Spring 2010 CIS 511

Introduction to the Theory of Computation
Jean Gallier

Homework 1

January 14, 2010; Due February 4, 2010
Beginning of class

"A problems" are for practice only, and should not be turned in.

Problem A1. Given an alphabet Σ, prove that the relation $\leq_1$ over Σ^* defined such that $u \leq_1 v$ iff u is a prefix of v, is a partial ordering. Prove that the relation $\leq_2$ over Σ^* defined such that $u \leq_2 v$ iff u is a substring of v, is a partial ordering.

Problem A2. Given an alphabet Σ, for any language $L \subseteq \Sigma^*$, prove that $L^{**} = L^*$ and $L^* L^* = L^*$.

Problem A3. Let $D = (Q, \Sigma, \delta, q_0, F)$ be a DFA. Prove that for all $p \in Q$ and all $u, v \in \Sigma^*$,

$$\delta^*(p, uv) = \delta^*(\delta^*(p, u), v).$$

"B problems" must be turned in.

Problem B1 (30 pts). Let $D = (Q, \Sigma, \delta, q_0, F)$ be a DFA. Recall that a state $p \in Q$ is *accessible* or *reachable* iff there is some string $w \in \Sigma^*$, such that

$$\delta^*(q_0, w) = p,$$

i.e., there is some path from q_0 to p in D. Consider the following method for computing the set Q_r of reachable states (of D): define the sequence of sets $Q_r^i \subseteq Q$, where

$Q_r^0 = \{q_0\}$,

$Q_r^{i+1} = \{q \in Q \mid \exists p \in Q_r^i, \exists a \in \Sigma,\ q = \delta(p, a)\}$.

(i) Prove by induction on i that Q_r^i is the set of all states reachable from q_0 using paths of length i (where i counts the number of edges).

Give an example of a DFA such that $Q_r^{i+1} \neq Q_r^i$ for all $i \geq 0$.

(ii) Give an example of a DFA such that $Q_r^i \neq Q_r$ for all $i \geq 0$.

(iii) Change the inductive definition of Q_r^i as follows:

$$Q_r^{i+1} = Q_r^i \cup \{q \in Q \mid \exists p \in Q_r^i, \exists a \in \Sigma,\ q = \delta(p, a)\}.$$

Prove that there is a smallest integer i_0 such that

$$Q_r^{i_0+1} = Q_r^{i_0} = Q_r.$$

Define the DFA D_r as follows: $D_r = (Q_r, \Sigma, \delta_r, q_0, F \cap Q_r)$, where $\delta_r \colon Q_r \times \Sigma \to Q_r$ is the restriction of δ to Q_r. Explain why D_r is indeed a DFA, and prove that $L(D_r) = L(D)$. A DFA is said to be *reachable, or trim*, if $D = D_r$.

Problem B2 (20 pts). Given a string w, its reversal w^R is defined inductively as follows: $\epsilon^R = \epsilon$ and $(ua)^R = au^R$, where $a \in \Sigma$ and $u \in \Sigma^*$. Prove that $(uv)^R = v^R u^R$. Prove that $(w^R)^R = w$.

Problem B3 (20 pts). Construct DFA's for the following languages:
(a) $\{w \mid w \in \{a, b\}^*,\ w$ has neither aa nor bb as a substring$\}$.
(b) $\{w \mid w \in \{a, b\}^*,\ w$ has an even number of a's and an odd number of b's$\}$.

Problem B4 (30 pts). Given any alphabet Σ, prove the following property: for any two strings $u, v \in \Sigma^*$, $uv = vu$ iff there is some $w \in \Sigma^*$ such that $u = w^m$ and $v = w^n$, for some $m, n \geq 0$.

Problem B5 (40 pts). (a) For any language $L \subseteq \{a\}^*$, prove that if $L = L^*$, then there is a finite language $S \subseteq L$ such that $L = S^*$. Prove that L is regular.

(b) Let $L \subseteq \{a\}^*$ be any infinite regular language. Prove that there is a finite set $F \subseteq \{a\}^*$, and some strings a^m, $a^{p_1}, \ldots, a^{p_k}$, and $a^q \neq \epsilon$, with $0 \leq p_1 < p_2 < \ldots < p_k < q$, such that

$$L = F \cup \bigcup_{i=1}^{k} a^{m+p_i}\{a^q\}^*.$$

Problem B6 (40 pts). Given any two relatively prime integers $p, q \geq 0$, with $p \neq q$, (p and q are relatively prime iff their greatest common divisor is 1), consider the language $L = \{a^p, a^q\}^*$. Prove that

$$\{a^p, a^q\}^* = \{a^n \mid n \geq (p-1)(q-1)\} \cup F,$$

where F is some finite set of strings (of length $< pq$). Prove that L is a regular language.

Extra Credit (20 pts). Given any two relatively prime integers $p, q \geq 0$, with $p \neq q$, prove that $pq - p - q = (p-1)(q-1) - 1$ is the largest integer not expressible as $ph + kq$ with $h, k \geq 0$.

Problem B7 (40 pts). (*Ultimate periodicity*) A subset U of the set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ of natural numbers is *ultimately periodic* if there exist $m, p \in \mathbb{N}$, with $p \geq 1$, so that $n \in U$ iff $n + p \in U$, for all $n \geq m$.

(i) Prove that $U \subseteq \mathbb{N}$ is ultimately periodic iff either U is finite or there is a finite subset $F \subseteq \mathbb{N}$ and there are $k \leq p$ numbers $m_1, \ldots, m_k$, with $m_1 < m_2 < \cdots < m_k < m_1 + p$, and with m_1 the smallest element of U so that for some $p \geq 1$, $n \in U$ iff $n + p \in U$, for all $n \geq m_1$, so that

$$U = F \cup \bigcup_{i=1}^{k} \{m_i + jp \mid j \in \mathbb{N}\}.$$

Give an example of an ultimately periodic set U such that m and p are not necessarily unique, i.e., U is ultimately periodic with respect to m_1, p_1 and m_2, p_2, with $m_1 \neq m_2$ and $p_1 \neq p_2$.

Remark: A subset of $\mathbb{N}$ of the form $\{m + ip \mid i \in \mathbb{N}\}$ (allowing $p = 0$) is called a *linear set*, and a finite union of linear sets is called a *semilinear set*. Thus, (i) says that a set is ultimately periodic iff it is semilinear.

(ii) Let $L \subseteq \{a\}^*$ be a language over the one-letter alphabet $\{a\}$. Prove that L is a regular language iff the set $\{m \in \mathbb{N} \mid a^m \in L\}$ is ultimately periodic. Prove that the family of semilinear sets is closed under union, intersection and complementation (i.e., it is a boolean algebra).

(iii) Let $L \subseteq \Sigma^*$ be a regular language over any alphabet Σ (not necessarily consisting of a single letter). Prove that the set

$$|L| = \{|w| \mid w \in L\}$$

is ultimately periodic.

TOTAL: 220 + 20 points.