Mutual Induction Proof From Lecture

CS 234

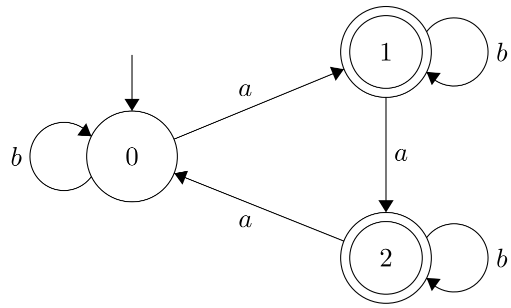
0 Introduction

This document contains an example of a good proof based on the mutual induction lecture. This is not the only ways to write good proofs.

These proofs may contain footnotes explaining different thought processes that occurred in their construction, to help show you how to think about writing proofs. Commentary may also be provided at the end about alternative approaches.

1 Proof

Let M be the following DFA:



Let $\#a(w)$ give the number of as in the string w. Formally, for the alphabet $\{a, b\}$, this function can be defined as:

$$\#a(w) = \begin{cases} 0 & w = \epsilon \\ \#a(u) & w = ub \\ \#a(u) + 1 & w = ua \end{cases}$$

Theorem 1. *$\mathcal{L}(M)$ is given by*

$$\{w \in \{a, b\}^* \mid (\exists z \in \mathbb{Z}.\, \#a(w) = 3z + 1) \vee (\exists z \in \mathbb{Z}.\, \#a(w) = 3z + 2)\}$$

Proof. This statement is proven by mutual induction using the following 3 predicates:

$$A(n) := \forall w \in \{a, b\}^*.\, |w| = n \to (\hat{\delta}(0, w) = 0 \leftrightarrow \exists z \in \mathbb{Z}.\, \#a(w) = 3z)$$

$$B(n) := \forall w \in \{a, b\}^*.\, |w| = n \to (\hat{\delta}(0, w) = 1 \leftrightarrow \exists z \in \mathbb{Z}.\, \#a(w) = 3z + 1)$$

$$C(n) := \forall w \in \{a, b\}^*.\, |w| = n \to (\hat{\delta}(0, w) = 2 \leftrightarrow \exists z \in \mathbb{Z}.\, \#a(w) = 3z + 2)$$

Base Case $n = 0$ Let w be a string over the alphabet $\{a, b\}$ of length 0. There is only one string of length 0, the empty string ϵ, so $w = \epsilon$. Then we know both that $\hat{\delta}(0, w) = \hat{\delta}(0, \epsilon) = 0 = 3 \cdot 0$ by the definition of $\hat{\delta}$, and that $\#a(w) = \#a(\epsilon) = 0$ by the definition of $\#a$.

Because $\hat{\delta}(0, w) = 0$ and $\#a(w) = 3 \cdot 0$, both sides of $A(0)$'s biconditional hold, rendering $A(0)$ true. Because $\hat{\delta}(0, w)$ is not 1 or 2 and 0 cannot be written as $3z+1$ or $3z+2$ for any integer z, both sides of $B(0)$'s and $C(0)$'s biconditionals are false, rendering both $B(0)$ and $C(0)$ true. This case is therefore complete.

Inductive Case Suppose for the inductive hypothesis that all of $A(n)$, $B(n)$, and $C(n)$ hold for some natural n. We want to show each of $A(n+1)$, $B(n+1)$, and $C(n+1)$.

Let w be an arbitrary string over the alphabet $\{a, b\}$ of length $n+1$. Because $n + 1 \geq 1$, it must be that $w = uc$ for some string u of length n and $c \in \{a, b\}$. The proof now proceeds by cases over the result of $\hat{\delta}(0, u)$ and the identity of c.

Subcase $\hat{\delta}(0,u) = 0, c = a$ Suppose that $\hat{\delta}(0,u) = 0$ and $c = a$. Observe then the following:

$$\begin{aligned}
\hat{\delta}(0,w) =& \hat{\delta}(0,ua) && [w = uc, c = a] \\
=& \delta(\hat{\delta}(0,u), a) && [\hat{\delta}\ def] \\
=& \delta(0,a) && [\hat{\delta}(0,u) = 0] \\
=& 1 && [\delta\ def]
\end{aligned}$$

Further, because $\hat{\delta}(0,u) = 0$, the inductive hypothesis guarantees for us that $\#a(u) = 3z$ for some integer z. As a result:

$$\begin{aligned}
\#a(w) =& \#a(ua) && [w = uc, c = a] \\
=& \#a(u) + 1 && [\#a\ def] \\
=& 3z + 1 && [\#a(u) = 3z]
\end{aligned}$$

Thus $\hat{\delta}(0,w) = 1$ and $\#a(w) = 3z+1$ for some integer z. These propositions satisfy both sides of $B(n+1)$'s biconditional, rednering $B(n+1)$ true. At the same time, Because $\hat{\delta}(0,w)$ is not 0 or 2 and a number of the form $3z+1$ cannot be written as $3z'$ or $3z'+2$ for any integer z',[1] if follows that both sides of $A(n+1)$ and $C(n+1)$'s biconditionals are false, rendering both $A(n+1)$ and $C(n+1)$ true.

