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

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.
   Solution:
   Mathematical Induction: We define P(n) which means $5^n \in S$.
   Basis Step: for $n = 1$ we see that P(1) means $5 \in S$,
   By Basis step of definition of S, we know that $5 \in S$. So P(1) is true.
   Inductive Step: assume that P(k) is true. So we know that $5^k \in S$. Now we want to show that P(k+1) true.
   By Basis step of definition of S we know $5 \in S$ and by Inductive Hypothesis we know that $5^k \in S$.
   By Inductive step of definition of S, we know that $5 \times 5^k \in S$. So $5^{k+1} \in S$. So P(k+1) is true.

   (b) **[6 Pts]** $S \subseteq A$ by structural induction.
   Solution:
   Structural Induction:
   Basis : By Basis step of definition of S we know that $5 \in S$. we know $5 = 5^1$, so $5 \in A$.
   We assume that there are x and y in S such that they're in A as well. We want to prove that $xy \in A$.
   $x \in A$ so we can write x in the form of 5^k.
   $y \in A$ so we can write y in the form of 5^l.
   $xy = 5^k \times 5^l = 5^{k+l} = 5^t$ such that $t = k + l$ and we know $5^t \in A$.

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 $a + b$.
   Solution:
   Basis: By the definition of S (Basis step), $(0, 0) \in S$. we know that $5|0 + 0 = 0$. So it's true.
   Inductive Step: Let $(a, b) \in S$. we assume that $5|a + b$. By inductive rules we know that if $(a, b) \in S$ then $(a, b + 5) \in S, (a + 1, b + 4) \in S, (a + 2, b + 3) \in S$
   We prove that 5 divides all of these:
   Case 1: (a,b+5); $a + (b + 5) = a + b + 5$. We know $5|a + b$ and $5|5$ so $5|a + b + 5$
   Case 2: (a+1,b+4); $(a + 1) + (b + 4) = a + b + 5$. We know $5|a + b$ and $5|5$ so $5|a + b + 5$
   Case 3: (a+2,b+3); $(a + 2) + (b + 3) = a + b + 5$. We know $5|a + b$ and $5|5$ so $5|a + b + 5$
   Therefore if $(a, b) \in S$, then $(a, b + 5) \in S$,$(a + 1, b + 4) \in S$ and $(a + 2, b + 3) \in S$.

(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.

Solution:

The counterexample is (5,0). 5 divides 5+0, but we can never get to (5,0) using the rules. Notice that we have (0,0) in our set (by Basis step) and all the inductive rules change b to one of the b+5,b+4 or b+3. So it couldn't remain 0 because b is increasing. For inductive step we need to modify the rules in order to cover all possibilities that are divisible by 5. Therefore we must add three new rules to our existing rule set
The inductive step must be :
if $(a,b) \in S$, then $(a, b+5) \in S$, $(a+1, b+4) \in S$, $(a+2, b+3) \in S$, $(a+3, b+2) \in S$, $(a+4, b+1) \in S$ and $(a+5, b) \in S$.

3. **[6 Pts]** Give a recursive definition of the set of bit strings that are palindromes.

Base: $\{\lambda, 0, 1\}$ are all palindromes (where λ is the empty string).

Recursive step: if w is a palindrome, then $0w0$ and $1w1$ are also palindromes.

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.
Base: $(0,0) \in L'$
Inductive rules: if $(a,b) \in L'$, then $(a, b-3) \in L', (a, b+3) \in L', (a+1, b+1) \in L'$ and $(a-1, b-1) \in L'$.
(As a side note, there is a set of 3 rules that is sufficient to generate all of L: $(a+3, b), (a, b+3), and (a-1, b-1)$. However, this set of rules makes the proof of part c easier.)

(b) **[6 Pts]** Prove that $L' \subseteq L$.
First, we prove that all of the base elements of L' are in L:
$0 - 0 = 0$, which is a multiple of 3. So, $(0,0) \in L$.
Now, we prove that if we apply our rules to something in L, we get something in L. ("L-ness" is preserved by our rules)
If (a,b) is in L, then our rules produce $(a, b-3)$, $(a, b+3)$, $(a+1, b+1)$ and $(a-1, b-1)$.
Since (a,b) is in L, $a-b$ is a multiple of 3. Then,
$a - (b-3) = a - b + 3$ is a multiple of 3
$a - b - 3$ is a multiple of 3
$(a-1) - (b-1) = a - b$ is a multiple of 3
$(a+1) - (b+1) = a - b$ is a multiple of 3
so if we apply our rules to an element of L, they produce elements of L. Since all of the elements initially in our set are in L, all of the elements added to our set are also in L. Thus, $L' \subset L$.

(c) **[6 Pts]** Prove that $L \subseteq L'$.
Let (x,y) be an arbitrary element of L. We show that (x,y) is an element of L', by constructing it using the rules of L'. Since $(x,y) \in L$, $x-y$ is a multiple of 3, so we can write y as $x - 3k$. We break it into four cases:

Case 1 ($x \geq 0$ and $k \geq 0$): we move from (0, 0) to $(x, x-3k)$ by first using the rule $(a+1, b+1)$ x times, then using the rule $(a, b-3)$ k times.

Case 2 ($x \geq 0$ and $k < 0$): we move from (0, 0) to $(x, x-3k)$ by first using the rule $(a+1, b+1)$ x times, then using the rule $(a, b+3)$ $-k$ times.

Case 3 ($x < 0$ and $k \geq 0$): we move from (0, 0) to $(x, x-3k)$ by first using the rule $(a-1, b-1)$ $-x$ times, then using the rule $(a, b-3)$ k times.

Case 4 ($x < 0$ and $k < 0$): we move from (0, 0) to $(x, x-3k)$ by first using the rule $(a1, b1)$ $-x$ times, then using the rule $(a, b+4)$ $-k$ times.

By this process we can reach any (x, y) in L, so $L \subseteq L'$.