Oberlin College
CSCI 383
Fall 2026
Lecture 3. An Automaton for Multiples of 3
Kozen - Sections 3 and 4

Last Time: A *deterministic finite automaton* (DFA) is a quintouple $M = (Q, \Sigma, \delta, s, F)$:

- Q is the *state space* (finite set)
- Σ is the input alphabet (finite set)
- $\delta : Q \times \Sigma \to Q$ is the *transition function*.
- s is the *start state*
- $F \subseteq Q$ is the set of *accept states*.

Def: The *language* $L(M)$ of a DFA M is the set of strings accepted by M.

A language A is *regular* if there exists some DFA M for which $L(M) = A$.

Today:

- Practice with definition.
- Formal analysis.

A question to think about: what languages are regular? What aren't?

Exercise: Given the following formal definition, build the transition diagram.

- $Q = \{0, 1, 2\}$
- $\Sigma = \{\mathtt{0}, \mathtt{1}\}$
- $\delta(0, \mathtt{0}) = 0$, $\delta(0, \mathtt{1}) = 1$, $\delta(1, \mathtt{0}) = 2$ $\delta(1, \mathtt{1}) = 0$, $\delta(2, \mathtt{0}) = 1$, $\delta(2, \mathtt{1}) = 2$.
- $s = 0$
- $F = \{0\}$

What language is this?

- 0?
- 1?
- 10?
- 11?
- 100?

Let $\#x$ be the number represented by x in binary.

Conjecture: Machine accepts binary strings x where $\#x \equiv 0 \mod 3$.

How would we prove this?

Inductive Extension

Idea: Keep track of where the automaton is after reading a prefix.

Informal: $\hat{\delta}(q, x)$ = where M is after reading x, starting in state q.

Example: What is $\hat{\delta}(2,\texttt{001})$?

Formal (recursive!) definition:

- $\hat{\delta}(q, \varepsilon) = q$
- $\hat{\delta}(q, xa) = \delta(\hat{\delta}(q, x), a)$

Formal definition of acceptance: $\hat{\delta}(s, x) \in F$

Let's return to our example.

- What is $\hat{\delta}(0, \texttt{0})$?
- $\hat{\delta}(0, \texttt{1})$?

etc.

Lemma: $\hat{\delta}(0, x) = \#x \mod 3$.

Proof: Structural induction.

- $x = \varepsilon$: $\#x = 0$. Hooray.
- $x = ya$.
  - Case 1: $\#y \equiv 0 \mod 3, a = 0$.
  - $\Rightarrow \#y = 3c$ for some c
  - $\Rightarrow \#x = 2(3c) + 0$
  - $\Rightarrow \#x = 3(2c)$.
  - $\Rightarrow \#x \equiv 0 \mod 3$

  - But then: $\hat{\delta}(0, ya) = \delta(\hat{\delta}(0, y), a) = \delta(0, 0) = 0$

  - Case 2: $\#y \equiv 0 \mod 3, a = 1$.
  - $\Rightarrow \#y = 3c$ for some c
  - $\Rightarrow \#x = 2(3c) + 1$
  - $\Rightarrow \#x = 3(2c) + 1$.
  - $\Rightarrow \#x \equiv 1 \mod 3$

  - But then: $\hat{\delta}(0, ya) = \delta(\hat{\delta}(0, y), a) = \delta(0, 1) = 1$

  - Case 3: $\#y \equiv 1 \mod 3, a = 0$.
  - $\Rightarrow \#y = 3c + 1$ for some c
  - $\Rightarrow \#x = 2(3c + 1) + 0$
  - $\Rightarrow \#x = 3(2c) + 2$.
  - $\Rightarrow \#x \equiv 2 \mod 3$

- But then: $\hat{\delta}(0, ya) = \delta(\hat{\delta}(0, y), a) = \delta(2, 0) = 0$

What are the other 3 cases?

Theorem: $L(M) = \{x \,|\, \#x \equiv 0 \mod 3\}$

Proof:

- $x \in L(M) \iff \hat{\delta}(0, x) = 0$
- $\Leftrightarrow x \equiv 0 \mod 3$.

General Approach for Proving Your DFA Works:

1. Figure out an interpretation of your states ("the current state represents the prefix we've read, mod 3")
2. Prove a corresponding lemma about $\hat{\delta}$ ("$\hat{\delta}(0, x) = \#x \mod 3$.")
3. Use your lemma to prove $L(M)$ is the desired language. ("$L(M) = \{x \,|\, \#x \equiv 0 \mod 3\}$")

Alternative proof of the lemma assuming we were designing the DFA

Proof. Since we designed the DFA, we know that $\delta(q, a) = 2q + a \mod 3$. (Check the table of the transition function to verify this fact.)

The proof proceeds by structural induction on the input string x. The base case is the same: if $x = \varepsilon$, then $\#x = 0$ and $\hat{\delta}(0, x) = 0$ as required.

The inductive step is much simpler as we do not need to consider 6 cases, we just do some algebraic manipulation. Assume $x = ya$ for $x \in \Sigma^*$ and $y \in \Sigma$. By the inductive hypothesis, we know $\hat{\delta}(0, y) = \#y \bmod 3$. We can plug that and the definition of δ into the definition of $\hat{\delta}$. Specifically,

$$\begin{aligned}
\hat{\delta}(0, x) &= \delta(\hat{\delta}(0, y), a) && \text{by definition of } \hat{\delta} \\
&= \delta(\#y \bmod 3, a) && \text{by inductive hypothesis} \\
&= [2(\#y \bmod 3) + a] \bmod 3 && \text{by definition of } \delta \\
&= [2(\#y) + a] \bmod 3 && \text{by modular arithmetic} \\
&= \#x \bmod 3 && \text{since } \#x = 2(\#y) + a. \square
\end{aligned}$$