Technische Universität München **Winter term 2013/2014**
I7
M. Kufleitner / A. Durand-Gasselin **31.10.2013**

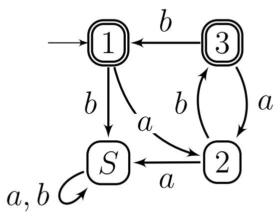
Automata and Formal Languages – Exercise sheet 2

Exercise 2.1

Let $L = \{ab, abb\}^*$. Give the minimal automata of $K_a = \{u \in \{a,b\}^* \mid u \equiv_L a\}$ and $K_b = \{u \in \{a,b\}^* \mid u \equiv_L b\}$.

Solution:

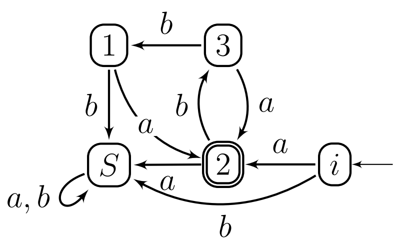
Here is A_L the minimal automaton accepting L:



As A_L is minimal we have that $u \equiv_L v$ iff $\forall q \in Q \cdot \delta(q,u) = \delta(q,v)$.
Therefore, we work with the transition monoid of A_L as it is the syntactic monoid of L.

Characterizing K_b:
Notice that $|\delta(Q,a)| = 2$, so if $Q' \subseteq Q$, $|\delta(Q',a)| \leq 2$.
If a word w contains an a (i.e. w can be written as uaw),
$\delta(Q,w) = \delta(\delta(\delta(Q,u),a),v) = \delta(\delta(Q',a),v) = \delta(Q'',v)$ for some $Q', Q'' \subseteq Q$ with $|Q''| \leq 2$, thus $|\delta(Q'',v)| \leq 2$, so if a word w contains an a, $|\delta(Q,w)| \leq 2$.
As $|\delta(Q,b)| = 3$ we deduce that words in K_b do not contain any a.
Also $|\delta(Q,bb)| = 2$ thus words in K_b do not contain bb. $\delta(1,b) \neq 1$ thus $\varepsilon \notin K_b$.
Therefore $K_b = \{b\}$.

Characterizing K_a:
Denote $L_{q,q'}$ the set of words such that $\delta(q,w) = q'$, we have $K_a = L_{1,2} \cap L_{2,S} \cap L_{3,2} \cap L_{S,S}$.
$L_{1,2} = a \cdot L_{2,2} \cup b \cdot L_{S,2}$, obviously $L_{S,2} = \emptyset$, so $L_{1,2} = a \cdot L_{2,2}$.
$L_{2,S} = a \cdot L_{S,S} \cup b \cdot L_{3,S}$, as $L_{S,S} = \{a,b\}^* \supset L_{2,2}$, we have $L_{1,2} \cap L_{2,S} = a \cdot L_{2,2}$
$L_{3,2} = a \cdot L_{2,2} \cup b \cdot L_{1,2}$, $L_{S,S} = \{a,b\}^*$, therfore $K_a = L_{1,2} \cap L_{2,S} \cap L_{3,2} \cap L_{S,S} = a \cdot L_{2,2}$.
It is easy to build an automaton accepting $L_{2,2}$ from A_L: its initial and final state is 2.
As the automaton accepting the language $\{a\}$ has only one final state, it is easy to build a deterministic automaton accepting the concatenation of the two languages. We obtain a deterministic automaton A_{K_a} accepting K_a.
This automaton is not minimal, applying Moore's minimization algorithm will indicate that states 1 and i can be merged.



Exercise 2.2

Let M be generated by $\Sigma \subseteq M$, let $\varphi : M \to N$ be a homomorphism to a finite monoid N, and let $P \subseteq N$. Give an algorithm for computing the syntactic monoid of $\varphi^{-1}(P)$.

Solution:

Denote $L = \varphi^{-1}(P)$, $N' = \varphi(N)$ and $P' = P \cap N$.
In order to present the algorithm, we first show that it suffices to compute the syntactic monoid of the language P' over the finite monoid N'. Then we devise an algorithm that relies on the finiteness of the monoid N' to compute the syntactic monoid of P'.
We first show that $\mathrm{Synt}_{N'}(P') = \mathrm{Synt}_M(L)$
φ is a surjective homorphism from M to N' recognizing L, therefore we can define the (surjective) homorphism ψ from N' to $\mathrm{Synt}(L)$ as $\psi : \varphi(u) \mapsto [u]_L$.
(This homomorphism is well-defined: if $\varphi(u) = \varphi(v)$ then –as φ recognizes L– $[u]_L = [v]_L$)
We denote ϕ_L the homomorphism $u \mapsto [u]_L$, and we remark $\phi_L = \psi \circ \varphi$.
As N' is a monoid, and $P' \subseteq N'$, we can define the syntactic monoid of P', $\mathrm{Synt}(P')$.
We now show that $\mathrm{Synt}(P')$ and $\mathrm{Synt}(L)$ are isomorphic:
Remark that $\mathrm{Synt}(L)$ recognizes P': for that we have to show that $\psi^{-1}(\psi(P')) = P'$ (by double inclusion, $\supseteq$ is trivial)
$\psi(P') = \phi_L(L)$, and $\phi_L^{-1}(\phi_L(L)) = L$ so if $x \in \psi^{-1}(\psi(P'))$, then $\varphi^{-1}(x) \in L$, as $\varphi(L) = P'$ which implies $x \in P'$.
Therefore there exists a surjective homorphism from $\mathrm{Synt}(L)$ to $\mathrm{Synt}(P')$.
For the same reason $\phi_L(L)$ is recognized by $\mathrm{Synt}(P')$. Hence there exists a surjective homorphism in the other direction, which implies that the two syntactic monoids are isomorphic.