Subcase $\hat{\delta}(0,u) = 0, c = b$ [2] Suppose that $\hat{\delta}(0,u) = 0$ and $c = b$. Observe then the following:

$$\begin{aligned}
\hat{\delta}(0,w) =& \hat{\delta}(0,ub) && [w = uc, c = b] \\
=& \delta(\hat{\delta}(0,u), b) && [\hat{\delta}\ def] \\
=& \delta(0,b) && [\hat{\delta}(0,u) = 0] \\
=& 0 && [\delta\ def]
\end{aligned}$$

Further, because $\hat{\delta}(0,u) = 0$, the inductive hypothesis guarantees for us that $\#a(u) = 3z$ for some integer z. As a result:

$$\begin{aligned}
\#a(w) =& \#a(ub) && [w = uc, c = b] \\
=& \#a(u) && [\#a\ def] \\
=& 3z && [\#a(u) = 3z]
\end{aligned}$$

[1] This is a slightly nontrivial mathematical fact. However, I think this is simple enough (and far enough away from the concepts I am trying to have you learn) that it is safe to accept as an assertion. Nontrivial mathematical facts will often require proof to make use of (or a citation to where it is proved), and part of knowing your audience is knowing when to prove them. I'll provide a proof after the end of this one just to show you.

[2] This case has almost the same wording as the previous. This is perfectly fine, and even signals to the reader that you are doing something repetitive.

Thus $\hat{\delta}(0, w) = 0$ and $\#a(w) = 3z$ for some integer z. These propositions satisfy both sides of $A(n+1)$'s biconditional, rednering $A(n+1)$ true. At the same time, Because $\hat{\delta}(0, w)$ is not 1 or 2 and a number of the form $3z$ cannot be written as $3z' + 1$ or $3z' + 2$ for any integer z', if follows that both sides of $B(n+1)$ and $C(n+1)$'s biconditionals are false, rendering both $B(n+1)$ and $C(n+1)$ true.

Subcase $\hat{\delta}(0, u) = 1, c = a$ Suppose that $\hat{\delta}(0, u) = 1$ and $c = a$. Observe then the following:

$$\begin{aligned} \hat{\delta}(0, w) =& \hat{\delta}(0, ua) && [w = uc, c = a] \\ =& \delta(\hat{\delta}(0, u), a) && [\hat{\delta}\ def] \\ =& \delta(1, a) && [\hat{\delta}(0, u) = 1] \\ =& 2 && [\delta\ def] \end{aligned}$$

Further, because $\hat{\delta}(0, u) = 1$, the inductive hypothesis guarantees for us that $\#a(u) = 3z + 1$ for some integer z. As a result:

$$\begin{aligned} \#a(w) =& \#a(ua) && [w = uc, c = a] \\ =& \#a(u) + 1 && [\#a\ def] \\ =& 3z + 2 && [\#a(u) = 3z + 1] \end{aligned}$$

Thus $\hat{\delta}(0, w) = 2$ and $\#a(w) = 3z+2$ for some integer z. These propositions satisfy both sides of $C(n+1)$'s biconditional, rednering $C(n+1)$ true. At the same time, Because $\hat{\delta}(0, w)$ is not 0 or 1 and a number of the form $3z+2$ cannot be written as $3z'$ or $3z'+1$ for any integer z', if follows that both sides of $A(n+1)$ and $B(n+1)$'s biconditionals are false, rendering both $A(n+1)$ and $B(n+1)$ true.

