

# Introduction to the Theory of Computation

Jean Gallier

## Homework 1

January 15, 2004; Due February 3, 2004

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

**Problem A1.** Given an alphabet  $\Sigma$ , prove that the relation  $\leq_1$  over  $\Sigma^*$  defined such that  $u \leq_1 v$  iff  $u$  is a prefix of  $v$ , is a partial ordering. Prove that the relation  $\leq_2$  over  $\Sigma^*$  defined such that  $u \leq_2 v$  iff  $u$  is a substring of  $v$ , is a partial ordering.

**Problem A2.** Given an alphabet  $\Sigma$ , 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 (30 pts).** 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  $\delta$  to  $Q_r$ . Explain why  $D_r$  is indeed a DFA, and prove that  $L(D_r) = L(D)$ . A DFA is said to be *reachable*, or *trim*, if  $D = D_r$ .

**Problem B2 (20 pts).** Given a string  $w$ , its reversal  $w^R$  is defined inductively as follows:  $\epsilon^R = \epsilon$  and  $(ua)^R = au^R$ , where  $a \in \Sigma$  and  $u \in \Sigma^*$ . Prove that  $(uv)^R = v^R u^R$ . Prove that  $(w^R)^R = w$ .

**Problem B3 (30 pts).** Given any alphabet  $\Sigma$ , prove the following property: for any two strings  $u, v \in \Sigma^*$ ,  $uv = vu$  iff there is some  $w \in \Sigma^*$  such that  $u = w^m$  and  $v = w^n$ , for some  $m, n \geq 0$ .

**Problem B4 (50 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)  $h(q_{0,1}) = q_{0,2}$ .

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

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

An *F<sup>-1</sup>-map*  $h: D_1 \rightarrow D_2$  of DFA's is a morphism satisfying the condition

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

A *proper homomorphism of DFA's* is an *F-map* of DFA's which is also an *F<sup>-1</sup>-map* of DFA's, i.e. it satisfies the condition

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

We say that a morphism (resp. *F-map*, resp. *F<sup>-1</sup>-map*)  $h: D_1 \rightarrow D_2$  is *surjective* if  $h(Q_1) = Q_2$ .

(a) Prove that if  $f: D_1 \rightarrow D_2$  and  $g: D_2 \rightarrow D_3$  are morphisms (resp. *F-maps*, resp. *F<sup>-1</sup>-maps*) of DFAs, then  $g \circ f: D_1 \rightarrow D_3$  is also a morphism (resp. *F-map*, resp. *F<sup>-1</sup>-map*) of DFAs.

Prove that if  $f: D_1 \rightarrow D_2$  is an *F-map* that is an isomorphism then it is also an *F<sup>-1</sup>-map*, and that if  $f: D_1 \rightarrow D_2$  is an *F<sup>-1</sup>-map* that is an isomorphism then it is also an *F-map*.

(b) 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 an  $F$ -map of DFA's, then  $L(D_1) \subseteq L(D_2)$ . If  $h: D_1 \rightarrow D_2$  is an  $F^{-1}$ -map 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  $L(D_1) = L(D_2)$ .

(c) 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 B1). 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  $h_r: (D_1)_r \rightarrow (D_2)_r$ .

(d) 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  $F$ -map*, *weak  $F^{-1}$ -map* 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  $F$ -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  $F^{-1}$ -map 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 B5 (40 pts).** (a) For any language  $L \subseteq \{a\}^*$ , prove that if  $L = L^*$ , then there is a finite language  $S \subseteq L$  such that  $L = S^*$ . Prove that  $L$  is regular.

(b) Let  $L \subseteq \{a\}^*$  be any infinite regular language. Prove that there is a finite set  $F \subseteq \{a\}^*$ , and some strings  $a^m, a^{p_1}, \dots, a^{p_k}$ , and  $a^q \neq \epsilon$ , with  $0 \leq p_1 < p_2 < \dots < p_k < q$ , such that

$$L = F \cup \bigcup_{i=1}^k a^{m+p_i} \{a^q\}^*.$$

**Problem B6 (50 pts).** (a) Given any two DFA's  $D_1$  and  $D_2$ , prove that there is a DFA  $D$  and two DFA  $F^{-1}$ -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  $F^{-1}$ -maps  $f: M \rightarrow D_1$  and  $g: M \rightarrow D_2$ , there is a *unique* DFA  $F^{-1}$ -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  $\pi_1$  and  $\pi_2$  are surjective. Prove that  $D$  is unique up to a DFA  $F^{-1}$ -map isomorphism. This means that if  $D'$  is another DFA and if there are two DFA  $F^{-1}$ -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  $F^{-1}$ -maps  $\varphi: D \rightarrow D'$  and  $\varphi': D' \rightarrow D$  so that  $\varphi' \circ \varphi = \text{id}_D$ ,  $\pi_1 = \pi'_1 \circ \varphi$ ,  $\pi_2 = \pi'_2 \circ \varphi$ ,  $\varphi \circ \varphi' = \text{id}_{D'}$ ,  $\pi'_1 = \pi_1 \circ \varphi'$  and  $\pi'_2 = \pi_2 \circ \varphi'$ . What is the language accepted by  $D$ ?

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

(b) Given any three DFA's  $D_1$ ,  $D_2$ , and  $D_3$  and any two DFA  $F^{-1}$ -maps  $f: D_1 \rightarrow D_3$  and  $g: D_2 \rightarrow D_3$ , prove that there is a DFA  $D$  and two DFA  $F^{-1}$ -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  $F^{-1}$ -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  $F^{-1}$ -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 DFA  $F^{-1}$ -map isomorphism. This means that if  $D'$  is another DFA and if there are two DFA  $F^{-1}$ -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  $F^{-1}$ -maps  $\varphi: D \rightarrow D'$  and  $\varphi': D' \rightarrow D$  so that  $\varphi' \circ \varphi = \text{id}_D$ ,  $\pi_1 = \pi'_1 \circ \varphi$ ,  $\pi_2 = \pi'_2 \circ \varphi$ ,  $\varphi \circ \varphi' = \text{id}_{D'}$ ,  $\pi'_1 = \pi_1 \circ \varphi'$  and  $\pi'_2 = \pi_2 \circ \varphi'$ .

**Remark:** We denote  $D$  by  $D_1 \prod_{D_3} D_2$  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  $\emptyset$  (this single state is rejecting), observe that there is a unique DFA  $F^{-1}$ -map from every DFA  $D$  to  $T$ . Use this to show that if  $D_1 \prod D_2$  is the product DFA arising in (a), then

$$D_1 \prod D_2 = D_1 \prod_T D_2.$$

**Extra Credit (40 points).** Redo questions (a) and (b) for  $F$ -maps instead of  $F^{-1}$ -maps.

**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, both for  $F$ -maps and  $F^{-1}$ -maps, but this is tricky.

**Problem B7 (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  $\Sigma$  (not necessarily consisting of a single letter). Prove that the set

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

is ultimately periodic.

**TOTAL: 260 + 40 points.**