Lecture 25: Constructing automata and proving them correct

Here is the automaton we presented last time, with alphabet $\Sigma = \{0, 1\}$:

Claim: $L(M) = \{ x \mid x \text{ has an odd number of 1's} \}$

Relevant definitions: Set equality $\equiv$, $L(M)$, and $x \in LHS$

Proof (attempt):

For all $x \in LHS$, work RHS

$\forall x \in \Sigma^*$, if $x \in LHS \text{ then } x \in RHS$

$\forall x \in \Sigma^*$, if $x \in RHS \text{ then } x \in LHS$

If $x \in LHS$, then $x \in RHS$.

By induction on $n$. Let $P(n)$ be "if $x \in LHS$ then $x \in RHS$".

Induction step: $P(n)$ implies $P(n+1)$.

We'll show $P(n)$ and $P(n+1)$ assuming $P(n)$.

$P(n)$: $x \in LHS$ implies $x$ has an odd number of 1's.

(i.e. $x \in LHS$ if $x \in \Sigma^*$ and $x$ has odd number of 1's.

Since $x \in \Sigma^*$, $x$ is vacuously true.

$P(n+1)$, assuming $P(n)$:

$x \in LHS$ if $x \in \Sigma^*$ and $x$ has odd number of 1's.

$\implies$ We assume $x \in \Sigma^*$ and $x$ has odd number of 1's.

Well $\delta(q_0, xa) = \delta(\delta(q_0, x), a)$

[knowing] $P(x)$ says if $x = 0$, then $x \in \Sigma^*$ has odd number of 1's.

There are two ways for $\delta(q_0, xa) = q_1$:

1. $a = 0$, $\delta(q_0, x) = q_1$.
   - In this case, $P(x)$ says $x$ has odd number of 1's, so $xa = x0$ has same (odd) number of 1's.

2. $a = 1$, $\delta(q_0, x) = q_0$
   - If $\delta(q_0, x) = q_0$ then...
   - Stuck!
Let \( P(x) \) be the statement:

1. If \( P(x) = 0 \), then \( x \) has an odd number of 1's.
2. If \( P(x) = 1 \), then \( x \) has an even number of 1's.

\( P(0) \) is vacuously true, because \( \delta(0,0) \) is not defined.

\( P(1) \):

\( P(0) \) and \( P(1) \), assume \( P(x) \)

- Assume \( \delta(g_0,0) = 0 \):
  - Either \( \delta(g_0,0) = 0 \) and \( a = 0 \)
  - or \( \delta(g_0,0) = 1 \) and \( a = 1 \)
  - know \( \delta(g_0,0) = 0 \), so by \( P(0) \), \( a \) is even.
  - we conclude \( x \) has even 1's.
  - so \( x \) is \( \text{even} \) (has one more 1 than \( \delta(0,0) \)).
  - so \( x \) is \( \text{even} \), so \( x \) has odd \#1's.

- Assume \( \delta(g_0,0) = 1 \):
  - \( \delta(g_0,0) = 0 \), so \( x \) has even \#1's
  - \( \delta(0,0) = 0 \) has even \#1's.

\( \delta(g_1,0) = 1 \), so \( x \) has odd \#1's

- \( \delta(0,0) = 1 \), so \( x \) has even \#1's.

Claim: \( L(M) = \{ x \mid x \text{ has odd } \#1 \text{\'s} \} \)

Subclaim: \( \forall \pi, \text{ if } \delta(g_0,0) = 0, \text{ then } x \text{ has even } \#1 \text{\'s} \)

- \( \delta(g_0,0) = 0 \), so \( x \) has odd \#1's.

Proof of Claim: \( \forall \pi, x \in \text{LHS} \text{ and } \forall \pi \notin \text{LHS}, x \notin \text{RHS}. \)

- If \( x \in \text{LHS} \), then \( \delta(g_0,0) = 0 \), so \( x \) has odd \#1's.

- If \( x \notin \text{LHS} \), then \( \delta(g_0,0) = 0 \), so \( x \) has even \#1's.
A general construction

Problem

Definition: A language $L$ is just a set of strings (i.e., a subset of $\Sigma^*$).

Definition: A language $L$ is DFA-recognizable if there exists a DFA $M$ with $L = L(M)$.

Claim: The intersection of two DFA-recognizable languages is DFA-recognizable.

Proof: Assume $L_1$ is DFA-recognizable and $L_2$ is DFA-recognizable.

Let $M_1$ be the DFA for $L_1$, and let $M_2$ be the DFA for $L_2$.

Let $M = M_1 \cap M_2$, which is a DFA with $L(M) = L_1 \cap L_2$.

Define $M$ as follows:

$M = (Q, \Sigma, \delta, q_0, A_1 \cap A_2)$

where $Q, \Sigma, q_0, A_1, A_2$ are defined as for $M_1$ and $M_2$.

The transition function $\delta$ of $M$ is defined by:

$\delta((q, x), a) = (\delta_1((q, x), a), \delta_2((q, x), a))$

Claim: $L(M) = L_1 \cap L_2$.

Proof: Let $P(x)$ be the statement:

"If $P(x)$ then $x \in L_1 \cap L_2$.

Equivalently, let $P(x)$ be the statement:

"$\delta((q_0, x), a) = (q_1, q_2)$ and $q_1 \in A_1$ and $q_2 \in A_2$.

$P(\varepsilon)$ and $P(a)$ imply $P(\varepsilon \cdot a)$.

Proof: Assume $P(x)$:

Let $\delta(x)$ be the transition function.

Then $\delta((q_0, x), a) = (\delta_1((q_0, x), a), \delta_2((q_0, x), a))$.

Well, $\delta((q_0, x), a) = \delta((\delta_1((q_0, x), a), \delta_2((q_0, x), a)))$ by $P(a)$.

Therefore, $\delta((q_0, x), a) = \delta((q_1, q_2), a)$ by definition.
Know: $δ(q_0, x) = (δ_1(q_0, x), δ_2(q_0, x))$

well $L(M) = L(M_1) \cup L(M_2)$

$= \{ x \mid δ(q_0, x) ∈ A_1 \}$

$= \{ x \mid (δ_1(q_0, x), δ_2(q_0, x)) ∈ A \}$

$= \{ x \mid \text{δ}_1(q_0, x) ∈ A_1 \text{ and } δ_2(q_0, x) ∈ A_2 \}$

$= L(M_1) \cup L(M_2)$