Models of computation and finite automata

(MPRI course 2.16, 2021-2022)

Part II: Automata, Monoids and Logic - Problem Sheet 2

Exercise 1. In this exercise, let u, v be Σ-words and $\bar{p} \in |u|^n$, $\bar{q} \in |v|^n$. Recall that $\mathrm{FO}_{n,k}$ denotes the set of first-order formulas with free variables among $x_1, \ldots, x_n$ and of quantifier depth $\leq k$, and $\equiv_{n,k}$ denotes the equivalence relation of satisfying the same $\mathrm{FO}_{n,k}$-formulas.

a. Deduce from Exercise 10(b) of Exercise Sheet 1 that $u, \bar{p} \equiv_{n,k+1} v, \bar{q}$ holds if, and only if, both of the following conditions are satisfied:

- for every $p' \in |u|$, there exists $q' \in |v|$ such that $u, \bar{p}p' \equiv_{n+1,k} v, \bar{q}q'$, and
- for every $q' \in |v|$, there exists $p' \in |u|$ such that $u, \bar{p}p' \equiv_{n+1,k} v, \bar{q}q'$.

b. We say that $\bar{p}$ and $\bar{q}$ *induce the same ordering* if, for all $1 \leq i, j \leq n$, $p_i < p_j$ iff $q_i < q_j$, and p_j is the successor of p_i iff q_j is the successor of q_i. The *partition induced by* $\bar{p}$ is defined by the equivalence relation $\sim_{\bar{p}}$ on $|u| \setminus \bar{p}$, where $p \sim p'$ iff there is no element from $\bar{p}$ between p and p'. Show that, if $\bar{p}$ and $\bar{q}$ induce the same ordering, then there is a bijection ϕ between blocks of $\sim_{\bar{p}}$ and blocks of $\sim_{\bar{q}}$.

c. Let $k \geq 1$. Show that $u, \bar{p} \equiv_{n,k} v, \bar{q}$ if, and only if, the following three conditions are satisfied:

- the markings $\bar{p}$ and $\bar{q}$ induce the same ordering,
- for every $1 \leq i, j \leq n$, the letters $u(p_i)$ and $v(q_i)$ are the same,
- for every block B of the partition induced by $\sim_{\bar{p}}$, the factor of u on the block B is $\equiv_{0,k}$-equivalent to the factor of v on $\phi(B)$.

d. Prove that, for any Σ-words w, x and markings $\bar{r} \in |w|^m$ and $\bar{s} \in |x|^m$, if $u, \bar{p} \equiv_{n,k} v, \bar{q}$ and $w, \bar{r} \equiv_{m,k} x, \bar{s}$, then $uw, \bar{p}\bar{r} \equiv_{n+m,k} vx, \bar{q}\bar{s}$.

e. Conclude that, for every $k \geq 0$, the equivalence relation $\equiv_{0,k}$ is a congruence on Σ^*.

Exercise 2. A semigroup is called *right simple* if there is no proper right ideal, i.e., if $sS = S$ for every $s \in S$. A semigroup is called *right zero* if $st = t$ for every $s, t \in S$.

a. Show that a finite aperiodic semigroup is right simple if, and only if, it is right zero.

b. More generally, show that a finite semigroup is right simple if, and only if, it is isomorphic to a Cartesian product $G \times R$, with G a group and R a right zero semigroup.

Exercise 3. Let M be a finite monoid.

a. Prove that, for any $x \in M$, $x^{|M|!}$ and $x^{|M|!+1}$ are $\mathcal{H}$-equivalent.

b. Prove that a finite monoid M is aperiodic if and only if it is $\mathcal{H}$-trivial, i.e., for any $m, n \in M$, $m \mathcal{H} n$ implies $m = n$.

Exercise 4. Let X a set and $M := X^X$ the monoid of functions from X to X, under composition, i.e., for functions f and g in M, the product $g \cdot f$ is defined by $(g \cdot f)(x) := g(f(x))$, for every $x \in X$. Recall that the *image* of $f \in M$ is $\mathrm{im}(f) := \{f(x) : x \in X\}$, and the *kernel* of $f \in M$ is $\ker(f) := \{(x, x') \in X^2 : f(x) = f(x')\}$. Show that:

a. for any $f, g \in M$, $f \leq_{\mathcal{R}} g$ if, and only if, $\mathrm{im}(f) \subseteq \mathrm{im}(g)$.

b. for any $f, g \in M$, $f \leq_{\mathcal{L}} g$ if, and only if, $\ker(g) \subseteq \ker(f)$.

