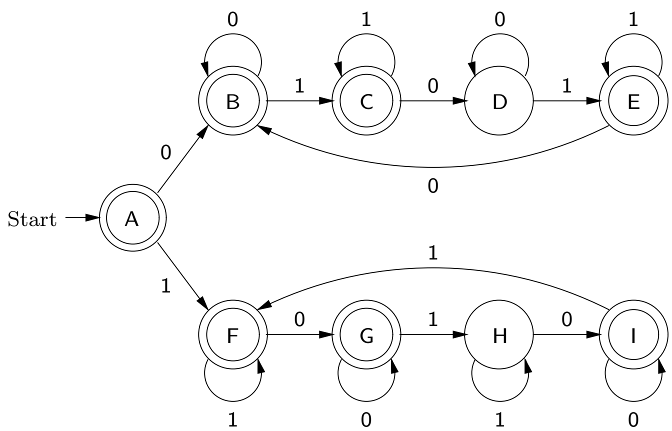
CS 516—Software Foundations via Formal Languages—Spring 2025

Problem Set 5

Model Answers

Problem 1

(a)



(b) We have that, for all $w \in \{0, 1\}^*$:

- $w \in X$ iff $\mathbf{zo}\, w$ is even or $\mathbf{oz}\, w$ is even; and
- $w \notin X$ iff $\mathbf{zo}\, w$ is odd and $\mathbf{oz}\, w$ is odd.

Because **alphabet** $M = \{0, 1\}$, we have that $\Lambda_{M,q} \subseteq \{0, 1\}^*$ for all $q \in Q_M$.

Lemma PS5.1.1

(A) For all $w \in \Lambda_{\mathsf{A}}$, $w = \%$.

(B) For all $w \in \Lambda_{\mathsf{B}}$, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is even and 0 is a suffix of w.

(C) For all $w \in \Lambda_{\mathsf{C}}$, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is even and 1 is a suffix of w.

(D) For all $w \in \Lambda_{\mathsf{D}}$, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is odd and 0 is a suffix of w.

(E) For all $w \in \Lambda_{\mathsf{E}}$, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is odd and 1 is a suffix of w.

(F) For all $w \in \Lambda_{\mathsf{F}}$, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is even and 1 is a suffix of w.

(G) For all $w \in \Lambda_{\mathsf{G}}$, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is odd and 0 is a suffix of w.

(H) For all $w \in \Lambda_{\mathsf{H}}$, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is odd and 1 is a suffix of w.

(I) *For all* $w \in \Lambda_{\mathsf{I}}$, $\mathbf{zo}\,w$ *is odd,* $\mathbf{oz}\,w$ *is even and* $\mathsf{0}$ *is a suffix of* w.

Proof. We proceed by induction on Λ. There are 19 parts to show.

