

Introduction to the Theory of Computation

Jean Gallier

Homework 3

February 19, 2004; Due March 4, 2004

“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 (100 pts). Let $D = (Q, \Sigma, \delta, q_0, F)$ be a DFA with n states, say q_1, \dots, q_n , where q_1 is the start state (Note, we denote the start state q_1 , not q_0 !) We associate with D the $n \times n$ boolean matrix, Δ_D , defined such that

$$\Delta_D(q_i, q_j) = \begin{cases} 1 & \text{if } (\exists a \in \Sigma)(\delta(q_i, a) = q_j), \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $\Delta_D(q_i, q_j) = 1$ iff there is some edge from q_i to q_j (regardless of the label of that edge). Add and multiply matrices treating $\{0, 1\}$ as truth values, i.e.

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 1$$

$$00 = 0$$

$$01 = 0$$

$$10 = 0$$

$$11 = 1.$$

(In other words, $\{0, 1\}$ is the two-element boolean ring).

(a) Prove that Δ_D^k gives the k -step reachability relation on D , i.e., $\Delta_D^k(q_i, q_j) = 1$ iff $\delta^*(q_i, w) = q_j$, for some string $w \in \Sigma^*$ with $|w| = k$ (We set $\Delta_D^0 = I$, the identity matrix).

Prove that there are only finitely many matrices Δ_D^k , where $k \geq 0$. For any $k \geq 0$, let

$$\Delta_D^{*[k]} = I + \Delta_D + \Delta_D^2 + \cdots + \Delta_D^k.$$

Prove that there is a smallest $k \leq n - 1$ so that $\Delta_D^{*[k]} = \Delta_D^{*[k+i]}$ for all $i \geq 1$. Let $\Delta_D^* = \Delta_D^{*[k]}$, for the above k . Prove that $\Delta_D^*(q_i, q_j) = 1$ iff $\delta^*(q_i, w) = q_j$, for some string $w \in \Sigma^*$.

For simplicity of notation, from now on drop the subscript D in Δ_D .

Warning: Questions (b)–(d) must be solved directly *without* appealing to the results of problem B2. Either construct DFA's or NFA's (which is very hard!) or use Myhill-Nerode (my advice).

(b) Prove that for any regular language, L , the languages

$$L_{2^n} = \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = 2^{|u|} \quad \text{and} \quad uv \in L)\}$$

and

$$L_{2^{2^n}} = \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = 2^{2^{|u|}} \quad \text{and} \quad uv \in L)\}$$

are also regular.

Hint: Use the Myhill-Nerode theorem, i.e., find a suitable right-invariant equivalence relation of finite index.

(c) Prove that for any regular language, L , the language

$$L_{n^2} = \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = |u|^2 \quad \text{and} \quad uv \in L)\}$$

is also regular.

Hint. Use the Myhill-Nerode theorem.

(d) Let $P(n)$ be any polynomial with integer coefficients, say $P(n) = a_0n^d + a_1n^{d-1} + \cdots + a_d$. Prove that for every regular language, L , and any polynomial, $P(n)$, the language

$$L_P = \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = P(|u|) \quad \text{and} \quad uv \in L)\}$$

is a regular language.

Hint. Use the Myhill-Nerode theorem.

Problem B2 (130 pts). Review the definition of an ultimately periodic subset of \mathbb{N} from Homework I, Problem B7. A function, $f: \mathbb{N} \rightarrow \mathbb{N}$ *preserves ultimate periodicity* iff $f^{-1}(U)$ is ultimately periodic whenever $U \subseteq \mathbb{N}$ is ultimately periodic.

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

$$\begin{aligned} L_f &= \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = f(|u|) \text{ and } uv \in L)\} \\ L'_f &= \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = f(|u|) \text{ and } v \in L)\}. \end{aligned}$$

(a) Assume that L is a regular language. Prove that for any function, $f: \mathbb{N} \rightarrow \mathbb{N}$, if f preserves ultimate periodicity then L'_f is regular.

(b) Prove that if L'_f is regular whenever L is regular, then L_f is regular whenever L is regular. Conclude that for any function, $f: \mathbb{N} \rightarrow \mathbb{N}$, if f preserves ultimate periodicity then L_f is regular.

(c) Prove that if L_f is regular whenever L is regular, then f preserves ultimate periodicity.

