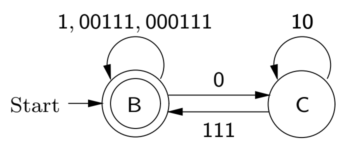
CS 516—Software Foundations via Formal Languages—Spring 2025

Problem Set 4

Model Answers

Problem 1

(a) The finite automaton M is



(b) First, we put the expression of M in Forlan's syntax

```
{states} B, C {start state} B {accepting states} B
{transitions}
B, 0 -> C; B, 1 -> B; B, 00111 -> B; B, 000111 -> B;
C, 10 -> C; C, 111 -> B
```

in the file `ps4-p1-fa` (see the course website), and load this file into Forlan, calling the result `fa`:

```
- val fa = FA.input "ps4-p1-fa";
val fa = - : fa
```

Next we load the file `ps4-p1.sml`

```
val A = StrSet.fromString "001, 011, 101, 111";

(* val inB : str -> bool

   tests whether a string over the alphabet {0, 1} is in B *)

fun inB nil       = true
  | inB (b :: bs) =
      if Sym.equal(b, Sym.fromString "0")
      then Set.exists (fn x => Str.prefix(x, bs)) A andalso
           inB bs
      else inB bs

(* val upto : int -> str set

   if n >= 0, then upto n returns all strings over alphabet {0, 1} of
   length no more than n *)
```

```
fun upto 0 : str set = Set.sing nil
  | upto n           =
      let val xs = upto(n - 1)
          val ys = Set.filter (fn x => length x = n - 1) xs
      in StrSet.union
         (xs, StrSet.concat(StrSet.fromString "0, 1", ys))
      end;

(* val partition : int -> str set * str set

   if n >= 0, then partition n returns (xs, ys) where:

   xs is all elements of upto n that are in B; and

   ys is all elements of upto n that are not in B *)

fun partition n = Set.partition inB (upto n);

(* val test = fn : int -> fa -> str option * str option

   if n >= 0, then test n returns a function f such that, for all FAs
   fa, f fa returns a pair (xOpt, yOpt) such that:

     If there is an element of {0, 1}* of length no more than n that
     is in B but is not accepted by fa, then xOpt = SOME x for some
     such x; otherwise, xOpt = NONE.

     If there is an element of {0, 1}* of length no more than n that
     is not in B but is accepted by fa, then yOpt = SOME y for some
     such y; otherwise, yOpt = NONE. *)

fun test n =
      let val (goods, bads) = partition n
      in fn fa =>
              let val accepted      = FA.accepted fa
                  val goodNotAccOpt = Set.position (not o accepted) goods
                  val badAccOpt     = Set.position accepted bads
              in ((case goodNotAccOpt of
                        NONE   => NONE
                      | SOME i => SOME(ListAux.sub(Set.toList goods, i))),
                  (case badAccOpt of
                        NONE   => NONE
                      | SOME i => SOME(ListAux.sub(Set.toList bads, i))))
              end
      end;
```

(see the course website) defining the function `test` into Forlan:

```
- use "ps4-p1.sml";
```

```
[opening ps4-p1.sml]
val A = - : str set
val inB = fn : sym list -> bool
val upto = fn : int -> str set
val partition = fn : int -> sym list set * sym list set
val test = fn : int -> fa -> sym list option * sym list option
val it = () : unit
```

Finally, we apply `test` to arguments 20 and `fa`:

```
- test 20 fa;
val it = (NONE,NONE) : sym list option * sym list option
```

Problem 2

(a) Let $C = \{\, w \in \{0,1\}^* \mid 0 \text{ is a suffix of } w \text{ and, for all } x, y \in \{0,1\}^*, \text{ if } w = x0y, \text{ then } y \in \{\%, 10\} \text{ or there is a } z \in A \text{ such that } z \text{ is a prefix of } y \,\}$. For example, 0 and 010 are both elements of C, even though they are not elements of B.