- (empty string) We have that $\% = \%$.
- $(\mathsf{A}, \mathsf{0} \to \mathsf{B})$ Suppose $w \in \Lambda_{\mathsf{A}}$ and assume the inductive hypothesis, $w = \%$. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w = \mathbf{zo}\,\% = 0$ is even, $\mathbf{oz}(w\mathsf{0}) = 0$ is even, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{A}, \mathsf{1} \to \mathsf{F})$ Suppose $w \in \Lambda_{\mathsf{A}}$ and assume the inductive hypothesis, $w = \%$. We have that $\mathbf{zo}(w\mathsf{1}) = 0$ is even, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w = \mathbf{oz}\,\% = 0$ is even, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.
- $(\mathsf{B}, \mathsf{0} \to \mathsf{B})$ Suppose $w \in \Lambda_{\mathsf{B}}$ (so that $w \in \{\mathsf{0}, \mathsf{1}\}^*$) and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is even and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w$ is even, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\,w$ is even, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{B}, \mathsf{1} \to \mathsf{C})$ Suppose $w \in \Lambda_{\mathsf{B}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is even and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\,w + 1$ is odd, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w$ is even, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.
- $(\mathsf{C}, \mathsf{0} \to \mathsf{D})$ Suppose $w \in \Lambda_{\mathsf{C}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is odd, $\mathbf{oz}\,w$ is even and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w$ is odd, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\,w + 1$ is odd, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{C}, \mathsf{1} \to \mathsf{C})$ Suppose $w \in \Lambda_{\mathsf{C}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is odd, $\mathbf{oz}\,w$ is even and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\,w$ is odd, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w$ is even, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.
- $(\mathsf{D}, \mathsf{0} \to \mathsf{D})$ Suppose $w \in \Lambda_{\mathsf{D}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is odd, $\mathbf{oz}\,w$ is odd and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w$ is odd, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\,w$ is odd, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{D}, \mathsf{1} \to \mathsf{E})$ Suppose $w \in \Lambda_{\mathsf{D}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is odd, $\mathbf{oz}\,w$ is odd and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\,w + 1$ is even, and $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w$ is odd, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.
- $(\mathsf{E}, \mathsf{0} \to \mathsf{B})$ Suppose $w \in \Lambda_{\mathsf{E}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is odd and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w$ is even, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}(w\mathsf{0}) + 1$ is even, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{E}, \mathsf{1} \to \mathsf{E})$ Suppose $w \in \Lambda_{\mathsf{E}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is odd and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\,w$ is even, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w$ is odd, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.
- $(\mathsf{F}, \mathsf{0} \to \mathsf{G})$ Suppose $w \in \Lambda_{\mathsf{F}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is even and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\,w$ is even, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\,w + 1$ is odd, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.
- $(\mathsf{F}, \mathsf{1} \to \mathsf{F})$ Suppose $w \in \Lambda_{\mathsf{F}}$ and assume the inductive hypothesis, $\mathbf{zo}\,w$ is even, $\mathbf{oz}\,w$ is even and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\,w$ is even, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\,w$ is even, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.

- $(\mathsf{G}, \mathsf{0} \to \mathsf{G})$ Suppose $w \in \Lambda_{\mathsf{G}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is odd and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\, w$ is even, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\, w$ is odd, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.

- $(\mathsf{G}, \mathsf{1} \to \mathsf{H})$ Suppose $w \in \Lambda_{\mathsf{G}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is even, $\mathbf{oz}\, w$ is odd and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\, w + 1$ is odd, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\, w$ is odd, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.

- $(\mathsf{H}, \mathsf{0} \to \mathsf{I})$ Suppose $w \in \Lambda_{\mathsf{H}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is odd and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\, w$ is odd, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\, w + 1$ is even, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.

- $(\mathsf{H}, \mathsf{1} \to \mathsf{H})$ Suppose $w \in \Lambda_{\mathsf{H}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is odd and $\mathsf{1}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\, w$ is odd, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\, w$ is odd, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.

- $(\mathsf{I}, \mathsf{0} \to \mathsf{I})$ Suppose $w \in \Lambda_{\mathsf{I}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is even and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{0}) = \mathbf{zo}\, w$ is odd, $\mathbf{oz}(w\mathsf{0}) = \mathbf{oz}\, w$ is even, and $\mathsf{0}$ is a suffix of $w\mathsf{0}$.

- $(\mathsf{I}, \mathsf{1} \to \mathsf{F})$ Suppose $w \in \Lambda_{\mathsf{I}}$ and assume the inductive hypothesis, $\mathbf{zo}\, w$ is odd, $\mathbf{oz}\, w$ is even and $\mathsf{0}$ is a suffix of w. We have that $\mathbf{zo}(w\mathsf{1}) = \mathbf{zo}\, w + 1$ is even, $\mathbf{oz}(w\mathsf{1}) = \mathbf{oz}\, w$ is even, and $\mathsf{1}$ is a suffix of $w\mathsf{1}$.

□

Now, we use Lemma PS5.1.1 to prove that $L(M) = X$.

