Solutions for Problem Set 3
CS 373: Theory of Computation

Assigned: January 31, 2013 Due on: February 7, 2013

Recommended Reading: Lectures 5 and 6.

Problem 1. [Category: Comprehension+Design+Proof] An ***all***-NFA M is a 5 tuple $(Q, \Sigma, \delta, q_0, F)$ like an NFA, where Q is a finite set of states, Σ is the input alphabet, $\delta : Q \times (\Sigma \cup \{\epsilon\}) \to 2^Q$ is the transition function, $q_0 \in Q$ is the initial state, and $F \subseteq Q$ is the set of final states. The only difference between an ***all***-NFA and an NFA is that M accepts $u \in \Sigma^*$ iff every possible state that M could be in after reading u is in F (and at least one state is in F, i.e., all threads cannot die).

1. Taking $q_1 \xrightarrow{w}_M q_2$ to be the same as definition 4 in lecture 4, define formally when an ***all***-NFA M accepts u, and the language recognized by M (definitions similar to definitions 5 and 6 in lecture 4). **[2 points]**
2. Give a formal definition of a DFA dfa(M) such that $\mathbf{L}(\text{dfa}(M)) = \mathbf{L}(M)$. Prove that your construction is correct. **[3+5 points]**

Solution:

1. An ***all***-NFA M accepts w iff there is $q \in F$ such that $q_0 \xrightarrow{w}_M q$ and for every q' if $q_0 \xrightarrow{w}_M q'$ then $q' \in F$. We could also define it using $\hat{\delta}$ as follows. Let $\hat{\delta}_M(q_1, w) = \{q_2 \in Q \mid q_1 \xrightarrow{w}_M q_2\}$. Then M accepts w iff $\hat{\delta}_M(q_0, w) \neq \emptyset$ and $\hat{\delta}_M(q_0, w) \subseteq F$.

   The language accepted/recognized by M is given by

   $$\mathbf{L}(M) = \{w \in \Sigma^* \mid M \text{ accepts } w\}$$

2. The DFA that recognizes the same language as M is going to have the same states and transitions as the DFA that we constructed for NFAs. The only difference will be in terms of the final states. Formally the DFA dfa$(M) = (2^Q, \Sigma, \delta', q_0', F')$ where

   - $q_0' = \hat{\delta}_M(q_0, \epsilon)$
   - $F' = 2^F \setminus \{\emptyset\}$, i.e., it is the set of all non-empty subsets of F.
   - $\delta'(A, a) = \cup_{q \in A} \hat{\delta}_M(q, a)$

   The correctness proof is identical to the correctness proof the DFA constructed which is equivalent to NFAs. Recall from lecture 5, for an NFA N and DFA dfa(N) we can prove

   - $\forall w \in \Sigma^*$, $\hat{\delta}_{\text{det}(N)}(q_0', w) = \{A\}$ iff $\hat{\delta}_N(q_0, w) = A$.

   Since for an all-NFA M, the DFA construction is the same in terms of states and transtions, this property holds here as well (and we don't need to reprove it). That is,

   $$\forall w \in \Sigma^*,\ \hat{\delta}_{\text{det}(M)}(q_0', w) = \{A\} \text{ iff } \hat{\delta}_M(q_0, w) = A$$

Using this observation correctness can be established as follows:

$$\begin{array}{llll} w \in \mathbf{L}(M) & \text{iff} & \hat{\delta}_M(q_0, w) = A \text{ and } A \neq \emptyset \text{ and } A \subseteq F & \text{defn. of acceptance} \\ & \text{iff} & \hat{\delta}_{\det(M)}(q_0', w) = \{A\} \text{ and } A \neq \emptyset \text{ and } A \subseteq F & \text{correctness property above} \\ & \text{iff} & \hat{\delta}_{\det(M)}(q_0', w) = \{A\} \text{ and } A \in F' & \text{defn. of } F' \\ & \text{iff} & w \in \mathbf{L}(\det(M)) & \text{defn. of language} \end{array}$$

■

Problem 2. [Category: Comprehension+Design]

1. Describe the language of the following regular expressions. A clear, crisp one-level interpretable English description is acceptable, like "This is the set of all binary strings with at least three 0s and at most hundred 1s", or like "$\{0^n(10)^m \mid n \text{ and } m \text{ are integers}\}$". A vague, recursive or multi-level-interpretable description is not, like "This is a set of binary strings that starts and ends in 1, and the rest of the string starts and ends in 0, and the remainder of the string is a smaller string of the same form!" or "This is a set of strings like 010, 00100, 0001000, and so on!". You need not prove the correctness of your answer.
   - (a) $0^*(10^*)^*$ **[1 points]**
   - (b) $0(10)^*1$ **[2 points]**
   - (c) $c^*(a \cup (bc^*))^*$ **[2 points]**
2. Give regular expressions that accurately describe the following languages. You need not prove the correctness of your answer.
   - (a) All binary strings with no more than three 0s. **[1 points]**
   - (b) All binary strings that have two or three occurrences of 1 such that the first and the second occurrence (of 1) are not consecutive. **[2 points]**
   - (c) All binary strings with exactly one occurrence of the substring 000. **[2 points]**

Solution: 1(a) The set of all binary strings.

