11-2018

Nondeterministic Finite Automata Correspond to Deterministic Ones

Doug Baldwin
SUNY Geneseo, baldwin@geneseo.edu

James Jasinski
SUNY Geneseo

Matt Klein
SUNY Geneseo

Jack McAlevey
SUNY Geneseo

Ian Parks
SUNY Geneseo

See next page for additional authors

Authors
Doug Baldwin, James Jasinski, Matt Klein, Jack McAlevey, Ian Parks, Susanna Rohe, Praveen Wakwella, John Wilson, and Kevin Wojick

Nondeterministic Finite Automata Are Equivalent to Deterministic Finite Automata

Doug Baldwin, James Jasinski, Matt Klein, Jack McAlevey,
Ian Parks, Susanna Rohe, Praveen Wakwella,
John Wilson, Kevin Wojick
Department of Mathematics, SUNY Geneseo

November 2018

That every nondeterministic finite automaton is equivalent to a deterministic one is a standard theorem in computability theory. Maheshwari and Smid's text [1] shows how to construct a deterministic automaton from a nondeterministic one, but does not show that the constructed automaton accepts the same language as the original. This document provides that proof.

Let us first define a notation for the configuration of a finite automaton, as well as the "yields" relation $\vdash$. Consider a finite automaton (either deterministic or nondeterministic) with alphabet Σ and transition function δ in some state q that has an unconsumed string w. We can say that the ordered pair (q, w) indicates the configuration of the automaton, i.e. that the automaton is in state q and computing on w. If $w = av$ where $a \in \Sigma$ and v is an arbitrary string, then we can also say that $(q, av) \vdash (r, v)$ where $r = \delta(q, a)$ for a deterministic finite automaton and $r \in \delta(q, a)$ for a nondeterministic one. For nondeterministic automata, we also say that $(q, u) \vdash (r, u)$ when $r \in \delta(q, \epsilon)$. We can further define the "transitively yields" relation $\vdash^*$, which describes a configuration that can be reached through zero or more "yields" transitions. These notations will be useful for the following proof.

Let $N = (Q, \Sigma, \delta, q_0, F)$ be a nondeterministic finite automaton, and let $M = (Q', \Sigma, \delta', q_0', F')$ be the deterministic finite automaton constructed from N by Maheshwari and Smid's construction. We show that $L(M) = L(N)$ as a corollary to the following pair of theorems:

Theorem 1. For every string u over Σ, if there is a state $R \in Q'$ such that $(q_0', u) \vdash^* (R, \epsilon)$ in M, then $(q_0, u) \vdash^* (r, \epsilon)$ in N for all states $r \in R$.

Proof. The proof is by induction on $|u|$, the length of the string u.

For the basis step, suppose $|u| = 0$, i.e., $u = \epsilon$. Then $(q_0', u) = (q_0', \epsilon) \vdash^* (R, \epsilon)$ in M, and we see that $R = q_0'$, since M goes from q_0' to R without consuming any input. From the construction, we know that q_0' is the ϵ-closure of q_0, which is exactly the set of states N can reach from q_0 without consuming input. In other words, for every one of the states r in q_0' (which is R), we can write that $(q_0, u) = (q_0, \epsilon) \vdash^* (r, \epsilon)$ in N, and thus we have proven the basis step.

For the induction step, we assume that for an integer $k = |u|$, the existence of a state $Y \in Q'$ such that $(q_0', u) \vdash^* (Y, \epsilon)$ in M implies that for all states $y \in Y$, $(q_0, u) \vdash^* (y, \epsilon)$ in N.

Now, let w be a string over Σ such that w is of length $k + 1$. We will show that for a new state R, if $(q_0', w) \vdash^* (R, \epsilon)$ in M, then $(q_0, w) \vdash^* (r, \epsilon)$ in N for all $r \in R$. Let $w = ua$, where $a \in \Sigma$, and let $(q_0', w) = (q_0', ua) \vdash^* (Y, a)$ in M. From the inductive hypothesis, we see that this implies that for all states $y \in Y$, $(q_0, ua) \vdash^* (y, a)$ in N. In M, we can consider the transition function at Y, $\delta'(Y, a)$. Because M is deterministic, we know $\delta'(Y, a) \neq \varnothing$. Therefore, we can write that $\delta'(Y, a)$ equals some state R. As a result, we can write $(q_0', w) = (q_0', ua) \vdash^* (Y, a) \vdash (R, \epsilon)$. In N, the set of all transitions from (y, a) for all $y \in Y$ is the union of the ϵ-closure of each state $\delta(y, a)$. In other words, the set of all transitions is

$$\bigcup_{y \in Y} C_\epsilon(\delta(y, a))$$

Notice that, because M has been created following the construction laid out in Maheshwari and Smid's text [1], the above is equal to $\delta'(Y, a)$, which is R. Therefore, we can write $(q_0, w) = (q_0, ua) \vdash^* (y, a) \vdash (r, \epsilon)$ in N for all states $r \in R$, and thus we have shown for $|w| = k + 1$, if $(q_0', w) \vdash^* (R, \epsilon)$ in M for $R \in Q'$, then $(q_0, w) \vdash^* (r, \epsilon)$ in N for all states $r \in R$, and the inductive step is proven.

Thus, because we have shown Theorem 1 to be true for the basis step, and true for each inductive step after, we know that Theorem 1 is true. □

Figure 1 demonstrates the relationship between the Y and R states in M and the corresponding y and r states in N.