Subcase $\hat{\delta}(0, u) = 1, c = b$ Suppose that $\hat{\delta}(0, u) = 1$ and $c = b$. Observe then the following:

$$\begin{aligned} \hat{\delta}(0, w) =& \hat{\delta}(0, ub) && [w = uc, c = b] \\ =& \delta(\hat{\delta}(0, u), b) && [\hat{\delta}\ def] \\ =& \delta(1, b) && [\hat{\delta}(0, u) = 1] \\ =& 1 && [\delta\ def] \end{aligned}$$

Further, because $\hat{\delta}(0, u) = 1$, the inductive hypothesis guarantees for us that $\#a(u) = 3z + 1$ for some integer z. As a result:

$$\begin{aligned} \#a(w) =& \#a(ub) && [w = uc, c = b] \\ =& \#a(u) && [\#a\ def] \\ =& 3z + 1 && [\#a(u) = 3z + 1] \end{aligned}$$

Thus $\hat{\delta}(0, w) = 1$ and $\#a(w) = 3z+1$ for some integer z. These propositions satisfy both sides of $B(n+1)$'s biconditional, rednering $B(n+1)$ true. At the same time, Because $\hat{\delta}(0, w)$ is not 0 or 2 and a number of the form $3z+1$ cannot be written as $3z'$ or $3z'+2$ for any integer z', if follows that both sides of $A(n+1)$ and $C(n+1)$'s biconditionals are false, rendering both $A(n+1)$ and $C(n+1)$ true.

Subcase $\hat{\delta}(0, u) = 2, c = a$ Suppose that $\hat{\delta}(0, u) = 2$ and $c = a$. Observe then the following:

$$\begin{aligned}
\hat{\delta}(0, w) =& \hat{\delta}(0, ua) && [w = uc, c = a] \\
=& \delta(\hat{\delta}(0, u), a) && [\hat{\delta}\ def] \\
=& \delta(2, a) && [\hat{\delta}(0, u) = 2] \\
=& 0 && [\delta\ def]
\end{aligned}$$

Further, because $\hat{\delta}(0, u) = 2$, the inductive hypothesis guarantees for us that $\#a(u) = 3z + 2$ for some integer z. As a result:

$$\begin{aligned}
\#a(w) =& \#a(ua) && [w = uc, c = a] \\
=& \#a(u) + 1 && [\#a\ def] \\
=& 3z + 3 && [\#a(u) = 3z + 2] \\
=& 3(z + 1) && [math]
\end{aligned}$$

Thus $\hat{\delta}(0, w) = 0$ and $\#a(w) = 3(z + 1)$ for some integer z. These propositions satisfy both sides of $A(n+1)$'s biconditional, rednering $A(n+1)$ true. At the same time, Because $\hat{\delta}(0, w)$ is not 1 or 2 and a number of the form $3z'$ cannot be written as $3z''$ or $3z''+1$ for any integer z'', if follows that both sides of $B(n+1)$ and $C(n+1)$'s biconditionals are false, rendering both $B(n+1)$ and $C(n+1)$ true.

Subcase $\hat{\delta}(0, u) = 2, c = b$ Suppose that $\hat{\delta}(0, u) = 2$ and $c = b$. Observe then the following:

$$\begin{aligned}
\hat{\delta}(0, w) =& \hat{\delta}(0, ub) && [w = uc, c = b] \\
=& \delta(\hat{\delta}(0, u), b) && [\hat{\delta}\ def] \\
=& \delta(2, b) && [\hat{\delta}(0, u) = 2] \\
=& 2 && [\delta\ def]
\end{aligned}$$

Further, because $\hat{\delta}(0, u) = 2$, the inductive hypothesis guarantees for us that $\#a(u) = 3z + 2$ for some integer z. As a result:

$$\begin{aligned}
\#a(w) =& \#a(ub) && [w = uc, c = b] \\
=& \#a(u) && [\#a\ def] \\
=& 3z + 2 && [\#a(u) = 3z + 2]
\end{aligned}$$

Thus $\hat{\delta}(0, w) = 2$ and $\#a(w) = 3z+2$ for some integer z. These propositions satisfy both sides of $C(n+1)$'s biconditional, rednering $C(n+1)$ true. At the same time, Because $\hat{\delta}(0, w)$ is not 0 or 1 and a number of the form $3z+2$ cannot be written as $3z'$ or $3z'+1$ for any integer z', if follows that both sides of $A(n+1)$ and $B(n+1)$'s biconditionals are false, rendering both $A(n+1)$ and $B(n+1)$ true.

Conclusion Thus, by mutual induction, $A(n)$, $B(n)$, and $C(n)$ hold for all naturals n.

Now observe that the following identities hold for the language of M:[3]

$$
\begin{aligned}
&\mathcal{L}(M) \\
=&\{w \in \{a, b\}^* \mid \hat{\delta}(0, w) \in \{1, 2\}\} && [\mathcal{L}\ def] \\
=&\{w \in \{a, b\}^* \mid \hat{\delta}(0, w) = 1 \lor \delta(0, w) = 2\} && [logic] \\
=&\{w \in \{a, b\}^* \mid \hat{(}\exists z \in \mathbb{Z}.\, \#a(w) = 3z+1) \lor (\exists z \in \mathbb{Z}.\, \#a(w) = 3z+2)\} && [B(|w|), C(|w|)]
\end{aligned}
$$

This confirms the desired identity for the language of M.

