CS 330 : Discrete Computational Structures
Fall Semester, 2015
ASSIGNMENT #7
Due Date: Sunday, Oct 25
Cahlen Brancheau

Suggested Reading: Rosen Section 5.3; LLM Chapter 6.1 - 6.3

These are the problems that you need to turn in. For more practice, you are encouraged to work on the other problems. **Always explain your answers and show your reasoning.**

1. **[12 Pts]** Let S defined recursively by (1) $5 \in S$ and (2) if $s \in S$ and $t \in S$, then $st \in S$. Let $A = \{5^i \mid i \in \mathcal{Z}^+\}$. Prove that

   (a) **[6 Pts]** $A \subseteq S$ by mathematical induction.
   Answer:

   Basis: $5^1 = 5$ and by definition $5 \in S$
   Inductive Step:
   Assume $5^k \in S$ where $k \in \mathcal{Z}$
   Prove: $5^{k+1} \in S$
   $5^{k+1} = 5^k * 5$, $5^k \in S$ by the IH and $5 \in S$ by step (1) in the recursive definition of S.
   Therefore $5^k * 5 \in S$ by step (2) in the recursive definition of S.

   Quod erat demonstrandum.

   (b) **[6 Pts]** $S \subseteq A$ by structural induction.
   Answer:

   Basis: $5 \in S$ by step (1) in the recursive definition of S and $5 = 5^1 \in A$
   Inductive Step:
   Let $a, b \in S$, $a * b \in S$ by step (2) in the recursive definition of S.
   Assume $a, b \in A$
   Prove: $a * b \in A$
   By the IH $a = 5^x$ and $b = 5^y$ where $x, y \in \mathcal{Z}$. $a * b = 5^x * 5^y = 5^{x+y}$. $x + y \in \mathcal{Z}$ therefore $a * b \in A$.

   Quod erat demonstrandum.

2. **[12 Pts]** Let S be defined by (1) $(0,0) \in S$, and (2) if $(a,b) \in S$, then $(a, b+5) \in S$, $(a+1, b+4) \in S$ and $(a+2, b+3) \in S$.

   (a) **[6 Pts]** Use structural induction to prove that if $(a,b) \in S$ then 5 divides $a+b$.
   Answer:

   Basis: $(0,0) \in S$ and 5 divides $0+0=0$

   Inductive Step:
   Assume $(a,b) \in S$ where 5 divides $a+b$ $(x,y) \in S$ and let $(a,b) \in S$ where (a,b) is the relation that the recursive definition of S was applied to in order to get to (x,y).

   It must be the case that $x = a, y = b+5$ or $x = a+1, y = b+4$ or $x = a+2, y = b+3$.

   Case 1: $x = a, y = b+5$. $x+y = a+b+5$. By the IH 5 divides $a+b$ and 5 divides 5.
   Case 2: $x = a+1, y = b+4$. $x+y = a+b+5$. By the IH 5 divides $a+b$ and 5 divides 5.
   Case 2: $x = a+2, y = b+3$. $x+y = a+b+5$. By the IH 5 divides $a+b$ and 5 divides 5.

   Quod erat demonstrandum.

   (b) **[6 Pts]** Disprove the converse of the statement above, *i.e.*, show that if $a, b \in \mathcal{N}$, and $a+b$ is divisible by 5, it does not follow that $(a,b) \in S$. Modify the recursive definition of S to make the converse true.
   Answer:

   5 divides $3+2=5$, but $(3,2) \notin S$

   New Definition of S

   (1) $(0,0) \in S$
   (2) if $(a,b) \in S$, then $(a, b+5) \in S$, $(a+1, b+4) \in S$, $(a+2, b+3) \in S$ $(a+3, b+2) \in S$, $(a+4, b+1) \in S$, $(a+5, b) \in S$.

   Quod erat demonstrandum.

3. **[6 Pts]** Give a recursive definition of the set of bit strings that are palindromes.
Answer:
Basis: An empty string is a palindrome and string with a one bit length is a palindrome.

Inductive Step:
A strings in the form pcp are palindromes, where c is a bit and p is a palindrome.

Quod erat demonstrandum.

4. **[20 Pts]**

(a) **[8 Pts]** Give an inductive definition of the set $L = \{(a, b) \mid a, b \in \mathcal{Z}, (a - b) \bmod 3 = 0\}$. Let L' be the set obtained by your inductive definition.
Answer:

Basis: $(0, 0) \in L'$

Recursive: if $(x, y) \in L'$ then $(x + 1, y + 1) \in L'$, $(x - 1, y - 1) \in L'$, $(x, y + 3) \in L'$, $(x, y - 3) \in L'$.

(b) **[6 Pts]** Prove that $L' \subseteq L$.
Answer:

By definition of $L' \subseteq L$ all pairs in L' must be divisible by 3. In other words for any $(a, b) \in L', a - b = 3k$ where $k \in \mathcal{Z}$
With the recursive definition of L' the possible options are thus:

Case 1: $(a - 1, b - 1)$, this is the same as $a - b$ therefore still divisible by 3.
Case 2: $(a + 1, b + 1)$, this is the same as $a - b$ therefore still divisible by 3.
Case 3: $(a, b + 3)$, $a - b + 3 = 3k - 3 = 3(k - 1)$ therefore still divisible by 3.
Case 4: $(a, b - 3)$, $a - b - 3 = 3k + 3 = 3(k + 1)$ therefore still divisible by 3.

(c) **[6 Pts]** Prove that $L \subseteq L'$.
Answer:

All pairs in L must be divisible by 3. In other words for any $(a, b) \in L, a - b = 3k \rightarrow b = 3k - a$ where $k \in \mathcal{Z}$.
Any element in L with be in the form $(a, 3k - a)$. To get to any other pair using the definition of L' we apply the following.

(1) $(0, 0)$ to $(0, 3k)$. If $k \geq 0$ apply $(x, y + 3)$ k times, else apply $(x, y - 3)$ k times.
(2) $(0, 3k)$ to $(a, 3k - a)$. If $a \geq 0$ apply $(x + 1, b + 1)$ a times, else apply $(x - 1, y - 1)$ a times.