

Introduction to the Theory of Computation

Homework 1

January 16, 2003; Due February 4, beginning of class

“A problems” are for practice only, and should not be turned in.

Problem A1. Let $D = (Q, \Sigma, \delta, q_0, F)$ be a DFA. Recall that a state $p \in Q$ is *accessible* or *reachable* iff there is some string $w \in \Sigma^*$, such that

$$\delta^*(q_0, w) = p,$$

i.e., there is some path from q_0 to p in D . Consider the following method for computing the set Q_r of reachable states (of D): define the sequence of sets $Q_r^i \subseteq Q$, where

$$Q_r^0 = \{q_0\},$$

$$Q_r^{i+1} = \{q \in Q \mid \exists p \in Q_r^i, \exists a \in \Sigma, q = \delta(p, a)\}.$$

(i) Prove by induction on i that Q_r^i is the set of all states reachable from q_0 using paths of length i (where i counts the number of edges).

Show that it is generally false that there is an index i_0 , such that $Q_r^{i_0+1} = Q_r^{i_0}$, by giving a counter-example.

(ii) Show that $Q_r^{i_0} = Q_r$ for some i_0 is generally false, by giving a counter-example.

(iii) Change the inductive definition of Q_r^i as follows:

$$Q_r^{i+1} = Q_r^i \cup \{q \in Q \mid \exists p \in Q_r^i, \exists a \in \Sigma, q = \delta(p, a)\}.$$

Prove that there is a smallest integer i_0 such that

$$Q_r^{i_0+1} = Q_r^{i_0} = Q_r.$$

Define the DFA D_r as follows: $D_r = (Q_r, \Sigma, \delta_r, q_0, F \cap Q_r)$, where $\delta_r: Q_r \times \Sigma \rightarrow Q_r$ is the restriction of δ to Q_r . Explain why D_r is indeed a DFA, and show that $L(D_r) = L(D)$. A DFA is said to be *reachable*, or *trim*, if $D = D_r$.

Problem A2. Given an alphabet Σ , for any language $L \subseteq \Sigma^*$, prove that $L^{**} = L^*$ and $L^*L^* = L^*$.

Problem A3. Let $D = (Q, \Sigma, \delta, q_0, F)$ be a DFA. Prove that for all $p \in Q$ and all $u, v \in \Sigma^*$,

$$\delta^*(p, uv) = \delta^*(\delta^*(p, u), v).$$

“B problems” must be turned in.

Problem B1 (20 pts). Let L be any language over some alphabet Σ .

(a) Prove that $L = L^+$ iff $LL \subseteq L$.

(b) Prove that $(L = \emptyset \text{ or } L = L^*)$ iff $LL = L$.

Problem B2 (20 pts). (a) Given the alphabet $\Sigma = \{0, 1, c\}$, construct a DFA accepting the following language:

$$L = \{u_1cu_2c \cdots cu_{n-1}cu_n \mid n \geq 1, u_i \in \{00, 01, 10\}\}.$$

(b) The strings in the above language can be interpreted as the coordinates of points in the plane as follows: Assume that you start with a square S_0 , say of dimension 2×2 , divided into four equal subsquares. Then the lower left corner of each subsquare is referenced by one of the strings 00, 01, 10, or 11. A string $u_1cu_2c \cdots cu_{n-1}cu_n$ determines a point in the original square by proceeding recursively as follows: u_1 determines the subsquare S_1 whose lower left corner has coordinates u_1 in the original square; within the square S_1 , u_2 determines the subsquare S_2 whose lower left corner has coordinates u_2 ; given the subsquare S_i obtained at the end of step i , within this subsquare S_i , u_{i+1} determines the subsquare S_{i+1} whose lower left corner has coordinates u_{i+1} . The procedure stops with a point in the square S_{n-1} obtained at stage $n - 1$, the lower left corner of the subsquare S_n whose coordinates with respect to S_{n-1} are determined by u_n .

Draw a rough picture by plotting a number of these points. What sort of shape do you get?

Remark: The set of points defined above is a subset of the set of rational points of a fractal set known as the *Sierpinski gasket*.

