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

April, 2003

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. The proof makes use of the following fact about DFA's and NFA's (e denotes the empty or null string throughout the proof):

Useful Fact about DFA's and NFA's: For a DFA or NFA N, for every $a \in \Sigma$, $(q_1, y) \vdash_N^* (q_2, e)$ for states q_1, q_2 and $y \in \Sigma^*$ if and only if $(q_1, ya) \vdash_N^* (q_2, a)$.

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 1 *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.

Let us define $\mathsf{Reach}_M(s, x) = \{q \mid (s, x) \vdash^*_M (q, e)\}$ since this set captures the states M can be at starting from s and reading string x. We have to prove the claim which states that for every $x \in \Sigma^*$, $(E(s), x) \vdash^*_{M'} (\mathsf{Reach}_M(s, x), e)$. We prove this by induction on $|x|$.

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

$$\begin{aligned} (E(s), e) \vdash^*_{M'} (Q, e) &\Leftrightarrow Q = s' \qquad \text{since } M' \text{ is deterministic} \\ &\Leftrightarrow Q = E(s) = \mathsf{Reach}_M(s, e) \end{aligned}$$

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

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

$$(E(s), w) \vdash^*_{M'} (Q, e) \Leftrightarrow Q = \mathsf{Reach}_M(s, w).$$

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 $Q = \mathsf{Reach}_M(s, x) = \{q \mid (s, x) \vdash^*_M (q, e)\}$. Since M' is a DFA, Q is uniquely defined and there is also a unique state $R \in K'$ such that

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

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 induction hypothesis for w to say that $R = \mathsf{Reach}_M(s, w) = \{r \mid (s, w) \vdash^*_M (r, e)\}$. 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 $Q = \mathsf{Reach}_M(s, wa)$ using these facts.

We first show $Q \subseteq \mathsf{Reach}_M(s, wa)$. Indeed, let $q \in Q = \delta(R, a)$. 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 $(s, w) \vdash^*_M (r, e)$ which implies that $(s, wa) \vdash^*_M (r, a)$ by the Useful Fact for NFA's. Putting these together we have

$$(s, wa) \vdash^*_M (r, a) \vdash_M (r', e) \vdash^*_M (q, e),$$

and so $(s, wa) \vdash^*_M (q, e)$, or in other words $q \in \mathsf{Reach}_M(s, wa)$.

We next show that $\mathsf{Reach}_M(wa) \subseteq Q$. Indeed let $q \in \mathsf{Reach}_M(s, wa)$ so that $(s, wa) \vdash^*_M (q, e)$. 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

$$(s, wa) \vdash^*_M (r, a) \vdash_M (r', e) \vdash^*_M (q, e)$$

Therefore we have (i) $(s, wa) \vdash^*_M (r, a)$, and (ii) $(r, a) \vdash_M (r', e) \vdash^*_M (q, e)$. Part (i) implies that $(s, w) \vdash^*_M (r, e)$ 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 $Q = \mathsf{Reach}_M(s, x)$ and the claim follows for $|x| = k + 1$ and by induction holds for all $x \in \Sigma^*$. $\square$