Correctness Proof for Theorem 1.19 in Sipser

CSE 322: Introduction to Formal Models in Computer Science
January 18, 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 ($w = xa$):

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

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

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

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

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

iff $(q_0', x) \vdash_M^* (S, \varepsilon)$ and $r \in \delta'(S, a)$ (defn of δ')

iff $(q_0', xa) \vdash_M^* (S, a)$ and $\delta'(S, a) = R$ and $r \in R$

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

iff $(q_0', xa) \vdash_M^* (R, \varepsilon)$ 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:

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

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

iff $(\exists r)$ $(q_0', w) \vdash_M^* (R, \varepsilon)$ and $r \in R$ and $r \in F$

iff $(\exists r)$ $(q_0, w) \vdash_N^* (r, \varepsilon)$ and $r \in F$ (Lemma 1)

iff $w \in L(N)$ (defn of $L(N)$)

□