1(b) The set of all binary strings with alternating 0s and 1s, which begin with a 0 and end with a 1.

1(c) The set of all strings over alphabet $\{a, b, c\}$ that do not have ac as substring.

2(a) $1^*(0 \cup \epsilon)1^*(0 \cup \epsilon)1^*(0 \cup \epsilon)1^*$

2(b) $0^*10^*010^*(10^* \cup \epsilon)$

2(c) $(1 \cup 01 \cup 001)^*000(1 \cup 01 \cup 001)^*(\epsilon \cup 0 \cup 00)$ ■

Problem 3. [Category: Proof] Let r and s be regular expressions. Consider the equation $X = rX \cup s$. A regular expression t is a solution to this equation if $t = rt \cup s$ (i.e., $\mathbf{L}(t) = \mathbf{L}(rt \cup s)$).

1. Assuming that $\epsilon \notin \mathbf{L}(r)$, prove that if t is a solution to the above equation then $\mathbf{L}(t) = \mathbf{L}(r^*s)$. **[7 points]**

   Hint: To show that $\mathbf{L}(t) \subseteq \mathbf{L}(r^*s)$, first show that $\mathbf{L}(t) \subseteq \mathbf{L}(r^n t \cup r^{n-1}s \cup \ldots \cup s)$, for all $n \geq 0$. What can you say about strings $w \in L$ such that $|w| < n$?

2. If $\epsilon \in \mathbf{L}(r)$ then the equation need not have a unique solution. Assuming $\epsilon \in \mathbf{L}(r)$, give a solution for $X = rX \cup s$ that does not depend on r or s. **[3 points]**

Solution: Part 1: We will show that $\mathbf{L}(r^*s) \subseteq \mathbf{L}(t)$ and $\mathbf{L}(t) \subseteq \mathbf{L}(r^*s)$, where t is a solution to the equation $t = rt \cup s$. Let us start with the first direction. Observe that $\mathbf{L}(r^*s) = \cup_{i\geq 0}(\mathbf{L}(r))^i\mathbf{L}(s)$. We will prove by induction on i that $(\mathbf{L}(r))^i\mathbf{L}(s) \subseteq \mathbf{L}(t)$; proving this establishes $\mathbf{L}(r^*s) \subseteq \mathbf{L}(t)$.

Base Case: When $i = 0$, $\mathbf{L}(r)^0\mathbf{L}(s) = \mathbf{L}(s)$. Since $t = rt \cup s$, we have $\mathbf{L}(s) \subseteq \mathbf{L}(t)$, which establishes the base case.

Induction Step: We assume that $\mathbf{L}(r)^i\mathbf{L}(s) \subseteq \mathbf{L}(t)$. Observe that $\mathbf{L}(r)^{i+1}\mathbf{L}(s) = \mathbf{L}(r)[\mathbf{L}(r)^i\mathbf{L}(s)] \subseteq \mathbf{L}(r)\mathbf{L}(t) = \mathbf{L}(rt)$. Since $t = rt \cup s$, $\mathbf{L}(rt) \subseteq \mathbf{L}(s)$, and so $(\mathbf{L}(r))^{i+1}\mathbf{L}(s) \subseteq \mathbf{L}(t)$.

$\mathbf{L}(t) \subseteq \mathbf{L}(r^*s)$**:** Let us assume that the hint holds, i.e., $\mathbf{L}(t) \subseteq \mathbf{L}(r^n t \cup r^{n-1}s \cup \cdots \cup s)$. We will first show how the hint can be used to establish that $\mathbf{L}(t) \subseteq \mathbf{L}(r^*s)$. Observe that since $\epsilon \notin \mathbf{L}(r)$, we can conclude that all strings in $\mathbf{L}(r^n t)$ have length at least n. Consider a string $w \in \mathbf{L}(t)$ such that $|w| = n$. From the hint, it follows that $w \in \mathbf{L}(r^{n+1}t \cup r^n s \cup \cdots \cup s)$. But since all strings in $\mathbf{L}(r^{n+1}t)$ have length at least $n+1$, $w \notin \mathbf{L}(r^{n+1}t)$ and so $w \in \mathbf{L}(r^n s \cup \cdots \cup s)$. Thus, $w \in \mathbf{L}(r^*s)$.