Problem B3 (40 pts). Given any two DFA's $D_1 = (Q_1, \Sigma, \delta_1, q_{0,1}, F_1)$ and $D_2 = (Q_2, \Sigma, \delta_2, q_{0,2}, F_2)$, a *morphism* $h: D_1 \rightarrow D_2$ of DFA's is a function $h: Q_1 \rightarrow Q_2$ satisfying the following two conditions:

(1) $h(\delta_1(p, a)) = \delta_2(h(p), a)$, for all $p \in Q_1$ and all $a \in \Sigma$;

(2) $h(q_{0,1}) = q_{0,2}$.

A *map* $h: D_1 \rightarrow D_2$ of DFA's is a morphism satisfying the condition

(3a) $h(F_1) \subseteq F_2$.

A *homomorphism* $h: D_1 \rightarrow D_2$ of DFA's is a morphism satisfying the condition

(3b) $h^{-1}(F_2) \subseteq F_1$.

A *proper homomorphism of DFA's* is a homomorphism of DFA's which is also a map of DFA's, i.e. it satisfies the condition

$$(3c) \quad h^{-1}(F_2) = F_1.$$

We say that a morphism, map, or homomorphism, $h: D_1 \rightarrow D_2$ is *surjective* if $h(Q_1) = Q_2$.

(a) If $h: D_1 \rightarrow D_2$ is a morphism of DFA's, prove that

$$h(\delta_1^*(p, w)) = \delta_2^*(h(p), w),$$

for all $p \in Q_1$ and all $w \in \Sigma^*$.

As a consequence, prove the following facts:

If $h: D_1 \rightarrow D_2$ is a map of DFA's, then $L(D_1) \subseteq L(D_2)$. If $h: D_1 \rightarrow D_2$ is a homomorphism of DFA's, then $L(D_2) \subseteq L(D_1)$. Finally, if $h: D_1 \rightarrow D_2$ is a proper homomorphism of DFA's, then $L(D_1) = L(D_2)$.

(b) Let D_1 and D_2 be DFA's and assume that there is a morphism $h: D_1 \rightarrow D_2$. Prove that h induces a unique surjective morphism $h_r: (D_1)_r \rightarrow (D_2)_r$ (where $(D_1)_r$ and $(D_2)_r$ are the trim DFA's defined in problem A1). This means that if $h: D_1 \rightarrow D_2$ and $h': D_1 \rightarrow D_2$ are DFA morphisms, then $h(p) = h'(p)$ for all $p \in (D_1)_r$, and the restriction of h to $(D_1)_r$ is surjective onto $(D_2)_r$. Moreover, if $L(D_1) = L(D_2)$, prove that h induces a unique surjective proper homomorphism $h_r: (D_1)_r \rightarrow (D_2)_r$.

(c) Relax the condition that a DFA morphism $h: D_1 \rightarrow D_2$ maps $q_{0,1}$ to $q_{0,2}$ (so, it is possible that $h(q_{0,1}) \neq q_{0,2}$), and call such a function a *weak morphism*. We have an obvious notion of *weak map*, *weak homomorphism* and *weak proper homomorphism* (by imposing condition (3a) or condition (3b), or (3c)). For any language, $L \subseteq \Sigma^*$ and any fixed string, $u \in \Sigma^*$, let $D_u(L)$, also denoted L/u (called the *(left) derivative of L by u*), be the language

$$D_u(L) = \{v \in \Sigma^* \mid uv \in L\}.$$

Prove the following facts, **assuming that D_2 is trim**: If $h: D_1 \rightarrow D_2$ is a weak map of DFA's, then $L(D_1) \subseteq D_u(L(D_2))$, for some suitable $u \in \Sigma^*$. If $h: D_1 \rightarrow D_2$ is a weak homomorphism of DFA's, then $D_u(L(D_2)) \subseteq L(D_1)$, for the same u as above. Finally, if $h: D_1 \rightarrow D_2$ is a weak proper homomorphism of DFA's, then $L(D_1) = D_u(L(D_2))$, for the same u as above.

