Proofs By Construction

Alyssa Lytle

Fall 2025

For a proof by construction, you're going to prove something exists by *constructing* it and then by proving it satisfies whatever property you're trying to prove.

It should have three clear elements: the construction, the property you want to prove about the construction (WTP), and the proof.

Example 1

Let $w^{\mathcal{R}}$ represent the string w in reverse order. Prove by construction that, for any language A, with $A^{\mathcal{R}} = \{w^{\mathcal{R}} | w \in A\}$, if A is regular, then so is $A^{\mathcal{R}}$.

You want to use the the automaton M that accepts A to construct a new automaton $M_{\mathcal{R}}$ and prove that $x \in L(M) \iff x^{\mathcal{R}} \in M_{\mathcal{R}}$.

So, for our proof by construction we would:

1. Construct a new automaton $M_{\mathcal{R}}$
2. We want to prove that for any x accepted by M, its reverse $x^{\mathcal{R}}$ would be accepted by $M_{\mathcal{R}}$
   WTP: $x \in L(M) \iff x^{\mathcal{R}} \in M_{\mathcal{R}}$
3. Prove that $x \in L(M) \iff x^{\mathcal{R}} \in M_{\mathcal{R}}$.

Part 1: Construction

Let A be a regular language. By the definition of regular language, there exists an NFA $M = (Q, \Sigma, \Delta, S, F)$ such that $L(M) = A$.

We will construct an NFA $M_{\mathcal{R}} = (Q, \Sigma, \Delta', S', F')$ such that:

- $\Delta'(q, a) = \{\, p \in Q \mid \; q \in \Delta(p, a)\,\}$. (Essentially, Δ' is the opposite mapping of Δ. If p maps to q over a in Δ, the q maps to p over a in Δ')
- $S' = F$. (The set of start states S' is M's accept states F.)
- $F' = S$. (The set of accept states F' is M's start states S.)

Part 2: Want to Prove (WTP)

We want to prove $\forall x, x \in L(M) \iff x^{\mathcal{R}} \in L(M_{\mathcal{R}})$.

Part 3: Proof

Since this is an $\iff$ statement, we should prove this in both directions, however, you'll see that both proofs are equivalent, so you can just do one direction (Right arrow proof or Left arrow proof).

Right arrow proof: $\forall x, x \in L(M) \implies x^{\mathcal{R}} \in L(M_{\mathcal{R}})$

$$\forall x, x \in L(M) \quad \text{(Given)} \tag{1}$$

$$\exists \text{ a sequence of states } r_0, r_1, \ldots, r_n \text{ such that: } r_0 \in S,\ r_n \in F,$$
$$\text{and } \Delta(r_i, w_{i+1}) = r_{i+1} \text{ for } i = 0, \ldots, n-1 \quad \text{(Definition of acceptance)} \tag{2}$$

$$\exists \text{ a sequence of states } r_n, r_{n-1}, \ldots, r_0 \text{ such that: } r_0 \in S,\ r_n \in F,$$
$$\text{and } \Delta'(r_{i+1}, w_{i+1}) = r_i \text{ for } i = 0, \ldots, n-1 \quad \text{(Applied definition of } \Delta' \text{ from construction)} \tag{3}$$

$$\exists \text{ a sequence of states } r_n, r_{n-1}, \ldots, r_0 \text{ such that: } r_0 \in F',\ r_n \in S',$$
$$\text{and } \Delta'(r_{i+1}, w_{i+1}) = r_i \text{ for } i = 0, \ldots, n-1 \quad \text{(Plugged in } S' = F \text{ and } F' = S \text{ from construction)} \tag{4}$$

$$\forall x, x \in L(M_{\mathcal{R}}) \square \quad \text{(Definition of acceptance)} \tag{5}$$

Left arrow proof: $\forall x, x^{\mathcal{R}} \in L(M_{\mathcal{R}}) \implies x \in L(M)$

$$\forall x, x^{\mathcal{R}} \in L(M_{\mathcal{R}}) \quad \text{(Given)} \tag{1}$$

$$\exists \text{ a sequence of states } r_0, r_1, \ldots, r_n \text{ such that: } r_0 \in S',\ r_n \in F',$$
$$\text{and } \Delta'(r_i, w_{i+1}) = r_{i+1} \text{ for } i = 0, \ldots, n-1 \quad \text{(Definition of acceptance)} \tag{2}$$

$$\exists \text{ a sequence of states } r_n, r_{n-1}, \ldots, r_0 \text{ such that: } r_0 \in S,\ r_n \in F,$$
$$\text{and } \Delta(r_{i+1}, w_{i+1}) = r_i \text{ for } i = 0, \ldots, n-1 \quad \text{(Applied definition of } \Delta \text{ from construction)} \tag{3}$$

$$\exists \text{ a sequence of states } r_n, r_{n-1}, \ldots, r_0 \text{ such that: } r_0 \in S',\ r_n \in F',$$
$$\text{and } \Delta(r_{i+1}, w_{i+1}) = r_i \text{ for } i = 0, \ldots, n-1 \quad \text{(Plugged in } S' = F \text{ and } F' = S \text{ from construction)} \tag{4}$$

$$\forall x, x^{\mathcal{R}} \in L(M) \square \quad \text{(Definition of acceptance)} \tag{5}$$