Lemma PS4.2.1
If $w \in B$, then either

- *$w = \%$; or*
- *$w = x1$, for some $x \in B$; or*
- *$w = x00111$, for some $x \in B$; or*
- *$w = x000111$, for some $x \in B$; or*
- *$w = x111$, for some $x \in C$.*

Proof. Suppose $w \in B$. If $w = \%$, then we are done, so suppose $w \neq \%$. Since $w \in B$, w cannot end in 0, so $w = t1$ for some $t \in \{0,1\}^*$. If $t \in B$, then we are done, so suppose $t \notin B$. Thus $t = y0z$ for some $y, z \in \{0,1\}^*$ such that there is no $u \in A$ such that u is a prefix of z. Thus $w = t1 = y0z1$. Because $w \in B$, there is an element of A that is a prefix of $z1$. Since the elements of A all have length 3, it follows that $|z| \geq 2$. If $|z| \geq 3$, then the fact that an element of A is a prefix of $z1$ would imply that it is also a prefix of z—contradiction. Thus $|z| = 2$. Because $w = y0z1$ and $w \in B$, z cannot be 00, 01 or 10, as then w would have a 0 not followed by at least three symbols. Thus $z = 11$, so that $w = y0z1 = y0111$. y cannot end with more than two occurrences of 0, as a string having 0000 as a substring cannot be in B. Thus we have the following three cases to consider.

- Suppose $y = s00$, for some $s \in \{0,1\}^*$ that does not end with a 0. Thus $w = y0111 = s000111$, and it will suffice to show that $s \in B$. Suppose $u, v \in \{0,1\}^*$ and $s = u0v$. We must show that there is an element of A that is a prefix of v. We have that $w = u0v000111$.

  Suppose, toward a contradiction, that $|v| \leq 2$. If $v = \%$ or v ends in a 0, then 0000 is a substring of w—contradiction. Otherwise, $v \in \{1, 01, 11\}$. If $v = 1$, then $w = u0(1000111)$, but no element of A is a prefix of 1000111—contradiction. If $v = 01$, then $w = u0(01000111)$, but no element of A is a prefix of 01000111—contradiction. Finally, if $v = 11$, then $w = u0(11000111)$, but no element of A is a prefix of $\mathsf{11000111}$—contradiction. Since we obtained a contradiction in all cases, we have an overall contradiction. Thus $|v| \geq 3$.

Since $w = u\mathsf{0}(v\mathsf{000111})$ and $w \in B$, it follows that there is an $r \in A$ such that r is a prefix of $v\mathsf{000111}$. But $|v| \geq 3$, and thus r is also a prefix of v.

- Suppose $y = s\mathsf{0}$, for some $s \in \{\mathsf{0}, \mathsf{1}\}^*$ that does not end with a $\mathsf{0}$. Thus $w = y\mathsf{0111} = s\mathsf{00111}$, so it will suffice to show that $s \in B$. Suppose $u, v \in \{\mathsf{0}, \mathsf{1}\}^*$ and $s = u\mathsf{0}v$. We must show that there is an element of A that is a prefix of v. We have that $w = u\mathsf{0}(v\mathsf{00111})$.

  Suppose, toward a contradiction, that $|v| \leq 2$. If $v = \%$ or v ends in a $\mathsf{0}$, then $s = u\mathsf{0}v$ ends in a $\mathsf{0}$—contradiction. Otherwise, $v \in \{\mathsf{1}, \mathsf{01}, \mathsf{11}\}$. If $v = \mathsf{1}$, then $w = u\mathsf{0}(\mathsf{100111})$, but there is no element of A that is a prefix of $\mathsf{100111}$—contradiction. If $v = \mathsf{01}$, then $w = u\mathsf{0}(\mathsf{0100111})$, but there is no element of A that is a prefix of $\mathsf{0100111}$. And if $v = \mathsf{11}$, then $w = u\mathsf{0}(\mathsf{1100111})$, but there is no element of A that is a prefix of $\mathsf{1100111}$. Since we obtained a contradiction in each case, we have an overall contradiction. Thus $|v| \geq 3$.

