CSE 322
Converting NFAs to DFAs
Correctness Proof for the Subset Construction

Though the basic idea is intuitive there is nothing "obvious" about the construction in the proof of Theorem 1.39 (Theorem 1.19 of the 1st edition) of the Sipser text, so the statement near the end of that "the construction of M obviously works correctly" is a bit of a stretch. We give a proof here after recapping the construction.

Let $N = (Q, \Sigma, \delta, q_0, F)$ be an NFA. First we review the construction. For $R \subseteq Q$ define $E(R) = \{q \mid q$ can be reached from R by travelling along 0 or more ε edges in $N\}$.
Define the DFA $M = (Q', \Sigma, \delta', q_0', F')$ based on N by:

1. $Q' = \mathcal{P}(Q)$, the set of all subsets of Q,
2. $q_0' = E(\{q_0\})$, and
3. For all $R \in Q'$ and all $a \in \Sigma$ let $\delta'(R, a) = \{q \in Q \mid q \in E(\delta(r, a))$ for some $r \in R\}$, i.e.,
$$\delta'(R, a) = \bigcup_{r \in R} E(\delta(r, a)),$$
4. $F' = \{R \in Q' \mid R$ contains a state in $F\}$.

Now to the proof that $L(M) = L(N)$. We need one convenient bit of notation to describe computations of NFAs. For $p, q \in Q$ and $x, y \in \Sigma^*$ write $(p, xy) \vdash^*_N (q, y)$ iff when NFA N is started in state p with input xy then in zero or more transitions N can get to state q with input y remaining unread and the input prefix x consumed. Simply write $(p, xy) \vdash_N (q, y)$ if this took precisely one transition of N. Note that $(p, xy) \vdash^*_N (q, y)$ if and only if $(p, x) \vdash^*_N (q, \varepsilon)$. Also note that $w \in L(N)$ if and only if there is some state $r \in F$ such that $(q_0, w) \vdash^*_N (r, \varepsilon)$.

Lemma 1. *For all $w \in \Sigma^*$, $(\delta')^*(q_0', w) = \{r \in Q \mid (q_0, w) \vdash^*_N (r, \varepsilon)\}$.*

Proof. Now we prove the claim by induction on w using the recursive definition of Σ^*.
BASE CASE: $w = \varepsilon$. In this case, by definition of $(\delta')^*$, we have $(\delta')^*(q_0', \varepsilon) = q_0' = E(\{q_0\})$. By definition of E, $r \in E(\{q_0\})$ if and only if r can be reached from q_0 by travelling along 0 or more ε edges of N. This condition on r is precisely the requirement that $(q_0, \varepsilon) \vdash^*_N (r, \varepsilon)$ which is what we needed to prove for $w = \varepsilon$.

INDUCTIVE HYPOTHESIS: Assume that for some $x \in \Sigma^*$

$$(\delta')^*(q_0', x) = \{r \in Q \mid (q_0, x) \vdash_N^* (r, \varepsilon)\}.$$

INDUCTION STEP: Consider $w = xa$ for $a \in \Sigma$. Since N reads at most one symbol per step,

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

iff $(\exists s, t \in Q)\ (q_0, xa) \vdash_N^* (s, a)$ and $(s, a) \vdash_N (t, \varepsilon)$ and $(t, \varepsilon) \vdash_N^* (r, \varepsilon)$

iff $(\exists s, t \in Q)\ (q_0, x) \vdash_N^* (s, \varepsilon)$ and $(s, a) \vdash_N (t, \varepsilon)$ and $r \in E(\{t\})$ (by prop of $\vdash_N^*$ and defn of E)

iff $(\exists s, t \in Q)\ s \in (\delta')^*(q_0', x)$ and $t \in \delta(s, a)$ and $r \in E(\{t\})$ (by Ind. Hyp. and defn of $\vdash_N$)

iff $(\exists s \in Q)\ s \in (\delta')^*(q_0', x)$ and $r \in E(\delta(s, a))$ (by defn of E)

iff $r \in \bigcup_{s \in S} E(\delta(s, a))$ for $S = (\delta')^*(q_0', x)$ (by defn of $\bigcup$)

iff $r \in \delta'(S, a)$ for $S = (\delta')^*(q_0', x)$ (by defn of δ')

iff $r \in \delta'((\delta')^*(q_0', x), a)$

iff $r \in (\delta')^*(q_0', xa)$ (by defn of $(\delta')^*$).

Therefore $(\delta')^*(q_0', xa) = \{r \in Q \mid (q_0, xa) \vdash_N^* (r, \varepsilon)\}$ as required and the result follows by induction. □

Now we can use this lemma to prove Theorem 1.39.

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

Proof. By definition,

$$\begin{aligned} w \in L(M) \quad & \text{iff} \quad (\delta')^*(q_0', w) \in F' \\ & \text{iff} \quad (\exists r \in F)\ r \in (\delta')^*(q_0', w) \qquad \text{(by defn of } F'\text{)} \\ & \text{iff} \quad (\exists r \in F)\ (q_0, w) \vdash_N^* (r, \varepsilon) \qquad \text{(by Lemma 1)} \\ & \text{iff} \quad w \in L(N) \qquad \text{(by definition of } L(N)\text{).} \end{aligned}$$

□