Section 3.7: Proving the Correctness of Finite Automata

In this section, we consider techniques for proving the correctness of finite automata, i.e., for proving that finite automata accept the languages we want them to. We begin with some propositions concerning the Δ function.

The LaTeX source of these slides, the associated book, and the distribution of the Forlan toolset are available on the WWW at http://people.cis.ksu.edu/~stough/forlan/.

(3.7) Propositions for Δ

Proposition 3.7.1

Suppose M is a finite automaton.

(1) *For all $q \in Q_M$, $q \in \Delta_M(\{q\}, \%)$.*

(2) *For all $q, r \in Q_M$ and $w \in \mathbf{Str}$, if $(q, w, r) \in T_M$, then $r \in \Delta_M(\{q\}, w)$.*

(3) *For all $p, q, r \in Q_M$ and $x, y \in \mathbf{Str}$, if $q \in \Delta_M(\{p\}, x)$ and $r \in \Delta_M(\{q\}, y)$, then $r \in \Delta_M(\{p\}, xy)$.*

(3.7) Propositions for Δ (Cont.)

Proposition 3.7.2
Suppose M is a finite automaton. For all $p, r \in Q_M$ and $w \in \mathbf{Str}$, if $r \in \Delta_M(\{p\}, w)$, then either:

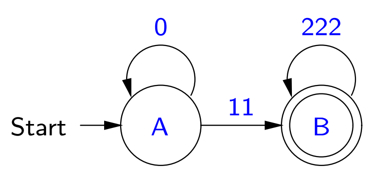
- $r = p$ *and* $w = \%$*; or*
- *there are* $q \in Q_M$ *and* $x, y \in \mathbf{Str}$ *such that* $w = xy$, $(p, x, q) \in T_M$ *and* $r \in \Delta_M(\{q\}, y)$.

Proposition 3.7.3
Suppose M is a finite automaton. For all $p, r \in Q_M$ and $w \in \mathbf{Str}$, if $r \in \Delta_M(\{p\}, w)$, then either:

- $r = p$ *and* $w = \%$*; or*
- *there are* $q \in Q_M$ *and* $x, y \in \mathbf{Str}$ *such that* $w = xy$, $q \in \Delta_M(\{p\}, x)$ *and* $(q, y, r) \in T_M$.

(3.7) Example Correctness Proof

Let M be the finite automaton



To prove that $L(M) = \{0\}^*\{11\}\{222\}^*$, it will suffice to show that $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$ and $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$.

First, we show that $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$; then, we show that $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$.

(3.7) $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$

First, we use mathematical induction to prove that, for all $n \in \mathbb{N}$, $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n)$.

- (Basis Step) By Proposition 3.7.1(1), we have that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \%)$. But $\mathsf{0}^0 = \%$, and thus $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^0)$.
- (Inductive Step) Suppose $n \in \mathbb{N}$, and assume the inductive hypothesis: $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n)$. We must show that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^{n+1})$. Since $(\mathsf{A}, \mathsf{0}, \mathsf{A}) \in T$, Proposition 3.7.1(2) tells us that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0})$. Since $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0})$ and $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n)$, Proposition 3.7.1(3) tells us that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{00}^n)$. Since $\mathsf{0}^{n+1} = \mathsf{00}^n$, it follows that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^{n+1})$.

Similarly, we can use mathematical induction to prove that, for all $n \in \mathbb{N}$, $\mathsf{B} \in \Delta(\{\mathsf{B}\}, (\mathsf{222})^n)$.

(3.7) $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$ (Cont.)

Now, suppose $w \in \{0\}^*\{11\}\{222\}^*$. Then $w = \mathsf{0}^n\mathsf{11}(\mathsf{222})^m$ for some $n, m \in \mathbb{N}$. By the result of our first induction, we have that $\mathsf{A} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n)$. Since $(\mathsf{A}, \mathsf{11}, \mathsf{B}) \in T$, we have that $\mathsf{B} \in \Delta(\{\mathsf{A}\}, \mathsf{11})$, by Proposition 3.7.1(2). Thus, by Proposition 3.7.1(3), we have that $\mathsf{B} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n\mathsf{11})$. By the result of our second induction, we have that $\mathsf{B} \in \Delta(\{\mathsf{B}\}, (\mathsf{222})^m)$. Thus, by Proposition 3.7.1(3), we have that $\mathsf{B} \in \Delta(\{\mathsf{A}\}, \mathsf{0}^n\mathsf{11}(\mathsf{222})^m)$. But $w = \mathsf{0}^n\mathsf{11}(\mathsf{222})^m$, and thus $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$. Since A is M's start state and B is an accepting state of M, it follows that $\Delta(\{s_M\}, w) \cap A_M \neq \emptyset$, so that (by Proposition 3.5.3) $w \in L(M)$.

(3.7) $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$

Since $\mathbf{alphabet}(M) = \{0, 1, 2\}$, it will suffice to show that, for all $w \in \{0, 1, 2\}^*$,

$$\text{if } \mathsf{B} \in \Delta(\{\mathsf{A}\}, w), \text{ then } w \in \{0\}^*\{11\}\{222\}^*.$$

(To see that this is so, suppose $w \in L(M)$. Then $\Delta(\{\mathsf{A}\}, w) \cap \{\mathsf{B}\} \neq \emptyset$, so that $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$. By Proposition 3.3.1, we have that

$$\mathbf{alphabet}(w) \subseteq \mathbf{alphabet}(L(M)) \subseteq \mathbf{alphabet}(M) = \{0, 1, 2\},$$

so that $w \in \{0, 1, 2\}^*$. Thus $w \in \{0\}^*\{11\}\{222\}^*$.)