  Since $w = u\mathsf{0}(v\mathsf{00111})$ and $w \in B$, it follows that there is an $r \in A$ such that r is a prefix of $v\mathsf{00111}$. But $|v| \geq 3$, and thus r is also a prefix of v.

- Suppose y does not end with a $\mathsf{0}$. Since $w = y\mathsf{0111} = (y\mathsf{0})(\mathsf{111})$, it will suffice to show that $y\mathsf{0} \in C$. Clearly $y\mathsf{0}$ ends in a $\mathsf{0}$. So suppose $u, v \in \{\mathsf{0}, \mathsf{1}\}^*$ and $y\mathsf{0} = u\mathsf{0}v$. We must show that $v \in \{\%, \mathsf{10}\}$ or there is an element of A that is a prefix of v. If $v = \%$, then we are done. So suppose $v \neq \%$. Since $y\mathsf{0} = u\mathsf{0}v$, it follows that $v = v'\mathsf{0}$ for some $v' \in \{\mathsf{0}, \mathsf{1}\}^*$. Because $y\mathsf{0} = u\mathsf{0}v = u\mathsf{0}v'\mathsf{0}$, it follows that $y = u\mathsf{0}v'$ and $w = u\mathsf{0}v'\mathsf{0111}$. We must show that $v'\mathsf{0} \in \{\%, \mathsf{10}\}$ or there is an element of A that is a prefix of $v'\mathsf{0}$. Suppose $|v'| \geq 2$. Since $w = u\mathsf{0}(v'\mathsf{0111})$ and $w \in B$, we have that there is an element of A that is a prefix of $v'\mathsf{0111}$. But $|v'\mathsf{0}| \geq 3$, and thus this prefix is also a prefix of $v'\mathsf{0}$. Otherwise, we have $|v'| \leq 1$. We cannot have $v' = \%$ or $v' = \mathsf{0}$, because then $y = u\mathsf{0}v'$ ends in $\mathsf{0}$—contradiction. So $v' = \mathsf{1}$. But then $v'\mathsf{0} = \mathsf{10} \in \{\%, \mathsf{10}\}$, and we are done.

□

Lemma PS4.2.2
If $w \in C$, then either

- *$w = x\mathsf{0}$, for some $x \in B$; or*
- *$w = x\mathsf{10}$, for some $x \in C$.*

Proof. Suppose $w \in C$. Thus $w = x\mathsf{0}$ for some $x \in \{\mathsf{0}, \mathsf{1}\}^*$. If $x \in B$, then we are done, so suppose $x \notin B$. Thus $x = u\mathsf{0}v$ for some $u, v \in \{\mathsf{0}, \mathsf{1}\}^*$ such that there is no $z \in A$ such that z is a prefix of v. Thus $w = u\mathsf{0}v\mathsf{0}$.

Suppose, toward a contradiction, that $v = \%$ or $\mathsf{0}$ is a suffix of v. Then $\mathsf{00}$ is a suffix of $w \in C$, so that $\mathsf{0} \in \{\%, \mathsf{10}\}$ or there is a $z \in A$ such that z is a prefix of $\mathsf{0}$—contradiction. Thus $|v| \geq 1$ and $\mathsf{0}$ is not a suffix of v.

Suppose, toward a contradiction, that $|v| \geq 2$. Then $|v\mathsf{0}| \geq 3$. Since $u\mathsf{0}(v\mathsf{0}) = w \in C$, either $v\mathsf{0} \in \{\%, \mathsf{10}\}$ or there is a $z \in A$ such that z is a prefix of $v\mathsf{0}$. The first case is impossible because

$|v0| \geq 3$. So we have that z is a prefix of $v0$, for some $z \in A$. If $|v0| = 3$, we have our contradiction, since all elements of A end in 1. And if $|v0| > 3$, then z is a prefix of v—contradiction. Thus $|v| \leq 1$.

