Fall, 2021   CIS 511

Introduction to the Theory of Computation
Jean Gallier

Homework 3

October 11, 2021; Due October 25, 2021

Problem B1 (60 pts). Let $D = (Q, \Sigma, \delta, q_0, F)$ be a *trim* DFA. Consider the following procedure:

(1) Form an NFA, N^R, by reversing all the transitions of D, i.e., there is a transition from p to q on input $a \in \Sigma$ in N iff $\delta(q, a) = p$ in D.

(2) Apply the subset construction to the NFA, N^R, obtained in (1), taking the start state to be the set F. The final states of the DFA obtained by applying the subset construction to N^R are all the subsets containing q_0. Then, trim the resulting DFA, to obtain the DFA D^R.

Observe that $L(D^R) = L(D)^R$.

Now, apply the above procedure to D, getting D^R, and apply this procedure again, to get D^{RR}. Prove that D^{RR} is a minimal DFA for $L = L(D)$.

Hint. First prove that if δ_R is the transition function of D^R, then for every $w \in \Sigma^*$ and for every state, $T \subseteq Q$, of D^R,

$$\delta_R^*(T, w) = \{q \in Q \mid \delta^*(q, w^R) \in T\}.$$

Problem B2 (60 pts). Let $D = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite automaton. Define the relations $\approx$ and $\sim$ on Σ^* as follows:

$$\begin{aligned} x \approx y \quad \text{if and only if,} \quad & \text{for all} \quad p \in Q, \\ & \delta^*(p, x) \in F \quad \text{iff} \quad \delta^*(p, y) \in F, \end{aligned}$$

and

$$x \sim y \quad \text{if and only if,} \quad \text{for all} \quad p \in Q, \quad \delta^*(p, x) = \delta^*(p, y).$$

(1) Show that $\approx$ is a left-invariant equivalence relation and that $\sim$ is an equivalence relation that is both left and right invariant. (A relation R on Σ^* is *left invariant* iff uRv implies that $wuRwv$ for all $w \in \Sigma^*$, and R is *left and right invariant* iff uRv implies that $xuyRxvy$ for all $x, y \in \Sigma^*$.)

(2) Let n be the number of states in Q (the set of states of D). Show that $\approx$ has at most 2^n equivalence classes and that $\sim$ has at most n^n equivalence classes.

Hint. In the case of $\approx$, consider the function $f\colon \Sigma^* \to 2^Q$ given by

$$f(u) = \{p \in Q \mid \delta^*(p, u) \in F\}, \quad u \in \Sigma^*,$$

and show that $x \approx y$ iff $f(x) = f(y)$. In the case of $\sim$, let Q^Q be the set of all functions from Q to Q and consider the function $g\colon \Sigma^* \to Q^Q$ defined such that $g(u)$ is the function given by

$$g(u)(p) = \delta^*(p, u), \quad u \in \Sigma^*,\ p \in Q,$$

and show that $x \sim y$ iff $g(x) = g(y)$.

(3) Given any language $L \subseteq \Sigma^*$, define the relations λ_L and μ_L on Σ^* as follows:

$$u \,\lambda_L\, v \quad \text{iff,} \quad \text{for all} \quad z \in \Sigma^*, \quad zu \in L \quad \text{iff} \quad zv \in L,$$

and

$$u \,\mu_L\, v \quad \text{iff,} \quad \text{for all} \quad x, y \in \Sigma^*, \quad xuy \in L \quad \text{iff} \quad xvy \in L.$$

Prove that λ_L is left-invariant, and that μ_L is left and right-invariant. Prove that if L is regular, then both λ_L and μ_L have a finite number of equivalence classes.

Hint: Show that the number of classes of λ_L is at most the number of classes of $\approx$, and that the number of classes of μ_L is at most the number of classes of $\sim$.

Problem B3 (100 pts). Which of the following languages are regular? Justify each answer.

(1) $L_1 = \{wcw \mid w \in \{a, b\}^*\}$. (here $\Sigma = \{a, b, c\}$).

(2) $L_2 = \{xy \mid x, y \in \{a, b\}^* \text{ and } |x| = |y|\}$. (here $\Sigma = \{a, b\}$)

(3) $L_3 = \{a^n \mid n \text{ is a prime number}\}$. (here $\Sigma = \{a\}$).

(4) $L_4 = \{a^m b^n \mid gcd(m, n) = 23\}$. (here $\Sigma = \{a, b\}$).