Suppose there is a weak morphism $h: D_1 \rightarrow D_2$. What can you say about the restriction of h to $(D_1)_r$? What can you say about surjectivity? (you may need to consider $(D_2)_r$ with respect to a **different** start state). What happens (and what can you say) if D_2 is **not** trim?

Problem B4 (50 pts). (a) Given any two DFA's D_1 and D_2 , prove that there is a DFA D and two DFA maps $\pi_1: D \rightarrow D_1$ and $\pi_2: D \rightarrow D_2$ such that the following *universal*

mapping property of products holds: For any DFA M and any two DFA maps $f: M \rightarrow D_1$ and $g: M \rightarrow D_2$, there is a *unique* DFA map $h: M \rightarrow D$ such that

$$f = \pi_1 \circ h \quad \text{and} \quad g = \pi_2 \circ h,$$

as shown in the diagram below:

$$\begin{array}{ccc} & & D_1 \\ & f \nearrow & \uparrow \pi_1 \\ M & \xrightarrow{h} & D \\ & g \searrow & \downarrow \pi_2 \\ & & D_2 \end{array}$$

Moreover, prove that π_1 and π_2 are surjective. Prove that D is unique up to a unique DFA map isomorphism. This means that if D' is another DFA and if there are two DFA maps $\pi'_1: D' \rightarrow D_1$ and $\pi'_2: D' \rightarrow D_2$ such that the universal mapping property of products holds, then there are two unique DFA maps $\varphi: D \rightarrow D'$ and $\varphi': D' \rightarrow D$ so that $\varphi' \circ \varphi = \text{id}_D$ and $\varphi \circ \varphi' = \text{id}_{D'}$. What is the language accepted by D ?

Remark: We call D the *product of D_1 and D_2* and we denote it by $D_1 \times D_2$.

(b) Given any three DFA's D_1 , D_2 , and D_3 and any two DFA maps $f: D_1 \rightarrow D_3$ and $g: D_2 \rightarrow D_3$, prove that there is a DFA D and two DFA maps $\pi_1: D \rightarrow D_1$ and $\pi_2: D \rightarrow D_2$ such that

$$f \circ \pi_1 = g \circ \pi_2,$$

as in the diagram below:

$$\begin{array}{ccc} D & \xrightarrow{\pi_1} & D_1 \\ \pi_2 \downarrow & & \downarrow f \\ D_2 & \xrightarrow{g} & D_3, \end{array}$$

and the following *universal mapping property of fibred products* holds: for any DFA M and any two DFA maps $f': M \rightarrow D_1$ and $g': M \rightarrow D_2$ such that

$$f \circ f' = g \circ g',$$

as in the diagram below:

$$\begin{array}{ccc} M & \xrightarrow{f'} & D_1 \\ g' \downarrow & & \downarrow f \\ D_2 & \xrightarrow{g} & D_3, \end{array}$$

there is a *unique* DFA map $h: M \rightarrow D$ such that

$$f' = \pi_1 \circ h \quad \text{and} \quad g' = \pi_2 \circ h.$$

Prove that D is unique up to a unique DFA map isomorphism. This means that if D' is another DFA and if there are two DFA maps $\pi'_1: D' \rightarrow D_1$ and $\pi'_2: D' \rightarrow D_2$ such that

$$f \circ \pi'_1 = g \circ \pi'_2$$

and the universal mapping property of fibred products holds, then there are two unique DFA maps $\varphi: D \rightarrow D'$ and $\varphi': D' \rightarrow D$ so that $\varphi' \circ \varphi = \text{id}_D$ and $\varphi \circ \varphi' = \text{id}_{D'}$.

Remark: We denote D by $D_1 \times_{D_3} D_2$ and call it a *fibred product of D_1 and D_2 over D_3* , or a *pullback of D_1 and D_2 over D_3* .

Letting T denote any one-state DFA accepting Σ^* (this single state is final), observe that there is a unique DFA map from every DFA D to T . Use this to show that if $D_1 \times D_2$ is the product DFA arising in (a), then

$$D_1 \times D_2 = D_1 \times_T D_2.$$

Remark: If we dualize (b), i.e., turn the arrows around, we get the notion of *fibred coproduct* or *pushout*. It can be shown that fibred coproducts exist, but this is a bit tricky.