Therefore, L_f is regular whenever L is regular iff f preserves ultimate periodicity.

(d) Checking that a function preserves ultimate periodicity is usually difficult. Hence, it is desirable to find more convenient criteria for the preservation of ultimate periodicity. Such a criterion is given below.

For any two integers $m \geq 0$ and $p \geq 1$, let $[m]_p$ denote the set of integers congruent to m modulo p , i.e., $[m]_p = \{n \in \mathbb{N} \mid n = pi + m, i \in \mathbb{Z}\}$. (Note: \mathbb{Z} consists of the positive *and* negative integers, \mathbb{N} of the *non-negative* integers.) Check quickly that Homework I, Problem B7, asserts that every ultimately periodic subset, U , of \mathbb{N} can be written as

$$U = F \oplus \bigcup_{i=1}^k [m_i]_p,$$

for some $p \geq 1$ and some pairwise distinct m_i 's, with F a finite set disjoint from each of the $[m_i]_p$. Here $X \oplus Y = (X - Y) \cup (Y - X)$, the symmetric difference of X and Y , i.e., \oplus corresponds to *exclusive or*. Also, the set of ultimately periodic subsets of \mathbb{N} is the smallest family containing all the finite sets and the sets $[m]_p$ and closed under union, intersection and complementation. Check that if U and V are two (infinite) ultimately periodic sets with periods p_1 and p_2 , then $U \cup V$ is ultimately periodic with period $\text{lcm}(p_1, p_2)$.

We say that a function, $f: \mathbb{N} \rightarrow \mathbb{N}$, is *ultimately periodic modulo m* (with $m \geq 1$) iff there is some $p \geq 1$ and some $N \geq 0$ so that

$$f(n) \equiv f(n + p) \pmod{m}, \quad \text{for all } n \geq N.$$

Prove that a function, f , is ultimately periodic modulo m for all $m \geq 1$ iff $f^{-1}([i]_m)$ is ultimately periodic for all $i \geq 0$ and all $m \geq 1$.

Assume that the function, f , is ultimately periodic modulo m for all $m \geq 1$ and that $f^{-1}(\{n\})$ is ultimately periodic for every $n \in \mathbb{N}$. Then, prove that f preserves ultimate periodicity. Prove that f preserves ultimate periodicity iff

(i) The function, f , is ultimately periodic modulo m for all $m \geq 1$, and

(ii) The set $f^{-1}(\{n\})$ is ultimately periodic for every $n \in \mathbb{N}$.

Remark: Using the above, it is easy to show that the class of functions that preserve ultimate periodicity contains the functions, n^k , k^n (for any fixed $k > 1$), and is closed under composition, addition, multiplication and exponentiation.

(e) Reprove B1 using B2(b,d) (i.e., show that the languages L_{2^n} , $L_{2^{2^n}}$, L_{n^2} , L_P , are regular if L is regular).

(f) Prove that the function $f(n) = \log n$ does not preserve ultimate periodicity. Deduce that there are regular languages, L , for which

$$L_{\log n} = \{u \in \Sigma^* \mid (\exists v \in \Sigma^*)(|v| = \log(|u|) \text{ and } uv \in L)\}$$

is **not** regular.

Problem B3 (50 pts). Which of the following languages are regular? Justify each answer.

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

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

(e) $L_5 = \{ww^R \mid w \in L\}$, where L is some given regular language.

Problem B4 (60 pts). Let Σ be an alphabet. An equivalence relation on Σ^* that is both left and right-invariant is called a *congruence*. Prove that a congruence satisfies the property: If $u \sim u'$ and $v \sim v'$, then $uv \sim u'v'$. Also recall that the reversal of a string, $w \in \Sigma^*$, is defined inductively as follows:

$$\begin{aligned} \epsilon^R &= \epsilon \\ (ua)^R &= au^R, \end{aligned}$$

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

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

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

Prove that the relation \approx is a congruence and that \approx has at most n^2 equivalence classes.

(ii) 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 (i).

(iii) Let L be any regular language over some alphabet Σ . For any natural number $k \geq 1$, let

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

Also define the languages

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

Prove that there are only finitely many languages of the form $L^{(1/k)}$ and that they are all regular. Prove that $L^{1/\infty}$ and L^∞ are regular.

TOTAL: 340 points.