Summarizing, we know that $|v| = 1$ and v does not end in 0. Hence $v = 1$, and $w = u0v0 = (u0)10$. It will suffice show that that $u0 \in C$. Clearly $u0$ ends in 0. Suppose $r, s \in \{0,1\}^*$ and $u0 = r0s$. We must show that $s \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of s. If $s = \%$, then we are done. So suppose $s \neq \%$. Since $u0 = r0s$, it follows that $s = s'0$ for some $s' \in \{0,1\}^*$. Thus $w = u010 = r0s10 = r0s'010$, and we must show that $s'0 \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of $s'0$. $s' \neq \%$, as otherwise we would have $r0(010) = r0s'010 = w \in C$, which is impossible. $s' \neq 0$, as otherwise we would have $(r0)0(010) = r0s'010 = w \in C$, which is impossible. Thus either $s' = 1$ or $|s'| \geq 2$, so there are two cases to consider.

- Suppose $s' = 1$. Then $s'0 = 10 \in \{\%, 10\}$.
- Suppose $|s'| \geq 2$. Then $|s'0| \geq 3$. Since $(r)0(s'010) = w \in C$, it follows that there is a $z \in A$ such that z is a prefix of $s'010$. But $|s'0| \geq 3$, and thus z is a prefix of $s'0$.

□

Lemma PS4.2.3
For all $w \in \{0,1\}^*$:

(B) if $w \in B$, then $w \in \Lambda_{\mathsf{B}}$;

(C) if $w \in C$, then $w \in \Lambda_{\mathsf{C}}$.

Proof. We proceed by strong string induction. Suppose $w \in \{0,1\}^*$, and assume the inductive hypothesis: for all $x \in \{0,1\}^*$, if x is a proper substring of w, then

(B) if $x \in B$, then $x \in \Lambda_{\mathsf{B}}$;

(C) if $x \in C$, then $x \in \Lambda_{\mathsf{C}}$.

We must show that

(B) if $w \in B$, then $w \in \Lambda_{\mathsf{B}}$;

(C) if $w \in C$, then $w \in \Lambda_{\mathsf{C}}$.

There are two parts to consider.

(B) Suppose $w \in B$. We must show that $w \in \Lambda_{\mathsf{B}}$. By Lemma PS4.2.1, there are five cases to consider.

- Suppose $w = \%$. Then $w = \% \in \Lambda_{\mathsf{B}}$, since B is M's start state.
- Suppose $w = x1$, for some $x \in B$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{B}}$. And $\mathsf{B}, 1 \to \mathsf{B} \in T_M$, so that $w = x1 \in \Lambda_{\mathsf{B}}$.
- Suppose $w = x00111$, for some $x \in B$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{B}}$. And $\mathsf{B}, 00111 \to \mathsf{B} \in T_M$, so that $w = x00111 \in \Lambda_{\mathsf{B}}$.
- Suppose $w = x000111$, for some $x \in B$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{B}}$. And $\mathsf{B}, 000111 \to \mathsf{B} \in T_M$, so that $w = x000111 \in \Lambda_{\mathsf{B}}$.

- Suppose $w = x\mathsf{111}$, for some $x \in C$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{C}}$. And $\mathsf{C}, \mathsf{111} \to \mathsf{B} \in T_M$, so that $w = x\mathsf{111} \in \Lambda_{\mathsf{B}}$.

(C) Suppose $w \in C$. We must show that $w \in \Lambda_{\mathsf{C}}$. By Lemma PS4.2.2, there are two cases to consider.

- Suppose $w = x\mathsf{0}$, for some $x \in B$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{B}}$. And $\mathsf{B}, \mathsf{0} \to \mathsf{C} \in T_M$, so that $w = x\mathsf{0} \in \Lambda_{\mathsf{C}}$.
- Suppose $w = x\mathsf{10}$, for some $x \in C$. By the inductive hypothesis, we have that $x \in \Lambda_{\mathsf{C}}$. And $\mathsf{C}, \mathsf{10} \to \mathsf{C} \in T_M$, so that $w = x\mathsf{10} \in \Lambda_{\mathsf{C}}$.

$\square$

Since B is M's only accepting state, we have that $L(M) = \Lambda_{\mathsf{B}}$, so that $B \subseteq \Lambda_{\mathsf{B}} = L(M)$, by Lemma PS4.2.3(B).