(3.7) $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$ (Cont.)

We use strong string induction to show that, for all $w \in \{0, 1, 2\}^*$,

(A) if $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*$;

(B) if $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*\{11\}\{222\}^*$.

Suppose $w \in \{0, 1, 2\}^*$, and assume the inductive hypothesis: for all $x \in \{0, 1, 2\}^*$, if $|x| < |w|$, then

(A) if $\mathsf{A} \in \Delta(\{\mathsf{A}\}, x)$, then $x \in \{0\}^*$;

(B) if $\mathsf{B} \in \Delta(\{\mathsf{A}\}, x)$, then $x \in \{0\}^*\{11\}\{222\}^*$.

We must show that

(A) if $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*$;

(B) if $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*\{11\}\{222\}^*$.

(3.7) $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$ (Cont.)

(A) Suppose $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$. We must show that $w \in \{0\}^*$. By Proposition 3.7.3, there are two cases to consider.

- Suppose $\mathsf{A} = \mathsf{A}$ and $w = \%$. Then $w = \% \in \{0\}^*$.
- Suppose there are $q \in Q$ and $x, y \in \mathbf{Str}$ such that $w = xy$, $q \in \Delta(\{\mathsf{A}\}, x)$ and $(q, y, \mathsf{A}) \in T$. Since $(q, y, \mathsf{A}) \in T$, we have that $q = \mathsf{A}$ and $y = 0$, so that $w = x0$ and $\mathsf{A} \in \Delta(\{\mathsf{A}\}, x)$. Since $|x| < |w|$, part (A) of the inductive hypothesis tells us that $x \in \{0\}^*$. Thus $w = x0 \in \{0\}^*\{0\} \subseteq \{0\}^*$.

(3.7) $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$ (Cont.)

(B) Suppose $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$. We must show that $w \in \{0\}^*\{11\}\{222\}^*$. Since $\mathsf{B} \neq \mathsf{A}$, Proposition 3.7.3 tells us that there are $q \in Q$ and $x, y \in \mathbf{Str}$ such that $w = xy$, $q \in \Delta(\{\mathsf{A}\}, x)$ and $(q, y, \mathsf{B}) \in T$. Thus there are two cases to consider.

- Suppose $q = \mathsf{A}$ and $y = 11$. Thus $w = x11$ and $\mathsf{A} \in \Delta(\{\mathsf{A}\}, x)$. Since $|x| < |w|$, part (A) of the inductive hypothesis tells us that $x \in \{0\}^*$. Thus $w = x11\% \in \{0\}^*\{11\}\{222\}^*$.
- Suppose $q = \mathsf{B}$ and $y = 222$. Thus $w = x222$ and $\mathsf{B} \in \Delta(\{\mathsf{A}\}, x)$. Since $|x| < |w|$, part (B) of the inductive hypothesis tells us that $x \in \{0\}^*\{11\}\{222\}^*$. Thus $w = x222 \in \{0\}^*\{11\}\{222\}^*\{222\} \subseteq \{0\}^*\{11\}\{222\}^*$.

(3.7) Alternative Approach to $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$

We could also prove $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$ by strong string induction. To prove that $L(M) \subseteq \{0\}^*\{11\}\{222\}^*$, we proved that, for all $w \in \{0,1,2\}^*$:

(A) if $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*$;

(B) if $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*\{11\}\{222\}^*$.

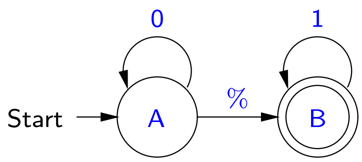
To prove that $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$, we could simply reverse the implications in (A) and (B) of this formula, proving that for all $w \in \{0,1,2\}^*$:

(A) if $w \in \{0\}^*$, then $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$;

(B) if $w \in \{0\}^*\{11\}\{222\}^*$, then $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$.

(3.7) Correctness Proofs for FAs with %-Moves

Suppose N is the finite automaton



To prove that $L(N) = \{0\}^*\{1\}^*$, it will suffice to show that $L(N) \subseteq \{0\}^*\{1\}^*$ and $\{0\}^*\{1\}^* \subseteq L(N)$.

The proof that $\{0\}^*\{1\}^* \subseteq L(N)$ is similar to our proof that $\{0\}^*\{11\}\{222\}^* \subseteq L(M)$.

(3.7) Correctness Proofs with %-Moves (Cont.)

To show that $L(N) \subseteq \{0\}^*\{1\}^*$, it would suffice to show that, for all $w \in \{0,1\}^*$,

(A) if $\mathsf{A} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*$;

(B) if $\mathsf{B} \in \Delta(\{\mathsf{A}\}, w)$, then $w \in \{0\}^*\{1\}^*$.

Can we prove this using strong string induction? No—because of the transition $(\mathsf{A}, \%, \mathsf{B})$, the proof of part (B) will fail. Here is how the failed proof begins.

> There are $q \in Q$ and $x, y \in \mathbf{Str}$ such that $w = xy$, $q \in \Delta(\{\mathsf{A}\}, x)$ and $(q, y, \mathsf{B}) \in T$. Since $(q, y, \mathsf{B}) \in T$, there are two cases to consider. Let's consider the case when $q = \mathsf{A}$ and $y = \%$. Then $w = x\%$ and $\mathsf{A} \in \Delta(\{\mathsf{A}\}, x)$.

Unfortunately, $|x| = |w|$, and so we won't be able to use part (A) of the inductive hypothesis to conclude that $x \in \{0\}^*$.

(3.7) Correctness Proofs with %-Moves (Cont.)

Instead, we would have to use mathematical induction on the length of the labeled paths taking us from A to A and B. See the book for the details.