CSE 322
Converting NFA's to DFA's: The Subset Construction

April 18, 2000

Theorem 1: For every NFA there is an equivalent DFA.

The key idea involved in converting an NFA to a DFA is that we can create individual states for our DFA that record *all* the possible states that our NFA can be in at a given point in the computation. Thus each state of our new DFA will be a *set* of states of the NFA, hence the name for the construction.

The following construction is exactly the same as that given by Lewis and Papadimitriou. The proof of its correctness is, however, slightly simpler than theirs.

Proof Let $M = (K, \Sigma, \delta, s', F')$. Let the e-closure of q, $E(q) = \{p \mid (q, e) \vdash_M^* (p, e)\}$, the set of states reachable from s by following only e-moves.

We define the DFA $M' = (K', \Sigma, \delta, s', F')$ based on M by:

- $K' = \mathcal{P}(K) = 2^K$, i.e., the set of all subsets of K,
- $F' = \{Q \subseteq K \mid Q \cap F \neq \emptyset\}$, i.e. $Q \in F'$ if and only if Q contains a final state of M,
- $s' = E(s)$, and
- for all $a \in \Sigma$ and all $R \in K'$,

  $$\delta(R, a) = \{q \mid (r, a) \vdash_M (r', e) \vdash_M^* (q, e) \text{ for some } r \in R \text{ and } r' \in K\},$$

  i.e., the set of all states of M reachable from some state in R by first reading a and then following a sequence of e-moves. Note that this is the same as saying

  $$\delta(R, a) = \{q \mid (r, a, r') \in \Delta \text{ and } q \in E(r') \text{ for some } r \in R \text{ and } r' \in K\}.$$

The idea behind this definition is that the state M' is in after reading an input represents the *set* of states that M could be in after reading that input. The following claim formalizes this property.

CLAIM: For all $w \in \Sigma^*$, let Q be the unique state of M' such that $(E(s), w) \vdash_{M'}^* (Q, e)$. Then $Q = \{q \mid (s, w) \vdash_M^* (q, e)\}$.

Before we go about proving this claim, let's see how we can use it to prove that M and M' are equivalent. To see that the claim implies the desired result we note that:

$$\begin{aligned}
w \in L(M') &\Leftrightarrow (s', w) \vdash_{M'}^* (Q, e) \text{ where } Q \in F' \\
&\Leftrightarrow (E(s), w) \vdash_{M'}^* (Q, e) \text{ where } Q \cap F \neq \emptyset \\
&\Leftrightarrow Q = \{q \mid (s, w) \vdash_M^* (q, e)\} \text{ and } Q \cap F \neq \emptyset \text{ by the claim} \\
&\Leftrightarrow (s, w) \vdash_M^* (q, e) \text{ for some } q \in F \\
&\Leftrightarrow w \in L(M)
\end{aligned}$$

which is what we needed to show.

Now we prove the claim by induction on $|w|$.

BASE CASE: $|w| = 0$ so $w = e$. In this case

$$\begin{aligned} (E(s), e) \vdash_{M'}^* (Q, e) &\Leftrightarrow Q = s' \qquad\qquad \text{since } M' \text{ is deterministic} \\ &\Leftrightarrow Q = E(s) = \{q \mid (s, e) \vdash_M^* (q, e)\} \end{aligned}$$

by the definition of s'. This is what we needed to show so the claim holds for $w = e$.

INDUCTION HYPOTHESIS: Assume that for all $x \in \Sigma^*$ with $|x| \leq k$,

$$(E(s), x) \vdash_{M'}^* (Q, e) \Leftrightarrow Q = \{q \mid (s, x) \vdash_M^* (q, e)\}.$$

INDUCTION STEP: Let $x \in \Sigma^*$ with $|x| = k + 1$. Therefore $x = wa$ for some $a \in \Sigma$ and $w \in \Sigma^*$ with $|w| = k$. Let $Q \in K'$ be such that $(E(s), x) \vdash_{M'}^* (Q, e)$. We must show that $Q = \{q \mid (s, x) \vdash_M^* (q, e)\}$. Since M' is a DFA, Q is uniquely defined and there is also a unique state $R \in K'$ such that

$$(E(s), x) = (s', wa) \vdash_{M'}^* (R, a) \vdash_{M'} (Q, e).$$

Using the Useful Fact about DFA's and NFA's, we also have $(E(s), w) \vdash_{M'}^* (R, e)$. Therefore, since $|w| = k$, we can apply the inductive hypothesis for w to say that $R = \{r \mid (s, w) \vdash_M^* (r, e)\}$. Furthermore, by the definition of δ,

$$Q = \delta(R, a) = \{q \mid (r, a) \vdash_M (r', e) \vdash_M^* (q, e) \text{ for some } r \in R \text{ and } r' \in K\}.$$

We will show that $Q = \{q \mid (s, ya) \vdash_M^* (q, e)\}$ using these facts.

First, suppose that $q \in Q = \delta(R, a)$. Then there is an $r \in R$ such that $(r, a) \vdash_M (r', e) \vdash_M^* (q, e)$, by the definition of δ. Furthermore, $r \in R$ implies that $(s, y) \vdash_M^* (r, e)$ which implies that $(s, ya) \vdash_M^* (r, a)$ by the Useful Fact for NFA's. Putting these together we have

$$(s, ya) \vdash_M^* (r, a) \vdash_M (r', e) \vdash_M^* (q, e),$$

and so $(s, ya) \vdash_M^* (q, e)$.

Now conversely suppose that $(s, ya) \vdash_M^* (q, e)$. Because M reads at most one symbol per step there must be some state r of M in which M reads the last a in the input during this computation. Thus there are states $r, r' \in K$ such that

$$(s, ya) \vdash_M^* (r, a) \vdash_M (r', e) \vdash_M^* (q, e)$$

Therefore we have (i) $(s, ya) \vdash_M^* (r, a)$, and (ii) $(r, a) \vdash_M (r', e) \vdash_M^* (q, e)$. Part (i) implies that $(s, y) \vdash_M^* (r, e)$ by the Useful Fact for NFA's and thus $r \in R$. This, coupled with part (ii) and the definition of δ, implies that $q \in \delta(R, a) = Q$.

The two preceding paragraphs imply that $Q = \{q \mid (s, x) \vdash_M^* (q, e)\}$ and the claim follows for $|x| = k + 1$ and by induction holds for all $x \in \Sigma^*$. $\square$

Notice that the subset construction will in general convert an NFA to a DFA with a large number of states ($2^{|K|}$). In the worst case, this increase is necessary, but in many cases this number of states can be reduced by eliminating states of the DFA that are not reachable on any input in Σ^*.