(b) Define C as in part (a).

Lemma PS4.2.4

(1) $\% \in B$.

(2) $B\{\mathsf{1}\} \subseteq B$.

(3) $B\{\mathsf{00111}\} \subseteq B$.

(4) $B\{\mathsf{000111}\} \subseteq B$.

(5) $B\{\mathsf{0}\} \subseteq C$.

(6) $C\{\mathsf{10}\} \subseteq C$.

(7) $C\{\mathsf{111}\} \subseteq B$.

Proof. From Section 3.2 of the slides and book, we know that, for all $x, y \in B$, $xy \in B$, and also that $\%$, $\mathsf{1}$, $\mathsf{0111}$, $\mathsf{00111}$ and $\mathsf{000111}$ are in B.

(1) ($\% \in B$) Clearly, $\% \in B$.

(2) ($B\{\mathsf{1}\} \subseteq B$) Suppose $w \in B\{\mathsf{1}\}$, so that $w = x\mathsf{1}$ for some $x \in B$. Because $x \in B$ and $\mathsf{1} \in B$, we have $w = x\mathsf{1} \in B$.

(3) ($B\{\mathsf{00111}\} \subseteq B$) Suppose $w \in B\{\mathsf{00111}\}$, so that $w = x(\mathsf{00111})$ for some $x \in B$. Because $x \in B$ and $\mathsf{00111} \in B$, we have $w = x(\mathsf{00111}) \in B$.

(4) ($B\{\mathsf{000111}\} \subseteq B$) Suppose $w \in B\{\mathsf{000111}\}$, so that $w = x(\mathsf{000111})$ for some $x \in B$. Because $x \in B$ and $\mathsf{000111} \in B$, we have $w = x(\mathsf{000111}) \in B$.

(5) $(B\{0\} \subseteq C)$ Suppose $w \in B\{0\}$, so that $w = x0$ for some $x \in B$. We must show that $w = x0 \in C$. Clearly, 0 is a suffix of $x0$. To complete the proof that $x0 \in C$, suppose $u, v \in \{0,1\}^*$ and $x0 = u0v$. We must show that $v \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of v. If $v = \%$, then we are done. Otherwise, because $x0 = u0v$, it follows that $v = v'0$ for some $v' \in \{0,1\}^*$. Since $x0 = u0v = u0v'0$, we have $x = u0v'$, so that $u0v' \in B$. We must show that $v'0 \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of $v'0$. Since $u0v' \in B$, there is a $z \in A$ such that z is a prefix of v'. So z is a prefix of $v'0$ and $z \in A$.

(6) $(C\{10\} \subseteq C)$ Suppose $w \in C\{10\}$ so that $w = x10$ for some $x \in C$. We must show that $w = x10 \in C$. Clearly 0 is a suffix of $x10$. Suppose $u, v \in \{0,1\}^*$ and $x10 = u0v$. We must show that $v \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of v. If $v = \%$ then we are done. Otherwise, because $x10 = u0v$, it follows that $v = v'0$ for some $v' \in \{0,1\}^*$. Since $x10 = u0v = u0v'0$, it follows that $x1 = u0v'$. We must show that $v'0 \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of $v'0$. Since $x1 = u0v'$, it follows that $v' = v''1$ for some $v'' \in \{0,1\}^*$. Because $x1 = u0v' = u0v''1$, it follows that $u0v'' = x \in C$. We must show that $v''10 \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of $v''10$. Since $u0v'' \in C$, either $v'' \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of v''. There are three cases to consider.

- Suppose $v'' = \%$. Then $v''10 = 10 \in \{\%, 10\}$.
- Suppose $v'' = 10$. Then $v''10 = 1010$, so that $101 \in A$ and 101 is a prefix of $v''10$.
- Suppose there is a $z \in A$ such that z is a prefix of v''. Then z is also a prefix of $v''10$.