□

This is not a necessary step, but if you wanted to prove that a number of the form $3z$ cannot be written as $3z'+1$, here is how you would do so. (A similar technique works for other forms, like $3z'+2$, and you could even generalize it to other coefficients and summands if you so desired.)

Consider the proposition that $3z = 3z'+1$ for some integers z, z'. The following logical equivalences hold:

$$
\begin{aligned}
&3z = 3z' + 1 \\
\iff &3z - 3z' = 1 && [algebra] \\
\iff &z - z' = \frac{1}{3} && [algebra]
\end{aligned}
$$

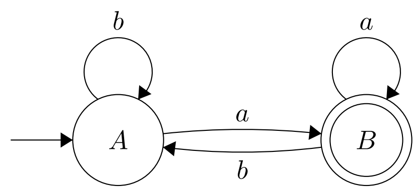
But note that integers are closed under subtraction, so $z - z'$ must be an integer, yet $\frac{1}{3}$ is not an integer. Thus the last equality in the above chain has to be false; an integer cannot be equal to a non-integer.

Since $3z = 3z'+1 \leftrightarrow z - z' = \frac{1}{3}$, and the righthand side of this biconditional is false, it must also be that $3z = 3z'+1$ is false, i.e., $3z \neq 3z'+1$. As a result, any number that is equal to $3z$ for some integer z cannot also be equal to $3z'+1$ for any integer z'.

[3]Note how the predicate A is not actually used for this reasoning. We needed it to prove B and C held in the first place, but now we no longer need it here. This is common when performing mutual induction; you usually only care about some of the predicates in the end, but more are needed to make the induction work. This is also common with induction in general; you sometimes need to induct with stronger predicates to make the proof work.

Mutual Induction (Red)

Let M be given by the following DFA:



Theorem 2. $\mathcal{L}(M) = \{w \in \{a,b\}^* \mid \exists u \in \{a,b\}^*.\, w = ua\}$

Proof. This proposition is proven by first mutually inducting with the following predicates:

$$Q(n) := \forall w \in \{a,b\}^*.\, |w| = n \to (\hat{\delta}(A,w) = A \leftrightarrow (w = \epsilon \vee \exists u \in \{a,b\}^*.\, w = ub))$$

$$R(n) := \forall w \in \{a,b\}^*.\, |w| = n \to (\hat{\delta}(A,w) = B \leftrightarrow \exists u \in \{a,b\}^*.\, w = ua)$$

Base Case $n = 0$ Let w be an arbitrary string over the alphabet $\{a,b\}$ that is of length 0. There is only one such string, the empty string, so $w = \epsilon$ and $\hat{\delta}(A,w) = \hat{\delta}(A,\epsilon)$. Further by the definition of $\hat{\delta}$, we find that $\hat{\delta}(A,\epsilon) = A$.

Thus, both sides of $Q(0)$'s biconditional are satisfied, rendering $Q(0)$ true. At the same time, since $A \neq B$ and ϵ does not end in b, both sides of $R(0)$'s biconditional are false, rendering $R(0)$ true.

Inductive Case Suppose for the inductive hypothesis that $Q(n)$ and $R(n)$ hold for some natural n. We want to now show $Q(n+1)$ and $R(n+1)$.

Let w be an arbitrary string of length $n+1$. Since $|w| > 0$, we know $w = vc$ for some $v \in \{a,b\}^*$ and $c \in \{a,b\}$.

We now proceed by cases on the result of $\hat{\delta}(A,v)$ and the identity of c.

Subcase $\hat{\delta}(A,v) = A$ **and** $c = a$ In this case the following identities hold:

$$\begin{aligned}
\hat{\delta}(A,w) =& \hat{\delta}(A,va) && [w = vc, c = a] \\
=& \delta(\hat{\delta}(A,v),a) && [\hat{\delta}\ def] \\
=& \delta(A,a) && [\hat{\delta}(A,v) = A] \\
=& B && [\delta\ def]
\end{aligned}$$

At the same time, since $\hat{\delta}(A,v) = A$, the inductive hypothesis tells us that $v = \epsilon$ or $v = ub$ for some string $u \in \{a,b\}^*$. Then $w = a$ or $w = uba$, which in either case means that the righthand side of $R(n+1)$'s biconditional is true. This leaves both sides of $R(n+1)$'s biconditional true, rendering $R(n+1)$ true.

