# Induction Proofs

CS 234

## 0 Introduction

This document contains examples of good proofs based on the induction activity completed in class. These are 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 Proofs

## Strong Induction (Blue)

```
1  def pow(n,k):
2      if k == 0:
3          return 1
4      elif k % 2 != 0:
5          return n * pow(n,k-1)
6      else:
7          x = pow(n,k//2)
8          return x * x
```

For this problem, let $0^0 = 1$.

**Theorem 1.** $\forall n, k \in \mathbb{N}.\, \texttt{pow}(n, k) = n^k$

*Proof.* The proof of this statement follows by induction over the parameter $k$. Let the inductive predicate be defined as follows:[1]

$$P(k) := \forall n \in \mathbb{N}.\, \texttt{pow}(n, k) = n^k$$

**Base Case $k = 0$:** Consider $\texttt{pow}(n, 0)$ for some arbitrary natural $n$. Because the second argument is 0, the condition on line 2 will be true, and thus $\texttt{pow}(n, 0)$ will return 1 according to line 3. Thus $\texttt{pow}(n, 0) = 1$. Because $n^0 = 1$ as well for any $n$, it follows by definition that $P(0)$ holds.

**Inductive Case:** For the inductive hypothesis, assume $P(k)$ holds for all $0 \leq k \leq m$ for some natural $m$. We want to show that $\texttt{pow}(n, m + 1) = n^{m+1}$ for any arbitrary natural $n$.

Note that since $m \geq 0$, it follows that $m + 1 \neq 0$, so the conditional on line 2 is never met. We now proceed by cases on whether $m + 1$ is even:

**Subcase $m + 1$ odd** Suppose $m + 1$ is odd. Then the following equalities hold:[2]

$$\begin{aligned} \texttt{pow}(n, m+1) &= n * \texttt{pow}(n, m) && [\textit{line 4 cond. true}] \\ &= n * n^m && [IH] \\ &= n^{m+1} && [\textit{math}] \end{aligned}$$

Therefore $\texttt{pow}(n, m + 1) = n^{m+1}$ and $P(m + 1)$ holds by definition in this case.

[1] Even though $n$ is a natural number too, we don't induct on it. This is because we can just prove the universal quantification for $n$ directly when inducting with $k$.

[2] I combine some of the computation, like defining $x$, into a single step here. This is ok for small amounts of computation.

**Subcase $m+1$ even** Suppose $m+1$ is even. Then the following equalities hold:

$$\begin{aligned}
\texttt{pow}(n, m+1) =& \texttt{pow}(n, (m+1)//2) * \texttt{pow}(n, (m+1)//2) && [line\ 4\ cond.\ false] \\
=& \texttt{pow}(n, (m+1)/2) * \texttt{pow}(n, (m+1)/2) && [m+1\ even] \\
=& n^{\frac{m+1}{2}} * n^{\frac{m+1}{2}} && [IH] \\
=& n^{m+1} && [math]
\end{aligned}$$

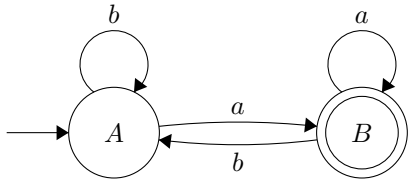
Note that we can apply the inductive hypothesis because $\frac{m+1}{2}$ is guaranteed to be a natural number due to $m+1$ being even, and that natural number must be between 0 and $m$ (inclusive) since $m+1$ is positive and at least 1.

Therefore $\texttt{pow}(n, m+1) = n^{m+1}$ and $P(m+1)$ holds by definition in this case too.

**Conclusion:** Because both the base case and inductive case hold, induction allows us to conclude $\forall n, k \in \mathbb{N}.\, \texttt{pow}(n, k) = n^k$. □

## 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 $\epsilon$ 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, $\forall n \in \mathbb{N}. Q(n) \wedge R(n)$. 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:

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

□

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.