- $(L(M) \subseteq X)$ Suppose $w \in L(M)$. Hence $w \in L(M) = \bigcup\{\, \Lambda_q \mid q \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{E}, \mathsf{F}, \mathsf{G}, \mathsf{I}\} \,\}$, so that $w \in \Lambda_q$ for some $q \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{E}, \mathsf{F}, \mathsf{G}, \mathsf{I}\}$, and thus $w \in (\mathbf{alphabet}\, M)^* = \{\mathsf{0}, \mathsf{1}\}^*$. Thus, there are seven cases to consider.
  - Suppose $q = \mathsf{A}$. Then $w \in \Lambda_{\mathsf{A}}$, so that $w = \%$, by Lemma PS5.1.1(A). Hence $\mathbf{zo}\, w = \mathbf{zo}\, \% = 0$ is even, so that $w \in X$.
  - Suppose $q = \mathsf{B}$. Then $w \in \Lambda_{\mathsf{B}}$, so that $\mathbf{zo}\, w$ is even, by Lemma PS5.1.1(B). Hence $w \in X$.
  - Suppose $q = \mathsf{C}$. Then $w \in \Lambda_{\mathsf{C}}$, so that $\mathbf{oz}\, w$ is even, by Lemma PS5.1.1(C). Hence $w \in X$.
  - Suppose $q = \mathsf{E}$. Then $w \in \Lambda_{\mathsf{E}}$, so that $\mathbf{zo}\, w$ is even, by Lemma PS5.1.1(E). Hence $w \in X$.
  - Suppose $q = \mathsf{F}$. Then $w \in \Lambda_{\mathsf{F}}$, so that $\mathbf{zo}\, w$ is even, by Lemma PS5.1.1(F). Hence $w \in X$.
  - Suppose $q = \mathsf{G}$. Then $w \in \Lambda_{\mathsf{G}}$, so that $\mathbf{zo}\, w$ is even, by Lemma PS5.1.1(G). Hence $w \in X$.
  - Suppose $q = \mathsf{I}$. Then $w \in \Lambda_{\mathsf{I}}$, so that $\mathbf{oz}\, w$ is even, by Lemma PS5.1.1(I). Hence $w \in X$.

- $(X \subseteq L(M))$ Suppose $w \in X$. Since $X \subseteq \{\mathsf{0}, \mathsf{1}\}^*$, we have that $w \in \{\mathsf{0}, \mathsf{1}\}^*$. Suppose, toward a contradiction, that $w \notin L(M)$. Thus $w \notin L(M) = \bigcup\{\, \Lambda_q \mid q \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{E}, \mathsf{F}, \mathsf{G}, \mathsf{I}\} \,\}$. But $w \in \{\mathsf{0}, \mathsf{1}\}^* = (\mathbf{alphabet}\, M)^* = \bigcup\{\, \Lambda_q \mid q \in Q_M \,\}$, so that $w \in \Lambda_{\mathsf{D}} \cup \Lambda_{\mathsf{H}}$. Thus there are two cases to consider.

– Suppose $w \in \Lambda_{\mathsf{D}}$. Thus **zo** w is odd and **oz** w is odd, by Lemma PS5.1.1(D). Hence $w \notin X$—contradiction.

– Suppose $w \in \Lambda_{\mathsf{H}}$. Thus **zo** w is odd and **oz** w is odd, by Lemma PS5.1.1(H). Hence $w \notin X$—contradiction.

Because we achieved a contradiction in both cases, we have an overall contradiction. Thus $w \in L(M)$.

Problem 2

First we put the Forlan description

```
{states} A, B {start state} A {accepting states} A
{transitions}
A, 0 -> B; A, 1 -> A;
B, 0 -> B; B, 1 -> A
```

of N in the file `ps5-p2-dfa` and load it into Forlan:

```
- val dfa = DFA.input "ps5-p2-dfa";
val dfa = - : dfa
```

Then we proceed as follows, trying all permutations on states using both unrestricted local and global simplification as the simplification method, with tracing turned on:

```
- fun simpLoc reg = #2(Reg.locallySimplify (NONE, Reg.obviousSubset) reg);
val simpLoc = fn : reg -> reg
- fun simpGlob reg = #2(Reg.globallySimplify (NONE, Reg.obviousSubset) reg);
val simpGlob = fn : reg -> reg
- val reg1 = faToRegPermsTrace (NONE, simpLoc) (injDFAToFA dfa);
using renaming "(A, A), (B, B)"
found regular expression "1*(% + 0(0 + 1)*1)"
simplest regular expression so far is "1*(% + 0(0 + 1)*1)"
using renaming "(A, B), (B, A)"
found regular expression "% + (0 + 1)*1"
simplest regular expression so far is "% + (0 + 1)*1"
val reg1 = - : reg
- Reg.output("", reg1);
% + (0 + 1)*1
val it = () : unit
- val reg2 = faToRegPermsTrace (NONE, simpGlob) (injDFAToFA dfa);
using renaming "(A, A), (B, B)"
found regular expression "1*(% + 0(0 + 1)*1)"
simplest regular expression so far is "1*(% + 0(0 + 1)*1)"
using renaming "(A, B), (B, A)"
found regular expression "% + (0 + 1)*1"
simplest regular expression so far is "% + (0 + 1)*1"
val reg2 = - : reg
- Reg.output("", reg2);
```

```
% + (0 + 1)*1
val it = () : unit
```

Note that both simplification methods gave the same result: $\% + (\mathsf{0} + \mathsf{1})^*\mathsf{1}$.