Similarly, since $\hat{\delta}(A,w) \neq A$ and w is a non-empty string that does not end in b, both sides of $Q(n+1)$'s biconditional are false, rendering $Q(n+1)$ true.

Subcase $\hat{\delta}(A, v) = B$ and $c = a$ In this case the following identities hold:

$$\begin{aligned}
\hat{\delta}(A, w) =& \hat{\delta}(A, va) && [w = vc, c = a] \\
=& \delta(\hat{\delta}(A, v), a) && [\hat{\delta}\ def] \\
=& \delta(B, a) && [\hat{\delta}(A, v) = B] \\
=& B && [\delta\ def]
\end{aligned}$$

At the same time, since $\hat{\delta}(A, v) = B$, the inductive hypothesis tells us that $v = ua$ for some string $u \in \{a, b\}^*$. Then $w = uaa$, so the string ua witnesses that the righthand side of $R(n + 1)$'s biconditional is true. This leaves both sides of $R(n + 1)$'s biconditional true, rendering $R(n + 1)$ true.

Similarly, since $\hat{\delta}(A, w) \neq A$ and w is a non-empty string that does not end in b, both sides of $Q(n + 1)$'s biconditional are false, rendering $Q(n + 1)$ true.

Subcase $\hat{\delta}(A, v) = A$ and $c = b$ In this case the following identities hold:

$$\begin{aligned}
\hat{\delta}(A, w) =& \hat{\delta}(A, vb) && [w = vc, c = b] \\
=& \delta(\hat{\delta}(A, v), b) && [\hat{\delta}\ def] \\
=& \delta(A, b) && [\hat{\delta}(A, v) = A] \\
=& A && [\delta\ def]
\end{aligned}$$

At the same time, since $\hat{\delta}(A, v) = A$, the inductive hypothesis tells us that $v = \epsilon$ or $v = ub$ for some string $u \in \{a, b\}^*$. Then $w = b$ or $w = ubb$, either of which witnesses that the righthand disjunct of the righthand side of $Q(n+1)$'s biconditional is true. This leaves both sides of $Q(n + 1)$'s biconditional true, rendering $Q(n + 1)$ true.

Similarly, since $\hat{\delta}(A, w) \neq B$ and w is a non-empty string ending in a, both sides of $R(n + 1)$'s biconditional are false, rendering $R(n + 1)$ true.

Subcase $\hat{\delta}(A, v) = B$ and $c = b$ In this case the following identities hold:

$$\begin{aligned}
\hat{\delta}(A, w) =& \hat{\delta}(A, vb) && [w = vc, c = b] \\
=& \delta(\hat{\delta}(A, v), b) && [\hat{\delta}\ def] \\
=& \delta(B, b) && [\hat{\delta}(A, v) = B] \\
=& A && [\delta\ def]
\end{aligned}$$

At the same time, since $\hat{\delta}(A, v) = A$, the inductive hypothesis tells us that $v = ua$ for some string $u \in \{a, b\}^*$. Then $w = uba$, so the string ua witnesses that the righthand side of $Q(n + 1)$'s biconditional is true. This leaves both sides of $Q(n + 1)$'s biconditional true, rendering $Q(n + 1)$ true.

Similarly, since $\hat{\delta}(A, w) \neq A$ and w is a non-empty string ending in b, both sides of $R(n + 1)$'s biconditional are false, rendering $R(n + 1)$ true.

Conclusion Thus, by mutual induction, $\forall n \in \mathbb{N}.\, Q(n) \land R(n)$. In particular, the fact that $\forall n \in \mathbb{N}.\, R(n)$ allows us to conclude what the language of the automaton M is as follows:

$$\begin{aligned}
\mathcal{L}(M) =& \{w \in \{a,b\}^* \mid \hat{\delta}(A,w) \in \{B\}\} && [\mathcal{L}\ def] \\
=& \{w \in \{a,b\}^* \mid \hat{\delta}(A,w) = B\} && [logic] \\
=& \{w \in \{a,b\}^* \mid \exists u \in \{a,b\}^*.\, w = ub\} && [R(|w|)]
\end{aligned}$$

$\square$

Funnily enough, I actually made this DFA too easy. No induction is needed to prove the language, and this can be noticed in the proof by how the inductive hypothesis did not really play a role—it never mattered what v was, only that $w = va$ or $w = vb$.

If we never actually need the inductive hypothesis, then this is a sign that the statement can be proven directly instead. But double check this sign! Failing to use the inductive hypothesis could also just mean that your reasoning has gone wrong. In this case, the key property could actually have been proven directly by making the same casing as the above proof, just without any reference to the inductive hypothesis.