Models of computation and finite automata

MPRI, course 2.16, 2022-2023

Automata, Monoids and Logic - Exercise Sheet

Exercise 1. Let $L \subseteq \Sigma^*$ be a regular language. For any word $\alpha \in \Sigma^*$, we write $\alpha^{-1}L := \{w \in \Sigma^* \mid \alpha w \in L\}$. Define the automaton $\mathcal{A}_L$ with set of states $Q := \{\alpha^{-1}L \mid \alpha \in \Sigma^*\}$, initial state $q_0 := L$, set of final states $F = \{u^{-1}L \mid u \in L\}$, and, for each $a \in \Sigma$, the transition function $\delta(a) \in \mathrm{End}(Q)$ defined by $\delta(a)(u^{-1}L) := (ua)^{-1}L$. We denote by $\overline{\delta}\colon \Sigma^* \to \mathrm{End}(Q)$ the unique extension to a homomorphism, where the multiplication of $\mathrm{End}(Q)$ is defined by $(f \cdot g)(q) := g(f(q))$. Prove that the image of $\overline{\delta}$ is isomorphic to the syntactic monoid of L.

Exercise 2. Let $\Sigma = \{a, b\}$. For each of the following languages L, give a full description of $\Sigma^* \to M_L$, describe the four Green relations $\leq_{\mathcal{L}}$, $\leq_{\mathcal{R}}$, $\leq_{\mathcal{H}}$ and $\leq_{\mathcal{J}}$ on S_L, and use it to decide if the language is definable in first-order logic, prefix- or suffix-unambiguous, or in $B\Sigma_1$.

(a) $L = \{w \in \Sigma^* \mid w \text{ has an odd number of } a\text{'s}\}$

(b) $L = (ab)^*$

(c) $L = (aa)^*b$

(d) $L = \Sigma^*a$

(e) $L = \Sigma^*a\Sigma^*b\Sigma^*$

Exercise 3. A *pseudovariety* of finite semigroups is a class of finite semigroups closed under subsemigroup, homomorphic image, and finite product.

An *ω-term* over a set of variables X is a term built from variables with binary product $\cdot$ and a unary operation $()^\omega$; write $T(X)$ for the set of ω-terms. For two ω-terms u and v, and a finite semigroup S, we say that *the equation $u = v$ holds in S* if for any function $f\colon X \to S$, we have $\bar{f}(u) = \bar{f}(v)$, where $\bar{f}\colon T(X) \to S$ is defined by induction, interpreting s^ω as the unique idempotent power of s.

Prove that, for any ω-terms u and v, the class of finite semigroups in which the equation $u = v$ holds is a pseudovariety.

Exercise 4. Show that for any $\mathcal{L}$-trivial monoid M there exists a poset $(X, \leq)$ such that M is isomorphic to a submonoid of $\mathcal{C}(X, \leq)$, the monoid of contractions on a poset $(X, \leq)$.

Exercise 5. (This exercise was already more or less treated in the lectures, modulo some details.)

Let $h\colon \Sigma^* \to M$ be a homomorphism to a finite $\mathcal{L}$-trivial monoid. Denote by $F(M) \subseteq M^+$ the set of finite sequences $(m_0, \ldots, m_n)$ such that $m_i <_{\mathcal{L}} m_{i+1}$ for all $0 \leq i < n$. For $\bar{m} \in M^+$ and $m' \in M$, we write $m' \cdot \bar{m}$ for the sequence obtained by extending $\bar{m}$ on the left with m'. We inductively define a function $c\colon \Sigma^* \to F(M)$ by

$$c(\epsilon) := (1), \quad c(aw) := \begin{cases} c(w) & \text{if } h(aw) = h(w), \\ h(aw) \cdot c(w) & \text{otherwise.} \end{cases}$$

(a) Show that, for any $w \in \Sigma^*$, $c(w) \in F(M)$ and the first element of the sequence $c(w)$ is $h(w)$.