Problem 3

We disprove the statement, showing that there exists a regular language L such that there is no reversible DFA M such that $L(M) = L$. Let $L = \{\mathsf{0}\}$. We have that L is a regular language because $L = L(\mathsf{0})$. We prove that there does not exist a reversible DFA M such that $L(M) = L$.

Suppose, toward a contradiction, that there is a reversible DFA M such that $L(M) = L$. Since $\mathsf{0} \in L = L(M)$, we have that $\mathsf{0} \in \textbf{alphabet}\, M$. Define $f \in \mathbb{N} \to Q_M$ by:

$$f\, n = \delta_M(s_M, \mathsf{0}^n).$$

Below, we write δ, s, A and T for δ_M, s_M, A_M and T_M, respectively.

We have that $f\, 0 = \delta(s, \mathsf{0}^0) = \delta(s, \%) = s$.

To see that, for all $n \in \mathbb{N}$, $(f\, n, \mathsf{0}, f(n+1)) \in T$, suppose $n \in \mathbb{N}$. We have $f(n+1) = \delta(s, \mathsf{0}^{n+1}) = \delta(s, \mathsf{0}^n\mathsf{0}) = \delta(\delta(s, \mathsf{0}^n), \mathsf{0}) = \delta(f\, n, \mathsf{0})$, showing that $\delta(f\, n, \mathsf{0}) = f(n+1)$, and thus that $(f\, n, \mathsf{0}, f(n+1)) \in T$.

Since Q is finite, there are $i, j \in \mathbb{N}$ such that $i < j$ but $f\, i = f\, j$. Let $n \in \mathbb{N}$ be least that there is an $m \in \mathbb{N}$ such that $m < n$ and $f\, m = f\, n$. Fix such an m. Then $n \geq 1$ and, (†) for all $i, j \in \mathbb{N}$, if $i < j < n$, then $f\, i \neq f\, j$. There are two cases to consider.

- Suppose $m = 0$. Then $\delta(s, \mathsf{0}^{n+1}) = \delta(s, \mathsf{0}^n\mathsf{0}) = \delta(\delta(s, \mathsf{0}^n), \mathsf{0}) = \delta(f\, n, \mathsf{0}) = \delta(f\, m, \mathsf{0}) = \delta(f\, 0, \mathsf{0}) = \delta(s, \mathsf{0}) \in A$, since $\mathsf{0} \in L = L(M)$. Thus $\mathsf{0}^{n+1} \in L(M) = L = \{\mathsf{0}\}$, so that $\mathsf{0}^{n+1} = \mathsf{0} = \mathsf{0}^1$, and thus $n + 1 = 1$. But then $n = 0$, contradicting the fact that $n \geq 1$.

- Suppose $m \geq 1$. Thus $m-1 \in \mathbb{N}$. And $n-1 \in \mathbb{N}$, since $n \geq 1$. We have $(f(m-1), \mathsf{0}, f((m-1)+1)) \in T$, so that $(f(m-1), \mathsf{0}, f\, m) \in T$. We also have $(f(n-1), \mathsf{0}, f((n-1)+1)) \in T$, so that $(f(n-1), \mathsf{0}, f\, n) \in T$. But $f\, n = f\, m$, so that $(f(n-1), \mathsf{0}, f\, m) \in T$. Because $(f(m-1), \mathsf{0}, f\, m)$ and $(f(n-1), \mathsf{0}, f\, m)$ are in T and M is reversible, it follows that $f(m-1) = f(n-1)$. But $m - 1 < n - 1 < n$, since $m < n$, and thus $f(m-1) \neq f(n-1)$ by (†)—contradiction.

Since we obtained a contradiction in both cases, we have an overall contradiction. Thus there does not exist a reversible DFA M such that $L(M) = L$.