We now give an algorithm to compute $\mathrm{Synt}(P')$ (actually $\equiv_{P'}$):
Take the (finite) graph $G = (N', \binom{N'}{2})$.
For $u, v \in N'$ remove edges (x, y) such that $uxv \in P'$ and $uyv \notin P'$.
Merge nodes that are still connected.

Its correctness stands in that if x and y are merged then for all $u, v \in N'$, $uxy \in P$ iff $vxy \in P$.

Exercise 2.3

Let S be a finite semigroup. An element $e \in S$ is *idempotent* if $e^2 = e$.

(a) Show that for every $x \in S$ there exists a unique idempotent element in the set $\{x^k \mid k \geq 1\} \subseteq S$.

(b) Show that $x^{|S|!}$ is idempotent for every $x \in S$.

Solution:

The unicity is easy to show: assume x^k and $x^{k'}$ are idempotent, then for any integer λ, $x^k = x^{\lambda k}$ and $x^{k'} = x^{\lambda k'}$; $x^k \overset{(\lambda:=k')}{=} x^{kk'} \overset{(\lambda:=k)}{=} x^{k'}$.
Let $n = |S|$. Take the sequence $x^1, \ldots, x^{n+1}$.
By pidgeon hole principle, there exists p, p', $p < p' \leq n+1$ such that $x^p = x^{p'}$, let $q = p' - p$.
Multiplying the equality $x^p = x^{p+q}$ by powers of x implies, that for any $k \geq p$, $x^k = x^{k+q}$.
We even have for any k, λ, $k \geq p, \lambda \geq 0$, that $x^k = x^{k+\lambda q}$. (obvious by induction over λ)
Let m the multiple of q between p and $p + q - 1$ (m can be written as λq for some λ),
$(x^m)^2 = x^{m+m} = x^{m+\lambda q} \overset{\text{as } m \geq p}{=} x^m$, so x^m is idempotent. Also $m \leq n$.
Showing that $x^{|S|!}$ is idempotent is easily shown from the fact that there exists an $m \leq n$ such that x^m is idempotent: this implies that $x^{|S|!} = x^{m\frac{|S|!}{m}} = x^m$ which is idempotent.

Exercise 2.4

Let $\varphi : \Sigma^* \to M$ be a homomorphism to a finite monoid M. Show that there exists an integer $n \geq 1$ such that $\varphi(\Sigma^n) = \varphi(\Sigma^{2n})$. As usual, $\varphi(L)$ denotes the subset $\{\varphi(u) \mid u \in L\}$ of M.

Solution:

Consider the semigroup $(2^M, \cdot)$ where $\cdot$ is defined as follows:
$A \cdot B = \{uv \mid u \in A, v \in B\}$
$\cdot$ is clearly associative.
Consider $x = \varphi(\Sigma)$, then applying solution of the preceeding exercise, we have that there exists an n such that $x^n = x^{2n}$.
We just need to establish that $x^n = \varphi(\Sigma^n)$.
By induction over n:
when $n = 1$, it is clear.
$x^{n+1} = x \cdot \varphi(\Sigma^n) = \{\varphi(\alpha) \cdot \varphi(u) \mid \alpha \in \Sigma, u \in \Sigma^n\} = \{\varphi(\alpha u) \mid \alpha \in \Sigma, u \in \Sigma^n\} = \varphi(\Sigma^{n+1})$.

Exercise 2.5

Given a word $w \in \Sigma^*$ and a subset $\Gamma \subseteq \Sigma$, we define informally $\pi_\Gamma(w)$ as the word obtained by erasing all letters of w that are not in Γ. More precisely, $\pi_\Gamma : \Sigma^* \to \Gamma^*$ is defined by $\pi_\Gamma(a) = a$ if $a \in \Gamma$ and $\pi_\Gamma(a) = \varepsilon$ otherwise. Show that if $L \subseteq \Sigma^*$ is recognizable, then $\pi_\Gamma(L) = \{\pi_\Gamma(u) \mid u \in L\}$ is recognizable.