

Introduction to the Theory of Computation

Jean Gallier

Homework 3

February 19, 2009; Due March 5, 2009

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

Problem A1. Prove that every finite language is regular.

Problem A2. Sketch an algorithm for deciding whether two regular expressions R, S are equivalent (i.e, whether $\mathcal{L}[R] = \mathcal{L}[S]$).

Problem A3. Given any language $L \subseteq \Sigma^*$, let

$$L^R = \{w^R \mid w \in L\},$$

the *reversal language of L* (where w^R denotes the reversal of the string w). Prove that if L is regular, then L^R is also regular.

“B problems” must be turned in.

Problem B1 (40 pts). (*Ultimate periodicity*) A subset U of the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ 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, \dots, m_k , with $m_1 < m_2 < \dots < m_k < m_1 + p$, 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.

Problem B2 (40 pts). Let $D = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite automaton. Define the relations \approx and \sim on Σ^* as follows:

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

and

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

(a) 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 $wuRvw$ for all $w \in \Sigma^*$, and R is *right invariant* iff uRv implies that $uwRvw$ for all $w \in \Sigma^*$.)

(b) 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.

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

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

and

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

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 (60 pts). Let L be any regular language over some alphabet Σ . Define the languages

$$\begin{aligned} L^\infty &= \bigcup_{k \geq 1} \{w^k \mid w \in L\}, \\ L^{1/\infty} &= \{w \mid w^k \in L, \text{ for all } k \geq 1\}, \text{ and} \\ \sqrt{L} &= \{w \mid w^k \in L, \text{ for some } k \geq 1\}. \end{aligned}$$

Also, for any natural number $k \geq 1$, let

$$L^{(k)} = \{w^k \mid w \in L\},$$

and

$$L^{(1/k)} = \{w \mid w^k \in L\}.$$

(a) Prove that $L^{(1/3)}$ is regular. What about $L^{(3)}$?

(b) Let $k \geq 1$ be any natural number. Prove that there are only finitely many languages of the form $L^{(1/k)} = \{w \mid w^k \in L\}$ and that they are all regular. (In fact, if L is accepted by a DFA with n states, there are at most 2^{n^k} languages of the form $L^{(1/k)}$).

(c) Is $L^{1/\infty}$ regular or not? Is \sqrt{L} regular or not? What about L^∞ ?

Problem B4 (40 pts). Which of the following languages are regular? Justify each answer.

(a) $L_1 = \{w^k \mid w \in \{a, b\}^*\}$

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

(c) $L_3 = \{a^n \mid n \text{ is a prime number}\}$

(d) $L_4 = \{a^m b^n \mid \gcd(m, n) = 17\}$.

Problem B5 (40 pts). (a) Prove again that the intersection, $L_1 \cap L_2$, of two regular languages, L_1 and L_2 , is regular, **using the Myhill-Nerode characterization** of regular languages.

(b) Let $h: \Sigma^* \rightarrow \Delta^*$ be a homomorphism, as defined on pages 24-26 of the slides on DFA's and NFA's. For any regular language, $L' \subseteq \Delta^*$, prove that $h^{-1}(L')$ is regular, **using the Myhill-Nerode characterization** of regular languages. Prove that the number of states of any minimal DFA for $h^{-1}(L')$ is at most the number of states of any minimal DFA for L' . Can it be strictly smaller?

Problem B6 (50 pts). The purpose of this problem is to get a fast algorithm for testing state equivalence in a DFA. Let $D = (Q, \Sigma, \delta, q_0, F)$ be a deterministic finite automaton. Recall that *state equivalence* is the equivalence relation \equiv on Q , defined such that,

$$p \equiv q \quad \text{iff} \quad \forall z \in \Sigma^* (\delta^*(p, z) \in F \quad \text{iff} \quad \delta^*(q, z) \in F).$$

and that *i-equivalence* is the equivalence relation \equiv_i on Q , defined such that,

$$p \equiv_i q \quad \text{iff} \quad \forall z \in \Sigma^*, |z| \leq i (\delta^*(p, z) \in F \quad \text{iff} \quad \delta^*(q, z) \in F).$$

A relation $S \subseteq Q \times Q$ is a *forward closure* iff it is an equivalence relation and whenever $(p, q) \in S$, then $(\delta(p, a), \delta(q, a)) \in S$, for all $a \in \Sigma$.

We say that a forward closure S is *good* iff whenever $(p, q) \in S$, then $good(p, q)$, where $good(p, q)$ holds iff either both $p, q \in F$, or both $p, q \notin F$.

Given any relation $R \subseteq Q \times Q$, recall that the smallest equivalence relation R_{\approx} containing R is the relation $(R \cup R^{-1})^*$ (where $R^{-1} = \{(q, p) \mid (p, q) \in R\}$, and $(R \cup R^{-1})^*$ is the reflexive and transitive closure of $(R \cup R^{-1})$). We define the sequence of relations $R_i \subseteq Q \times Q$ as follows:

$$R_0 = R_{\approx}$$

$$R_{i+1} = (R_i \cup \{(\delta(p, a), \delta(q, a)) \mid (p, q) \in R_i, a \in \Sigma\})_{\approx}.$$

(i) Prove that $R_{i_0+1} = R_{i_0}$ for some least i_0 . Prove that R_{i_0} is the smallest forward closure containing R .

We denote the smallest forward closure R_{i_0} containing R as R^\dagger , and call it the *forward closure of R* .

(ii) Prove that $p \equiv q$ iff the forward closure R^\dagger of the relation $R = \{(p, q)\}$ is good.

TOTAL: 270 points.