Problem B5 (40 pts). (*Ultimate periodicity*) A subset U of the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ of natural numbers is *ultimately periodic* if there exist $m, p \in \mathbb{N}$, with $p \geq 1$, so that $n \in U$ iff $n + p \in U$, for all $n \geq m$.

(i) Prove that $U \subseteq \mathbb{N}$ is ultimately periodic iff either U is finite or there is a finite subset $F \subseteq \mathbb{N}$ and there are $k \leq p$ numbers m_1, \dots, m_k , with $m_1 < m_2 < \dots < m_k < m_1 + p$, and with m_1 the smallest element of U so that for some $p \geq 1$, $n \in U$ iff $n + p \in U$, for all $n \geq m_1$, so that

$$U = F \cup \bigcup_{i=1}^k \{m_i + jp \mid j \in \mathbb{N}\}.$$

Give an example of an ultimately periodic set U such that m and p are not necessarily unique, i.e., U is ultimately periodic with respect to m_1, p_1 and m_2, p_2 , with $m_1 \neq m_2$ and $p_1 \neq p_2$.

Remark: A subset of \mathbb{N} of the form $\{m + ip \mid i \in \mathbb{N}\}$ (allowing $p = 0$) is called a *linear set*, and a finite union of linear sets is called a *semilinear set*. Thus, (i) says that a set is ultimately periodic iff it is semilinear.

(ii) Let $L \subseteq \{a\}^*$ be a language over the one-letter alphabet $\{a\}$. Prove that L is a regular language iff the set $\{m \in \mathbb{N} \mid a^m \in L\}$ is ultimately periodic. Prove that the family of semilinear sets is closed under union, intersection and complementation (i.e., it is a boolean algebra).

(iii) Let $L \subseteq \Sigma^*$ be a regular language over any alphabet Σ (not necessarily consisting of a single letter). Prove that the set

$$|L| = \{|w| \mid w \in L\}$$

is ultimately periodic.

Problem B6 (90 pts). (*wqo's*) We let \mathbb{N} denote the set $\{0, 1, 2, \dots\}$ of natural numbers, and \mathbb{N}_+ denote the set $\{1, 2, \dots\}$ of positive natural numbers. Given a set S , an *infinite sequence* is a function $s : \mathbb{N}_+ \rightarrow S$. An infinite sequence s is also denoted by $(s_i)_{i \geq 1}$, or by $\langle s_1, s_2, \dots, s_i, \dots \rangle$. Given an infinite sequence $s = (s_i)_{i \geq 1}$, an *infinite subsequence* of s is any infinite sequence $s' = (s'_j)_{j \geq 1}$ such that there is a strictly monotonic function $f : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ and $s'_i = s_{f(i)}$ for all $i > 0$ (recall that a function $f : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ is *strictly monotonic* (or *increasing*) iff for all $i, j > 0$, $i < j$ implies that $f(i) < f(j)$). An infinite subsequence s' of s associated with the function f is also denoted as $s' = (s_{f(i)})_{i \geq 1}$.

We now review preorders and well-foundedness.

Given a set A , a binary relation $\preceq \subseteq A \times A$ on the set A is a *preorder* (or *quasi-order*) iff it is reflexive and transitive. A preorder that is also antisymmetric is called a *partial order*. A preorder is *total* iff for every $x, y \in A$, either $x \preceq y$ or $y \preceq x$. The relation \succeq is defined such that $x \succeq y$ iff $y \preceq x$, the relation \prec such that

$$x \prec y \quad \text{iff} \quad x \preceq y \quad \text{and} \quad y \not\preceq x,$$

and the relation \succ such that $x \succ y$ iff $y \prec x$. We say that x and y are *incomparable* iff $x \not\preceq y$ and $y \not\preceq x$, and this is also denoted by $x \mid y$.