To complete the proof we need to prove the hint. We will prove "$\mathbf{L}(t) \subseteq \mathbf{L}(r^n t \cup r^{n-1}s \cup \cdots \cup s)$" by induction on n. For the base case, $n = 1$, observe that $\mathbf{L}(r^n t \cup r^{n-1}s \cup \cdots \cup s) = \mathbf{L}(rt \cup s)$, and since $\mathbf{L}(t) = \mathbf{L}(rt \cup s)$, the base case holds. Assume that $\mathbf{L}(t) \subseteq \mathbf{L}(r^n t \cup r^{n-1}s \cup \cdots \cup s)$. Observe that

$$\begin{array}{lll}
\mathbf{L}(t) & \subseteq \mathbf{L}(rt \cup s) & \text{(defn. of } t\text{)} \\
& \subseteq \mathbf{L}(r[r^n t \cup r^{n-1}s \cup \cdots s] \cup s) & \text{(ind. hyp.)} \\
& = \mathbf{L}(r^{n+1}t \cup r^n s \cup \cdots \cup s) & \text{(defn.)}
\end{array}$$

Alternate Proof for $\mathbf{L}(t) \subseteq \mathbf{L}(r^*s)$: Here is an alternate proof for this direction that does not use the hint provided in the problem. This proof is due to Jordan Luber. Before presenting this proof, we need a couple definitions.

Recall that a string v is a suffix of w if there is some string u such that $w = uv$. We say that v is a *proper suffix* of w if v is a suffix of w and $w \neq v$. For a language L and string w, let us denote by $ps_L(w)$ the number of proper suffixes of w in L. Or more formally,

$$ps_L(w) = |\{v \in L \mid v \text{ is a proper suffix of } w\}|$$

We are ready now to prove the result. Let w be an arbitrary string in $\mathbf{L}(t)$. We will prove by induction on $ps_{\mathbf{L}(t)}(w)$ that $w \in \mathbf{L}(r^*s)$.

Base Case: Consider $w \in \mathbf{L}(t)$ such that $ps_{\mathbf{L}(t)}(w) = 0$. Now since $w \in \mathbf{L}(t)$ and $\mathbf{L}(t) = \mathbf{L}(r)\mathbf{L}(t) \cup \mathbf{L}(s)$, it means that either $w \in \mathbf{L}(s)$ or $w \in \mathbf{L}(r)\mathbf{L}(t)$. Now if $w \in \mathbf{L}(r)\mathbf{L}(t)$ then $w = uv$ where $u \in \mathbf{L}(r)$ and $v \in \mathbf{L}(t)$. Moreover, since $\epsilon \notin \mathbf{L}(r)$, $u \neq \epsilon$ which means that v is a proper suffix of w and so $ps_{\mathbf{L}(t)}(w) \neq 0$. Thus, for $w \in \mathbf{L}(t)$, if $ps_{\mathbf{L}(t)}(w) = 0$ then $w \in \mathbf{L}(s)$. In addition, since $\mathbf{L}(s) \subseteq \mathbf{L}(r^*s)$, we have $w \in \mathbf{L}(r^*s)$.

Induction Step: We will assume that if $w \in \mathbf{L}(t)$ and $ps_{\mathbf{L}(t)}(w) < n$ then $w \in \mathbf{L}(r^*s)$. Consider $w \in \mathbf{L}(t)$ with $ps_{\mathbf{L}(t)}(w) = n$. Once again, since $\mathbf{L}(t) = \mathbf{L}(r)\mathbf{L}(t) \cup \mathbf{L}(s)$, it means that either $w \in \mathbf{L}(s)$ or $w \in \mathbf{L}(r)\mathbf{L}(t)$. If $w \in \mathbf{L}(s)$ then since $\mathbf{L}(s) \subseteq \mathbf{L}(r^*s)$, we have $w \in \mathbf{L}(r^*s)$. On the other hand, suppose $w \in \mathbf{L}(r)\mathbf{L}(t)$ then there are u, v such that $w = uv$ and $u \in \mathbf{L}(r)$ and $v \in \mathbf{L}(t)$. Since $\epsilon \notin \mathbf{L}(r)$, we have v is a proper suffix of w. In addition, every proper suffix of v in $\mathbf{L}(t)$ is also a proper suffix of w and therefore,

$ps_{\mathbf{L}(t)}(v) < ps_{\mathbf{L}(t)}(w) = n$. Thus, by the induction hypothesis, $v \in \mathbf{L}(r^*s)$. Since $w = uv$ and $u \in \mathbf{L}(r)$, we have $w \in \mathbf{L}(r)\mathbf{L}(r^*s) \subseteq \mathbf{L}(r^*s)$. Hence the induction step is established.

Part 2: Observe that $r(\Sigma^*) \cup s = \Sigma^*$ when $\epsilon \in \mathbf{L}(r)$; thus, Σ^* is a solution to the equation. ■