University of Washington

CSE 322: Introduction to Formal Models in Computer Science
Correctness Proof of Theorem 1.19 in Sipser

Spring 2002 Handout 3

April 12, 2002

There is nothing obvious about the construction in the proof of Theorem 1.19, so the statement near the end of the proof that "the construction of M obviously works correctly" is obviously incorrect. Here is a proof.

Let $A = (Q, \Sigma, \delta, q_0, F)$ be any finite automaton (either deterministic or nondeterministic), $p, q \in Q$, and $x, y \in \Sigma^*$. The notation $(p, xy) \vdash_A^* (q, y)$ means that, if you start A in state p with input xy, then in zero or more transitions A can get to state q with input y remaining unread (that is, A can get to state q after consuming just the prefix x). The notation $\vdash_A$ without the $*$ is analogous, but is used to indicate that the move from p to q happens after exactly one transition rather than in zero or more transitions.

Lemma 1 *$(q_0, w) \vdash_N^* (r, \varepsilon)$ iff $(q_0', w) \vdash_M^* (R, \varepsilon)$ and $r \in R$.*

Proof: The proof is by induction on $|w|$.

Basis ($w = \varepsilon$):

$$
\begin{aligned}
(q_0, \varepsilon) \vdash_N^* (r, \varepsilon) \quad & \text{iff} \quad r \in E(\{q_0\}) && \text{(defn of } E\text{)} \\
& \text{iff} \quad q_0' = R \text{ and } r \in R && \text{(defn of } q_0'\text{)} \\
& \text{iff} \quad (q_0', \varepsilon) \vdash_M^* (R, \varepsilon) \text{ and } r \in R && \text{(no } \varepsilon \text{ transitions)}
\end{aligned}
$$

Induction ($w = xa, a \in \Sigma$):

$$(q_0, xa) \vdash_N^* (r, \varepsilon)$$

$$\text{iff} \quad (\exists s, t) \;\; (q_0, xa) \vdash_N^* (s, a) \text{ and } (s, a) \vdash_N (t, \varepsilon) \text{ and } (t, \varepsilon) \vdash_N^* (r, \varepsilon)$$

$$\text{iff} \quad (\exists s, t) \;\; (q_0, x) \vdash_N^* (s, \varepsilon) \text{ and } t \in \delta(s, a) \text{ and } r \in E(\{t\}) \qquad \text{(Fact 2, defn of } E\text{)}$$

$$\text{iff} \quad (\exists s,t) \;\; (q_0', x) \vdash_M^* (S, \varepsilon) \text{ and } s \in S \text{ and } t \in \delta(s,a) \text{ and } r \in E(\{t\}) \quad \text{(Ind Hyp)}$$

$$\text{iff} \quad (q_0', x) \vdash_M^* (S, \varepsilon) \text{ and } r \in \bigcup_{s \in S} E(\delta(s,a))$$

$$\text{iff} \quad (q_0', x) \vdash_M^* (S, \varepsilon) \text{ and } r \in \delta'(S,a) \qquad \text{(defn of } \delta'\text{)}$$

$$\text{iff} \quad (q_0', xa) \vdash_M^* (S, a) \text{ and } \delta'(S,a) = R \text{ and } r \in R \qquad \text{(Fact 1)}$$

$$\text{iff} \quad (q_0', xa) \vdash_M^* (S, a) \text{ and } (S,a) \vdash_M (R, \varepsilon) \text{ and } r \in R$$

$$\text{iff} \quad (q_0', xa) \vdash_M^* (R, \varepsilon) \text{ and } r \in R$$

□

Now we can use this lemma to prove the correctness of the construction in Theorem 1.19.

Theorem 2 $L(M) = L(N)$.

Proof:

$$w \in L(M) \quad \text{iff} \quad (q_0', w) \vdash_M^* (R, \varepsilon) \text{ and } R \in F' \qquad \text{(defn of } L(M)\text{)}$$

$$\text{iff} \quad (q_0', w) \vdash_M^* (R, \varepsilon) \text{ and } R \cap F \neq \emptyset \qquad \text{(defn of } F'\text{)}$$

$$\text{iff} \quad (\exists r) \;\; (q_0', w) \vdash_M^* (R, \varepsilon) \text{ and } r \in R \text{ and } r \in F$$

$$\text{iff} \quad (\exists r) \;\; (q_0, w) \vdash_N^* (r, \varepsilon) \text{ and } r \in F \qquad \text{(Lemma 1)}$$

$$\text{iff} \quad w \in L(N) \qquad \text{(defn of } L(N)\text{)}$$

□