of S that do not include x are also k-subsets of $S \setminus \{x\}$. Since $|S \setminus \{x\}| = n$ and $0 < k \le n$, by the IH we know that there are $\binom{n}{k} = n!/(k!(n-k)!)$ such subsets.

The k-subsets of S that do contain x are formed by the union of $\{x\}$ with each of the $(k-1)$-subsets of $S \setminus \{x\}$. Since $0 \le k-1 < n+1$, by the IH we know that there are $\binom{n}{k-1} = n!/((k-1)!(n-k+1)!)$ such subsets.
Altogether this makes

$$\begin{aligned}\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \qquad \text{(by IH)}\\ &= \frac{(n-k+1)n!}{k!(n-k+1)!} + \frac{k \times n!}{k!(n-k+1)!}\\ &= \frac{(n+1)n! + (k-k)n!}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} \qquad \blacksquare\end{aligned}$$

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.

Sample solution: The set of disjoint two-set partitions of $S_2 = \{1, 2\}$ is:

$$\{\{\{1,2\}, \emptyset\}, \{\{1\}, \{2\}\}\}$$

The set of disjoint two-set partitions of $S_3 = \{1, 2, 3\}$ is:

$$\{\{\{1,2,3\}, \emptyset\}, \{\{1\}, \{2,3\}\}, \{\{2\}, \{1,3\}\}, \{\{3\}, \{1,2\}\}\}$$

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

Sample solution: The closed form also provides the predicate to be proved:

$$P(n) : |DTP_n| = \begin{cases} 1 & \text{if } n = 0 \\ 2^{n-1} & \text{if } n > 0 \end{cases}$$

:Claim: $\forall n \in \mathbb{N}, P(n)$.

Proof (induction on n):

Base cases: There is exactly one 2-set partition of S_0, the empty set, which verifies $P(0)$. There is also exactly one 2-set partition of S_1, the partition formed by its pair of subsets, which verifies $P(1)$

Inductive step: Let $n \in \mathbb{N}$. Assume $n > 0$ and assume $P(n)$. I will show that $P(n+1)$ follows.
Let $\{A, B\}$ be an arbitary 2-set partition of S_{n+1} where $1 \in A$, and note that $n+1 \neq 1$. I construct a correspondence between pairs of 2-set partitions of S_{n+1} and single 2-set partitions of S_n. There are two cases to consider:

Case $n+1 \in A$: Let $A' = A \setminus \{n+1\}$, $B' = B \cup \{n+1\}$, that is, move element $n+1$ from one set to the other. Then the 2-set partitions $\{A, B\} \neq \{A', B'\}$ since $C = \{1, n+1\} \subseteq A$, but $C \subsetneq A'$ and $C \subsetneq B'$.

Case $n+1 \in B$: Let $A' = A \cup \{n+1\}$, $B' = B \setminus \{n+1\}$, that is, move element $n+1$ from one set to the other. Then the 2-set partitions $\{A, B\} \neq \{A', B'\}$, since $C = \{1, n+1\} \subseteq A'$, but $C \subsetneq A$ and $C \subsetneq B$.

Removing element $n+1$ from both partitions we have $\{A' \setminus \{x\}, B' \setminus \{x\}\} = \{A \setminus \{x\}, B \setminus \{x\}\}$, a 2-set partition of S_n. Hence, each 2-set partition of S_n corresponds to two 2-set partitions of S_{n+1}, so by the IH there are:

$$|DTP_{n+1}| = 2 \times |DTP_n| = 2 \times 2^{n-1} = 2^n \qquad \blacksquare$$

3. **[11 marks] asymptotics**

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

Solution

Claim:

$$\forall f : \mathbb{N} \mapsto \mathbb{R}^+, [\exists n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow f(n) \geq 1] \Rightarrow \lfloor f \rfloor \in \Theta(f) \land \lceil f \rceil \in \Theta(f)$$

For $x \in \mathbb{R}$, I use the following characterizations of $\lfloor x \rfloor$ and $\lceil x \rceil$ in the proof below:

$$x - 1 < \lfloor x \rfloor \leq x \qquad\qquad x \leq \lceil x \rceil < x + 1$$

Proof: Let f be an arbitrary function from $\mathbb{N}$ to $\mathbb{R}^+$. Assume $\exists n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow f(n) \geq 1$. Let n_0 be such a value. Let $c_1 = 1, c_2 = 1/2, c_3 = 2, c_4 = 1$. Let $n \in \mathbb{N}$ and assume $n \geq n_0$. Then

$$\begin{aligned}
\lfloor f(n) \rfloor &\leq 1 \times f(n) = c_1 f(n) && \text{(definition of floor)} \\
f(n) \geq 1 \Rightarrow \lfloor f(n) \rfloor &\geq 1 && \\
2\lfloor f(n) \rfloor = \lfloor f(n) \rfloor + \lfloor f(n) \rfloor &\geq \lfloor f(n) \rfloor + 1 \geq f(n) && \text{(by characterization of floor)} \\
2\lfloor f(n) \rfloor &\geq f(n) && \\
\lfloor f(n) \rfloor &\geq \frac{1}{2} f(n) = c_2 f(n) && \\
& \lfloor f \rfloor \in \Theta(f) \quad \blacksquare && \\
\lceil f(n) \rceil &\geq 1 \times f(n) = c_4 f(n) && \text{(definition of ceiling)} \\
\lceil f(n) \rceil \leq f(n) + 1 &\leq 2f(n) = c_3 f(n) && \text{(by characterization of ceiling)} \\
& \lceil f \rceil \in \Theta(f) \quad \blacksquare &&
\end{aligned}$$