(7) $(C\{111\} \subseteq B)$ Suppose $w \in C\{111\}$, so that $w = x111$ for some $x \in C$. We must show that $w = x111 \in B$. Suppose $u, v \in \{0,1\}^*$ and $x111 = u0v$. We must show that there is a $z \in A$ such that z is a prefix of v. Since $x111 = u0v$, we have that $v = v'1$ for some $v' \in \{0,1\}^*$. We must show that there is a $z \in A$ such that z is a prefix of $v'1$. Since $x111 = u0v = u0v'1$, it follows that $x11 = u0v'$. Consequently, $v' = v''1$ for some $v'' \in \{0,1\}^*$. We must show that there is a $z \in A$ such that z is a prefix of $v''11$. Since $x11 = u0v' = u0v''1$, we have that $x1 = u0v''$. Thus $v'' = v'''1$ for some $v''' \in \{0,1\}^*$. We must show that there is a $z \in A$ such that z is a prefix of $v'''111$. Since $x1 = u0v'' = u0v'''1$, we have that $u0v''' = x \in C$. Since $u0v''' \in C$, either $v''' \in \{\%, 10\}$ or there is a $z \in A$ such that z is a prefix of v'''. Thus there are three cases to consider.

- Suppose $v''' = \%$. Then 111 is a prefix of $111 = v'''111$ and $111 \in A$.
- Suppose $v''' = 10$. Then 101 is a prefix of $10111 = v'''111$ and $101 \in A$.
- Suppose there is a $z \in A$ such that z is a prefix of v'''. Then z is also a prefix of $v'''111$.

□

Lemma PS4.2.5

(B) For all $w \in \Lambda_{\mathsf{B}}$, $w \in B$.

(C) For all $w \in \Lambda_{\mathsf{C}}$, $w \in C$.

Proof. We proceed by induction on Λ. There are 7 (1 plus the number of transitions) parts to show.

(empty string) We have that $\% \in B$ by Lemma PS4.2.4(1), as required.

($\mathsf{B}, \mathsf{0} \to \mathsf{C}$) Suppose $w \in \Lambda_{\mathsf{B}}$, and assume the inductive hypothesis: $w \in B$. Then $w\mathsf{0} \in B\{\mathsf{0}\} \subseteq C$, by Lemma PS4.2.4(5), as required.

($\mathsf{B}, \mathsf{1} \to \mathsf{B}$) Suppose $w \in \Lambda_{\mathsf{B}}$, and assume the inductive hypothesis: $w \in B$. Then $w\mathsf{1} \in B\{\mathsf{1}\} \subseteq B$, by Lemma PS4.2.4(2), as required.

($\mathsf{B}, \mathsf{00111} \to \mathsf{B}$) Suppose $w \in \Lambda_{\mathsf{B}}$, and assume the inductive hypothesis: $w \in B$. Then $w(\mathsf{00111}) \in B\{\mathsf{00111}\} \subseteq B$, by Lemma PS4.2.4(3), as required.

($\mathsf{B}, \mathsf{000111} \to \mathsf{B}$) Suppose $w \in \Lambda_{\mathsf{B}}$, and assume the inductive hypothesis: $w \in B$. Then $w(\mathsf{000111}) \in B\{\mathsf{000111}\} \subseteq B$, by Lemma PS4.2.4(4), as required.

($\mathsf{C}, \mathsf{10} \to \mathsf{C}$) Suppose $w \in \Lambda_{\mathsf{C}}$, and assume the inductive hypothesis: $w \in C$. Then $w(\mathsf{10}) \in C\{\mathsf{10}\} \subseteq C$, by Lemma PS4.2.4(6), as required.

($\mathsf{C}, \mathsf{111} \to \mathsf{B}$) Suppose $w \in \Lambda_{\mathsf{C}}$, and assume the inductive hypothesis: $w \in C$. Then $w(\mathsf{111}) \in C\{\mathsf{111}\} \subseteq B$, by Lemma PS4.2.4(7), as required.

□

Since B is M's only accepting state, we have that $L(M) = \Lambda_{\mathsf{B}}$, so that $L(M) = \Lambda_{\mathsf{B}} \subseteq B$, by Lemma PS4.2.5(B).