Given a preorder \preceq over a set A , an infinite sequence $(x_i)_{i \geq 1}$ is an *infinite decreasing chain* iff $x_i \succ x_{i+1}$ for all $i \geq 1$. An infinite sequence $(x_i)_{i \geq 1}$ is an *infinite antichain* iff $x_i \mid x_j$ for all i, j , $1 \leq i < j$. We say that \preceq is *well-founded* and that \succ is *Noetherian* iff there are no infinite decreasing chains w.r.t. \succ .

We now turn to the fundamental concept of a well quasi-order (wqo).

Given a preorder \preceq over a set A , an infinite sequence $(a_i)_{i \geq 1}$ of elements in A is termed *good* iff there exist positive integers i, j such that $i < j$ and $a_i \preceq a_j$, and otherwise, it is termed a *bad* sequence. A preorder \preceq is a *well quasi-order*, abbreviated as *wqo*, iff every infinite sequence of elements of A is good.

Prove that the standard total ordering \leq on \mathbb{N} is a wqo. If \preceq is a wqo on a set A , a *finite* sequence is not necessarily good (why?).

(a) Prove the following characterizations of *wqo's*. Given a preorder \preceq on a set A , the following conditions are equivalent:

- (1) Every infinite sequence is good (w.r.t. \preceq).

(2) There are no infinite decreasing chains and no infinite antichains (w.r.t. \preceq).

Given a preorder \preceq on a set A , say that a member s_i of an infinite sequence s is *terminal* iff there is no $j > i$ such that $s_i \preceq s_j$.

(b) Prove that the following statements are equivalent:

(1) \preceq is a *wqo* on A .

(2) Every infinite sequence $s = (s_i)_{i \geq 1}$ over A contains some infinite subsequence $s' = (s_{f(i)})_{i \geq 1}$ such that $s_{f(i)} \preceq s_{f(i+1)}$ for all $i > 0$.

Hint. First, prove that if \preceq is a wqo, then the number of terminal elements in any infinite sequence s is finite.

Given two preorders $\langle \preceq_1, A_1 \rangle$ and $\langle \preceq_2, A_2 \rangle$, the cartesian product $A_1 \times A_2$ is equipped with the preorder \preceq defined such that $(a_1, a_2) \preceq (a'_1, a'_2)$ iff $a_1 \preceq_1 a'_1$ and $a_2 \preceq_2 a'_2$.

(c) Prove that if \preceq_1 and \preceq_2 are *wqo*, then \preceq is a *wqo* on $A_1 \times A_2$.

Remark: This is due to Nash-Williams.

(d) Prove the following result.

Let n be any integer such that $n > 1$. Given any infinite sequence $(s_i)_{i \geq 1}$ of n -tuples of natural numbers, there exist positive integers i, j such that $i < j$ and $s_i \preceq_n s_j$, where \preceq_n is the partial order on n -tuples of natural numbers induced by the natural ordering \leq on \mathbb{N}

Remark: This is due to Dickson, 1913!

Let \sqsubseteq be a preorder on a set A . We define the preorder \ll (*string embedding*) on A^* as follows:

$\epsilon \ll u$ for each $u \in A^*$, and, for any two strings $u = u_1 u_2 \dots u_m$ and $v = v_1 v_2 \dots v_n$, $1 \leq m \leq n$,

$$u_1 u_2 \dots u_m \ll v_1 v_2 \dots v_n$$

iff there exist integers j_1, \dots, j_m such that $1 \leq j_1 < j_2 < \dots < j_{m-1} < j_m \leq n$ and

$$u_1 \sqsubseteq v_{j_1}, \dots, u_m \sqsubseteq v_{j_m}.$$

(e) Prove that \ll is a preorder. Prove that \ll is a partial order if \sqsubseteq is a partial order. Prove that \ll is the least preorder on A^* satisfying the following two properties:

(1) (deletion property) $uv \ll uav$, for all $u, v \in A^*$ and $a \in A$;

(2) (monotonicity) $uav \ll ubv$ whenever $a \sqsubseteq b$, for all $u, v \in A^*$ and $a, b \in A$.

Remark: The following theorem due to Higman can be proved, but the proof is hard.

Theorem If \sqsubseteq is a *wgo* on A , then \ll is a *wgo* on A^* .

You do **not** have to prove Higman's theorem for this homework!

TOTAL: 260 points.