(b) Prove that, for any $\bar{m} \in F(M)$, $c^{-1}(\bar{m})$ is a suffix unambiguous language.

(c) Deduce that $h^{-1}(m)$ is suffix unambiguous for every $m \in M$.

Exercise 6. Let S be a finite semigroup.

(a) Prove that, for any $x, y \in S$, if $x \leq_{\mathcal{J}} xy$ then $x \leq_{\mathcal{R}} xy$. (This property is known as *stability*.)

(b) Prove that $\mathcal{J} = \mathcal{R} \circ \mathcal{L}$, i.e., if $x\mathcal{J}y$, then there exists $z \in S$ such that $x\mathcal{R}z\mathcal{L}y$.

(c) Deduce that $\mathcal{J}$ is the least equivalence relation on S that contains $\mathcal{L} \cup \mathcal{R}$. (In a general semigroup, the least equivalence relation containing $\mathcal{L} \cup \mathcal{R}$ is denoted $\mathcal{D}$, so this question shows that $\mathcal{J} = \mathcal{D}$ in a finite semigroup.)

Exercise 7. Let X be a finite set and $\mathrm{End}(X)$ the monoid of functions from X to itself, with composition. Describe the preorders $\leq_{\mathcal{L}}$, $\leq_{\mathcal{R}}$ and $\leq_{\mathcal{J}}$ on $\mathrm{End}(X)$.

Exercise 8. Let S, T be finite semigroups and $h \colon S \to T$ a homomorphism. Prove that, if S is a group, then the image of h is a subgroup of T, and h is a group homomorphism from S onto $\mathrm{im}(h)$.

Exercise 9. Let G be a finite group and A, B finite sets. We write G^0 for the semigroup $G \cup \{0\}$ with $x0 = 0 = 0x$ for all x. An $A \times B$-*matrix* is a function $M \colon A \times B \to G^0$. We denote the everywhere zero matrix by 0, and for $g \in G^0$, scalar multiplication gM is defined by $(gM)(a, b) = gM(a, b)$. Denote by E_{ab} the $(A \times B)$-matrix which is 0 everywhere except at (a, b), where it is 1. We define

$$\mathcal{M} = \{gE_{ab} \;:\; g \in G, a \in A, b \in B\}$$

and $\mathcal{M}^0 := \mathcal{M} \cup \{0\}$. Given a matrix $C \colon B \times A \to G^0$, we define the *Rees semigroup* with group G and structure matrix C as $R^0(G, C) := (\mathcal{M}^0, \diamond)$, where for any $X, Y \in \mathcal{M}^0$,

$$X \diamond Y := X \cdot C \cdot Y,$$

where $\cdot$ is matrix multiplication. We assume that C does not have any zero rows or columns.

(a) Define a monoid multiplication on the set $(A \times G \times B) \cup \{0\}$ such that it becomes isomorphic to the monoid $R^0(G, C)$.

(b) Describe $\mathcal{J}$, $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{H}$ on $R^0(G, C)$.

(c) Show that the $\mathcal{H}$-class of E_{ab} is a subgroup iff $C(b, a) \neq 0$, and in this case it is isomorphic to G.

Note. One may prove that a $\mathcal{J}$-class in a finite semigroup always looks like $R^0(G, C) \setminus \{0\}$ for some finite group G and some matrix C. See for example Section A.4 of Rhodes & Steinberg, "The q-theory of finite semigroups".

Exercise 10. (*) Give an alternative proof of Schützenberger's Theorem that avoids writing down FO formulas explicitly, and instead uses directly the FO-equivalence relations $\equiv_k$ and an induction on the $\mathcal{J}$-order of the aperiodic semigroup. In particular, show that there is a *linear* function $f \colon \mathbb{N} \to \mathbb{N}$ such that, for any finite aperiodic semigroup S, if any strict $\mathcal{J}$-chain in S has size at most n, then any language recognized by S is definable with a first order sentence of quantifier rank at most $f(n)$. (Only try this if all the previous exercises were too easy.)