(5) Consider the language

$$L_5 = \{a^{4n+3} \mid 4n + 3 \text{ is prime}\}.$$

Assuming that L_5 is infinite, prove that L_5 is not regular.

(6) Let $F_n = 2^{2^n} + 1$, for any integer $n \geq 0$, and let

$$L_6 = \{a^{F_n} \mid n \geq 0\}.$$

Here $\Sigma = \{a\}$.

Extra Credit (from 10 up to 10^{100} pts). Find explicitly what F_0, F_1, F_2, F_3 are, and check that they are prime. What about F_4 and F_5?

Is the language

$$L_7 = \{a^{F_n} \mid n \geq 0,\ F_n \text{ is prime}\}$$

regular?

Extra Credit (20 pts). Prove that there are infinitely many primes of the form $4n + 3$.

The list of such primes begins with

$$3,\ 7,\ 11,\ 19,\ 23,\ 31,\ 43, \cdots$$

Say we already have $n + 1$ of these primes, denoted by

$$3,\ p_1,\ p_2, \cdots, p_n,$$

where $p_i > 3$. Consider the number

$$m = 4p_1p_2 \cdots p_n + 3.$$

If $m = q_1 \cdots q_k$ is a prime factorization of m, prove that $q_j > 3$ for $j = 1, \ldots k$ and that no q_j is equal to any of the p_i's. Prove that one of the q_j's must be of the form $4n+3$, which shows that there is a prime of the form $4n + 3$ greater than any of the previous primes of the same form.

Problem B4 (80 pts). This problem illustrates the power of the congruence version of Myhill-Nerode.

Recall that the reversal of a string, $w \in \Sigma^*$, is defined inductively as follows:

$$\epsilon^R = \epsilon$$
$$(ua)^R = au^R,$$

for all $u \in \Sigma^*$ and all $a \in \Sigma$.

Let $\sim$ be a congruence (on Σ^*) and assume that $\sim$ has n equivalence classes. Define $\sim_R$ and $\approx$ by

$$u \sim_R v \quad \text{iff} \quad u^R \sim v^R, \quad \text{for all } u, v \in \Sigma^* \quad \text{and} \quad \approx = \sim \cap \sim_R .$$

(1) Prove that the equivalence class $[u]_{\sim_R}$ of any string $u \in \Sigma^*$ is given by

$$[u]_{\sim_R} = ([u^R]_{\sim})^R.$$

Consider the map $\rho\colon (\Sigma^*/\sim_R) \to (\Sigma^*/\sim)$ given by

$$\rho([u]_{\sim_R}) = [u^R]_{\sim}.$$

Prove that

$$\rho([u]_{\sim_R}) = ([u]_{\sim_R})^R,$$

which shows that the map ρ is well defined.

(2) Prove that ρ is bijective. Prove that $\sim$ and $\sim_R$ have the same number of equivalence classes.

(3) Prove that the relation $\approx$ is a congruence. Prove that $\approx$ has at most n^2 equivalence classes.

(4) Given any regular language L over Σ^* let

$$L^{(1/2)} = \{w \in \Sigma^* \mid ww^R \in L\}.$$

Prove that $L^{(1/2)}$ is also regular using the relation $\approx$ of part (1).

(5) Let L be any regular language over some alphabet Σ. For any natural number $k \geq 2$, let

$$L^{(1/k)} = \{w \in \Sigma^* \mid (ww^R)^{k-1} \in L\} = \{w \in \Sigma^* \mid \underbrace{ww^R ww^R \cdots ww^R}_{k-1} \in L\}.$$

Also the languages $L^{1/\infty}$ and L^∞ are defined by

$$\begin{aligned} L^{1/\infty} &= \{w \in \Sigma^* \mid (ww^R)^{k-1} \in L, \quad \text{for all } k \geq 2\}, \quad \text{and} \\ L^{\infty} &= \{w \in \Sigma^* \mid (ww^R)^{k-1} \in L, \quad \text{for some } k \geq 2\}. \end{aligned}$$

Prove that every language $L^{(1/k)}$ is regular.

(6) Prove that there are only finitely many distinct languages of the form $L^{(1/k)}$ (this means that the set of languages $\{L^{(1/k)}\}_{k\geq 2}$ is finite). Prove that $L^{1/\infty}$ and L^∞ are regular.

TOTAL: 300 + 40 points.