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

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

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

Solution

Claim: I use the negation of $b \in \mathcal{O}(a)$:

$$\forall a, b \in \mathbb{R}^+, [b > a \land a > 1] \Rightarrow \forall c, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, n \geq n_0 \land b^n > ca^n$$

Proof: Let $a, b \in \mathbb{R}^+$. Assume $a > 1$ and $b > a$. Let c, n_0 be arbitrary positive real numbers. Let $n = 1 + \max(n_0, \lg c/(\lg b - \lg a)$. Then $n \geq n_0$ and

$$\begin{aligned} n &> \frac{\lg c}{\lg b - \lg a} \\ n(\lg b - \lg a) &> \lg c \qquad \text{(monotonicity of lg and } b > a > 1) \\ \left(\frac{b}{a}\right)^n &> c \\ b^n &> ca^n \qquad \blacksquare \end{aligned}$$

(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 $n \in \mathbb{N}$. 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?

Solution

Define $r0_i$ as the value of $r0$ at the end (line 7) of the ith iteration, and $r1_i$ as the value of $r1$ at the end (line 7) of the ith iteration, and q_i as the value of quotient at the end of the ith iteration.

Claim #1: If $r0_i, r1_i \in \mathbb{N}$, $r0_i \geq r1_i$ and there is an iteration $i+2$ of the list then:

- $r0_{i+2}, r1_{i+2} \in \mathbb{N}$
- $r0_{i+2} \geq r1_{i+2}$
- $r0_i \geq 2 \times r0_{i+2}$

Proof of Claim #1: Let $r0_i, r1_i \in \mathbb{N}$. Assume $r0_i \geq r1_i$ and that there are iterations $i+1$ and $i+2$. Since iteration $i+1$ occurs, $r1_i \neq 0$, so by the Quotient-Remainder Theorem and lines 4 and 5:

$$r0_i = q_{i+1} r1_i + r1_{i+1} \wedge r1_i > r1_{i+1} \wedge r1_{i+1} \geq 0$$

Also, by line 5, $r0_{i+1} = r1_i$ and $r1_{i+1}$ (being the remainder) is strictly smaller than $r0_{i+1}$. Since iteration $i+2$ occurs, by the Quotient-Remainder Theorem and lines 4 and 5:

$$r0_{i+1} = q_{i+2} r1_{i+1} + r1_{i+2} \wedge r1_{i+1} > r1_{i+2} \wedge r1_{i+2} \geq 0$$

Again, by line 5, $r0_{i+2} = r1_{i+1}$ and $r1_{i+2}$ (being the remainder) is strictly smaller than $r0_{i+2}$, so

- $r0_{i+2}, r1_{i+2} \in \mathbb{N}$, by the Quotient-Remainder Theorem
- $r0_{i+2} \geq r1_{i+2}$, since the latter is the remainder
- $r0_i \geq 2 \times r0_{i+2}$, by considering two cases:

Case $r0_i \geq 2r1_i$: Then $r0_i \geq 2r1_{i+1}$, since the latter is the remainder. But $r0_{i+2} = r1_{i+1}$, by line 5, so $r0_i \geq 2r0_{i+2}$. ■

Case $r0_i < 2r1_i$: This can be rewritten as $r0_i/2 < r1_i$, and since $r0_i \geq r1_i$ we know that $q_{i+1} > 0$, so

$$\begin{aligned} r0_i &= q_{i+1}r1_i + r1_{i+1} \\ r0_i - q_{i+1}r1_i &= r1_{i+1} \\ \frac{r0_i}{2} = r0_i - \frac{r0_i}{2} > r0_i - q_{i+1}r1_i &= r1_{i+1} \end{aligned}$$

But $r0_{i+2} = r1_{i+1}$, by line 5, so $r0_i \geq 2r0_{i+2}$. ■

Claim #2: If $r0_i, r1_i \in \mathbb{N}$, $r0_i < r1_i$ and there is an iteration $i+3$ of the list then:

- $r0_{i+3}, r1_{i+3} \in \mathbb{N}$
- $r0_{i+3} \geq r1_{i+3}$
- $r0_i \geq 2 \times r0_{i+3}$

In this case line 4 sets $q_{i+1} = 0$, so line 5 sets $r0_{i+1} = r1_i$, and $r1_{i+1} = r0_i$, and now $r0_{i+1}$ and $r1_{i+1}$ satisfy the assumptions for Claim #1, so the conclusions follow substituting $i+1$ for i. ■

Claim #3: $\forall n, m \in \mathbb{N}, \exists c \in \mathbb{R}^+, n > 1 \Rightarrow RT(\text{xgcd}(n)) \leq c\lg(n)$

Proof: Let $n, m \in \mathbb{N}$ and assume $n > 1$. By line 2 we know that the initial values of $r0 = n$ and $r1 = m$. By Claim #1 and Claim #2 we know that the maximum number of iterations, i of the loop that may occur before $r0 = 1$ is no more than when

$$\begin{aligned} \lfloor n \times \left(\frac{1}{2}\right)^{i/3} \rfloor &= 1 \\ n \times \left(\frac{1}{2}\right)^{i/3} &\geq 1 \\ \lg(n) + \frac{i}{3}(0 - \lg(2)) &\geq 0 \\ \lg(n) - \frac{i}{3} &\geq 0 \\ 3\lg(n) &\geq i \end{aligned}$$

Once $r0 = 1$, by Claim #1 there are at most 2 iterations before $r1 = 0$ and the loop terminates. Thus $RT(\text{xgcd}(n)) \leq 3\lg(n) + 2 \leq 5\lg(n)$, provided $n \geq 2$. ■