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 nondetermin-
istic), \( p, q \in Q \), and \( x, y \in \Sigma^* \). The notation \( (p, xy) \xrightarrow{A}^*(q, y) \) 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 \( \xrightarrow{A} \) 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** \( (q_0, w) \xrightarrow{N}^*(r, \varepsilon) \) iff \( (q'_0, w) \xrightarrow{M}^*(R, \varepsilon) \) and \( r \in R \).

**Proof:** The proof is by induction on \( |w| \).

**Basis** (\( w = \varepsilon \)):

\[
(q_0, \varepsilon) \xrightarrow{N}^*(r, \varepsilon) \quad \text{iff} \quad r \in E(\{q_0\}) \quad \text{(defn of } E) \\
\quad \text{iff} \quad q'_0 = R \text{ and } r \in R \quad \text{(defn of } q'_0) \\
\quad \text{iff} \quad (q'_0, \varepsilon) \xrightarrow{M}^*(R, \varepsilon) \text{ and } r \in R \quad \text{(no } \varepsilon \text{ transitions)}
\]

**Induction** (\( w = xa \)):

\[
(q_0, xa) \xrightarrow{N}^*(r, \varepsilon) \\
\quad \text{iff} \quad (\exists s, t) \ (q_0, xa) \xrightarrow{N}^*(s, a) \text{ and } (s, a) \xrightarrow{N}^*(t, \varepsilon) \text{ and } (t, \varepsilon) \xrightarrow{N}^*(r, \varepsilon) \\
\quad \text{iff} \quad (\exists s, t) \ (q_0, x) \xrightarrow{N}^*(s, \varepsilon) \text{ and } t \in \delta(s, a) \text{ and } r \in E(\{t\}) \quad \text{(defn of } E) \\
\quad \text{iff} \quad (\exists s, t) \ (q'_0, x) \xrightarrow{M}^*(S, \varepsilon) \text{ and } s \in S \text{ and } t \in \delta(s, a) \text{ and } r \in E(\{t\}) \text{(Ind Hyp)} \\
\quad \text{iff} \quad (q'_0, x) \xrightarrow{M}^*(S, \varepsilon) \text{ and } r \in \bigcup_{s \in S} E(\delta(s, a))
\]
iff \((q_0', x) \vdash_{M}^*(S, \varepsilon)\) and \(r \in \delta'(S, a)\) \hspace{1cm} \text{(defn of } \delta')

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 \(r \in R\)

\(\Box\)

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 \(R \in F'\) \hspace{1cm} \text{(defn of } L(M)\)

iff \((q_0', w) \vdash_{M}^*(R, \varepsilon)\) and \(R \cap F \neq \emptyset\) \hspace{1cm} \text{(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 \(r \in F\) \hspace{1cm} \text{(Lemma 1)}

iff \(w \in L(N)\) \hspace{1cm} \text{(defn of } L(N)\)

\(\Box\)