Theorem 2. For every string u over Σ, if R is the set of all states r in Q for which $(q_0, u) \vdash^* (r, \epsilon)$ in N, then $(q_0', u) \vdash^* (R, \epsilon)$ in M.

Proof. Once again, the proof is by induction on the length of u. For the basis step, suppose $|u| = 0$, i.e., $u = \epsilon$. Then $(q_0, \epsilon) \vdash^* (r, \epsilon)$ in N where the set of all states r defines R. Notice that $R = C_\epsilon(q_0)$ because N goes from q_0 to r without consuming any input. Furthermore, we also know that $q_0' = C_\epsilon(q_0)$ from the construction in the text [1]. Therefore, $R = q_0'$, and so $(q_0', u) = (q_0', \epsilon) \vdash^* (q_0', \epsilon) = (R, \epsilon)$, and the basis step is proven.

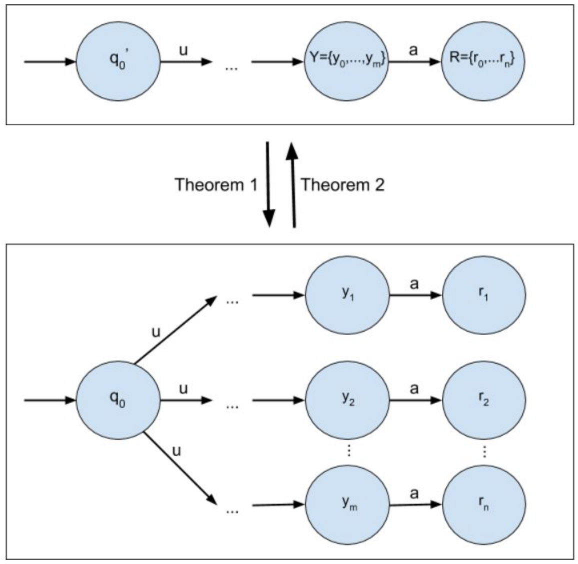

Figure 1: This image illustrates the relationship between the states Y and R in M and the corresponding states y and r in N. Theorem 1 describes the existence of the y and r states in N given the existence of the states Y and R in M, whereas Theorem 2 does the opposite.

For the inductive step, we assume that for an integer $k = |u|$, the existence of Y where Y is the set of all states $y \in Q$ for which $(q_0, u) \vdash^* (y, \epsilon)$ in N implies that $(q_0', u) \vdash^* (Y, \epsilon)$ in M.

Now, let w be a string over Σ of length $k+1$. We will show that for a new set of states R, if $(q_0, w) \vdash^* (r, \epsilon)$ in N for all $r \in R$, then in M $(q_0', w) \vdash^* (R, \epsilon)$. Let $w = ua$, where $a \in \Sigma$, and let $(q_0, w) = (q_0, ua) \vdash^* (y, a)$ in N where the set of all y is Y. From the inductive hypothesis we can see that this implies that $(q_0', ua) \vdash^* (Y, a)$ in M. In N, we can consider the set of states r that result from the transition function at each $y \in Y$, $\delta(y, a)$. This set is the union of the ϵ-closure of each transition $\delta(y, a)$. Let this set be R, which is described as follows:

$$R = \bigcup_{y \in Y} C_\epsilon(\delta(y, a))$$

By the construction laid out in the text [1], we know that

$$\bigcup_{y \in Y} C_\epsilon(\delta(y, a)) = \delta'(Y, a)$$

and so $\delta'(Y, a) = R$. Therefore, we can write $(q_0', w) = (q_0', ua) \vdash^* (Y, a) \vdash (R, \epsilon)$ in M, and thus we have shown for $|w| = k + 1$, if $(q_0, w) \vdash^* (r, \epsilon)$ in N for all $r \in R$, then $(q_0', w) \vdash^* (R, \epsilon)$ in M, and the inductive step is proven.

Thus, because we have shown Theorem 2 to be true for a basis step, and true for each inductive step after, we know that Theorem 2 is true. □

Again, Figure 1 demonstrates the relationship between the y and r states in N and the corresponding Y and R states in M.

We can now show that a nondeterministic finite automaton and the deterministic automaton created from it using the construction in the Maheshwari and Smid text [1] accept the same language.

Corollary 1. $L(M) = L(N)$.

Proof. We show that $L(M) = L(N)$ by showing that for all strings w over Σ, M accepts w if and only if N does. We prove each direction separately.

If. Suppose N accepts w, i.e., $(q_0, w) \vdash^* (r, \epsilon)$ for at least one $r \in F$. Let R be the set of all states r such that $(q_0, w) \vdash^* (r, \epsilon)$. Then by Theorem 2, $(q_0', w) \vdash^* (R, \epsilon)$ in M, and since at least one member of R is an accepting state of N, R is an accepting state of M. Thus M accepts w.

Only if. Suppose M accepts w, i.e., $(q_0', w) \vdash^* (R, \epsilon)$ for some state $R \in F'$. Then by Theorem 1, $(q_0, w) \vdash^* (r, \epsilon)$ in N for all states $r \in R$. The only way R can be an accepting state of M is if at least one such r is an accepting state of N, so N accepts w.

Since we have shown that M accepts w if N does, and N accepts w if M does, then we can conclude that $L(M) = L(N)$. □

References

[1] Anil Maheshwari and Michiel Smid. Introduction to theory of computation. (http://cglab.ca/∼michiel/TheoryOfComputation/), School of Computer Science, Carleton University, March 2017.