Exercise 5. Prove that a finite monoid is $\mathcal{L}$-trivial if, and only if, for all elements x and y, $(xy)^m = y(xy)^m$, where m denotes any positive integer such that $(xy)^m$ is idempotent.

Exercise 6. The aim of this exercise is to prove the following result, due to Higman, and relevant to the study of piecewise testable languages. Let Σ be a finite alphabet. Recall that the (scattered) *subword* ordering on finite words is a partial order defined by $a_1 \dots a_n \preceq w$ if, and only if, $w \in \Sigma^* a_1 \Sigma^* \dots \Sigma^* a_n \Sigma^*$. An *antichain* in a poset $(P, \leq)$ is a subset $X \subseteq P$ such that for any $x, y \in X$, if $x \leq y$ then $x = y$. *Higman's Lemma* says that the subword ordering on finite words does not contain infinite antichains.
In fact, we will prove a somewhat stronger claim:
Claim. For any sequence $(w_n)_{n<\omega}$, there exist $i < j < \omega$ such that $w_i \preceq w_j$.

a. Show that the claim indeed implies Higman's Lemma.

b. Let $<_\Sigma$ be an arbitrary total ordering of the alphabet. Show that the ordering $<_r$ on Σ^*, defined by $u <_r v$ if $|u| < |v|$ or $|u| = |v|$ and u is below v in the lexicographic ordering, is a well-founded ordering. (One may prove for example that if $\Sigma = \{0 < 1 < \dots < m\}$, the order $<_r$ corresponds to the ordering on natural numbers, viewed as m-ary strings.)

c. Let $(w_n)_{n<\omega}$ be any infinite sequence of finite Σ-words. Show that there exists a letter $a \in \Sigma$ which occurs infinitely often as the first letter of w_n.

d. Call a finite sequence of words $(w_i)_{i<n}$ *extendible* if it is possible to extend it to an infinite sequence that is a counterexample to the claim. Show that, if the claim is false, then there exists a *$<_r$-minimal sequence with extendible initial segments*, i.e., an infinite sequence $(w_n)_{n<\omega}$ of finite words such that $(w_i)_{i<n}$ is extendible for all $n < \omega$, and such that, for any $n < \omega$ and any finite word $v <_r w_n$, the sequence $w_1, \dots, w_{n-1}, v$ is not extendible.

e. Let $(w_n)_{n<\omega}$ be a sequence as in (d). By (c), choose a letter $a \in \Sigma$ that occurs infinitely often as first letter of w_n. Write $N_a := \{i < \omega : w_i \in a\Sigma^*\}$ and $n_0 := \min N_a$. Show that the sequence $w_1, \dots, w_{n-1}, v_{n_0}$ is extendible, where v_{n_0} is the finite word such that $a v_{n_0} = w_{n_0}$. *Hint.* Use only the w_n with $n \in N_a$ to extend the sequence.

f. Conclude from the previous two items, using a proof by contradiction.

g. (*) How difficult is it to find, for a given sequence $(w_i)_{i<\omega}$ of finite words, two indices $i < j$ such that $w_i \preceq w_j$? Does the above proof give an algorithm? Is this question even well-defined?

Exercise 7. Let Σ a finite alphabet. For any $m < \omega$, $u, v \in \Sigma^*$, write $u \sim_m v$ if u and v have the same subwords of length m. Prove that $\sim_m$ is a congruence, i.e., if $u \sim_m v$ then $uw \sim_m vw$ and $wu \sim_m wv$ for any $w \in \Sigma^*$. Further show that a language L is recognizable by $h_m \colon \Sigma^* \to \Sigma^*/\sim_m$ for some $m < \omega$ if, and only if, L is a Boolean combination of sets that are upward closed in the subword ordering.