Spring, 2025 CIS 5110

Introduction to the Theory of Computation
Jean Gallier

Homework 3

February 27, 2025; Due March 27, 2025

Problem B1 (80 pts). (i) Prove that the conclusion of the pumping lemma holds for the following language L over $\{a,b\}^*$, and yet, L is **not** regular!

$$L = \{w \mid \exists n \geq 1, \exists x_i \in a^+, \exists y_i \in b^+, 1 \leq i \leq n, n \text{ is not prime}, w = x_1 y_1 \cdots x_n y_n\}.$$

(ii) Consider the following version of the pumping lemma. For any regular language L, there is some $m \geq 1$ so that for every $y \in \Sigma^*$, if $|y| = m$, then there exist $u, x, v \in \Sigma^*$ so that

(1) $y = uxv$;

(2) $x \neq \epsilon$;

(3) For all $z \in \Sigma^*$,
$$yz \in L \quad \text{iff} \quad ux^i vz \in L$$
for all $i \geq 0$.

Prove that this pumping lemma holds.

(iii) Prove that the converse of the pumping lemma in (ii) also holds, i.e., if a language L satisfies the pumping lemma in (ii), then it is regular.

(iv) Consider yet another version of the pumping lemma. For any regular language L, there is some $m \geq 1$ so that for every $y \in \Sigma^*$, if $|y| \geq m$, then there exist $u, x, v \in \Sigma^*$ so that

(1) $y = uxv$;

(2) $x \neq \epsilon$;

(3) For all $\alpha, \beta \in \Sigma^*$,
$$\alpha u \beta \in L \quad \text{iff} \quad \alpha u x^i \beta \in L$$
for all $i \geq 0$.

Prove that this pumping lemma holds.

(v) Prove that the converse of the pumping lemma in (iv) also holds, i.e., if a language L satisfies the pumping lemma in (iv), then it is regular.

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

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

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^n} languages of the form $L^{(1/k)}$).

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

TOTAL: 310 + 40 points.